

# Aktif Bilgi Toplama

# NMAP

```
bl4ck@bl4ck:~$ whatis nmap
nmap (1)           - Network exploration tool and security / port scanner
```

The screenshot shows a presentation slide titled "NMAP" with a dark background and red and yellow diagonal stripes. The slide content is as follows:

**NAME**  
nmap - Network exploration tool and security / port scanner

**SYNOPSIS**  
`nmap [Scan Type...] [Options] {target specification}`

**DESCRIPTION**  
Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

The output from Nmap is a list of scanned targets, with supplemental information on each depending on the options used. Key among that information is the "interesting ports table". That table lists the port number and protocol, service name, and state. The state is either open, filtered, closed, or unfiltered. Open means that an application on the target machine is listening for connections/packets on that port. Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed. Closed ports have no application listening on them, though they could open up at any time. Ports are classified as unfiltered when they are responsive to Nmap's probes, but Nmap cannot determine whether they are open or closed. Nmap reports the state combinations open|filtered and closed|filtered when it cannot determine which of the two states describe a port. The port table may also include software version details when version detection has been requested. When an IP protocol scan is requested (-sO), Nmap provides information on supported IP protocols rather than listening ports.

In addition to the interesting ports table, Nmap can provide further information on targets, including reverse DNS names, operating system guesses, device types, and MAC addresses.

A typical Nmap scan is shown in Example 1. The only Nmap arguments used in this example are -A, to enable OS and version detection, script scanning, and traceroute; -T4 for faster execution; and then the hostname.

# NMAP - Basic Scan - IP

```
bl4ck@bl4ck:~$ sudo nmap 192.168.73.128
```

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-31 16:48 +03  
Nmap scan report for 192.168.73.128  
Host is up (0.00038s latency).  
Not shown: 977 closed ports

PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
53/tcp	open	domain
80/tcp	open	http
111/tcp	open	rpcbind
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
512/tcp	open	exec
513/tcp	open	login
514/tcp	open	shell
1099/tcp	open	rmiregistry
1524/tcp	open	ingreslock
2049/tcp	open	nfs
2121/tcp	open	ccproxy-ftp
3306/tcp	open	mysql
5432/tcp	open	postgresql
5900/tcp	open	vnc
6000/tcp	open	X11
6667/tcp	open	irc
8009/tcp	open	ajp13
8180/tcp	open	unknown

MAC Address: 00:0C:29:F3:BE:D9 (VMware)

```
File Virtual Machine Help
```

No mail.  
To run a command as administrator (user "root"), u  
See "man sudo\_root" for details.

```
msfadmin@metasploitable:~$ ifconfig
```

eth0	Link encap:Ethernet HWaddr 00:0c:29:f3: Inet addr:192.168.73.128 Bcast:192.168. inet6 addr: fe80::20c:29ff:fe:f3:bed9/64 UP BROADCAST RUNNING MULTICAST MTU:1500 RX packets:66 errors:0 dropped:0 overrun RX bytes:6871 (6.7 KB) TX bytes:11911 (
	Interrupt:19 Base address:0x2000

```
msfadmin@metasploitable:~$ _
```

lo	Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 inet6 addr: ::1/128 Scope:Host UP LOOPBACK RUNNING MTU:16436 Metric:1 RX packets:156 errors:0 dropped:0 overrun TX packets:156 errors:0 dropped:0 overrun collisions:0 txqueuelen:0 RX bytes:50421 (49.2 KB) TX bytes:50421
----	---

## TOP 1000 Port

# NMAP – Basic Scan - Domain

```
bl4ck@bl4ck:~$ nmap scanme.nmap.org
```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-31 20:00 +03
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.21s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 16.36 seconds
bl4ck@bl4ck:~$ 
```

TOP 1000 Port

## DNS Lookup

# NMAP – IP Range

```
bl4ck@bl4ck:~$ sudo nmap 192.168.73.0/24
Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-31 16:58 +03
Nmap scan report for 192.168.73.128
Host is up (0.00024s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
514/tcp   open  rmiregistry
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
8180/tcp  open  unknown
MAC Address: 00:0C:29:F3:BE:D9 (VMware)
MAC Address: 00:0C:29:F3:BE:D9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.67 seconds
bl4ck@bl4ck:~$
```

# NMAP - Specific Port

-p 80

```
bl4ck@bl4ck:~$ sudo nmap 192.168.73.128 -p 80

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-31 17:08 +03
Nmap scan report for 192.168.73.128
Host is up (0.00023s latency).

PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:0C:29:F3:BE:D9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.58 seconds
bl4ck@bl4ck:~$ █
```

# NMAP - Specific Ports

-p 80,443,21

```
bl4ck@bl4ck:~$ sudo nmap 192.168.73.128 -p 80,443,21

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-31 17:13 +03
Nmap scan report for 192.168.73.128
Host is up (0.00025s latency).

PORT      STATE    SERVICE
21/tcp    open     ftp
80/tcp    open     http
443/tcp   closed   https
MAC Address: 00:0C:29:F3:BE:D9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.73 seconds
bl4ck@bl4ck:~$ █
```

# NMAP - OS Detection

## -O

```
bl4ck@bl4ck:~$ sudo nmap 192.168.73.128 -O

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-31 17:17 +03
Nmap scan report for 192.168.73.128
Host is up (0.00052s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
```

```
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

```
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.80 seconds
bl4ck@bl4ck:~$ 
```

# NMAP - Version Detection

-sV

```
bl4ck@bl4ck:~$ sudo nmap 192.168.73.128 -sV

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-31 17:22 +03
Nmap scan report for 192.168.73.128
Host is up (0.00050s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
1524/tcp  open  shell        Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:F3:BE:D9 (VMware)
Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 109.04 seconds
```

# NMAP - All Ports Scan

```
bl4ck@bl4ck:~$ sudo nmap 192.168.73.128 -p 0-65535
```

```
bl4ck@bl4ck:~$ sudo nmap 192.168.73.128 -p-
```

# NMAP

## -A

```
bl4ck@bl4ck:~/Desktop/1KasımEğitim$ sudo nmap 192.168.73.128 -A
[sudo] password for bl4ck:

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-31 23:54 +03
Nmap scan report for 192.168.73.128
Host is up (0.00026s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|     Connected to 192.168.73.1
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntul (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
```

OS Detection  
Version Detection  
Scripts  
Traceroute

# NMAP – Ports Range

```
bl4ck@bl4ck:~$ sudo nmap 192.168.73.128 -p 21-45

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-31 17:53 +03
Stats: 0:00:06 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:09 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.73.128
Host is up (0.0014s latency).

PORT      STATE    SERVICE
21/tcp    open     ftp
22/tcp    open     ssh
23/tcp    open     telnet
24/tcp    closed   priv-mail
25/tcp    open     smtp
26/tcp    closed   rsftp
27/tcp    closed   nsw-fe
28/tcp    closed   unknown
29/tcp    closed   msg-icp
30/tcp    closed   unknown
31/tcp    closed   msg-auth
32/tcp    closed   unknown
33/tcp    closed   dsp
34/tcp    closed   unknown
35/tcp    closed   priv-print
36/tcp    closed   unknown
37/tcp    closed   time
38/tcp    closed   rap
39/tcp    closed   rlp
40/tcp    closed   unknown
41/tcp    closed   graphics
42/tcp    closed   nameserver
43/tcp    closed   whois
```

# NMAP – Open Ports Scan

```
bl4ck@bl4ck:~$ sudo nmap 192.168.73.128 -p 21-45 --open

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-31 17:56 +03
Nmap scan report for 192.168.73.128
Host is up (0.00077s latency).
Not shown: 21 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
MAC Address: 00:0C:29:F3:BE:D9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.62 seconds
bl4ck@bl4ck:~$ 
```

# NMAP

```
bl4ck@bl4ck:~$ sudo nmap 192.168.73.128 -p 21-45 --open -sV

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-31 17:59 +03
Nmap scan report for 192.168.73.128
Host is up (0.0011s latency).
Not shown: 21 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp    Postfix smtpd
MAC Address: 00:0C:29:F3:BE:D9 (VMware)
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.38 seconds
bl4ck@bl4ck:~$ █
```

# NMAP - Top ports

```
bl4ck@bl4ck:~$ sudo nmap 192.168.73.128 --top-ports 20
[sudo] password for bl4ck:

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-31 20:06 +03
Nmap scan report for 192.168.73.128
Host is up (0.0011s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
110/tcp   closed pop3
111/tcp   open  rpcbind
135/tcp   closed msrpc
139/tcp   open  netbios-ssn
143/tcp   closed imap
443/tcp   closed https
445/tcp   open  microsoft-ds
993/tcp   closed imaps
995/tcp   closed pop3s
1723/tcp  closed pptp
3306/tcp  open  mysql
3389/tcp  closed ms-wbt-server
5900/tcp  open  vnc
8080/tcp  closed http-proxy
MAC Address: 00:0C:29:F3:BE:D9 (VMware)
```

Nmap done: 1 IP address (1 host up) scanned in 14.68 seconds

# NMAP - IP From Txt

```
bl4ck@bl4ck:~/Desktop/1KasımEğitim$ sudo nmap -iL IP.txt
[sudo] password for bl4ck:

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-31 23:02 +03
Nmap scan report for 192.168.73.128
Host is up (0.00043s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:F3:BE:D9 (VMware)

Nmap done: 6 IP addresses (1 host up) scanned in 14.88 seconds
bl4ck@bl4ck:~/Desktop/1KasımEğitim$ █
```

-iL  
parametresi

# NMAP – Exclude IP

```
bl4ck@bl4ck:~/Desktop/1KasımEğitim$ sudo nmap 192.168.73.0/24 --exclude 192.168.73.100
Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-31 23:16 +03
Nmap scan report for 192.168.73.128
Host is up (0.00027s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:F3:BE:D9 (VMware)

Nmap scan report for 192.168.73.254
```

# NMAP – Exclude Ports

```
bl4ck@bl4ck:~/Desktop/1KasımEğitim$ sudo nmap 192.168.73.128 --exclude-ports 0-5999
Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-31 23:25 +03
WARNING: a TCP ping scan was requested, but after excluding requested TCP ports, none
Nmap scan report for 192.168.73.128
Host is up (0.00085s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
6000/tcp   open  X11
6667/tcp   open  irc
8009/tcp   open  ajp13
8180/tcp   open  unknown
MAC Address: 00:0C:29:F3:BE:D9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.83 seconds
bl4ck@bl4ck:~/Desktop/1KasımEğitim$ █
```

# NMAP – NSE Scripts

/usr/share/nmap/scripts

```
bl4ck@bl4ck:/usr/share/nmap/scripts$ nmap 192.168.73.128 -p 21 --script=ftp-anon.nse
Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-01 11:36 +03
Nmap scan report for 192.168.73.128
Host is up (0.00025s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)

Nmap done: 1 IP address (1 host up) scanned in 13.20 seconds
bl4ck@bl4ck:/usr/share/nmap/scripts$ 
```

# Nessus Vulnerability Scanner Kurulum

```
bl4ck@bl4ck:~/Downloads$ sudo dpkg -i Nessus-6.11.2-debian6_amd64.deb
[sudo] password for bl4ck:
Selecting previously unselected package nessus.
(Reading database ... 495686 files and directories currently installed.)
Preparing to unpack Nessus-6.11.2-debian6_amd64.deb ...
Unpacking nessus (6.11.2) ...
Setting up nessus (6.11.2) ...
Unpacking Nessus Core Components...
nessusd (Nessus) 6.11.2 [build M20102] for Linux
Copyright (C) 1998 - 2017 Tenable Network Security, Inc
```

Processing the Nessus plugins...

```
[########################################]
```

All plugins loaded (1sec)

- You can start Nessus by typing /etc/init.d/nessusd start
- Then go to <https://bl4ck:8834/> to configure your scanner

Processing triggers for systemd (235-2) ...

```
bl4ck@bl4ck:~/Downloads$ sudo apt-get install nessus
```

# Nessus Vulnerability Scanner Servisinin Başlatılması

```
bl4ck@bl4ck:~/Downloads$ sudo service nessusd start
bl4ck@bl4ck:~/Downloads$ sudo service nessusd status
● nessusd.service - LSB: Starts and stops the Nessus
  Loaded: loaded (/etc/init.d/nessusd; generated; vendor preset: disabled)
  Active: active (running) since Tue 2017-10-31 20:21:12 +03; 3s ago
    Docs: man:systemd-sysv-generator(8)
  Process: 23121 ExecStart=/etc/init.d/nessusd start (code=exited, status=0/SUCC
  Tasks: 26 (limit: 4915)
  CGroup: /system.slice/nessusd.service
          └─23123 /opt/nessus/sbin/nessus-service -D -q
              ├─23124 nessusd -q

Oct 31 20:21:12 bl4ck systemd[1]: Starting LSB: Starts and stops the Nessus...
Oct 31 20:21:12 bl4ck systemd[1]: Started LSB: Starts and stops the Nessus.
Oct 31 20:21:13 bl4ck nessusd[23121]: Starting Nessus : .
bl4ck@bl4ck:~/Downloads$ 
```

# Nessus Vulnerability Scanner Kurulum



`https://bl4ck:8834/#/`

| `https://127.0.0.1:8834/#/`

| `https://localhost:8834/#/`



# Nessus Vulnerability Scanner

## Kurulum

### Welcome to Nessus



Thank you for installing Nessus, the industry leader in vulnerability scanning. This application allows you to:

- Run high-speed vulnerability and discovery scans on your network
- Conduct agentless auditing on hosts to confirm they are running up-to-date software
- Perform compliance checks on hosts to verify they are adhering to your security policy
- Schedule scans to launch automatically at the frequency you select
- And much more!

Press continue to perform account setup, register or link this scanner, and download the latest plugins.

Continue

# Nessus Vulnerability Scanner Kurulum

## Account Setup



In order to use this scanner, an administrative account must be created. This user has full control of the scanner—with the ability to create/delete users, stop running scans, and change the scanner configuration.

Username

Password



*NOTE: In addition to scanner administration, this account also has the ability to execute commands on hosts being scanned. As such, access should be limited and treated the same as a system-level "root" (or administrator) user.*

[Continue](#)

[Back](#)

© 2017 Tenable Network Security®

## Kullanıcı Adı ve Parola Belirliyoruz

# Nessus Vulnerability Scanner Kurulum

## Registration



As new vulnerabilities are discovered and released into the public domain, Tenable's research staff creates plugins that allow Nessus to detect their presence. These plugins contain vulnerability information, algorithms to test for the presence of the issue, and a set of remediation actions. [Registering this scanner](#) will grant you access to download these plugins.

Registration

Nessus (Home, Professional or Manager)

Activation Code

Nessus (Home, Professional or Manager)

Link to Tenable.io

Link to Nessus Manager

Continue

Back

Managed by SecurityCenter

Advanced Settings

Offline

© 2017 Tenable Network Security®

## Offline Mod

# Nessus Vulnerability Scanner Kurulum

## Registration

As new vulnerabilities are discovered and released into the public domain, Tenable's research staff creates plugins that allow Nessus to detect their presence. These plugins contain vulnerability information, algorithms to test for the presence of the issue, and a set of remediation actions. [Registering this scanner](#) will grant you access to download these plugins.

Registration      Offline

To create a key, [click here](#) and use the following challenge code:  
**f38a2167542d61387bdc6d3985bcfff26cddb4d7**

Nessus License

true

[Continue](#)    [Back](#)    [Advanced Settings](#)



# Nessus Vulnerability Scanner Kurulum



Cyber Exposure   Products   Services   Company   Partners   Blog

Login

Try/Buy

Nessus® Home allows you to scan your personal home network (up to 16 IP addresses per scanner) with the same high-speed, in-depth assessments and agentless scanning convenience that Nessus subscribers enjoy.

Please note that Nessus Home does not provide access to support, allow you to perform compliance checks or content audits, or allow you to use the Nessus virtual appliance. If you require support and these [additional features](#), please purchase a [Nessus](#) subscription.

**Nessus Home is available for personal use in a home environment only. It is not for use by any commercial organization.**

## Register for an Activation Code

First Name \*

Last Name \*

Email \*

Check to receive updates from Tenable

Register

## Aktivasyon Kodunun Gelmesi İçin Üye Oluyoruz

<https://www.tenable.com/products/nessus-home>

# Nessus Vulnerability Scanner Kurulum



Products Try Buy Partners Support Company

Generate a license for Nessus 6.3 and newer.

To generate a license for an older version of Nessus click [here](#).

Type 'nessuscli fetch --challenge' on your nessusd server and type in the result :

f38a2167542d61387bdc6d3985bcfff26cddb4d7

Enter your activation code :

90EE-2976-E82F-525F-A5FA

Submit

<https://plugins.nessus.org/v2/offline.php>

# Nessus Vulnerability Scanner Kurulum

-----BEGIN TENABLE LICENSE-----

Q1llejlzK0RHk2JBTDmzLzVpc2RnNzk0d0lXMWxDZlhubGVQS3BTZGltWUYx0GFtdk1naVJqeDUw  
MGYwNEVMSkJGN1ZyVzlRT2dCMWNNd1RianJKcjMvQ2FQVytK0hoSkh0Z280S3JSbndoа0RNv3J3  
S002SmJuR1BkZHfqrmtpzWhaUHMnJLcTYxa1cxTVhzQTVSDd3QlI1SkFJREpCakxyVE0zK05H  
NlZPYVQ4UDAxTytEc3h5dWF0UDE0aHEyNHliQ294Y3ZMNjJl0EZFXdZTmZsczdpdERnSDNKS1ly  
QU03cE5KTzhMUU92NGRKZkxwbzFYcmZjazdWSVdNVU52RmZq0VJHRTNveElnaTNKZTFiUXp6N1Vn  
Q2VJcVpPdlh5M1E2bEZTZDhDdHRUcGVmUCtSRlRk0Gx2NlNWQm4vNXpaWDJls1BXWVVETmxKd29w  
UTlpTDYwTnRU0FUvVXhLKzNaenBLdzRGV0prYU1DVWFhS2crU093YzBpZEcd2FIQ3A0S2dsb1E1  
VVYxSwg3SVZIa2hPT0xsL2VlN0xSL1J0WDV0blNHUUJ2c083MFcxWXdrdVpjaiI1Zeg4clVvRm5q  
SE4vdjh0MnVLMmlaN0trNXFTZVVrNkY5bi9I0UFsR21PY09ka3VvTXFna0xzSWpsSWFjUm50c2NW  
dmxQYlRWNgWXg0STBVY3R0c3BrVnJGRnNsN0hhSytHdGQxUGJ0NjNIUXlaM3ErTFo5clpK0Ehd  
ZXU4aS8vQTbV51JM03hudXJHV3BnQ1Z2UHh2QmJramdwczRPRkxkeW9Lekx4dzAzbC9UaDEyT2xs  
aitDckY2RzhJU01vR1JGa3hlcTVGZGFURk450VFmWnp2NDFGZ1VaWnJTTFpiRjMxTnduUXBHUEE9  
DQp7ImFjdG12YXRpb25fY29kZSI6IjkwRUUtMjk3Ni1F0DJGLTUyNUYtQTVGQSIisInVwZGF0ZV9w  
YXNzd29yZCI6IjM2MGM0ZWFlNDE00DViYTM4ZjgyMTdhMDY1Nzc4Zjg0IiwibmFtZSI6Ik5lc3N1  
cyBIb21lIiwidXBkYXRlX3VybCI6Imh0dHBz0i8vcGx1Z2lucy5uZXNzdXMub3JnL3YyL25lc3N1  
cy5waHAiLCJ0eXB1IjoiaG9tZSIisImV4cGlyYXRpb25fZGF0ZSI6MTY2NzE1Mjk5MSwidXBkYXRl  
X2xvZ2luIjoiNWEyMDExMzVjYzQ3ZDU2ZmY40DU10DFhNzUzNGI2YWYiLCJkcm0i0iIzMGY2YTbm  
YmU1ZDYxYTdjNjYyMjM4NDg4NTYwMmU30CJ9

-----END TENABLE LICENSE-----

# Nessus Vulnerability Scanner Kurulum

## Registration

As new vulnerabilities are discovered and released into the public domain, Tenable's research staff creates plugins that allow Nessus to detect their presence. These plugins contain vulnerability information, algorithms to test for the presence of the issue, and a set of remediation actions. [Registering this scanner](#) will grant you access to download these plugins.

Registration      Offline

To create a key, [click here](#) and use the following challenge code:  
**f38a2167542d61387bdc6d3985bcfff26cddb4d7**

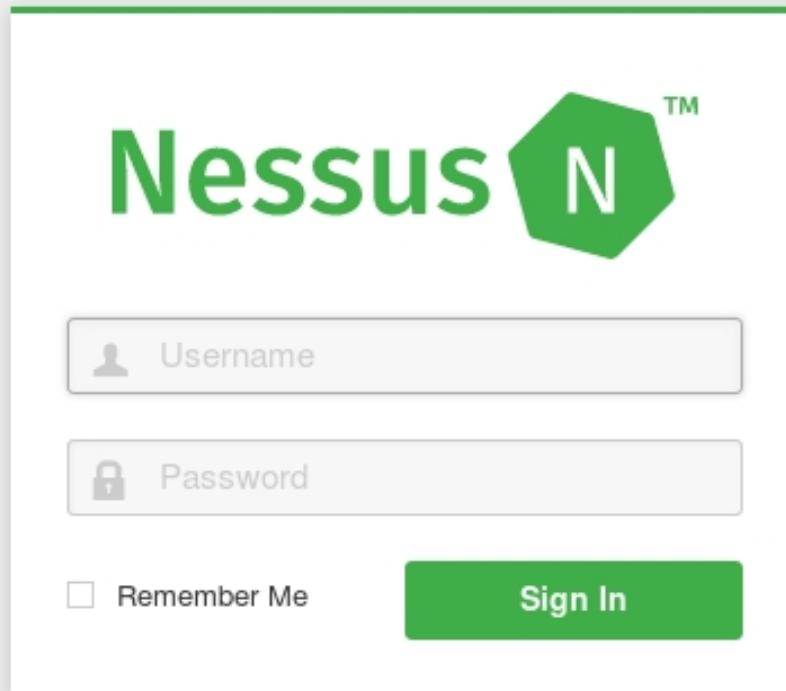
Nessus License

----BEGIN TENABLE LICENSE----  
Q1llejIzK0RHK2JBTDmzLzVpc2RnNzk0d0lXMWxDZIhubGVQS3BTZGltWUYxOGFtdk1naVJqeDUw  
MCVwNEVMSk1CNH7uVgIDT2HOMM/NKNDIion1KcIMvO9EOVutk

[Continue](#) [Back](#) [Advanced Settings](#)

# Nessus Vulnerability Scanner Kurulum



Kurulum Tamamlandı

# Nessus Vulnerability Scanner

The screenshot shows the Nessus web interface with a dark header bar. The header includes the 'Nessus' logo, 'Scans' and 'Settings' links, a notification bell icon, and an 'admin' user profile.

The main area is titled 'My Scans'. It features a search bar with 'Search Scans' and a magnifying glass icon, followed by a message '1 Scan'. Below this is a table with the following data:

<input type="checkbox"/> Name	Schedule	Last Modified
<input type="checkbox"/> metasploitable2	On Demand	✓ Today at 9:43 PM

On the left side, there is a sidebar with sections for 'FOLDERS' (My Scans, Egitim, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Scanners). Navigation arrows are located at the bottom left and right of the main content area.

# Nessus Vulnerability Scanner Servisinin Durdurulması

```
bl4ck@bl4ck:~/Downloads$ sudo service nessusd stop
bl4ck@bl4ck:~/Downloads$ sudo service nessusd status
● nessusd.service - LSB: Starts and stops the Nessus
  Loaded: loaded (/etc/init.d/nessusd; generated; vendor preset: disabled)
  Active: inactive (dead)
    Docs: man:systemd-sysv-generator(8)

Oct 31 20:21:12 bl4ck systemd[1]: Starting LSB: Starts and stops the Nessus...
Oct 31 20:21:12 bl4ck systemd[1]: Started LSB: Starts and stops the Nessus.
Oct 31 20:21:13 bl4ck nessusd[23121]: Starting Nessus : .
Oct 31 20:26:57 bl4ck systemd[1]: Stopping LSB: Starts and stops the Nessus...
Oct 31 20:26:57 bl4ck nessusd[24303]: Shutting down Nessus : .
Oct 31 20:26:57 bl4ck systemd[1]: Stopped LSB: Starts and stops the Nessus.
bl4ck@bl4ck:~/Downloads$ █
```

# OpenVAS - Open Vulnerability Assessment System Kurulum

```
bl4ck@bl4ck:~$ sudo apt-get install openvas
[sudo] password for bl4ck:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  doc-base fonts-texgyre greenbone-security-assistant greenbone-security-assistant-common icc-profiles icc
  libuuid-perl libyaml-tiny-perl openvas-cli openvas-manager openvas-manager-common openvas-scanner previe
  tex-gyre texlive-fonts-recommended texlive-fonts-recommended-doc texlive-latex-extra texlive-latex-extra
  texlive-latex-recommended-doc texlive-pictures texlive-pictures-doc texlive-plain-generic tipa
Suggested packages:
  openvas-client pnscan strobe ruby-redis libfile-which-perl libspreadsheet-parseexcel-perl texlive-pstric
  | libtcltk-ruby
The following NEW packages will be installed:
  doc-base fonts-texgyre greenbone-security-assistant greenbone-security-assistant-common icc-profiles icc
  libuuid-perl libyaml-tiny-perl openvas openvas-cli openvas-manager openvas-manager-common openvas-scanne
  redis-tools tex-gyre texlive-fonts-recommended texlive-fonts-recommended-doc texlive-latex-extra texlive
  texlive-latex-recommended-doc texlive-pictures texlive-pictures-doc texlive-plain-generic tipa
0 upgraded, 29 newly installed, 0 to remove and 4 not upgraded.
Need to get 691 MB of archives.
After this operation, 1,045 MB of additional disk space will be used.
```

Uzun Sürer

# OpenVAS - Open Vulnerability Assessment System Kurulum

```
bl4ck@bl4ck:~$ sudo openvas-setup
[sudo] password for bl4ck:
ERROR: Directory for keys (/var/lib/openvas/private/CA) not found!
ERROR: Directory for certificates (/var/lib/openvas/CA) not found!
ERROR: CA key not found in /var/lib/openvas/private/CA/cakey.pem
ERROR: CA certificate not found in /var/lib/openvas/CA/cacert.pem
ERROR: CA certificate failed verification, see /tmp/tmp.5zxk98Hyj0/openvas-manage-certs.log for details. Aborting.

ERROR: Your OpenVAS certificate infrastructure did NOT pass validation.
      See messages above for details.
Generated private key in /tmp/tmp.mz7RbKkIT6/cakey.pem.
Generated self signed certificate in /tmp/tmp.mz7RbKkIT6/cacert.pem.
Installed private key to /var/lib/openvas/private/CA/cakey.pem.
Installed certificate to /var/lib/openvas/CA/cacert.pem.
Generated private key in /tmp/tmp.mz7RbKkIT6/serverkey.pem.
Generated certificate request in /tmp/tmp.mz7RbKkIT6/serverrequest.pem.
Signed certificate request in /tmp/tmp.mz7RbKkIT6/serverrequest.pem with CA certificate in /var/lib/openvas/CA/cacert..
tmp/tmp.mz7RbKkIT6/servercert.pem
Installed private key to /var/lib/openvas/private/CA/serverkey.pem.
Installed certificate to /var/lib/openvas/CA/servercert.pem.
Generated private key in /tmp/tmp.mz7RbKkIT6/clientkey.pem.
Generated certificate request in /tmp/tmp.mz7RbKkIT6/clientrequest.pem.
Signed certificate request in /tmp/tmp.mz7RbKkIT6/clientrequest.pem with CA certificate in /var/lib/openvas/CA/cacert..
tmp/tmp.mz7RbKkIT6/clientcert.pem
Installed private key to /var/lib/openvas/private/CA/clientkey.pem.
Installed certificate to /var/lib/openvas/CA/clientcert.pem.
Removing temporary directory /tmp/tmp.mz7RbKkIT6.
--2017-10-31 23:11:18-- http://dl.greenbone.net/community-nvt-feed-current.tar.bz2
Resolving dl.greenbone.net (dl.greenbone.net)... 89.146.224.58, 2a01:130:2000:127::d1
Connecting to dl.greenbone.net (dl.greenbone.net)|89.146.224.58|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 35074167 (33M) [application/octet-stream]
Saving to: '/tmp/greenbone-nvt-sync.6abeS6oVav/openvas-feed-2017-10-31-14925.tar.bz2'
```

# OpenVAS - Open Vulnerability Assessment System Kurulum

```
shalsums
      2,002 100%    3.04kB/s    0:00:00 (xfr#33, to-chk=4/38)
sha256sums
      2,818 100%    4.28kB/s    0:00:00 (xfr#34, to-chk=3/38)
sha256sums.asc
          181 100%    0.27kB/s    0:00:00 (xfr#35, to-chk=2/38)
timestamp
           13 100%    0.02kB/s    0:00:00 (xfr#36, to-chk=1/38)
timestamp.asc
      181 100%    0.27kB/s    0:00:00 (xfr#37, to-chk=0/38)

sent 757 bytes  received 41,395,925 bytes  399,967.94 bytes/sec
total size is 41,383,350  speedup is 1.00
/usr/sbin/openvasmd
User created with password 'd360b666-4d28-42c3-a1b8-438e1d351b65'.
```

# OpenVAS - Open Vulnerability Assessment System

```
bl4ck@bl4ck:~$ sudo openvas-start
Starting OpenVas Services
```

```
bl4ck@bl4ck:~$ sudo service openvas-scanner status
● openvas-scanner.service - Open Vulnerability Assessment System Scanner Daemon
  Loaded: loaded (/lib/systemd/system/openvas-scanner.service; disabled; vendor preset: disabled)
  Active: active (running) since Wed 2017-11-01 00:08:01 +03; 31min ago
    Docs: man:openvassd(8)
          http://www.openvas.org/
   Process: 18100 ExecStart=/usr/sbin/openvassd --unix-socket=/var/run/openvassd.sock (code=exited, status=0/SUCCESS)
 Main PID: 18101 (openvassd)
    Tasks: 1 (limit: 4915)
   CGroup: /system.slice/openvas-scanner.service
           └─18101 openvassd: Waiting for incoming connections

Nov 01 00:08:00 bl4ck systemd[1]: Starting Open Vulnerability Assessment System Scanner Daemon...
Nov 01 00:08:01 bl4ck systemd[1]: Started Open Vulnerability Assessment System Scanner Daemon.
```

# OpenVAS - Open Vulnerability Assessment System



<https://127.0.0.1:9392>

<https://localhost:9392>



# OpenVAS - Open Vulnerability Assessment System

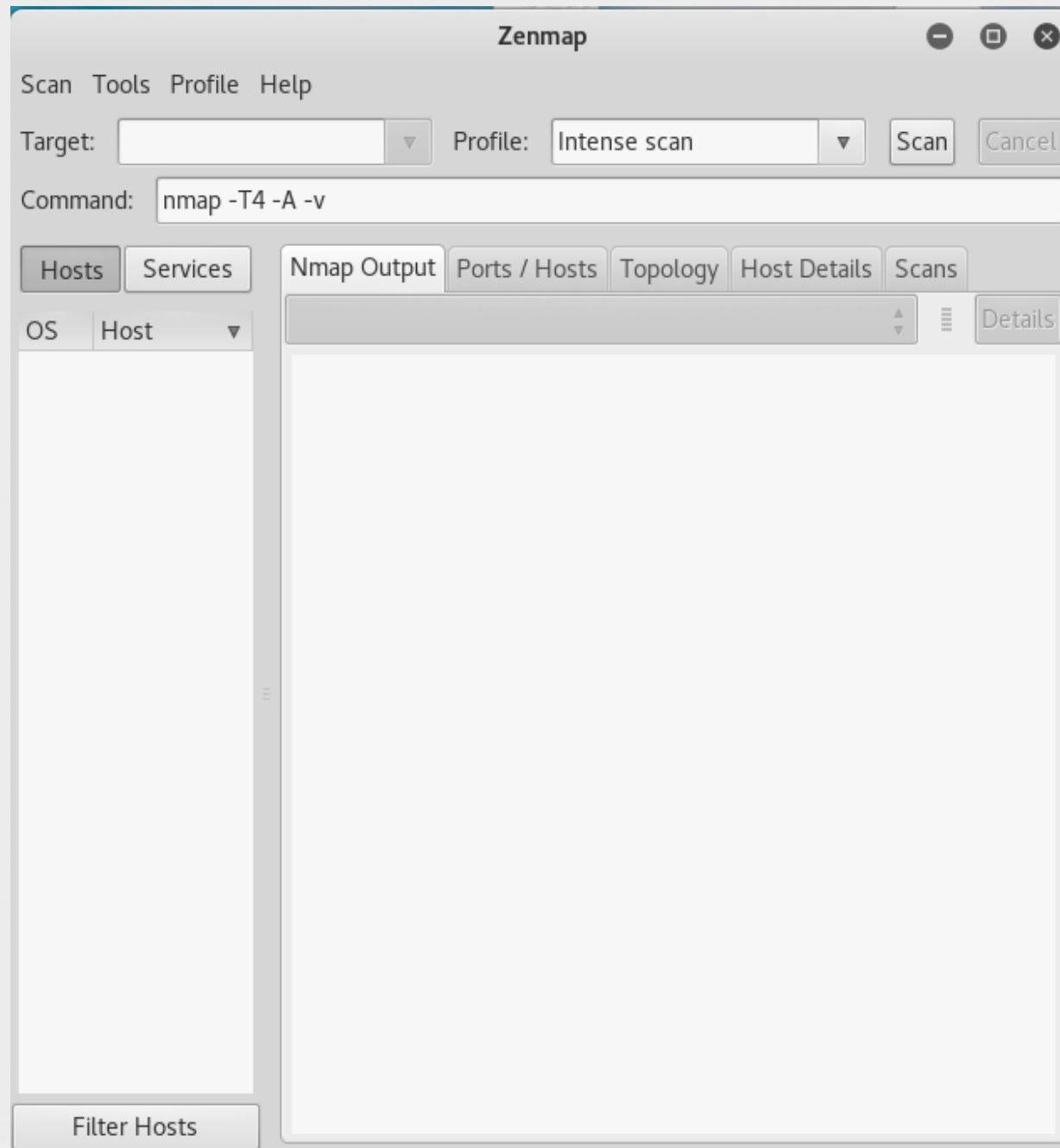


# OpenVAS - Open Vulnerability Assessment System



Sistem tarafından oluşturulan ilk parola ile giriş yapılır

# Zenmap



# Zenmap

Zenmap

Scan Tools Profile Help

Target: 192.168.73.128 Profile: Quick scan Scan Cancel

Command: nmap -T4 -F 192.168.73.128

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

192.168.73.128

nmap -T4 -F 192.168.73.128

Host is up (0.003/s latency).  
Not shown: 82 closed ports

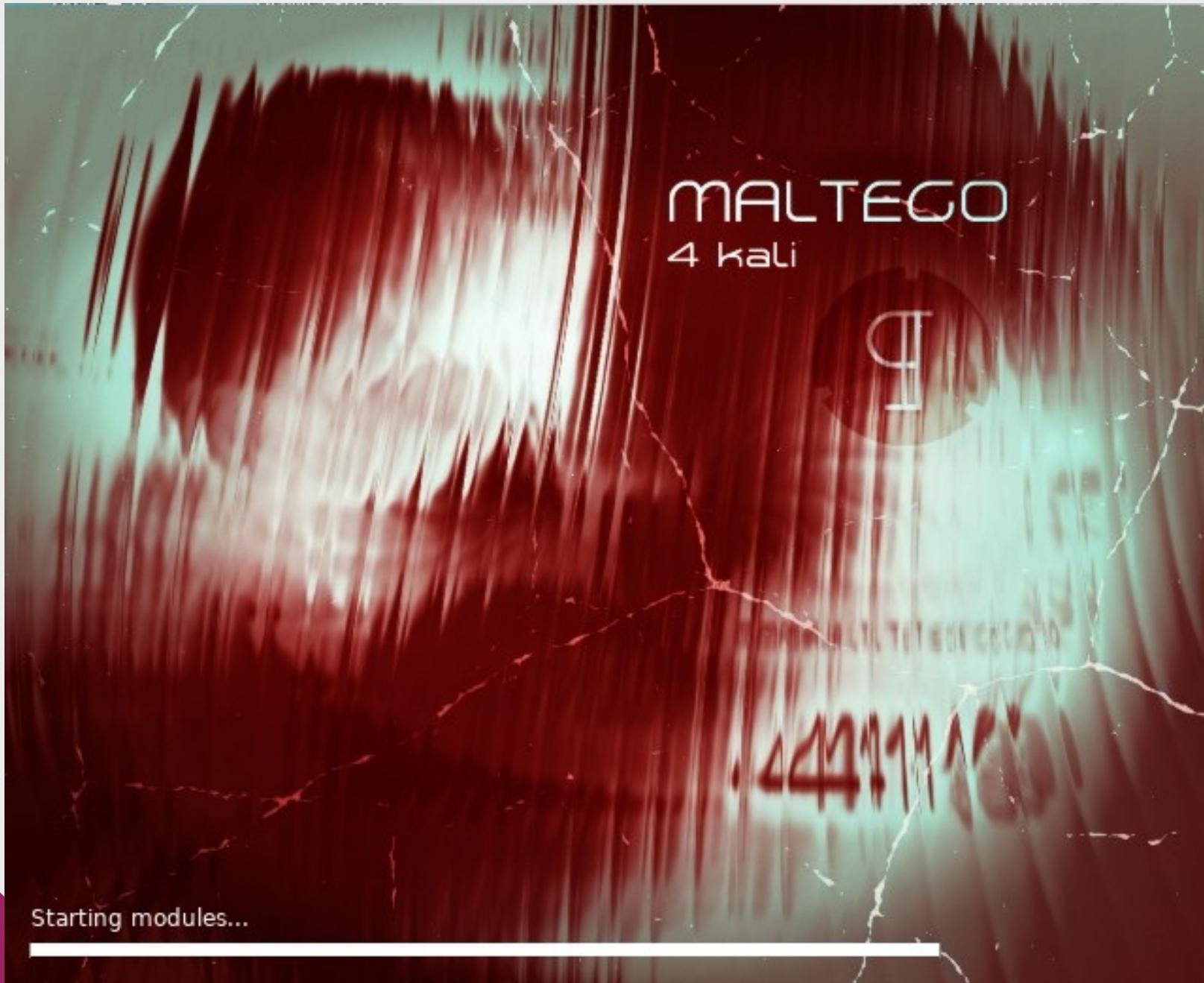
PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
53/tcp	open	domain
80/tcp	open	http
111/tcp	open	rpcbind
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
513/tcp	open	login
514/tcp	open	shell
2049/tcp	open	nfs
2121/tcp	open	ccproxy-ftp
3306/tcp	open	mysql
5432/tcp	open	postgresql
5900/tcp	open	vnc
6000/tcp	open	X11
8009/tcp	open	ajp13

MAC Address: 00:0C:29:F3:BE:D9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.92 seconds

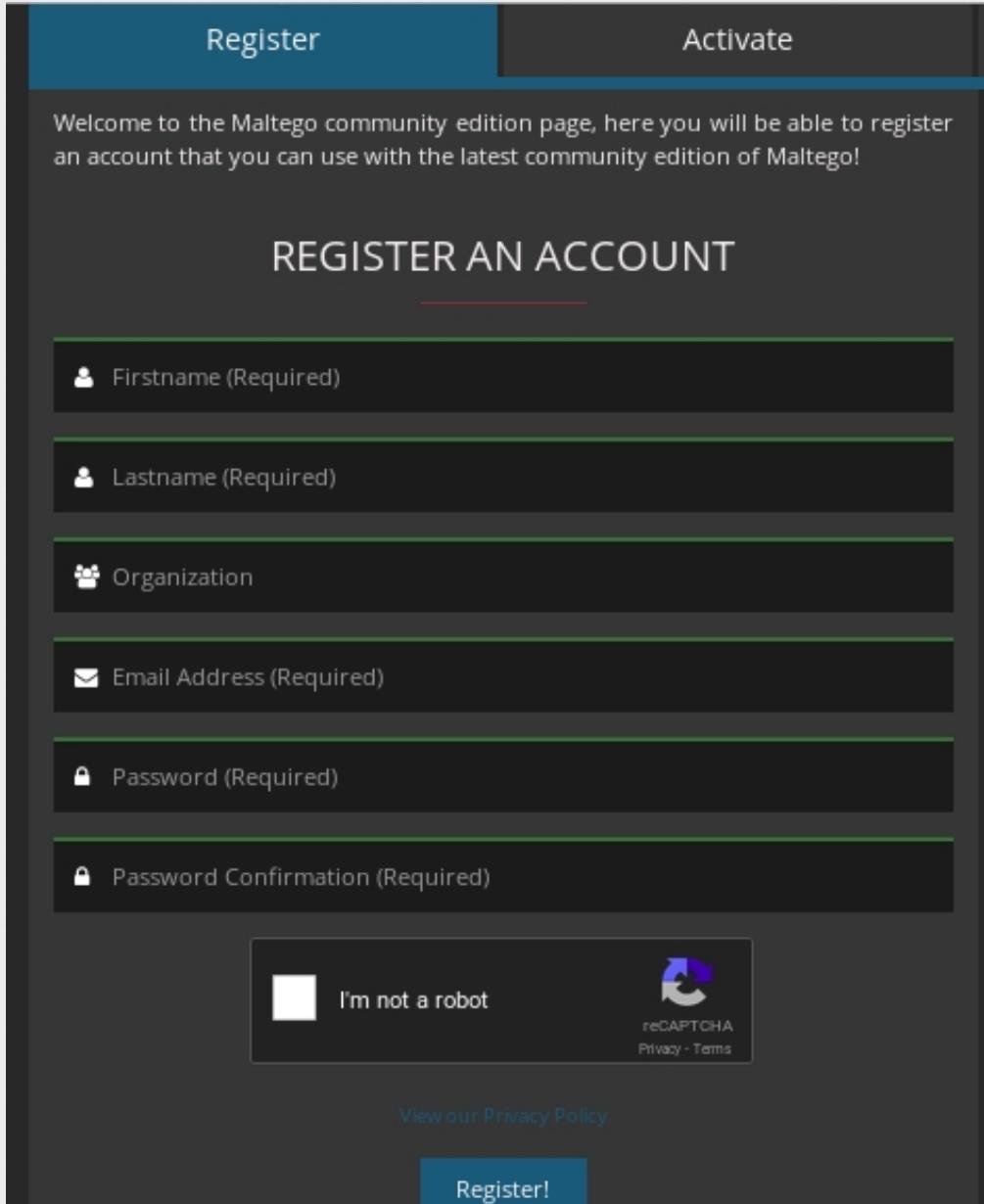
Filter Hosts

# Maltego



# Maltego

<https://www.paterva.com/web7/community/community.php>



The image shows a registration form for the Maltego community edition. The top navigation bar has two tabs: "Register" (highlighted in blue) and "Activate". A welcome message states: "Welcome to the Maltego community edition page, here you will be able to register an account that you can use with the latest community edition of Maltego!". The main title "REGISTER AN ACCOUNT" is centered above six input fields. Each field is preceded by a small icon: a person for Firstname, a person for Lastname, a group for Organization, an envelope for Email Address, a lock for Password, and a lock for Password Confirmation. Below the input fields is a reCAPTCHA verification box containing a checkbox labeled "I'm not a robot" and the reCAPTCHA logo. At the bottom, there is a link to "View our Privacy Policy" and a prominent blue "Register!" button.

Welcome to the Maltego community edition page, here you will be able to register an account that you can use with the latest community edition of Maltego!

## REGISTER AN ACCOUNT

Firstname (Required)

Lastname (Required)

Organization

Email Address (Required)

Password (Required)

Password Confirmation (Required)

I'm not a robot  reCAPTCHA  
Privacy - Terms

[View our Privacy Policy](#)

[Register!](#)

# Maltego

## ACTIVATE YOUR ACCOUNT

**Account successfully activated! You may now login into your Maltego community edition!**

Email Address (Required)

Activation Code (Required)

I'm not a robot   
reCAPTCHA  
Privacy - Terms

**Activate!**