TÜBİTAK

Keşif ve Zafiyet Tarama

TÜBİTAK BİLGEM
Siber Güvenlik Enstitüsü

Amaç

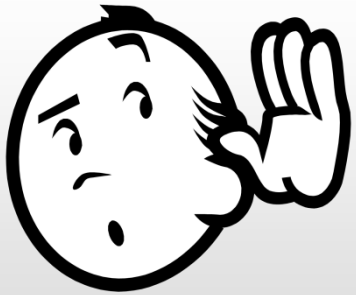
- Açık sunucuların tespiti
- Ağ topolojisi keşfi
- Açık portların tespiti
- Versiyon tespiti
- İşletim sistemi keşfi
- Zafiyet tespiti

Keşif Türleri

Keşif Türleri

Pasif Keşif

- Ağın dinlenilmesi
  - Tcpdump
  - Wireshark
- ARP tablosu



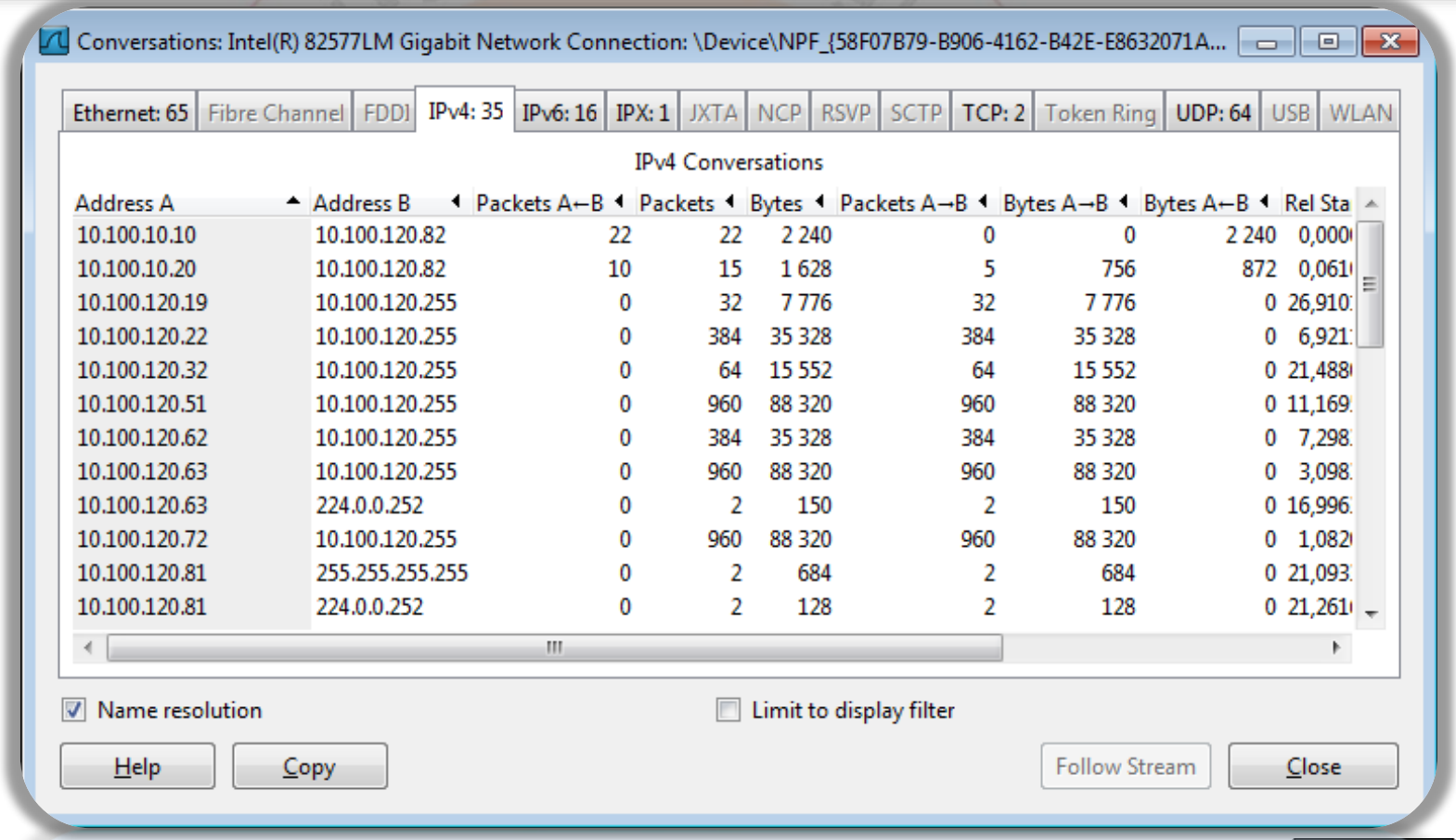
Aktif Keşif

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

Keşif Türleri

Pasif Keşif

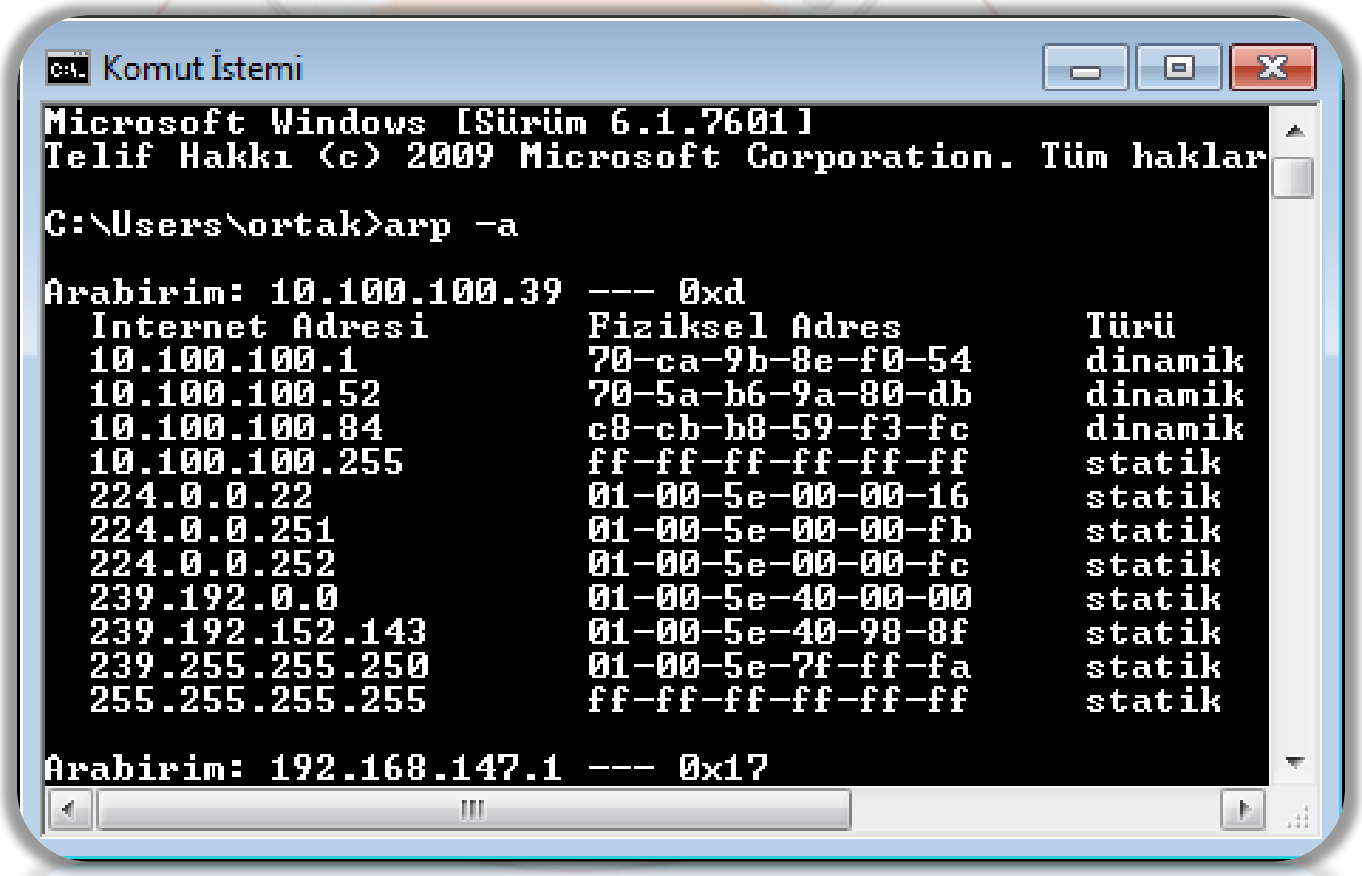
Wireshark



Keşif Türleri

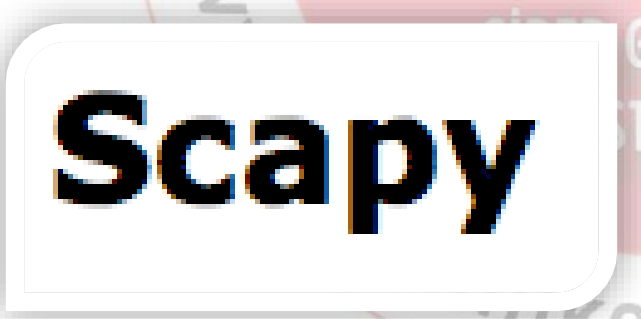
Pasif Keşif

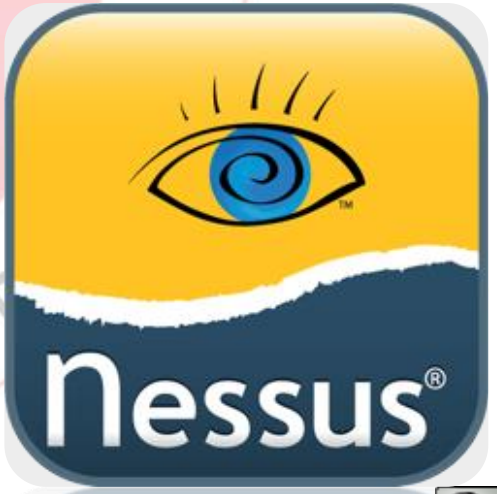
ARP Tablosu



Keşif Türleri

Aktif Keşif



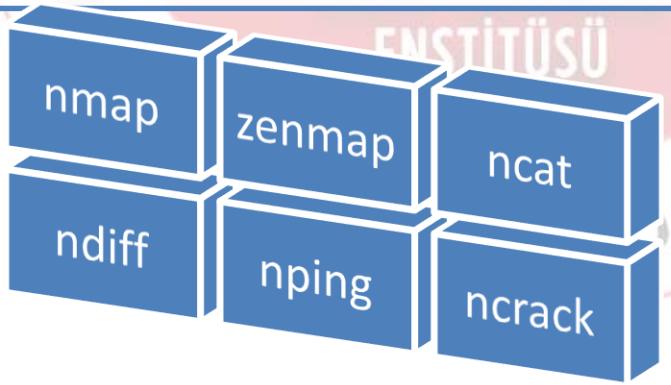


NMAP

NMAP

NMAP

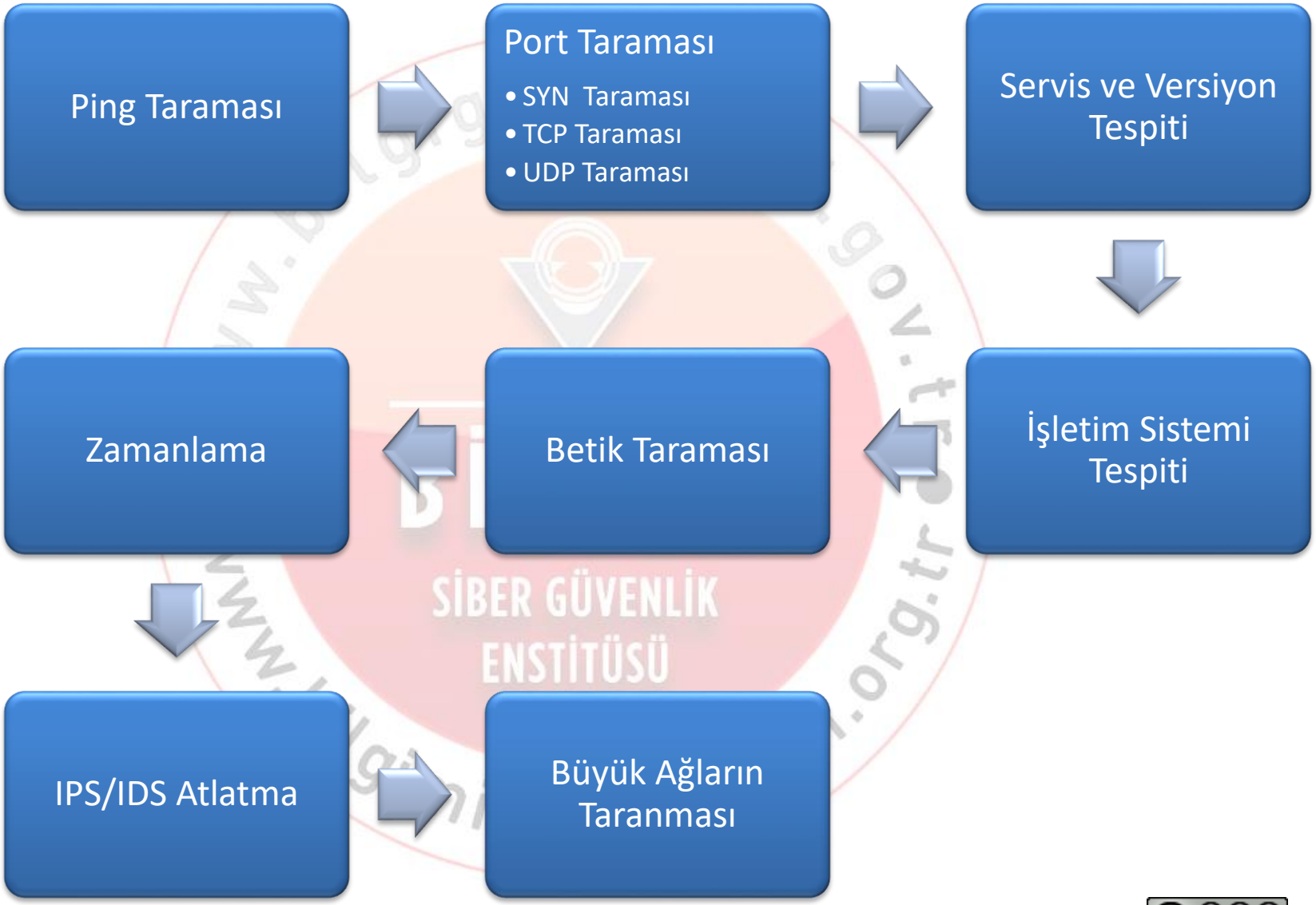
- Ağ tarama aracı
- Açık kaynak kodlu
- Ücretsiz
- Yaygın kullanım
- Geniş bir topluluk desteği
- Güçlü
- Birçok işi tek başına yapabilir
- Her platformda çalışır
- İyi dokümantasyon



NMAP

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

NMAP



NMAP Ping Taraması

NMAP Ping Taraması

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”

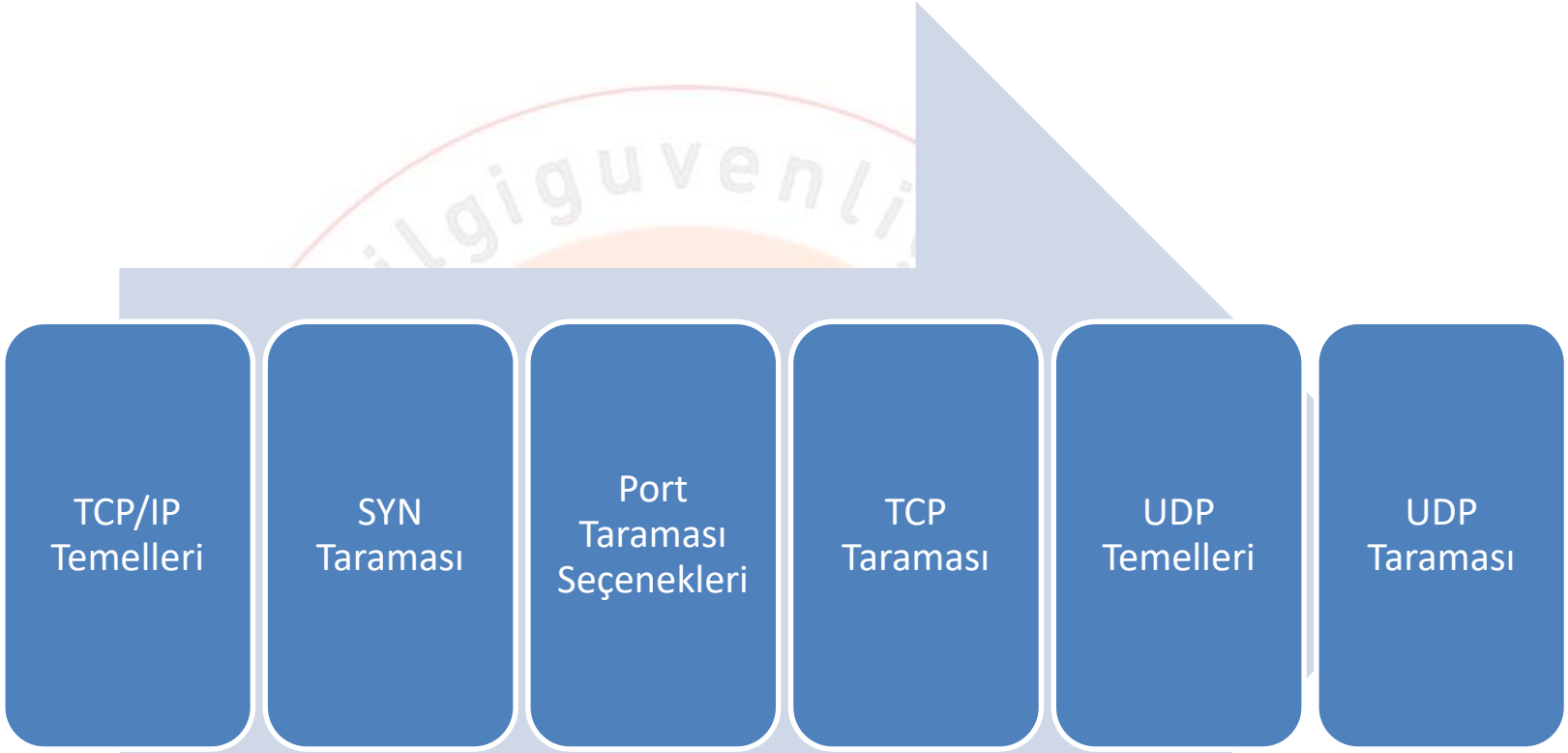
NMAP Ping Taraması

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

NMAP Port Taraması



TCP/IP Temelleri

OSI Referans Modeli

Kullanıcı etkileşimli uygulamalar: HTTP, SMTP

Farklı veri formatlarını birbirine dönüşümü: ASCII,MP3,JPG

Soket açma, oturum kurma: SQL, RPC

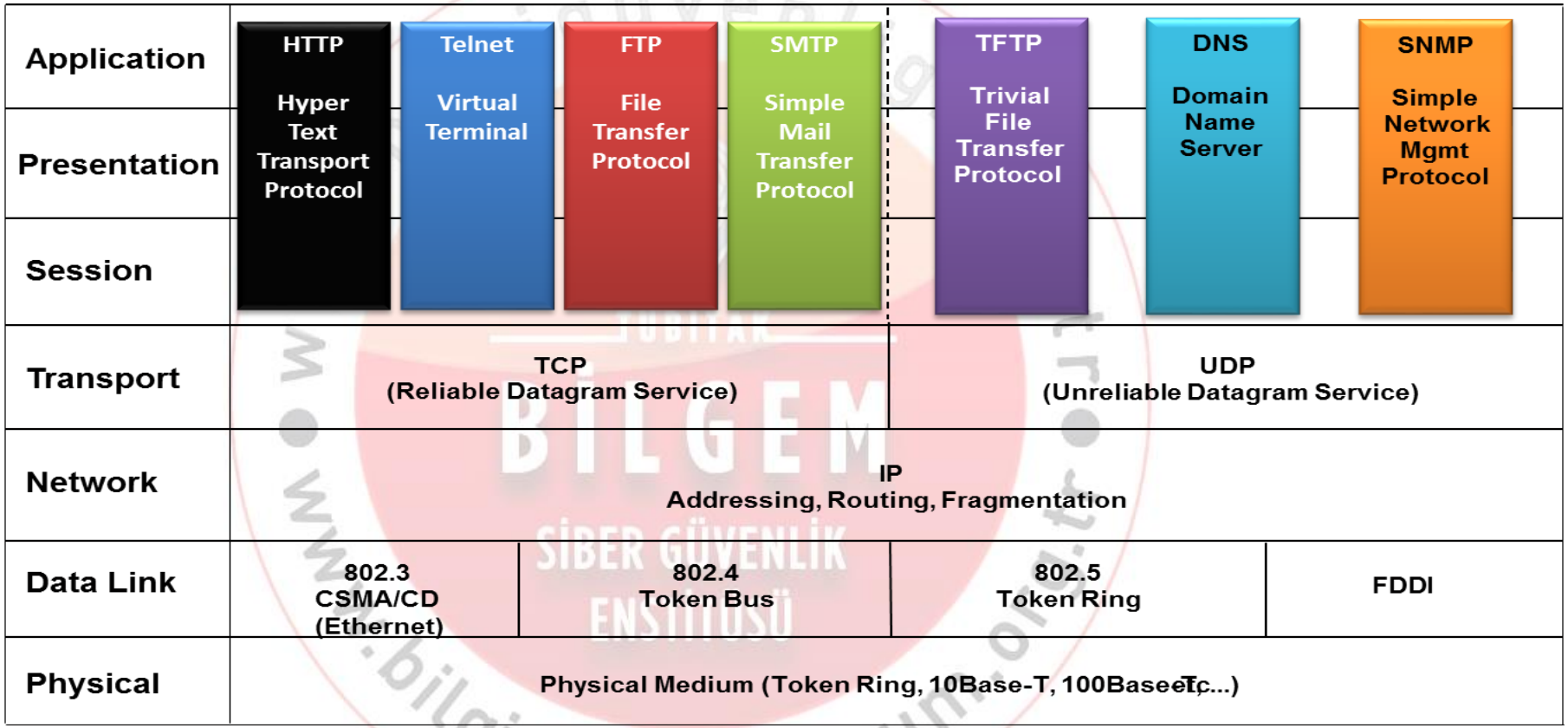
Hata ve akış kontrolü: TCP, UDP

Uçtan uca iletişim, sanal adresleme: IP

Ortama Erişim: Ethernet, Wireless

İkili iletim: Koaksiyel, UTP ve fiber kablolar

Katmanlar ve Protokoller



Örnek: DNS Protokolü

mail.yahoo.com

ENTER

DNS Sunucu

Uygulama Katmanı (L5)

DNS S.Q. “mail.yahoo.com”

Taşıma Katmanı (L4)

UDP | DNS S.Q. “mail.yahoo.com”

Ağ Katmanı (L3)

IP | UDP | DNS S.Q. “mail.yahoo.com”

Veri Bağı Katmanı (L2)

Eth. | IP | UDP | DNS S.Q. “mail.yahoo.com”

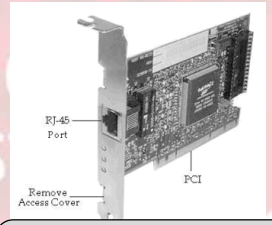
Fiziksel Katman (L1)

WEB Tarayıcı

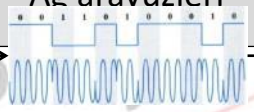
DNS Servisi

CPU

İşletim Sistemi



Ağ aravüzleri



Fiziksel İletim

Uygulama Katmanı (L5)

DNS S.Q. “mail.yahoo.com”

Taşıma Katmanı (L4)

UDP | DNS S.Q. “mail.yahoo.com”

Ağ Katmanı (L3)

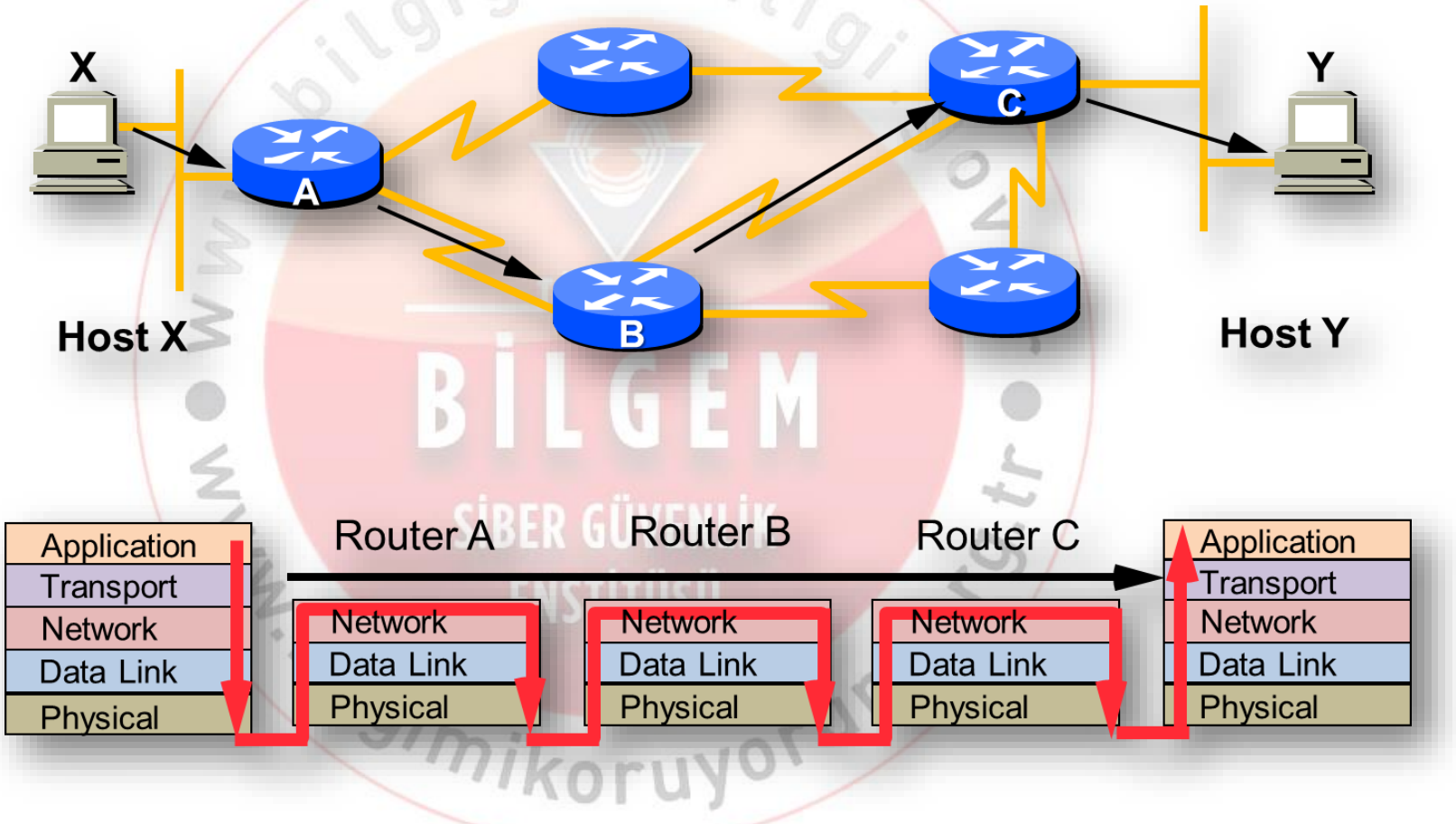
IP | UDP | DNS S.Q. “mail.yahoo.com”

Veri Bağı Katmanı (L2)

Eth. | IP | UDP | DNS S.Q. “mail.yahoo.com”

Fiziksel Katman (L1)

TCP/IP ile İletişim



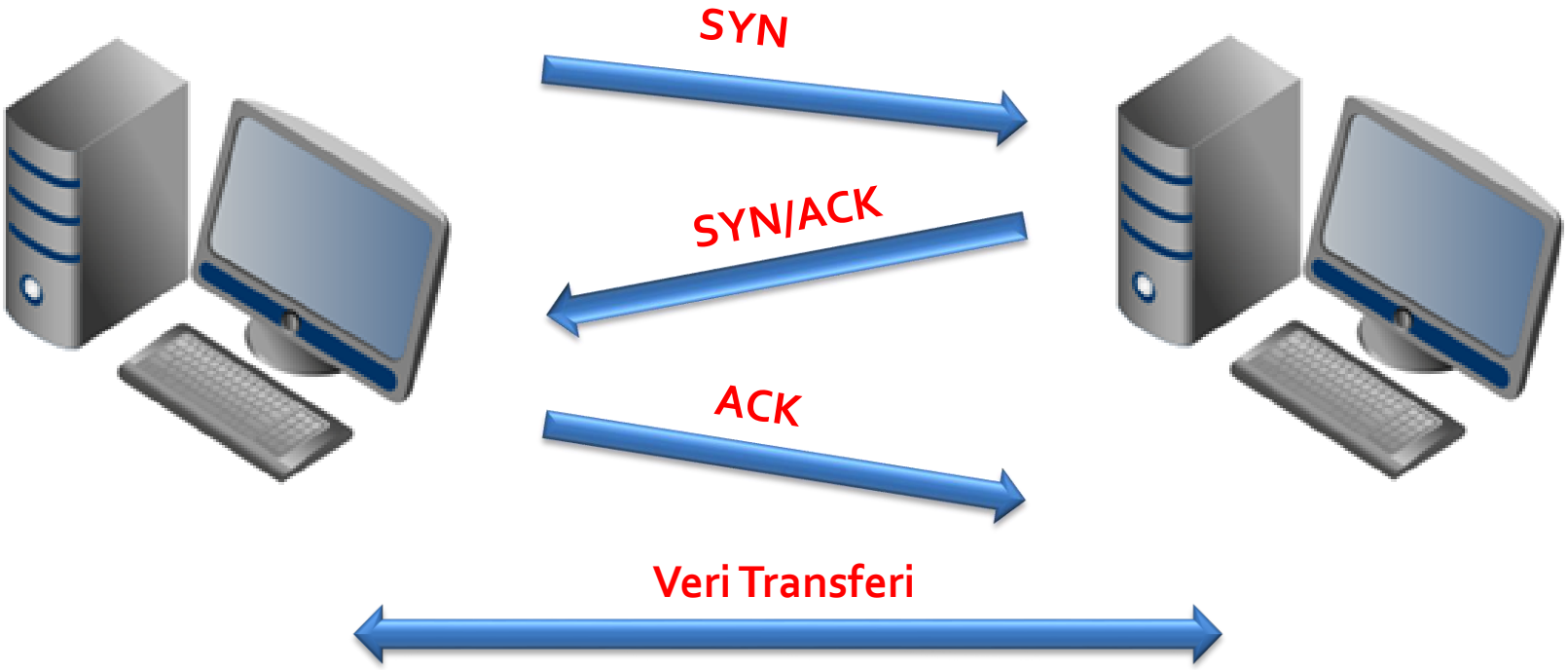
TCP Temelleri

Özellikler

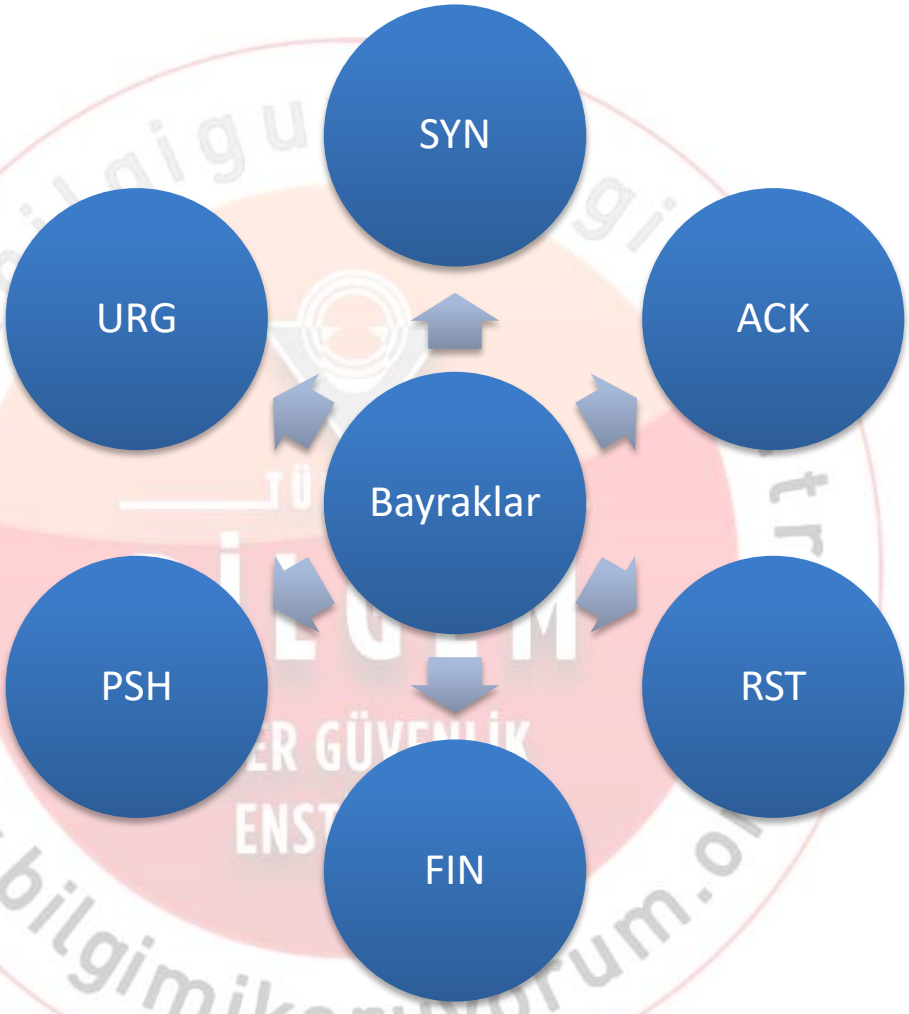
- Bağlantı yönelimlidir
- Verilere sıra numarası eklenir
- Veriler parçalara bölünebilir
- Güvenilirdir
- Akış kontrolü mekanizması vardır
- Çift yönlüdür

TCP Temelleri

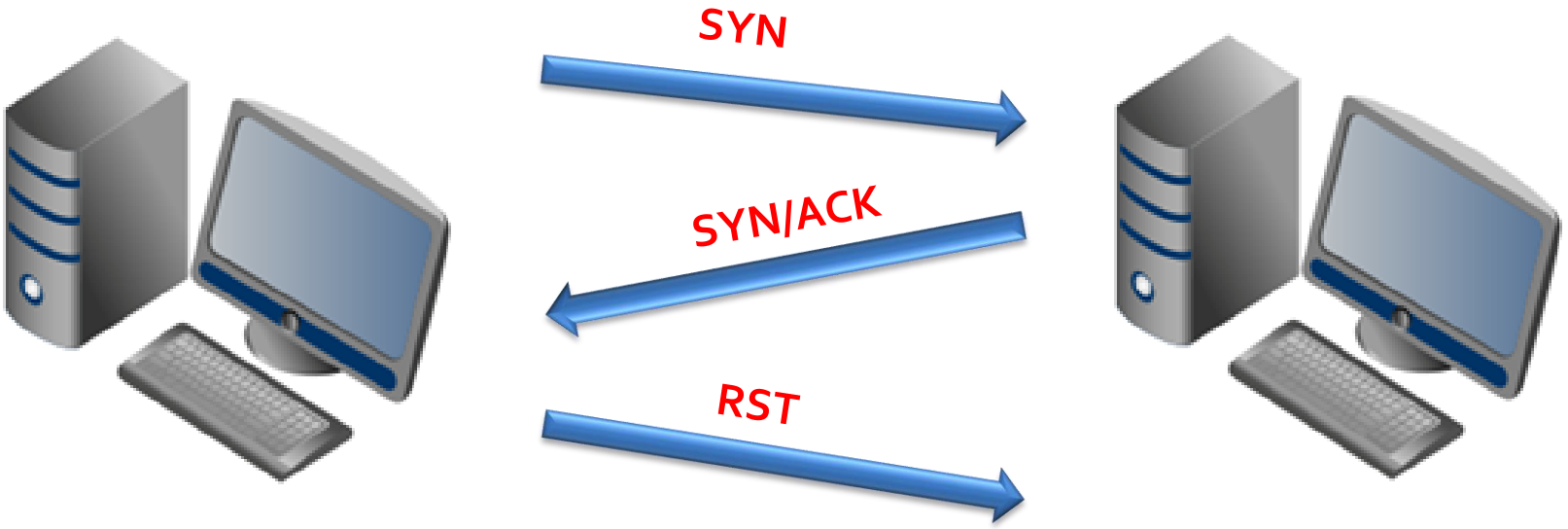
TCP 3'lü el sıkışma



TCP Temelleri



SYN Taraması



SYN Taraması

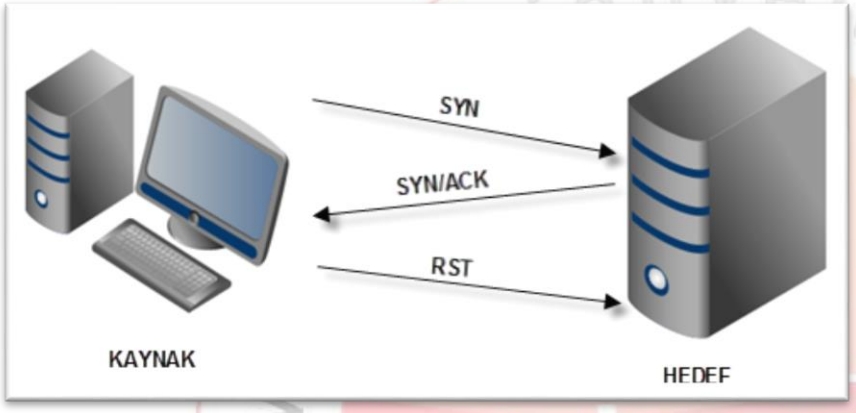
```
root@SGE:~# nmap -sS 10.0.0.1 -p22,23,25

Starting Nmap 6.25 ( http://nmap.org ) at 2(
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

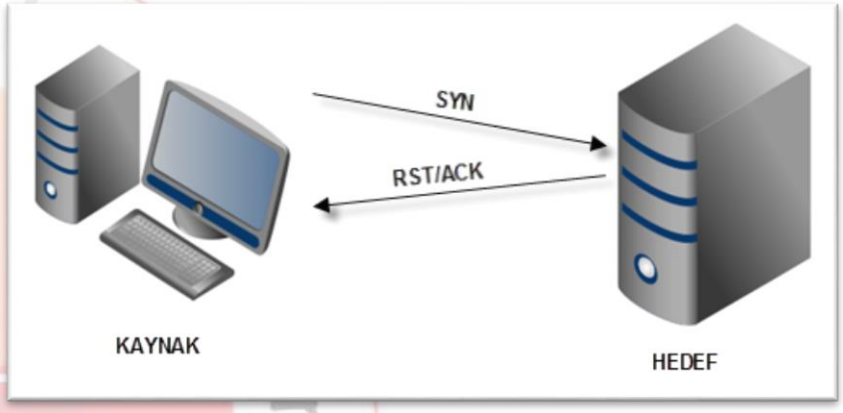
Source	Destination	Protocol	Info
10.100.120.102	10.0.0.1	TCP	40131 > smtp [SYN] Seq=0 Win=1024
10.100.120.102	10.0.0.1	TCP	40131 > telnet [SYN] Seq=0 Win=10
10.100.120.102	10.0.0.1	TCP	40131 > ssh [SYN] Seq=0 Win=1024
10.0.0.1	10.100.120.102	TCP	smtp > 40131 [SYN, ACK] Seq=0 Ack
10.100.120.102	10.0.0.1	TCP	40131 > smtp [RST] Seq=1 Win=0 Le
10.0.0.1	10.100.120.102	TCP	telnet > 40131 [RST, ACK] Seq=1 A
10.100.120.102	10.0.0.1	TCP	40132 > ssh [SYN] Seq=0 Win=1024

SYN Taraması

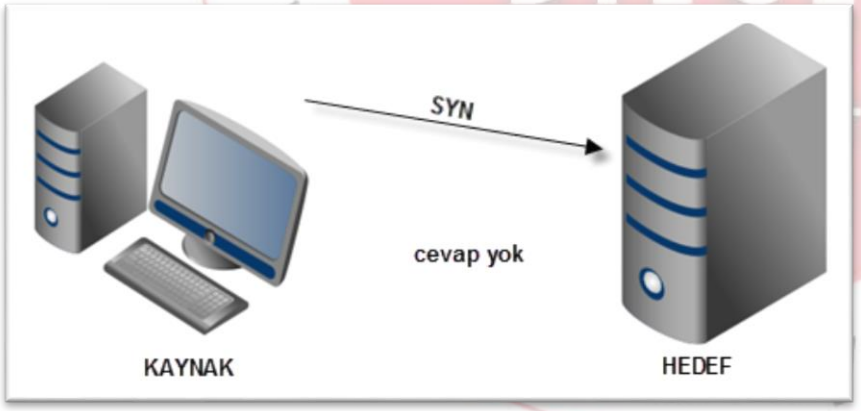
OPEN



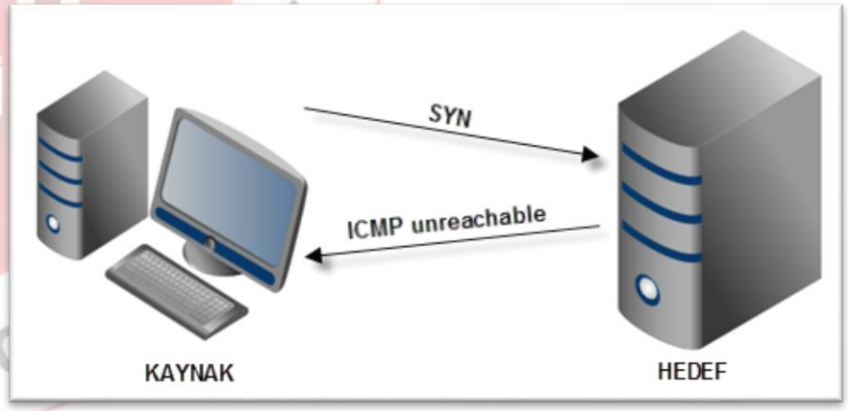
CLOSED



FILTERED



FILTERED



Terimler - Port Durumları

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

Terimler - Port Durumları

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

Port Taraması

Önemli Port Numaraları

21 - FTP	443 - HTTPS
22 - SSH	445 - SMB, Microsoft-DS
23 - Telnet	514 - RSH
25 - SMTP	902 - VMware
53 (UDP) - DNS	1433 - MSSQL
80 - HTTP	1521 - Oracle
110 - POP3	3306 - MySQL
139 - Netbios	3389 - RDP
143 - IMAP	5900 - VNC
161 (UDP) - SNMP	8080, 8081 - Proxy, Uygulama Sunucu

www.iana.org

Port Taraması

TÜBİTAK

- 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
```

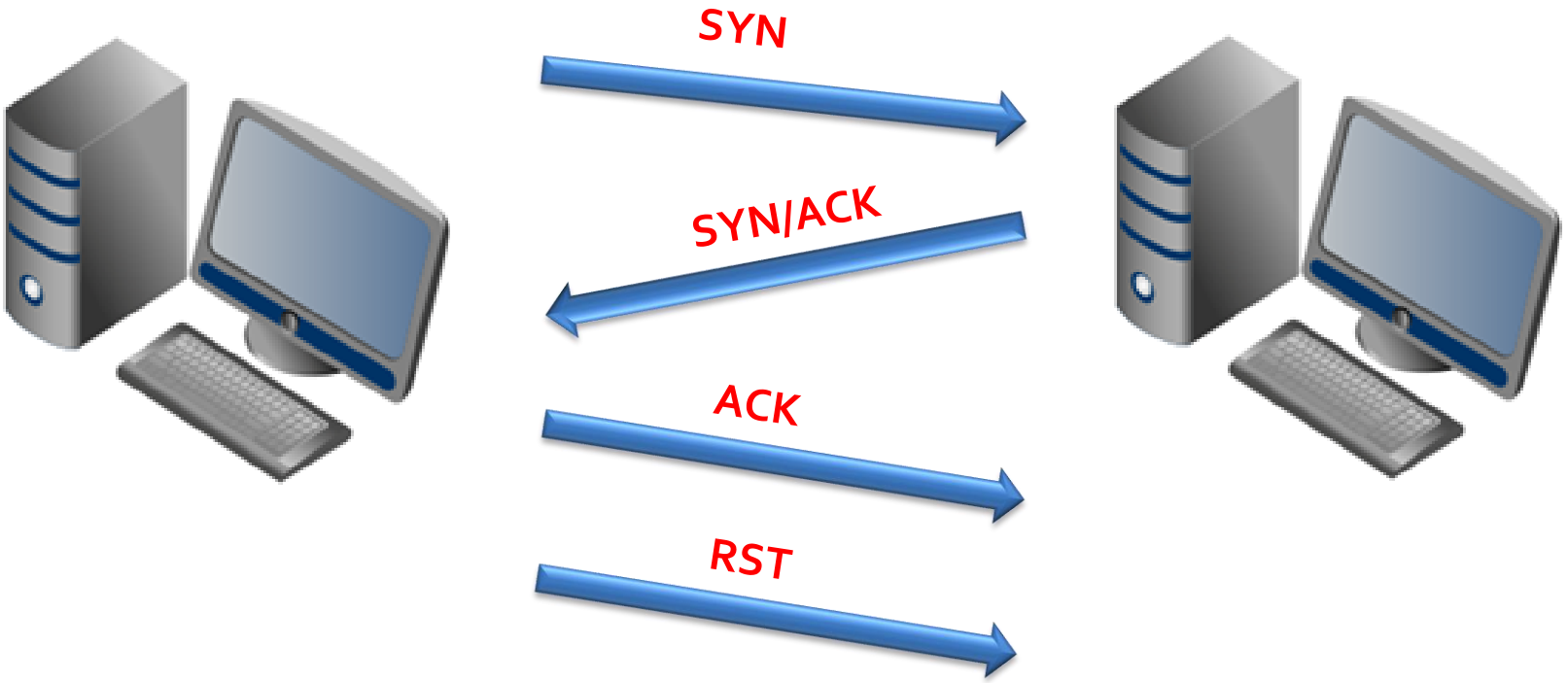
Port Taraması

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

TCP Taraması

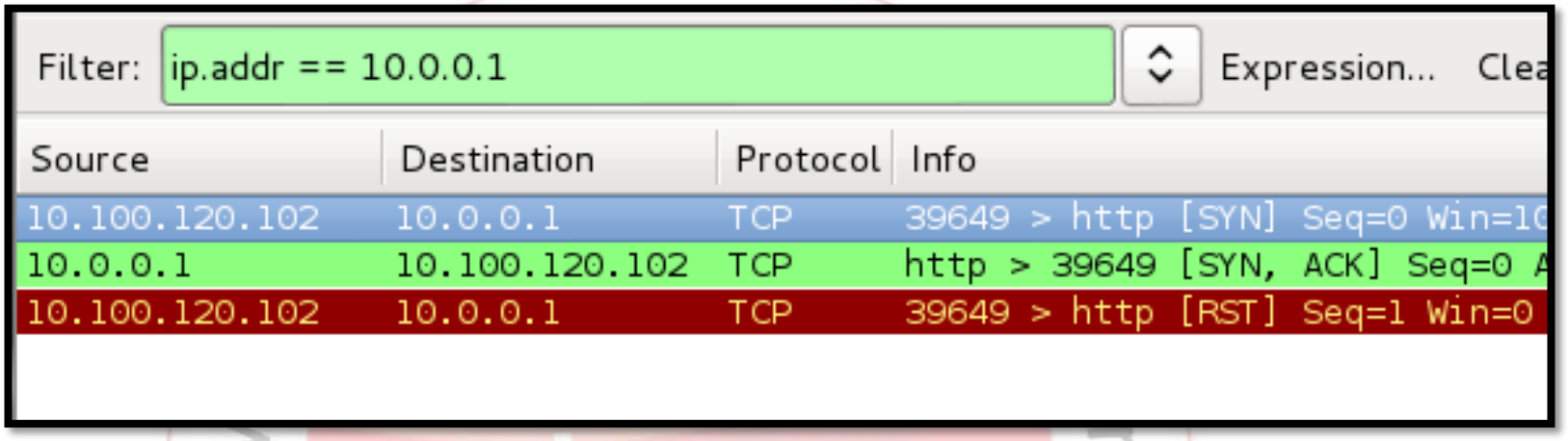
```
# nmap -sT 10.0.0.1 -PN -n -p80
```



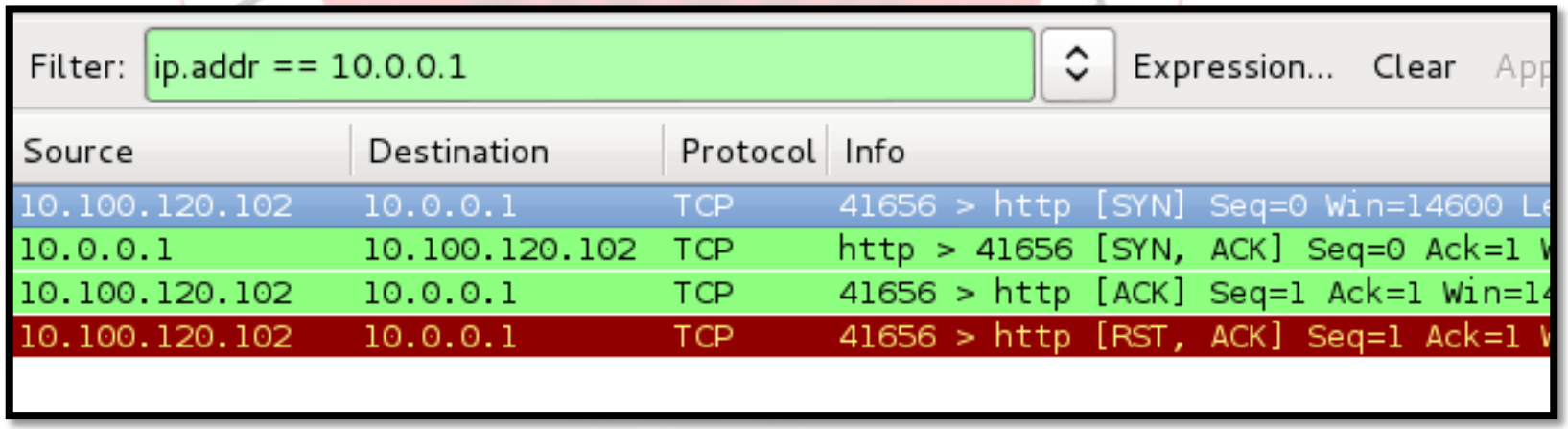
SYN Taraması - TCP Taraması

TÜBİTAK

SYN Taraması



TCP Taraması



SYN Taraması - TCP Taraması

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

UDP Temelleri

OSI Referans Modeli

Kullanıcı etkileşimli uygulamalar: HTTP, SMTP

Farklı veri formatlarını birbirine dönüşümü: ASCII,MP3,JPG

Soket açma, oturum kurma: SQL, RPC

Hata ve akış kontrolü: TCP, UDP

Uçtan uca iletişim, sanal adresleme: IP

Ortama Erişim: Ethernet, Wireless

İkili iletim: Koaksiyel, UTP ve fiber kablolar

UDP Temelleri

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

UDP Taraması

 # nmap -sU -p161 10.0.0.1

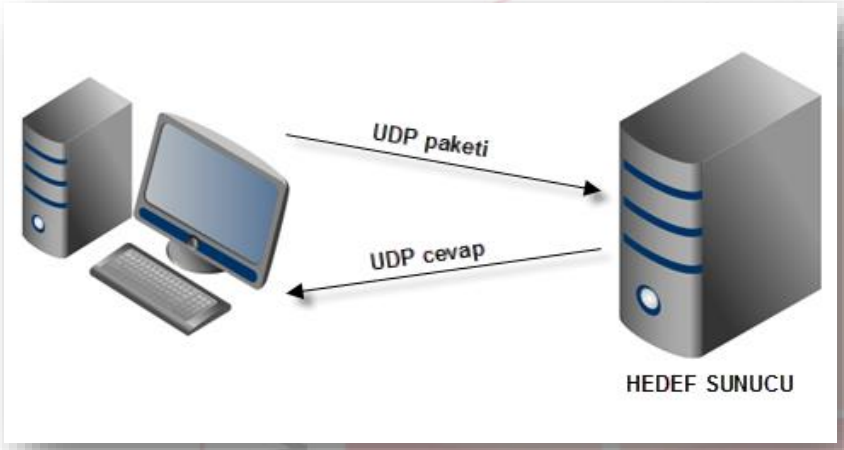
- Uzun zaman alır (timeouts)
- Belirli portlar:
  - DNS (53), TFTP (69), DHCP (67-68), NTP (123), SNMP (161-162)
- Boş UDP paketi gönderir
- Versiyon tespiti ile birlikte çalıştırılmalı

UDP Taraması

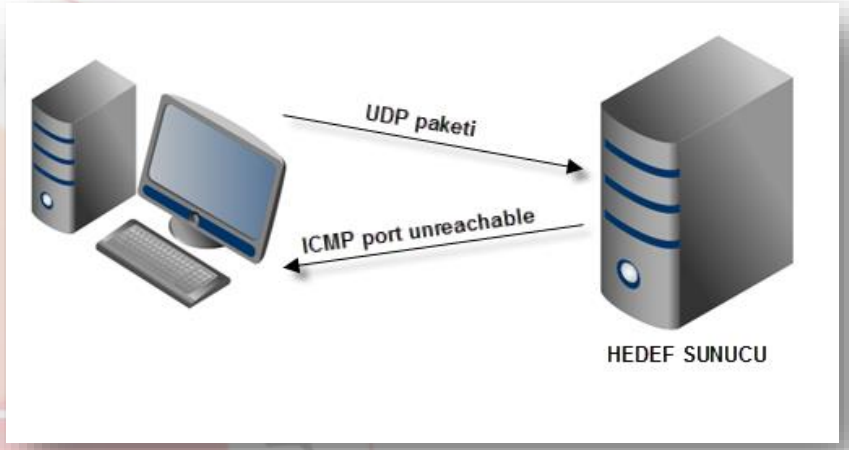
```
root@SGE:~# nmap -sU --top-ports 10 -Pn -n --reason 10.0.0.254

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:~#
```

UDP Taraması

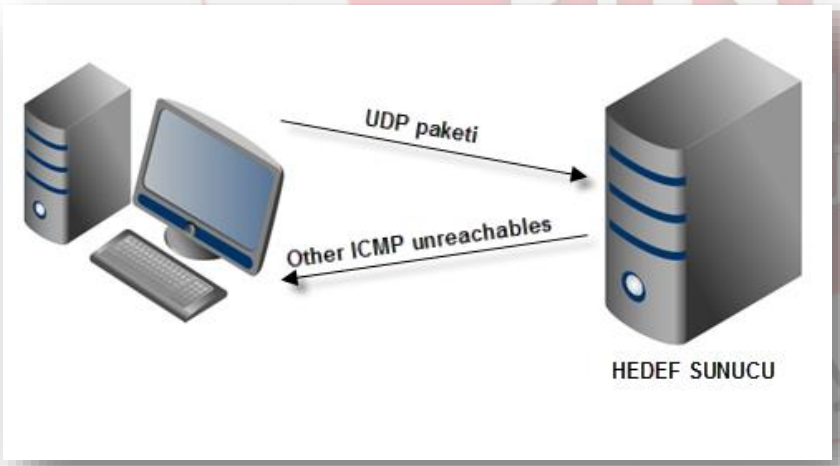
OPEN



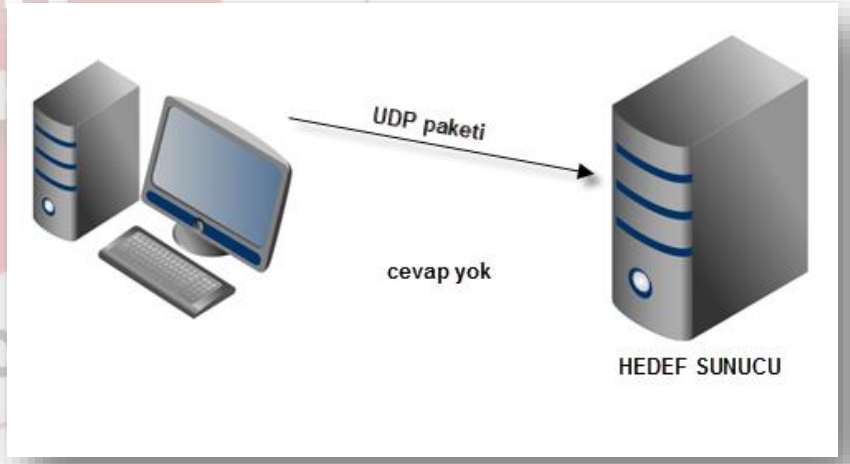
CLOSED



FILTERED



OPEN|FILTERED



NMAP

- [x] Ping Taraması
- [x] Port Taraması
- [x] SYN ve TCP Taramaları
- [x] 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

Servis ve Versiyon Tespiti

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, ...)

Servis ve Versiyon Tespiti

```
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
```

Servis ve Versiyon Tespiti

```
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
```

İşletim Sistemi Tespiti

```
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 - Çıktı Yönetimi

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

Uygulama - 1

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

NMAP

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

NMAP Betik Taraması

Betik Taraması

Nmap Scripting Engine

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

Betik Taraması

-sC (--script=default)

--script “default and safe”

Kategoriler

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

Betik Taraması

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-*”

Betik Taraması

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.
```

Betik Taraması

--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 datatabse.
  Telnet servers that require only a password (but not a username) are
  currently not supported.
root@SGE:~#
```

Betik Taraması

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:b1:7c:77:af:3a:89: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/subm
Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
root@SGE:~#
```

Betik Taraması

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

Betik Taraması

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

Betik Taraması

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:~#
```

Betik Taraması

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:~#
```

NMAP

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

Zamanlama, IPS/IDS Atlatma

Zamanlama

-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

Zamanlama

Paralel Taramanın Kapatılması

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

IPS/IDS Atlatma

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

www.bilgiguvenligi.gov.tr
TÜBİTAK
BİLGEM
SİBER GÜVENLİK
ENSTİTÜSÜ
www.bilgimikoruyorum.org.tr

NMAP

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

Büyük Ağların Taranması

Büyük Ağlarda Tarama

TÜBİTAK

Büyük ağların küçük alt ağlara bölünmesi

- Örnekleme 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

Büyük Ağlarda Tarama

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 unreachables dönmeli

IP blokları ve adresleri istenebilir

Büyük Ağlarda Tarama

TÜBİTAK

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/$/\.0\/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 Taraması

ACK bayrağı işaretli paket gönderilir

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

Filtreleme olup olmadığı tespit edilir

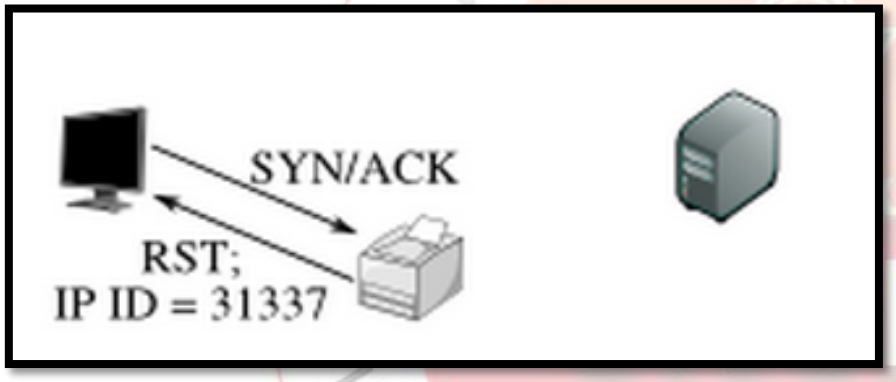
Durum

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

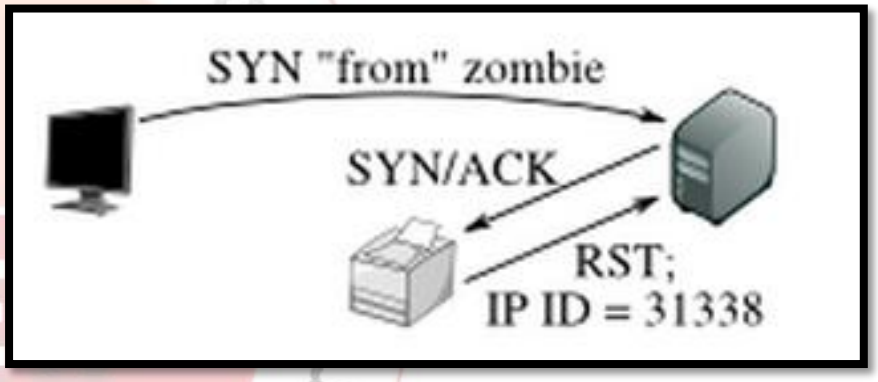
Nmap Idle Scan

open

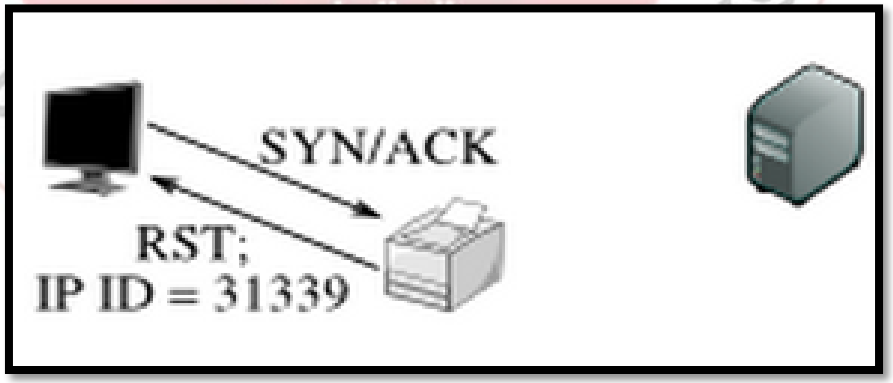
1



2



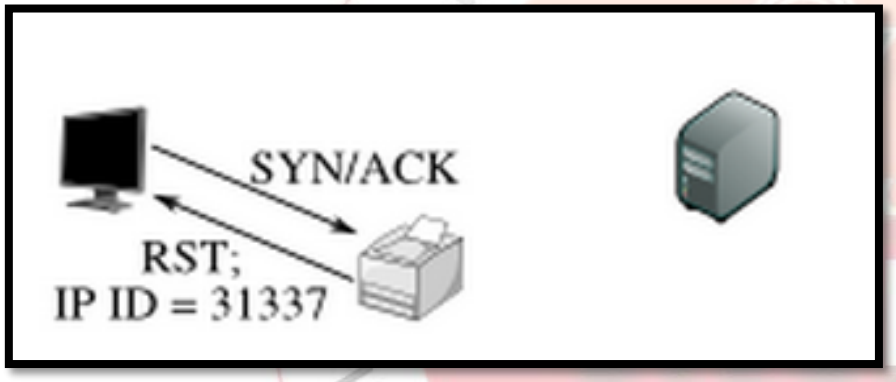
3



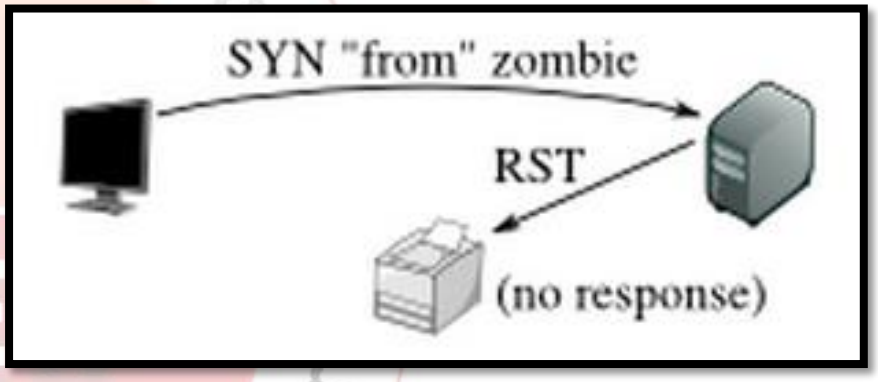
Nmap Idle Scan

closed

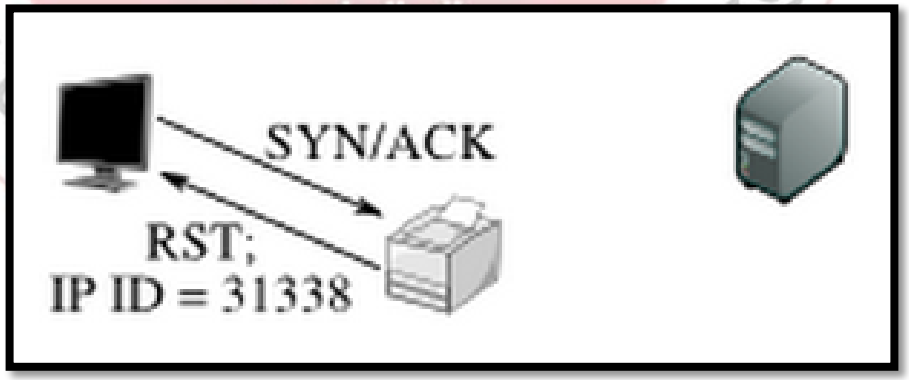
1



2

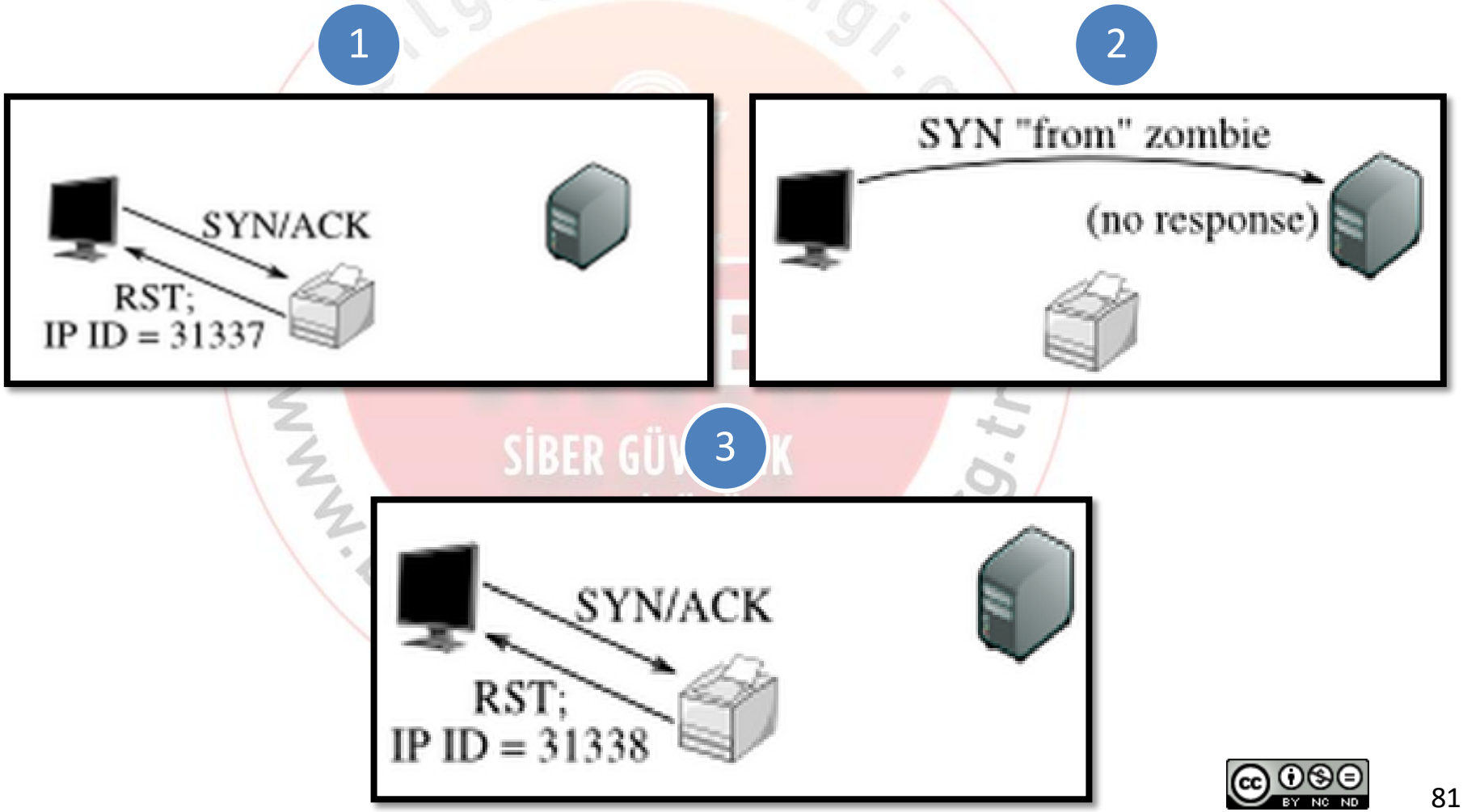


3



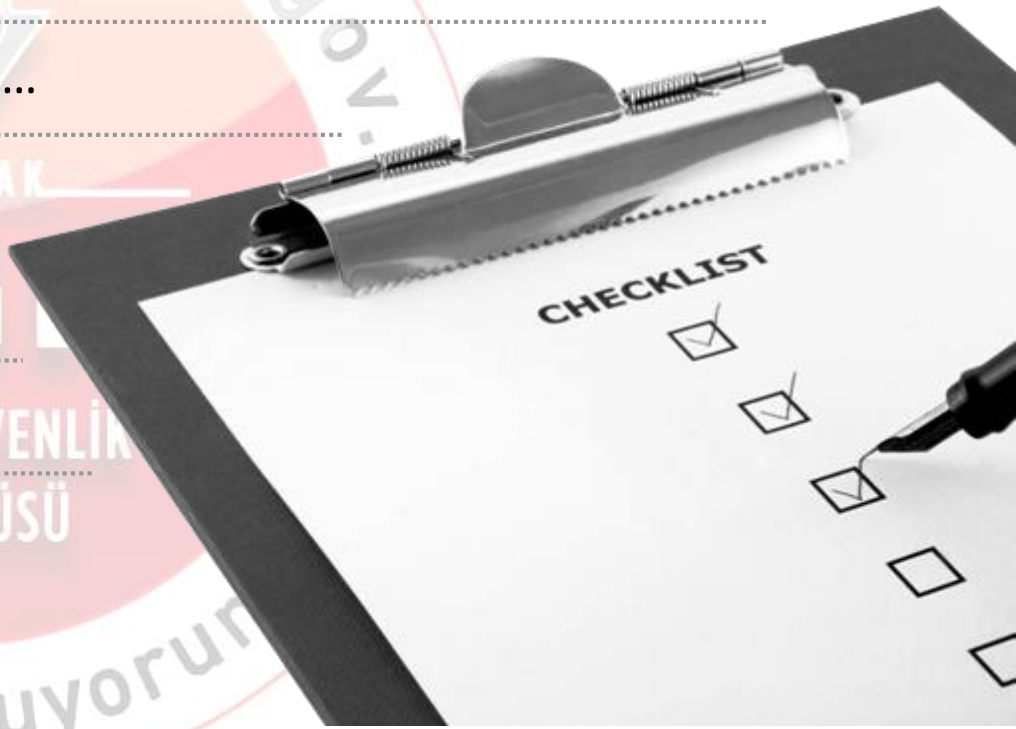
Nmap Idle Scan

filtered



NMAP

- **Keşif**
  - Pasif Keşif
    - Wireshark, tcpdump, …
  - Aktif Keşif
    - Nmap
- **Zafiyet Tarama**
  - Nessus



Zafiyet Taraması

Terimler

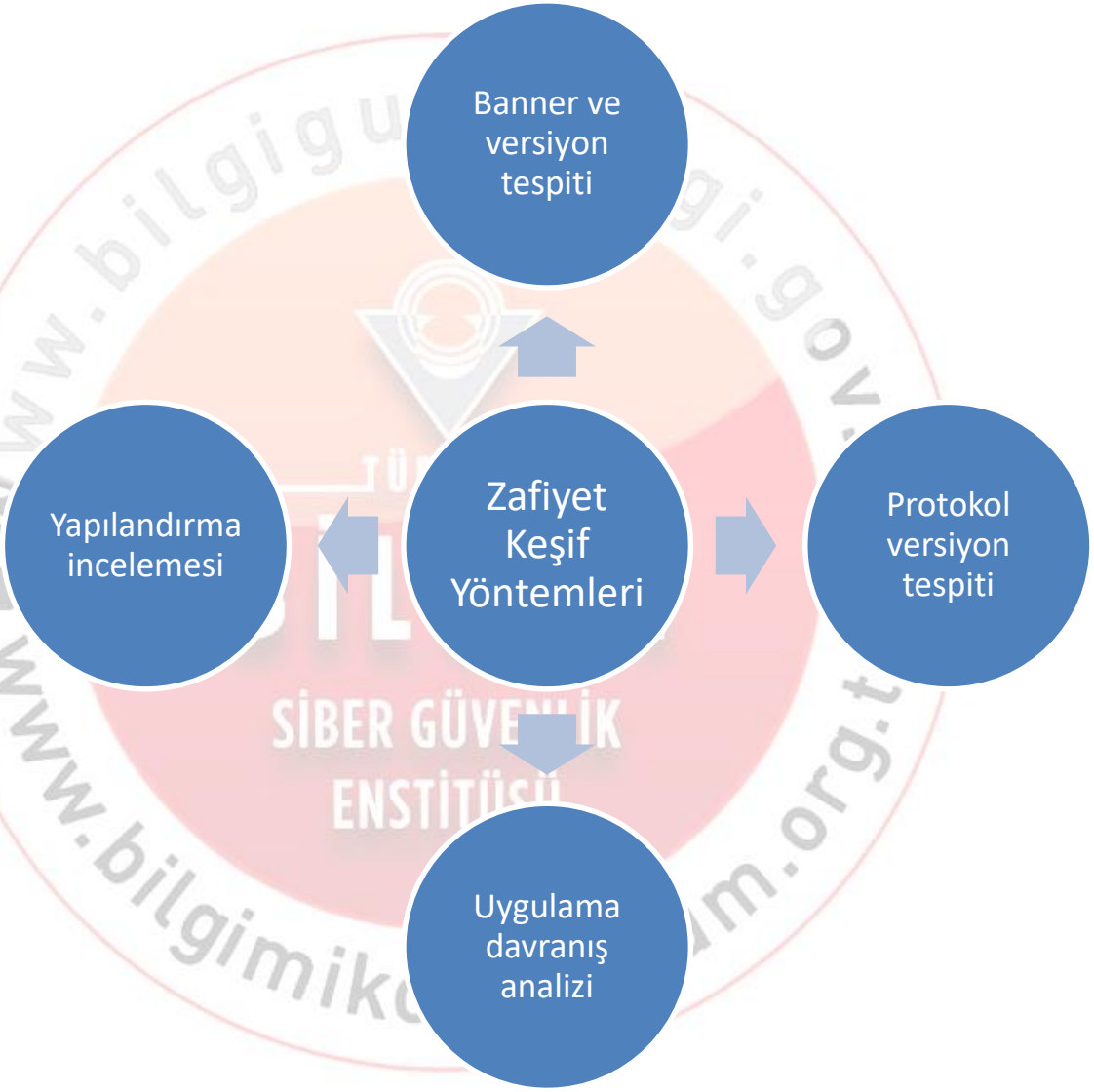
Zafiyet

- “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 Yönetimi

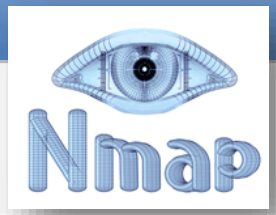
Zafiyet Taraması

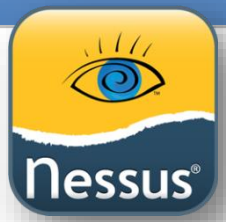


Zafiyet Taraması

Zafiyet Tarayıcıları

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





Zafiyet Taraması

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

Nessus

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

Nessus - Kurulum

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:~#
```

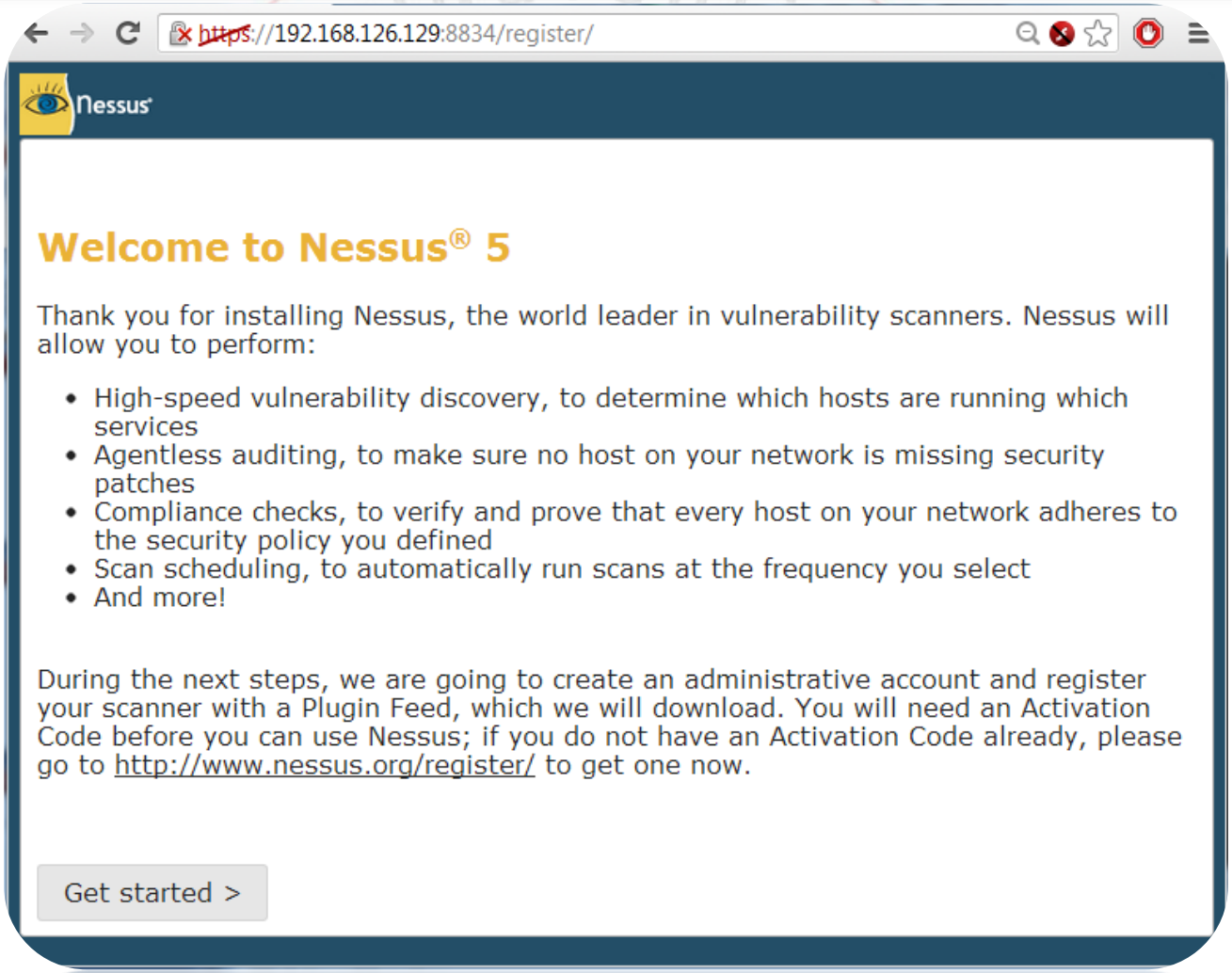
Nessus - Kurulum

Servis Başlatmak

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

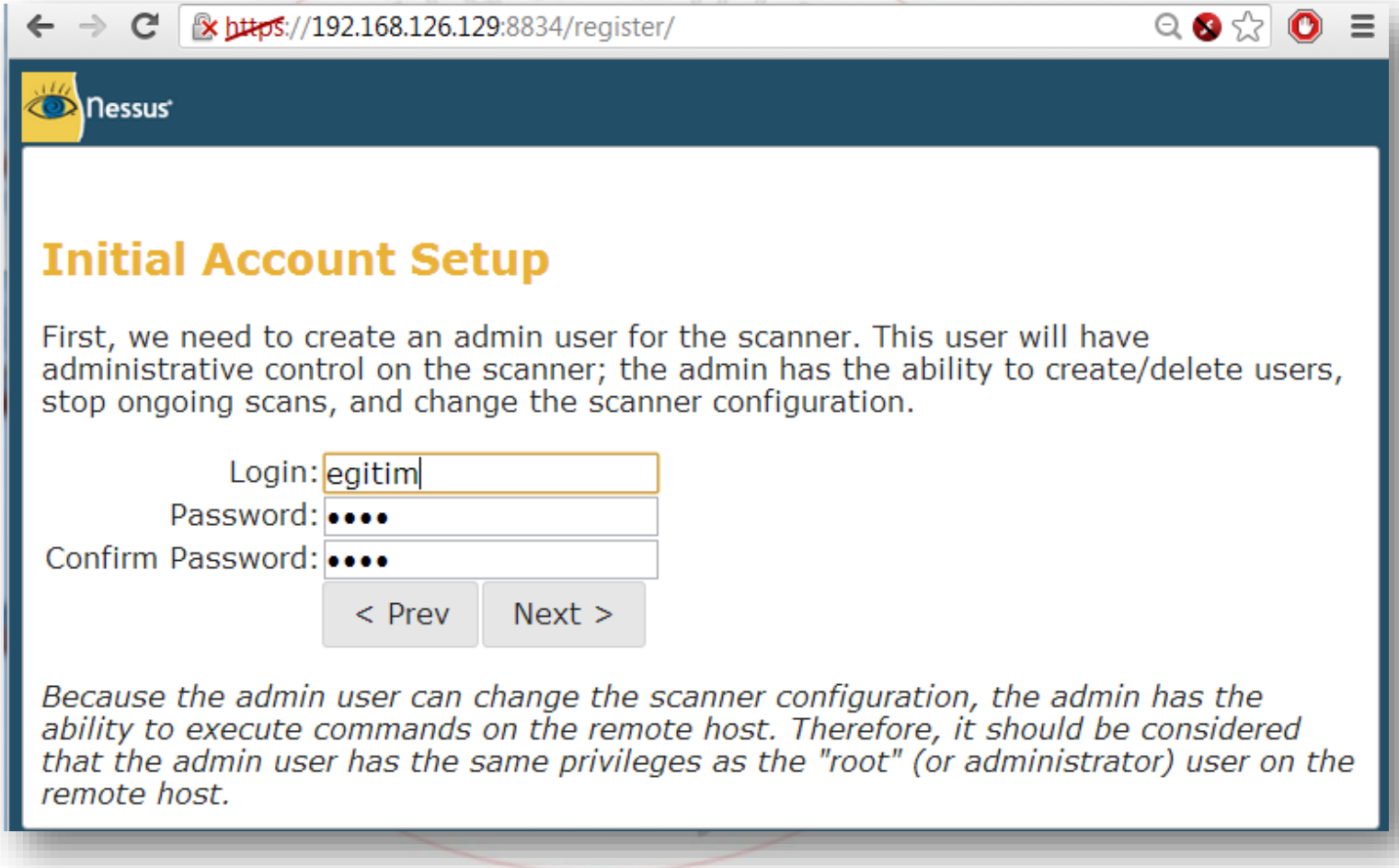
Nessus - Kurulum

İlk Kurulum Ekranı



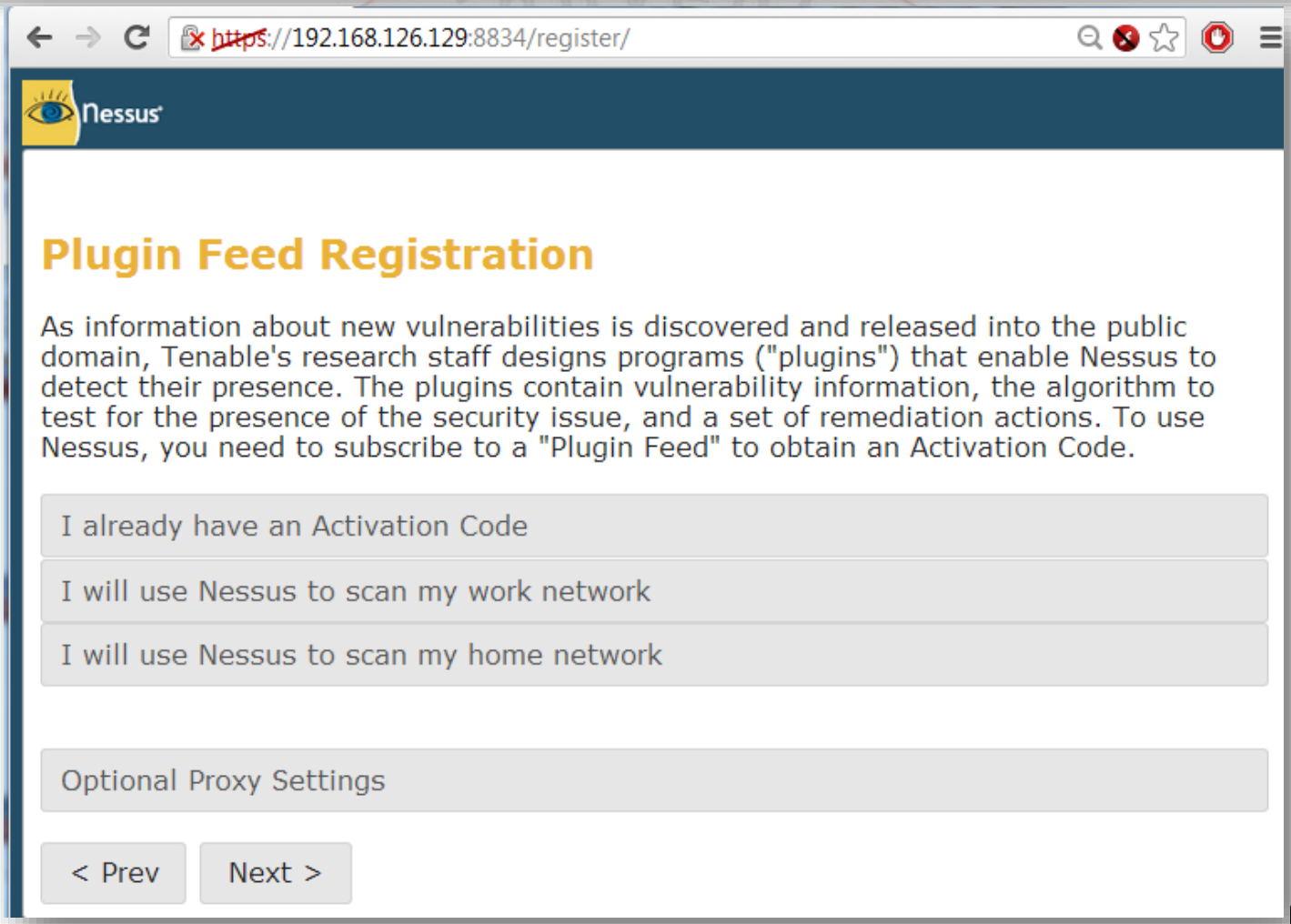
Nessus - Kurulum

İlk Kullanıcının Oluşturulması



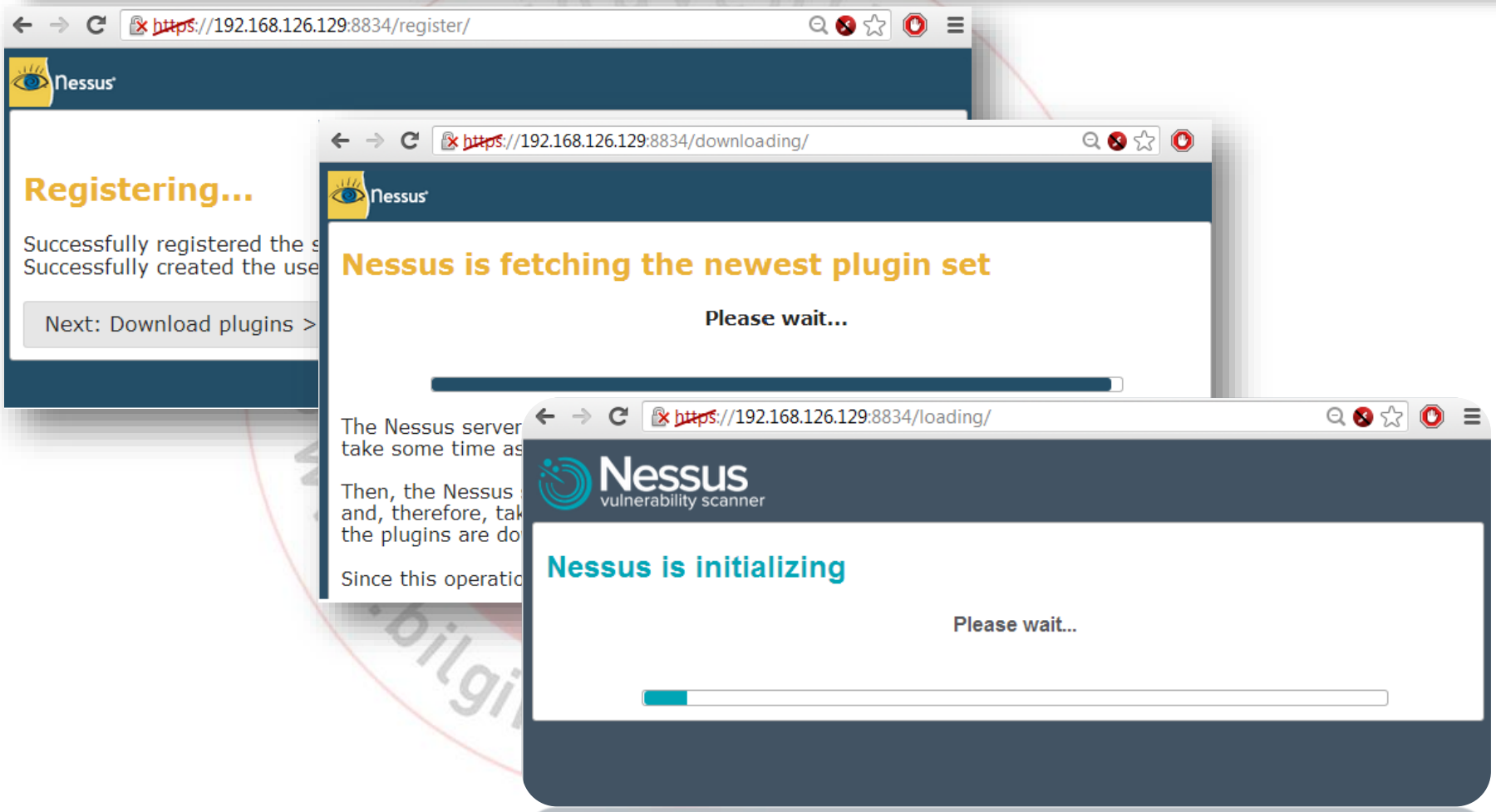
Nessus - Kurulum

Aktivasyon Kodu Elde Edilmesi/Girilmesi



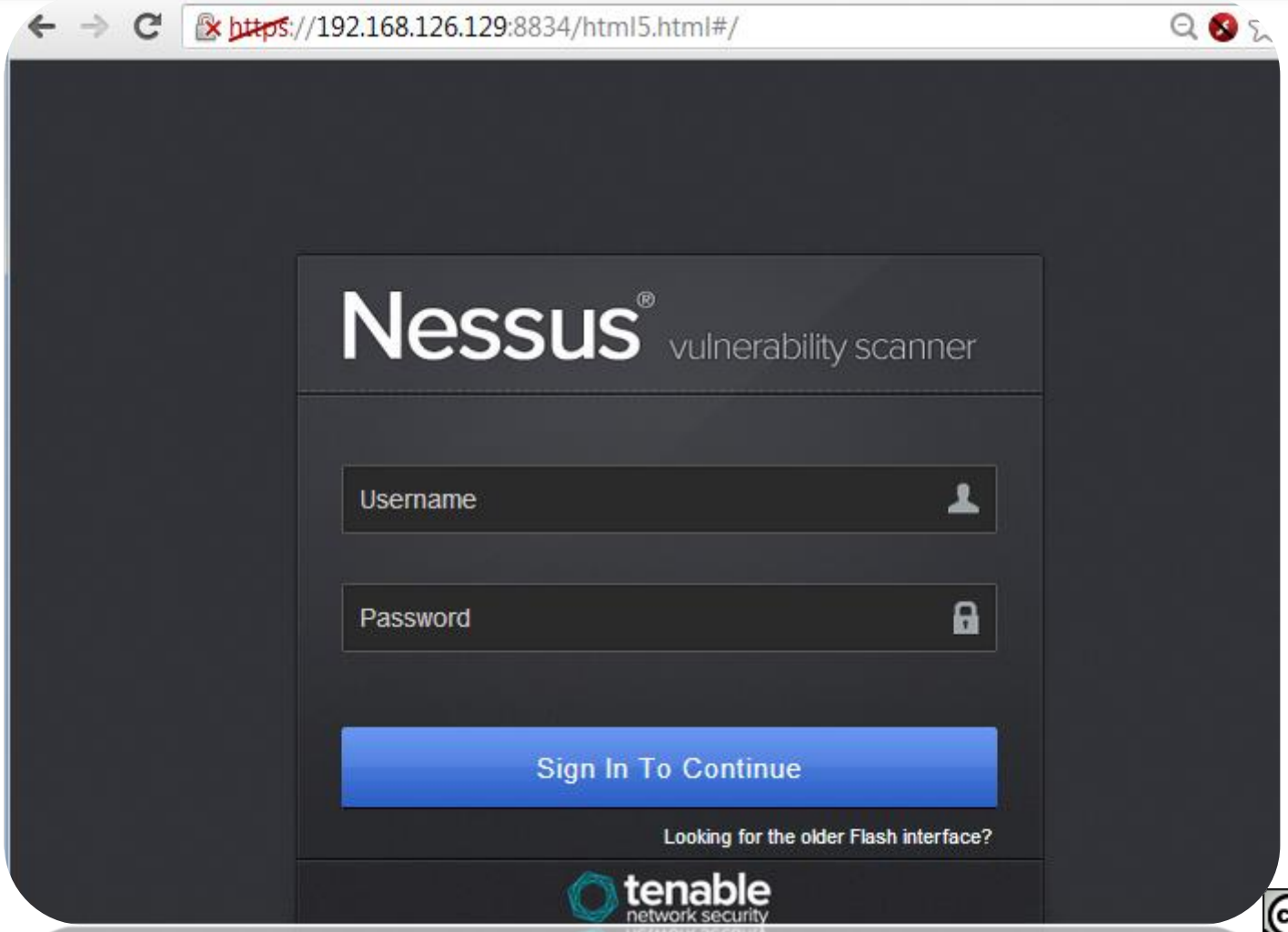
Nessus - Kurulum

Kurulum



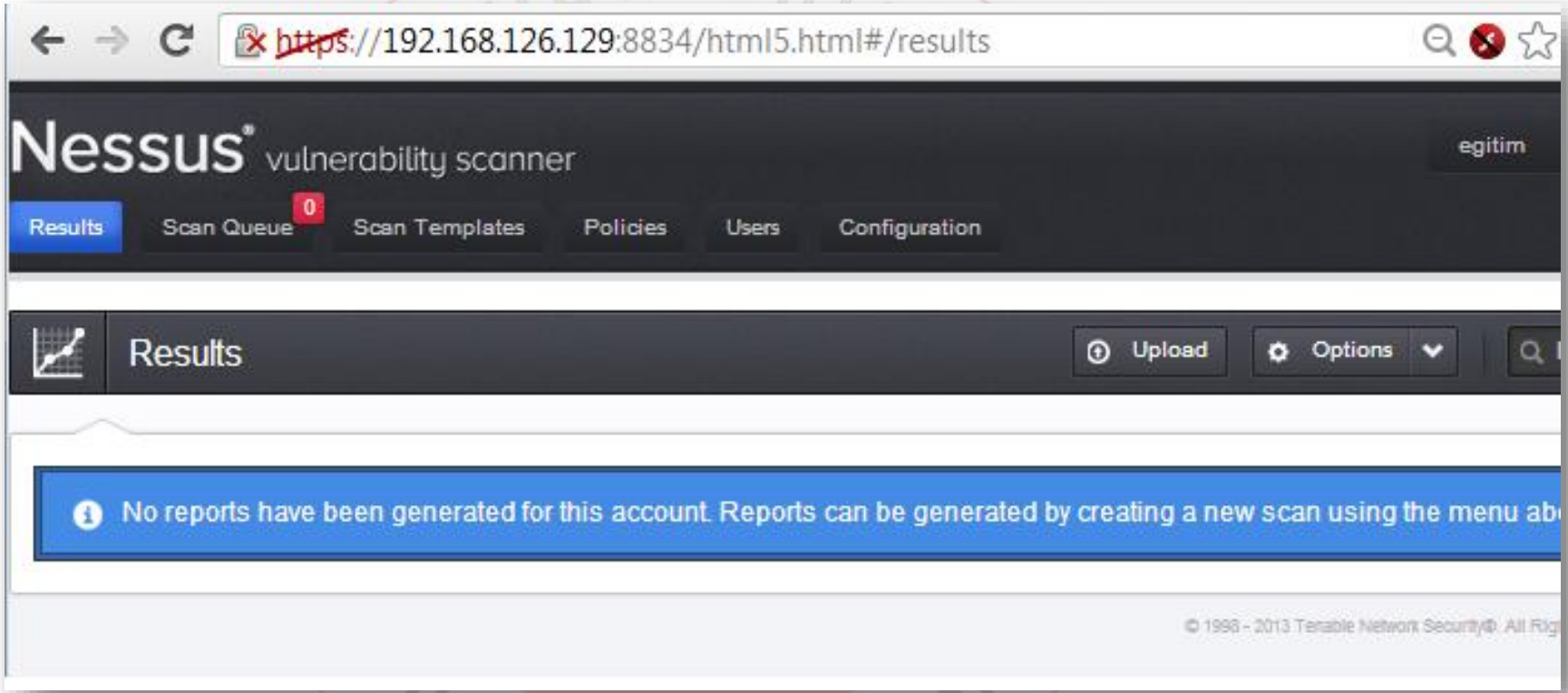
Nessus - Kurulum

Ana Giriş Ekranı



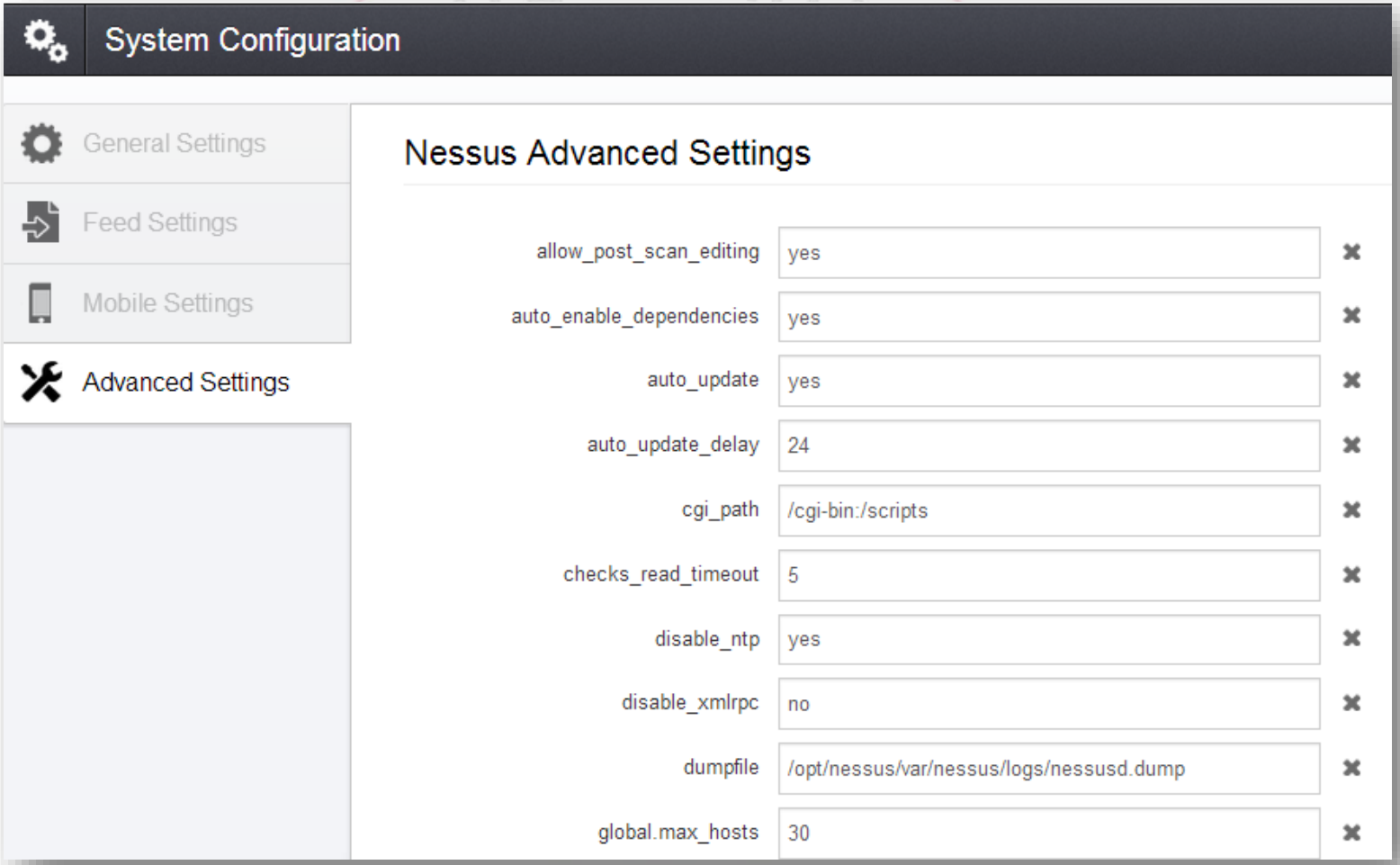
Nessus - Kurulum

Ana Giriş Ekranı



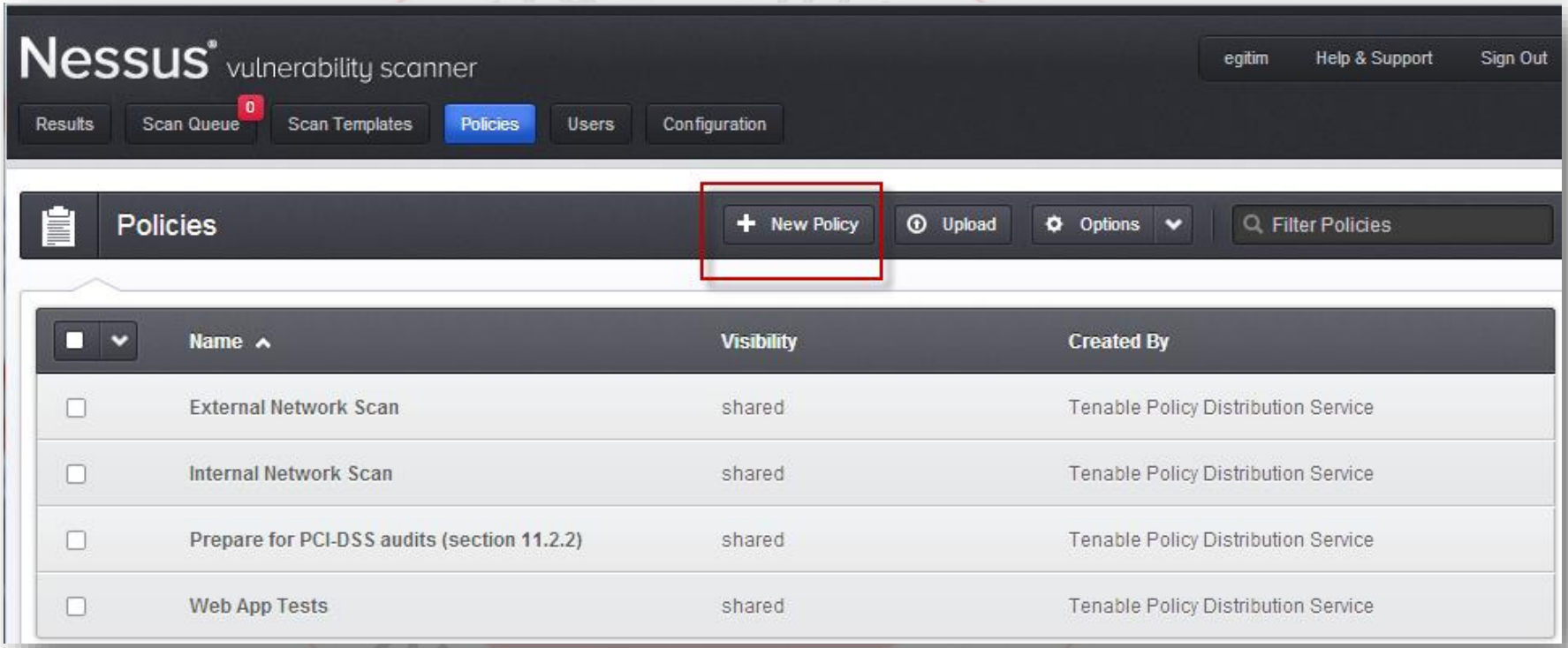
Nessus - Kurulum

Ayarlar



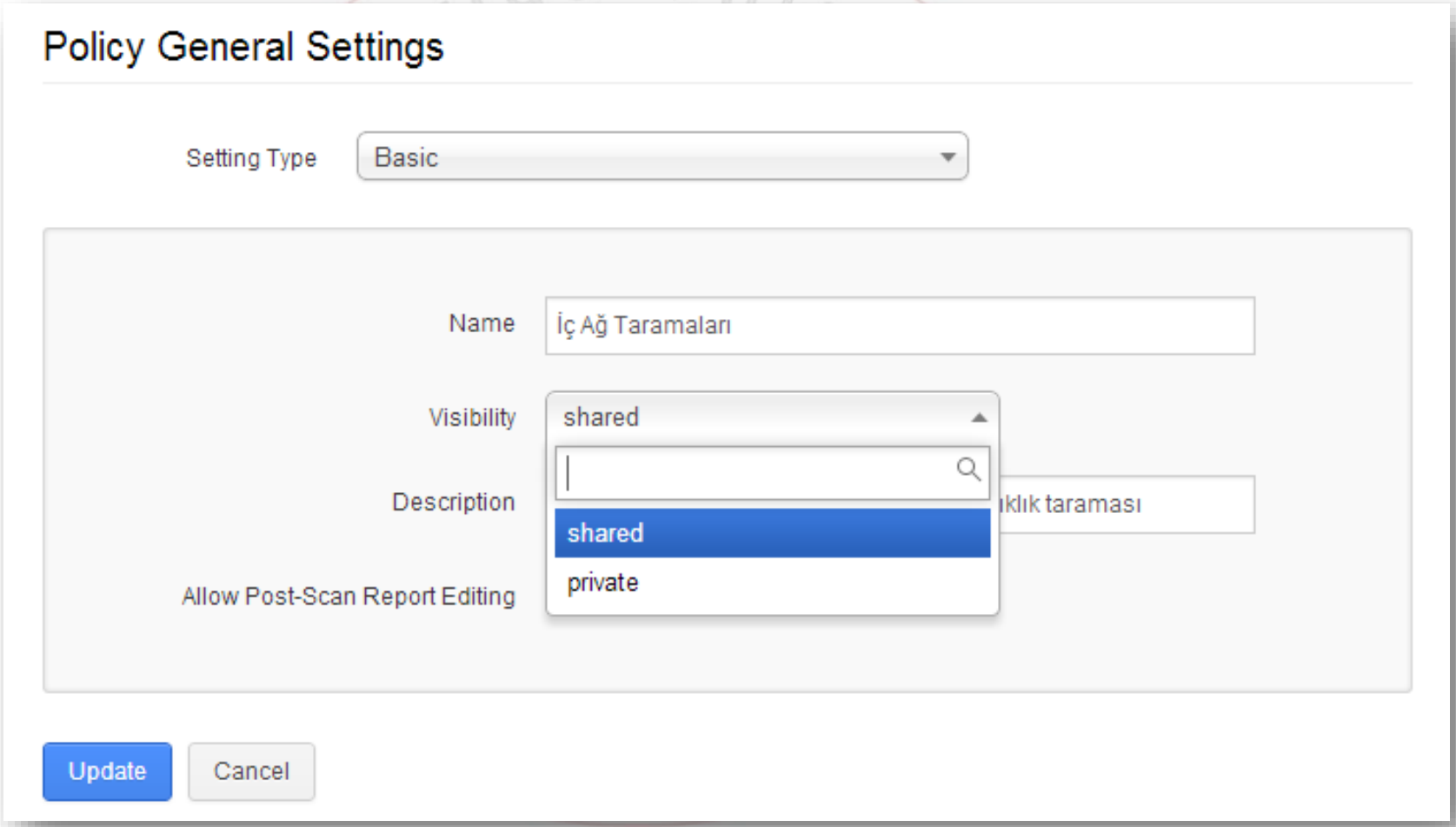
Nessus - Politika Oluşturma

Yeni Politika Oluşturma



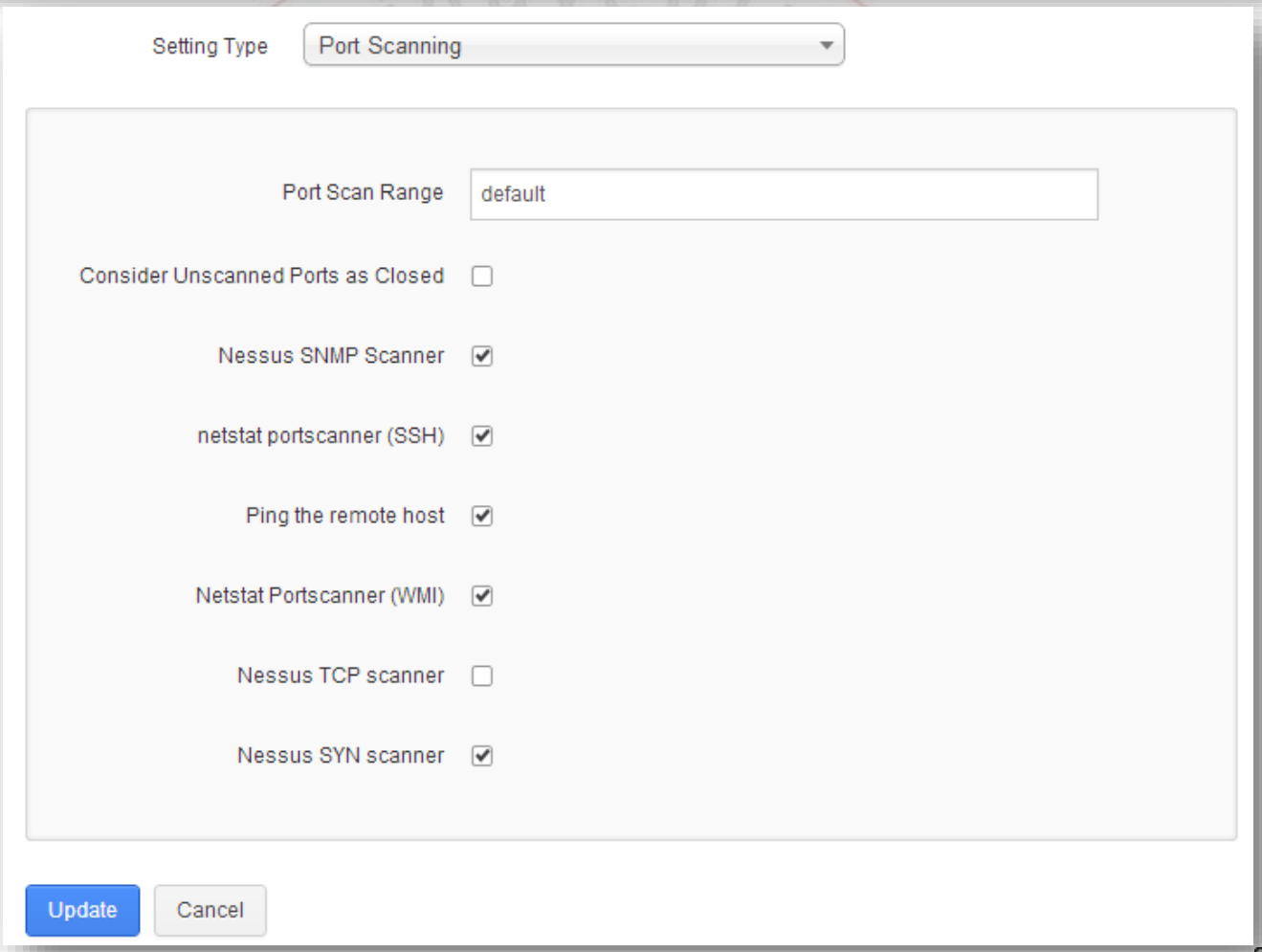
Nessus - Politika Oluşturma

Politika Seçenekleri



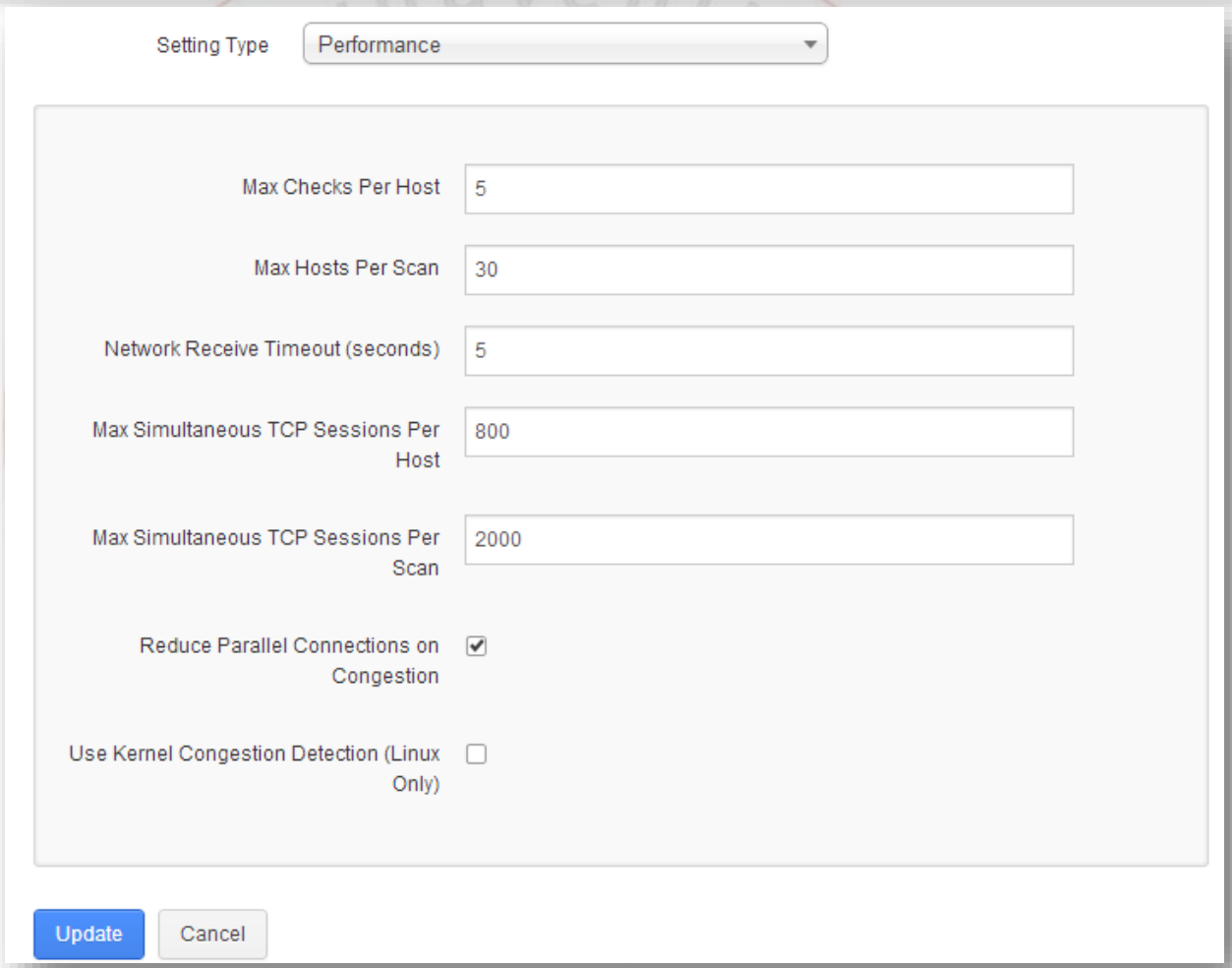
Nessus - Politika Oluşturma

Tarama Ayarları



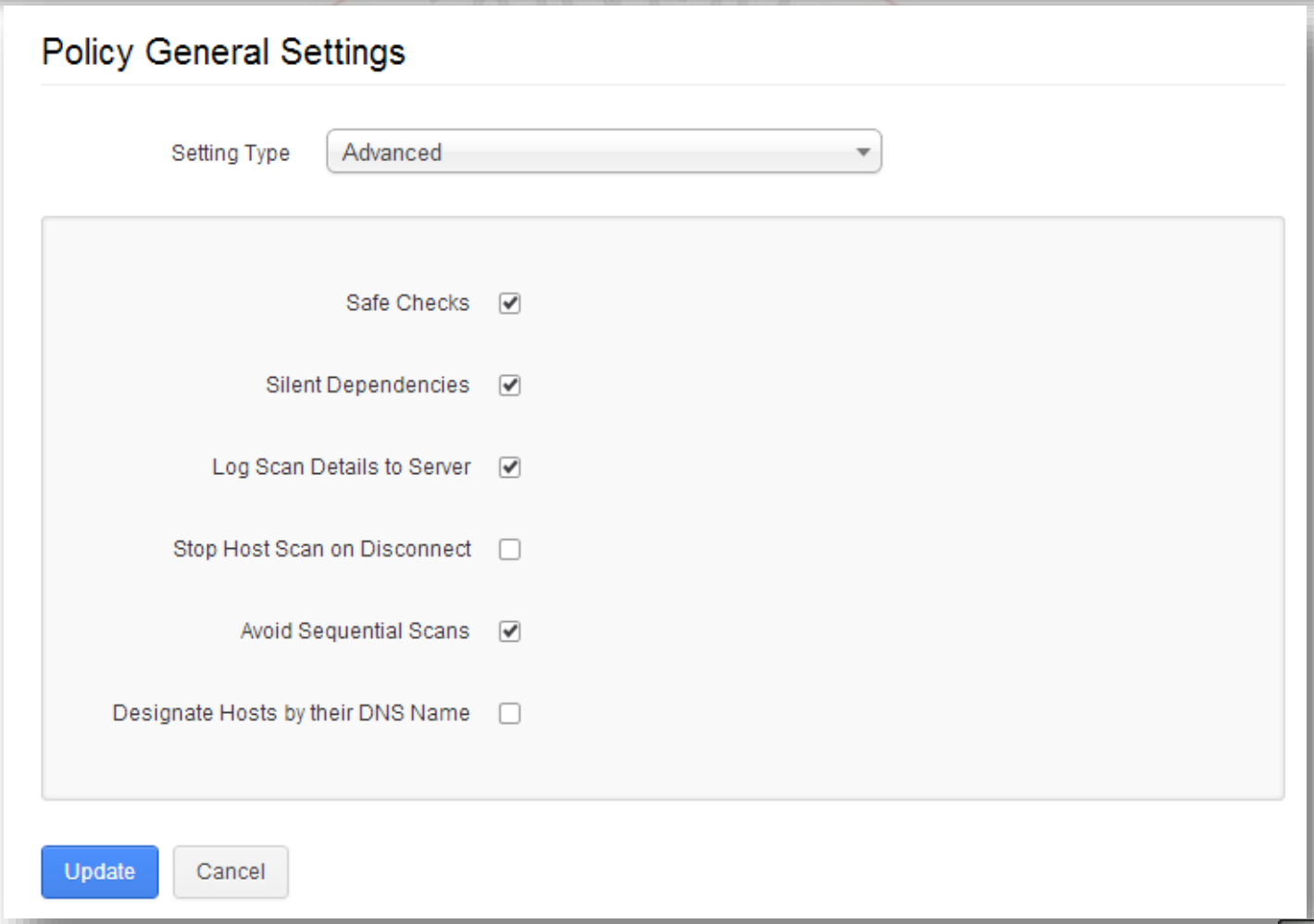
Nessus - Politika Oluşturma

Performans Ayarları



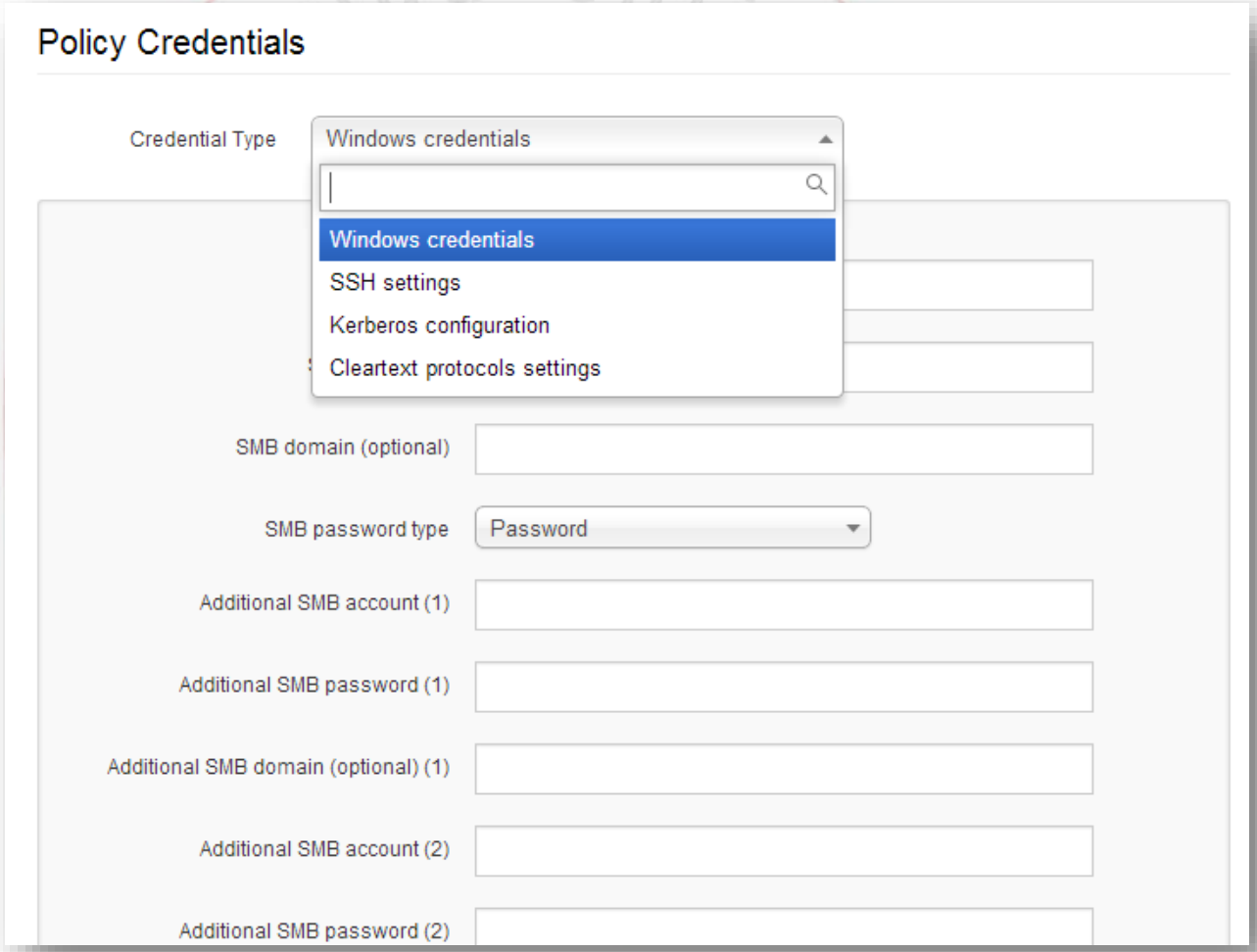
Nessus - Politika Oluşturma

Gelişmiş Ayarlar



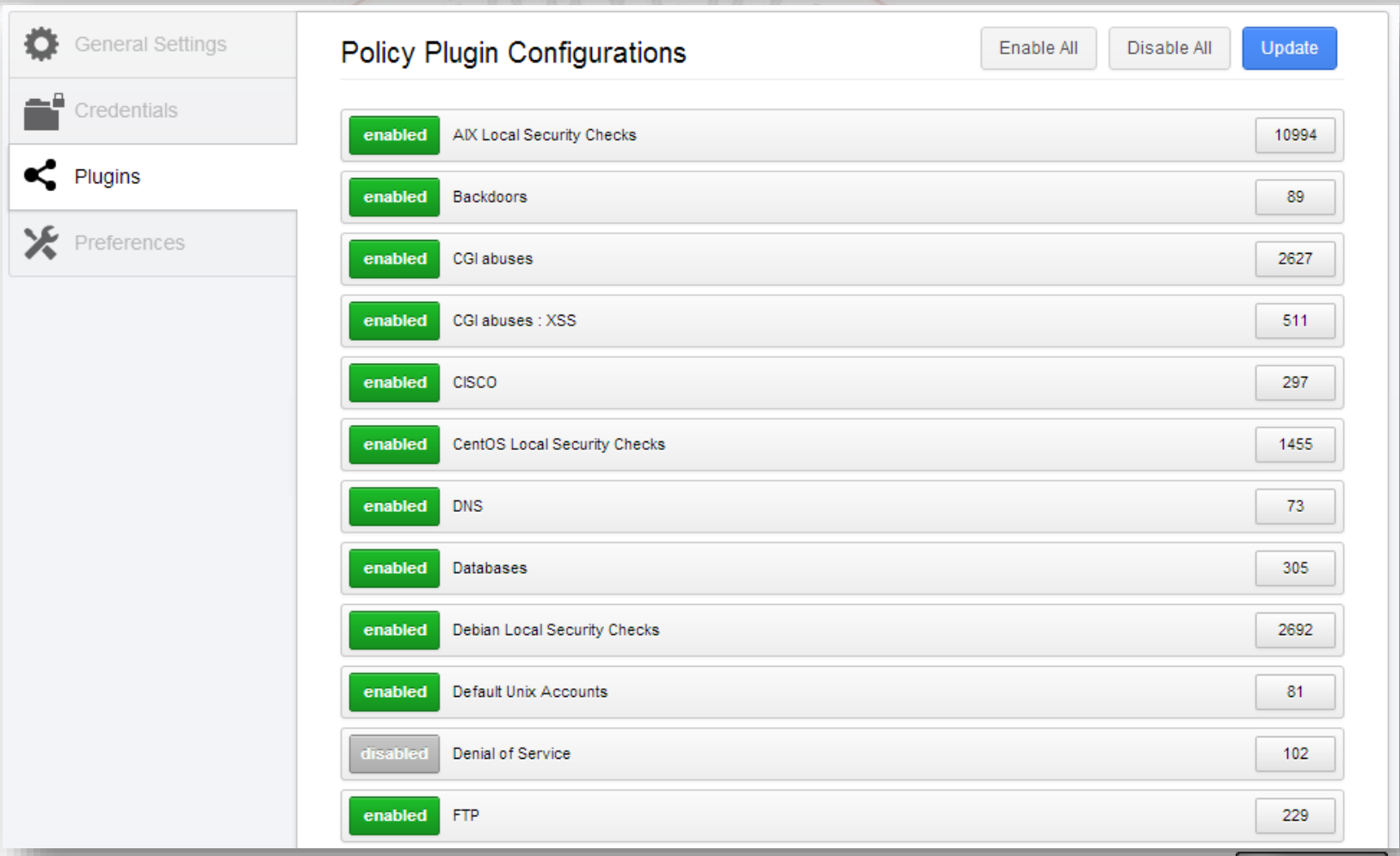
Nessus - Politika Oluşturma

Kullanıcı Bilgisi Ekleme



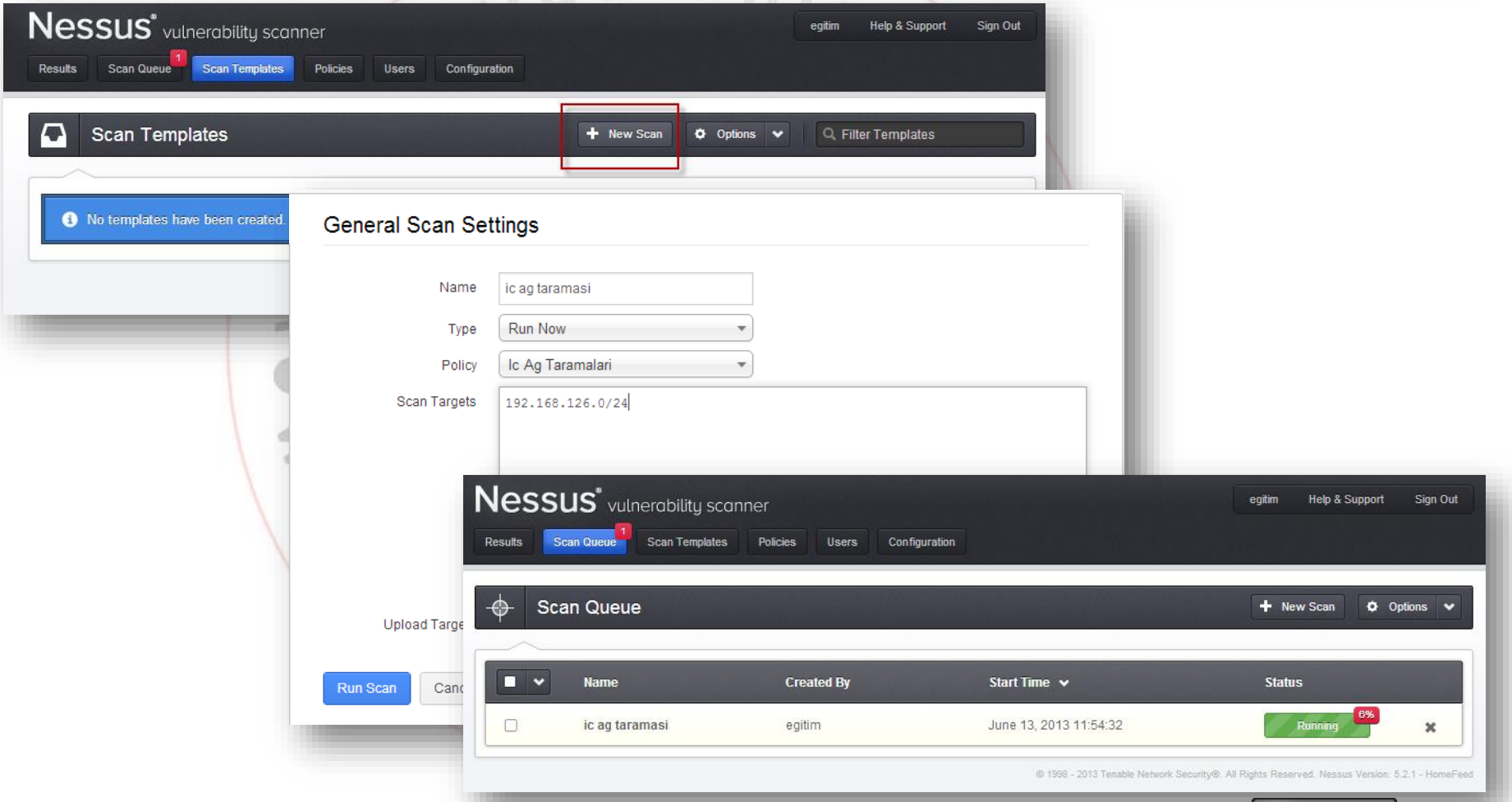
Nessus - Politika Oluşturma

Plugin Ayarları



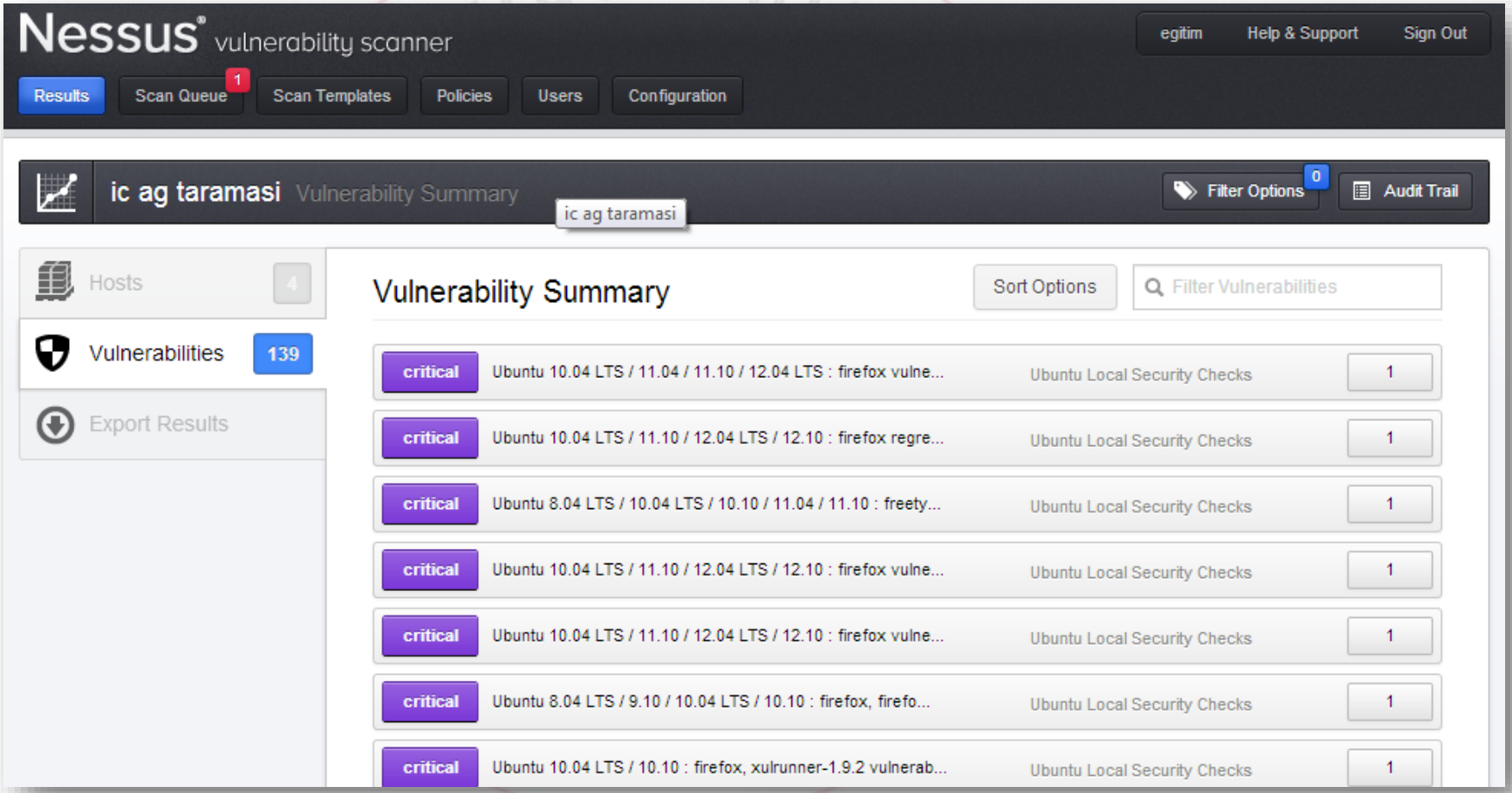
Nessus - Tarama

Yeni Tarama



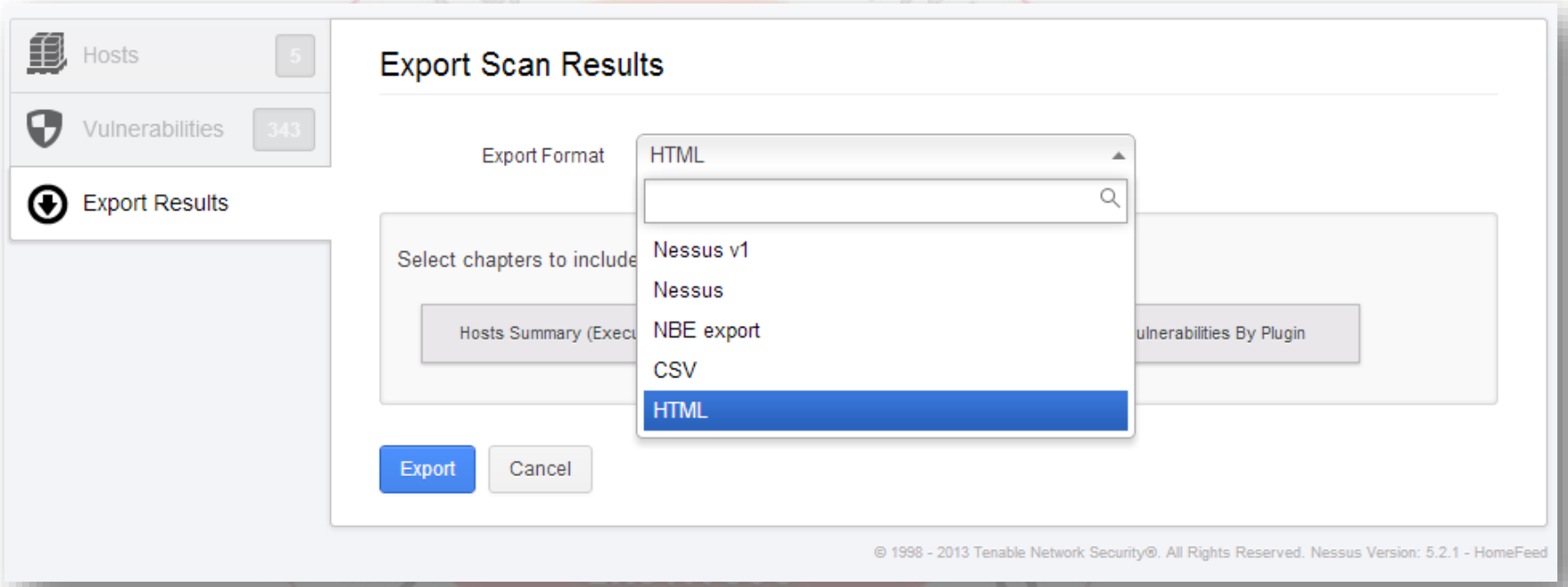
Nessus - Raporlama

Tarama Sonuçlarının İncelenmesi



Nessus - Raporlama

Rapor Formatları



Nessus - Raporlama

Rapor Örneği

Nessus vulnerability scanner

Nessus Scan Report

Table Of Contents

Uygulama - 2

- Nessus Web Arayüzünden Bağlan
- Tarama Politikası Tanımla
- Hedefleri Seç
- Taramayı Çalıştır
- Sonuçları Teftiş Et

TÜBİTAK

Teşekkürler