



# Derinlemesine Nmap Kullanımı

12/02/2020

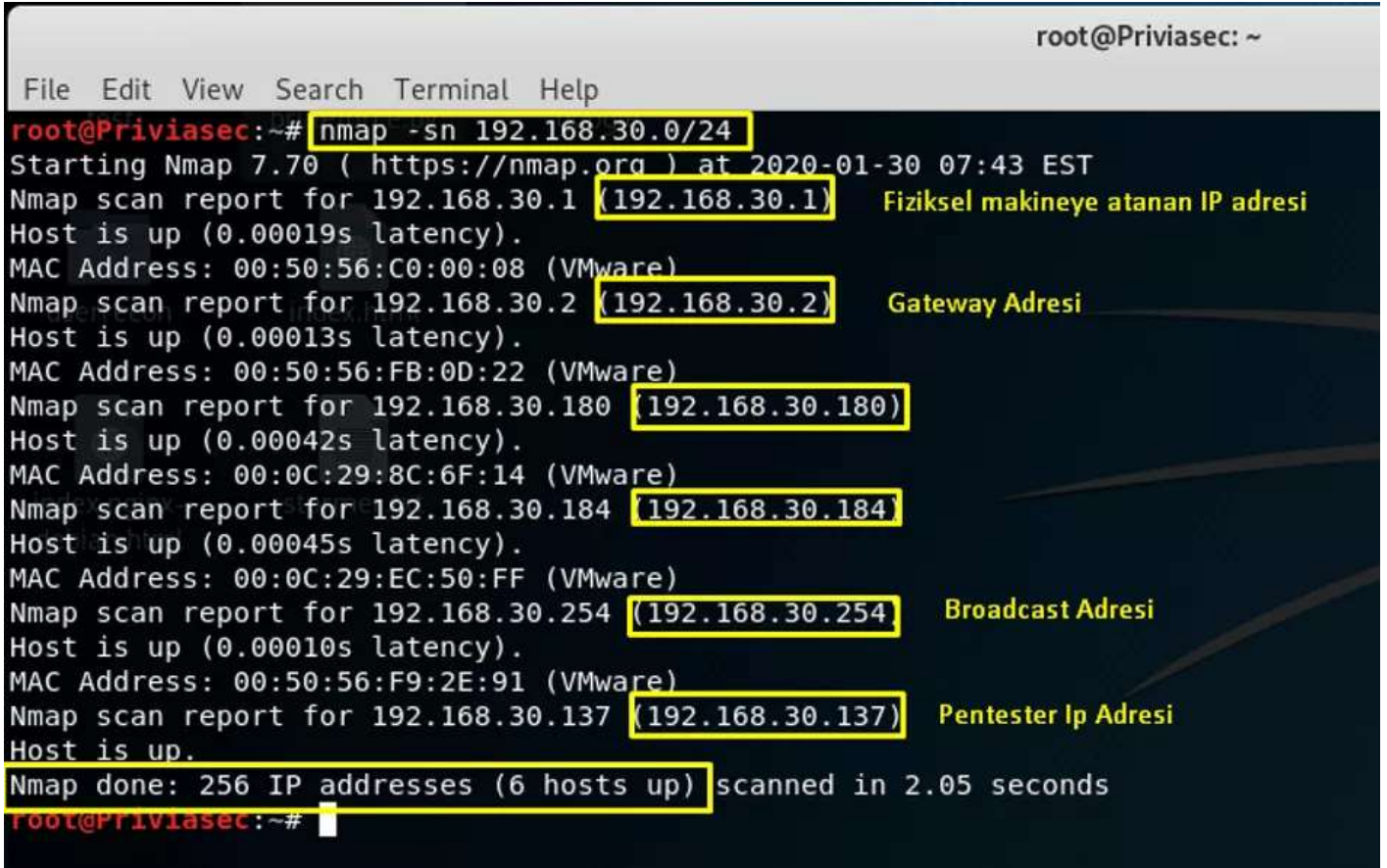


Nmap, günümüzdeki en gelişmiş ağ tarama araçlarının başında gelir. Nmap, ağda bulunan cihazların IP adreslerini, cihaz bilgisini, açık portlarını, işletim sistemini, açık portlarda çalışan servisleri ve cihazlarda bulunan güvenlik açıklarını tespit etmek için kullanılır.

Herhangi bir kurum veya kuruluşa yönelik yapılan güvenlik testlerinde, sızma testi aşamalarından bilgi toplama, tarama ve listeleme aşamaları **Nmap** aracı ile yapılabilir. Öncelikle hedef ağ üzerinde bilgi toplama aşamasını gerçekleştirmek için hedef ağ taranır ve hedef ağ üzerinde çalışan cihazlar

hakkında bilgi elde edilir. Çalışan cihazların IP adresleri, Hostname bilgileri bu bilgiler arasında yer alır.

Örnek **192.168.30.0/24 CIDR** bilgisine sahip bir ağ üzerinde, Nmap aracı ile sızma testinin yaşam döngüsünde bulunan bilgi toplama, tarama ve listeleme aşamaları gerçekleştirilebilir.



```
root@Priviassec: ~  
File Edit View Search Terminal Help  
root@Priviassec:~# nmap -sn 192.168.30.0/24  
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-30 07:43 EST  
Nmap scan report for 192.168.30.1 (192.168.30.1) Fiziksel makineye atanan IP adresi  
Host is up (0.00019s latency).  
MAC Address: 00:50:56:C0:00:08 (VMware)  
Nmap scan report for 192.168.30.2 (192.168.30.2) Gateway Adresi  
Host is up (0.00013s latency).  
MAC Address: 00:50:56:FB:0D:22 (VMware)  
Nmap scan report for 192.168.30.180 (192.168.30.180)  
Host is up (0.00042s latency).  
MAC Address: 00:0C:29:8C:6F:14 (VMware)  
Nmap scan report for 192.168.30.184 (192.168.30.184)  
Host is up (0.00045s latency).  
MAC Address: 00:0C:29:EC:50:FF (VMware)  
Nmap scan report for 192.168.30.254 (192.168.30.254) Broadcast Adresi  
Host is up (0.00010s latency).  
MAC Address: 00:50:56:F9:2E:91 (VMware)  
Nmap scan report for 192.168.30.137 (192.168.30.137) Pentester Ip Adresi  
Host is up.  
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.05 seconds  
root@Priviassec:~#
```

Resim 1

Resim 1'de, 192.168.30.0/24 IP aralığında hangi makinelerin açık olduğu tespit edildi. **-sn** parametresi, hedef makinelerle herhangi bir port taraması yapmadan, makinelerin açık olup olmadığını kontrol etmek için kullanılır. Yapılan taramada 192.168.30.1 IP adresli fiziksel makine dışında 5 tane IP adresine sahip sistemin açık olduğu tespit edildi. 192.168.30.2 Gateway IP adresi, 192.168.30.254 Broadcast IP adresi ve 192.168.30.137 ise taramayı gerçekleştiren IP adresidir. 192.168.30.180 ve 192.168.30.184 IP adresleri açık

olarak tespit edilen hedef makinelerdir. Makineler ARP Ping Scan Taraması sonucunda tespit edilmiştir. Bazı güvenlik duvarları, Ping taramasını engeller. Ping taramasını engelleyen güvenlik duvarlarını atlatmak için **-Pn** parametresi kullanılabilir.

```
root@Priviasec:~# nmap -A -p- 192.168.30.180 192.168.30.184
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-30 08:35 EST
Nmap scan report for 192.168.30.180 (192.168.30.180)
Host is up (0.00040s latency).
Not shown: 65532 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      Microsoft IIS httpd 10.0
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: IIS Windows Server
2121/tcp  open  ftp       Microsoft ftpd
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ 01-06-20 12:32AM      3716 ab.aspx
|_ 12-24-19 02:57AM      <DIR>  aspnet_client
|_ 12-24-19 02:56AM      703 iisstart.htm
|_ 12-24-19 02:56AM      99710 iisstart.png
|_ 12-24-19 04:31AM      281 web.config
|_ ftp-syst:
|_ SYST: Windows NT
5985/tcp  open  http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
MAC Address: 00:0C:29:8C:6F:14 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2016
OS CPE: cpe:/o:microsoft:windows_server_2016
OS details: Microsoft Windows Server 2016
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT      ADDRESS
1 0.40 ms 192.168.30.180 (192.168.30.180)
```

Resim 2

Resim2'de 192.168.30.180 ve 192.168.30.184 IP adreslerine yönelik agresif modda (-A) ve full port taraması (-p-) yapılmıştır. 192.168.30.180 IP adresli makinede 80, 2121, 5985 numaralı portlar ve bu portlar üzerinde çalışan servisler tespit edilmiştir. 2121. portta çalışan FTP servisine yönelik **ftp-anon** NSE script'i kullanılarak Anonymous kullanıcısının sistemde aktif olduğu tespit edilmiştir. Makinenin işletim sistemi Microsoft Windows Server 2016 olarak işaretlenmiştir. 192.168.30.184 IP adresli makine Resim3'te gösterilmektedir.

```
Nmap scan report for 192.168.30.184 [192.168.30.184]
Host is up (0.00037s latency).
Not shown: 65533 filtered ports
PORT      STATE SERVICE          VERSION
445/tcp    open  microsoft-ds     Windows Server 2012 R2 Standard Evaluation 9600 microsoft-ds
5985/tcp    open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
MAC Address: 00:0C:29:EC:50:FF (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2012
OS CPE: cpe:/o:microsoft:windows_server_2012:r2
OS details: Microsoft Windows Server 2012 or Windows Server 2012 R2
Network Distance: 1 hop
Service Info: OSs: Windows Server 2008 R2 - 2012, Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 3h59m59s, deviation: 5h39m24s, median: 0s
|_nbstat: NetBIOS_name: WIN-0C1MP71QVGS, NetBIOS_user: <unknown>, NetBIOS_MAC: 00-0c-29-ec-50-ff (VMware)
|_smb-os-discovery:
|   OS: Windows Server 2012 R2 Standard Evaluation 9600 (Windows Server 2012 R2 Standard Evaluation 6.3)
|   OS CPE: cpe:/o:microsoft:windows_server_2012::-
|   Computer name: WIN-0C1MP71QVGS
|   NetBIOS computer name: WIN-0C1MP71QVGS\x00
|   Workgroup: WORKGROUP\x00
|   System time: 2020-01-30T05:38:16-08:00
|_smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|   message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
```

Resim 3

Resim3'te 192.168.30.184 IP adresine yapılan tarama sonucunda 445 ve 5985 numaraları portların açık olduğu tespit edilmiştir. 445. portta çalışan microsoft-ds servisinin versiyon bilgisinde işletim sistemi bilgisi **“Microsoft Server 2012 R2 Evaluation 9600”** olarak tespit edilmiştir. Ayrıca agresif modda tarama yapıldığı için 445 numaralı portta çalışan SMB servisine yönelik bazı NSE script'leri kullanılmıştır. **smb-os-discovery** script'inin ürettiği çıktı içerisinde işletim sistemi bilgisi, bilgisayar adı, sistem zamanı bilgisi tespit edilmiştir. Smb-security-mode NSE script'i kullanılarak guest kullanıcısının hedef sistemde aktif olduğu belirtilmiştir. Sonuç olarak sisteme yönelik tarama ve bilgi toplama işlemleri Nmap aracı ile gerçekleştirilmiştir.

Bilgi toplama ve tarama işlemleri yapıldıktan sonra açık portlarda zafiyet olup olmadığını kontrol etmek için Nmap içerisinde bulunan script'ler kullanılır. Hedef sistemde zafiyet olup olmadığını kontrol eden bu script'ler **vuln**



kategorisinde yer almaktadır. Resim4'te hedef sistemlere yönelik güvenlik açığı tespiti yapılmıştır.

```
root@Priviassec:~# nmap -p 80,445,2121,5985 --script=vuln,auth 192.168.30.180 192.168.30.184
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-30 08:45 EST
Nmap scan report for 192.168.30.180 (192.168.30.180)
Host is up (0.00026s latency).

PORT      STATE      SERVICE
80/tcp    open      http
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
445/tcp    filtered  microsoft-ds
2121/tcp   open      ccproxy-ftp
5985/tcp   open      wsman
MAC Address: 00:0C:29:8C:6F:14 (VMware)

Nmap scan report for 192.168.30.184 (192.168.30.184)
Host is up (0.00040s latency).

PORT      STATE      SERVICE
80/tcp    filtered  http
445/tcp    open      microsoft-ds
2121/tcp   filtered  ccproxy-ftp
5985/tcp   open      wsman
MAC Address: 00:0C:29:EC:50:FF (VMware)

Host script results:
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
smb-vuln-ms17-010:
  VULNERABLE:
  Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
  State: VULNERABLE
  IDs: CVE:CVE-2017-0143
  Risk factor: HIGH
  A critical remote code execution vulnerability exists in Microsoft SMBv1
  servers (ms17-010).

  Disclosure date: 2017-03-14
  References:
  https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
  https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_ smb-vuln-regsvcs-dos: ERROR: Script execution failed (use -d to debug)

Nmap done: 2 IP addresses (2 hosts up) scanned in 144.19 seconds
root@Priviassec:~#
```

Resim 4

Resim 4'te 192.168.30.180 ve 192.168.30.184 IP adresine sahip makinelerin 80, 445, 2121 ve 5985 numaralı portlarına yönelik tarama yapıldı. Yapılan taramada vuln ve auth kategorisindeki script'ler kullanıldı. Vuln script'leri zafiyet tespiti için, auth script'leri ise kimlik doğrulama işlemleri için kullanıldı.

Resim 4'te 192.168.30.180 IP adresinin 80. portunda HTTP servisi çalıştığı için http-csrf, http-dombased-xss, http-stored-xss script'leri kullanıldı. 192.168.30.184 IP adresli makinenin 445. portuna, smb-vuln-ms10-054, smb-vuln-ms10-061, smb-vuln-ms17-010 ve smb-vuln-regsvcs-dos script'leri kullanıldı. Vuln script kategorisinde olan smb-vuln-ms17-010 script'i, hedef sistemde MS17-010 olarak adlandırılan uzaktan kod çalıştırma zafiyetini tespit eder. Oluşan script çıktısı içerisinde **VULNERABLE** sözcüğünün olması makinenin zafiyetli olduğunu gösterir.

Zafiyet tespitinde, -script parametresine, sadece script'lerin kategorileri değil, script'lerin isimleri ve uzantıları da atanabilir. Resim5'te, 192.168.30.184 IP adresli makinenin 445. portuna yönelik zafiyet tespiti yapılmıştır.

```
root@Priviassec: ~
File Edit View Search Terminal Help
root@Priviassec:~# nmap -p 445 --script=smb-vuln-* 192.168.30.184
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-31 07:42 EST
Nmap scan report for 192.168.30.184 (192.168.30.184)
Host is up (0.00029s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:EC:50:FF (VMware)

Host script results:
| smb-vuln-ms10-054: false
| smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|   State: VULNERABLE
|   IDs: CVE:CVE-2017-0143
|   Risk factor: HIGH
|   A critical remote code execution vulnerability exists in Microsoft SMBv1
|   servers (ms17-010).
|
|   Disclosure date: 2017-03-14
|   References:
|   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|   https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
| smb-vuln-regsvcs-dos: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 5.68 seconds
root@Priviassec:~#
```

Resim 5

Resim5'te **smb-vuln-\*** değerindeki yıldız (\*) işareti, **smb-vuln-** sözcüğü ile başlayıp farklı sözcükle biten bütün script'lerin kullanılmasını sağlar. Aynı şekilde farklı portlara yönelik taramalarda script'lerin kullanımı özelleştirilebilir. Örneğin, "**nmap -p80 --script=http-\* 192.168.30.180**" komutu kullanılabilir.

Ek olarak, hedef sistemde Windows güvenlik duvarının aktif veya pasif olduğu durumlarda, Nmap aracının üretmiş olduğu çıktıların nasıl olduğunu bilmek gerekir. Resim6'da, Nmap aracı ile gerçekleştirilen bir taramada güvenlik duvarının aktif ve pasif olduğu durumlardaki çıktısı gösterilmektedir.

```
File Edit View Search Terminal Help
root@Priviassec:~# nmap 192.168.30.184
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-03 03:41 EST
Nmap scan report for 192.168.30.184 (192.168.30.184)
Host is up (0.00040s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
445/tcp    open  microsoft-ds
MAC Address: 00:0C:29:EC:50:FF (VMware)
Nmap done: 1 IP address (1 host up) scanned in 5.09 seconds
root@Priviassec:~# nmap 192.168.30.184
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-03 03:42 EST
Nmap scan report for 192.168.30.184 (192.168.30.184)
Host is up (0.00047s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
49158/tcp  open  unknown
MAC Address: 00:0C:29:EC:50:FF (VMware)
Nmap done: 1 IP address (1 host up) scanned in 4.12 seconds
root@Priviassec:~#
```

Firewall Enable

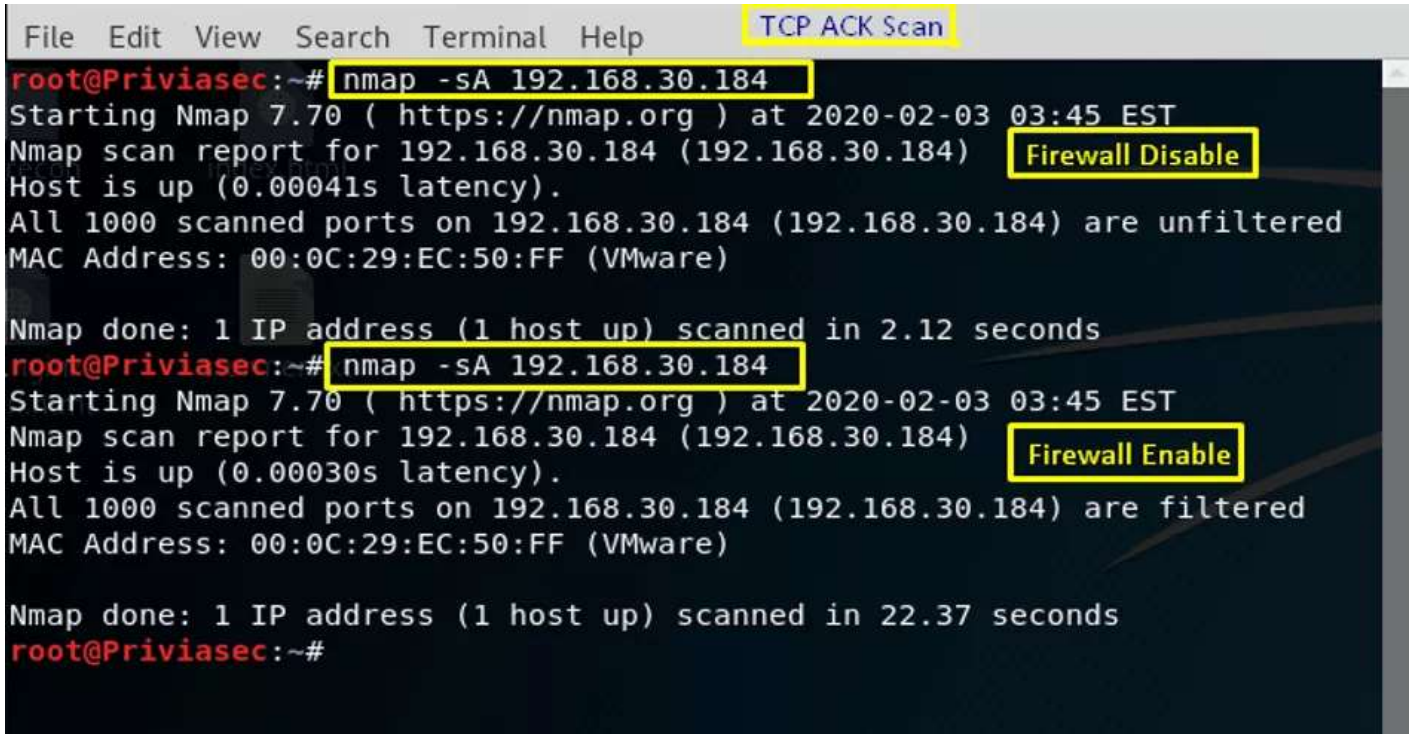
Firewall Disable



## Resim 6

Resim6'da **"nmap 192.168.30.184"** komutu kullanılarak yapılan varsayılan taramada, Windows güvenlik duvarı aktif iken, 445. port açık olarak tespit edilmiştir. 445. portun açık olarak tespit edilmesinin sebebi, güvenlik duvarında bulunan Inbound kurallarında 445. port üzerindeki trafiğe izin veren bir kuralın aktif edilmesidir. İkinci Nmap taramasında ise **445, 139, ve 135** numaralı portların açık olduğu tespit edilmiştir. Bu iki örnekle Windows güvenlik duvarının aktif ve pasif olduğu durumlarındaki farklılıklar görülebilir. Resim7'de ise, güvenlik duvarlarını atlatma tekniklerinden biri olan TCP ACK Scan yapılmıştır. Resim6'da **"nmap 192.168.30.184"** komutu kullanılarak yapılan varsayılan taramada, Windows güvenlik duvarı aktif iken, 445. port açık olarak tespit edilmiştir. 445. portun açık olarak tespit edilmesinin sebebi, güvenlik duvarında bulunan Inbound kurallarında 445. port üzerindeki trafiğe izin veren bir kuralın aktif edilmesidir. İkinci Nmap taramasında ise 445, 139, ve 135 numaralı portların açık olduğu tespit edilmiştir. Bu iki örnekle Windows güvenlik duvarının aktif ve pasif olduğu durumlarındaki farklılıklar görülebilir. Resim7'de ise, güvenlik duvarlarını atlatma tekniklerinden biri olan TCP ACK Scan yapılmıştır.





```
File Edit View Search Terminal Help TCP ACK Scan
root@Priviassec:~# nmap -sA 192.168.30.184
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-03 03:45 EST
Nmap scan report for 192.168.30.184 (192.168.30.184) Firewall Disable
Host is up (0.00041s latency).
All 1000 scanned ports on 192.168.30.184 (192.168.30.184) are unfiltered
MAC Address: 00:0C:29:EC:50:FF (VMware)

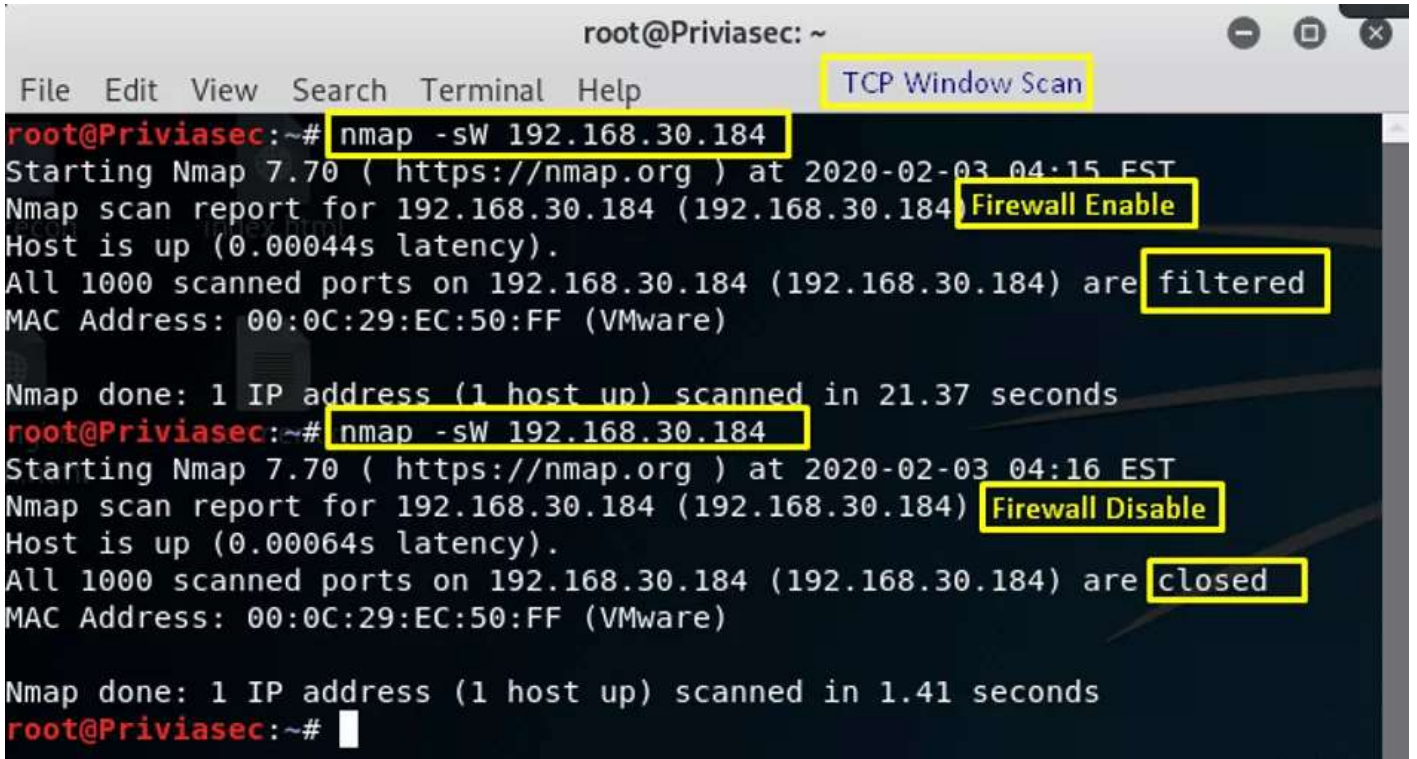
Nmap done: 1 IP address (1 host up) scanned in 2.12 seconds
root@Priviassec:~# nmap -sA 192.168.30.184
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-03 03:45 EST
Nmap scan report for 192.168.30.184 (192.168.30.184) Firewall Enable
Host is up (0.00030s latency).
All 1000 scanned ports on 192.168.30.184 (192.168.30.184) are filtered
MAC Address: 00:0C:29:EC:50:FF (VMware)

Nmap done: 1 IP address (1 host up) scanned in 22.37 seconds
root@Priviassec:~#
```

Resim 7

Resim 7’de `-sA` parametresi kullanılarak TCP ACK Scan yapılmıştır. Resim 7’de güvenlik duvarının pasif olduğu durumda varsayılan olarak belirtilen 1000 port **unfiltered** olarak işaretlenir. Güvenlik duvarının aktif olduğu durumda ise, belirtilen 1000 port **filtered** olarak işaretlenir.

TCP ACK Scan dışında, güvenlik duvarlarını atlatmak için kullanılan tekniklerden bir diğeri ise TCP Window Scan’dır. Resim8’de TCP Window Scan gösterilmektedir.



```
root@Priviasec: ~  
File Edit View Search Terminal Help TCP Window Scan  
root@Priviasec:~# nmap -sW 192.168.30.184  
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-03 04:15 EST  
Nmap scan report for 192.168.30.184 (192.168.30.184) Firewall Enable  
Host is up (0.00044s latency).  
All 1000 scanned ports on 192.168.30.184 (192.168.30.184) are filtered  
MAC Address: 00:0C:29:EC:50:FF (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 21.37 seconds  
root@Priviasec:~# nmap -sW 192.168.30.184  
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-03 04:16 EST  
Nmap scan report for 192.168.30.184 (192.168.30.184) Firewall Disable  
Host is up (0.00064s latency).  
All 1000 scanned ports on 192.168.30.184 (192.168.30.184) are closed  
MAC Address: 00:0C:29:EC:50:FF (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 1.41 seconds  
root@Priviasec:~#
```

Resim 8

Resim8'de "**nmap -sW 192.168.30.184**" komutuyla TCP Window Scan yapılmıştır. Windows güvenlik duvarının aktif olduğu durumda 1000 port **filtered** olarak işaretlemiştir. Windows güvenlik duvarının pasif olduğu durumda ise, 1000 port **closed** olarak işaretlemiştir.

Windows güvenlik duvarının pasif olduğu durumda, TCP ACK Scan taramasında oluşan çıktıda 1000 port **unfiltered** olarak işaretlenirken, TCP Window Scan taramasında 1000 port **closed** olarak işaretlenir. Bu şekilde iki tarama tekniği karşılaştırılabilir. Son olarak Resim9'da fragmentation tekniği kullanılarak güvenlik duvarının aktif ve pasif olduğu durumlarda tarama yapılmıştır.

Resim 9

Fragmentation tekniđi, gönderilen paketlerin parçalanarak gönderilmesini sağlayarak güvenlik duvarının paket içeriđini algılamasını zorlaştırır. Resim 9'da Windows Güvenlik duvarının aktif olduđu durumda fragmentation tekniđi ile yapılan taramada 445. portun açık olduđu tespit edilmiştir. Yukarıda bahsedilen örnekteki gibi burada da 445. portun açık olarak tespit edilmesinin sebebi, güvenlik duvarında bulunan Inbound kurallarında 445. port üzerindeki trafiđe izin veren bir kuralın aktif edilmesidir.



Windows güvenlik duvarının pasif edilmesi durumunda ise, 445,139,135 numaralı portların açık olduğu tespit edilmiştir. Bu şekilde Windows güvenlik duvarının aktif ve pasif olduğu durumlarda Nmap aracının üretmiş olduğu çıktılardaki farklılıklar görülmektedir.

- < **WhatsApp Masaüstü Uygulamasında Kritik Zafiyetler Keşfedildi #41**
- > **Cisco Cihazları Etkileyen 5 Kritik Zafiyet Keşfedildi #42**

**Tel:** +90 216 820 14 55

**Posta:** [info@priviasecurity.com](mailto:info@priviasecurity.com)

E-Bülten Abonelik

Gizlilik ve Çerez Politikası | Bilgi Güvenliği Politikası

Privia Security © 2018 Privacy For You



Automated page speed optimizations for fast site performance