



Keşif ve Zafiyet Tarama

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.

Açık sunucuların tespiti

Ağ topolojisi keşfi

Açık portların tespiti

Versiyon tespiti

İşletim sistemi keşfi

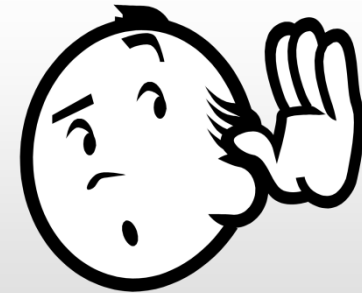
Zafiyet tespiti

Keşif Türleri

SİBER GÜVENLİK
KEŞİF ENSTİTÜSÜ

Pasif Keşif

- Ağın dinlenilmesi
 - Tcpdump
 - Wireshark
- ARP tablosu



Aktif Keşif

- Aktif paket gönderme
 - Nmap
 - Hping
 - Scapy
 - Ping, tracert, vb.



Pasif Keşif

Wireshark

Conversations: Intel(R) 82577LM Gigabit Network Connection: \Device\NPF_{58F07B79-B906-4162-B42E-E8632071A...}

Ethernet: 65 Fibre Channel FDDI IPv4: 35 IPv6: 16 IPX: 1 JXTA NCP RSVP SCTP TCP: 2 Token Ring UDP: 64 USB WLAN

IPv4 Conversations

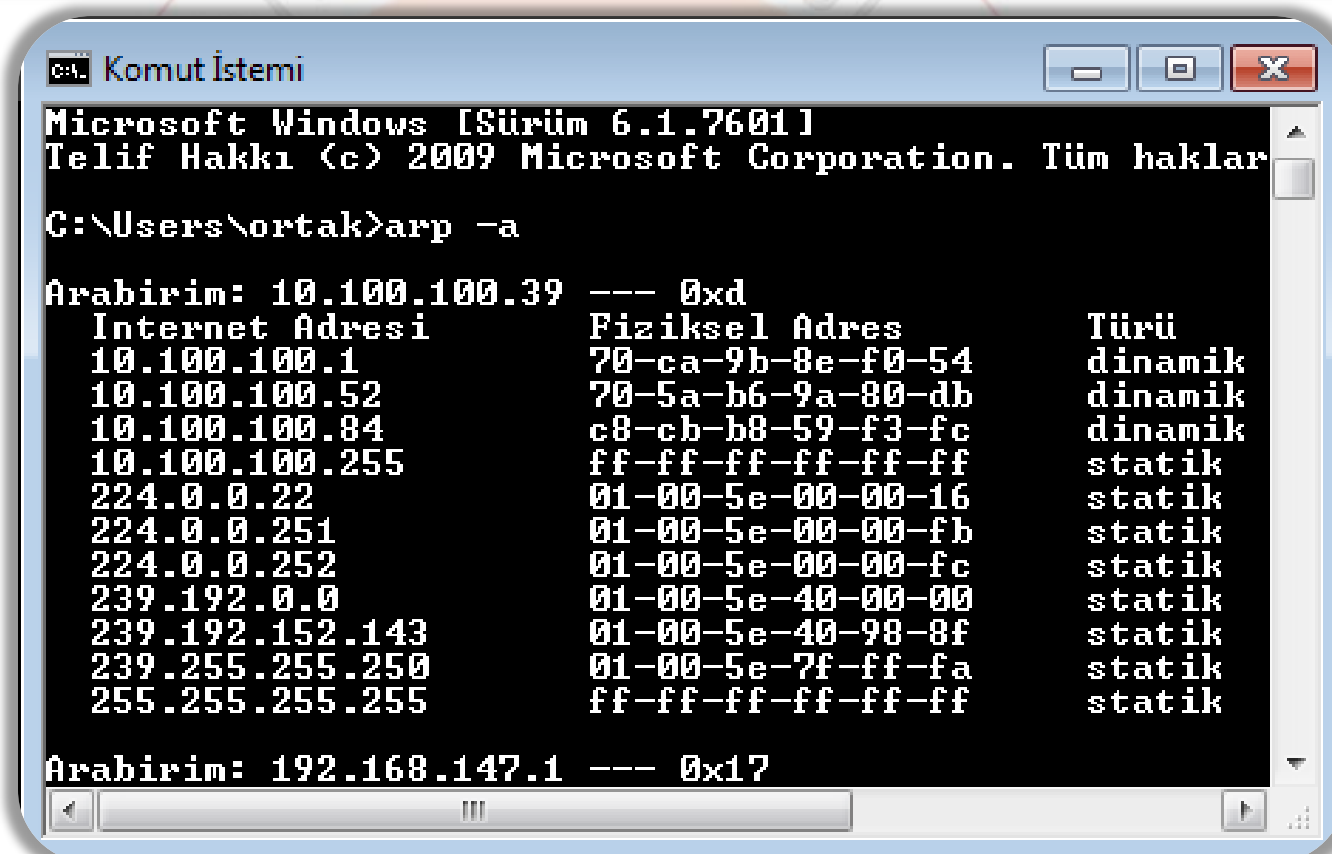
Address A	Address B	Packets A→B	Packets B→A	Bytes A→B	Bytes B→A	Rel. Size	Rel. Sta
10.100.10.10	10.100.120.82	22	22	2 240	0	0	2 240 0,000
10.100.10.20	10.100.120.82	10	15	1 628	5	756	872 0,061
10.100.120.19	10.100.120.255	0	32	7 776	32	7 776	0 26,910
10.100.120.22	10.100.120.255	0	384	35 328	384	35 328	0 6,921
10.100.120.32	10.100.120.255	0	64	15 552	64	15 552	0 21,488
10.100.120.51	10.100.120.255	0	960	88 320	960	88 320	0 11,169
10.100.120.62	10.100.120.255	0	384	35 328	384	35 328	0 7,298
10.100.120.63	10.100.120.255	0	960	88 320	960	88 320	0 3,098
10.100.120.63	224.0.0.252	0	2	150	2	150	0 16,996
10.100.120.72	10.100.120.255	0	960	88 320	960	88 320	0 1,082
10.100.120.81	255.255.255.255	0	2	684	2	684	0 21,093
10.100.120.81	224.0.0.252	0	2	128	2	128	0 21,261

☒ Name resolution ☐ Limit to display filter

Help Copy Follow Stream Close

Pasif Keşif

ARP Tablosu

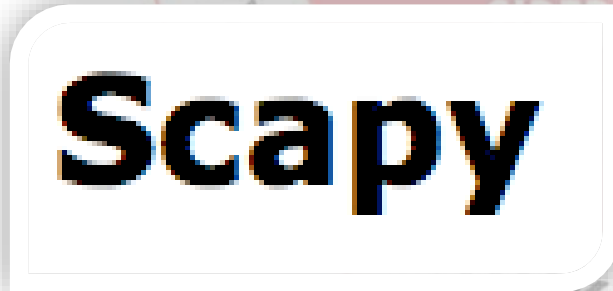


```
Microsoft Windows [Sürüm 6.1.7601]
Telif Hakkı (c) 2009 Microsoft Corporation. Tüm haklar
C:\Users\ortak>arp -a

Arabirim: 10.100.100.39 --- 0xd
Internet Adresi      Fiziksel Adres      Türü
10.100.100.1         70-ca-9b-8e-f0-54   dinamik
10.100.100.52        70-5a-b6-9a-80-db   dinamik
10.100.100.84        c8-cb-b8-59-f3-fc   dinamik
10.100.100.255       ff-ff-ff-ff-ff-ff   statik
224.0.0.22           01-00-5e-00-00-16   statik
224.0.0.251          01-00-5e-00-00-fb   statik
224.0.0.252          01-00-5e-00-00-fc   statik
239.192.0.0           01-00-5e-40-00-00   statik
239.192.152.143      01-00-5e-40-98-8f   statik
239.255.255.250      01-00-5e-7f-ff-fa   statik
255.255.255.255      ff-ff-ff-ff-ff-ff   statik

Arabirim: 192.168.147.1 --- 0x17
```

Aktif Keşif

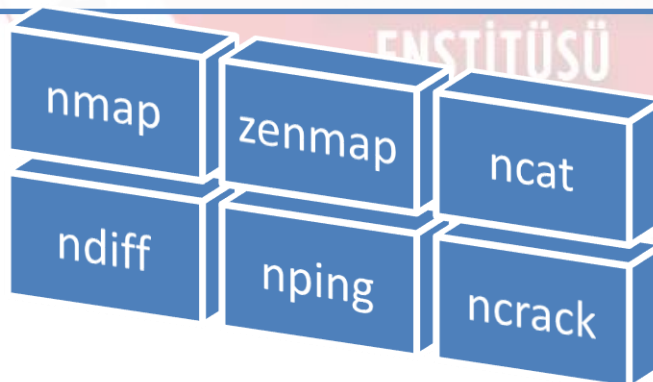


NMAP

SİBER GÜVENLİK
ENSTİTÜSÜ

NMAP

- Ağ tarama aracı
- Açık kaynak kodlu
- Ücretsiz
- Yaygın kullanım
- Geniş bir topluluk desteği
- Güçlü
- Birçok işi tek başına yapabilir
- Her platformda çalışır
- İyi dokümantasyon



Sunucu keşfi

Ağ topolojisi keşfi

Port taraması

Servis ve versiyon tespiti

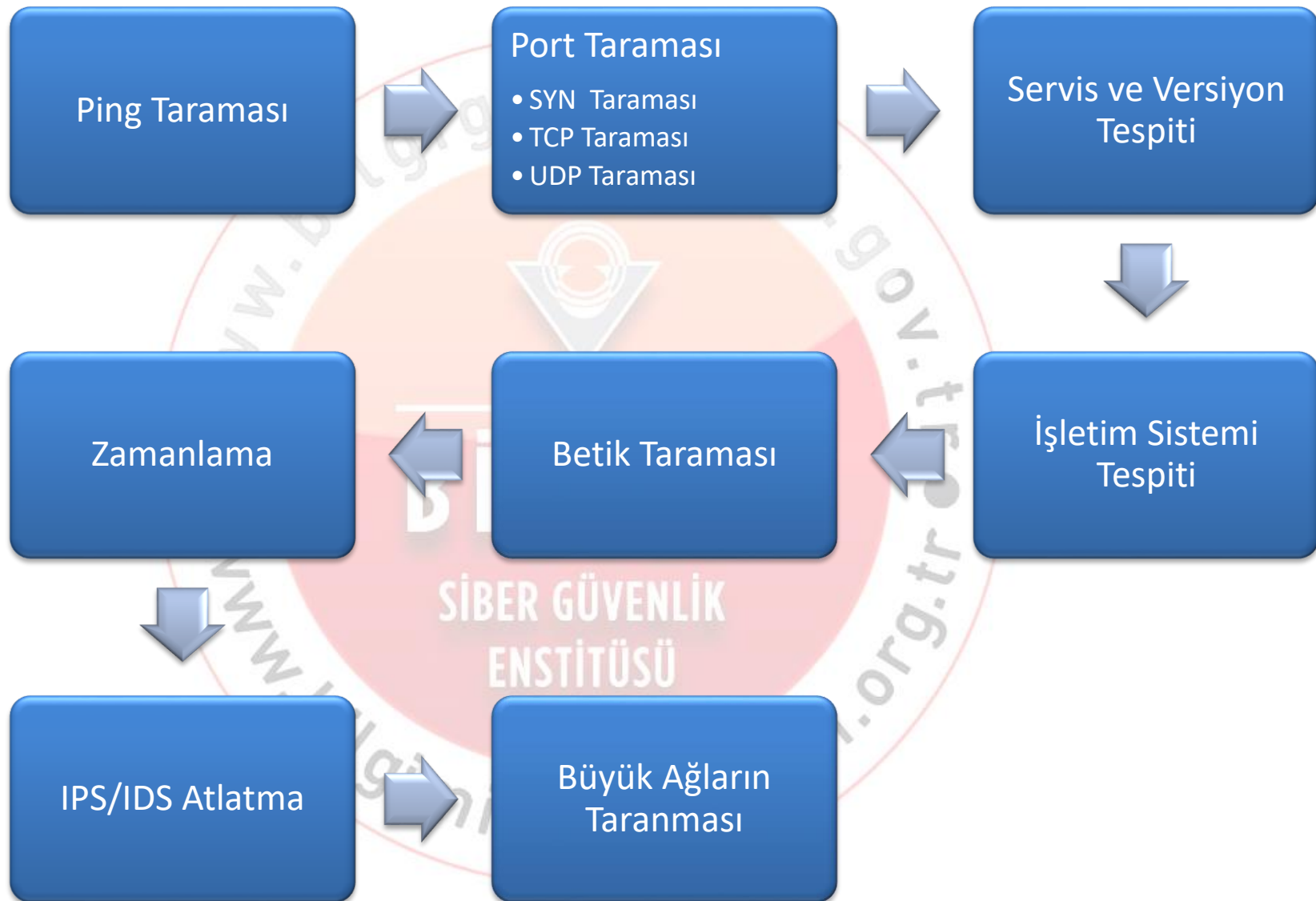
İşletim sistemi tespiti

Güvenlik duvarı tespiti

Zafiyet tespiti

Kaba kuvvet saldırısı

Exploit



NMAP Ping Taraması

SİBER GÜVENLİK
ENSTİTÜSÜ

Açık sunucuların tespiti

```
# nmap -sP 172.20.1.0/24
```

- ICMP echo request
- TCP 443 portuna SYN
- TCP 80 portuna ACK
- ICMP timestamp request

Lokal ağda "ARP scan"

Nmap Ping Taraması

```
root@SGE:~# nmap -sP -n 192.168.161.0/24
```

```
Starting Nmap 6.25 ( http://nmap.org ) at
Nmap scan report for 192.168.161.1
Host is up (0.00029s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.161.2
Host is up (0.00032s latency).
MAC Address: 00:50:56:E4:8A:9F (VMware)
Nmap scan report for 192.168.161.132
Host is up.
Nmap scan report for 192.168.161.254
Host is up (0.00046s latency).
MAC Address: 00:50:56:EB:1D:06 (VMware)
Nmap done: 256 IP addresses (4 hosts up) scanned in 6.26 seconds
```

```
root@SGE:~#
```

```
root@SGE:~#
```

```
root@SGE:~# nmap -sP -n 192.168.161.0/24 | grep "Nmap scan" | cut -d' ' -f5
192.168.161.1
192.168.161.2
192.168.161.132
192.168.161.254
```

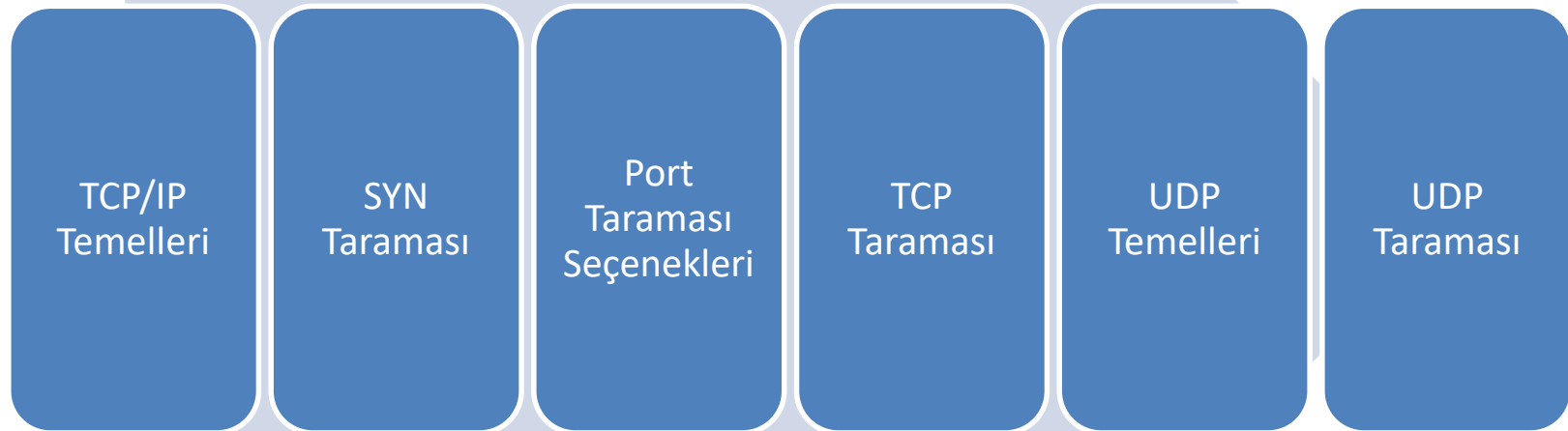
```
root@SGE:~#
```

```
root@SGE:~#
```

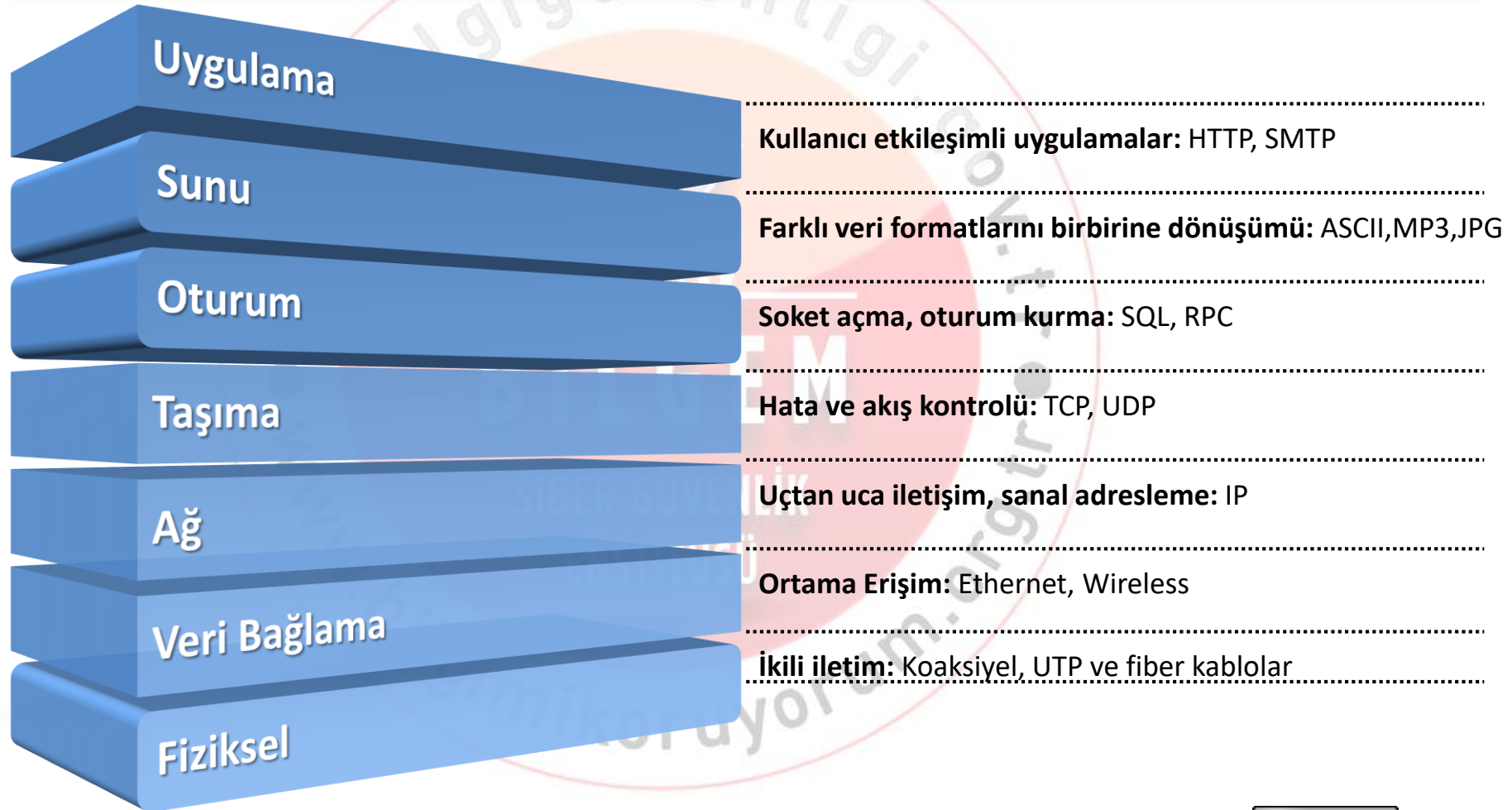
```
root@SGE:~#
```

NMAP Port Taraması

SİBER GÜVENLİK
ENSTİTÜSÜ

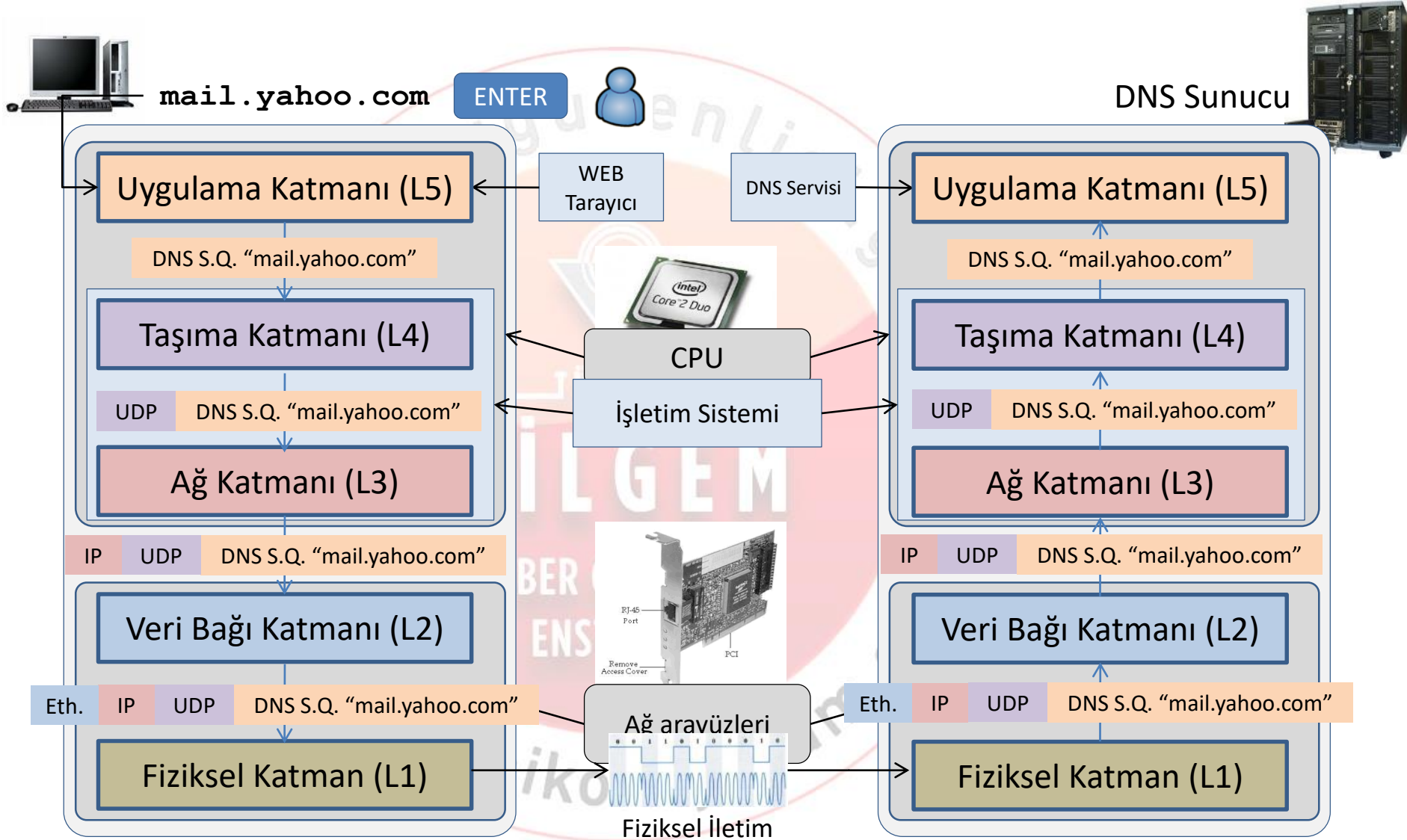


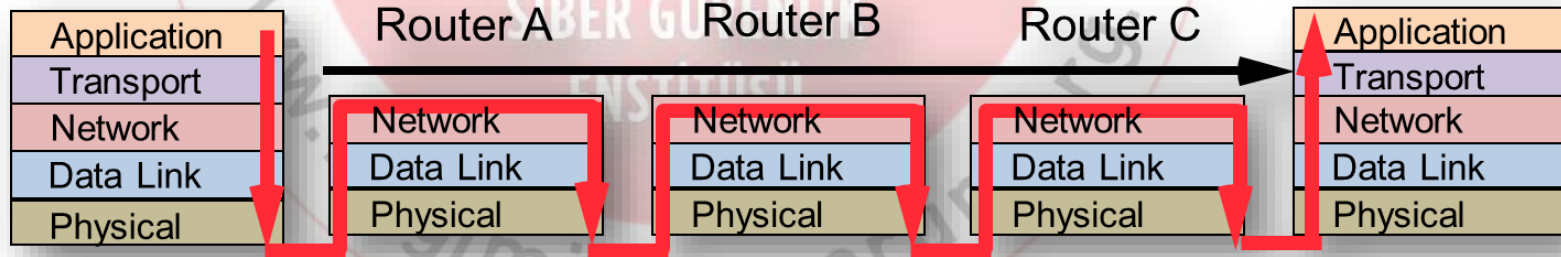
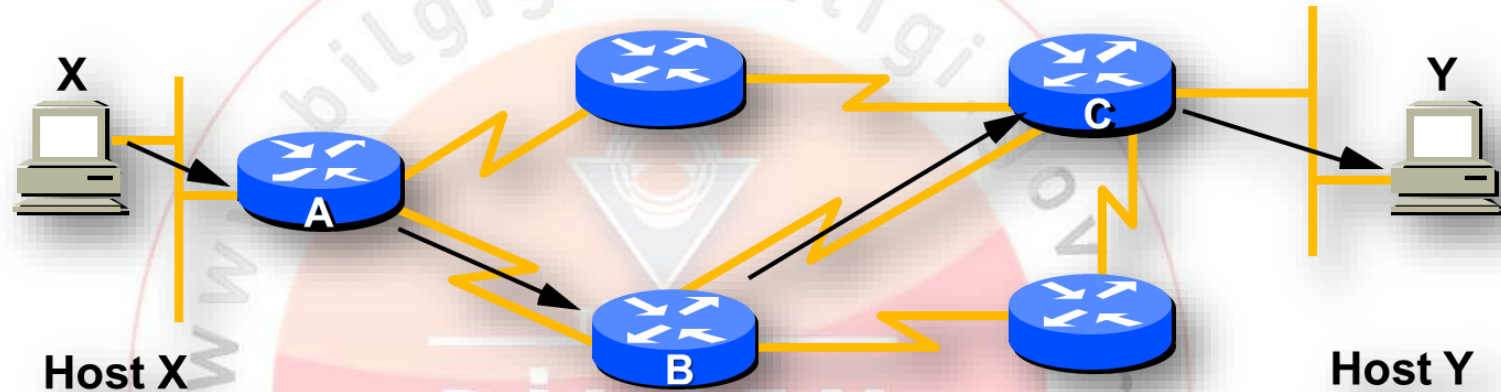
OSI Referans Modeli



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, 100Base-Tc...)						

Örnek: DNS Protokolü



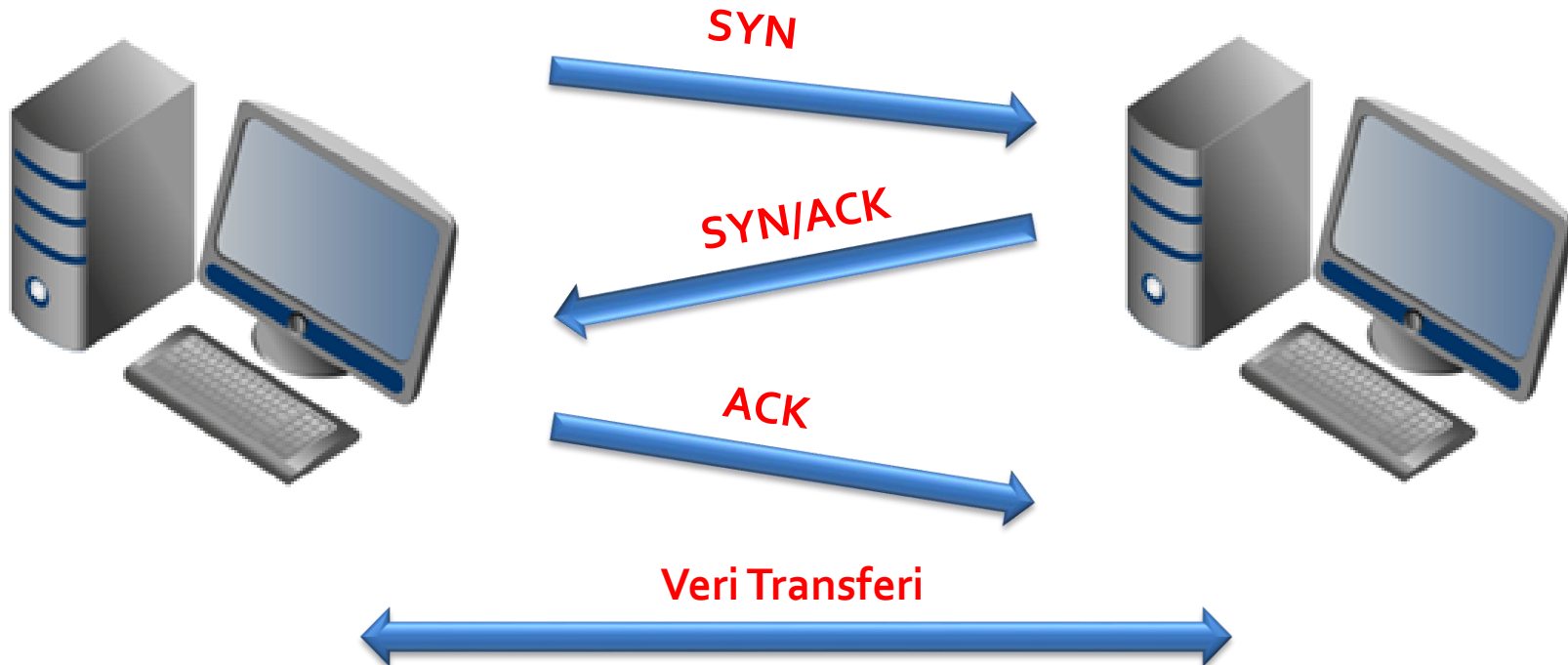


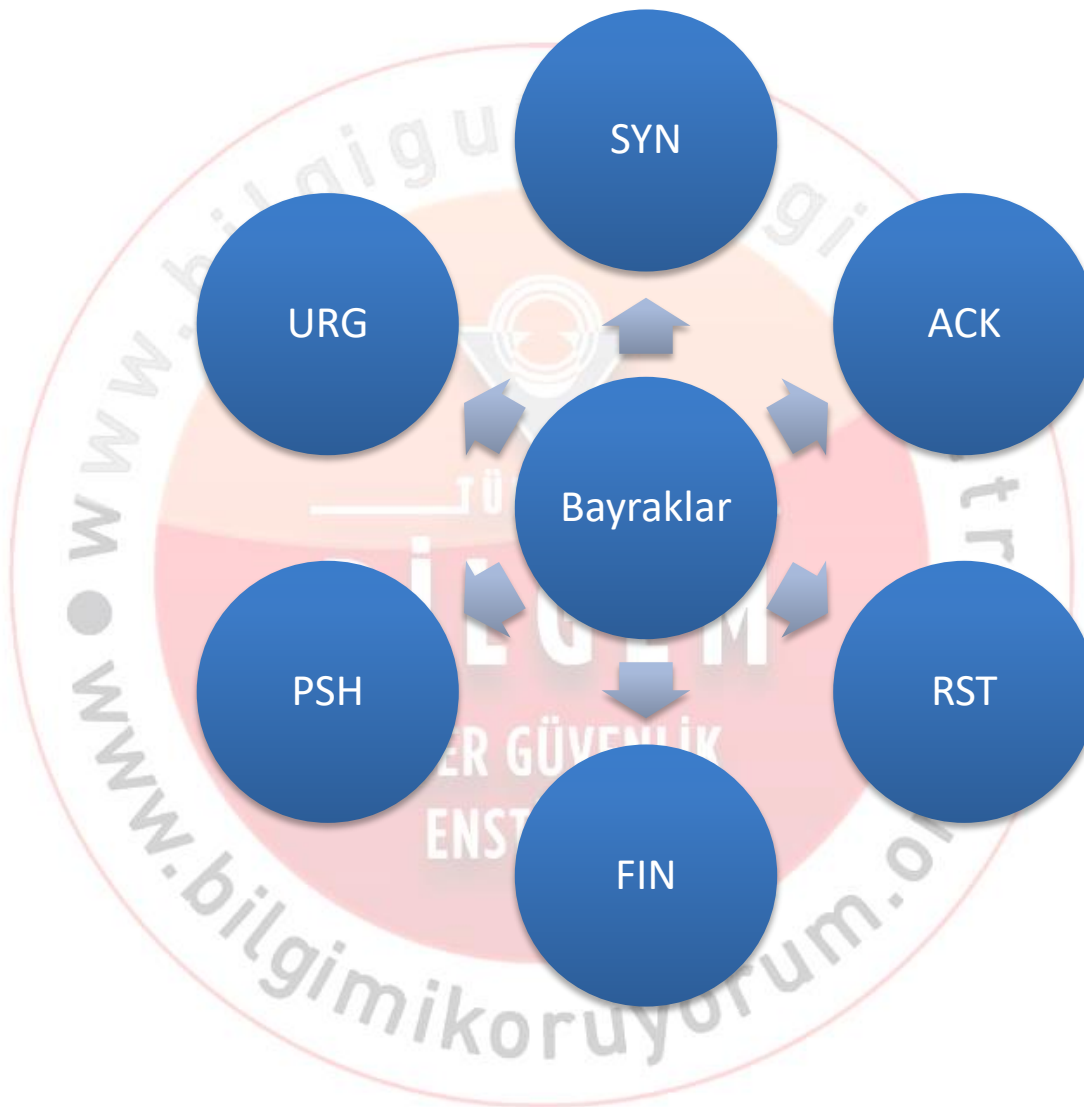
Özellikler

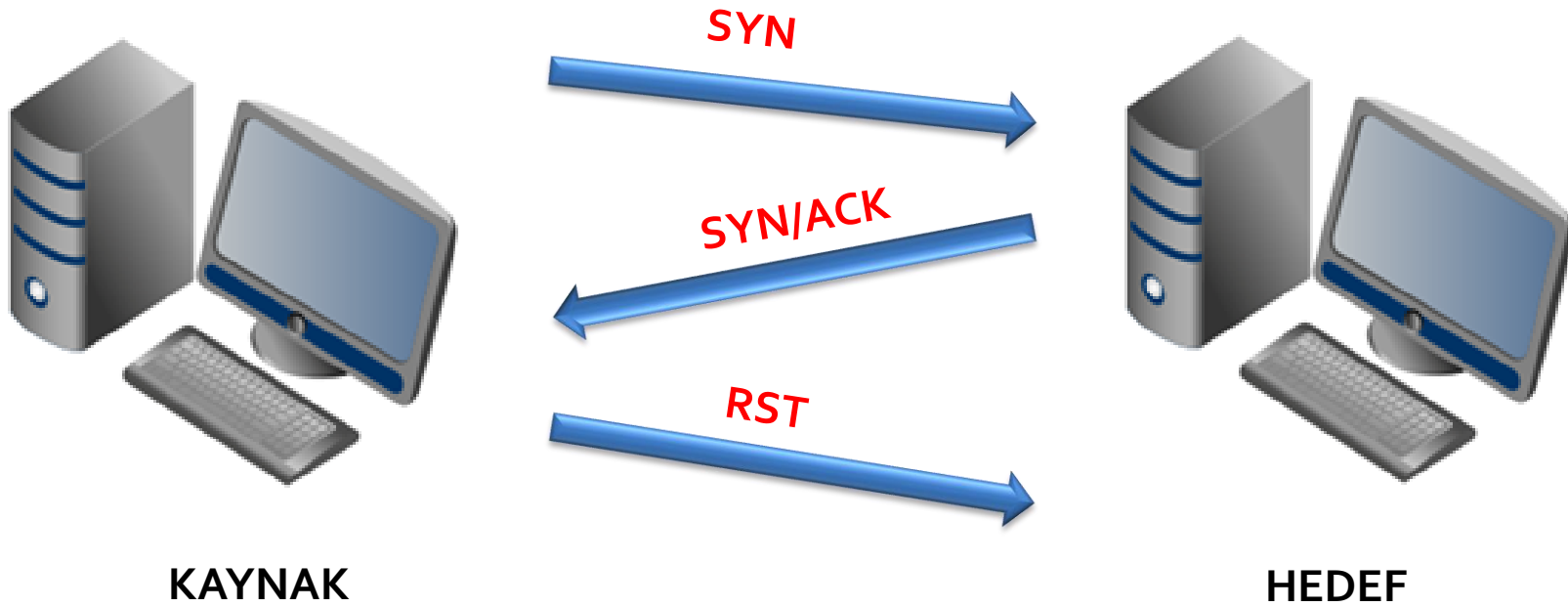
- Bağlantı yönelimlidir
- Verilere sıra numarası eklenir
- Veriler parçalara bölünebilir
- Güvenilirdir
- Akış kontrolü mekanizması vardır
- Çift yönlüdür



TCP 3'lü el sıkışma







```
root@SGE:~# nmap -sS 10.0.0.1 -p22,23,25

Starting Nmap 6.25 ( http://nmap.org ) at 20
Nmap scan report for 10.0.0.1
Host is up (0.0013s latency).
PORT      STATE      SERVICE
22/tcp    filtered  ssh
23/tcp    closed    telnet
25/tcp    open      smtp

Nmap done: 1 IP address (1 host up) scanned
root@SGE:~#
```

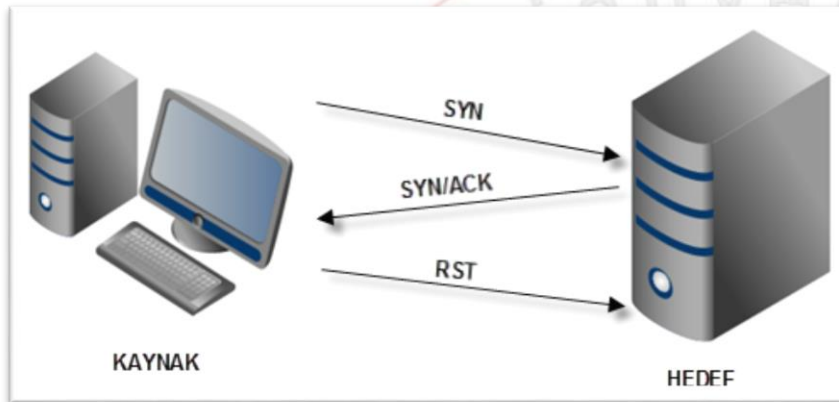
Filter: ip.addr == 10.0.0.1



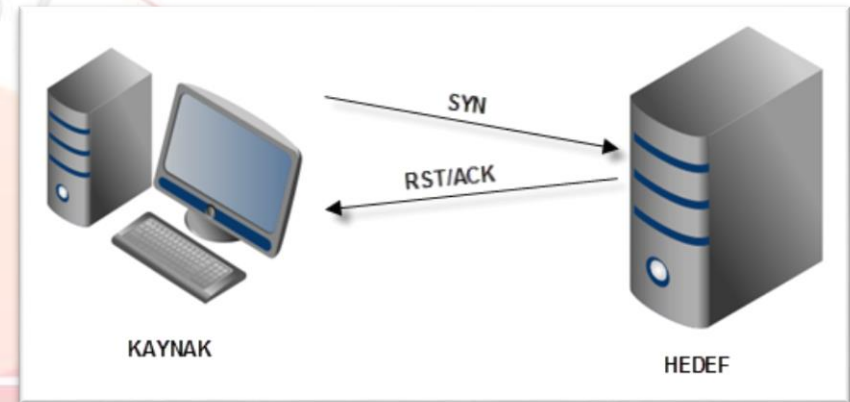
Expression... Clear

Source	Destination	Protocol	Info
10.100.120.102	10.0.0.1	TCP	40131 > smtp [SYN] Seq=0 Win=1024
10.100.120.102	10.0.0.1	TCP	40131 > telnet [SYN] Seq=0 Win=1024
10.100.120.102	10.0.0.1	TCP	40131 > ssh [SYN] Seq=0 Win=1024
10.0.0.1	10.100.120.102	TCP	smtp > 40131 [SYN, ACK] Seq=0 Ack=40132
10.100.120.102	10.0.0.1	TCP	40131 > smtp [RST] Seq=1 Win=0 Len=0
10.0.0.1	10.100.120.102	TCP	telnet > 40131 [RST, ACK] Seq=1 Ack=40132
10.100.120.102	10.0.0.1	TCP	40132 > ssh [SYN] Seq=0 Win=1024

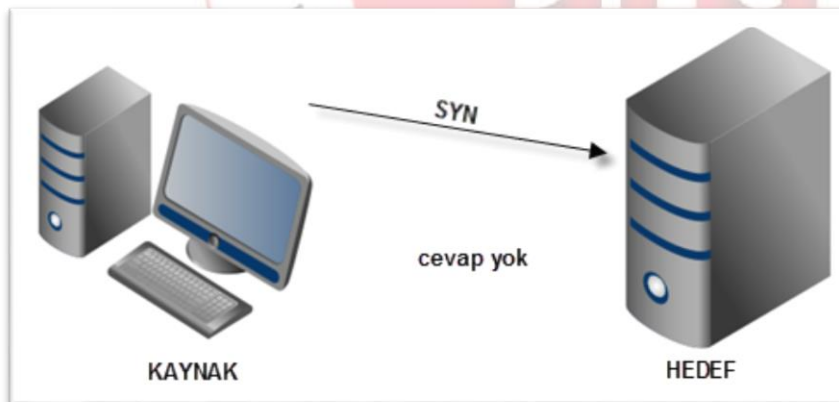
OPEN



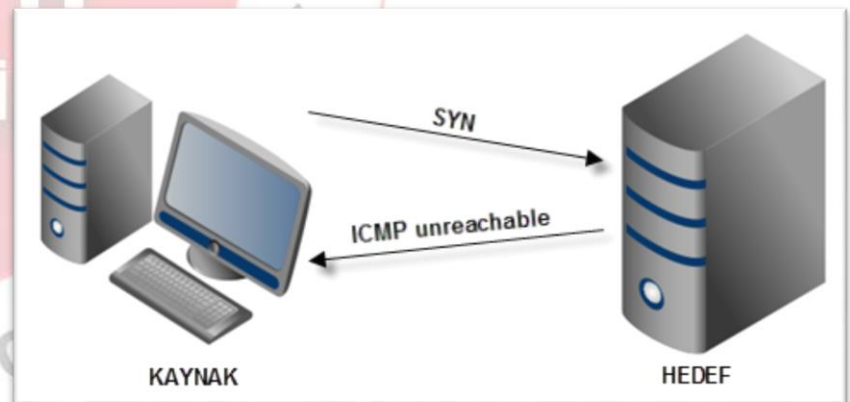
CLOSED



FILTERED



FILTERED



open

- Porta erişim var
- Bir servis dinliyor

closed

- Porta erişim var
- Güvenlik duvarı trafiği filtrelemiyor
- Port üzerinde dinleyen bir servis yok
- Örnek: Sunucu RST dönmüş

filtered

- Cevap alınamamış
- Güvenlik duvarı trafiği filtrelemiş
- Port açık veya kapalı olabilir

open | filtered

- Cevap alınamamış
- Güvenlik duvarı filtrelemiş olabilir
- Uygulama cevap dönmemiş olabilir
- UDP taraması

Önemli Port Numaraları

21 - FTP

22 - SSH

23 - Telnet

25 - SMTP

53 (UDP) - DNS

80 - HTTP

110 - POP3

139 - Netbios

143 - IMAP

161 (UDP) - SNMP

443 - HTTPS

445 - SMB, Microsoft-DS

514 - RSH

902 - VMware

1433 - MSSQL

1521 - Oracle

3306 - MySQL

3389 - RDP

5900 - VNC

8080, 8081 - Proxy, Uygulama Sunucu

En sık kullanılan 1000 port

--top-ports 10

-p 80,443,445-447

-F (fast)

-sU -sT -pU:53,T:21-25,80

Tüm portlar: -p1-65535

```
root@SGE:~# nmap -sS --reason 10.0.0.1 --top-ports 10 -n

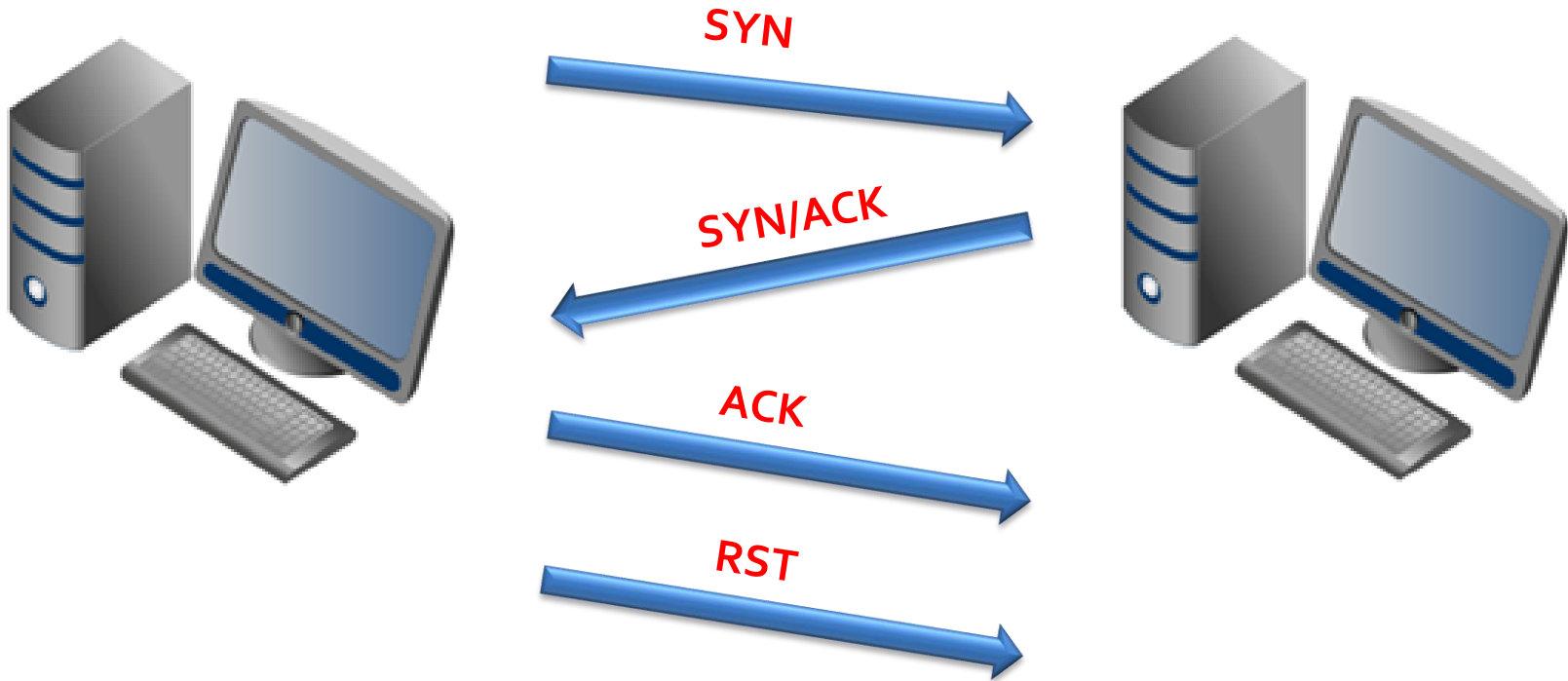
Starting Nmap 6.25 ( http://nmap.org ) at
Nmap scan report for 10.0.0.1
Host is up, received reset (0.00089s latency).
PORT      STATE      SERVICE      REASON
21/tcp    closed    ftp          reset
22/tcp    filtered  ssh          no-response
23/tcp    closed    telnet       reset
25/tcp    open      smtp         syn-ack
80/tcp    open      http         syn-ack
110/tcp   open      pop3         syn-ack
139/tcp   open      netbios-ssn  syn-ack
443/tcp   closed    https        reset
445/tcp   open      microsoft-ds syn-ack
3389/tcp  closed    ms-wbt-server reset

Nmap done: 1 IP address (1 host up) scanned in 1.30 seconds
```

Port Taraması ile Sunucu keşfi

- Sunucular ping'e kapalı ise
- Özellikle dış taramalar veya sunucu bloğu taramaları
- # `nmap -sS --top-ports 10 --open 172.20.1.0/24 -PN -n`

```
# nmap -sT 10.0.0.1 -PN -n -p80
```



SYN Taraması

Filter: `ip.addr == 10.0.0.1` Expression... Clear

Source	Destination	Protocol	Info
10.100.120.102	10.0.0.1	TCP	39649 > http [SYN] Seq=0 Win=10
10.0.0.1	10.100.120.102	TCP	http > 39649 [SYN, ACK] Seq=0 A
10.100.120.102	10.0.0.1	TCP	39649 > http [RST] Seq=1 Win=0

TCP Taraması

Filter: `ip.addr == 10.0.0.1` Expression... Clear App

Source	Destination	Protocol	Info
10.100.120.102	10.0.0.1	TCP	41656 > http [SYN] Seq=0 Win=14600 L
10.0.0.1	10.100.120.102	TCP	http > 41656 [SYN, ACK] Seq=0 Ack=1 W
10.100.120.102	10.0.0.1	TCP	41656 > http [ACK] Seq=1 Ack=1 Win=14
10.100.120.102	10.0.0.1	TCP	41656 > http [RST, ACK] Seq=1 Ack=1 W

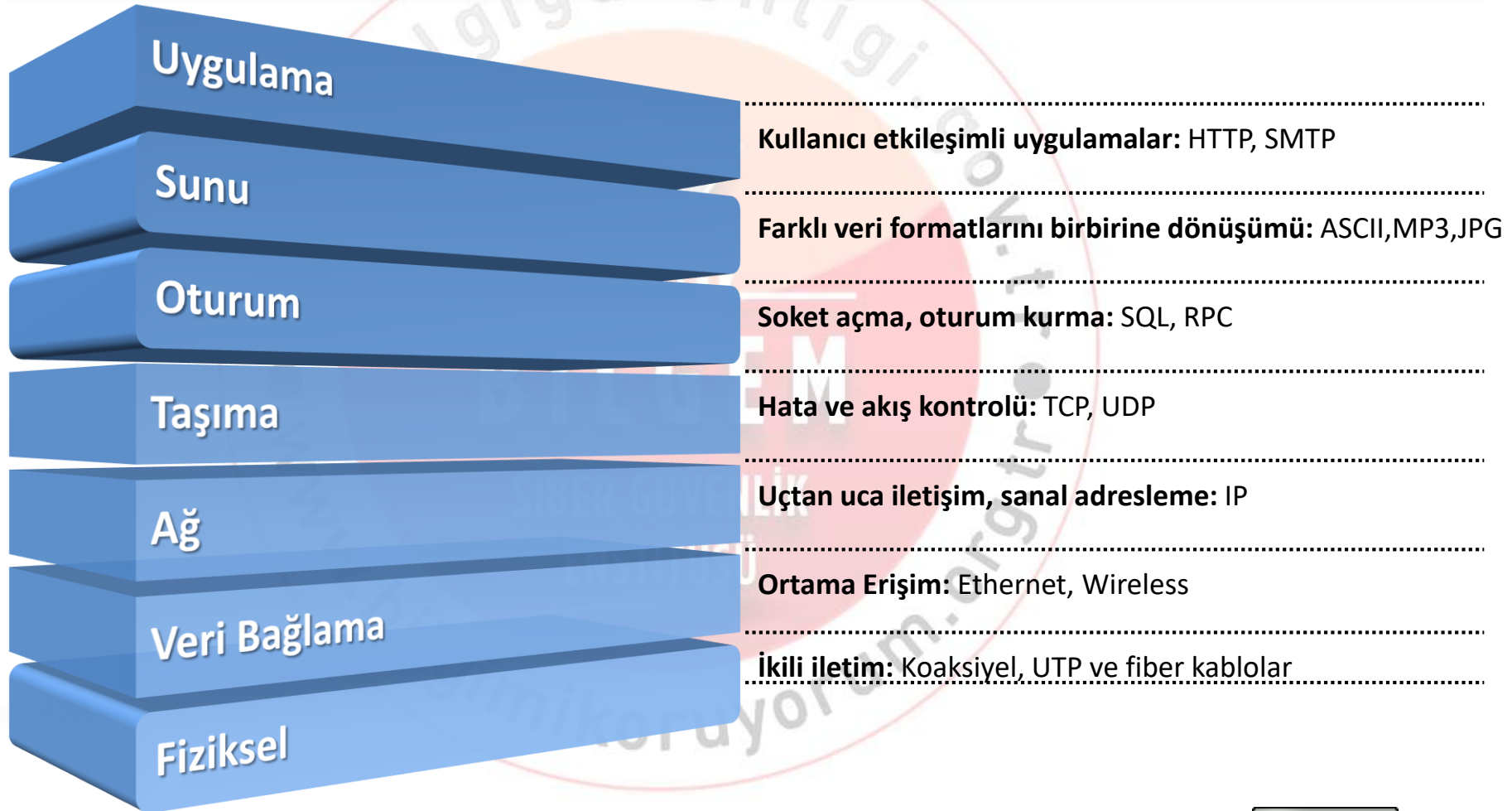
SYN Taraması

- 3'lü el sıkışma tamamlanmaz
- SYN+ACK gelirse RST ile bağlantı kapatılır
- Sunucuda kayıt tutulmaz
- Root hakkı gerektirir
 - Paketlere müdahale gerekli

TCP Taraması

- 3'lü el sıkışma tamamlanır
- SYN+ACK gelirse ACK ile bağlantı tamamlanır
- Sunucuda bağlantıya ilişkin kayıt tutulur
- İşletim sistemi TCP connect() metodu kullanır, root hakkı gerektirmez

OSI Referans Modeli



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

```
# nmap -sU -p161 10.0.0.1
```

- Uzun zaman alır (timeouts)
- Belirli portlar:
 - DNS (53), TFTP (69), DHCP (67-68), NTP (123), SNMP (161-162)
- Boş UDP paketi gönderir
- Versiyon tespiti ile birlikte çalıştırılmalı



```
root@SGE:~# nmap -sU --top-ports 10 -Pn -n --reason 10.0.0.254
```

```
Starting Nmap 6.25 ( http://nmap.org )
```

```
Nmap scan report for 10.0.0.254
```

```
Host is up, received user-set (0.0056s latency).
```

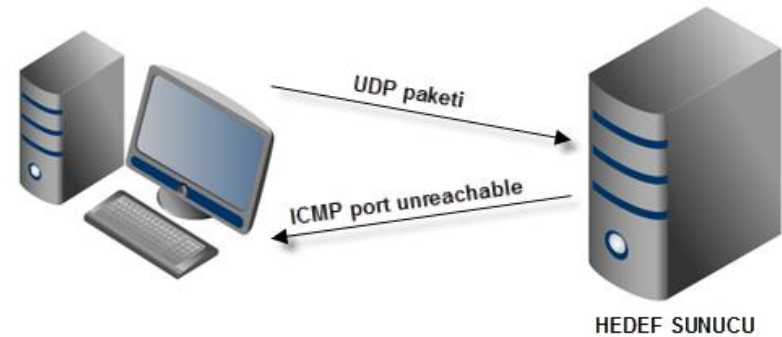
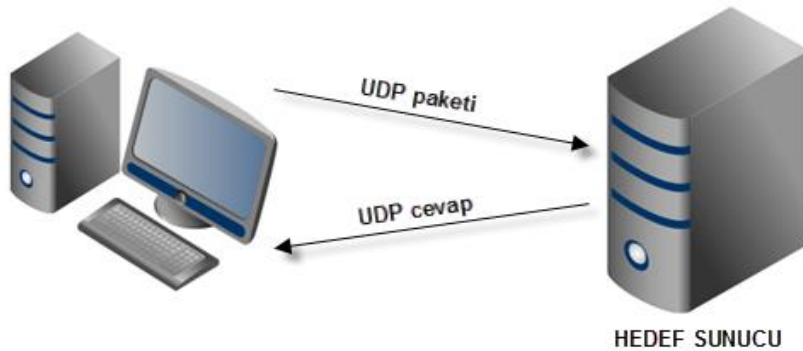
PORT	STATE	SERVICE	REASON
53/udp	filtered	domain	port-unreach from 192.168.20.100
67/udp	open filtered	dhcps	no-response
123/udp	open	ntp	udp-response
135/udp	filtered	msrpc	port-unreach from 192.168.20.100
137/udp	filtered	netbios-ns	port-unreach from 192.168.20.100
138/udp	filtered	netbios-dgm	port-unreach from 192.168.20.100
161/udp	open	snmp	udp-response
445/udp	open filtered	microsoft-ds	no-response
631/udp	filtered	ipp	port-unreach from 192.168.20.100
1434/udp	filtered	ms-sql-m	port-unreach from 192.168.20.100

```
Nmap done: 1 IP address (1 host up) scanned in 6.10 seconds
```

```
root@SGE:~#
```

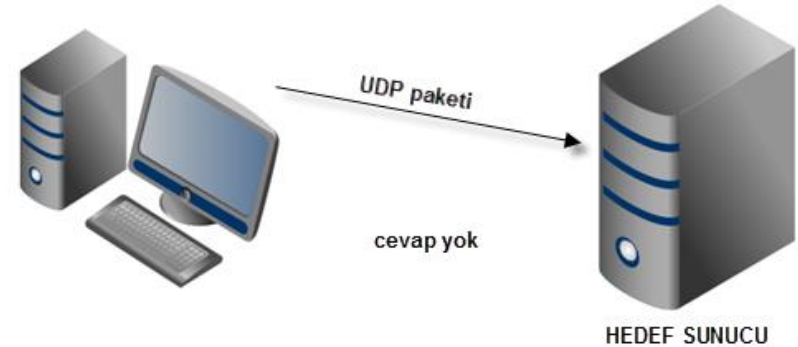
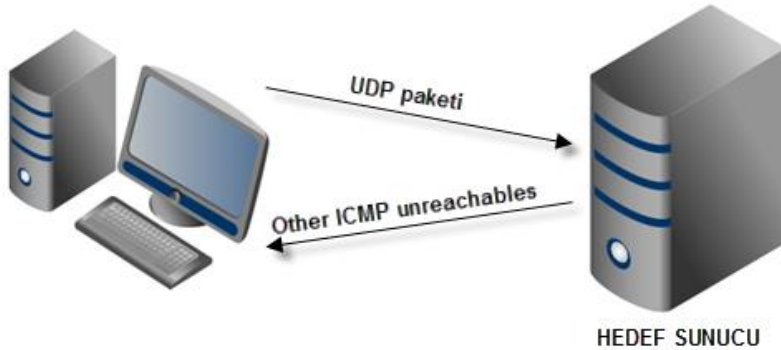
OPEN

CLOSED



FILTERED

OPEN|FILTERED





- ☒ Ping Taraması
- ☒ Port Taraması
- ☒ SYN ve TCP Taramaları
- ☒ UDP Taraması
- ☐ Servis ve Versiyon Tespiti
- ☐ İşletim Sistemi Tespiti
- ☐ Betik Taraması
- ☐ Zamanlama ve IPS/IDS Atlatma
- ☐ Büyük Ağların Taranması



Servis, Versiyon ve İşletim Sistemi Tespiti

İşletim Sistemi Tespiti
SİBER GÜVENLİK
ENSTİTÜSÜ

Port üzerinde çalışan servisin tespiti

- Uygulama belirli portta çalışmak zorunda değil
- TCP/443 portunda SSH çalışabilir

Portta çalışan uygulamanın versiyonu

- ISC BIND DNS veya Microsoft DNS
- ISC BIND DNS versiyon numarası

nmap-service-probes veritabanı

- Uygulama protokolü (FTP, SSH, ...)
- Uygulama adı (ISC BIND, Apache httpd, ...)
- Versiyon numarası
- Sunucu adı
- Cihaz türü (yazıcı, yönlendirici, ...)
- İşletim sistemi ailesi (Windows, Linux, ...)

```
root@SGE:~# nmap -sT 10.100.120.136 -n -Pn
```

```
Starting Nmap 6.25 ( http://nmap.org )
```

```
Nmap scan report for 10.100.120.136
```

```
Host is up (0.00076s latency).
```

```
Not shown: 997 closed ports
```

```
PORT      STATE SERVICE
```

```
22/tcp    open  ssh
```

```
80/tcp    open  http
```

```
443/tcp   open  https
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

```
root@SGE:~# nmap -sT 10.100.120.136 -n -Pn -sV
```

```
Starting Nmap 6.25 ( http://nmap.org )
```

```
Nmap scan report for 10.100.120.136
```

```
Host is up (0.00065s latency).
```

```
Not shown: 997 closed ports
```

```
PORT      STATE SERVICE      VERSION
```

```
22/tcp    open  ssh          OpenSSH 5.3p1 Debian 3ubuntu7 (Ubuntu Linux; protocol 2.0)
```

```
80/tcp    open  tcpwrapped
```

```
443/tcp   open  ssh          OpenSSH 5.3p1 Debian 3ubuntu7 (Ubuntu Linux; protocol 2.0)
```

```
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Service detection performed. Please report any incorrect results at http://nmap.org.
```

```
Nmap done: 1 IP address (1 host up) scanned in 34.04 seconds
```

```
root@SGE:~# nmap -sU -p161 10.1.0.3 -Pn -n
```

```
Starting Nmap 6.25 ( http://nmap.org )
```

```
Nmap scan report for 10.1.0.3
```

```
Host is up.
```

PORT	STATE	SERVICE
161/udp	open filtered	snmp

```
Nmap done: 1 IP address (1 host up) scanned in 2.08 seconds
```

```
root@SGE:~# nmap -sU -p161 10.1.0.3 -Pn -n -sV
```

```
Starting Nmap 6.25 ( http://nmap.org )
```

```
Nmap scan report for 10.1.0.3
```

```
Host is up.
```

PORT	STATE	SERVICE	VERSION
161/udp	open	snmp	SNMPv1 server (public)

```
Service Info: Host:
```

```
Service detection performed. Please report any incorrect results a
```

```
Nmap done: 1 IP address (1 host up) scanned in 2.21 seconds
```

```
root@SGE:~# nmap -sS 192.168.109.134 -Pn -n -O
```

```
Starting Nmap 6.25 ( http://nmap.org ) at
Nmap scan report for 192.168.109.134
Host is up (0.00035s latency).
Not shown: 995 closed ports
PORT      STATE      SERVICE
21/tcp    filtered  ftp
22/tcp    open       ssh
23/tcp    open       telnet
80/tcp    open       http
443/tcp   open       https
MAC Address: 00:0C:29:B4:9A:46 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.17 - 2.6.36
Network Distance: 1 hop
```

```
root@ubuntu:~# uname -a
Linux ubuntu 2.6.32-21-generic #32-Ubuntu SMP Fri Apr 16 08:10:02 UTC
 2010 i686 GNU/Linux
root@ubuntu:~#
```



Girdi Yönetimi

- -iL ip_listesi.txt
- 192.168.1-255.0-255
- 192.168.1.0/24 10.0.0.0/16
- 192.168.1-255.1-10,254

Çıktı Yönetimi

- -oN: Normal (Okunabilir)
- -oG: Grepable (Parsing)
- -oX: XML (Veritabanına atmak için)
- -oA: Tüm formatlarda

U1

- Ping taraması ile 172.20.0.0/24 ve 172.20.40.0/24 ağ bloklarındaki açık sunucuların tespiti

U2

- Grepable formatındaki çıktıdan açık sunucuların liste olarak çıkarılması

U3

- Liste olarak çıkarılan sunuculara SYN taraması yapılması

U4

- Liste olarak çıkarılan sunuculara versiyon ve işletim sistemi tespiti yapılması

U5

- 22/SSH, 3389/RDP ve 80/HTTP servisleri açık olan sunucuların tespiti



- ☒ Ping Taraması
- ☒ Port Taraması
- ☒ SYN ve TCP Taramaları
- ☒ UDP Taraması
- ☒ Servis ve Versiyon Tespiti
- ☒ İşletim Sistemi Tespiti
- ☐ Betik Taraması
- ☐ Zamanlama ve IPS/IDS Atlatma
- ☐ Büyük Ağların Taranması



NMAP Betik Taraması

SİBER GÜVENLİK
ENSTİTÜSÜ

Nmap Scripting Engine

- Lua programlama dili
- Ağ keşfi
- Gelişmiş servis tespiti
- Zafiyet tespiti
- Arka kapı tespiti
- Zafiyet sömürme

www.bilgimikoruyorum

SİBER GÜVENLİK
ENSTİTÜSÜ



-sC (--script=default)

--script "default and safe"

Kategoriler

- auth
- brute
- default
- dos
- exploit
- intrusive
- malware
- safe
- version
- vuln

Betik veritabanının güncellenmesi

- `# nmap --script-updatedb`

Betik aramak

- `# locate *.nse | grep telnet`

Betik çalıştırmak

- `# nmap -sS -p23 10.0.0.1 --script telnet-brute`
- `# nmap -sU -p53 10.0.0.1 --script "dns-*`

telnet-brute.nse

```
local comm = require "comm"
local nmap = require "nmap"
local shortport = require "shortport"
local stdnse = require "stdnse"
local strbuf = require "strbuf"
local string = require "string"
local unpwdb = require "unpwdb"

description = [[
Tries to get Telnet login credentials by guessing usernames and passwords.
]]

author = "Eddie Bell, Ron Bowes"
license = "Same as Nmap--See http://nmap.org/book/man-legal.html"
categories = {'brute', 'intrusive'}

---
-- @output
-- PORT      STATE SERVICE
-- 23/tcp    open  telnet
-- |_telnet-brute: root - 1234
-- Update (Ron Bowes, November, 2009): Now uses unpwdb database.
```

--script-help

```
root@SGE:~# nmap --script-help telnet-brute
```

```
Starting Nmap 6.40 ( http://nmap.org ) at .
```

```
telnet-brute
```

```
Categories: brute intrusive
```

```
http://nmap.org/nsedoc/scripts/telnet-brute.html
```

```
  Tries to get Telnet login credentials by guessing usernames and passwords.  
  Username and password combinations are retrieved from the unpwdb database.  
  Telnet servers that require only a password (but not a username) are  
  currently not supported.
```

```
root@SGE:~#
```

```
root@SGE:~#
```

ENSTİTÜSÜ

www.bilgimikoruyorum.org

Betik Taraması - Versiyon Tespiti İlişkisi

- Betik Taraması versiyon tespiti yapılmazsa sadece varsayılan portlara uygulanır

```
root@SGE:~# nmap --script ssh-* 192.168.126.129 -Pn -n -p443
```

```
Starting Nmap 6.25 ( http://nmap.org ) at
Nmap scan report for 192.168.126.129
Host is up (0.00023s latency).
PORT      STATE SERVICE
443/tcp   open  https
MAC Address: 00:0C:29:B4:9A:46 (VMware)
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
root@SGE:~# nmap --script ssh-* 192.168.126.129 -Pn -n -p443 -sV
```

```
Starting Nmap 6.25 ( http://nmap.org ) at
Nmap scan report for 192.168.126.129
Host is up (0.00024s latency).
PORT      STATE SERVICE VERSION
443/tcp   open  ssh      OpenSSH 5.3p1 Debian 3ubuntu7 (Ubuntu Linux: protocol 2.0)
| ssh-hostkey: 1024 ea:56:ca:80:ae:26:af:c3:1a:82:fd:a3:6d:58:4b:94 (DSA)
|_ 2048 f0:51:c2:b4:7c:77:af:3a:09:f0:02:9c:fe:aa:07:7c (RSA)
MAC Address: 00:0C:29:B4:9A:46 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Service detection performed. Please report any incorrect results at http://nmap.org/submit
Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

Kullanışlı birkaç betik

- *-brute.nse
- *-info.nse
- dns-recursion
- dns-zone-transfer
- http-slowloris-check
- ms-sql-info
- ms-sql-dump-hashes
- nbstat
- smb-check-vulns
- smb-enum-users
- smb-enum-shares

Kullanışlı birkaç betik - *.brute.nse

- ftp-brute
- ftp-anon
- ms-sql-brute
- mysql-brute
- oracle-sid-brute
- snmp-brute
- telnet-brute
- vmauthd-brute
- vnc-brute

nbstat

```
root@SGE:~# nmap --script-help nbstat

Starting Nmap 6.40 ( http://nmap.org )

nbstat
Categories: default discovery safe
http://nmap.org/nsedoc/scripts/nbstat.html
  Attempts to retrieve the target's NetBIOS names and MAC address.

  By default, the script displays the name of the computer and the logged-in
  user; if the verbosity is turned up, it displays all names the system thinks it
  owns.
root@SGE:~# █
```

nbstat

```
root@SGE:~# nmap --script nbstat 192.168.20.100 -Pn -n -p135,139,445

Starting Nmap 6.40 ( http://nmap.org )
Nmap scan report for 192.168.20.100
Host is up (0.00093s latency).
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds

Host script results:
| nbstat:
|   NetBIOS name: DC1, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:84:55:7b (VMware)
|   Names
|     DC1<00>                Flags: <unique><active>
|     TUBITAK<00>            Flags: <group><active>
|     TUBITAK<1c>            Flags: <group><active>
|     DC1<20>                Flags: <unique><active>
|_    TUBITAK<1b>            Flags: <unique><active>

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
root@SGE:~#
```



- ☒ Ping Taraması
- ☒ Port Taraması
- ☒ SYN ve TCP Taraması
- ☒ UDP Taraması
- ☒ Servis ve Versiyon Tespiti
- ☒ İşletim Sistemi Tespiti
- ☒ Betik Taraması
- ☐ Zamanlama ve IPS/IDS Atlatma
- ☐ Büyük Ağların Taranması



Zamanlama, IPS/IDS Atlatma

SİBER GÜVENLİK
ENSTİTÜSÜ

-T paranoid | sneaky | polite | normal | aggressive | insane

- -T0 (paranoid) : 5 dk
- -T1 (sneaky) : 15 sn
- -T2 (polite) : 0.4 sn
- -T3 (normal) : Varsayılan tarama, paralel tarama
- -T4 (aggressive)
- -T5 (insane)



--max-retries 2

--host-timeout 30m

Paralel Taramanın Kapatılması

- -T 0|1|2
- --scan-delay 1
- --max-parallelism 1
- --max-hostgroup 1



BİLGEM
SİBER GÜVENLİK
ENSTİTÜSÜ
www.bilgimikoruyorum.org.tr

Zamanlama

- Paketler arası süreyi uzat
- Paralel taramayı kapat

Fragmentation

- -f

Kaynak portu

- --source-port
- Kaynak portu 80 olan bir bağlantı daha güvenilir olabilir

Tarama sırasını karıştırma

- --randomize-hosts
- Sıra ile taramayı engeller

IP sahteciliği

- Gönderilen paket geri dönmez
- UDP trafiği için mantıklı

Güvenlik duvarı ve IPS/IDS tespiti

- TTL
- --badsum



- ☒ Ping Taraması
- ☒ Port Taraması
- ☒ SYN ve TCP Taraması
- ☒ UDP Taraması
- ☒ Servis ve Versiyon Tespiti
- ☒ İşletim Sistemi Tespiti
- ☒ Betik Taraması
- ☒ Zamanlama ve IPS/IDS Atlama
- ☐ Büyük Ağların Taranması



Büyük Ağların Taranması

SİBER GÜVENLİK
ENSTİTÜSÜ

Büyük ağların küçük alt ağlara bölünmesi

- Örneklem kümesi alınabilir

IP keşfi için ping taraması kullanımı

İsim çözümleme yapılmaması (-n)

Hızlı tarama seçeneklerinin kullanılması

- -T4|5
- --max-retries
- --host-timeout
- Paket kaybı yaşanabilir (timeouts)
- Servis dışı kalma

Taranacak sunuculara yakın (yüksek hızlı) konumdan tarama

- Ağ performansı en yüksek bölge

Port taramasında dikkat edilecekler

- En sık kullanılan portları kullan
- --top-ports
- -F
- Belirli portları tara
- Güvenlik duvarından izin verilen portlara kısıtla

Taramayı yavaşlatan tarama seçenekleri

- Versiyon tespiti
- İşletim sistemi tespiti
- Betik taraması
- UDP taraması

Güvenlik duvarı yapılandırmasını değiştirme

- Kapalı portlar için RESET veya ICMP unreachable's dönmeli

IP blokları ve adresleri istenebilir

Örnek

B class ağ bloğu verilmiş

- 10.0.0.0/16

Tüm blok taranamaz

Her bir C class için aşağıdaki tarama yapılır

- .1, .254, ilk 10 IP adresi
- # nmap -sP -n -T5 10.0.0-255.1-10,254 -oA out
- 11 adet C class tarama süresi (muhtemelen daha uzun)

Elde edilen açık sunucuların olduğu bloklar taranır

- # cat out.gnmap | grep Up | cut -d' ' -f2 | cut -d':' -f1,2,3 | sed 's/\$/\./24/' | sort | uniq > iplistesi.txt
- # nmap -sP -n -T5 -iL iplistesi.txt -oA out



Diğer NMAP Tarama Türleri

NULL, FIN, XMAS Taraması

SYN, ACK ve RST içermeyen paketler

NULL

- Hiçbir bayrak işaretlenmez

FIN

- Sadece FIN bayrağı işaretli

XMAS

- FIN,PSH ve URG bayrakları işaretli

Durumlar

Closed

Open | Filtered

Filtered

Hedef RST döner

Hedef cevap dönmez

Hedef ICMP unreachable döner

ACK bayrağı işaretli paket gönderilir

Portun **open** veya **closed** olduğu anlaşılmaz

Filtreleme olup olmadığı tespit edilir

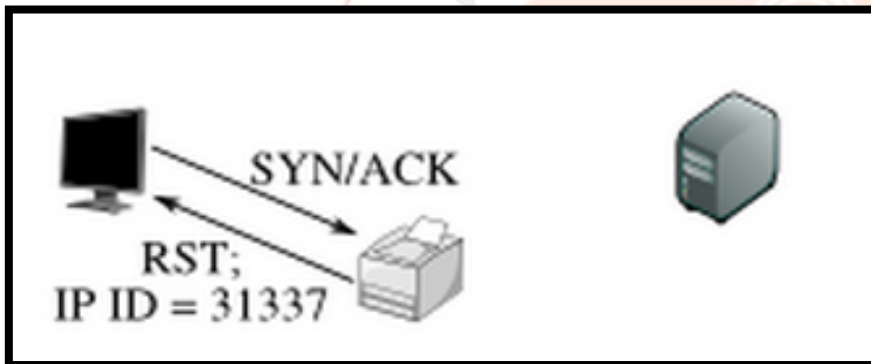
Durum

- Unfiltered
 - Hedef RST döner
 - Port open veya closed durumdadır
- Filtered
 - Hedef cevap vermez
 - Hedef ICMP unreachable döner

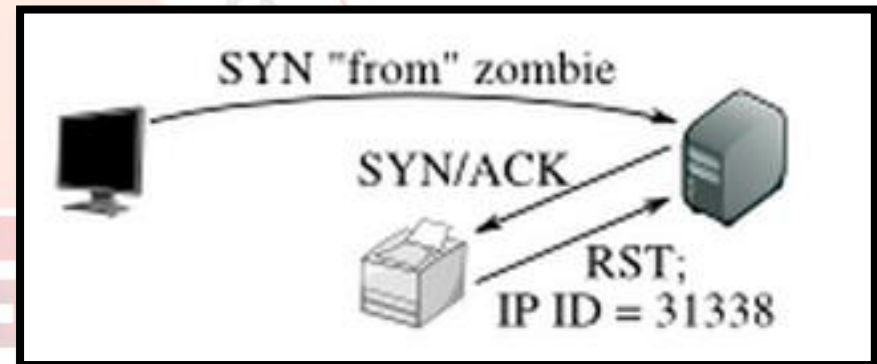
Nmap Idle Scan

open

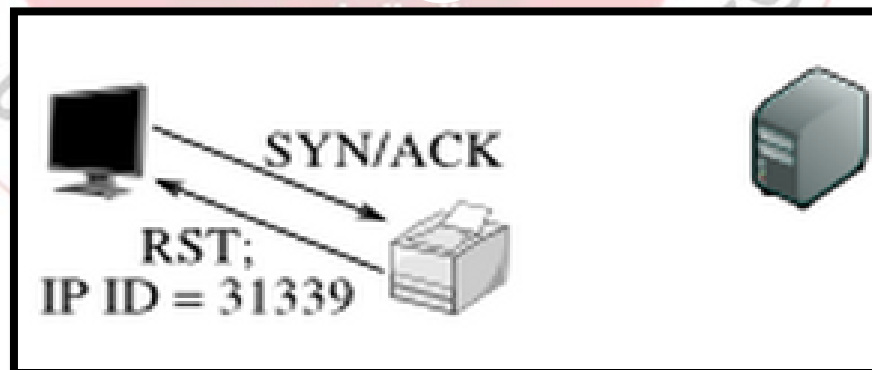
1



2



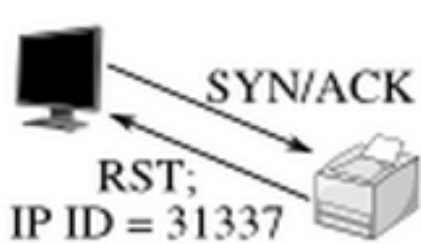
3



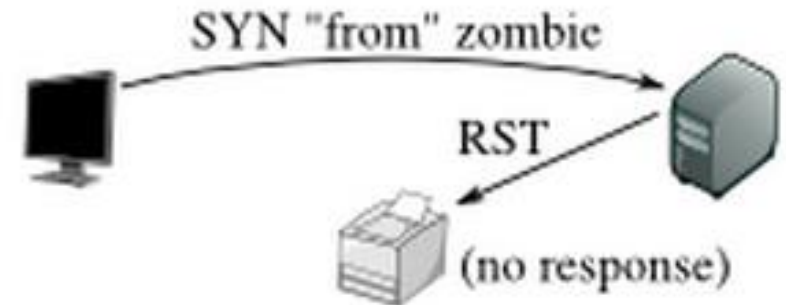
Nmap Idle Scan

closed

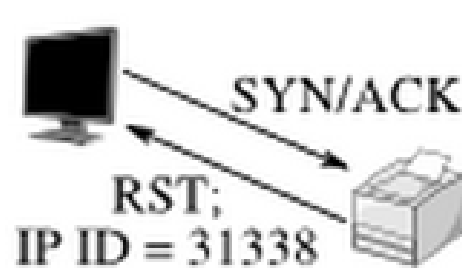
1



2



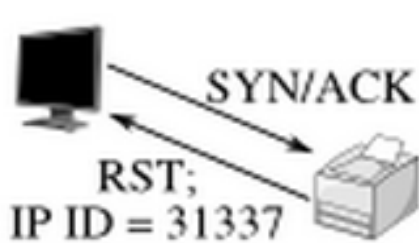
3



Nmap Idle Scan

filtered

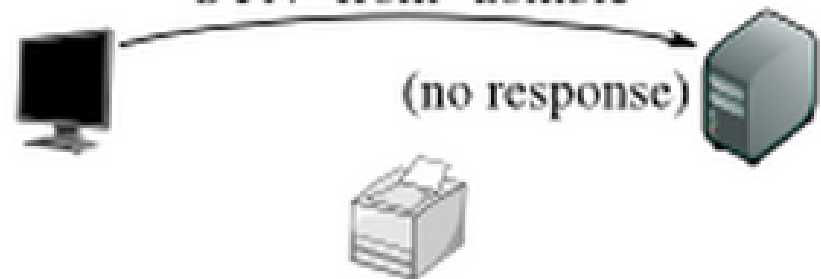
1



2

SYN "from" zombie

(no response)



3







Keşif



Pasif Keşif



Wireshark, tcpdump, ...



Aktif Keşif



Nmap



Zafiyet Tarama



Nessus



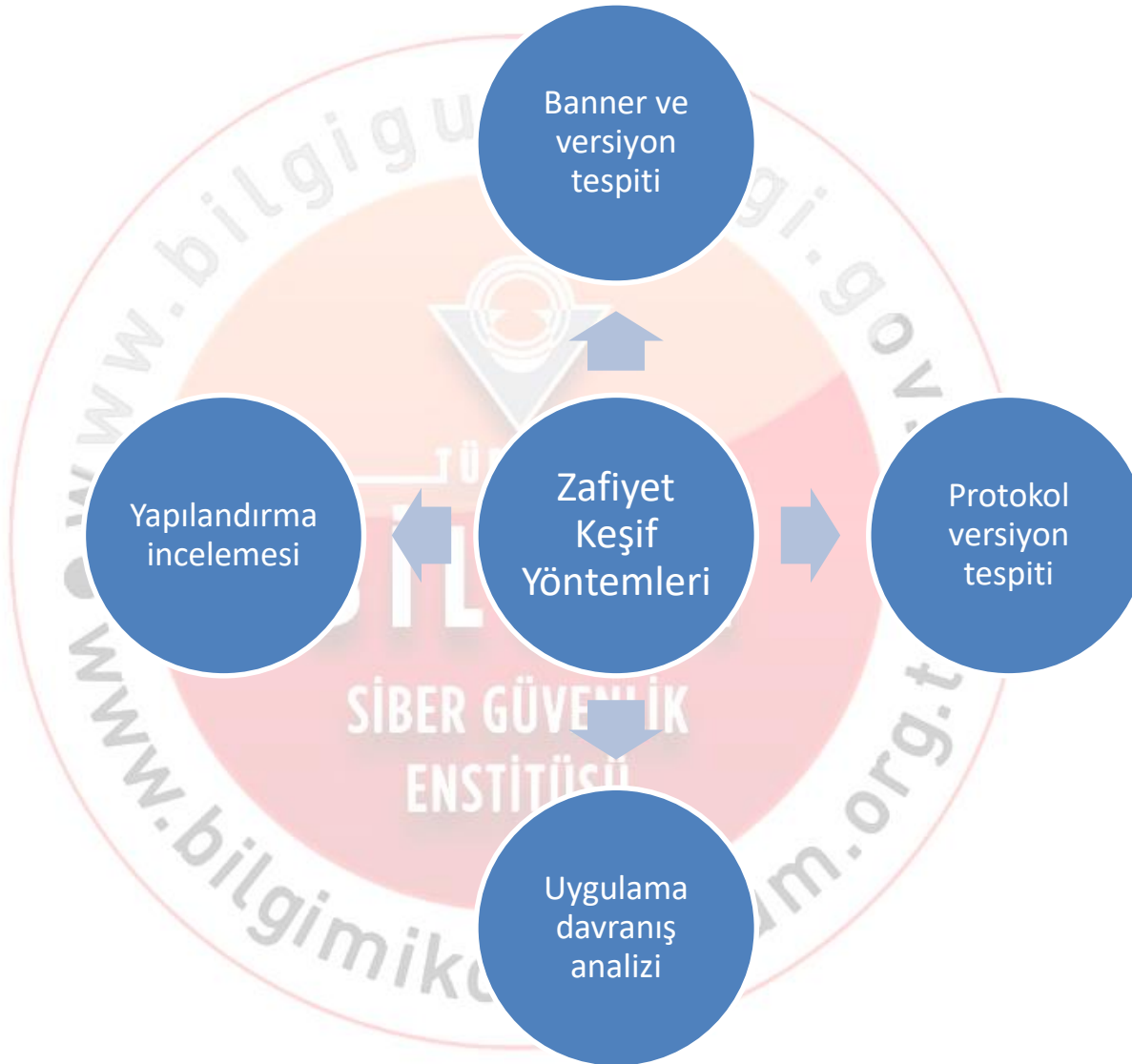
Zafiyet Taraması

SİBER GÜVENLİK
ENSTİTÜSÜ

Zafiyet

- “Bir veya birden çok tehdit tarafından istismar edilen varlık veya varlıklar grubunun zayıflığı” – ISO 27005
- “Sistem güvenlik prosedürlerindeki, tasarımındaki, uygulanmasındaki, veya icra edilen ve güvenlik açığı veya sistemin güvenlik politikasının ihlali ile sonuçlanan dahili kontrollerdeki güçsüzlük veya zayıflık
- NIST





Zafiyet Tarayıcıları

- Nmap NSE
- Nessus
- Microsoft MBSA
- NeXpose
- OpenVAS
- SAINT
- eEye Retine
- GFI LanGuard
- QualysGuard
- Secunia PSI



Zafiyet Veritabanları

Open Source Vulnerability Database (OSVDB)

- <http://osvdb.org/>

NIST National Vulnerability Database

- <http://nvd.nist.gov/>

Common Vulnerabilities and Exposures (CVE)

- <http://www.cvedetails.com/>

NESSUS

SİBER GÜVENLİK
ENSTİTÜSÜ

Yetenekleri

- Ajan kurmadan yama eksikliği testi
- Zayıf yapılandırma tespiti
- Port taraması
- Servis tespiti
- Kullanıcı denemesi
- Exploit uygulanabilirliği
- Yetkili (credential) tarama yeteneği
- 55000+ plugin
- Raporlama özellikleri

Kurulum

```
root@ubuntu:~# ls
Nessus-5.2.1-ubuntu910 i386.deb
root@ubuntu:~# dpkg -i Nessus-5.2.1-ubuntu910 i386.deb
Selecting previously deselected package nessus.
(Reading database ... 125424 files and directories currently installed.)
Unpacking nessus (from Nessus-5.2.1-ubuntu910_i386.deb) ...
Setting up nessus (5.2.1) ...
nessusd (Nessus) 5.2.1 [build N24021] for Linux
Copyright (C) 1998 - 2013 Tenable Network Security, Inc

Processing the Nessus plugins...
[#####]

All plugins loaded

- You can start nessusd by typing /etc/init.d/nessusd start
- Then go to https://ubuntu:8834/ to configure your scanner

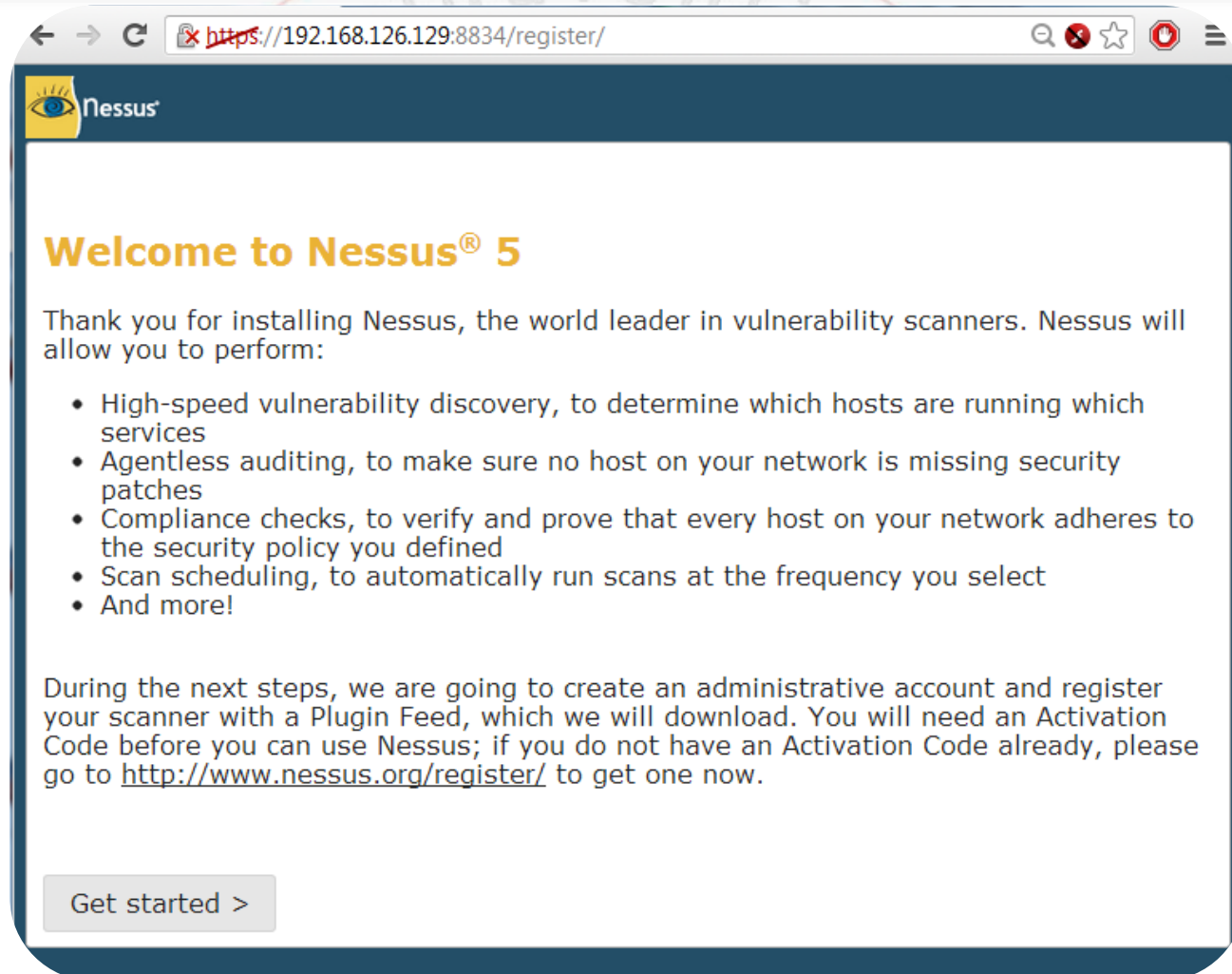
Processing triggers for ureadahead ...
ureadahead will be reprofiled on next reboot
root@ubuntu:~#
```

Servis Başlatmak

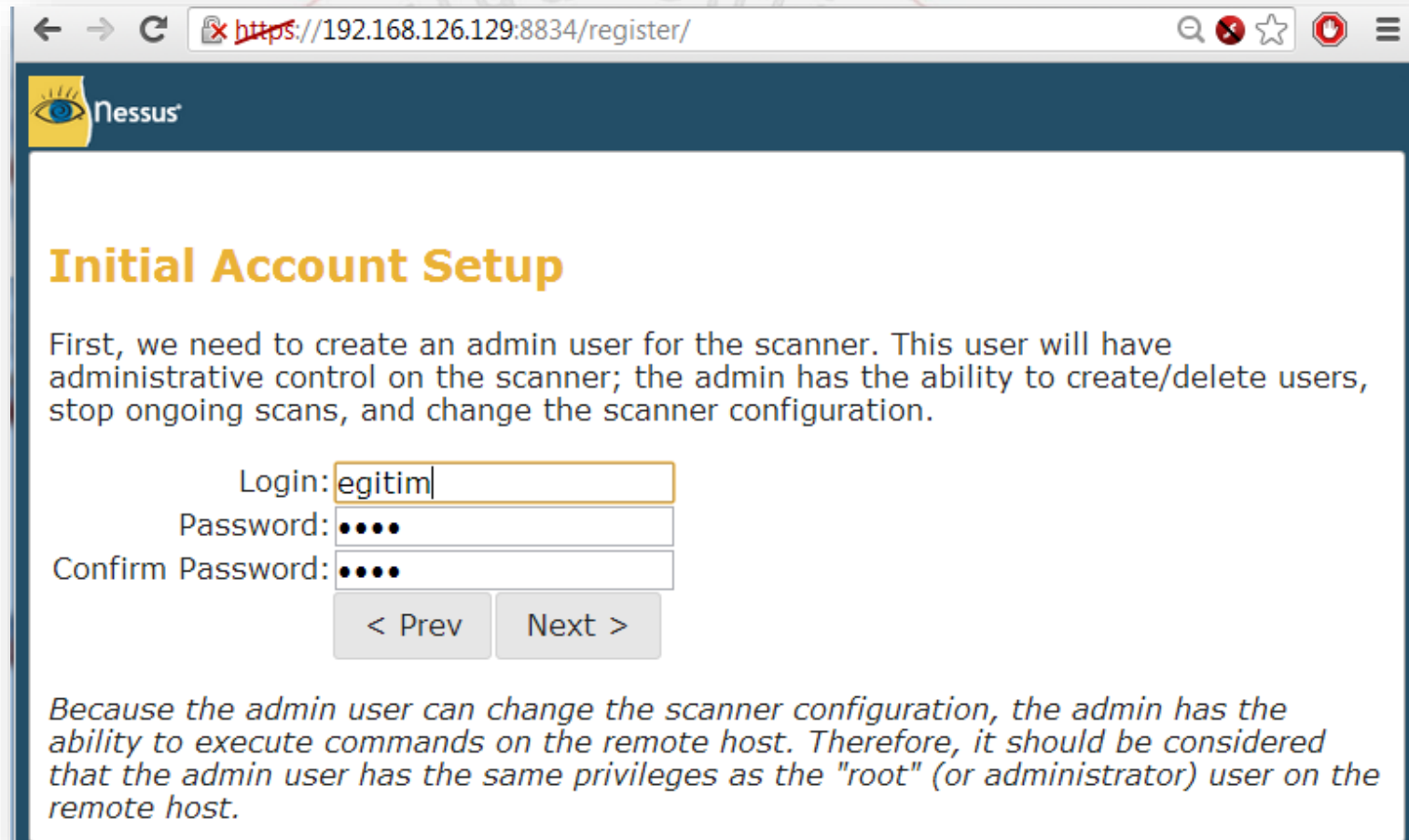
```
root@ubuntu:~# /etc/init.d/nessusd start
$Starting Nessus : .
root@ubuntu:~# █
```

SİBER GÜVENLİK
ENSTİTÜSÜ
www.bilgimikoruyorum.org.tr


İlk Kurulum Ekranı



İlk Kullanıcının Oluşturulması



← → ↻ <https://192.168.126.129:8834/register/> 🔍 ✖ ☆ 🛑 ☰

 **Nessus**

Initial Account Setup

First, we need to create an admin user for the scanner. This user will have administrative control on the scanner; the admin has the ability to create/delete users, stop ongoing scans, and change the scanner configuration.

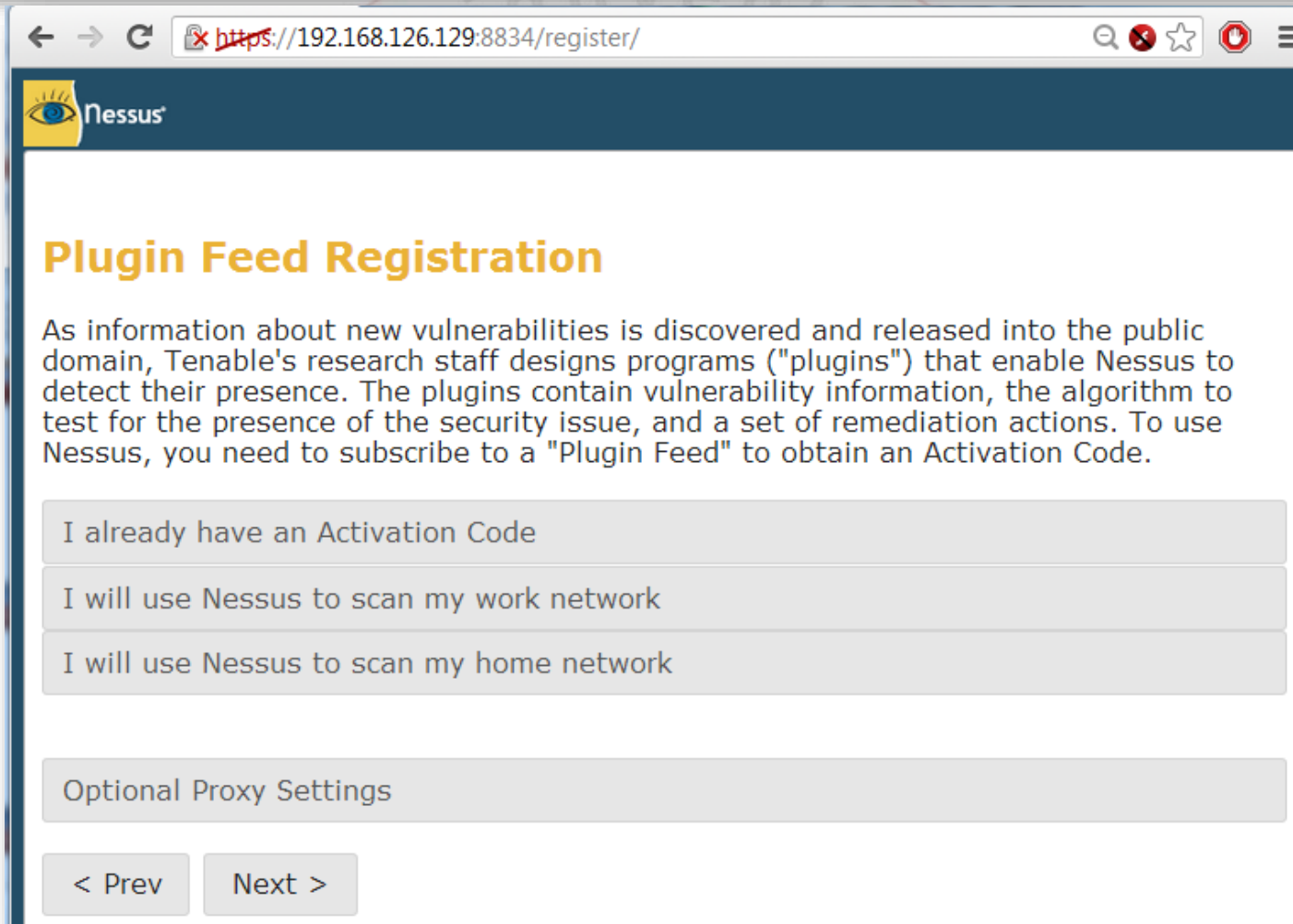
Login:

Password:

Confirm Password:

Because the admin user can change the scanner configuration, the admin has the ability to execute commands on the remote host. Therefore, it should be considered that the admin user has the same privileges as the "root" (or administrator) user on the remote host.

Aktivasyon Kodu Elde Edilmesi/Girilmesi



The screenshot shows a web browser window with the URL <https://192.168.126.129:8834/register/>. The page features the Nessus logo and a title "Plugin Feed Registration". Below the title, there is a paragraph explaining the purpose of the registration. Three radio buttons are provided for selection: "I already have an Activation Code", "I will use Nessus to scan my work network", and "I will use Nessus to scan my home network". An "Optional Proxy Settings" section is also visible. At the bottom, there are "Prev" and "Next" navigation buttons.

Plugin Feed Registration

As information about new vulnerabilities is discovered and released into the public domain, Tenable's research staff designs programs ("plugins") that enable Nessus to detect their presence. The plugins contain vulnerability information, the algorithm to test for the presence of the security issue, and a set of remediation actions. To use Nessus, you need to subscribe to a "Plugin Feed" to obtain an Activation Code.

☐ I already have an Activation Code

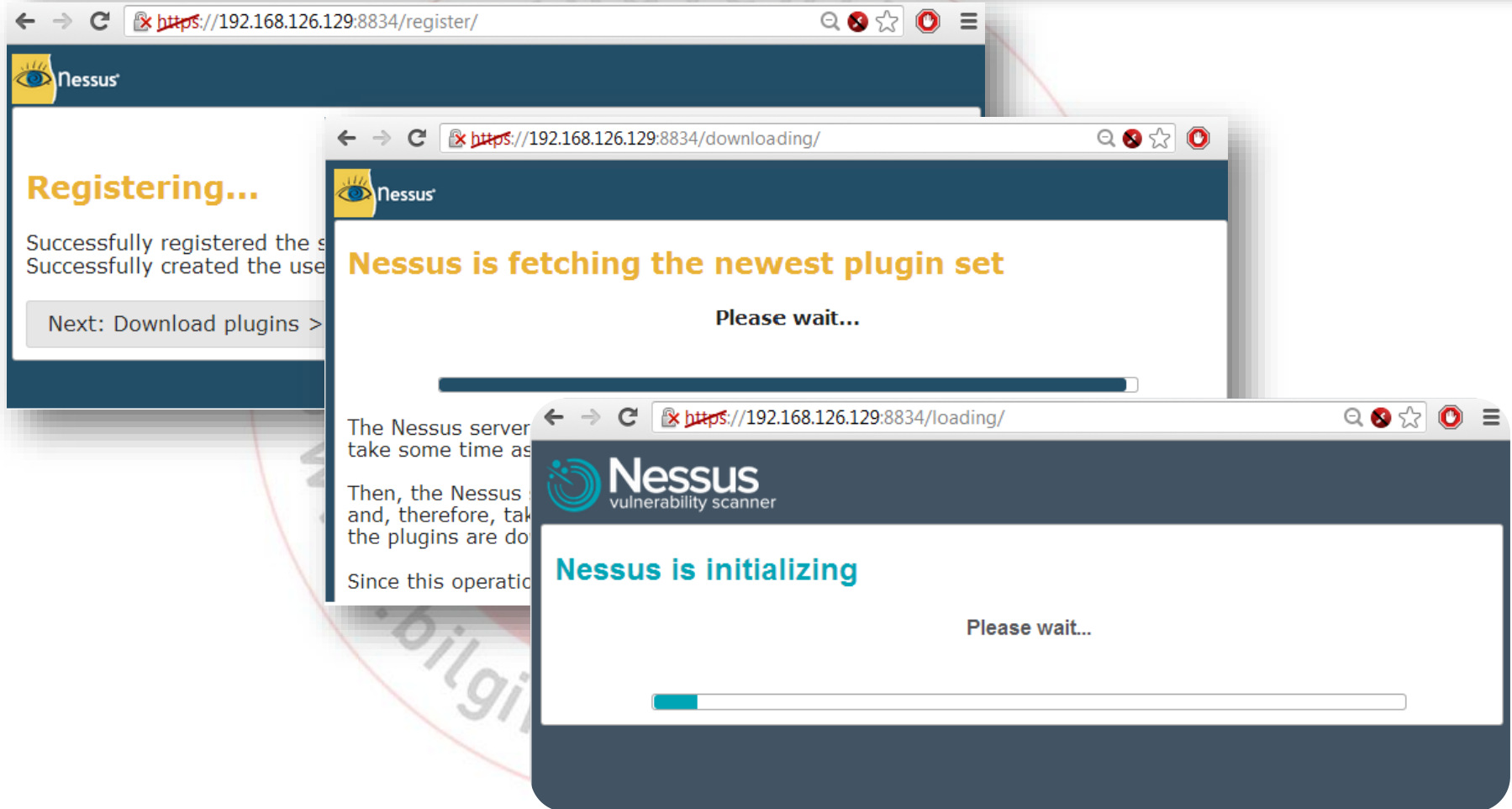
☐ I will use Nessus to scan my work network

☐ I will use Nessus to scan my home network

Optional Proxy Settings

< Prev Next >

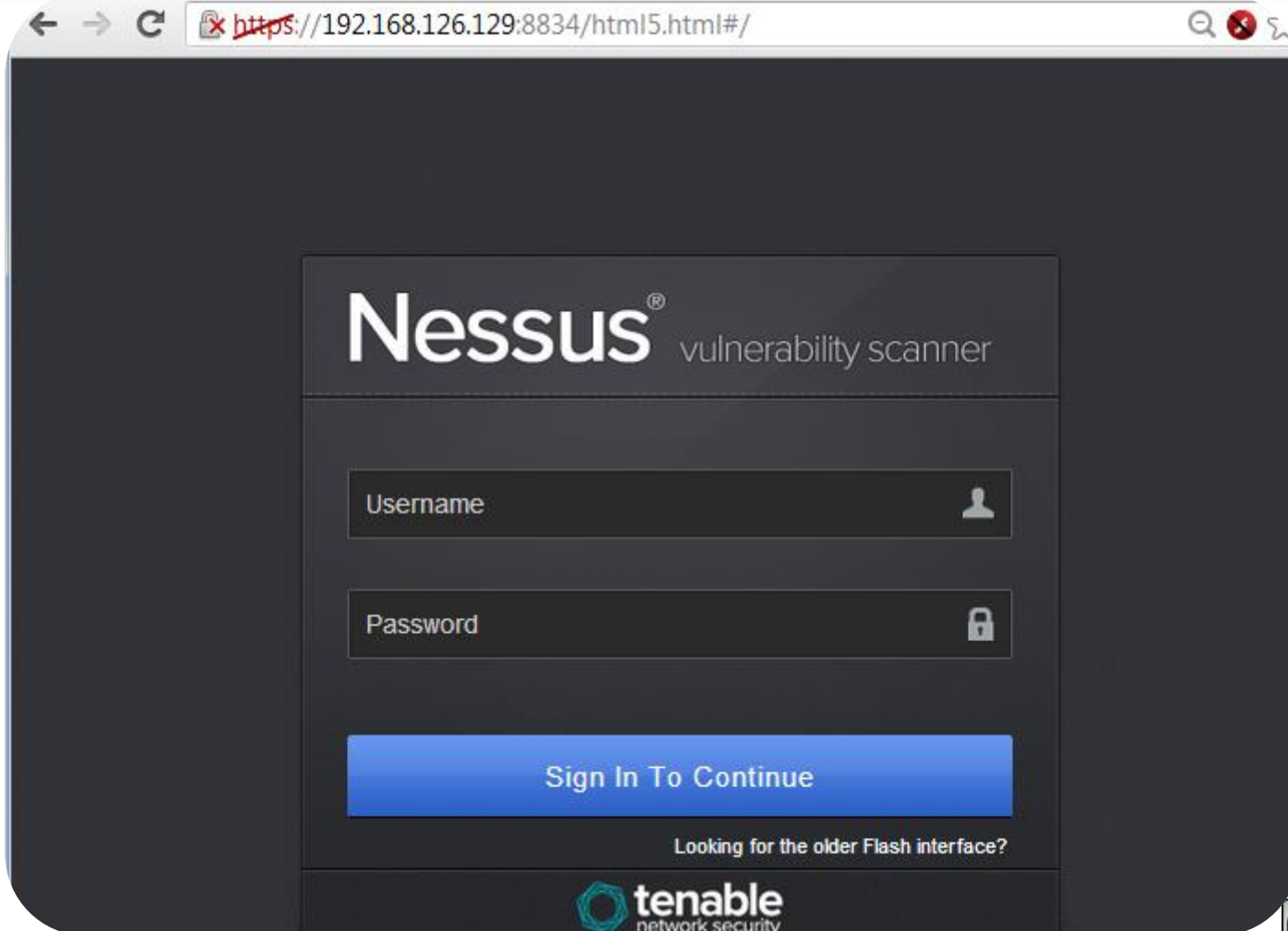
Kurulum



The image displays three overlapping browser windows illustrating the Nessus installation process:

- Top Window (register/):** Shows the "Registering..." screen. It indicates successful registration and creation of the user. A button labeled "Next: Download plugins >" is visible.
- Middle Window (downloading/):** Shows the "Nessus is fetching the newest plugin set" screen. It includes the text "Please wait..." and a progress bar.
- Bottom Window (loading/):** Shows the "Nessus is initializing" screen. It includes the text "Please wait..." and a progress bar.


Ana Giriş Ekranı




The screenshot shows the Nessus login interface in a web browser. The address bar displays a URL with a red 'x' icon, indicating a connection error. The main content area has a dark background with the Nessus logo and 'vulnerability scanner' text. Below this are two input fields for 'Username' and 'Password', each with a corresponding icon (a person for username and a padlock for password). A large blue button labeled 'Sign In To Continue' is positioned below the password field. At the bottom of the main content area, there is a link that says 'Looking for the older Flash interface?'. The footer of the page features the Tenable logo and the text 'network security'.

← → ↻ [!\[\]\(7bc68ae64e3837236c350f81f7844365_img.jpg\) https://192.168.126.129:8834/html5.html#/](https://192.168.126.129:8834/html5.html#/) 🔍 ⌵


Nessus[®] vulnerability scanner

Username 

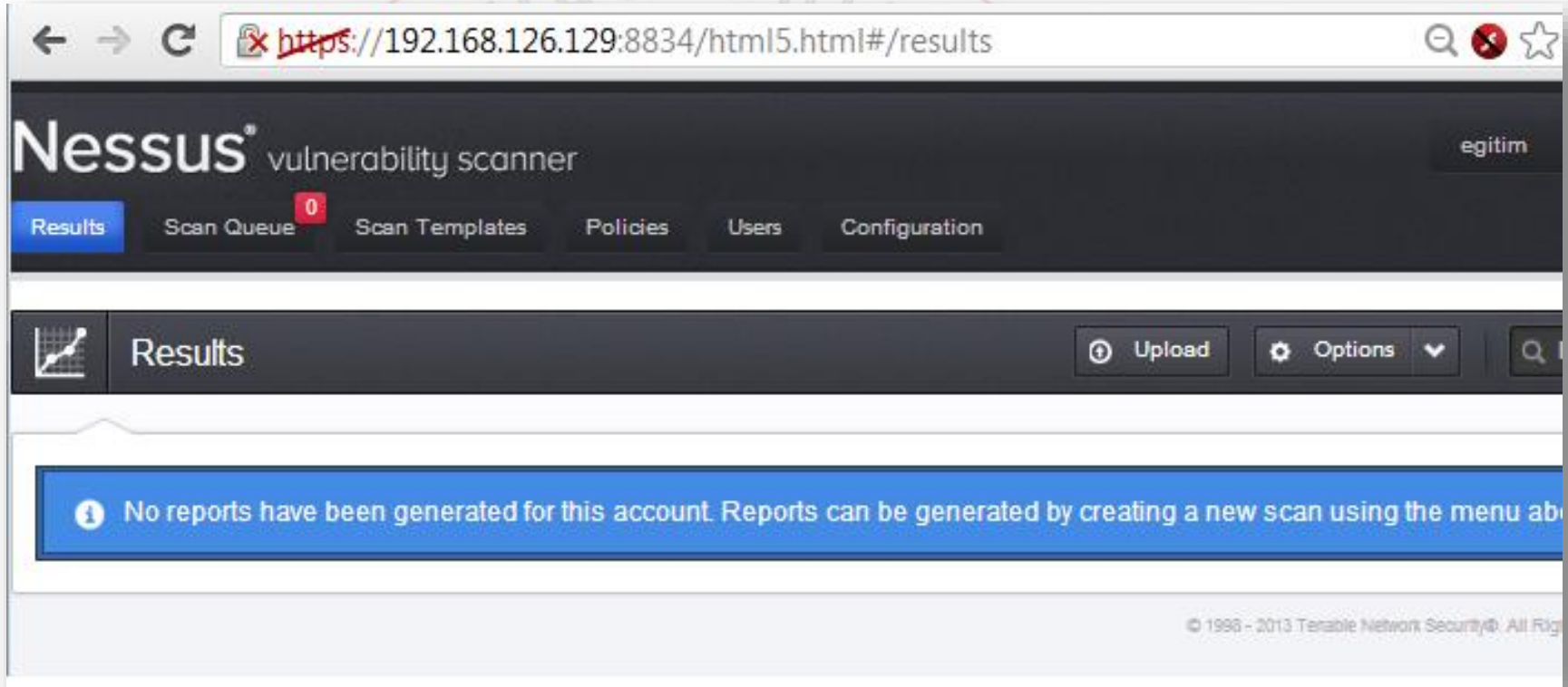
Password 

Sign In To Continue


[Looking for the older Flash interface?](#)


 **tenable**
network security


Ana Giriş Ekranı





Ayarlar

 System Configuration

 General Settings

 Feed Settings

 Mobile Settings

 Advanced Settings

Nessus Advanced Settings

allow_post_scan_editing	<input type="text" value="yes"/>	×
auto_enable_dependencies	<input type="text" value="yes"/>	×
auto_update	<input type="text" value="yes"/>	×
auto_update_delay	<input type="text" value="24"/>	×
cgi_path	<input type="text" value="/cgi-bin:/scripts"/>	×
checks_read_timeout	<input type="text" value="5"/>	×
disable_ntp	<input type="text" value="yes"/>	×
disable_xmlrpc	<input type="text" value="no"/>	×
dumpfile	<input type="text" value="/opt/nessus/var/nessus/logs/nessusd.dump"/>	×
global.max_hosts	<input type="text" value="30"/>	×

Yeni Politika Oluřturma

Nessus® vulnerability scanner

egitim Help & Support Sign Out

Results Scan Queue ⁰ Scan Templates Policies Users Configuration

Policies + New Policy Upload Options Filter Policies

<input type="checkbox"/>	Name ^	Visibility	Created By
<input type="checkbox"/>	External Network Scan	shared	Tenable Policy Distribution Service
<input type="checkbox"/>	Internal Network Scan	shared	Tenable Policy Distribution Service
<input type="checkbox"/>	Prepare for PCI-DSS audits (section 11.2.2)	shared	Tenable Policy Distribution Service
<input type="checkbox"/>	Web App Tests	shared	Tenable Policy Distribution Service

Politika Seçenekleri

Policy General Settings

Setting Type

Basic

Name

İç Ağ Taramaları

Visibility

shared

Description

shared

private

İç Ağ taraması

Allow Post-Scan Report Editing

Update

Cancel

Tarama Ayarları

Setting Type Port Scanning

Port Scan Range

Consider Unscanned Ports as Closed ☐

Nessus SNMP Scanner ☒

netstat portscanner (SSH) ☒

Ping the remote host ☒

Netstat Portscanner (WMI) ☒

Nessus TCP scanner ☐

Nessus SYN scanner ☒

Update Cancel

Performans Ayarları

Setting Type Performance

Max Checks Per Host	<input type="text" value="5"/>
Max Hosts Per Scan	<input type="text" value="30"/>
Network Receive Timeout (seconds)	<input type="text" value="5"/>
Max Simultaneous TCP Sessions Per Host	<input type="text" value="800"/>
Max Simultaneous TCP Sessions Per Scan	<input type="text" value="2000"/>
Reduce Parallel Connections on Congestion	<input checked="" type="checkbox"/>
Use Kernel Congestion Detection (Linux Only)	<input type="checkbox"/>

Geliřmiř Ayarlar

Policy General Settings

Setting Type

Advanced

Safe Checks ☒

Silent Dependencies ☒

Log Scan Details to Server ☒

Stop Host Scan on Disconnect ☐

Avoid Sequential Scans ☒

Designate Hosts by their DNS Name ☐

Update

Cancel

Kullanıcı Bilgisi Ekleme

Policy Credentials

Credential Type

Windows credentials

Windows credentials

SSH settings

Kerberos configuration

Cleartext protocols settings

SMB domain (optional)

SMB password type

Password

Additional SMB account (1)


Additional SMB password (1)


Additional SMB domain (optional) (1)


Additional SMB account (2)


Additional SMB password (2)

Plugin Ayarları

 General Settings

 Credentials

 Plugins

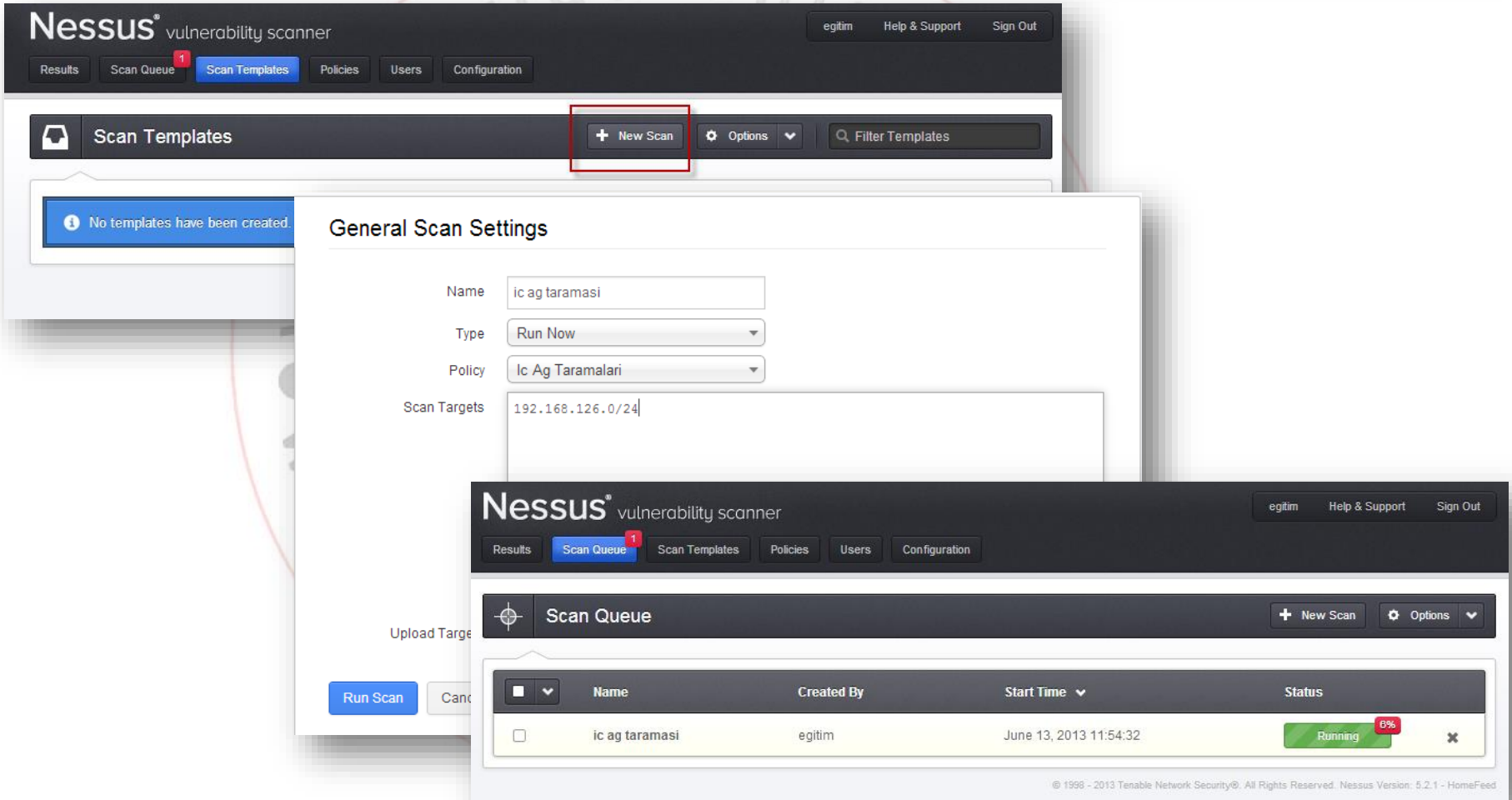
 Preferences

Policy Plugin Configurations

Enable All Disable All Update

enabled	AIX Local Security Checks	10994
enabled	Backdoors	89
enabled	CGI abuses	2627
enabled	CGI abuses : XSS	511
enabled	CISCO	297
enabled	CentOS Local Security Checks	1455
enabled	DNS	73
enabled	Databases	305
enabled	Debian Local Security Checks	2692
enabled	Default Unix Accounts	81
disabled	Denial of Service	102
enabled	FTP	229

Yeni Tarama



The screenshot displays the Nessus vulnerability scanner interface. The top navigation bar includes 'Results', 'Scan Queue', 'Scan Templates', 'Policies', 'Users', and 'Configuration'. The 'Scan Templates' section is active, showing a message 'No templates have been created.' and a '+ New Scan' button highlighted with a red box. The 'General Scan Settings' dialog box is open, showing the following fields:

- Name: ic ag taramasi
- Type: Run Now
- Policy: Ic Ag Taramalari
- Scan Targets: 192.168.126.0/24

The bottom section of the interface shows the 'Scan Queue' with a table of scans. The table has columns for 'Name', 'Created By', 'Start Time', and 'Status'.


Name	Created By	Start Time	Status
ic ag taramasi	egitim	June 13, 2013 11:54:32	Running 8%


Tarama Sonuçlarının İncelenmesi


Nessus® vulnerability scanner


egitim Help & Support Sign Out

Results Scan Queue ¹ Scan Templates Policies Users Configuration

 **ic ag taramasi** Vulnerability Summary ic ag taramasi Filter Options ⁰ Audit Trail

 Hosts 4

 Vulnerabilities 139

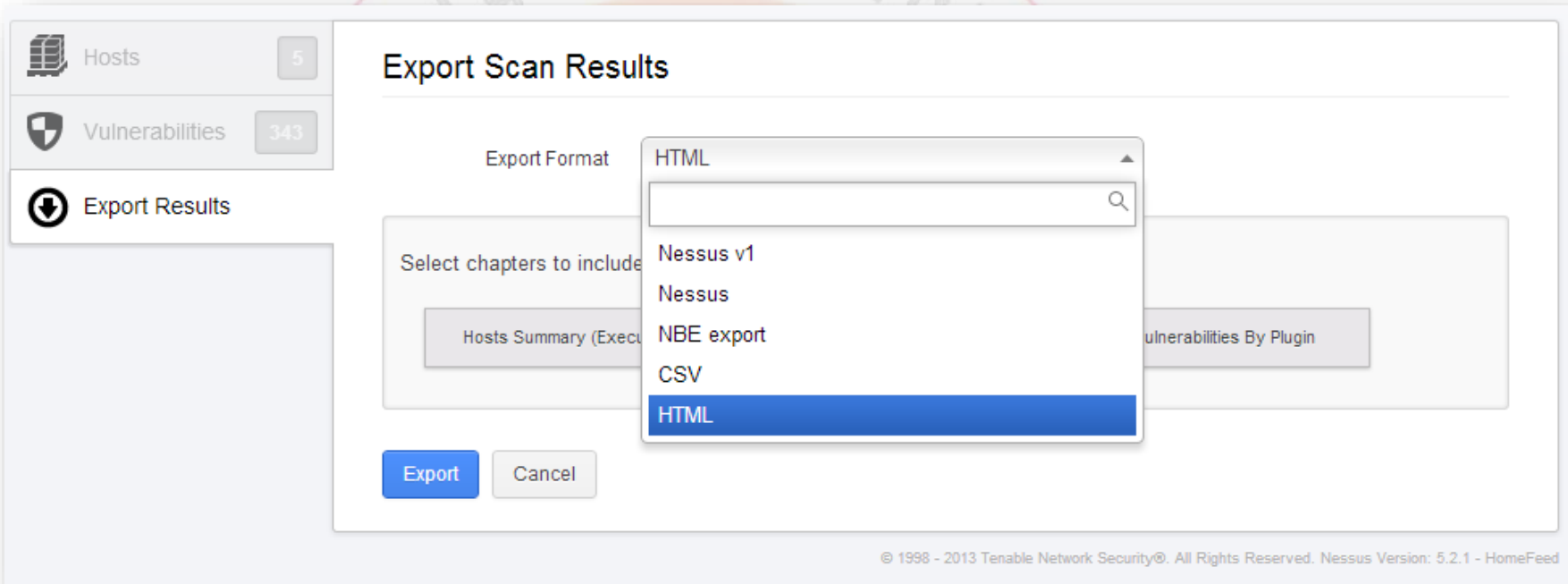
 Export Results

Vulnerability Summary

Sort Options

critical	Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : firefox vulne...	Ubuntu Local Security Checks	1
critical	Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : firefox regre...	Ubuntu Local Security Checks	1
critical	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : freety...	Ubuntu Local Security Checks	1
critical	Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : firefox vulne...	Ubuntu Local Security Checks	1
critical	Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : firefox vulne...	Ubuntu Local Security Checks	1
critical	Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : firefox, firefo...	Ubuntu Local Security Checks	1
critical	Ubuntu 10.04 LTS / 10.10 : firefox, xulrunner-1.9.2 vulnerab...	Ubuntu Local Security Checks	1

Rapor Formatları



The image shows the 'Export Scan Results' dialog box in the Nessus interface. On the left, there is a sidebar with three items: 'Hosts' (5), 'Vulnerabilities' (343), and 'Export Results' (selected). The main area is titled 'Export Scan Results'. It features a 'Select chapters to include' section with two checkboxes: 'Hosts Summary (Executed)' and 'Vulnerabilities By Plugin'. Below this is an 'Export Format' dropdown menu, which is currently open, showing a search bar and a list of options: 'HTML' (selected), 'Nessus v1', 'Nessus', 'NBE export', 'CSV', and 'HTML' (repeated). At the bottom of the dialog are 'Export' and 'Cancel' buttons. The footer of the dialog contains the text: '© 1998 - 2013 Tenable Network Security®. All Rights Reserved. Nessus Version: 5.2.1 - HomeFeed'.

Rapor Örneği



Nessus Scan Report

Table Of Contents

Vulnerabilities By Plugin

- [47161 \(1\) - Ubuntu 8.04 LTS / 10.04 LTS : firefox, firefox-3.0, xulrunner-1.9.2 vulnerabilities \(USN-930-1\)](#)
- [47856 \(1\) - Ubuntu 8.04 LTS / 10.04 LTS : firefox, firefox-3.0, xulrunner-1.9.2 vulnerability \(USN-957-2\)](#)
- [49805 \(1\) - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS / 10.10 : openssl vulnerabilities \(USN-1003-1\)](#)
- [50044 \(1\) - Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS / 10.10 : linux, linux-ec2, linux-source-2.6.15 vulnerabilities \(USN-1000-1\)](#)
- [50046 \(1\) - Ubuntu 9.10 / 10.04 LTS / 10.10 : webkit vulnerabilities \(USN-1006-1\)](#)
- [52526 \(1\) - Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : firefox, firefox-{3.0,3.5}, xulrunner-1.9.2 vulnerabilities \(USN-1049-1\)](#)
- [52579 \(1\) - Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : firefox, firefox-{3.0,3.5}, xulrunner-1.9.2 regression \(USN-1049-2\)](#)
- [55070 \(1\) - Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : firefox, firefox-3.0, firefox-3.5, xulrunner-1.9.2 vulnerabilities \(USN-1112-1\)](#)

Uygulama - 2



Nessus Web
Arayüzünden
Bağlan

Tarama
Politikası
Tanımla

Hedefleri Seç

Taramayı
Çalıştır

Sonuçları
Teftiş Et



TÜBİTAK

Teşekkürler