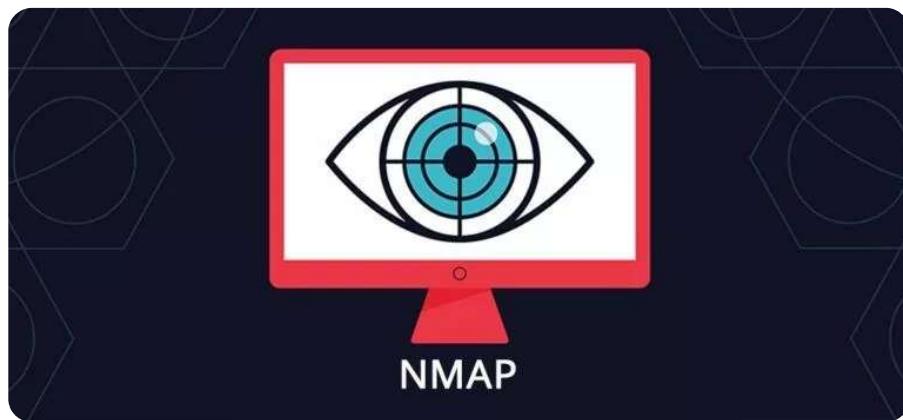


Kurumunuza Özel **Sızma Testi Pentest Hizmeti İndirim Fırsatı!**



Nmap Nedir? – Temel ve İleri Seviye – Part 2

28/01/2020



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 çıktıların 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 bulunduğuunu belirten 8 bitlik bir alandır. IPv4 adresleri 32 bit uzunlığında 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 kullandığı port numarasıdır.

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

Port 443 (HTTPS): Varsayılan olarak kullanılan HTTP protokolünün SSL ile şifrelerek iletişimin sağlanması ile güvenliği arttırmaktadır. 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 iletişimi 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 porttur.

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 iletilerinin doğrudan sunucu üzerinden yönetilmesini sağlayan bir TCP protokolüdür.

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

Port 993 (IMAPS): IMAPv2 protokolünün daha güvenli iletişimini sağlamaası için 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 yapılmamakte

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

Port 1433 (MSSQL): Microsoft SQL Server veritabanı ile iletişimini 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 sırasında 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 dinlenilip bağlantının güvenli olup olmadığı ve hangi servisler üzerinden işlemler yapılmış yapılmadığı tespit edilmektedir. Portların durumları, aşağıdaki durumlardan oluşmaktadır.

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

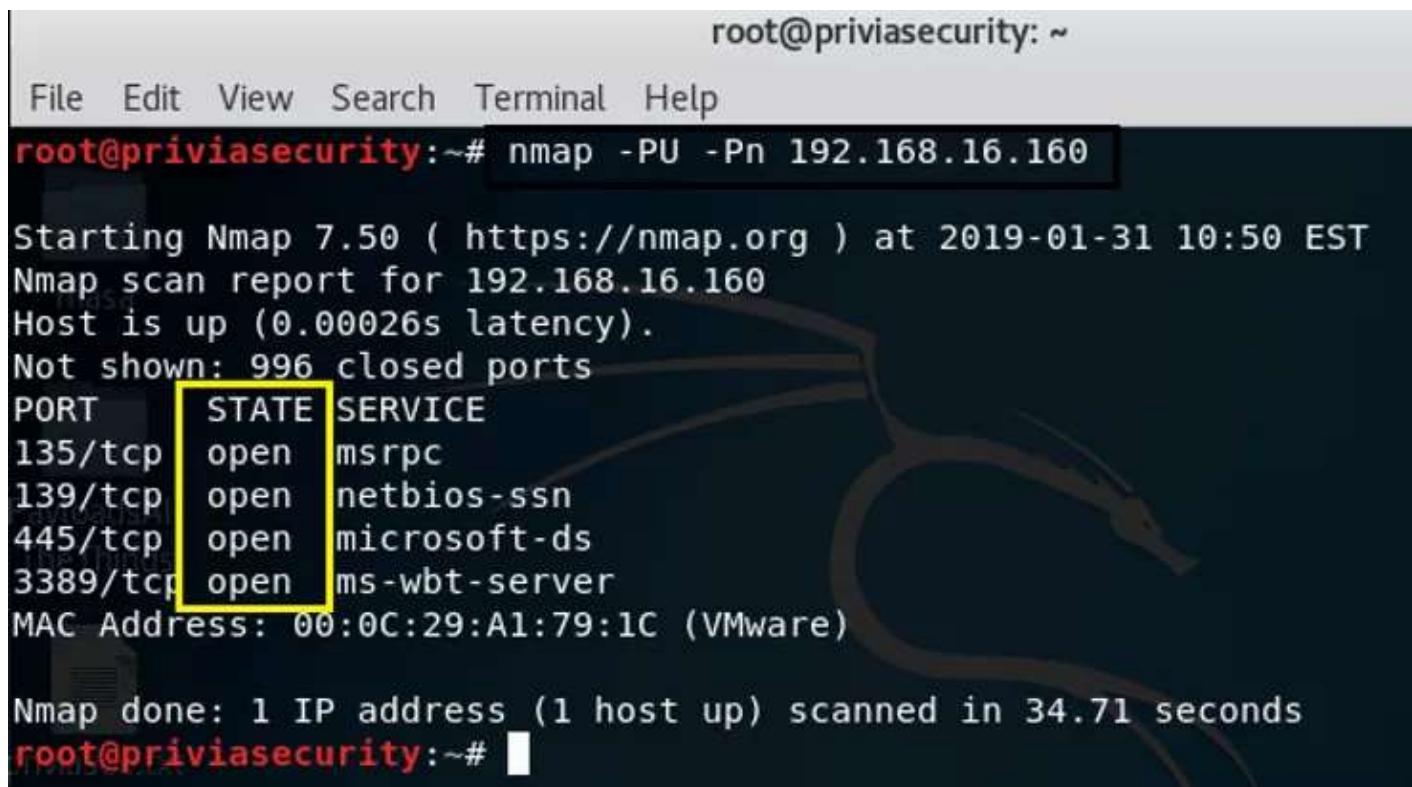
Closed: Portun kapalı olduğunu belirtmektedir.

Filtered: Portun açık olup olmadığı belirlenememektedir. Çünkü paket filtreleme, probalarının 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 olmadığını belirtir.

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



```
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:~#
```

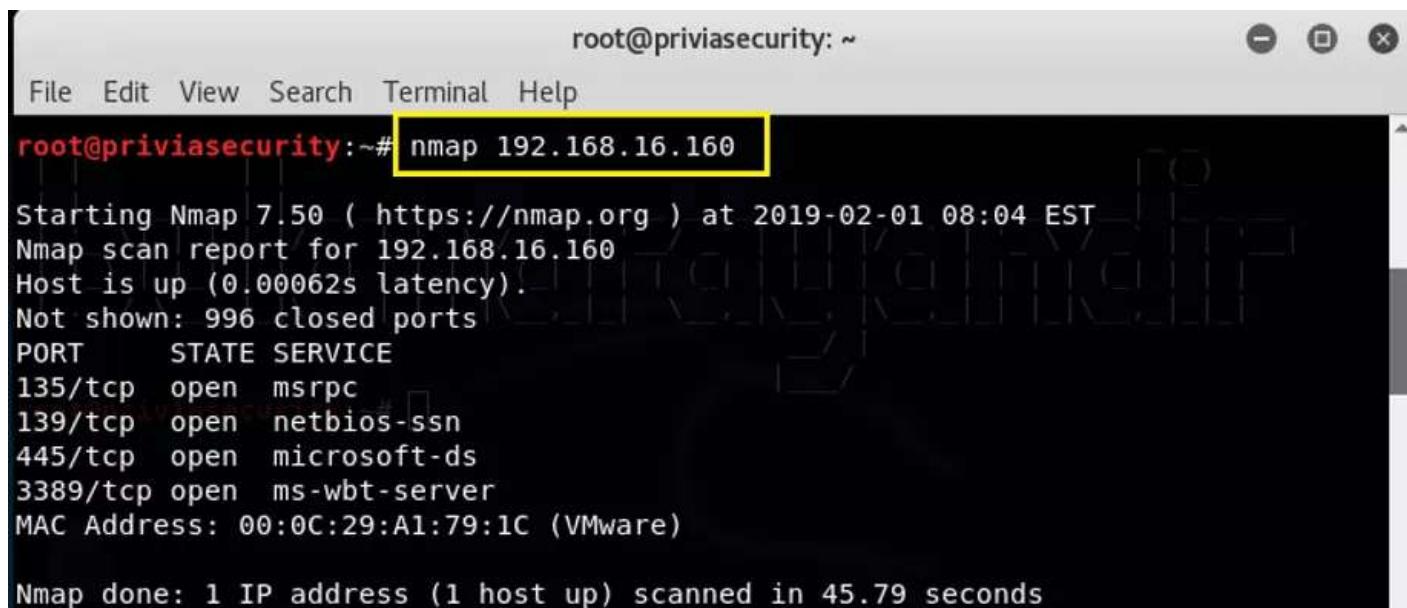
Şekil 4.2 – Portların Durumlarının Görüntülenmesi

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 kullanılmiyorsa, kapatılmalıdır.

Gerçekleştirilen 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 zamanandan tasarruf ederek sonuçlar elde edilir.



The screenshot shows a terminal window titled "root@priviasecurity: ~". The menu bar includes File, Edit, View, Search, Terminal, and Help. The command "nmap 192.168.16.160" is highlighted with a yellow box. The output shows the following information:

```
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)

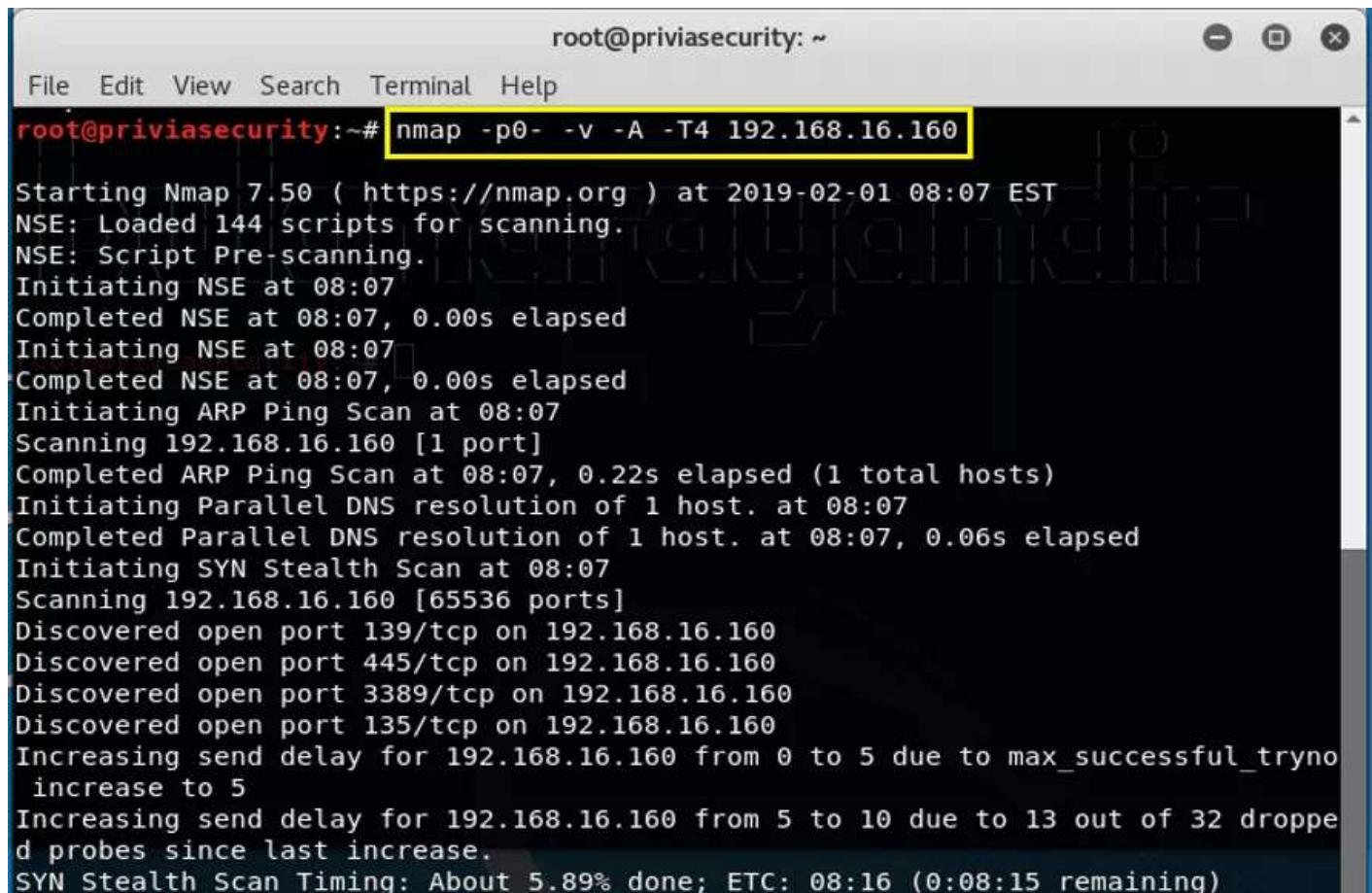
Nmap done: 1 IP address (1 host up) scanned in 45.79 seconds
```

Şekil 4.2.1 – Genel Bir Nmap Taraması

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

görmektedir.

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 taraması saatler alabilir. Çünkü varsayılan 1000 tane portun yerine 65535 tane port taranır.



The screenshot shows a terminal window titled 'root@priviasecurity: ~'. The command entered is 'nmap -p0- -v -A -T4 192.168.16.160'. The output details the scanning process:

```
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 – Nmap Kapsamlı Tarama Örneği

Şekil 4.2.2'de kapsamlı bir nmap taraması gerçekleştirılmıştır. 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 tarama zamanlamasına yönelik kullanılan bir parametredir. -T parametresinin

özelliklerinden biri zaman aşımı özelliğidir. Hedef makinelерden 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 türündür. 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

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 40 filtreli port ve 956 kapalı port tespit edilmiştir. Şekil 4.3.1.b'de 40 tane portun SYN paketine cevap vermediği için filtreli 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 taramamları gerçekleştirilmektedir.

Şekil 4.3.2 – TCP Connect Scan Gösterimi

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 gerçekleştiriliip 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 döndürülürse 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

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 gönderilmektedir. TCP bayrak başlık değeri 0'dır. TCP FIN Scan taraması, `-sF` parametresi kullanılarak TCP FIN bitinin ayarlanmasıyla gerçekleştirilen tarama türündür. TCP Xmas Scan taraması ise `-sX` parametresi kullanılarak FIN, PSH ve URG bayraklarının ayarlanmasıyla gerçekleştirilen tarama türündür.

Tarama türünün en önemli avantajı, durum bildirmeyen güvenlik duvarları ve paket filterleme yönlendiricileri üzerinden gizlice tarama yapmayan olanak 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 SYN taramasına göre daha gizlidir.



Şekil 4.3.4.a – TCP NULL Scan Gösterimi

Şekil 4.3.4.a'da gösterildiği gibi TCP NULL taraması gerçekleştirılmıştır. Bu tarama sonucunda varsayılan 1000 port taramış olup açık portların olmadığı bilgisi elde edilmiştir. Ayrıca -n parametresi kullanılarak Reverse DNS çözümlemesi yapılması istenilmemiştir. -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

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

TCP ACK Scan (-sA)

Durum bilgisi veren güvenlik duvarları, ağ bağlantılarının gezinimini, çalışma durumunu ve karakteristik özelliklerini izleyen güvenlik duvarlarıdır. Bu tarama türü güvenlik duvarı 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 durumuna 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

Şekil 4.3.5'te gösterilen bir TCP ACK Scan tarama türündür. Bu taramanın gerçekleştirilemesi için –sA parametresi kullanılmaktadır. Şekil 4.3.5'te gösterildiği gibi problemlerin bazıları 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

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

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 türündür. 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

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 türündür. Aynı zamanda bu tarama türü yavaş ve karmaşıktır.

Şekil 4.3.8.a – TCP IDLE SCAN Port Durumlarının Gösterimi

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, saldırgan makineye IP ID değeri 31339 olan bir RST bayrağı gönderir.
- Saldırgan makine, zombi makinesindeki IP ID değerinin 2 sayısı kadar arttığını 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, saldırgan 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, saldırgan 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, saldırgan 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 gönd

- Zombi makinesi, saldırgan 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 açısıyla bakıldığından filtrelenmiş 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 yazılmaktadır. –p parametresinin protokol veya port taraması olup olmadığından ayırt edilebilmesi için –sO parametresi kullanılır. –p parametresine atanan protokol 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

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 yapılırken, TCP olup olmadığına bakılmayıp port durumu **open|filtered** olarak işaretlenmiştir. Ayrıca ilk taramada ekstra servis tespiti için parameter girilmesine ihtiyaç duyulmayıp varsayılan olarak protokolün kullanmış olduğu servis hakkında bilgi verir. İkinci taramadaki çıktıda Protokol başlığı yerine varsayılan Port başlığı adı altında **135/TCP** belirtildiğinde 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 koyulur. 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

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 eşdeğерidir. Engellenmeyen bir ağda saniyede binlerce port taranabilir. TCP SYN taraması gibi INIT taraması da SCTR ilişkilerini tamamlamadığı için göze çarpmayan gizli bir taramadır.

Şekil 4.3.11 – SCTP INIT Scan Gösterimi

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 yapılmamış gibi hedefe gösterilerek hedef makineden bir cevap beklenilir. 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 filtreli olduğu 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 filtreli portları birbirinden ayırt edememesidir. Bu durum dışında portun kapalı olması durumunda SCTP INIT taramasındaki gibi bir ABORT cevabı aldığında 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 atıldığı 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 gerçekleştirilir.

Resim 4.3.13 – Özel TCP Taraması Gösterimi

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

Port Seçerek Tarama

Nmap varsayılan olarak port taraması yaptığından 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 gerçekleştiriliyor. Bu parametre ^{–sT} 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 taramasını 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 sıraya görmek için bu parametre kullanılmaktadır.

-port-ration: 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 proların cevap verebilecekleri minimum ve maximum sürelerin ayarlanması için kullanılır. Şekil 4.4.1 üzerinde gösterilmiştir.

Resim 4.4.1 – rtt-timeout Parametrelerinin Gösterimi

-host-timeout: Host başına belirtilen tarama süresidir. Zaman aşımı durumunda tarama iptal edilir.

-min-rate, -max-rate: Taramada kullanılacak proların 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 cevabin beklemesi için bir sınırlamadır. Çünkü büyük bir taramada gecikme olması durumunda tarama süresi uzayabilir.

-defeat-rst-ratelimit: Yalnızca açık portlara önem verildiğinde kullanılmalıdır. 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 arttırmır. 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 ağdaki 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 geçirilebilir. 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

Şekil 4.6.a'da –T parametresinin agresif modu kullanıldı. Bu mod ile –sV parametresi kullanılarak sürüm tespit yapılır. –n parametresinin kullanımı ile DNS çözümlenmesi 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 varsaymaktadır. 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 büyülüğu ile yasaklamaktadır. Şablonlar, ince ayarlı kontrollerle birlikte kullanılabilir ve ayrıntılı parametreler bu belirli değerler için genel

zamanlama şablonlarını geçersiz kılmaktadır. Oldukça modern ve güvenilir ağlar taranırken -T4 kullanılabilir.

Şekil 4.6.b -T parametresine yönelik Şablonları Gösterimi

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

Şekil 5.b -A Parametresinin Kullanımı

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 ver alındığında, Nmap-service-probes dosyasındaki 3.000 tane NULL probe imzası

ile karşılaşılır. 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 eşlestiği 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

Şekil 5.c'de sürüm taramasında yoğunluk değeri 0 ile 9 arasında verilen de ile ayarlanabilir. Yoğunluk değeri 0 olarak atanırsa, yalnızca NULL probu (TCP

icin) 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 probalar 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 tekniğinde –version-trace ve debugging kullanımı

Şekil 5.d’de SYN taraması sonucu 100 tane açık port tespit edilmiştir. Açık portların tespit edilmesinden sonra paralel olarak her bir porta yönelik ser

taraması başlatılacaktır. Şekil 5.3'de NULL probu ile TCP bağlantı isteğinde bulunulduğu gösterilmektedir.

Şekil 5.e – NULL probu için TCP bağlantısı

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

Şekil 5.f – NULL Probünum Kullanıldığı Gösterimi

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

Şekil 5.g – SMTP sürüm keşfi

Şekil 5.g'de 25 numaralı portta posta sunucusunun tespit edildiği gösterilmiştir. Normal şartlarda ne tür bir posta sunucusu olduğu bilinmemektedir. Dikkatli bakıldığında posta sunucusunun sürüm bilgisi olarak ESMTP Postfix olduğu görülmektedir. Nmap, SMTP ile eşleştiği için yalnızca SMTP sunucularını eşleştirebilen problkar 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 tünelleme -“..”

RPC Grinding

SunRPC (Sun Remote Procedure Call), NFS dâhil 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

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 engelleerek 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 k

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

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 açıklarını 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 görülsel 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

Device type bölümü, router, yazıcı, güvenlik duvarı veya general purpose gibi bir veya daha fazla üst düzey aygit türüyle sınıflandırılabilir. **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 sonununda 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'ın 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 sınırlandırılması “–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

Şekil 6.b'de gösterildiği gibi **–osscan-limit** parametresi kullanılarak bir tarar gerçekleştirılmıştır. İşletim sistemi tespitine yönelik taramalarda bazen işlenemeyen

sistemi eşleştirmesi gerçekleşmemektedir. Bu durumlarda “**–osscan-guess**” veya “**–fuzzy**” parametreleri kullanılarak işletim sisteme en yakın sonuç tahmin edilmektedir. Tahminin güven düzeyi yüzdelik olarak verilmektedir.

Şekil 6.c – (–fuzzy) parametresinin kullanılması

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

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 probları göndererek çalışmaktadır. Bu problar, standart protokol RFC’lerinde çeşitli belirsizliklerden yararlanmak için özel olarak tasarlanmıştır. Nmap, problemleri 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 problemler, 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. Problemler gönderilip yanıtlar alınır. Alınan yanıtlar veritabanı ile karşılaştırılır. Farklılıklar kullanılan spesifik problemlerde ve eşleştirme tarzlarında mevcuttur. IPv6 OS tespiti, IPv4 gibi kullanılır. Sadece -6 ve -O parametreleri birlikte kullanılmalıdır.

< **Nmap Nedir?**

> **Nmap Nedir? – Temel ve İleri Seviye – Part 3**

Tel: +90 216 820 14 55

Posta: info@priviasecurity.com

Email Adresiniz

E-Bülten Abonelik

Gizlilik ve Çerez Politikası Bilgi Güvenliği Politikası

Privia Security © 2018 Privacy For You



Automated page speed optimizations for fast site performance