

## Nmap İleri Seviye Part 2

Nmap, ağ tarama ve zafiyet tespiti için kullanılan açık kaynaklı bir araçtır. Bu araç birçok sisteme yönelik taramaları gerçekleştirerek esnek, hızlı ve anlamlı bir şekilde sonuç üretmektedir. Sistemlerin açık olup olmadığını, açık olan sistemlerin portlarını durumları, hangi servislerin çalıştığı ve kullanılan işletim sistemi gibi birçok bilgiyi verebilmektedir. Nmap ile tespit edilen servislerin güvenlik açığı barındırıp barındırmadığı ve kullanılan servisler hakkında bilgi elde edilebilir.

Ayrıca içerisinde barındırmış olduğu scriptler ile hedef sisteme yönelik tarama gerçekleştirildiğinde hedef sistem hakkında detaylı bilgi ve güvenlik açığı olup olmamasına yönelik sonuç üretmektedir. Nmap aracı, alanının en iyi araçları araçları arasında yer almaktadır.

### PORT TARAMA

Bilgisayar ve bilişim sistemlerinin birbirleri arasında iletişimini sağlamaları için kullanmış oldukları bağlantı noktalarının her birine port denilmektedir. Yapılan iletişimde türüne veya iletişim çeşidine göre belirli protokoller kullanılmaktadır. Bu protokollere tahsis edilen portlar doğrultusunda iletişim sağlanılmaktadır. Portlar, bilişim sistemlerine girdi ve çıktılarının geçiş noktasıdır. Nmap, portları kullanan iki protokolle çalışmaktadır.

Bu protokoller TCP ve UDP protokolleridir. Her protokol için bir bağlantı dört öğe tarafından gerçekleştirilmektedir. Bu öğeler: kaynak IP adresi, hedef IP adresi, kaynak port adresi ve hedef port adresidir. Protokol, IP veri bölümünde ne tür bir paketin bulunduğu belirten 8 bitlik bir alandır. IPv4 adresleri 32 bit uzunluğunda iken, portlar ise 16 bit uzunluğundadır. IPv6 adresleri ise 128 bit uzunluğundadır. Port numarası alanı 16 bit uzunluğundadır. Bundan dolayı 65535 adet port numarası kullanılabilir. En küçük değer olan 0 değeri geçersizdir. Port numarasının 0 olarak belirtilmesi joker görevi görmektedir. Sistemin varsayılan kendince port atamasına zemin hazırlamaktadır. Kötü amaçlı dinlemelerde saldırganlar port 0 noktasını dinlemektedir. Nmap açıkça belirtildiğinde (-p0-65535) port sıfır taraması gerçekleştirilebilmektedir.

### En Popüler TCP ve UDP Portları

**Port 80 (HTTP):** En sık kullanılan TCP portlarının arasında yer almaktadır. Varsayılan olarak web sayfaları kullanımında istemcinin bağlantı için kullanmış olduğu port numarasıdır.

**Port 23 (Telnet):** Telnet şifresiz iletişim ile internet üzerindeki bulunan bir makineye istemci olarak bağlanması sağlanmaktadır. Şifresiz iletişim olduğundan dolayı güvenli değildir. Fakat yönlendiricilerde yönetim portu olarak çalışabilmektedir.

**Port 443 (HTTPS):** Varsayılan olarak kullanılan HTTP protokolünün SSL ile şifrelenerek iletişim saflanması ile güvenliği artırmaktadır. Web sunucularına yönelik yapılan istekler şifreli gönderilmektedir.

**Port 21 (FTP):** Dosya aktarım protokolüdür. Telnet protokolü gibi veriler şifresiz açık halde aktarılmaktadır. Güvenli bir protokol olmayıp, halen kullanılmaktadır.

**Port 22 (SSH):** Secure Shell olarak bilinip kullanıcıların sunucuları internet üzerinden kontrol etmesini ve düzenlemesini sağlayan bir yönetim protokolüdür. Uzak makine arasında şifreli iletişimini sağlamaktadır.

**Port 25 (SMTP):** Mail gönderme protokolüdür.

**Port 53 (DNS):** Domain Name Server, domain adları ve bu domainlerin sahip olduğunu IP adresleri arasında dönüşüm yapmak için kullanılmaktadır. Hem TCP hem de UDP protokolü tarafından kullanılabilen bir porttir.

**Port 67 (DHCP):** Dynamic Host Configuration Protocol Server olarak bilinir ve ağa dahil olacak istemci makinelere IP adresi atamaktadır. UDP protokolü tarafından kullanılmaktadır.

**Port 68 (DHCP):** DHCP istemci portudur. UDP protokolü tarafından kullanılmaktadır.

**Port 69 (TFTP):** Özel dosya aktarım UDP protokolüdür. Trivial File Transfer Protocol olarak bilinmektedir.

**Port 110 (POP3):** Post Office Protocol version 3 olarak bilinmektedir. Yerel email istemcilerinin uzak email sunucuları ile iletişime geçmesi ile kullanılan bir protokoldür. Uzak sunuculardan email indirip bir kopyasını kendi sunucusunda bulundurma özelliği bulunmaktadır.

**Port 135 (MSRPC):** Microsoft Remote Procedure Call olarak adlandırılmaktadır. Sunucu ile istemci arasındaki iletişim için kullanılıp uzaktan kod çalıştırılmayı sağlamaktadır.

**Port 139 (NetBIOS-SSN):** MS-Windows hizmetleriyle iletişim kurmak için kullanılan ve NETBIOS Oturum Hizmeti sunan bir TCP protokolüdür.

**Port 445 (SMB):** Server Message Block Protocol tarafından kullanılmaktadır. SMB, dosya paylaşım için kullanılan bir protokoldür.

**Port 143 (IMAP):** Internet Message Access Protocol tarafından kullanılmaktadır. E-posta iletisi sunucu üzerinden yönetilmesini sağlayan bir TCP protokolüdür.

**Port 995 (POP3S):** POP3 protokolüne SSL eklenerek yapılan iletişimin daha güvenli hale gelmesini sağlamaktadır.

**Port 993 (IMAPS):** IMAPv2 protokolünün daha güvenli iletişimini sağlama amacıyla SSL eklenilen halidir.

**Port 5900 (VNC):** Güvenli olmayan bağlantı ile grafiksel masaüstü paylaşım sistemi için kullanılan bir TCP protokolüdür.

**Port 3389 (ms-term-server):** Remote Desktop Protocol (RDP) olarak bilinmektedir. Uzak masaüstü bağlantısı sağlayan bir TCP protokolüdür. Bağlantının güvenliği için network tabanlı port değişikliği yapılmaktadır.

**Port 3306 (MySQL):** MySQL veritabanı ile iletişimi sağlayan bir TCP protokolüdür.

**Port 1433 (MSSQL):** Microsoft SQL Server veritabanı ile iletişimi sağlayan bir TCP protokolüdür. Ayrıca UDP 1434 numaralı MS-SQL-DS protokolü aynı işlemleri gerçekleştirebilmektedir.

**Port 8080 (HTTP-Proxy):** HTTP Proxy'leri ve web sunucuları için kullanılan alternatif bir TCP protokolüdür.

**Port 1723 (PPTP):** VPN ağlarına güvenli bir şekilde bağlanması için altyapı sağlamaktadır.

**Port 161 (SNMP):** Simple Network Management Protocol tarafından kullanılmaktadır. Network bileşenlerinin veya network kartı olan UPS gibi cihazların yönetimini sağlama amacıyla kullanılan bir UDP protokolüdür.

## Port Taraması Nedir?

Hedef üzerinde bulunan portların durumlarını tespit etmek için uzaktan test etme işlemidir. Portların durumları açık ise port üzerinde gerçekleşen bağlantılar dinlenip bağlantının güvenli olup olmadığı ve hangi servisler üzerinden işlemler yapılmıştır yapılmadığı tespit edilmektedir. Portların durumları, aşağıdaki durumlardan oluşmaktadır.

**Open:** Portun açık olduğunu belirtmektedir. Genellikle açık olan portlarda servisler çalışmaktadır.

**Closed:** Portun kapalı olduğunu belirtmektedir.

**Filtered:** Portun açık olup olmadığı belirlenememektedir. Çünkü paket filtreleme, problemin porta ulaşmasını engellemektedir.

**Unfiltered:** Portun erişilebilir olduğunu göstermektedir. Ancak nmap, portun açık veya kapalı olduğu belireyememektedir.

**Open|Filtered:** Portun açık veya filtreli olup olmadığı belli olmadığı belirtir.

**Closed|Filtered:** Portun kapalı veya filtreli olup olmadığı belli olmadığı belirtir.

Şekil 4.2 – Portların Durumlarının Görüntülenmesi

```

root@priviasecurity: ~
File Edit View Search Terminal Help
root@priviasecurity:~# nmap -PU -Pn 192.168.16.160

Starting Nmap 7.50 ( https://nmap.org ) at 2019-01-31 10:50 EST
Nmap scan report for 192.168.16.160
Host is up (0.00026s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
MAC Address: 00:0C:29:A1:79:1C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 34.71 seconds
root@priviasecurity:~# █

```

Şekil 4.2'de gösterildiği gibi yapılan tarama sonucunda STATE(Durum) başlığı altında portların durumu açık olarak gösterilmiştir. Portların açık olan bir sistem üzerinde servislerin çalıştırılıp çalıştırılmayacağı hakkında bilgi edilebilir. Hatta açık port üzerinden güvenlik açığı var mı, yok mu diye tarama gerçekleştirilebilir. Bundan dolayı açık portların kontrol altında olması önemlidir. Sistem ve ağ yöneticileri, sistem güvenliği için kullanılan açık portları filtrelemelidir. Port kullanılmıyorsa, kapatılmalıdır.

Geçerleştirilen bir port taramasında açık port bulunursa, portta çalışan servis tespit edilir. Tespit edilen servisin zafiyetli olup olmadığı araştırılır. Yapılan araştırma sonucunda bir güvenlik açığının olabileceği düşünülürse güvenlik taraması gerçekleştirilir. Güvenlik taraması sonucunda servisin sürümünde güvenlik açığı olduğu belirtildiğinde, doğrulamak için sızma girişiminde bulunulmaktadır. Bu işlemleri saldırgan gerçekleştirmesi halinde hedef sisteme kritik derecede zararlar verebilir.

## Varsayılan Port Taraması

Nmap veritabanında belirlenmiş olan 1000 tane portun taraması yapılır. Bu taramalar genellikle hızlı bir şekilde biter. Ayrıca taramaların kısa sürmesi açısından tarama türü üzerinde değişiklikler yapılabilir. “-n” parametresi ile DNS çözümlemesinin yapılmaması istenir. Böylelikle portlar üzerinde DNS çözümlemesi gerçekleştirilmeyip zamanın tasarruf ederek sonuçlar elde edilir.

Şekil 4.2.1 – Genel Bir Nmap Taraması

```

root@priviasecurity: ~
File Edit View Search Terminal Help
root@priviasecurity:~# nmap 192.168.16.160

Starting Nmap 7.50 ( https://nmap.org ) at 2019-02-01 08:04 EST
Nmap scan report for 192.168.16.160
Host is up (0.00062s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
MAC Address: 00:0C:29:A1:79:1C (VMware)

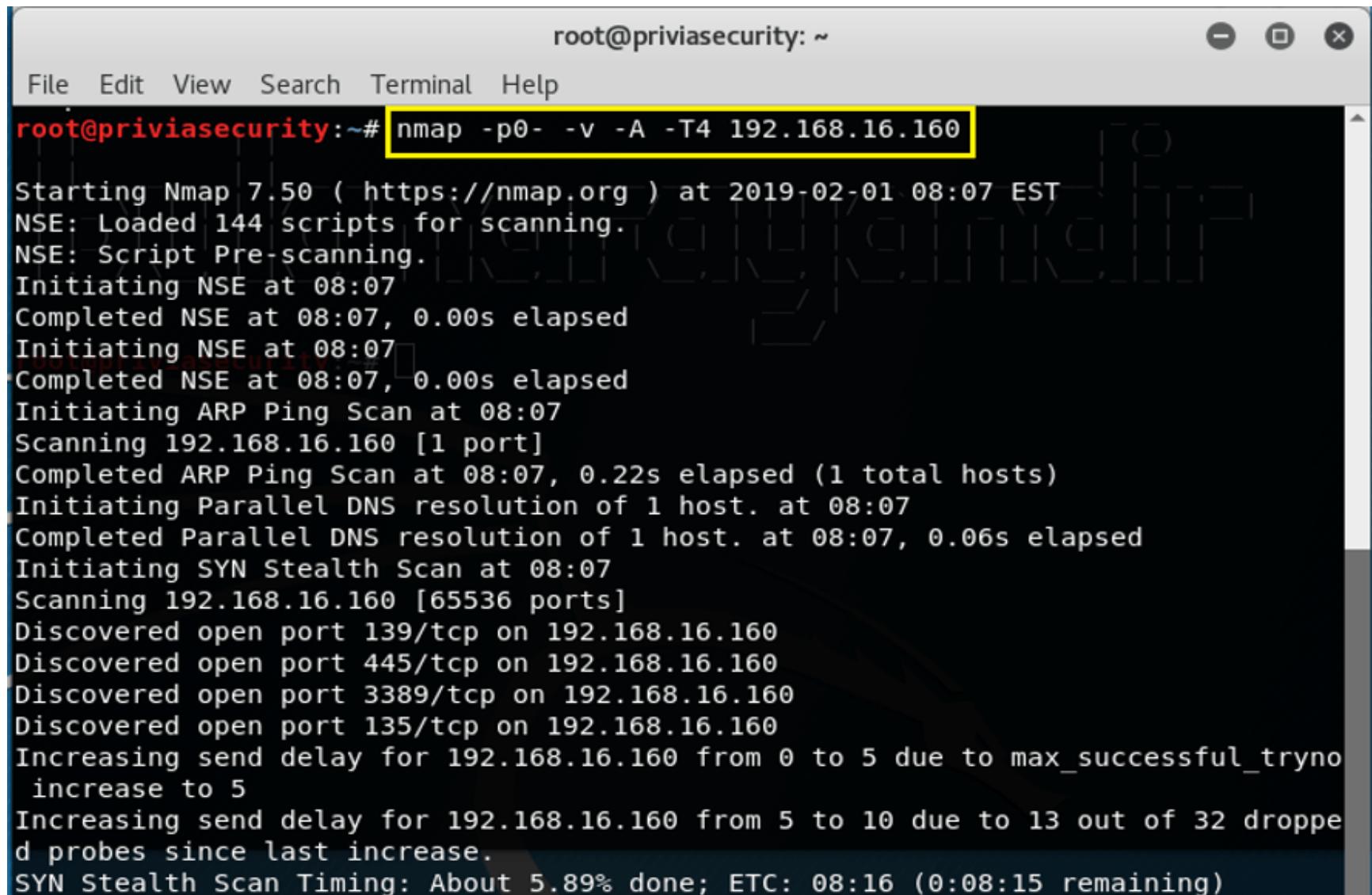
Nmap done: 1 IP address (1 host up) scanned in 45.79 seconds

```

Şekil 4.2.1'de belirtilen tarama türü genel bir nmap taraması olup, sonuçlarda bir IP adresine yönelik taramanın 45.79 saniyede gerçekleştirildiği görülmektedir.

Spesifik olarak portların belirtilmesi durumunda -p parametresi kullanılır. -p0- parametresinin kullanıldığı bir taramada hedef sistemin 65535 portunun hepsi taranacaktır. Bu durum bir makine için yapıldığı zaman çok uzun sürmeyebilir. Fakat bir makine yerine bir ağın taranması saatler alabilir. Çünkü varsayılan 1000 tane portun yerine 65535 tane port taranır.

Şekil 4.2.2 – Nmap Kapsamlı Tarama Örneği



```
root@priviasecurity: ~
File Edit View Search Terminal Help
root@priviasecurity:~# nmap -p0- -v -A -T4 192.168.16.160

Starting Nmap 7.50 ( https://nmap.org ) at 2019-02-01 08:07 EST
NSE: Loaded 144 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:07
Completed NSE at 08:07, 0.00s elapsed
Initiating NSE at 08:07
Completed NSE at 08:07, 0.00s elapsed
Initiating ARP Ping Scan at 08:07
Scanning 192.168.16.160 [1 port]
Completed ARP Ping Scan at 08:07, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:07
Completed Parallel DNS resolution of 1 host. at 08:07, 0.06s elapsed
Initiating SYN Stealth Scan at 08:07
Scanning 192.168.16.160 [65536 ports]
Discovered open port 139/tcp on 192.168.16.160
Discovered open port 445/tcp on 192.168.16.160
Discovered open port 3389/tcp on 192.168.16.160
Discovered open port 135/tcp on 192.168.16.160
Increasing send delay for 192.168.16.160 from 0 to 5 due to max_successful_tryno
increase to 5
Increasing send delay for 192.168.16.160 from 5 to 10 due to 13 out of 32 droppe
d probes since last increase.
SYN Stealth Scan Timing: About 5.89% done; ETC: 08:16 (0:08:15 remaining)
```

Şekil 4.2.2'de kapsamlı bir nmap taraması gerçekleştirilmiştir. Bu taramanın detaylı bir şekilde çıktıları ekrana basması için –v parametresi kullanılmıştır. –A parametresi ile agresif tarama gerçekleştirilir. Agresif tarama, port taraması, servis sürüm tespiti, işletim sistemi tespiti gibi taramaları yapar. Ayrıca gerçekleştirdiği taramada NSE scriptlerini de kullanır. –T4 değeri ise taramanın zamanlamasına yönelik kullanılan bir parametredir. –T parametresinin özelliklerinden biri zaman aşımı özelliğidir. Hedef makinelerden gelen cevapların süresi belirlenen sürenin üzerinde ise zaman aşımına uğrar. Böylece, Nmap bir sonraki makineye geçer.

## Port Tarama Tekniklerinin Seçilmesi

Port tarama tekniklerinin seçilmesi, port tarama işleminin başarılı bir şekilde gerçekleşebilmesi için büyük önem arz etmektedir. Çünkü taramanın hızlı olmasına ek olarak başarılı ve tutarlı bir tarama olması gerekmektedir.

### TCP SYN(Stealth) Scan (-sS)

TCP portlarını taramanın en hızlı yolu olduğu için en popüler tarama türüdür. Hedef sisteme bir SYN bayraklı TCP paketi gönderilerek gelen cevap doğrultusunda portun açık olup olmadığı tespit edilmektedir. Gönderilen SYN paketine, SYN/ACK paketi ile cevap gelirse hedef port açıktır. RST paketi ile cevap dönerse hedef port kapalıdır. Herhangi bir cevap gelmezse port filtreli sonucunu elde edilir. Alınan SYN/ACK paketine RST paketi gönderilip bağlantı düşürülür.

Şekil 4.3.1.b – TCP SYN (Stealth) Taramasının Bir Örneği

```

root@priviasecurity: ~
File Edit View Search Terminal Help
root@priviasecurity:~# nmap -sS 192.168.16.160

Starting Nmap 7.50 ( https://nmap.org ) at 2019-02-01 12:38 EST
Nmap scan report for 192.168.16.160
Host is up (0.0014s latency).
Not shown: 956 closed ports, 40 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
MAC Address: 00:0C:29:A1:79:1C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.04 seconds
root@priviasecurity:~# 

```

Şekil 4.3.1.b'de gösterildiği gibi –sS parametresi ile hedef IP adresine yönelik TCP SYN taraması gerçekleştirılmıştır. Bu tarama 2.04 saniye içerisinde bitmiştir. Sonuç olarak 4 açık port 40filtreli port ve 956 kapalı port tespit edilmiştir. Şekil 4.3.1.b'de 40 tane portun SYN paketine cevap vermediği içinfiltreli olarak işaretlendiği gösterilmiştir.

## TCP Connect Scan (-sT)

TCP Connect Scan taraması genellikle yetkisiz Unix makinelerine ve IPv6 hedeflerine yönelik yapılmaktadır. Ayrıca TCP SYN Scan taramasını çalışmadığı veya yetersiz kaldığı durumlarda işlem görmektedir. Nmap aracı, işletim sistemi üzerinden connect system çağrılarında bulunarak hedef makine ile port üzerinden bağlantı kurulmasını sağlayacaktır. Böylelikle port taramaları gerçekleştirilmektedir.

Şekil 4.3.2 – TCP Connect Scan Gösterimi

```

root@priviasecurity:~# nmap -sT -v 192.168.16.160

Starting Nmap 7.50 ( https://nmap.org ) at 2019-02-09 07:07 EST
Initiating ARP Ping Scan at 07:07
Scanning 192.168.16.160 [1 port]
Completed ARP Ping Scan at 07:07, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:07
Completed Parallel DNS resolution of 1 host. at 07:07, 0.01s elapsed
Initiating Connect Scan at 07:07
Scanning 192.168.16.160 [1000 ports]
Discovered open port 135/tcp on 192.168.16.160
Discovered open port 445/tcp on 192.168.16.160
Discovered open port 3389/tcp on 192.168.16.160
Discovered open port 139/tcp on 192.168.16.160
Completed Connect Scan at 07:07, 1.19s elapsed (1000 total ports)
Nmap scan report for 192.168.16.160
Host is up (0.0053s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
MAC Address: 00:0C:29:A1:79:1C (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
Raw packets sent: 1 (28B) | Rcvd: 1 (28B)

```

Şekil 4.3.2'de –sT parametresi kullanılarak TCP Connect Scan taraması gerçekleştirildi. Tarama sırasında gerçekleştirilen işlemlerin detaylı bir şekilde gösterilmesi için –v parametresi kullanıldı. Öncelikle ARP Ping Scan taraması gerçekleştiriliyor makinenin aktif olduğu tespit edildi. Sonrasında DNS çözümlemesi yapıldı. DNS çözümlemesinden sonra Connect Scan taraması yapılarak açık portlar elde edildi.

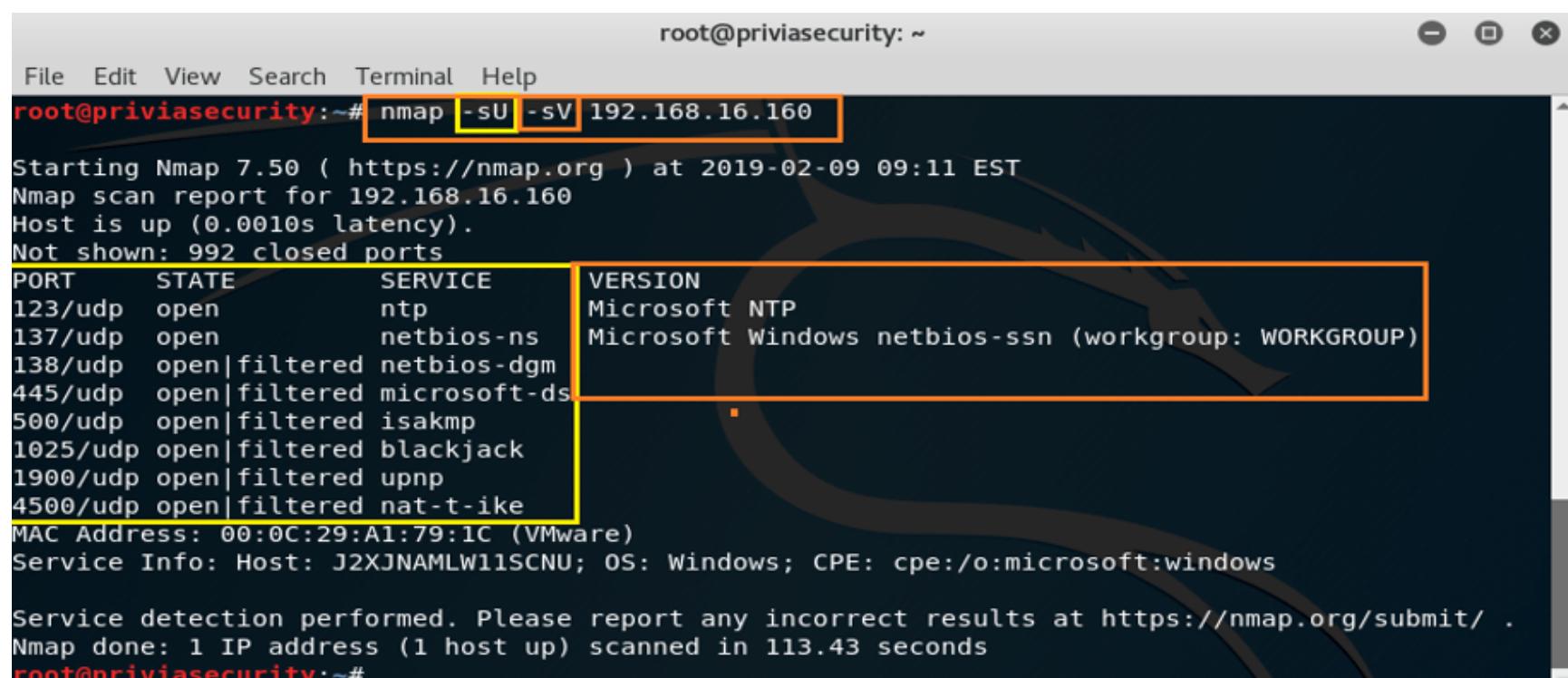
## UDP Scan (-sU)

Sistemlere yönelik taramalarda sadece TCP portlarına yönelik taramalar gerçekleştirmemek gereklidir. Çünkü UDP portlarına yönelik güvenlik açıkları da bulunmaktadır. En popüler servisler TCP protokolü üzerinde çalışabilir. Fakat UDP

üzerinde de servisler çalışmaktadır. Örneğin, DNS, SNMP ve DHCP servisleri UDP'yi kullanır. UDP taraması, TCP taramasına göre yavaş ve zor bir tarama olduğu için güvenlik uzmanları genellikle bu taramaları yapmama hatasına düşmektedir. Ayrıca sistem ve ağ yöneticileri de genellikle UDP portlarına yönelik güvenlik önlemlerini eksik almaktadır. Bu durum göz önüne alındığında UDP protokollerinde güvenlik açığı ortaya çıkma olasılığı yüksektir.

Nmap üzerinden UDP taraması gerçekleştirmek için `-sU` parametresi kullanılır. UDP portlarını tespit etmek için UDP paketleri gönderilmektedir. Fakat, `-data`, `-data-string` veya `-data-length` parametrelerini kullanmadan tarama yapılrsa UDP paketleri boş gidecektir. Cevap olarak ICMP port Unreachable hatası döndürürse port kapalıdır. UDP paketi ile cevap dönerse port açıktır. Herhangi bir cevap alınmadığında port açık veya filtreli olabilir. Ayrıca, UDP taramalarında hızlı bir şekilde tarama yapmak, yavaş hostları atlamak ve güvenlik duvarını atlatmak için `-host-timeout` parametresi kullanılmaktadır.

Şekil 4.3.3 – UDP Scan Gösterimi



```
root@priviasecurity: ~
File Edit View Search Terminal Help
root@priviasecurity:~# nmap -sU -sV 192.168.16.160
Starting Nmap 7.50 ( https://nmap.org ) at 2019-02-09 09:11 EST
Nmap scan report for 192.168.16.160
Host is up (0.0010s latency).
Not shown: 992 closed ports
PORT      STATE     SERVICE
123/udp   open      ntp
137/udp   open      netbios-ns
138/udp   open|filtered netbios-dgm
445/udp   open|filtered microsoft-ds
500/udp   open|filtered isakmp
1025/udp  open|filtered blackjack
1900/udp  open|filtered upnp
4500/udp  open|filtered nat-t-ike
MAC Address: 00:0C:29:A1:79:1C (VMware)
Service Info: Host: J2XJNAMLW11SCNU; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 113.43 seconds
root@priviasecurity:~#
```

Şekil 4.3.3'te gönderilen bazı UDP paketlerine karşı herhangi bir cevap gelmediği için Nmap portları `open|filtered` olarak belirtmiştir. Açık UDP portlarında kullanılan servislerin sürüm bilgisini elde etmek için `-sV` parametresi kullanılır.

## TCP NULL, FIN, Xmas Scans (-sN, -sF, -sX)

TCP NULL Scan taramasında `-sN` parametresi kullanılarak boş bir TCP paketi gönderilmiştir. TCP bayrak başlık değeri 0'dır. TCP FIN Scan taraması, `-sF` parametresi kullanılarak TCP FIN bitinin ayarlanmasıyla gerçekleştirilen tarama türüdür. TCP Xmas Scan taraması ise `-sX` parametresi kullanılarak FIN, PSH ve URG bayraklarının ayarlanmasıyla gerçekleştirilen tarama türüdür.

Tarama türünün en önemli avantajı, durum bildirmeyen güvenlik duvarları ve paket filterleme yönlendiricileri üzerinden gizlice tarama yapmayan olak vermesidir. Bu tür güvenlik duvarları, SYN biti set edilen ve ACK biti silinen TCP paketlerini engeller. NULL, FIN ve Xmas taramaları SYN bitini silerek tarama yaptığı için bu kuralı atlayabiliyor. Diğer avantajı ise, bu tarama türleri bir TCP SYN taramasına göre daha gizlidir.

Şekil 4.3.4.a – TCP NULL Scan Gösterimi

```
root@priviasecurity:~# nmap -sN -v -n 192.168.16.160
Starting Nmap 7.50 ( https://nmap.org ) at 2019-02-09 10:18 EST
Initiating ARP Ping Scan at 10:18
Scanning 192.168.16.160 [1 port]
Completed ARP Ping Scan at 10:18, 0.23s elapsed (1 total hosts)
Initiating NULL Scan at 10:18
Scanning 192.168.16.160 [1000 ports]
Increasing send delay for 192.168.16.160 from 0 to 5 due to 343 out of 1143 dropped probes since last increase.
Increasing send delay for 192.168.16.160 from 5 to 10 due to 11 out of 25 dropped probes since last increase.
Increasing send delay for 192.168.16.160 from 10 to 20 due to 11 out of 29 dropped probes since last increase.
Completed NULL Scan at 10:18, 6.54s elapsed (1000 total ports)
Nmap scan report for 192.168.16.160
Host is up (0.00062s latency).
All 1000 scanned ports on 192.168.16.160 are closed
MAC Address: 00:0C:29:A1:79:1C (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 7.01 seconds
  Raw packets sent: 1411 (56.428KB) | Rcvd: 1211 (48.428KB)
root@priviasecurity:~#
```

Şekil 4.3.4.a'da gösterildiği gibi TCP NULL taraması gerçekleştirilmiştir. Bu tarama sonucunda varsayılan 1000 port taramış olup açık portların olmadığı bilgisi elde edilmiştir. Ayrıca -n parametresi kullanılarak Reverse DNS çözümlemesi yapılması istenmemiştir. -v parametresi ile detaylı bilgi göstermesi sağlanmıştır. Ek olarak, tarama sırasında kullanılan problardan bazıları gecikmeden dolayı drop edilmiştir.

Şekil 4.3.4.b – TCP FIN Scan Gösterimi

```
root@priviasecurity:~# nmap -sF -v -n 192.168.16.160
Starting Nmap 7.50 ( https://nmap.org ) at 2019-02-09 10:44 EST
Initiating ARP Ping Scan at 10:44
Scanning 192.168.16.160 [1 port]
Completed ARP Ping Scan at 10:44, 0.22s elapsed (1 total hosts)
Initiating FIN Scan at 10:44
Scanning 192.168.16.160 [1000 ports]
Completed FIN Scan at 10:44, 2.67s elapsed (1000 total ports)
Nmap scan report for 192.168.16.160
Host is up (0.00098s latency).
All 1000 scanned ports on 192.168.16.160 are closed
MAC Address: 00:0C:29:A1:79:1C (VMware)
```

Şekil 4.3.4.b'de TCP FIN taraması gerçekleştirilmiştir. Bu tarama türünde de varsayılan 1000 port taramış olup, açık port olmadığı bilgisi elde edilmiştir.

## TCP ACK Scan (-sA)

Durum bilgisi veren güvenlik duvarları, ağ bağlantılarının gezinimini, çalışma durumunu ve karakteristik özelliklerini izleyen güvenlik duvarlarıdır. Bu tarama türü güvenlik duvari kural kümelerini eşleyerek durum bilgisi verip vermediğini veya hangi portunu filtereli olup olmadığını tespit etmek için kullanılır. Port taramalarında portun açık veya kapalı olduğunu tespit etmemesi bir dezavantajıdır.

Açık ve kapalı portların olup olmadığını tespit edememesinin sebebi ise tarama sırasında cevap olarak iki port durumunda da RST paketi gönderilmesidir. Nmap bu cevabı unfiltered olarak işaretlemektedir. Unfiltered işaretlenme durumu, ACK paketlerinin hedef makineye ulaştığı ve erişimin sağlandığını belirtir.

Şekil 4.3.5 – TCP ACK Scan Gösterimi

```
root@priviasecurity:~# nmap -sA -n -v 192.168.16.160

Starting Nmap 7.50 ( https://nmap.org ) at 2019-02-09 11:06 EST
Initiating ARP Ping Scan at 11:06
Scanning 192.168.16.160 [1 port]
Completed ARP Ping Scan at 11:06, 0.22s elapsed (1 total hosts)
Initiating ACK Scan at 11:06
Scanning 192.168.16.160 [1000 ports]
Increasing send delay for 192.168.16.160 from 0 to 5 due to 248 out of 825 dropped packets increase.
Increasing send delay for 192.168.16.160 from 5 to 10 due to 11 out of 23 dropped packets increase.
Increasing send delay for 192.168.16.160 from 10 to 20 due to 11 out of 33 dropped packets increase.
Increasing send delay for 192.168.16.160 from 20 to 40 due to 11 out of 33 dropped packets increase.
Increasing send delay for 192.168.16.160 from 40 to 80 due to 11 out of 32 dropped packets increase.
Completed ACK Scan at 11:06, 25.14s elapsed (1000 total ports)
Nmap scan report for 192.168.16.160
Host is up (0.00060s latency).
All 1000 scanned ports on 192.168.16.160 are unfiltered
MAC Address: 00:0C:29:A1:79:1C (VMware)
```

Şekil 4.3.5'te gösterilen bir TCP ACK Scan tarama türüdür. Bu taramanın gerçekleştirilmesi için –sA parametresi kullanılmaktadır. Şekil 4.3.5'te gösterildiği gibi problemler bazları drop edilmiştir. Bu durum bütün tarama türlerinde meydana gelmektedir. Çünkü problemlerin gönderiminde herhangi bir gecikme olduğunda ağ üzerinde düşebilmektedir.

## TCP Window Scan (-sW)

Bu tarama türü TCP ACK Scan tarama türüne benzemektedir. Tarama sırasında cevap olarak alınan RST paketlerini unfiltered olarak işaretlemek yerine, RST paketlerinin TCP Window alanına bakılarak işlem yapılır. TCP Window alanında pozitif window ise portu open, sıfır window ise portu kapalı olarak işaretlemektedir. Bu tarama türü, internet üzerindeki az sayıdaki sistemlerin uygulama detaylarına dayandığı için az kullanılıp güvenilmemektedir.

Şekil 4.3.6 – TCP Window Scan Gösterimi

```
root@priviasecurity:~# nmap -sW -n -v 192.168.16.160

Starting Nmap 7.50 ( https://nmap.org ) at 2019-02-09 11:14 EST
Initiating ARP Ping Scan at 11:14
Scanning 192.168.16.160 [1 port]
Completed ARP Ping Scan at 11:14, 0.22s elapsed (1 total hosts)
Initiating Window Scan at 11:14
Scanning 192.168.16.160 [1000 ports]
Completed Window Scan at 11:14, 3.69s elapsed (1000 total ports)
Nmap scan report for 192.168.16.160
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.16.160 are closed
MAC Address: 00:0C:29:A1:79:1C (VMware)
```

Şekil 4.3.6'da gösterildiği gibi TCP Window taraması –sW parametresi kullanılarak gerçekleştirilen bir tarama türüdür.

## TCP Maimon Scan (-sM)

Bu tarama türü, FIN, NULL ve Xmas tarama türleri ile benzerdir. Farklı olan tarafı ise hedef sisteme gönderilen probun FIN/ACK olmasıdır. Bu tarama, gizli bir firewall-evading tarama türüdür. TCP FIN ve ACK bayraklarının ayarlamasını ile gerçekleştirilen taramadır. Bu tarama ile paket filtreleyen güvenlik duvarları atlatılabilir.

Şekil 4.3.7 – TCP Maimon Scan Gösterimi

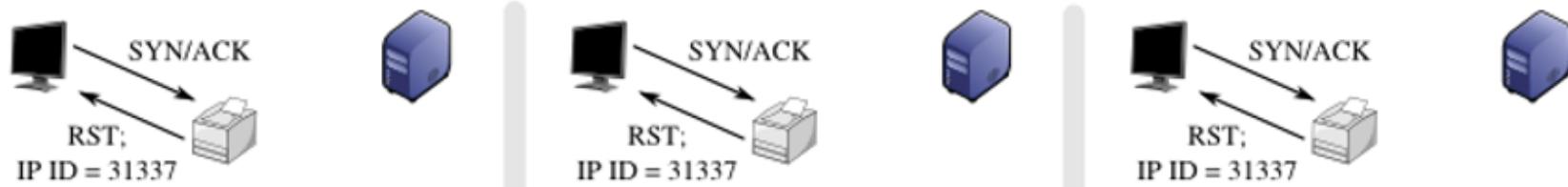
```
root@priviasecurity:~# nmap -SM -v priviasecurity.com
Starting Nmap 7.50 ( https://nmap.org ) at 2019-02-09 11:30 EST
Initiating Ping Scan at 11:30
Scanning priviasecurity.com (104.18.40.10) [4 ports]
Completed Ping Scan at 11:30, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:30
Completed Parallel DNS resolution of 1 host. at 11:30, 0.03s elapsed
Initiating Maimon Scan at 11:30
Scanning priviasecurity.com (104.18.40.10) [1000 ports]
Completed Maimon Scan at 11:30, 1.28s elapsed (1000 total ports)
Nmap scan report for priviasecurity.com (104.18.40.10)
Host is up (0.00014s latency).
Other addresses for priviasecurity.com (not scanned): 104.18.41.10 2606:4700:30::6812:280a 2606:4700:30::6812:290a
All 1000 scanned ports on priviasecurity.com (104.18.40.10) are closed
```

## TCP Idle Scan (-sI)

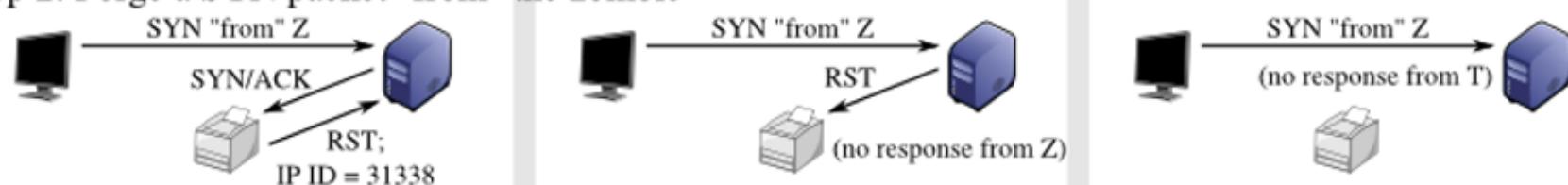
Bu tarama yöntemi, hedefe yönelik kör bir TCP tarama yapılmasını sağlamaktadır. Kör bir TCP taraması denenmesinin sebebi ise hedef makineye gönderilen paketlerin hiçbirinin taramayı gerçekleştiren makinenin IP adresi ile gönderilmemesidir. Side-channel saldırısı ile ağ üzerindeki zombi makineler tahmin edilir ve IP Fragmentation ID dizisi oluşturularak kullanılır. Ayrıca TCP Idle Scan, en gizli tarama türüdür. Aynı zamanda bu tarama türü yavaş ve karmaşıktır.

Şekil 4.3.8.a – TCP IDLE SCAN Port Durumlarının Gösterimi

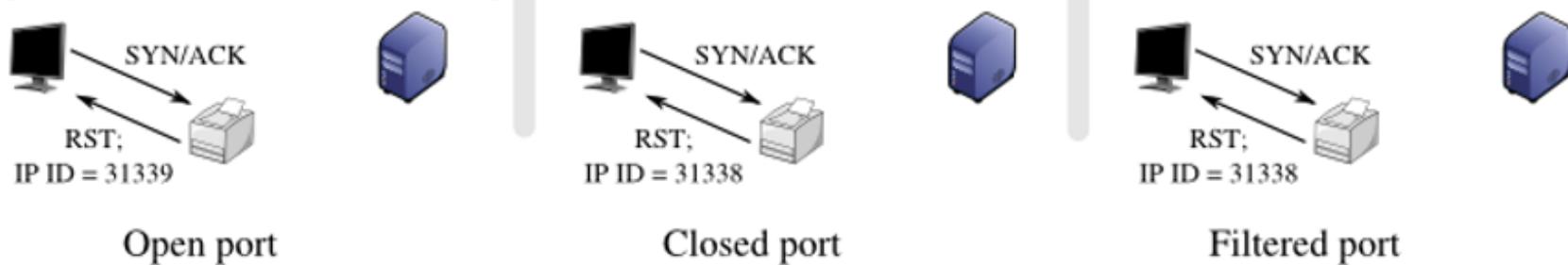
Step 1: Probe the zombie's IP ID.



Step 2: Forge a SYN packet "from" the zombie



Step 3: Probe the zombie's IP ID again.



Şekil 4.3.8.a 'da gösterildiği gibi TCP Idle Scan taramasında port durumları IP ID fragmentation işlemine göre belirlenir.

**Açık port durumunun belirlenmesi:**

- Saldırgan makine, zombi makinesine SYN/ACK bayrağı gönderir.
- Zombi makinesi, saldırıcı makineye IP ID değeri 31337 olan bir RST bayrağı gönderir.
- Saldırgan makine, zombie makinesinin paket bilgileri ile hedef makineye SYN bayrağı gönderir.
- Hedef makine, zombi makinesine SYN/ACK bayrağı gönderir.
- Zombi makinesi, hedef makineye IP ID değeri 31338 olan bir RST bayrağı gönderir.
- Saldırgan makine tekrar zombie makinesine SYN/ACK bayrağı gönderir.
- Zombi makinesi, saldırıcı makineye IP ID değeri 31339 olan bir RST bayrağı gönderir.
- Saldırgan makine, zombi makinesindeki IP ID değerinin 2'sini artırdığını tespit ederek hedef makine ile iletişime geçtiğini doğrulayıp hedef makine portunu açık olarak işaretler.

**Kapalı port durumunun belirlenmesi:**

- Saldırgan makine, zombi makinesine SYN/ACK bayrağı gönderir.
- Zombi makinesi, saldırıcı makineye IP ID değeri 31337 olan bir RST bayrağı gönderir.
- Saldırgan makine, zombie makinesinin paket bilgileri ile hedef makineye SYN bayrağı gönderir.
- Hedef makine, zombi makinesine RST bayrağı gönderir.
- Saldırgan makine tekrar zombie makinesine SYN/ACK bayrağı gönderir.
- Zombi makinesi, saldırıcı makineye IP ID değeri 31338 olan bir RST bayrağı gönderir.
- Saldırgan makine, zombi makinesindeki IP ID değerinin 1 sayısı kadar arttığını tespit ederek hedef makine ile iletişime geçmediğini doğrulayıp hedef makine portunu kapalı olarak işaretler.

#### Filtrelenmiş port durumunun belirlenmesi:

- Saldırgan makine, zombi makinesine SYN/ACK bayrağı gönderir.
- Zombi makinesi, saldırıcı makineye IP ID değeri 31337 olan bir RST bayrağı gönderir.
- Saldırgan makine, zombie makinesinin paket bilgileri ile hedef makineye SYN bayrağı gönderir.
- Hedef makine, zombi makinesine hiçbir dönüş yapmaz.
- Saldırgan makine tekrar zombie makinesine SYN/ACK bayrağı gönderir.
- Zombi makinesi, saldırıcı makineye IP ID değeri 31338 olan bir RST bayrağı gönderir.
- Saldırgan makine, zombi makinesindeki IP ID değerinin 1 sayısı kadar arttığını tespit ederek hedef makine ile iletişime geçmediğini doğrular. Saldırgan bakış açısından bakıldığından滤relenmiş port ve kapalı port ayırt edilmez.

Şekil 4.3.8.b – TCP Idle Scan Gösterimi

Şekil 4.3.8.b'de gösterildiği gibi TCP Idle Scan taramasını başlatmak için **-sI** parametresinin kullanılması yeterli olacaktır. Parametreden sonra gelen IP adresi zombi IP adresidir. Varsayılan olarak 80. Portu kullanmaktadır. İsteğimiz dahilinde zombi bilgisayardaki açık olan portlardan biri **[IP:Port]** formatında girilebilir. Zombi makina IP adresinden sonra hedef makinanın IP adresi girilmelidir. Daha sonra taramada istenilen özelliğe göre parametreler girilebilir. Örnek olarak pingsiz tarama için **-Pn** parametresi kullanılmıştır. Ayrıca wireshark aracı üzerinden ağ dinlemeye alındığında zombi makina kullanılarak tarama işlemi yapıldığı görülmektedir.

## IP Protocol Scan (-sO)

Bu tarama türü teknik olarak port taraması değildir. Hedef sistem üzerinde hangi protokollerin çalıştığını tespit etmek için kullanılır. **-p** parametresi kullanılarak port numarası yerine protocol numarası yazılmalıdır. **-p** parametresinin protocol veya port taraması olup olmadığından ayırt edilebilmesi için **-sO** parametresi kullanılır. **-p** parametresine atanınan protocol numarası ile IP Protocol taraması gerçekleştirilir. Çıktı formatı normal formata benzemektedir. Fakat numaralarının yazıldığı yerde protokol yazılmıştır.

Şekil 4.3.9 – IP Protocol Scan Gösterimi

```
root@priviasecurity:~# nmap -sO -p135 -v -n 192.168.16.160
Starting Nmap 7.50 ( https://nmap.org ) at 2019-02-10 11:03 EST
Initiating ARP Ping Scan at 11:03
Scanning 192.168.16.160 [1 port]
Completed ARP Ping Scan at 11:03, 0.22s elapsed (1 total hosts)
Initiating IPProto Scan at 11:03
Scanning 192.168.16.160 [1 port]
Completed IPProto Scan at 11:03, 0.24s elapsed (1 total ports)
Nmap scan report for 192.168.16.160
Host is up (0.00040s latency).

PORT      STATE SERVICE
135      open|filtered mobility-hdr
MAC Address: 00:0C:29:A1:79:1C (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
  Raw packets sent: 3 (68B) | Rcvd: 1 (28B)
root@priviasecurity:~# nmap -p135 -sV -n 192.168.16.160
Starting Nmap 7.50 ( https://nmap.org ) at 2019-02-10 11:04 EST
Nmap scan report for 192.168.16.160
Host is up (0.00030s latency).

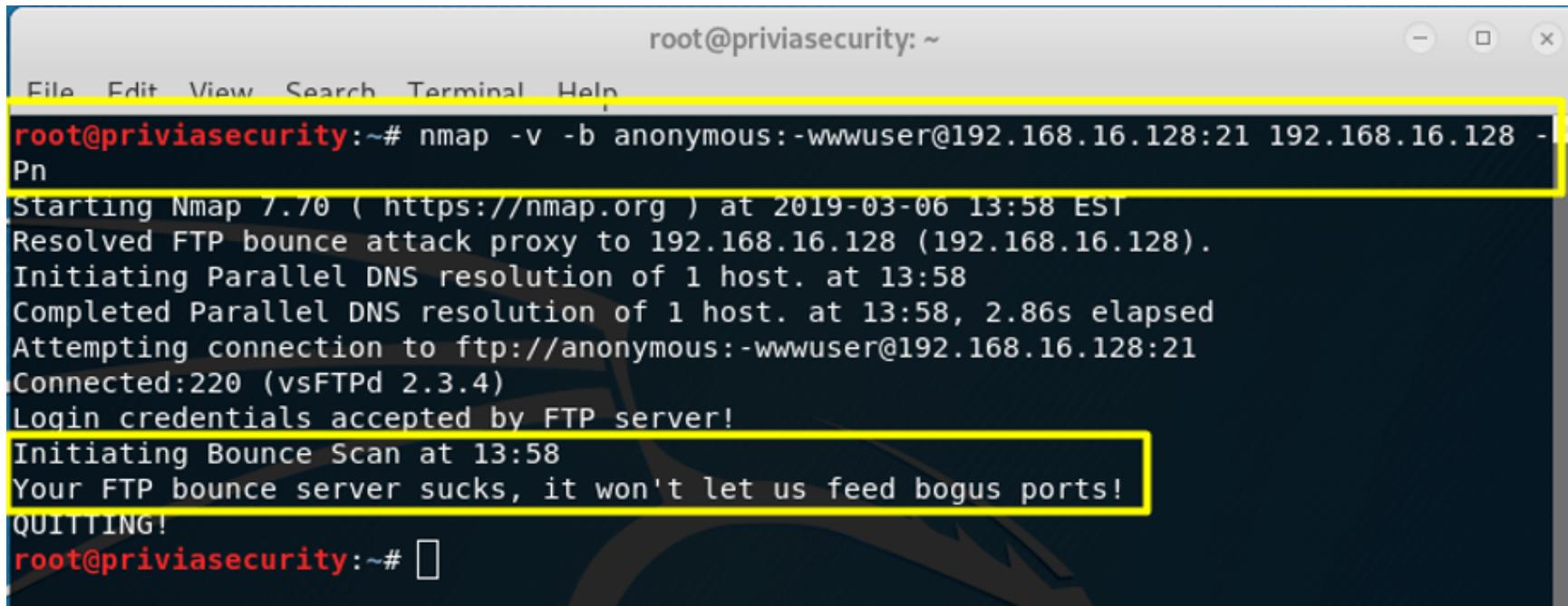
PORT      STATE SERVICE VERSION
135/tcp    open  msrpc    Microsoft Windows RPC
MAC Address: 00:0C:29:A1:79:1C (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Şekil 4.3.9'de iki farklı özelliğe göre tarama yapılmıştır. İlk tarama komutu, **-sO** parametresi ile protokol taraması gerçekleştirileceği belirtilir. **-p** parametresine protokol numarası atanır. Detaylı çıktı olması için **-v** parametresi, DNS çözümlemesinin yapılmaması için **-n** parametresi kullanılmıştır. İkinci tarama komutunda da port taraması yapılmıştır. İlk taramada 135 numaralı protokole yönelik tarama yapılrken, TCP olup olmadığına bakılmayıp port durumu **open|filtered** olarak işaretlenmiştir. Ayrıca ilk taramada ekstra servis tespiti için parameter girilmesine ihtiyaç duyulmayıp varsayılan olarak protokolün kullanılmış olduğu servis hakkında bilgi verir. İkinci taramadaki çıktıda Protokol başlığı yerine varsayılan Port başlığı adı altında **135/TCP** belirtilip durumu **open** olarak işaretlenmiştir. Port üzerinde çalışan servis sürümünün tespiti için **-sV** parametresi kullanılır.

## TCP FTP Bounce Scan (-b)

FTP protokolünün Proxy FTP bağlantısı özelliği vardır. Bu özellik, kullanıcının bir FTP sunucusuna bağlanması ve ardından dosyaları üçüncü taraf bir sunucuya göndermesini sağlar. Bu özellikler saldırganlar tarafından kullanıldığı için az sunucu bu özelliği kullanır. Bir diğer dezavantaj ise FTP sunucusunun diğer hostları taramasına izin verilmesidir. Bu tarama ise FTP sunucu tespit ettiği zaman sırasıyla diğer hostlara dosya gönderir. Alınan hata mesajından portun açık olup olmadığı anlaşılmaktadır. Bu durum güvenlik duvarlarını atlatmak için kullanılır. Çünkü kurumsal FTP sunucuları, genellikle bütün ana bilgisayarların erişebilecekleri bir konuma koymak ister. Bu tarama **-b** parametresi ile kullanılmaktadır. "kullanıcıadi:parola@ftpserver\_IP:port" şeklinde argüman almaktadır. Port numarası girilmezse varsayılan 21. port üzerinden işlem yapmaktadır. Bir güvenlik duvarını atlatmak için sadece 21. port numarası taranıp ftp-bounce NSE dosyası kullanılabilir.

Şekil 4.3.10 – TCP FTP Bounce Scan Gösterimi



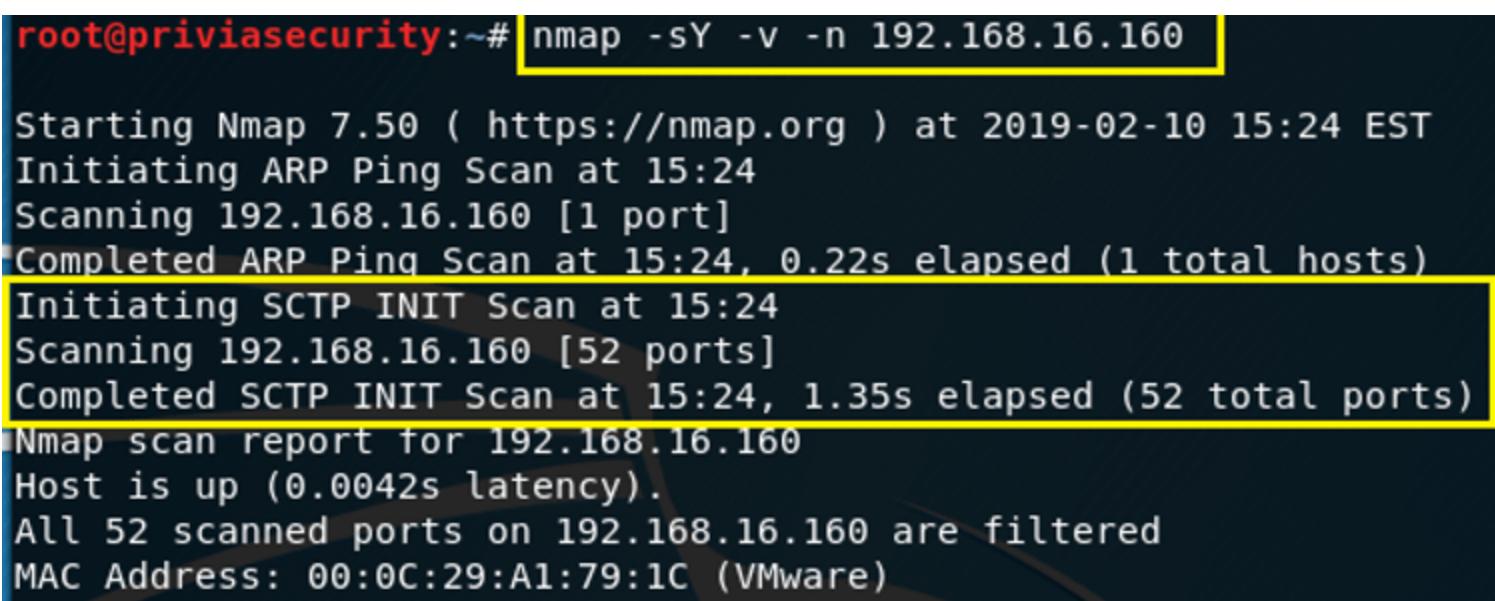
```
root@priviasecurity:~# nmap -v -b anonymous:-wwwuser@192.168.16.128:21 192.168.16.128 -Pn
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-06 13:58 EST
Resolved FTP bounce attack proxy to 192.168.16.128 (192.168.16.128).
Initiating Parallel DNS resolution of 1 host. at 13:58
Completed Parallel DNS resolution of 1 host. at 13:58, 2.86s elapsed
Attempting connection to ftp://anonymous:-wwwuser@192.168.16.128:21
Connected:220 (vsFTPD 2.3.4)
Login credentials accepted by FTP server!
Initiating Bounce Scan at 13:58
Your FTP bounce server sucks, it won't let us feed bogus ports!
QUITTING!
root@priviasecurity:~#
```

Resim 4.3.10 da gösterildiği gibi tarama işlemi gerçekleştirildi. FTP Bounce Scan taramasının yapılması aynı zamanda bir saldırı olarak görülür. Çünkü FTP Bounce sunucuları üzerinde başka makinelere yönelik port taraması ve dosya gönderilmesi kolaylıkla yapılabilir.

## SCTP INIT Scan (-sY)

Bu tarama türü, TCP SYN taramasının SCTP eşdeğeridir. Engellenmeyen bir ağıda saniyede binlerce port taranabilir. TCP SYN taraması gibi INIT taraması da SCTP ilişkilerini tamamlamadığı için göze çarpmayan gizli bir taramadır.

Şekil 4.3.11 – SCTP INIT Scan Gösterimi



```
root@priviasecurity:~# nmap -sY -v -n 192.168.16.160
Starting Nmap 7.50 ( https://nmap.org ) at 2019-02-10 15:24 EST
Initiating ARP Ping Scan at 15:24
Scanning 192.168.16.160 [1 port]
Completed ARP Ping Scan at 15:24, 0.22s elapsed (1 total hosts)
Initiating SCTP INIT Scan at 15:24
Scanning 192.168.16.160 [52 ports]
Completed SCTP INIT Scan at 15:24, 1.35s elapsed (52 total ports)
Nmap scan report for 192.168.16.160
Host is up (0.0042s latency).
All 52 scanned ports on 192.168.16.160 are filtered
MAC Address: 00:0C:29:A1:79:1C (VMware)
```

Şekil 4.3.11'de gösterildiği gibi –sY parametresi kullanılarak tarama başlatılabilir. Bu tarama tekniği half-open scanning olarak adlandırılır. Çünkü tam bir SCTP ilişkilendirmesi açılmamaktadır. Bir INIT chuck gönderilip, gerçek bir ilişkilendirme yapılmış gibi hedefe gösterilerek hedef makineden bir cevap beklenir. Dönen cevap bir INIT-ACK chuck ise portun açık olduğunu, bir ABORT chuck ise portun kapalı olduğunu belirtmektedir. Birkaç INIT chuck isteğinden sonra herhangi bir cevap alınmadığında portun filtreliliği belirtilmektedir.

## SCTP COOKIE ECHO Scan (-sZ)

Bu tarama türü gelişmiş bir SCTP taramasıdır. Bu tarama türünün avantajı, INIT taramasına göre bir port taraması olarak görülmemesidir. Dezavatajı ise, tarama sırasında açık ve filtrelili portları birbirinden ayırt edememesidir. Bu durum dışında portun kapalı olması durumunda SCTP INIT taramasındaki gibi bir ABORT cevabı alındığında portun kapalı olduğu belirtilir.

## Özel TCP Taraması (-scanflags)

TCP bayraklarının özel olarak seçiliip kullanılması durumunda –scanflags parametresi kullanılır. –scanflags parametresi, güvenlik duvarlarının atlatılmasında kullanılabilir. –scanflags parametresine TCP bayraklarının isimleri atandığı gibi TCP bayraklarını ifade eden sayısal değerlerde atanabilir. Örnek olarak, 9 sayısı PSH ve FIN bayraklarının bir arada kullanılacağı anlamına gelmektedir. Ayrıca herhangi bir tarama türü belirtilmezse varsayılan olarak SYN taraması gerçekleştiriliyor.

Resim 4.3.13 – Özel TCP Taraması Gösterimi

```
root@priviasecurity:~# nmap --scanflags PSH -v -n 192.168.16.160
Starting Nmap 7.50 ( https://nmap.org ) at 2019-02-10 16:02 EST
Initiating ARP Ping Scan at 16:02
Scanning 192.168.16.160 [1 port]
Completed ARP Ping Scan at 16:02, 0.23s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 16:02
Scanning 192.168.16.160 [1000 ports]
Completed SYN Stealth Scan at 16:02, 4.09s elapsed (1000 total ports)
Nmap scan report for 192.168.16.160
Host is up (0.00096s latency).
All 1000 scanned ports on 192.168.16.160 are closed
MAC Address: 00:0C:29:A1:79:1C (VMware)
```

Şekil 4.3.13 üzerinde gösterildiği gibi –scanflags parametresi kullanılarak özel bir tarama gerçekleştirilmiştir. Bu taramada ek olarak bir tarama türü seçilmemişi için varsayılan olarak SYN taraması gerçekleştirilmiştir.

## Port Seçerek Tarama

Nmap varsayılan olarak port taraması yaptığındı popüler 1000 portu taramaktadır. -F parametresi kullanılarak hızlı tarama yapılması istenildiğinde popüler 100 port taranır. Ayrıca –top-ports parametresi kullanılarak popüler portlar taranır. Popüler port taramaları dışında -p parametresi kullanılarak port numarası, taranılacak port aralığı veya protokol numarası belirtilerek tarama yapılabilir. -p parametresinin kullanım şekilleri aşağıdaki gibidir:

- **p 445**: Yalnızca SMB portuna yönelik bir tarama gerçekleştirilmesini ifade eder.
- **p ssh**: SSH servisinin çalıştığı 22 numaralı porta yönelik bir tarama belirtir.
- **p 22,25,80**: Birden çok porta yönelik tarama gerçekleştirilir. Bu parametreden sonra –sS parametresi kullanılırsa sadece TCP portları, -sU parametresi kullanılırsa UDP portları taranmaktadır.
- **p 22-89,110**: Böylelikle 22 ve 89 numaralı portlar arasındaki portları ve 110 numaralı portu taramaktadır.
- **p- :**  Bu parametrenin kullanımı ise 65535 tane portun taranmasını sağlar. (-p0-)
- **pT:22,U:53**: TCP 22. port ve UDP 53. port taraması yapılır.
- **p http\***: HTTP ile başlayan bütün servislerin olduğu portlar taranır.

Yukarıda gösterilen parametreler –p parametresi ile kullanılmakta olup, port taraması için ek olarak kullanılan parametreler de aşağıdaki gibidir:

**-exclude-ports 20-30**: Bu parametre ile 20 ile 30 numaralı portlar arasındaki port taramaları yapılmayacağını göstermektedir.

- **F**: Bu parametre ile hızlı port taraması için kullanılır. Varsayılan olarak taranan popüler 1000 port yerine popüler 100 port taraması yapılmaktadır.
- **r**: Nmap, port taramalarını varsayılan olarak rasgele yapmaktadır. Bu port taramalarını belirli bir sırada görmek için bu parametre kullanılmaktadır.

**-port-ratio**: Port taramalarının sıklık derecesini belirtmek için kullanılır. Atanan değer 0 ile 1 sayısı arasında olmalıdır.

**-top-ports**: Taranacak popüler port sayısı verilir.

## Port Taramada Zamanlama Önemi

Nmap aracı, hedef sistemlere yönelik port taramalarını gerçekleştirirken hız ve zaman önemli bir yer tutmaktadır. Özellikle büyük ağlara yönelik gerçekleştirilen taramalarda önemlidir. Ayrıca verimlilik ve performansında iyi olması gereklidir. Port taramalarında zamanlama ile ilgili kullanılan bazı parametreler aşağıdaki gibidir:

**-min-rtt-timeout, -max-rtt-timeout, -initial-rtt-timeout**: Port taramalarında kullanılan problemlerin cevap verebilecekleri minimum ve maximum sürelerin ayarlanması için kullanılır. Şekil 4.4.1 üzerinde gösterilmiştir.

Resim 4.4.1 – rtt-timeout Parametrelerinin Gösterimi

```
root@priviasecurity:~# nmap -T4 -Pn -p135,139,445 -v -n --max-rtt-timeout 200ms
--initial-rtt-timeout 150ms 192.168.16.160

Starting Nmap 7.50 ( https://nmap.org ) at 2019-02-13 10:03 EST
Initiating ARP Ping Scan at 10:03
Scanning 192.168.16.160 [1 port]
Completed ARP Ping Scan at 10:03, 0.22s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 10:03
Scanning 192.168.16.160 [3 ports]
Discovered open port 139/tcp on 192.168.16.160
Discovered open port 135/tcp on 192.168.16.160
Discovered open port 445/tcp on 192.168.16.160
Completed SYN Stealth Scan at 10:03, 0.22s elapsed (3 total ports)
Nmap scan report for 192.168.16.160
Host is up (-0.10s latency).

PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 00:0C:29:A1:79:1C (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds
    Raw packets sent: 5 (188B) | Rcvd: 4 (160B)
```

- host-timeout:** Host başına belirtilen tarama süresidir. Zaman aşımı durumunda tarama iptal edilir.
- min-rate, -max-rate:** Taramada kullanılacak probaların saniyede kaç adet gönderileceğini belirler.
- max-retries:** Tek bir porta verilen maksimum iletim sayısını belirtir.
- min-hostgroup, -max-hostgroup:** Paralel olarak taranacak minimum ve maksimum host sayısını belirtir.
- min-parallelism, -max-parallelism:** Paralel olarak taranacak minimum ve maksimum prob sayısını belirtir.
- scan-delay, -max-scan-delay:** Tarama sırasında gönderilen probun vereceği cevabı beklemesi için bir sınırlamadır. Çünkü büyük bir taramada gecikme olması durumunda tarama süresi uzayabilir.
- defeat-rst-ratelimit:** Yalnızca açık portlara önem verildiğinde kullanışlıdır. Bu parametre kullanılarak hız sınırlamaları göz ardı edilir. Taramalarda RST cevabı için uzun bir süre beklenmediğinde, bazı portların yanıt vermeyeceği için doğruluğu azaltabilir.
- defeat-icmp-ratelimit:** Hız için doğruluk sunan bir parametre olup ICMP hata mesajlarını hızlandıran hostlara karşı UDP tarama hızını arttırır. Yanıt vermeyen portları varsayılan olarak open|filtered yerine close|filtered olarak işaretler.
- nsock-engine epoll|kqueue|poll|select:** Bir nsock IO multiplexing motorunun kullanımını sağlamaktadır. “**nmap -V**” parametresi ile hangi motorların desteklediğini görülebilir.

## Nmap Performansının Optimize Edilmesi

Nmap aracı ile büyük ağlarda tarama yapılrken performansın optimize edilmesi gerekmektedir. Optimize işlemi iyi yapıldığı sürece kısa sürede sonuçlar elde edilebilir. Bunun en önemli yollarından biri, **-sN** parametresi kullanılarak açık hostların önceden tespit edilmesidir. Böylece ağıdaki kapalı hostlara yönelik gereksiz port taramaları yapılmayıp, taramanın hızlı ve kısa sürede sonuçlanması sağlanır. Nmap aracı varsayılan olarak en yaygın 1000 portu taramaktadır. Gereksiz port taramalarının önüne geçmek için **-p**, **-F** ve **-top-ports** parametreleri kullanılabilir. **-A** parametresi ile yapılacak agresif taramalarda işletim sistemi tespiti, servis versiyon tespiti, traceroute, port taraması gibi işlemler yapılmaktadır. Bu taramalarda **-osscan-limit** ve **-max-os-tries** gibi parametreler kullanılarak işletim sistemi tespitinin defalarca kez tekrarlanmasıının önüne geçilebilir. Gerekmediği sürece DNS çözümlemesi işleminin yapılmaması için **-n** parametresi kullanılabilir. Ayrıca ping atılmadan tarama yapılması istenildiğinde **-Pn** parametresi kullanılabilir.

Taramaların zamanında bitmesi ve sonuç üretmesi için **-T** parametresi ile belirtilen zamanlama şablonları kullanılabilir. UDP taraması yapılması durumunda TCP taraması ile beraber yapılmaması daha uygundur. Çünkü TCP taramasında ICMP hata oranı sınırlaması ile karşılaşılabilir. Önemli noktalardan biri de Nmap aracının güncel tutulması gerekmektedir. Çünkü, Nmap geliştiricileri aracı her geçen gün geliştirip optimize çalışmaları yapmaktadır. Son olarak band genişliği ve CPU'nun arttırılması, nmap aracı üzerindeki iş yükünü azaltmak için kullanılabilir.

## Zamanlama Şablonları (-T)

Nmap aracı ile taramalardaki zamanlama ayarları -T parametresi kullanılarak ayarlanabilmektedir. Hedef ağa yönelik nasıl bir tarama gerçekleştirmek istersek ona göre -T parametresine değer veriyoruz. Bu tür işlemler şablonlar haline getirilmiştir. Toplamda 6 şablon bulunmaktadır. Bunlar, **paranoid(0)**, **sneaky(1)**, **polite(2)**, **normal(3)**, **aggressive(4)** ve **insane(5)** olarak adlandırılır. Bu şablonlar -T parametresi ile kullanılmaktadır.

Şekil 4.6.a – T parametresinin Kullanımı

```
root@priviasecurity:~/Desktop# nmap -sV -T4 -n 192.168.16.160
Starting Nmap 7.50 ( https://nmap.org ) at 2019-02-16 07:10 EST
Nmap scan report for 192.168.16.160
Host is up (0.00078s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
3389/tcp   open  ms-wbt-server Microsoft Terminal Service
MAC Address: 00:0C:29:A1:79:1C (VMware)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 13.45 seconds
```

Şekil 4.6.a'da -T parametresinin agresif modu kullanıldı. Bu mod ile -sV parametresi kullanılarak sürüm tespit yapılır. -n parametresinin kullanımı ile DNS çözümlemesi yapılmamıştır. Böylece taramanın sonuçlanması için gereken zaman kısalır.

Polite(2) mod, daha az bant genişliği kullanmak ve makine kaynaklarını hedeflemek için taramayı yavaşlatmaktadır. Normal(3) mod, -T3 olarak gösterilip zamanlama ayarlaması için herhangi bir özelliği tetiklemez. Aggressive(4) mod, oldukça hızlı olup güvenilir bir ağda tarama yapıyormuş gibi taramaları hızlandırır. Insane(5) mod ise, olağanüstü hızlı bir ağda olduğunuzu veya hız için kesin bir hassasiyetten ödün vermeye istekli olduğunuzu varsayılmaktadır. Bu şablonlar kullanıcının Nmap'in tam zamanlama değerlerini seçmesini sağlarken ne kadar agresif olmak istediklerini belirlemesini sağlar. Şablonlar ayrıca hassas kontrol seçeneklerinin bulunmadığı bazı küçük hız ayarlamaları da yapar. Örneğin, -T4, TCP taramaları için dinamik tarama gecikmesinin 10 ms'yi geçmesini ve bu değeri 5 ms'de -T5 büyülüklüğü ile yasaklamaktadır. Şablonlar, ince ayarlı kontrollerle birlikte kullanılabilir ve ayrıntılı parametreler bu belirli değerler için genel zamanlama şablonlarını geçersiz kılmaktadır. Oldukça modern ve güvenilir ağılar taranırken -T4 kullanılabilir.

Şekil 4.6.b -T parametresine yönelik Şablonları Gösterimi

	T0	T1	T2	T3	T4	T5
Name	Paranoid	Sneaky	Polite	Normal	Aggressive	Insane
min-rtt-timeout	100	100	100	100	100	50
max-rtt-timeout	300,000	15,000	10,000	10,000	1,250	300
initial-rtt-timeout	300,000	15,000	1,000	1,000	500	250
max-retries	10	10	10	10	6	2
Initial (and minimum) scan delay ( --scan-delay )	300,000	15,000	400	0	0	0
Maximum TCP scan delay	300,000	15,000	1,000	1,000	10	5
Maximum UDP scan delay	300,000	15,000	1,000	1,000	1,000	1,000
host-timeout	0	0	0	0	0	900,000
min-parallelism	Dynamic, not affected by timing templates					
max-parallelism	1	1	1	Dynamic	Dynamic	Dynamic
min-hostgroup	Dynamic, not affected by timing templates					
max-hostgroup	Dynamic, not affected by timing templates					
min-rate	No minimum rate limit					
max-rate	No maximum rate limit					
defeat-rst-ratelimit	Not enabled by default					

## SERVİS VE UYGULAMA SÜRÜM TESPİTİ

Nmap aracının en önemli özelliklerinden biri port tarama işlemidir. Port tarama işlemi sonucunda elde edilen açık portlara yönelik güvenlik açıklarının olup olmadığını tespit etmek için, öncelikle açık port üzerinde çalışan servislerin veya uygulamaların tespit edilmesi gerekmektedir. Nmap aracının önemli özelliklerinden biri de servis ve uygulama sürüm tespitidır. Tarama yapılan bir ağ üzerindeki makinelerde bulunan servislerin ve uygulamaların sürüm bilgilerinin tespiti için **-sV** parametresi kullanılmaktadır. Ayrıca bu parametre dışında **-A** parametresi ile yapılan agresif taramanın içerisinde de **-sV** parametresi kullanılır. Şekil 5.a ve 5.b üzerinde **-sV** parametresi ve **-A** parametresi arasındaki fark uygulamalı olarak görülmektedir.

Şekil 5.a – **-sV** Parametresinin Kullanımı

```
root@priviasecurity:~# nmap -sV -T4 localhost

Starting Nmap 7.50 ( https://nmap.org ) at 2019-02-16 12:59 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000030s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
3001/tcp  open  http    Thin httpd

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.73 seconds
```

Şekil 5.b -**A** Parametresinin Kullanımı

```
root@priviasecurity:~# nmap -A -T4 localhost

Starting Nmap 7.50 ( https://nmap.org ) at 2019-02-16 13:02 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000018s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
3001/tcp  open  http    Thin httpd
| http-robots.txt: 1 disallowed entry
|_/
| http-server-header: thin
| http-title: Metasploit - Setup and Configuration
|_Requested resource was http://localhost:3001/users/new
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.8 - 4.9
Network Distance: 0 hops
```

Nmap portun açık olup olmadığını tespit ettikten sonra tespit ettiği porta bağlanmaktadır. Bu bağlantı sonucunda Nmap, bağlandığı portu beş saniye dinlemektedir. Böylece portta herhangi bir servis çalıştığını tespit etmektedir. Çünkü FTP, SSH, SMTP, Telnet, POP3 ve IMAP sunucuları dahil olmak üzere birçok servis, kendilerini ilk açılış banner'ında tanımlamaktadır. Nmap bu durumu "Null Probe" olarak adlandırmaktadır. Çünkü Nmap herhangi bir probe verisi göndermeden gelen yanıtları dinlemektedir. Herhangi bir veri alındığında, Nmap-service-probes dosyasındaki 3.000 tane NULL probe imzası ile karşılaştırılır. İmzalardaki düzenli ifadeler, alınan yanıtta sürüm numaralarını seçmek için alt dizilim eşleşmeleri içerebilir. Bu işlemler biraz zaman alabilir. Çünkü Nmap her probun sonucu için 5 saniye beklemektedir. Problardan bir tanesi hedef portun SSL kullanıp kullanmadığını test etmek için kullanılır. OpenSSL varsa, Nmap SSL üzerinden bağlanıp şifrelemenin ardından neyin dinlediğini belirlemek için servis taramasını yeniden başlatmaktadır.

Nmap'in hangi probu kullanacağı Precise Algoritmasının kullanılmasıyla belirlenmektedir. TCP için ilk önce NULL probu denenmektedir. Nadir bir değere sahip olan veya tamamının mevcut olan yoğunluk değerine eşit olan probalar, Nmap-service-probe'un belirlediği sıraya göre denemektedir. Bir probe'un eşleştiği tespit edildiğinde, algoritma sonra erer ve sonuç bildirilir. Sürüm tespitinde, belirtilen yoğunluk seviyesi ne kadar yüksek olursa, denenecek prob sayısı o kadar yüksek olur. Nmap'in varsayılan yoğunluk seviyesi 7'dir.

Şekil 5.c –**version-intensity** Parametresinin Kullanımı

```
root@priviasecurity: ~/Desktop
File Edit View Search Terminal Help
root@priviasecurity:~/Desktop# nmap -sV --version-intensity 3 -v 192.168.16.128
Starting Nmap 7.50 ( https://nmap.org ) at 2019-02-21 09:25 EST
NSE: Loaded 41 scripts for scanning.
Initiating ARP Ping Scan at 09:25
Scanning 192.168.16.128 [1 port]
Completed ARP Ping Scan at 09:25, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:25
Completed Parallel DNS resolution of 1 host. at 09:25, 0.26s elapsed
Initiating SYN Stealth Scan at 09:25
Scanning 192.168.16.128 [1000 ports]
Discovered open port 139/tcp on 192.168.16.128
Discovered open port 3306/tcp on 192.168.16.128
Discovered open port 445/tcp on 192.168.16.128
Discovered open port 23/tcp on 192.168.16.128
Discovered open port 21/tcp on 192.168.16.128
```

Şekil 5.c'de sürüm taramasında yoğunluk değeri 0 ile 9 arasında verilen değer ile ayarlanabilir. Yoğunluk değeri 0 olarak atanırsa, yalnızca NULL probu (TCP için) ve portu varsayılan bir port olarak listeleyen prob taraması yapılır. Ayrıca “–version-light” parametresinin kullanılması yoğunluk değerinin 2 olması ile eşdeğerdir. Yoğunluk seviyesinin 9 olarak ayarlanması için ise, “–version-all” parametresi kullanılabilir. Böylece bütün problar denenmektedir. Yalnız servis tespiti uzun sürmektedir.

Nmap ile gerçekleştirilen taramada –sV parametresi ile servis sürüm tespiti, -T4 parametresi ile zamanlama ayarlaması, -F parametresi ile popüler 100 port taraması, -d parametresi ile debug modda çalışma yapılır. Ayrıca –version-trace parametresi kullanılarak sürüm tespiti sırasında işlemleri ekrana detaylı basar. Şekil 5.d'de gösterilmektedir.

Şekil 5.d – Tarama teknlığında –version-trace ve debugging kullanımı

```
root@priviasecurity: ~/Desktop
File Edit View Search Terminal Help
root@priviasecurity:~/Desktop# nmap -sSV -T4 -F -d --version-trace -n 192.168.16.128
Starting Nmap 7.50 ( https://nmap.org ) at 2019-02-21 09:38 EST
Fetchfile found /usr/bin/../share/nmap/nmap-services
PORTS: Using top 100 ports found open (TCP:100, UDP:0, SCTP:0)
Fetchfile found /usr/bin/../share/nmap/nmap.xsl
The max # of sockets we are using is: 0
----- Timing report -----
hostgroups: min 1, max 100000
rtt-timeouts: init 500, min 100, max 1250
max-scan-delay: TCP 10, UDP 1000, SCTP 10
parallelism: min 0, max 0
max-retries: 6, host-timeout: 0
min-rate: 0, max-rate: 0
----- Settings -----
NSE: Using Lua 5.3.
Fetchfile found /usr/bin/../share/nmap/nse_main.lua
Fetchfile found /usr/bin/../share/nmap/nselib/lpeg-utility.lua
Fetchfile found /usr/bin/../share/nmap/nselib/stdnse.lua
Fetchfile found /usr/bin/../share/nmap/nselib/strict.lua
Fetchfile found /usr/bin/../share/nmap/scripts/script.db
```

Şekil 5.d'de SYN taraması sonucu 100 tane açık port tespit edilmiştir. Açık portların tespit edilmesinden sonra paralel olarak her bir porta yönelik servis taraması başlatılacaktır. Şekil 5.3'de NULL probu ile TCP bağlantı isteğiinde bulunulduğu gösterilmektedir.

Şekil 5.e – NULL probu için TCP bağlantısı

```
root@priviasecurity: ~/Desktop
File Edit View Search Terminal Help
Scanning 18 services on 192.168.16.128
NSOCK INFO [2.4620s] nsock_iod_new2(): nsock_iod_new (IOD #1)
Starting probes against new service: 192.168.16.128:21 (tcp)
NSOCK INFO [2.4630s] nsock_connect_tcp(): TCP connection requested to 192.168.16.128:21 (IOD #1) EID 8
NSOCK INFO [2.4630s] nsock_iod_new2(): nsock_iod_new (IOD #2)
Starting probes against new service: 192.168.16.128:22 (tcp)
NSOCK INFO [2.4630s] nsock_connect_tcp(): TCP connection requested to 192.168.16.128:22 (IOD #2) EID 16
NSOCK INFO [2.4630s] nsock_iod_new2(): nsock_iod_new (IOD #3)
Starting probes against new service: 192.168.16.128:23 (tcp)
NSOCK INFO [2.4630s] nsock_connect_tcp(): TCP connection requested to 192.168.16.128:23 (IOD #3) EID 24
NSOCK INFO [2.4630s] nsock_iod_new2(): nsock_iod_new (IOD #4)
Starting probes against new service: 192.168.16.128:25 (tcp)
```

Şekil 5.e'de, NULL prob bağlantıları dört portta bulunan servislere yönelik başarılı bir şekilde uygulanmıştır.

Şekil 5.f – NULL Probunun Kullanıldığı Gösterimi

```
root@priviasecurity: ~/Desktop
File Edit View Search Terminal Help
ID 274 [192.168.16.128:5900] (12 bytes): RFB 003.003.
Service scan match (Probe NULL matched with NULL line 4872): 192.168.16.128:5900
is vnc. Version: |VNC||protocol 3.3|
NSOCK INFO [2.4800s] nsock_iod_delete(): nsock_iod_delete (IOD #16)
NSOCK INFO [2.4800s] nsock_trace_handler_callback(): Callback: READ SUCCESS for E
ID 258 [192.168.16.128:3306] (66 bytes): >seq-5.0.51a-3ubuntu5.....:vf{Z1%.,.....
.....dHyJF_-_ydfv.
Service scan match (Probe NULL matched with NULL line 2178): 192.168.16.128:3306
is mysql. Version: |MySQL|5.0.51a-3ubuntu5||
NSOCK INFO [2.4800s] nsock_iod_delete(): nsock_iod_delete (IOD #14)
NSOCK INFO [2.4830s] nsock_trace_handler_callback(): Callback: READ SUCCESS for E
ID 154 [192.168.16.128:21] (20 bytes): 220 (vsFTPd 2.3.4)..
Service scan match (Probe NULL matched with NULL line 760): 192.168.16.128:21 is
ftp. Version: |vsftpd|2.3.4|||
NSOCK INFO [2.4830s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [2.4840s] nsock_trace_handler_callback(): Callback: READ SUCCESS for E
ID 250 [192.168.16.128:2121] (59 bytes): 220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.16.128]..
Service scan match (Probe NULL matched with NULL line 716): 192.168.16.128:2121 i
is ftp. Version: |ProFTPD|1.3.1|||
```

Şekil 5.f'de NULL probe kullanılarak FTP servisinin sürüm bilgisi tespit edilmiştir.

Şekil 5.g – SMTP sürüm keşfi

```
root@priviasecurity: ~/Desktop
File Edit View Search Terminal Help
170 [192.168.16.128:23] (12 bytes): ..... .#...
Service scan match (Probe NULL matched with NULL line 3862): 192.168.16.128:23 is t
elnet. Version: |Linux telnetd|||
NSOCK INFO [2.5140s] nsock_iod_delete(): nsock_iod_delete (IOD #3)
NSOCK INFO [2.5170s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID
178 [192.168.16.128:25] (55 bytes): 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)..
Service scan match (Probe NULL matched with NULL line 3056): 192.168.16.128:25 is s
mtp. Version: |Postfix smtpd|||
NSOCK INFO [2.5170s] nsock_iod_delete(): nsock_iod_delete (IOD #4)
NSOCK INFO [2.5200s] nsock_trace_handler_callback(): Callback: READ_EOF for EID 234
```

Şekil 5.g'de 25 numaralı portta posta sunucusunun tespit edildiği gösterilmiştir. Normal şartlarda ne tür bir posta sunucusu olduğu bilinmemektedir. Dikkatli bakıldığından posta sunucusunun sürüm bilgisi olarak ESMTP Postfix olduğu

görmektedir. Nmap, SMTP ile eşleştiği için yalnızca SMTP sunucularını eşleştirebilen problemler denenir.

Nmap'te, **-sV** parametresi ile sürüm tespiti yapılırken sürüm tespiti sırasında nelerin yapıldığını detaylı olarak görüntülemek için **“-version-trace”** parametresi kullanılır.

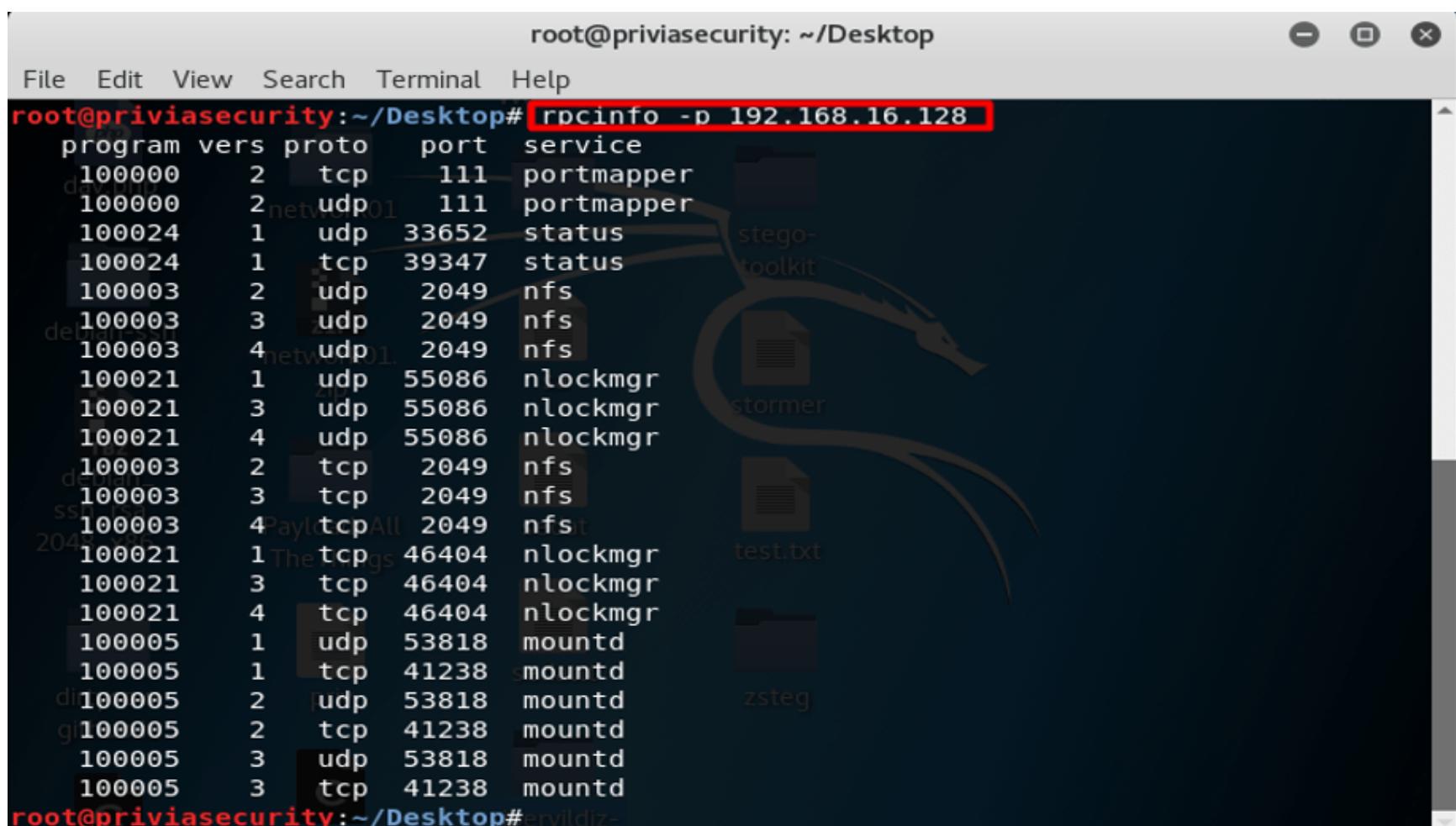
## Post-Processors

Açık portların tespit edilmesi ve açık portların üzerinde çalışan servislerin sürüm bilgilerinin tespit edilmesi dışında Nmap'in sunduğu ek hizmetler bulunmaktadır. Bu hizmetlerden bazıları, PRC Grinding ve SSL tünellemedir.

## RPC Grinding

SunRPC (Sun Remote Procedure Call), NFS dahil birçok hizmetin çalışması için kullanılan ortak bir Unix protokolüdür. Nmap'in içerisinde nmap-rpc veritabanı bulunmaktadır. Birçok RPC hizmeti yüksek numaralı portları veya UDP protokolünü kullanmaktadır. RPC Grinding, kötü yapılandırılmış güvenlik duvarlarını atlatmak için kullanılabilir. RPC hizmeti üzerinde uzaktan kontrol edilip kod çalıştırılabilen kritik güvenlik açıkları bulunmaktadır.

Şekil 5.1.1 – Rpcinfo ile RPC servisine yönelik bilgi elde edilmesi



```
root@priviasecurity:~/Desktop# rpcinfo -p 192.168.16.128
program vers proto port service
 100000    2    tcp   111  portmapper
 100000    2    udp  111  portmapper
 100024    1    udp  33652  status
 100024    1    tcp  39347  status
 100003    2    udp   2049  nfs
 100003    3    udp   2049  nfs
 100003    4    udp   2049  nfs
 100021    1    udp  55086  nlockmgr
 100021    3    udp  55086  nlockmgr
 100021    4    udp  55086  nlockmgr
 100003    2    tcp   2049  nfs
 100003    3    tcp   2049  nfs
 100003    4    tcpAll 2049  nfs
 100021    1    tcp  46404  nlockmgr
 100021    3    tcp  46404  nlockmgr
 100021    4    tcp  46404  nlockmgr
 100005    1    udp   53818  mountd
 100005    1    tcp   41238  smountd
 100005    2    udp   53818  mountd
 100005    2    tcp   41238  mountd
 100005    3    udp   53818  mountd
 100005    3    tcp   41238  mountd
root@priviasecurity:~/Desktop#
```

Şekil 5.1.1'da hostların birçok RPC hizmetini sunduğunu ve bu hizmetlerin kötüye kullanılma ihtimalinin yüksek olduğu görülmektedir. RPC hizmeti bilgileri çok hassas olduğundan dolayı birçok ağ yöneticisi 111 numaralı portu engelleyerek hassas bilgileri gizlemek ister. Nmap aracı üç adımda diğer RPC portları ile iletişime geçerek hassas bilgileri elde edebilir. Bunun için TCP/UDP port taraması yaparak açık portlar tespit etmelidir. Sürüm tespiti yapılarak, açık portlardan RPC hizmeti kullanan portları belirlemek gerekmektedir. Son olarak RPC Bruteforce Engine kullanılarak Nmap, içerisindeki nmap-rpc veritabanındaki RPC hizmetlerine ait bilgileri sırasıyla RPC hizmetinin çalıştığı açık portlara denemektedir.

## SSL Tünelleme

Nmap, SSL şifreleme protokolünü tespit etme ve ardından sürüm tespitini gerçekleştiren şifreli bir oturum başlatma özelliğine sahiptir.

Şekil 5.1.2 – SSL için servis taraması

```
root@priviasecurity: ~
File Edit View Search Terminal Help
root@priviasecurity:~# nmap -Pn -sSV -T4 -p http,https 192.168.16.128
masa2      masa
Starting Nmap 7.50 ( https://nmap.org ) at 2019-02-23 11:58 EST
Nmap scan report for 192.168.16.128
Host is up (0.00026s latency).

PORT      STATE SERVICE VERSION
80/tcp      open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
443/tcp     closed https
8008/tcp    closed http
MAC Address: 00:0C:29:9C:96:DD (VMware)
```

Şekil 5.1.2'de gerçekleştirilen tarama sonucunda SSL kullanıldığı tespit edilmiştir. Nmap aracının, SSL kullanıldığını tespit etmemesi durumunda "SERVICE" bölümünde "ssl/unknown" olarak belirtilir. Nmap, SSL tespiti için OpenSSL kütüphanelerini ücretsiz olarak kullanmaktadır.

## İŞLETİM SİSTEMİ TESPİTİ

Yapılan güvenlik taramalarında açık portların bulunup üzerinde çalışan servisler tespiti dışında işletim sistemi tespiti de büyük bir önem arz etmektedir. Çünkü yapılan bir güvenlik tespitinde keşif ve bilgi toplama evresi önemlidir. İşletim sisteminin adı, sürümü vb. bilgilerin tespit edilmesi, hedef sistem üzerinde bulabilecek güvenlik açıklarının daha kolay tespit edilmesini sağlamaktadır. Güvenlik testlerinde uzmanlar tarafından güvenlik açıkları tespit edilip hedef sistemler ele geçirilmektedir. Ardından raporlanıp sistemden sorumlu yöneticiye bildirilmektedir. Hedef sistem hakkında elde edilen işletim sistemi bilgilerini bir saldırganın elde etmesiyle birlikte sistem üzerinde tespit ettiği güvenlik açıklarını kullanarak sistemlere zarar verebilir. Bundan dolayı, işletim sistemi ile ilgili bilgilerin ifşası önemsiz görülselise bile sistemi ele geçirmeye kadar ki sürecin bir başlangıcıdır.

- İşletim sistemi tespit etmenin nedenleri aşağıdaki gibidir:
- Hedef sistemin güvenlik açıklarını belirlemek
- Exploit Uyarlaması yapmak
- Ağ envânteri ve desteğinin belirlenmesi
- Yetkisiz ve tehlikeli cihazların tespit edilmesi
- Sosyal mühendislik

İşletim sistemi tespiti için -O parametresi kullanılmaktadır.

Şekil 6.a – İşletim Sistemi Tespitinin Yapılması

```
root@priviasecurity: ~
File Edit View Search Terminal Help
root@priviasecurity:~# nmap -O -v www.priviasecurity.com
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-28 13:39 EST
Initiating Ping Scan at 13:39
Scanning www.priviasecurity.com (104.18.40.10) [4 ports]
Completed Ping Scan at 13:39, 0.05s elapsed (1 total hosts)
Initiating OS detection (try #1) against www.priviasecurity.com (104.18.40.10)
Nmap scan report for www.priviasecurity.com (104.18.40.10)
Host is up (0.0089s latency).
Other addresses for www.priviasecurity.com (not scanned): 104.18.41.10 2606:4700:30::68
12:280a 2606:4700:30::6812:290a
Not shown: 997 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp  open  http-proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open and
1 closed port
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4.37
OS details: DD-WRT v24-sp2 (Linux 2.4.37)
TCP Sequence Prediction: Difficulty=251 (Good luck!)
IP ID Sequence Generation: Incremental
```

**Device type** bölümü, router, yazıcı, güvenlik duvarı veya general purpose gibi bir veya daha fazla üst düzey aygıtları sınırlayabilir. **Running** bölümünde, işletim sistemi ailesini (Windows/Linux) ve varsa işletim sistemini (10/2.4.X) göstermektedir. Birden fazla işletim sistemi ailesi varsa aralarına virgül koyularak gösterilmektedir. Herhangi bir eşleştirme olmadığı bir durumda ise, **Running** bölümü JUST GUESSING olarak değiştirilir. Genelde her işletim sistemi ailesinin sonunda doğruluk yüzdeliği eklenmektedir. **OS CPE** bölümünde, işletim sisteminin Common Platform Enumeration (CPE) temsili gösterilmektedir. Ayrıca donanım türünün CPE temsiline sahip olabilir. İşletim sistemi CPE'si cpe:/o ile başlarken donanım CPE'si cpe:/h ile başlamaktadır. **OS Details** bölümünde, eşleşen her fingerprint için ayrıntılı açıklama sağlanmaktadır. **TCP Sequence Prediction** bölümünde, TCP başlangıç sıra numarası zayıf olan sistemler, TCP spoofing saldırılara karşı savunmasızdır. Bu sistemler ile bağlantı kurulabilir ve farklı IP adresini taklit ederek veri gönderebilirler. **IP ID Sequence Generation** bölümünde, birçok sistem istemeden IP paketlerinde 16 bitlik ID alanını nasıl oluşturduklarına bağlı olarak trafik seviyeleri hakkında hassas bilgileri verir. Bu alan Nmap'in ayırt edebildiği ID oluşturma algoritmasını açıklamaktadır. **Uptime Guess** bölümünde, işletim sistemi tespitinin bir parçası olarak, Nmap üst üste birkaç SYN/ACK TCP paketi alır ve üst bilgileri zaman damgası seçeneği olup olmadığını denetlemektedir. **Network Distance** bölümü, Nmap'in hedef host ile bağlantı kurarken kaç tane yönlendirici ve host üzerinden geçtiğini gösterir. İşletim sistemi tespiti taramalarında hedef sistemlere yönelik taramaların sınırlanması “–osscan-limit” parametresi kullanılarak sağlanmaktadır. İşletim sistemi tespitinde, en az bir açık ve bir kapalı TCP portu bulunursa daha etkili olur. Nmap, bu kurallara uymayan hostlara karşı işletim sistemi tespitini gerçekleştirmez. Bu durum –PN taramalarında birok hosta karşı önemli ölçüde zaman kazandırmaktadır.

Şekil 6.b – (–osscan-limit) parametresinin kullanılması

```
root@priviasecurity:~# nmap -O --osscan-limit -n 192.168.16.128
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-01 10:47 EST
Nmap scan report for 192.168.16.128
Host is up (0.00073s latency).
Not shown: 94 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
MAC Address: 00:0C:29:9C:96:DD (VMware)
Device type: general purpose
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
```

Şekil 6.b'de gösterildiği gibi **--osscan-limit** parametresi kullanılarak bir tarama gerçekleştirilmiştir. İşletim sistemi tespitine yönelik taramalarda bazen işletim sistemi eşleştirmesi gerçekleşmemektedir. Bu durumlarda **--osscan-guess** veya **--fuzzy** parametreleri kullanılarak işletim sistemine en yakın sonuç tahmin edilmektedir. Tahminin güven düzeyi yüzdelik olarak verilmektedir.

Şekil 6.c – (–fuzzy) parametresinin kullanılması

```
root@priviasecurity:~# nmap -O --fuzzy -n 192.168.16.128
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-01 10:47 EST
Nmap scan report for 192.168.16.128
Host is up (0.00048s latency).
Not shown: 94 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
MAC Address: 00:0C:29:9C:96:DD (VMware)
Device type: general purpose
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
```

Şekil 6.c'de gösterildiği gibi **--fuzzy** parametresi kullanılmıştır. Fakat bu parametre tek bir hosta gerçekleştirilmiş olup işletim sistemi eşleştirmesi yapılmıştır. Eğer işletim sistemi eşleştirmesi yapılmamasaydı, parametrenin gereği olarak en yakın sonuç güven düzeyi yüzdeliğiyle görüntülenecekti.

Hedef sisteme karşı maksimum işletim sistemi tespiti deneme sayısını belirlemek için **--max-os-tries** parametresi kullanılmaktadır. Nmap bir sisteme karşı işletim sistemi tespiti taraması gerçekleştirdiğinde, sistem ile ilgili bir eşleşme bulmadığında genellikle girişimi tekrarlamaktadır. Değeri düşük vermek taramayı hızlandıracaktır. Fakat işletim sistemini tanımlayabilen denemeler azalacaktır.

Şekil 6.d – (–max-os-tries) parametresinin kullanılması

```
root@priviasecurity:~# nmap -O --max-os-tries 10 -n 192.168.16.128
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-01 10:56 EST
Nmap scan report for 192.168.16.128
Host is up (0.00052s latency).
Not shown: 94 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
MAC Address: 00:0C:29:9C:96:DD (VMware)
Device type: general purpose
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
```

Şekil 6.d'de işletim sistemi tespiti için yapılacak olan deneme sayısı maksimum 10 olarak ayarlanmıştır.

## TCP/IP Fingerprinting Yöntemleri

Nmap OS fingerprinting, hedef makinenin bilinen açık ve kapalı portlarına 16'ya kadar TCP, UDP ve ICMP protollerini göndererek çalışmaktadır. Bu protoller, standart protokol RFC'lerinde çeşitli belirsizliklerden yararlanmak için özel olarak tasarlanmıştır. Nmap, protoller gönderdikten sonra dönen cevapları dinlemektedir. Dönen cevaplardaki nitelikler analiz edilir ve fingerprint oluşturmak için birleştirilir. Her prob paketi en az bir kez izlenir ve cevap verilemezse tekrar gönderilir. Tüm paketler, rastgele bir IP ID değerine sahip IPv4'tür. Açık bir TCP portuna giden protoller, eğer böyle bir port bulunamamışsa port atlanır. Kapalı TCP veya UDP portları için Nmap ilk önce böyle bir portun bulunup bulunmadığını kontrol etmektedir.

## IPv6 Fingerprinting Yöntemleri

Nmap, IPv6 için gelişmiş benzer ancak ayrı bir işletim sistemi tespiti motoruna sahiptir. Genellikle teknik açıdan aynıdır. Protoller gönderilip yanıtlar alınır. Alınan yanıtlar veritabanı ile karşılaştırılır. Farklılıklar kullanılan spesifik protollerde ve eşleştirme tarzlarında mevcuttur. IPv6 OS tespiti, IPv4 gibi kullanılır. Sadece -6 ve -O parametreleri birlikte kullanılmalıdır.