



# Ağ Sızma Testleri ve 2. Katman Saldırıları

**TÜBİTAK BİLGEM**  
**Siber Güvenlik Enstitüsü**



Bu doküman, alıntı vererek kullanılabilir ya da paylaşılabılır ancak değiştirilemez ve ticari amaçla kullanılamaz. Detaylı bilgiye <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.tr> bağlantısından erişebilirsiniz.

TCP/IP Temelleri

Ağı Dinleme

MAC Adres Tablosu Doldurma

ARP Zehirlenmesi

DHCP Sunucusu IP Adres Havuzunu Doldurma

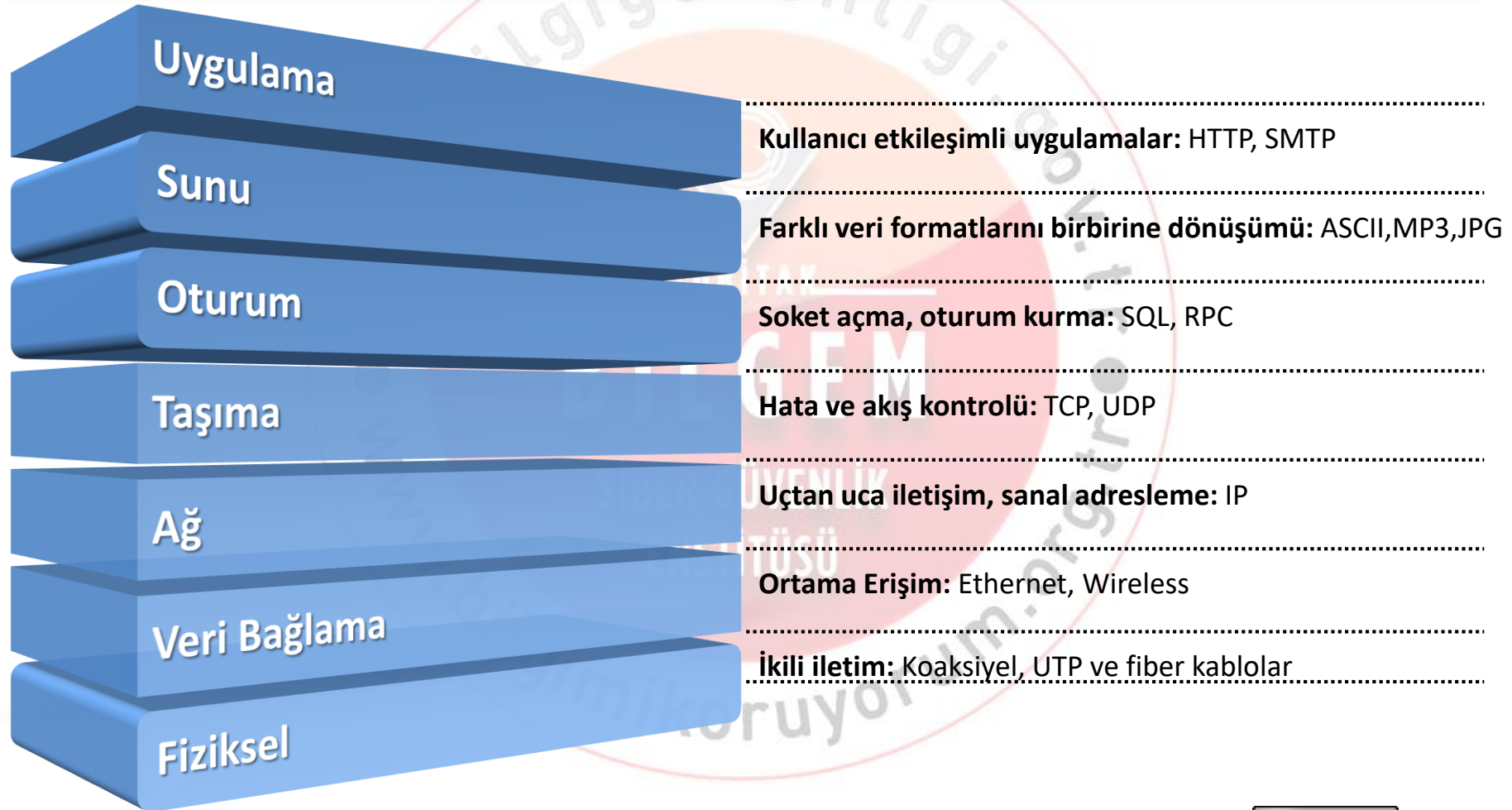
VLAN Hopping

Aktif Cihaz Sızma Testi

Anahtar Yapılandırma Denetimleri

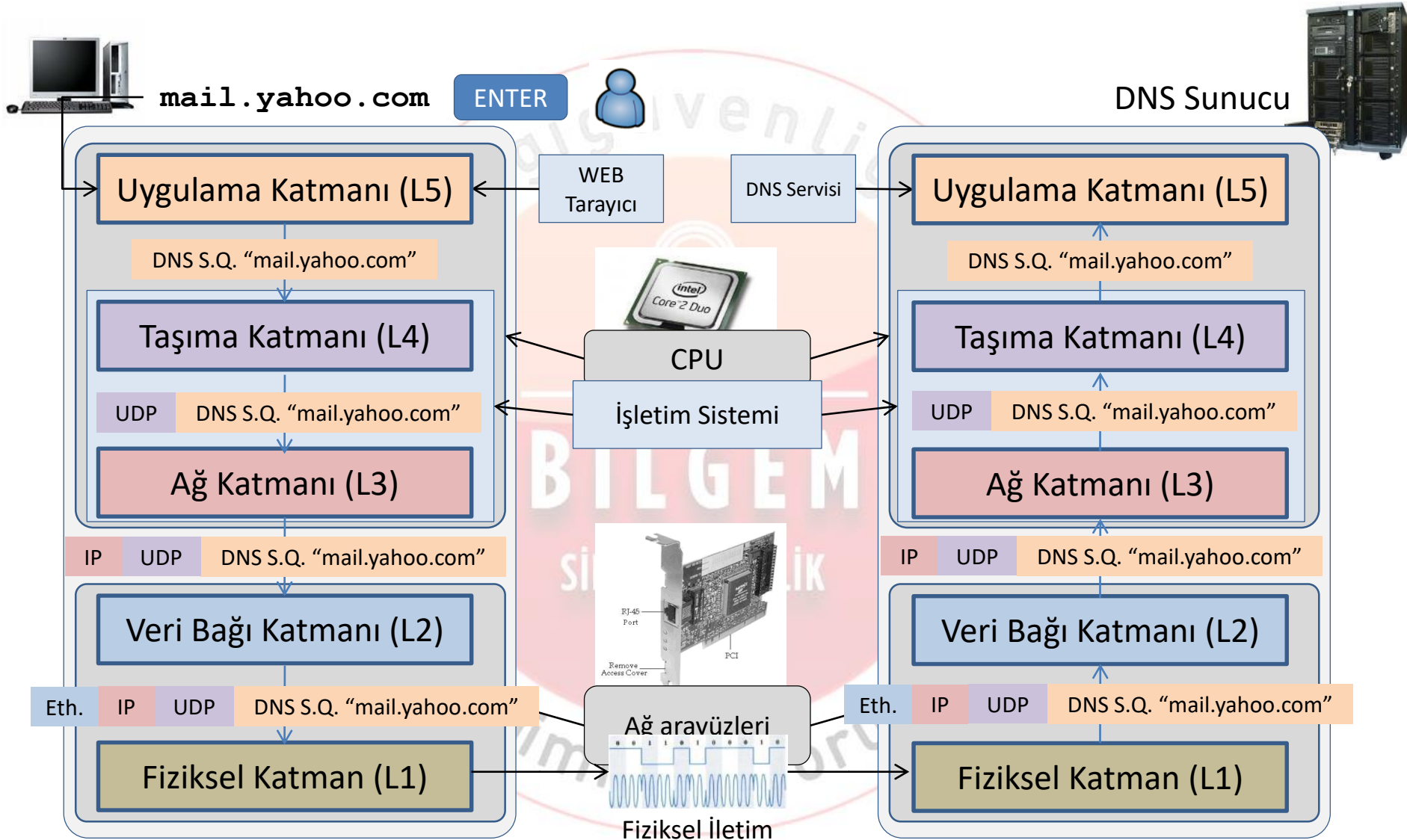
# TCP/IP Temelleri

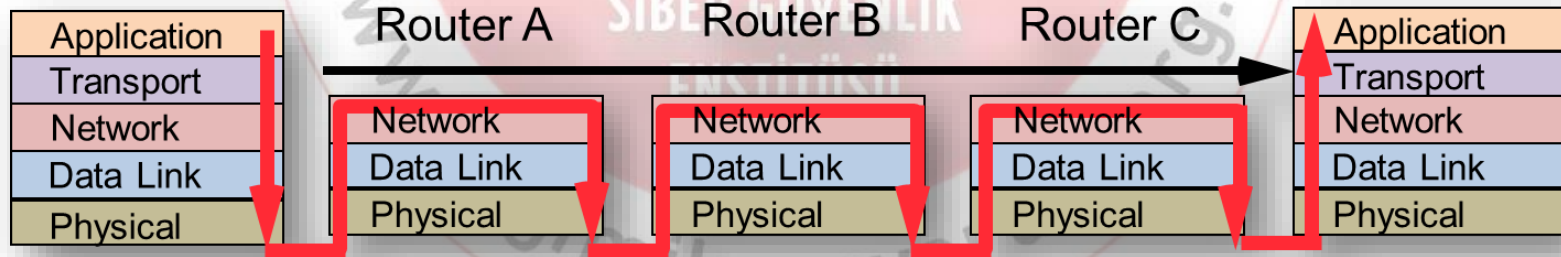
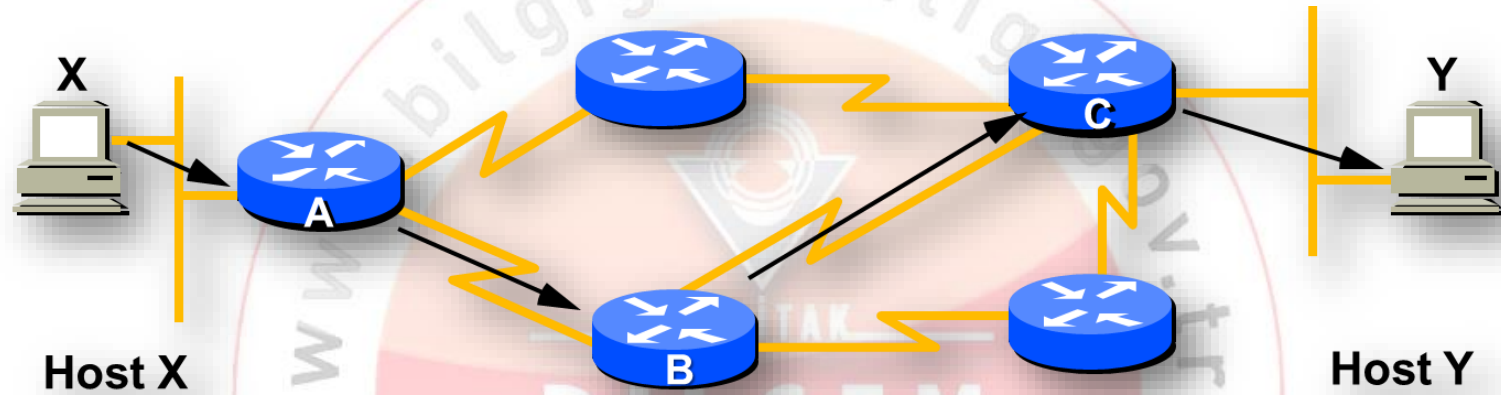
## OSI Referans Modeli



Application	HTTP	Telnet	FTP	SMTP	TFTP	DNS	SNMP
Presentation	Hyper Text Transport Protocol	Virtual Terminal	File Transfer Protocol	Simple Mail Transfer Protocol	Trivial File Transfer Protocol	Domain Name Server	Simple Network Mgmt Protocol
Session							
Transport	TCP (Reliable Datagram Service)				UDP (Unreliable Datagram Service)		
Network	IP Addressing, Routing, Fragmentation						
Data Link	802.3 CSMA/CD (Ethernet)	802.4 Token Bus		802.5 Token Ring		FDDI	
Physical	Physical Medium (Token Ring, 10Base-T, 100BaseTc...)						

# Örnek: DNS Protokolü



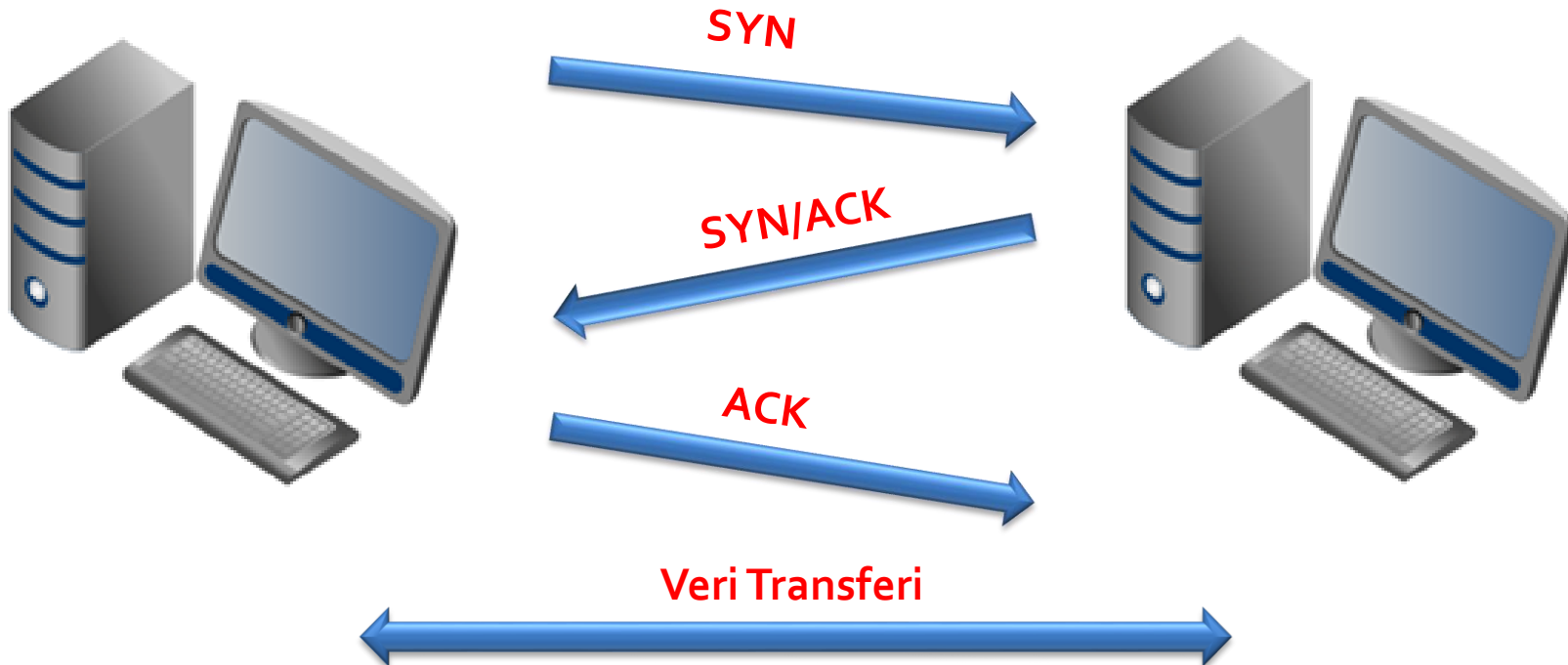


## Özellikler

- Bağlantı yönelimlidir
- Verilere sıra numarası eklenir
- Veriler parçalara bölünebilir
- Güvenilirdir
- Akış kontrolü mekanizması vardır
- Çift yönlüdür



## TCP 3'lü el sıkışma



İletişim sırasında bağlantı oluşturmaz

Hata denetimi yoktur

- Kaybolan paket yeniden gönderilmez

Veri aktarımı hızlıdır

- Multimedia için uygundur

Doğrulama mekanizması yoktur

- IP sahteciliği yapılabilir

Örnek kullanım alanları

- DNS
- DHCP
- Multimedia

# Ağı Dinleme

SİBER GÜVENLİK  
ENSTİTÜSÜ

## Neden dinleme

- Taramaların doğru çalıştığının kontrolü
- Pasif olarak IP adresi, servis, uygulama tespiti
- Pasif olarak protokol tespiti
- Ağ altyapısındaki teknolojiler hakkında bilgi edinme
- Hedef sunucu veya kişilerin trafiğini dinleme
- Gizli bilgilere ulaşma

## tcpdump

### Komutlar

- -D: Arayüzleri listeler
- -i: Dinlenecek arayüz
- -n: İsim çözme
- -nn: İsim ve port çözme
- -v: Ek bilgi
- -w: Kaydetmek
- -r: Dosyadan okumak
- -X: ASCII formatında
- -x: hexadecimal formatında
- -A: ASCII formatında

## tcpdump - Filtreleme

Prokol

- ip, arp, udp, tcp, icmp, ...

Sunucu ve ağ

- host, net

Port

- port, portrange

Kaynak - hedef

- src, dst

Bağlama

- and, or

## Uygulama - tcpdump

eth0 arayüzündeki trafik

172.20.40.111 sunucusu ile yapılan TCP trafiği

172.20.40.111 sunucusundan gelen ip trafiği

172.20.40.0/24 ağındaki web uygulamaları ile yapılan TCP trafiği

192.168.1.10 IP adresinden 172.20.0.120 IP adresine giden RDP trafiği

## Wireshark

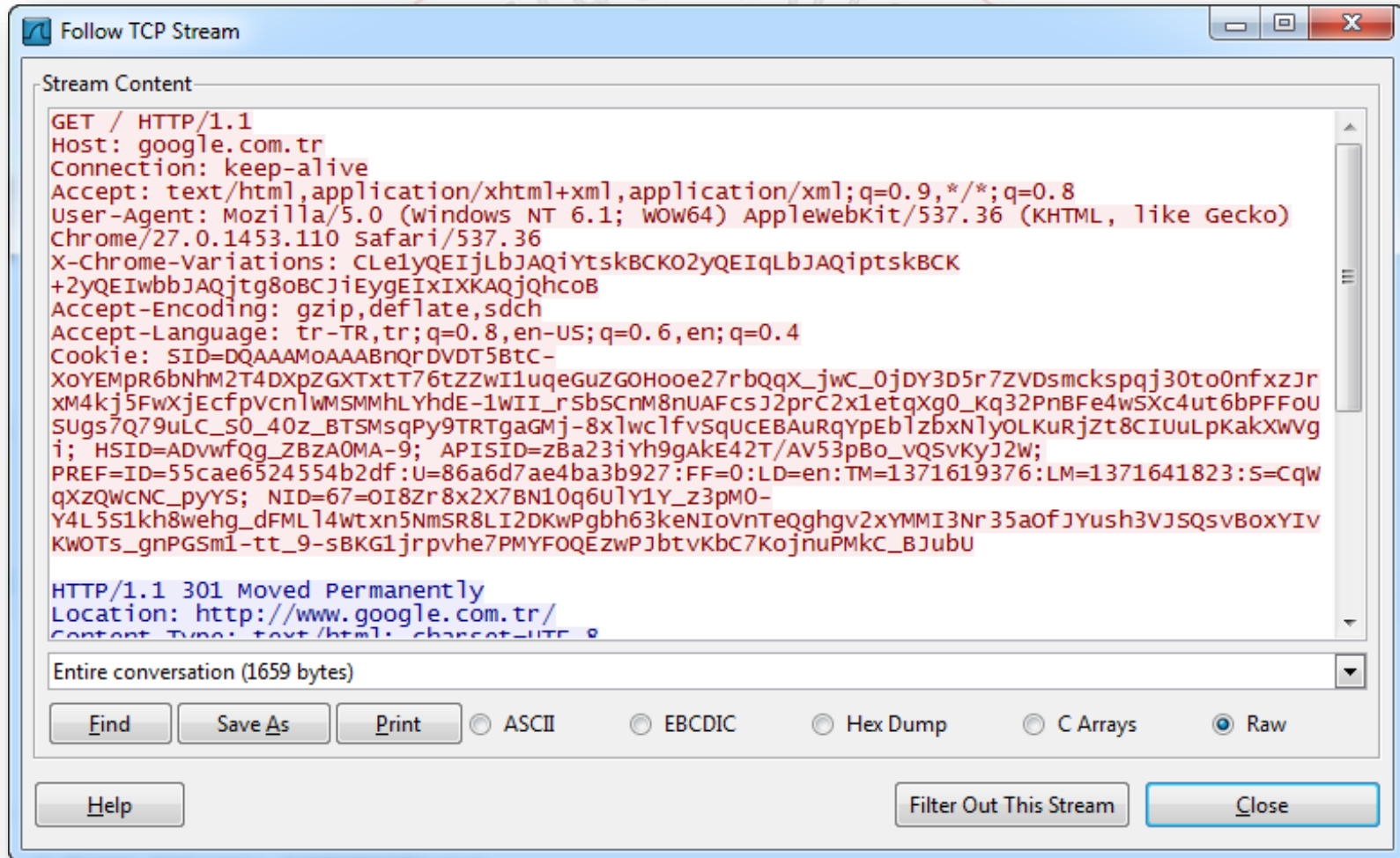
Filter: (tcp.port == 80) && (ip.addr == 10.20.20.103)

No.	Time	Source	Destination	Protocol	Length	Info
62	11.3816400	10.20.20.103	173.194.113.56	TCP	66	6266 > http [SYN] Seq
67	11.4356430	173.194.39.215	10.20.20.103	TCP	66	http > 6265 [SYN, ACK]
68	11.4357070	10.20.20.103	173.194.39.215	TCP	54	6265 > http [ACK] Seq
69	11.4662550	173.194.113.56	10.20.20.103	TCP	66	http > 6266 [SYN, ACK]
70	11.4663230	10.20.20.103	173.194.113.56	TCP	54	6266 > http [ACK] Seq
71	11.4667870	10.20.20.103	173.194.113.56	HTTP	1167	GET / HTTP/1.1
72	11.5565210	173.194.113.56	10.20.20.103	TCP	60	http > 6266 [ACK] Seq
73	11.5645180	173.194.113.56	10.20.20.103	HTTP	600	HTTP/1.1 301 Moved Per
75	11.5696060	10.20.20.103	173.194.39.215	HTTP	1166	GET / HTTP/1.1
77	11.6481830	173.194.39.215	10.20.20.103	TCP	60	http > 6265 [ACK] Seq
78	11.6909250	173.194.39.215	10.20.20.103	HTTP	534	HTTP/1.1 302 Found
92	11.7664380	10.20.20.103	173.194.113.56	TCP	54	6266 > http [ACK] Seq
109	11.8894380	10.20.20.103	173.194.39.215	TCP	54	6265 > http [ACK] Seq

Frame 78: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface 0

- Ethernet II, Src: Hewlett-\_54:7f:56 (00:1f:29:54:7f:56), Dst: HonHaiPr\_39:d0:5c (c4:17:fe:39:d0:5c)
- Internet Protocol Version 4, Src: 173.194.39.215 (173.194.39.215), Dst: 10.20.20.103 (10.20.20.103)
- Transmission Control Protocol, Src Port: http (80), Dst Port: 6265 (6265), Seq: 1, Ack: 1113, Len: 480
- Hypertext Transfer Protocol
  - HTTP/1.1 302 Found\r\nLocation: <https://www.google.com.tr/>\r\nCache-Control: private\r\nContent-Type: text/html; charset=UTF-8\r\n

## Wireshark



## Dinleme Alanı

- Anahtarlama cihazları, trafiği sadece ilgili porta gönderir
- Bu işlemi MAC adresi tablosuna bakarak gerçekleştirir
- Hub, trafiği tüm portlara gönderir

## Dinleme Alanını Genişletme

- SPAN port (mirroring)
- MAC adres tablosu doldurma
- ARP zehirlenmesi
- Sahte DHCP

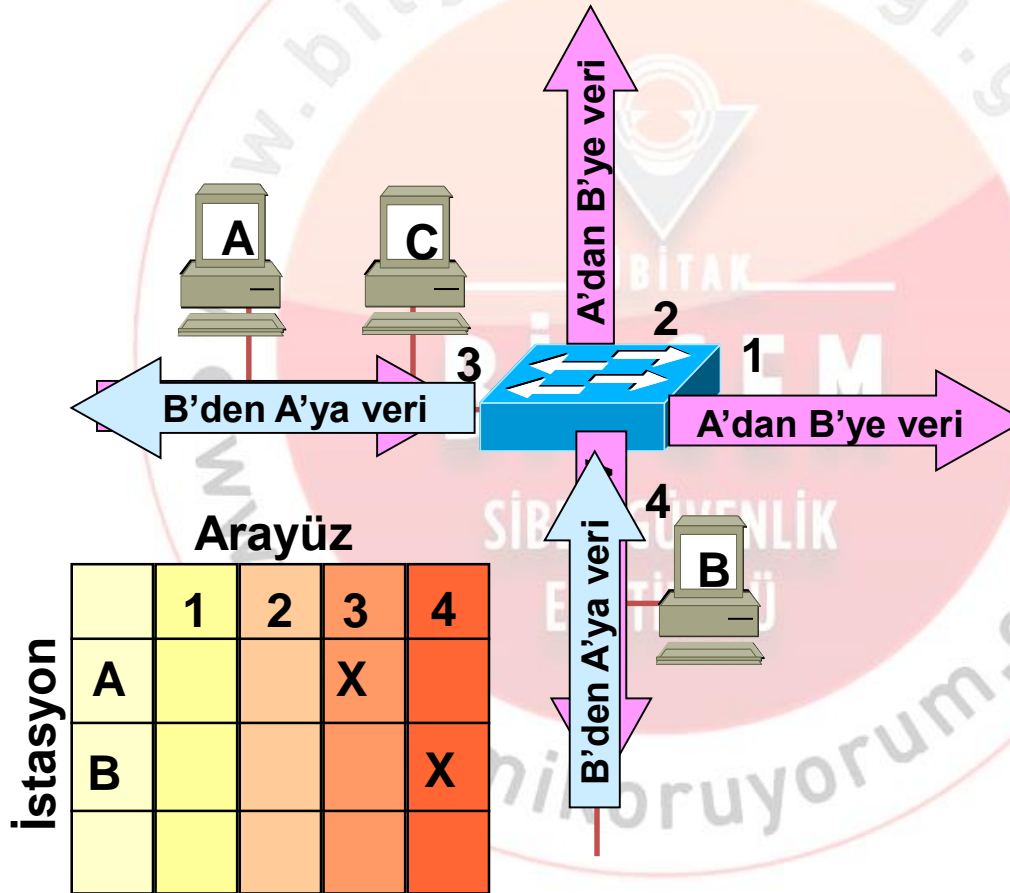
# MAC Adres Tablosu Doldurma

## MAC Adres Tablosu

- VLAN numarası - MAC adresi - Port numarası
- Çerçevenin (frame) hedef adresine bakılır
- MAC adres tablosunda kayıt varsa o porttan gönderilir
- Kayıt yoksa tüm portlardan gönderilir
- Sahte MAC adresleri ile tablo doldurulabilir - yeni kayıt eklenemez
- Anahtar; hub gibi çalışır - trafik tüm portlara gönderilir

```
Switch#  
Switch#show mac address-table dynamic  
      Mac Address Table  
-----  
  
Vlan    Mac Address      Type      Ports  
----    -  
1       000c.2956.2b2a   DYNAMIC   Fa0/3  
1       705a.b69a.877e   DYNAMIC   Fa0/3  
10      000c.2956.2b7a   DYNAMIC   Fa0/22  
10      68b5.99f2.123f   DYNAMIC   Fa0/22  
Total Mac Addresses for this criterion: 4  
Switch#  
Switch#
```

## Anahtarlama



# MAC Adres Tablosu Doldurma

```
macof -d 10.1.1.1 -n 100000 -i eth1
```

```
root@SGE:~# macof -d 10.1.1.1 -n 100000 -i eth1
```

```
a4:5d:fa:10:46:68 63:34:31:6d:f7:8 0.0.0.0.32298 > 10.1.1.1.57522: S 1016801417:1016801417(0) win 512  
82:3:91:3b:26:9f 5:8f:9c:2f:63:9e 0.0.0.0.52559 > 10.1.1.1.22763: S 796897861:796897861(0) win 512  
87:e1:59:46:8b:e5 7e:1c:67:2c:f7:97 0.0.0.0.57470 > 10.1.1.1.5414: S 454174648:454174648(0) win 512  
f4:34:cb:56:ad:c7 bb:2d:69:f:b9:52 0.0.0.0.42346 > 10.1.1.1.29773: S 1920781511:1920781511(0) win 512  
d5:92:a3:5f:f6:9f af:6c:2d:b:b6:45 0.0.0.0.5892 > 10.1.1.1.1112: S 1761318001:1761318001(0) win 512  
af:f7:f7:59:57:d6 59:1f:24:c:e9:23 0.0.0.0.4361 > 10.1.1.1.27855: S 1197395665:1197395665(0) win 512  
19:76:34:57:55:ab a:64:22:15:db:12 0.0.0.0.16602 > 10.1.1.1.20480: S 1450029921:1450029921(0) win 512  
5e:75:c:0:1c:7e 63:a5:6:11:23:8 0.0.0.0.54879 > 10.1.1.1.32768: S 589337386:589337386(0) win 512  
20:cc:e3:4a:a2:3a 24:9a:b1:18:bc:60 0.0.0.0.35117 > 10.1.1.1.35897: S 1114566084:1114566084(0) win 512  
68:f5:da:27:2:1d a5:8a:f1:12:a5:53 0.0.0.0.18668 > 10.1.1.1.52433: S 1987053242:1987053242(0) win 512  
45:85:66:8:2a:4d 37:40:99:49:d1:84 0.0.0.0.34797 > 10.1.1.1.15164: S 874714773:874714773(0) win 512
```

SİBER GÜVENLİK  
ENSTİTÜSÜ  
www.bilgimikoruyorum.org

## MAC adres tablosu - sahte MAC adresleri

```
Switch#show mac address-table dynamic
Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
1       0003.cb22.1bb5   DYNAMIC Fa0/3
1       0009.5740.3762   DYNAMIC Fa0/3
1       000c.2956.2b2a   DYNAMIC Fa0/3
1       0011.dd3d.7270   DYNAMIC Fa0/3
1       0029.e000.5bf8   DYNAMIC Fa0/3
1       0030.204d.e70e   DYNAMIC Fa0/3
1       0042.e77f.4aff   DYNAMIC Fa0/3
1       004a.1b15.6318   DYNAMIC Fa0/3
1       004d.2d4a.3315   DYNAMIC Fa0/3
1       0050.b758.afc4   DYNAMIC Fa0/3
1       0052.443b.63da   DYNAMIC Fa0/3
1       005e.4660.4e98   DYNAMIC Fa0/3
1       0068.7077.c98a   DYNAMIC Fa0/3
1       0069.2a26.8857   DYNAMIC Fa0/3
1       0072.2644.2b75   DYNAMIC Fa0/3
1       0080.f66a.96ef   DYNAMIC Fa0/3
1       008a.ce55.e892   DYNAMIC Fa0/3
1       009a.a40e.fc75   DYNAMIC Fa0/3
1       009a.b413.da1b   DYNAMIC Fa0/3
1       00b2.ab29.c64a   DYNAMIC Fa0/3
1       00b6.3134.d9f6   DYNAMIC Fa0/3
1       00c1.1c07.749b   DYNAMIC Fa0/3
1       00c2.6325.46a4   DYNAMIC Fa0/3
1       00c7.1533.17ac   DYNAMIC Fa0/3
--More--
```

## Uygulama

Saldırı öncesi  
trafik analizi

Saldırı

Saldırı sonrası  
trafik analizi

## Çözüm

Bir portta kullanılabilen MAC sayısının kısıtlanması

- interface fastethernet 0/1
- switchport mode access
- switchport port-security
- switchport port-security maximum 2

# ARP Zehirlemesi

SİBER GÜVENLİK  
ENSTİTÜSÜ

## ARP

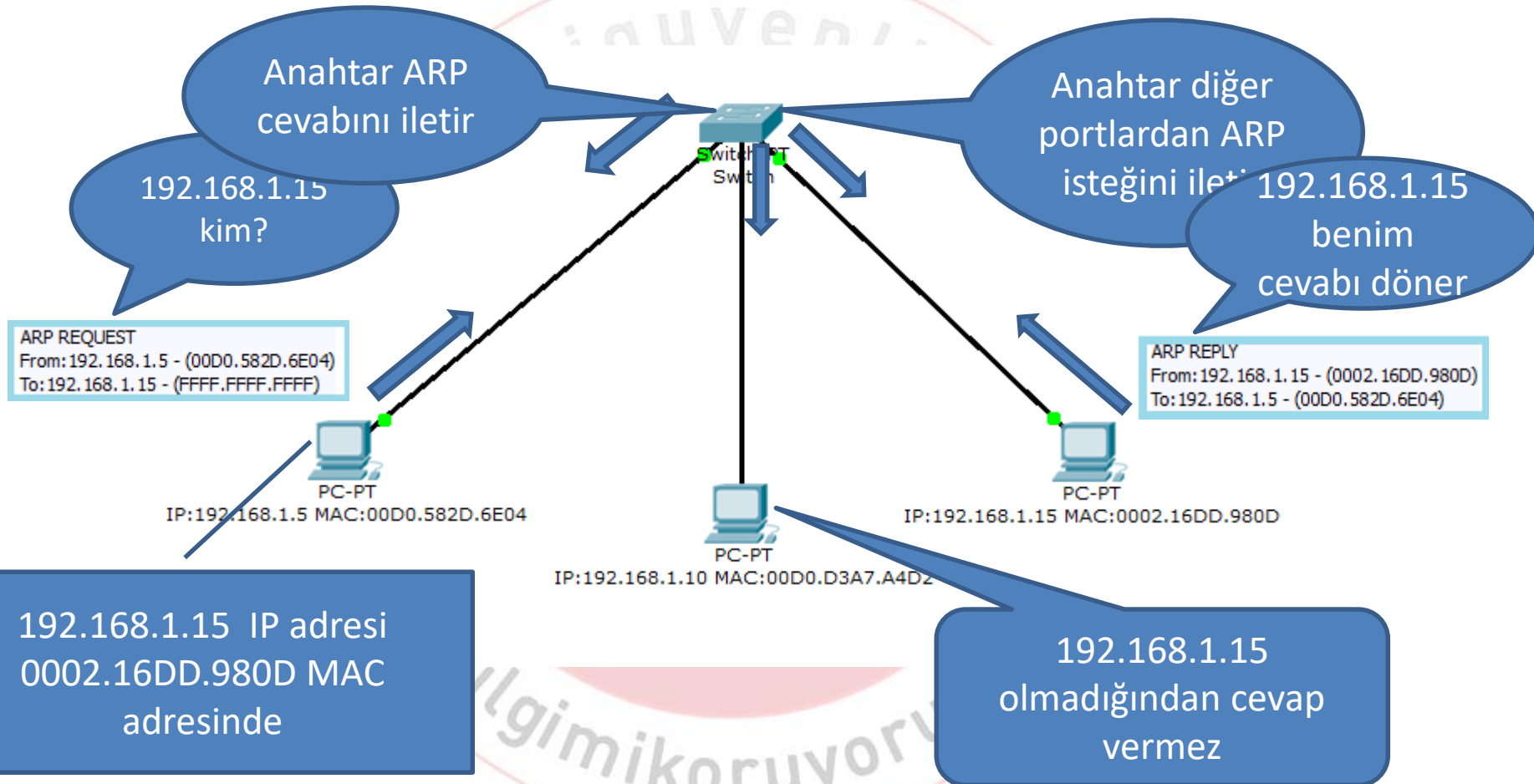
Address Resolution Protocol

L2'de IP adresleri yerine MAC adresleri kullanılır

IP adresinden MAC adresi öğrenme mekanizması

İstek broadcast, cevap unicast





```
1 0.000000 HonHaiPr_6e:8b:24 Broadcast ARP 42 who has 192.168.0.1? Tell 192.168.0.114
2 0.004081 D-Link_0b:22:ba HonHaiPr_6e:8b:24 ARP 46 192.168.0.1 is at 00:13:46:0b:22:ba
```

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)  
Ethernet II, Src: HonHaiPr\_6e:8b:24 (00:16:ce:6e:8b:24), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
Address Resolution Protocol (request)  
Hardware type: Ethernet (1)  
Protocol type: IP (0x0800)  
Hardware size: 6  
Protocol size: 4  
Opcode: request (1)  
Sender MAC address: HonHaiPr\_6e:8b:24 (00:16:ce:6e:8b:24)  
Sender IP address: 192.168.0.114 (192.168.0.114)  
Target MAC address: 00:00:00\_00:00:00 (00:00:00:00:00:00)  
Target IP address: 192.168.0.1 (192.168.0.1)

*ARP Request*

```
1 0.000000 HonHaiPr_6e:8b:24 Broadcast ARP 42 who has 192.168.0.1? Tell 192.168.0.114
2 0.004081 D-Link_0b:22:ba HonHaiPr_6e:8b:24 ARP 46 192.168.0.1 is at 00:13:46:0b:22:ba
```

Frame 2: 46 bytes on wire (368 bits), 46 bytes captured (368 bits)  
Ethernet II, Src: D-Link\_0b:22:ba (00:13:46:0b:22:ba), Dst: HonHaiPr\_6e:8b:24 (00:16:ce:6e:8b:24)  
Address Resolution Protocol (reply)  
Hardware type: Ethernet (1)  
Protocol type: IP (0x0800)  
Hardware size: 6  
Protocol size: 4  
Opcode: reply (2)  
Sender MAC address: D-Link\_0b:22:ba (00:13:46:0b:22:ba)  
Sender IP address: 192.168.0.1 (192.168.0.1)  
Target MAC address: HonHaiPr\_6e:8b:24 (00:16:ce:6e:8b:24)  
Target IP address: 192.168.0.114 (192.168.0.114)

*ARP Reply*

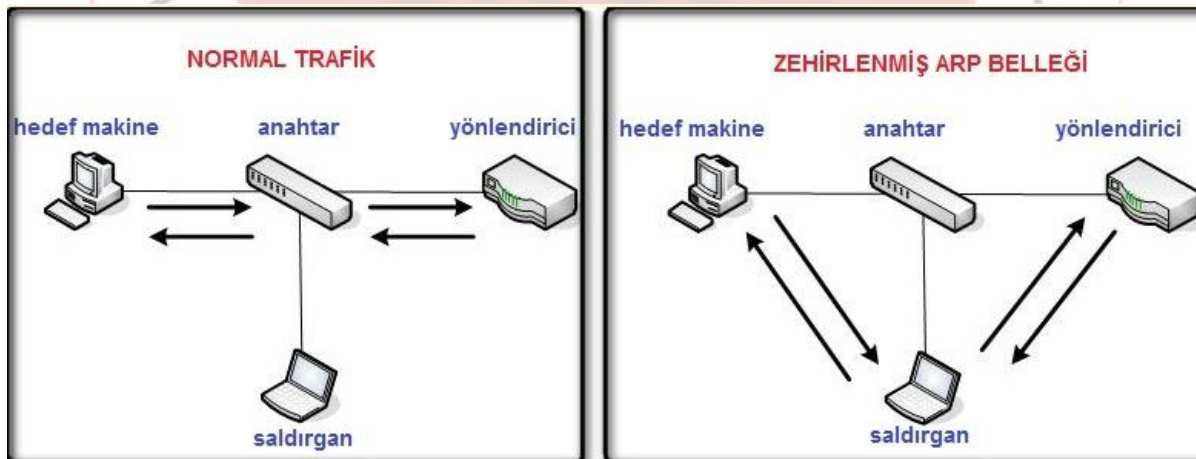
## ARP Zehirlenmesi

ARP mekanizmasında kimlik doğrulama yok

Başka bir IP adresi için ARP cevabı dönebilirsin

L2'de çerçeveler kurban yerine saldırgan üzerinden gider

Ağ geçidine yapılırsa tüm subnet dinlenebilir



## ARP Zehirlenmesi

### Kısıtlar

- Sadece bulunulan subnet için yapılabilir
- Yönlendiricide Proxy-ARP varsa diğer subnetlere çıkabilir
- Sadece bağlı olunan anahtar değil, tüm subnet dinlenebilir
- Yönlendirme açılmazsa trafik saldırıganda sonlanır - bağlantı çöker
- Ek yöntemler kullanılmazsa sadece açık metin bilgiler elde edilebilir

## ARP Zehirlenmesi

### Yönlendirme açık mı kontrolü

- `# cat /proc/sys/net/ipv4/ip_forward`
- 0 -> yönlendirme kapalı, 1 -> yönlendirme açık

### Yönlendirme açma

- Anlık yapılandırma
  - `# sysctl -w net.ipv4.ip_forward=1`
- Kalıcı yapılandırma
  - `/etc/sysctl.conf` dosyası içerisinde `"net.ipv4.ip_forward = 1"` parametresi ayarlanır
  - `# sysctl -p /etc/sysctl.conf`

## Uygulama

Yönlendirmenin  
Açılması

ARP  
Zehirlemesi  
Saldırısı

Trafik Analizi

## DHCP Sunucu IP Adres Havuzunun Tüketilmesi ve Sahte DHCP

SİBER GÜVENLİK  
ENSTİTÜSÜ

## DHCP (Dynamic Host Configuration Protocol)

IP adresi, ağ geçidi, DNS sunucu gibi ağ ayarlarını dağıtır

UDP protokolü

DHCP isteği (request) - broadcast

İlk cevap veren DHCP, ayarları belirler

Kimlik doğrulama yoktur

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	314	DHCP Discover - Transaction ID 0x3d1d
2	0.000295	192.168.0.1	192.168.0.10	DHCP	342	DHCP Offer - Transaction ID 0x3d1d
3	0.070031	0.0.0.0	255.255.255.255	DHCP	314	DHCP Request - Transaction ID 0x3d1e
4	0.070345	192.168.0.1	192.168.0.10	DHCP	342	DHCP ACK - Transaction ID 0x3d1e

Frame 4: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
Ethernet II, Src: DellComp_ad:f1:9b (00:08:74:ad:f1:9b), Dst: Grandstr_01:fc:42 (00:0b:82:01:fc:42)
Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.10 (192.168.0.10)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
Bootstrap Protocol
Message type: Boot Reply (2)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x00003d1e
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0 (0.0.0.0)
Your (client) IP address: 192.168.0.10 (192.168.0.10)
Next server IP address: 0.0.0.0 (0.0.0.0)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: Grandstr_01:fc:42 (00:0b:82:01:fc:42)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type
Length: 1
DHCP: ACK (5)
Option: (58) Renewal Time Value
Option: (59) Rebinding Time Value
Option: (51) IP Address Lease Time
Option: (54) DHCP Server Identifier
Option: (1) Subnet Mask
Option: (255) End
Padding

## Sahte DHCP Sunucusu

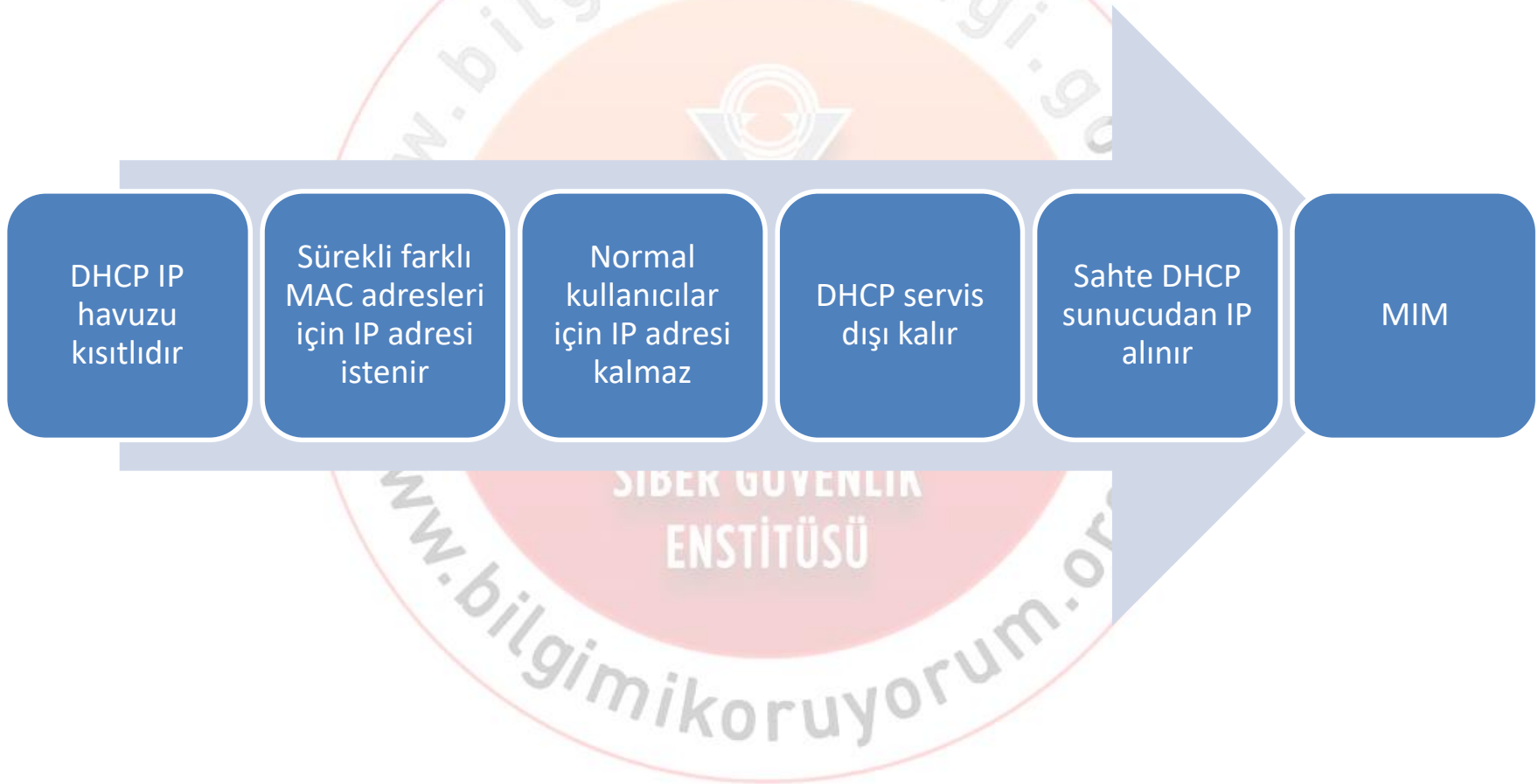
### Sahte IP adresi ve ağ geçidi

- Trafik saldırgan üzerinden geçirilir
- Trafik dinlenebilir ve değiştirilebilir
- MIM

### Sahte DNS

- DNS cevapları değiştirilir
- Kullanıcı sahte - web sayfalarına yönlendirilir
- Sosyal mühendislik
- İstemci tarafı zafiyet sömürme

## DHCP Sunucu IP Havuzu Tüketme Saldırısı





## Uygulama

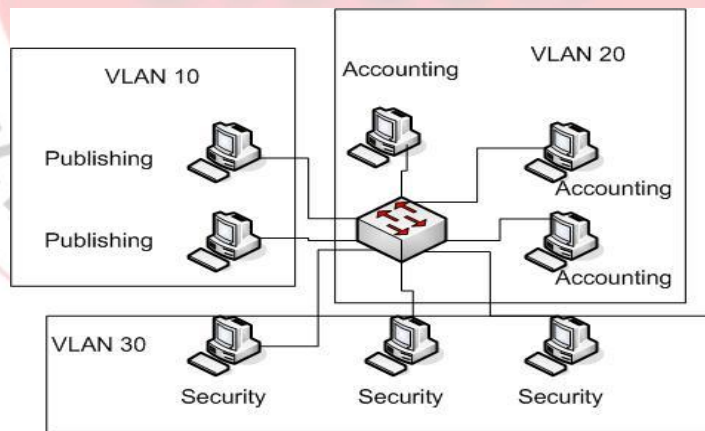
- Yersinia aracı ile DHCP IP havuzunu tüketme

# VLAN Hopping

SİBER GÜVENLİK  
ENSTİTÜSÜ

## Sanal Yerel Alan Ağları

- Yerel alan ağı üzerindeki kullanıcıların mantıksal olarak gruplandırılmasıdır.
- Her VLAN sadece kendi **broadcast** paketlerini alır.
- Daha verimli bantgeniřlięi, daha fazla güvenlik
- 802.1q etiketleme (tagging)

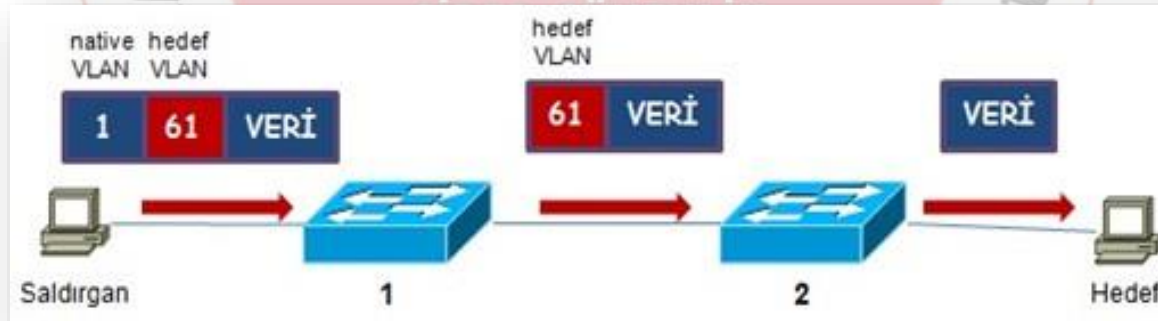


## Anahtar Kandırma (Switch Spoofing)

- Varsayılan olarak anahtar portları “Dynamic Desirable” modundadır
- Porta takılan cihaz bilgisayar ise port “access” moda geçer
- Porta takılan cihaz anahtar ise port “trunk” moda geçer
- Saldırgan hedef anahtara, kendini anahtar gibi tanıtır
- Tüm VLAN’lere erişebilir
- (conf-if)# switchport mode access

## Çift Etiketleme (Double Tagging)

- Çerçevelere iki adet 802.1q başlığı eklenir
- İlk eklenen başlık ulaşmak istenen VLAN numarası
- Sonra eklenen başlık native VLAN numarası
- Native VLAN varsayılan olarak VLAN 1
- İlk anahtar birinci başlığı çıkarır
- İkinci anahtar ikinci VLAN başlığını okur ve ilgili VLAN'ye paketi gönderir





Ağı Dinleme



MAC Adres Tablosu Doldurma



ARP Zehirlemesi



DHCP sunucu IP adres havuzunun tüketilmesi



VLAN Hopping



Aktif Cihaz Sızma Testi



Anahtar Yapılandırma Denetimleri



# Aktif Cihaz Sızma Testi



## Tarama

### Açık portlar

- TCP/22 SSH
- TCP/23 Telnet
- TCP/80 HTTP
- TCP/443 HTTPS
- UDP/161 SNMP

```
nmap -sS -p22,23,80,443 --open
```

### İşletim sistemi tespiti

### Versiyon tespiti

## Trafiği dinlemek

CDP

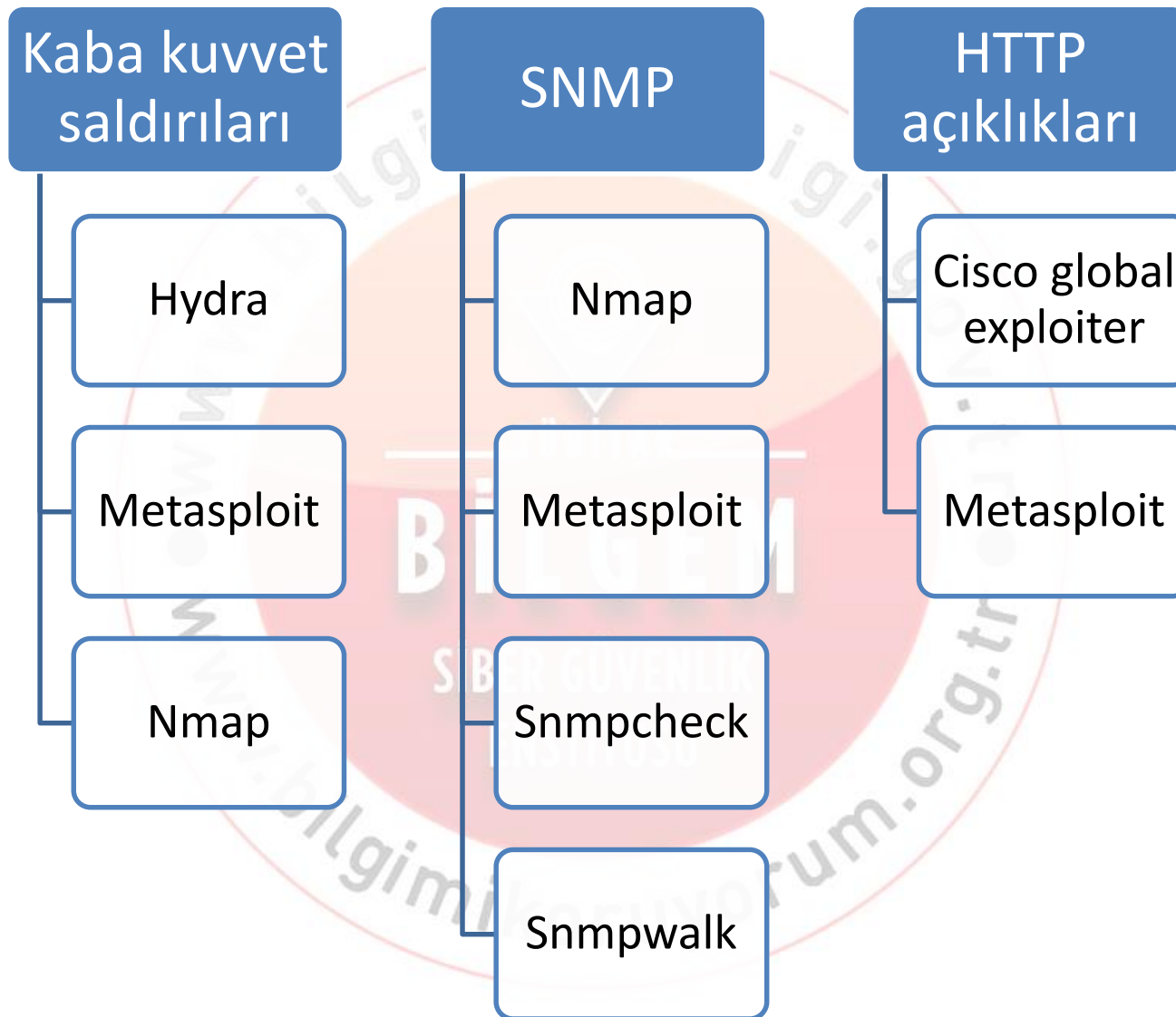
STP

Yönlendirme protokolleri

VTP

SNMP





## Kaba kuvvet saldırıları

- HTTP(S)
- SNMP
- Telnet
- SSH

## Parola korumasız HTTP arayüzleri

## Sistem yöneticilerinde bulunan yapılandırma yedekleri

## Sistem yöneticilerinde bulunan parola dosyaları

## Ağı dinlemek

- Telnet
- SNMP
- HTTP

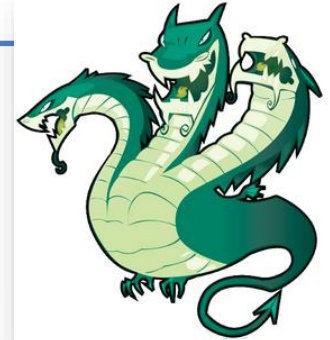
## Basit parolalar

## Tüm cihazlarda aynı parolanın kullanılması

## Kaba Kuvvet Saldırısı

### Hydra

- -l : Kullanıcı adı
- -L : Kullanıcı listesi
- -p : Parola
- -P : Parola listesi
- -V : Denemeleri göster
- -e nsr : Boş, aynı ve tersini dene
- -f: İlk doğru sonuçta sonlandır
- -M : Hedef sunucu listesi
- -o: Dosyaya yaz



### Kullanım

- Hydra <seçenekler> hedef\_IP servis

## Kaba Kuvvet Saldırısı

```
root@SGE:~# hydra -L userlist.txt -P passwd.txt -e nsr -V -f 10.1.1.1 telnet
Hydra V7.4.2 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at
[WARNING] telnet is by its nature unreliable to analyze reliable, if possible better
[DATA] 4 tasks, 1 server, 4 login tries (l:1/p:4), ~1 try per task
[DATA] attacking service telnet on port 23
[ATTEMPT] target 10.1.1.1 - login "cisco" - pass "cisco" - 1 of 4 [child 0]
[ATTEMPT] target 10.1.1.1 - login "cisco" - pass "" - 2 of 4 [child 1]
[ATTEMPT] target 10.1.1.1 - login "cisco" - pass "ocsic" - 3 of 4 [child 2]
[ATTEMPT] target 10.1.1.1 - login "cisco" - pass "passwd" - 4 of 4 [child 3]
[23][telnet] host: 10.1.1.1 login: cisco password: cisco
[STATUS] attack finished for 10.1.1.1 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at
root@SGE:~#
```

Telnet

HTTP

SSH

SNMP



## SNMP - Nmap Betiği ile Topluluk İsmi Keşfi

```
root@SGE:~# nmap -sU -p161 10.1.1.1 -sV -sC --script snmp-brute -n -Pn

Starting Nmap 6.25 ( http://nmap.org ) at
Nmap scan report for 10.1.1.1
Host is up (0.0011s latency).
PORT      STATE SERVICE VERSION
161/udp open  snmp     SNMPv1 server (public)
| snmp-brute:
|   private - Valid credentials
|   public - Valid credentials
MAC Address: 00:0B:5F:18:80:00 (Cisco Systems)
Service Info: Host: Switch.test

Service detection performed. Please report any incorrect results at http://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 1.80 seconds
root@SGE:~#
```

## SNMP - Yazma Hakkı Testi

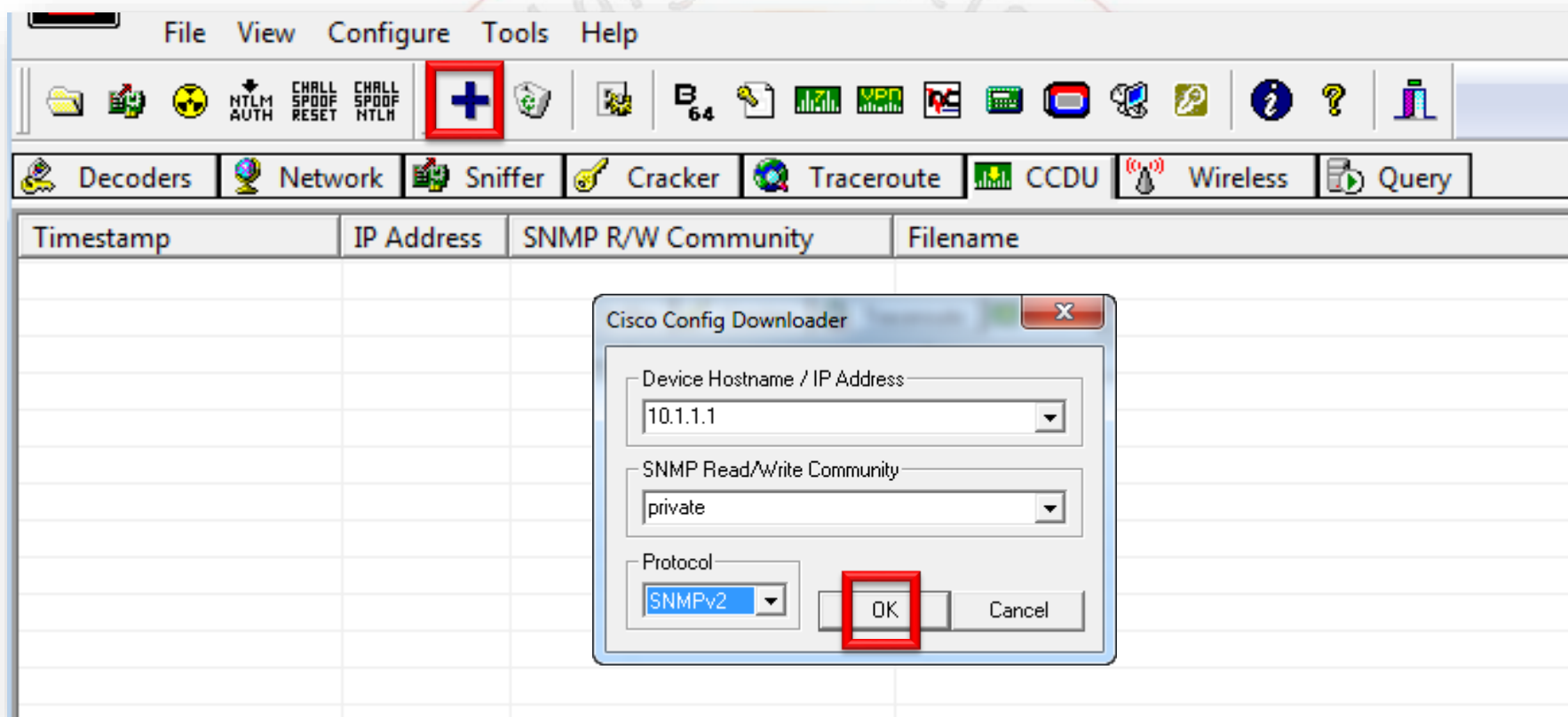
```
root@SGE:~# snmpcheck -t 10.1.1.1 -c private -w
snmpcheck.pl v1.8 - SNMP enumerator
Copyright (c) 2005-2011 by Matteo Cantoni (www.nothink.org)

[*] Try to connect to 10.1.1.1
[*] Connected to 10.1.1.1
[*] Starting enumeration at
[*] Write access enabled!
[*] Checked 10.1.1.1 in 0.02 seconds
root@SGE:~#
```

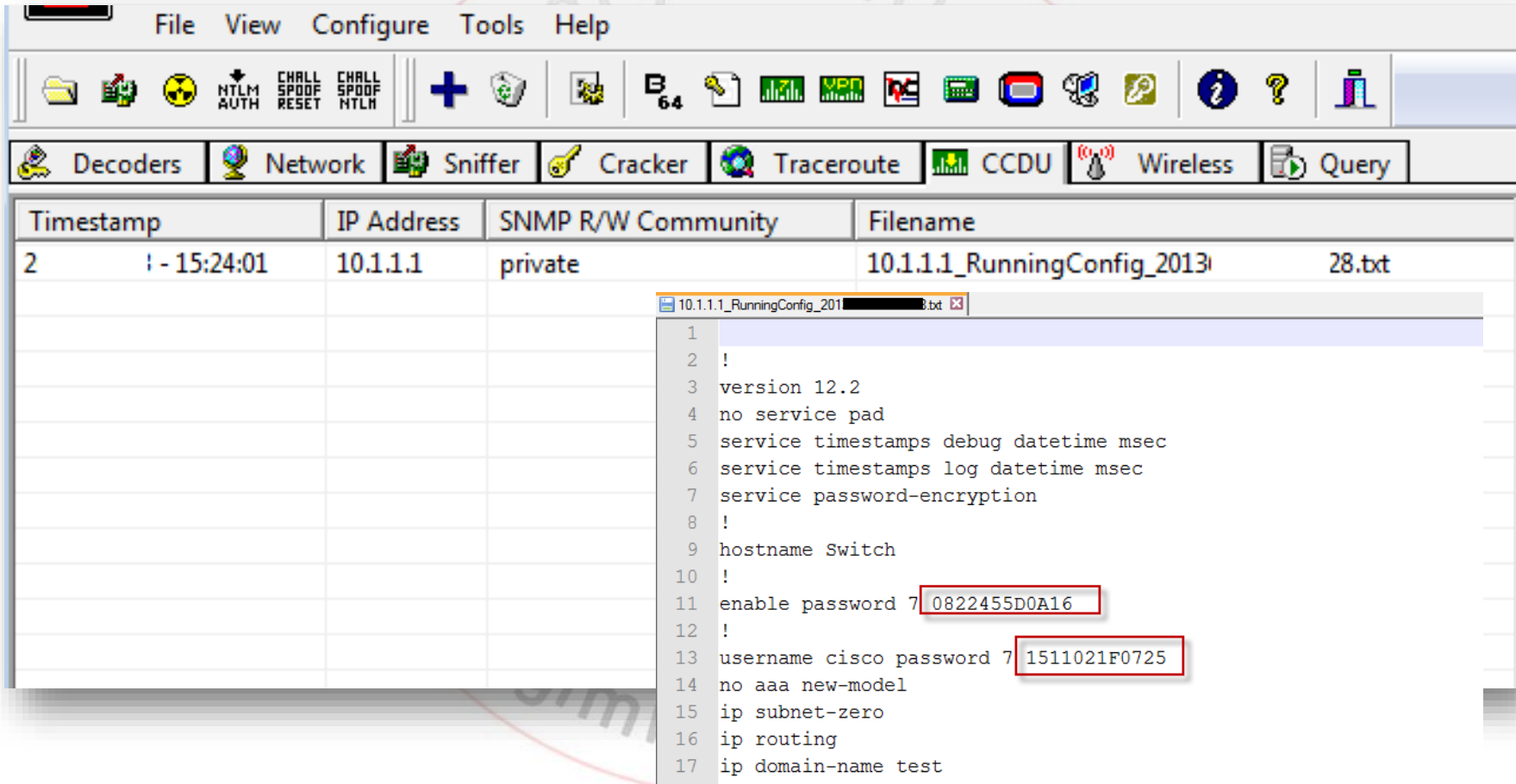
### Snmpcheck

- -t: Hedef IP adres
- -p: port numarası
- -c: Topluluk adı
- -w: Yazma hakkı kontrolü

## CAIN - SNMP ile Yapılandırma Çekilmesi



## CAIN - SNMP ile Yapılandırma Çekilmesi



The image shows the CAIN interface with a table of SNMP R/W Community entries. The table has columns for Timestamp, IP Address, SNMP R/W Community, and Filename. The first entry is for IP 10.1.1.1 with community 'private' and filename '10.1.1.1\_RunningConfig\_2013\_28.txt'. A detailed view of this configuration is shown in a separate window, listing various configuration commands.

Timestamp	IP Address	SNMP R/W Community	Filename	
2	! - 15:24:01	10.1.1.1	private	10.1.1.1_RunningConfig_2013_28.txt

```
1  
2 !  
3 version 12.2  
4 no service pad  
5 service timestamps debug datetime msec  
6 service timestamps log datetime msec  
7 service password-encryption  
8 !  
9 hostname Switch  
10 !  
11 enable password 7 0822455D0A16  
12 !  
13 username cisco password 7 1511021F0725  
14 no aaa new-model  
15 ip subnet-zero  
16 ip routing  
17 ip domain-name test
```

## Cisco Password 7 Şifresi Kırılması

10.1.1.1\_RunningConfig\_2018.txt

```
1
2 !
3 version 12.2
4 no service timestamps debug
5 service timestamps log
6 service timestamps msec
7 service password-encryption
8 !
9 hostname Switch
10 !
11 enable password 7 0822455D0A16
12 !
13 username cisco password 7 1511021F0725
14 no aaa new-model
15 ip subnet-zero
16 ip routing
17 ip domain-name test
```

Password to Decrypt: 0822455D0A16

Gönder

Your Password is cisco

[Decrypt another Password](#)

[Decrypt another Password](#)

## Yetkili Telnet Bağlantısı

```
C:\ Telnet 10.1.1.1

User Access Verification

Username: cisco
Password:
Switch>en
Password:
Switch#
Switch#sh run
Building configuration...

Current configuration : 7027 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Switch
!
enable password 7 0822455D0A16
!
username cisco password 7 1511021F0725
```

```
username cisco password 7 1511021F0725
!
enable password 7 0822455D0A16
!
hostname Switch
```

Erişim kontrol listelerinin olmaması

Anahtarların güvenli bir ağda olmaması

Password yönteminin kullanılması

HTTP ve HTTPS kullanımı

SNMP v1,2 kullanımı

Telnet kullanımı

Tek kullanıcı olması (ortak kullanımı)

Port güvenliğinin olmaması

Basit parolalar



Nmap ile  
anahtar tespit  
edilir

SSH servisine  
hydra ile kaba  
kuvvet saldırısı  
yapılır

SNMP  
servisine  
nmap ile kaba  
kuvvet saldırısı  
yapılır

SNMP topluluk  
ismi  
kullanılarak  
yapılandırma  
dosyası çekilir

Password ile  
şifrelenmiş  
parola kırılır



Ağı Dinleme



MAC Adres Tablosu Doldurma



ARP Zehirlemesi



DHCP sunucu IP adres havuzunun tüketilmesi



VLAN Hopping



Aktif Cihaz Sızma Testi



Anahtar Yapılandırma Denetimleri



# Anahtar Yapılandırma Denetimleri

## Parola Oluşturma Yöntemi

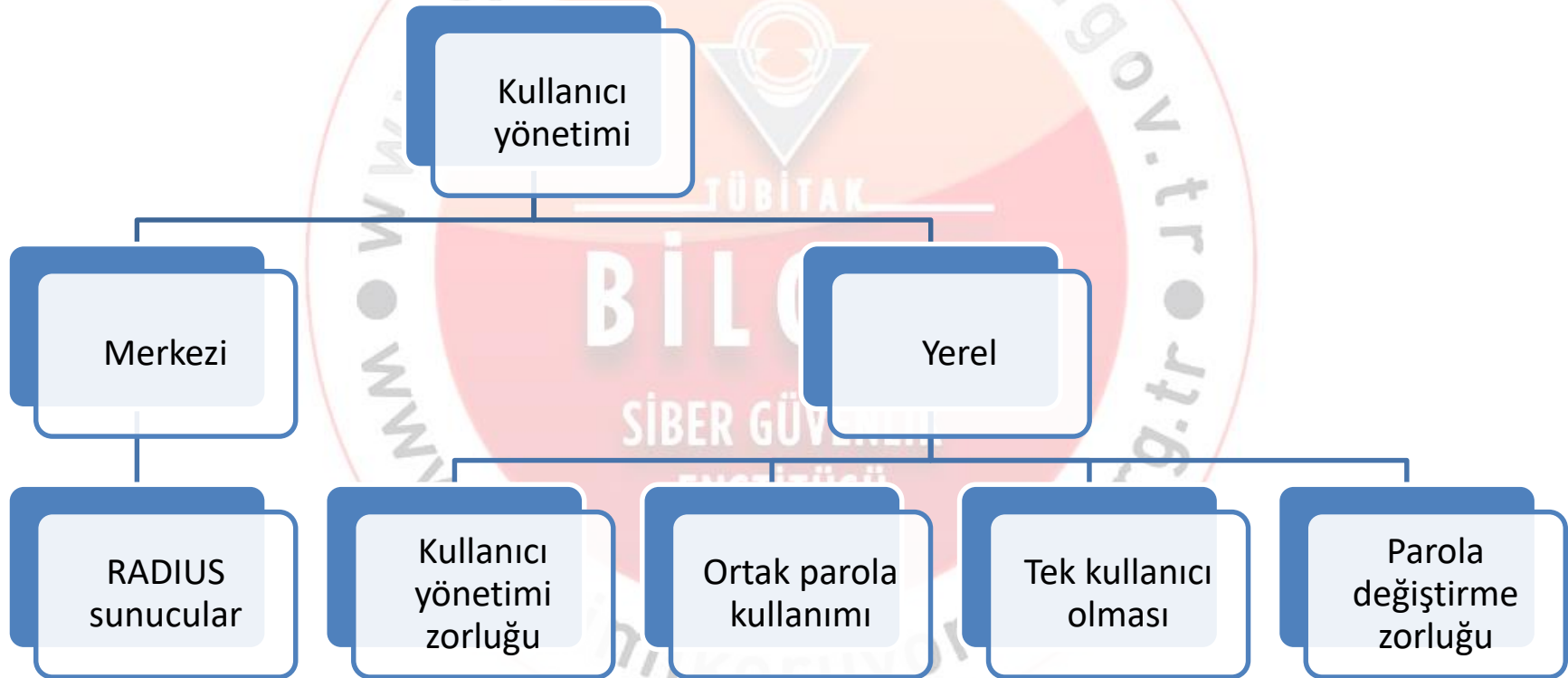
### Password

- Şifrelenmemiş parola üretir
- “service password-encryption”
- Saniyeler içinde kırılır
- Geri çevrilebilir, zayıf algoritma

### Secret

- MD5 şifreleme
- Geri çevrilemez
- Sözlük saldırısı gerekli

## Kullanıcı Yönetimi



## Erişim Kontrol Listeleri

### Yönetimsel servisler

- SNMP
- Telnet
- SSH

```
PORT  STATE SERVICE REASON
23/tcp open  telnet  syn-ack
MAC Address: 00:0B:5F:18:80:00 (Cisco Systems)
```

```
PORT  STATE SERVICE REASON
23/tcp closed telnet  reset
MAC Address: 00:0B:5F:18:80:00 (Cisco Systems)
```

```
access-list 10 permit 10.1.1.1
access-list 10 deny any
cdp timer 5
cdp holdtime 10
snmp-server community public RO
!
control-plane
!
!
line con 0
 logging synchronous
line vty 0 4
 access-class 10 in
 logging synchronous
 login local
 transport input all
```

## Servis Güvenliği

### Güvensiz

- HTTP(S)
- Telnet
- CDP
- SNMP

### Güvenli

- SSH
- Konsol erişimi

## SNMP Güvenliği

### SNMP v1,2

- Açık metin
- Kullanıcı yetkilendirme yok
- Güvenlik SNMP topluluk ismine bağlı

### SNMP v3

- Şifreleme yeteneği
- Kullanıcı yetkilendirme

Erişim Kontrol Listesi

## Port Güvenliği

Bir porttan kaç kişinin ağa bağlanabileceği

Bir porttan hangi MAC adreslerinin bağlanabileceği

## Yöntemler

- MAC kısıtlaması
- 802.1x
- NAC

## MAC kısıtlaması

- MAC sayısını kısıtla
- protect, restrict, shutdown
- ARP zehirlemesi saldırılarını önlemez !!



**TÜBİTAK**

**Teşekkürler**