

BSM 471-AĞ GÜVENLİĞİ

Hafta2: Ağ Güvenliği Test ve Denetim Araçları

Dr. Öğr. Üyesi Musa BALTA
Bilgisayar Mühendisliği Bölümü
Bilgisayar ve Bilişim Bilimleri Fakültesi

Haftalık İçerik

- Ağ dinleme araçları
- Port tarayıcılar
- Açıklık tarayıcılar
- Açıklık gerçekleştirme araçları
- Paket üreticileri
- Topoloji çıkarım araçları
- İşletim sistemi tespit araçları
- Şifre kırma araçları
- Kablosuz ağ araçları
- VPN test araçları
- Web güvenliği test araçları
- Veritabanı test araçları

Ağ Dinleme Araçları

- Ağ üzerindeki trafiği sezebilen, çözebilen ve değiştirebilen donanım ve yazılım araçlarının bir kombinasyonudur;
 - **Pasif izleme (sezme)**
 - **Aktif (atak yapma)**
- Hem ticari hem de ücretsiz sürümleri bulunmaktadır
- Genelde yazılım tabanlıdır.
- Sniffer olarak da bilinirler;
 - Ağ üzerindeki veriyi pasif olarak izleyen bir programdır.
 - Makineniz üzerinde çalışan uygulamalar ve protokoller tarafından gönderilen ya da alınan paketlerin bir kopyasını alır
- Yaygın kullanılan ağ protokolü analiz programları;
 - **Wireshark** , Ethereal , Windump, Ve diğerleri
- Sniffer programlarını efektif bir şekilde kullanmak için iyi bir ağ bilgisine sahip olmak gerekmektedir.

Ağ Dinleme Araçları (devam)

- **Sistem yöneticileri;**
 - Sistem problemlerini ve performansını anlama
 - Saldırıları tespit etme
 - Uygulama operasyonlarını test etme
- **Saldırganlar (Kötü niyetli kişiler);**
 - Protokoller üzerinden pasif olarak veri toplar
 - FTP, POP3, IMAP, SMTP, rlogin, HTTP, vb.
 - VoIP data
 - Hedef ağın trafiğini keşfeder
 - Trafik desenini keşfeder
 - Ağ içerisine dahil olur (backdoor teknikleri ile)

Ağ Dinleme Araçları (Wireshark)

- Gerald Combs tarafından Ethereal ismi ile başlatılan bir projedir.
- İlk versiyonu 1998 yılında yayınlanmıştır, Wireshark ismi haziran 2006'da verilmiştir.
- **Paket sniffer** uygulamasıdır, dolayısıyla bir ağın haritasını çıkartmak için kullanılamaz.
- Fonksiyonelliği tcpdump'a çok benzerdir ve diğer bir çok sniffer ile de uyumludur.
- Birçok bilgiyi sıralayan ve filtreleyen özelliklere, komut satırına ve grafik arabirimine sahiptir.
- **750'**nin üzerinde protokol destekler ve bu protokollerin yapısını gösterir.
- **Kapsüllemeli** bir yapıda görünüm sunar ve anlamlarını yorumlar.
- Sadece **pcap** tarafından desteklenen ağlar üzerinde veri yakalama yapabilir.
- Açık kaynak kodludur ve farklı işletim sistemleri üzerinde çalışabilir.
- İnternet ortamında bir çok online kaynak mevcuttur.
- Pasif bir izleme aracıdır, dolayısıyla ağ verisi üretmez.

Ağ Dinleme Araçları (Wireshark-WinPcap&libpcap)

Wireshark – Paketleri Snif etmek için uygulama

WinPcap – Paket yakalamak için açık kaynak kütüphanesi

Operating System – Windows & Unix/Linux

Network Card Drivers – Ethernet/WiFi Kartı

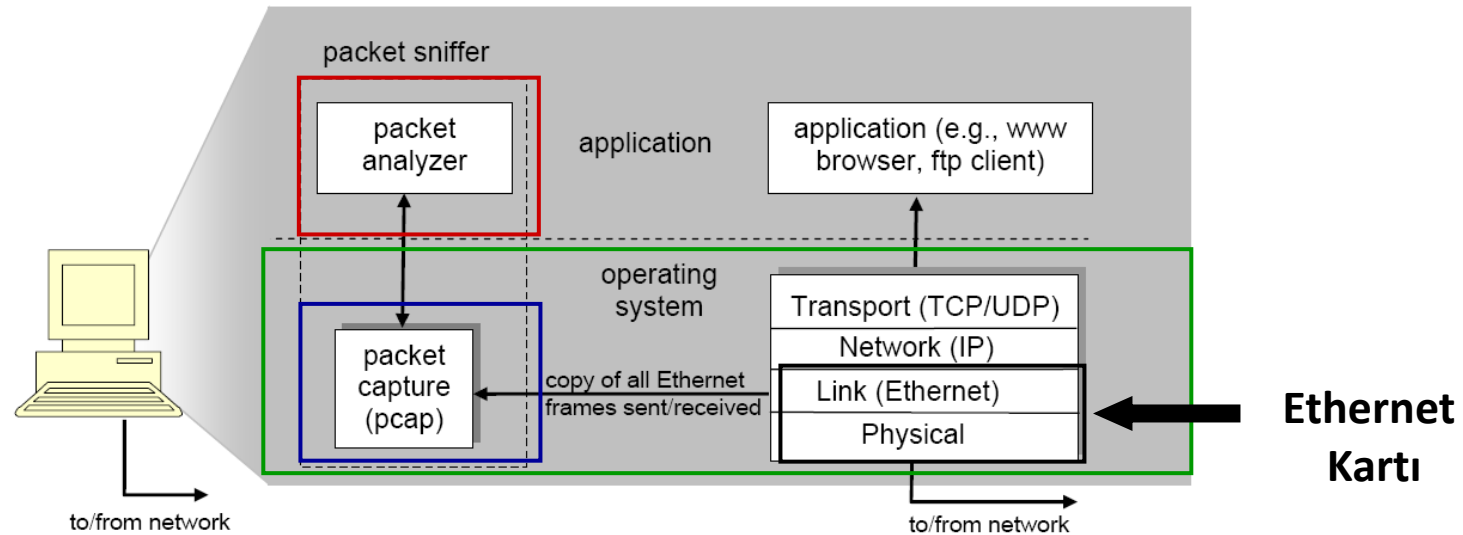
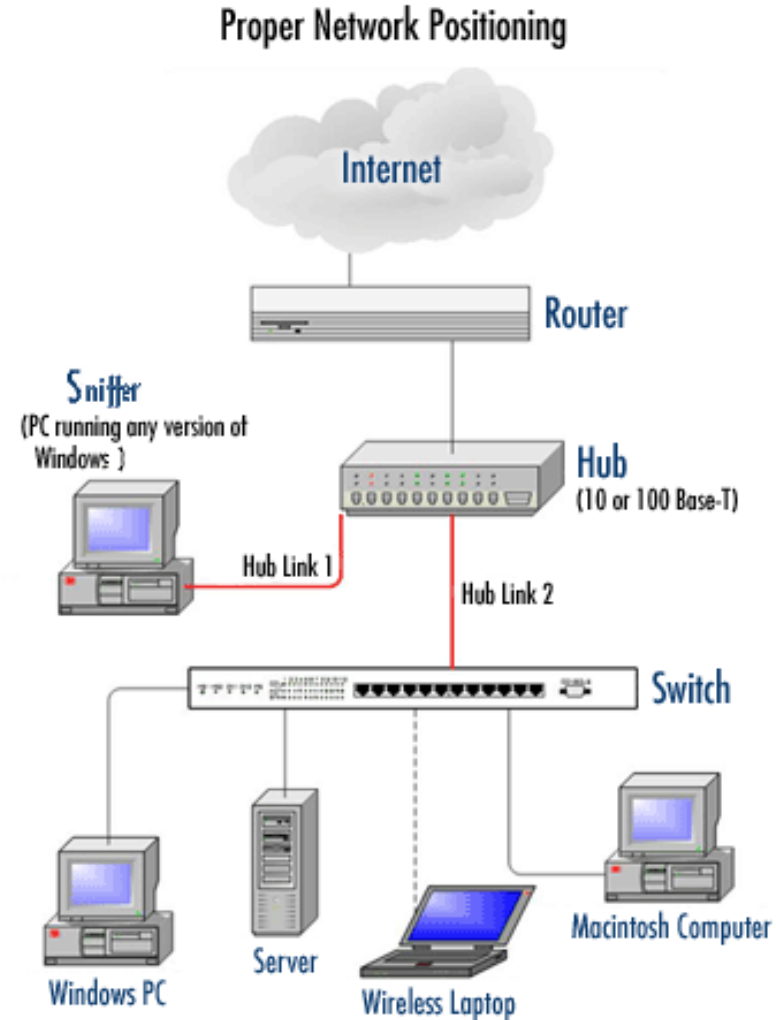
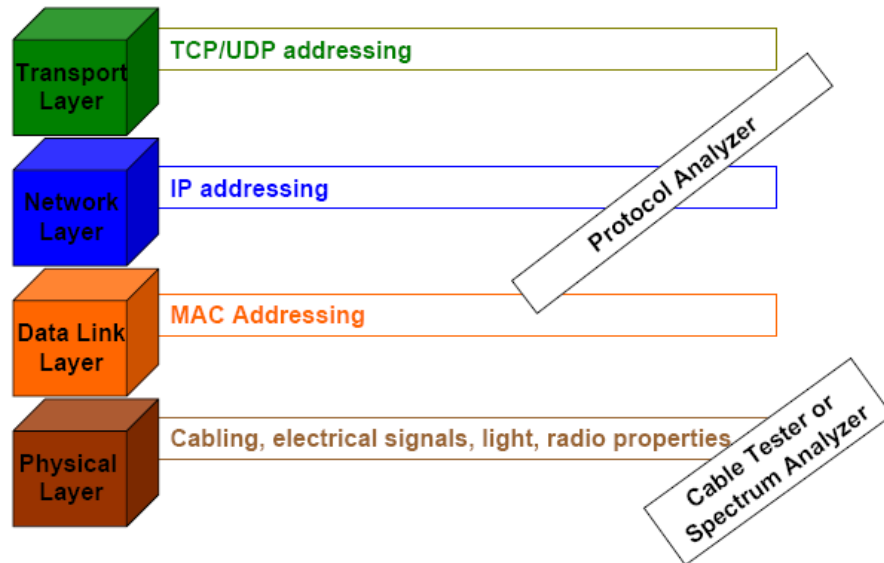


Figure 1: Packet sniffer structure

Ağ Dinleme Araçları (Sniffer ve Topolojideki Yeri)



Ağ Dinleme Araçları (Wireshark Kullanıcı Arayüzü)

The image shows the Wireshark network protocol analyzer interface. The main packet list displays several captured packets. A red circle highlights a specific packet (No. 6) with the following details:

| No. | Time | Source | Destination | Protocol | Info |
|-----|----------|-------------------|-------------------|----------|-------------------------------------|
| 2 | 0.002401 | Cisco-Li_f6:53:23 | Cisco-Li_7c:6a:35 | ARP | 192.168.1.1 is at 00:1a:70:f6:53:23 |
| 3 | 0.002432 | 192.168.1.103 | 68.105.28.12 | DNS | Standard query A www.google.com |
| 4 | 0.014577 | 68.105.28.12 | 192.168.1.103 | DNS | Standard query response CNAME ww |
| 5 | 0.015472 | 192.168.1.103 | 64.233.169.99 | TCP | 49591 > http [SYN] Seq=0 Len=0 M |
| 6 | 0.031934 | 64.233.169.99 | 192.168.1.103 | TCP | http > 49591 [SYN, ACK] Seq=0 Ac |

Below the packet list, a diagram illustrates the protocol stack layers for the selected packet:

- MAC Header
- IP Header
- TCP Header
- Data

Red arrows point from these labels to the corresponding sections in the packet details pane. The details pane shows the following structure:

- Frame (577 bytes on wire, 577 bytes captured)
- Ethernet II, Src: Cisco-Li_7c:6a:35 (00:14:bf:7c:6a:35), Dst: Cisco-Li_f6:53:23 (00:1a:70:f6:53:23)
- Internet Protocol, Src: 192.168.1.103 (192.168.1.103), Dst: 64.233.169.99 (64.233.169.99)
- Transmission Control Protocol, Src Port: 49591 (49591), Dst Port: http (80), Seq: 1, Ack: 1, Len: 523

The packet data is displayed in hexadecimal and ASCII. The ASCII column shows the text "MS IE7.0" and "ASCII equivalent of data".

File: "C:\Users\Joe\AppData\Local\Temp\etherXXXXa01124" 5905 Bytes 00:00... P: 17 D: 17 M: 0 Drops: 0

Port Tarayıcılar (Nmap)

- En yaygın olarak kullanılan port tarayıcı program **Nmap** yazılımıdır.
- Nmap, açık kaynak kodlu bir yazılım olup ücretsizdir.
- Hem Windows hem de Linux üzerinde çalışabilmektedir.
- Nmap programının en önemli özellikleri şunlardır:
 - TCP ve UDP port taraması yapabilmektedir.
 - İşletim sistemi tespiti yapabilmektedir.
 - Çalışan servisleri tespit edebilmektedir.
 - Yazılımların sürümünü tahmin edebilmektedir.
 - Bir ağdaki canlı bilgisayarları tespit edebilmektedir.
 - Raporlama yeteneği bulunmaktadır.

```
root@kali:~# nmap -help
Nmap 7.60 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
```

Base Syntax

nmap [ScanType] [Options] {targets}

Target Specification

IPv4 address: 192.168.1.1

IPv6 address: AABB:CCDD::FF%eth0

Host name: www.target.tgt

IP address range: 192.168.0-255.0-255

CIDR block: 192.168.0.0/16

Use file with lists of targets: -iL <filename>

Target Ports

No port range specified scans 1,000 most popular ports

- F Scan 100 most popular ports
- p<port1>-<port2> Port range
- p<port1>,<port2>,... Port List
- pU:53,U:110,T20-445 Mix TCP and UDP
- r Scan linearly (do not randomize ports)
- top-ports <n> Scan n most popular ports
- p-65535 Leaving off initial port makes Nmap scan start at port 1
- pO- Leaving off end port makes Nmap scan up to port 65535
- p- Leaving off start and end port makes Nmap scan ports 1-65535



Probing Options

- Pn Don't probe (assume all hosts are up)
- PB Default probe (TCP 80, 445 & ICMP)
- PS<portlist>
Check whether targets are up by probing TCP ports
- PE Use ICMP Echo Request
- PP Use ICMP Timestamp Request
- PM Use ICMP Netmask Request

Scan Types

- sn Probe only (host discovery, not port scan)
- sS SYN Scan
- sT TCP Connect Scan
- sU UDP Scan
- sV Version Scan
- O OS Detection
- scanflags Set custom list of TCP using URGACKPSHRSTSYNFIN in any order

Aggregate Timing Options

- T0 Paranoid: Very slow, used for IDS evasion
- T1 Sneaky: Quite slow, used for IDS evasion
- T2 Polite: Slows down to consume less bandwidth, runs ~10 times slower than default
- T3 Normal: Default, a dynamic timing model based on target responsiveness
- T4 Aggressive: Assumes a fast and reliable network and may overwhelm targets
- T5 Insane: Very aggressive; will likely overwhelm targets or miss open ports

Output Formats

- oN Standard Nmap output
- oG Greppable format
- oX XML format
- oA <basename>
Generate Nmap, Greppable, and XML output files using basename for files

Misc Options

- n Disable reverse IP address lookups
- 6 Use IPv6 only
- A Use several features, including OS Detection, Version Detection, Script Scanning (default), and traceroute
- reason Display reason Nmap thinks port is open, closed, or filtered



www.sans.org

Açıklık Tarayıcılar

- Açıklık tarayıcı programlar, herhangi bir bilgisayarda veya bilgisayar sisteminde bulunan açıklıkları veya servisleri tespit eden programlardır.
- Bunlardan en yaygın olanları ***Nessus, GFI Languard, Microsoft Baseline Security Analyser, Internet Security Scanner, NetIQ, Foundstone*** vb... programlardır.
- Açıklık tarayıcı olarak kullanılabilecek en önemli program olan Nessus, Tenable şirketi tarafından ticari bir ürün olarak satılmaktadır (<http://www.nessus.org/nessus>).
- Nessus, hem Linux hem de Windows işletim sistemleri üzerinde çalışmaktadır.
- Bilinen açıklıkları, işletim sistemleri ve servis tespitini yapabilmektedir.
- Domainle entegre olarak çalışabilmekte olup html, xml, latex gibi değişik formatta raporlar üretebilmektedir.

Açıklık Tarayıcılar-Nessus

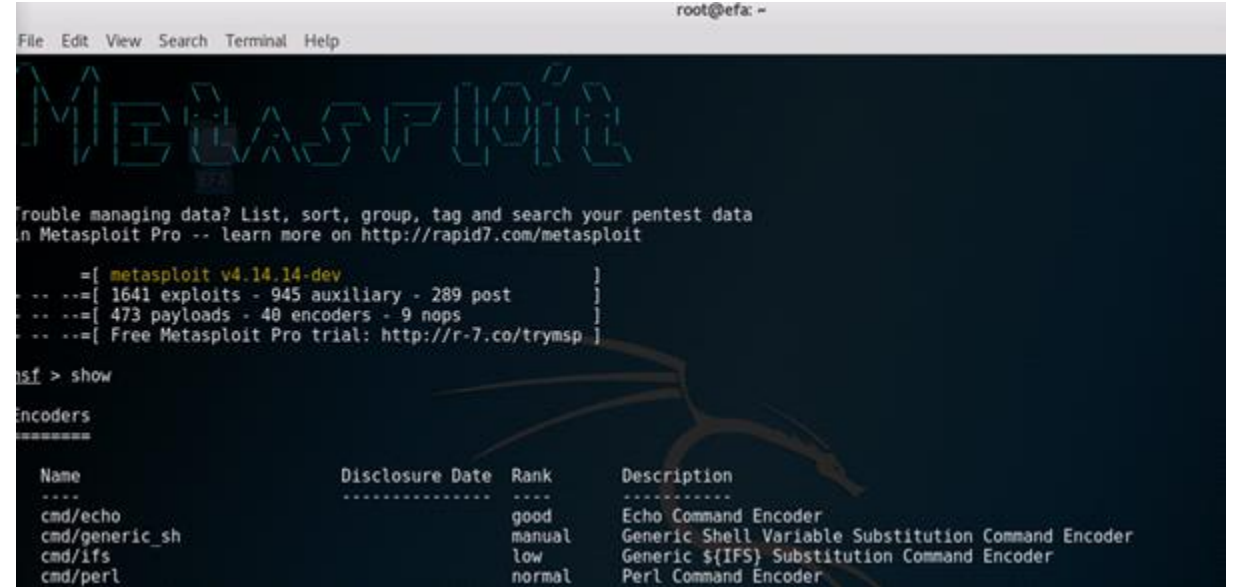


Açıklık Tarayıcılar (devam)

- Diğer açıklık tarayıcı programların ortak özellikleri;
 - Ofis güvenlik güncellemeleri
 - Windows güvenlik güncellemeleri
 - Yerel parola politikaları
 - Yönetici hesapları
 - Parola bitim tarihleri
 - Otomatik güncellemeler
 - Güvenlik duvarları
 - Auto logon
 - Anonymous hesabı
 - İzleme
 - Servisler
 - Paylaşımlar
 - Windows sürümü
 - IIS hakkında bilgiler
 - Sql hakkında bilgiler
 - Macro güvenliği
 - IE güvenlik ayarları

Açıklık Gerçekleme Araçları

- Güvenlik açıklığı gerçekleştirme programları sistemde bulunan bazı açıklıkları hedef cihaza uygulayabilmektedir. Bu programlar kendileri açıklık taraması yapabilmesinin yanında diğer açıklık tarayıcı programlarla entegre edilerek, onların bulduğu açıklıkları gerçekleyebilmektedir.
- Açıklık gerçekleştirme araçlarının en önemlilerinden biri olan **Metasploit**, açık kaynak kodlu bir program olup hem Windows hem de Linux işletim sistemleri üzerinde çalışabilmektedir



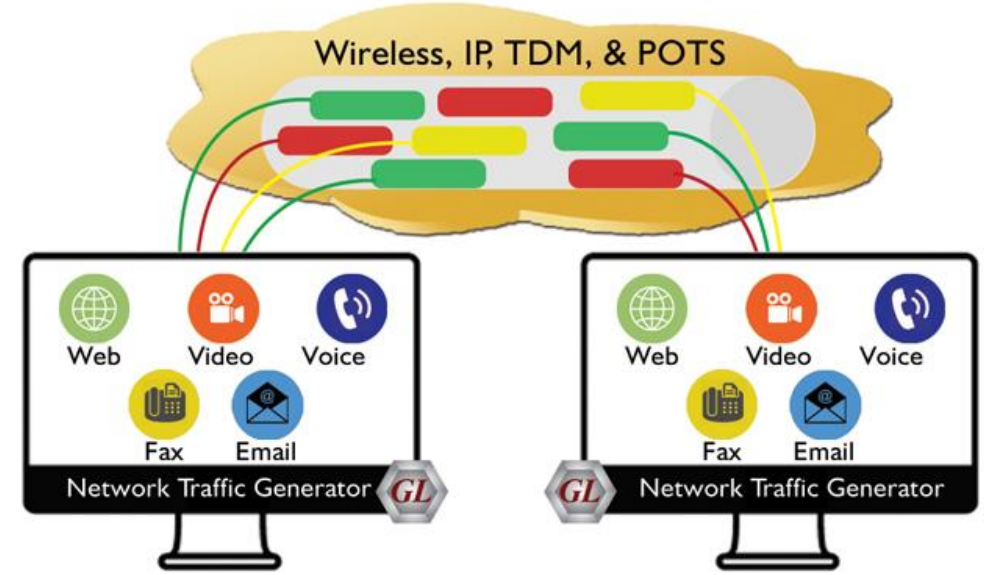
```
root@efa: ~  
File Edit View Search Terminal Help  
Metasploit  
Trouble managing data? List, sort, group, tag and search your pentest data  
in Metasploit Pro -- learn more on http://rapid7.com/metasploit  
msf5 > show  
Encoders  
=====
```

| Name | Disclosure Date | Rank | Description |
|----------------|-----------------|--------|---|
| cmd/echo | | good | Echo Command Encoder |
| cmd/generic_sh | | manual | Generic Shell Variable Substitution Command Encoder |
| cmd/ifs | | low | Generic \${IFS} Substitution Command Encoder |
| cmd/perl | | normal | Perl Command Encoder |

Paket Üreteçleri

- Paket üreteçleri karşıdaki sisteme özel bir paket göndermek için kullanılan programlardır. Bu programlar aşağıdaki amaçlar için yaygın olarak kullanılır:

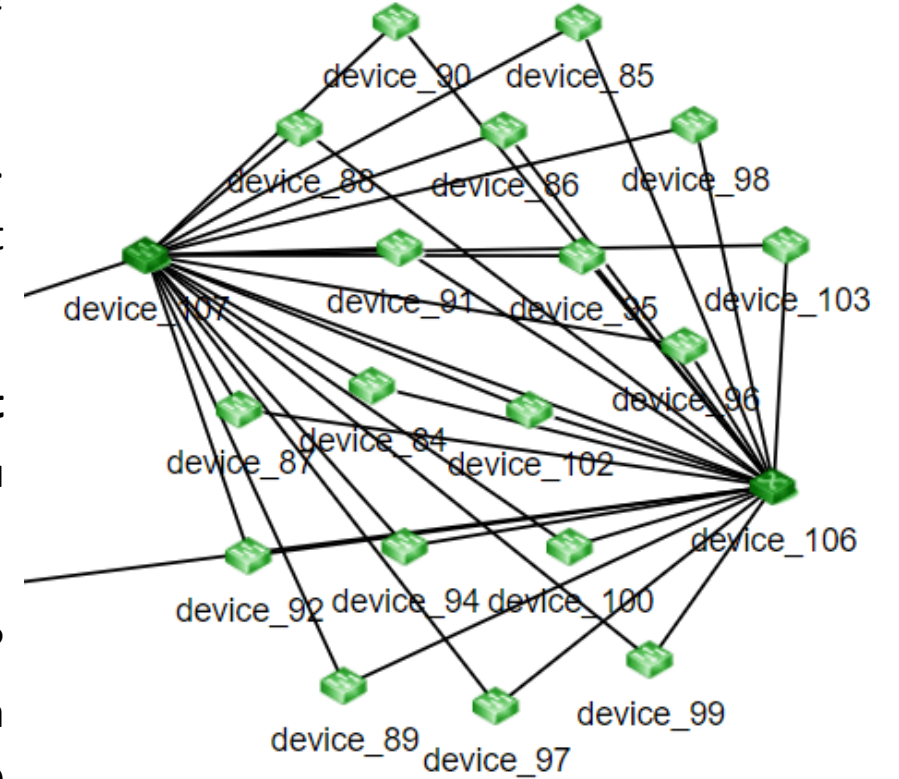
- TCP/IP yığınını test etmek
- Güvenlik duvarı kural tablosunu test etmek
- Parçalı paketler göndermek
- Pakete ait bayrakları (flag) değiştirerek sistemin işletim sistemini tanımak
- Sistemi devre dışı bırakmak ya da ele geçirmek
- Yakalanmış paketleri göndererek bağlantı kurmaya çalışmak
- İleri düzey port tarama



- **Hping** (<http://www.hping.org>), **Scapy**, Nemesis, Engage Packet Builder ve **TCPReplay** programları paket üreteç programlarına örnek olarak verilebilir.

Topoloji Çıkarım Araçları

- Hedef sistemde yer alan cihazların konumlarını tespit etmek ve topolojisini elde etmek için topoloji çıkarım araçları kullanılır.
- Bu alanda en önemli araçlardan biri sıklıkla kullanılan ping komutudur. **Ping** komutu çoğu işletim sisteminde bulunmaktadır. Bu komut kullanılarak hedef cihazın ayakta olup olmadığı tespit edilir.
- Ping komutuna benzer bir yapıda çalışan diğer bir komut **tracert** komutudur. Bu komut hedef cihaza giden yol üzerindeki cihazları (yönlendirici, güvenlik duvarı, anahtar vb...) tespit etmek için kullanılır.
- **Tracert** komutuna benzer çalışan ama ICMP protokolü ile değil, TCP protokolü vasıtasıyla cihaz tespiti yapan Tcptraceroute komutu da oldukça kullanışlıdır. Örneğin hedef ağda bulunan bir web sunucu ve 80 numaralı tcp portu kullanılarak, Web sunucuya giden yol üzerindeki cihazlar kolaylıkla tespit edilebilir.



İşletim Sistemi Tespit Araçları

- Hedef cihazda çalışan işletim sistemini tespit etmek, bir saldırgan için en önemli aşamalardan biridir. Bu işlemi yapmak için işletim sistemi tespit araçları kullanılır. Bu araçlardan en önemlileri **Hping**, **Xprobe2**, **POF**, **Nmap** programlarıdır.
- Hping değişik ICMP paketleri göndererek karşı cihazın işletim sistemini tespit etmeye çalışır.
- Xprobe2 hedef cihazda çalışan işletim sistemine ait tahminler ve bu tahminlerin doğruluğuna ilişkin yüzdeler vermektedir (<http://xprobe.sourceforge.net>). Linux işletim sisteminde ve komut satırında çalışmaktadır.
- Diğer bir işletim sistemi tespit aracı da POF (Passive OS Fingerprinting) programıdır.
- Windows ve Linux işletim sistemlerinde çalışabilmektedir.



- [illegible]

Kablosuz Ağ Araçları

- *Kablosuz ağ araçlarını üç grup altında toplamak mümkündür:*
- **Tespit ve Analiz Araçları:** Kablosuz cihazların tespit edilmesi, kanallardaki cihazların tespit edilmesi, sinyal analizi, kablosuz ağ trafiğinin dinlenmesi ve kaydedilmesi için geliştirilmiş araçlardır. **Kismet ve Netstumbler**
- **Denetleme araçları:** Kablosuz haberleşmede kullanılan şifreleme ve kimlik doğrulama yöntemleri, paket dinleme, analiz etme ve önemli olayların kaydını tutma gibi işlemlerde denetleme araçları kullanılır. **Airmagnet, Airdefense ve AiropEEK**
- **Saldırı araçları:** WEP/WPA anahtarlarının ele geçirilmesi, hedef bilgisayara erişim, hedef bilgisayarın veya erişim noktasının (EN) ağa erişiminin engellenmesi, yetkilendirme ve doğrulama mekanizmasının aşılması veya etkisiz hale getirilmesi gibi işlemler için saldırı araçları kullanılır. **Aircrack, HostAP, Airjack, Aircrack-ng ve LEAPcracker**



Web Güvenliği Test Araçları



- Web uygulama güvenliği alanında en önemli araçlardan bazıları şunlardır;
- **Paros**, açık kaynak kodlu bir yazılım olup platform bağımsız çalışmaktadır.
- Genellikle internet tarayıcı ara yüzünden girilmesine izin verilmeyen karakterlerin uygulama yazılımına gönderilmesi için kullanılır. Aynı şekilde uygulama yazılımına paketler gönderilirken yakalanarak içerikleri değiştirilip gönderilebilir. Ya da daha önceden yakalanmış olan paketler gönderilir. Bunların sonucunda uygulama devre dışı bırakılmaya zorlanabilir ya da uygulamanın yapısı hakkında bilgi toplanabilir.
- **FireBug**, Mozilla Firefox'un bir uzantısı olarak çalışır. Platformdan bağımsız olarak çalışır.
- Web sayfasının istenilen herhangi bir yerine gelindiğinde o kısımla ilgili kodu gösterebilir ve o kısımda inceleme yapılabilir. O kısmın kodu kolayca değiştirilebilir. Bu araç hem geliştiriciler hem de testçiler tarafından etkin olarak kullanılabilir.
- Ticari bir yazılım olan **Acunetix**, Windows işletim sistemi üzerinde çalışmakta olup version check, CGI kontrol, parametre değişimi, dosya kontrolü, izin kontrolü gibi testleri yapmaktadır.
- Uygulama açıklığı taraması yapmaktadır. İstenilen açıklıkları ekleyebilme yeteneği mevcuttur. Yapılan açıklıklarla ilgili detaylı raporlar üretmesinin yanında tek tuşla internetten güncellenebilmektedir.

Veritabanı Test Araçları

- **ISS Database Scanner** güvenlik açıklıklarını ve yanlış konfigürasyonları tespit etmek için kullanılan ticari bir yazılımdır. Bu açıklıklar veritabanında bulunan yama eksiklikleri, varsayılan kullanıcı şifrelerinin değiştirilmemesi ya da basit şifreler verilmesi gibi açıklıkları test eder. Oracle, MSSQL ve Sybase veritabanları üzerinde tarama yapabilir. Seçilen bir sözlük üzerinden veritabanı kullanıcı şifreler için sözlük atağı yapabilir.
- **Appdedective** ticari bir ürün olup açıklık tespiti ve yapılandırma hatalarını tespit edebilmektedir. Çok geniş bir veritabanı tarama seçeneğine sahiptir. Sözlük atağı yapabilme yeteneğinden dolayı sızma aracı olarak da kullanılabilir.
- **Bruteforce Script**, varsayılan kullanıcı isimleri ve şifreleri ile veritabanlarına bağlantı yapmaya çalışan bir perl betiğidir. Bağlanılmak için istenilen veritabanının IP adresi port numarası ve kullanıcı isim/şifrelerinin olduğu bir dosya girilir. Bu script üzerinde yapılan değişikliklerle Oracle veritabanının değişik sürümlerinin parola bilgilerinin kontrolü yapılabilmektedir.

