



Nmap Nedir?

27/01/2020



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 arasında yer almaktadır.

NMAP TARAMA AŞAMALARI

Nmap uygulaması kullanılarak taramanın başarılı bir şekilde sonuçlanması için belirli aşamalar takip edilerek tarama işlemleri yapılmalıdır.

Tarama Öncesi Scriptlerin Kullanılması

Nmap aracı, taranacak ağ hakkında bilgi toplamak için scriptler barındırır. Örneğin, ağ servislerinden bilgi almak için broadcast sorgularını kullanan dhcp-discover ve broadcast-dns-service-discover gibi scriptler kullanılmaktadır.

Hedef Numaralandırma

Nmap, hedef numaralandırma işlemlerinde DNS, IP adresleri, CIDR değerleri gibi host belirteçlerini tespit etmektedir. Hedef hostları belirlemek için -iR parametresi kullanılabilir.

Host Keşif İşlemleri

Nmap'te host keşif işlemleri genellikle bir makinenin aktif olup olmadığını tespit etmek için yapılmaktadır. Nmap varsayılan olarak önce host keşfi yapar ve sonra port taramasına başlar. Eğer port taraması yapmadan sadece host keşif işlemi yapılmak isteniyorsa -sn parametresi kullanılır. Host keşif işleminin yapılması istenmiyorsa -Pn parametresi kullanılabilir. -Pn parametresinin kullanılması ile hostlara ping atılmaz. Böylelikle host keşfi yapılmaz.

Reverse-DNS Resolution

Nmap, ping taraması ile tarayıp belirlediği aktif makinelere yönelik Reverse-DNS çözümleme işlemi gerçekleştirilmektedir. Reverse-DNS çözümlemesi, -R parametresi ile yapılır. Normal şartlarda yalnızca açık makinelere yapılır.

Port Taraması

Port taraması, Nmap aracının ana işlevlerinden biridir. Aktif olan bir sistemin portlarına istek atarak, portların açık veya kapalı olma durumunu tespit eder.

Versiyon Tespiti

Tespit edilen açık portlarda hangi servisin çalıştığının tespiti için kullanılır. Nmap aracı içerisinde barındırmış olduğu problemler ve 6500'den fazla servis imzası ile portlarda bulunan servisleri karşılaştırıp tespit etmektedir. Bu işlem -sV parametresi kullanılarak gerçekleştirilmektedir.

İşletim Sistemi Tespiti

Nmap ile açık olan makinelere yönelik işletim sistemi tespiti yapılmaktadır. Nmap içerisinde bulunan bir veritabanında işletim sistemlerinin yanıtları bulunmaktadır. Nmap oluşturmuş olduğu problemleri makinelere göndererek makinelerden gelen yanıtları veritabanında bulunan yanıtlarla karşılaştırılmaktadır. Böylelikle kullanılan işletim sistemi bilgisi elde edilmektedir. Nmap aracı üzerinde bu işlem -O parametresi kullanılarak gerçekleştirilmektedir.

Traceroute İşlemi

Nmap, `-traceroute` parametresi ile her hedef için paketlerin hangi yoldan geçtiğini tespit edebilir.

Script Taraması

Nmap içerisinde, Nmap Script Engine(NSE) adı verilen bir yapı bulunmaktadır. Bu yapı içerisinde birçok script bulunur. Bu scriptler kullanılarak hedefe yönelik bilgi toplama ve güvenlik açığı tespit etme gibi birçok işlem gerçekleştirilebilmektedir. NSE, lua programlama dili ve ağ üzerinde bilgi toplama için tasarlanmış standart bir kütüphane tarafından desteklenmektedir. Bu scriptler genellikle tespit edilen her host üzerinde bulunan her bir port için bir kere çalıştırılmaktadır. `-script` veya `-sC` parametreleri kullanarak Nmap üzerindeki script'ler çalıştırılabilir.

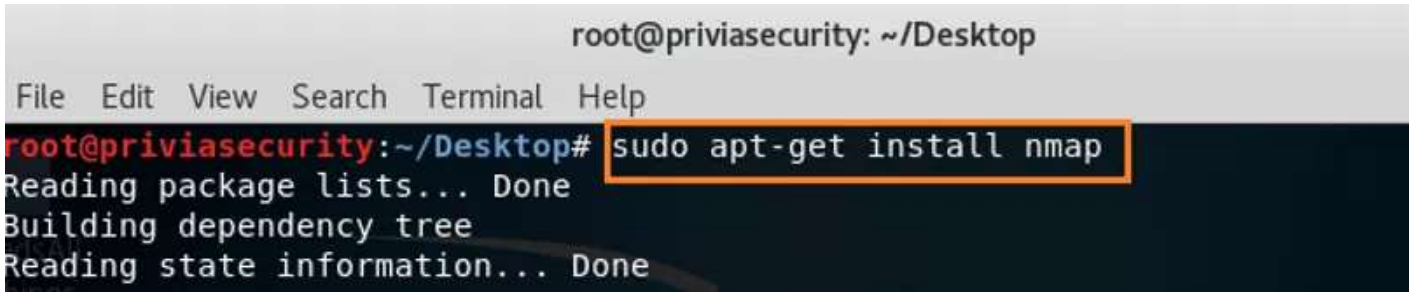
Çıktı Alma

Nmap, tarama işlemleri sonucunda elde ettiği bilgileri ekrana basar. Bu sonuçlar farklı dosya formatlarında kaydedilebilir.

Nmap Kurulumu

Linux (Debian/Ubuntu) Ortamı

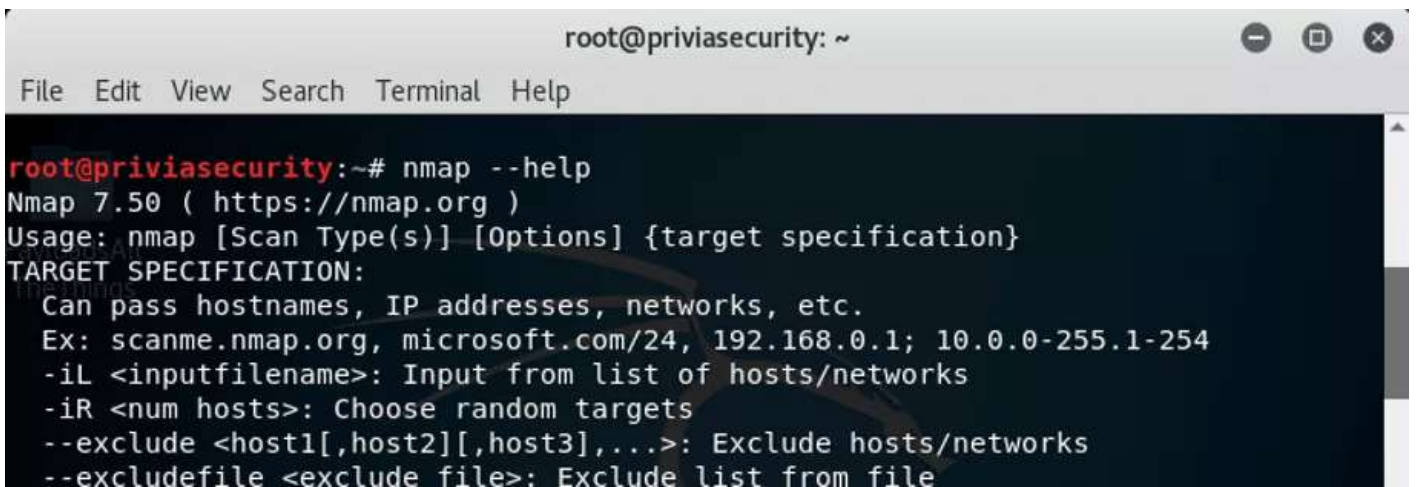
Terminal'de "`sudo apt-get install nmap`" komutu çalıştırıldığında Nmap yüklenmeye başlayacaktır. Ayrıca nmap, sitesinden `.rpm` veya `.deb` uzantılı setup dosyaları indirilerek kurulabilir.



```
root@priviasecurity: ~/Desktop
File Edit View Search Terminal Help
root@priviasecurity:~/Desktop# sudo apt-get install nmap
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

Şekil 2.1.1 – Linux Ortamında Kurulum

Şekil 2.1.1’de gösterildiği gibi “sudo apt-get install nmap” komutu ile kolay bir şekilde kurulum gerçekleştirilebilir.



```
root@priviasecurity: ~
File Edit View Search Terminal Help
root@priviasecurity:~# nmap --help
Nmap 7.50 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude file>: Exclude list from file
```

Şekil 2.1.2 – Linux Terminal Ekran Görüntüsü

Windows Ortamı

Nmap aracının Windows ortamındaki kurulumunu sağlamak için <http://nmap.org/download.html> uzantılı sayfasından aşağıda gösterileceği gibi indirme işlemi gerçekleştirilecektir.

<https://nmap.org/download.html>

Microsoft Windows binaries

Please read the [Windows section](#) of the Install Guide for limitations and installation instructions (includes dependencies and also the Zenmap GUI) or the much smaller command-line zip file 2008 and newer. We also maintain a [guide for users who must run Nmap on earlier Windows](#)

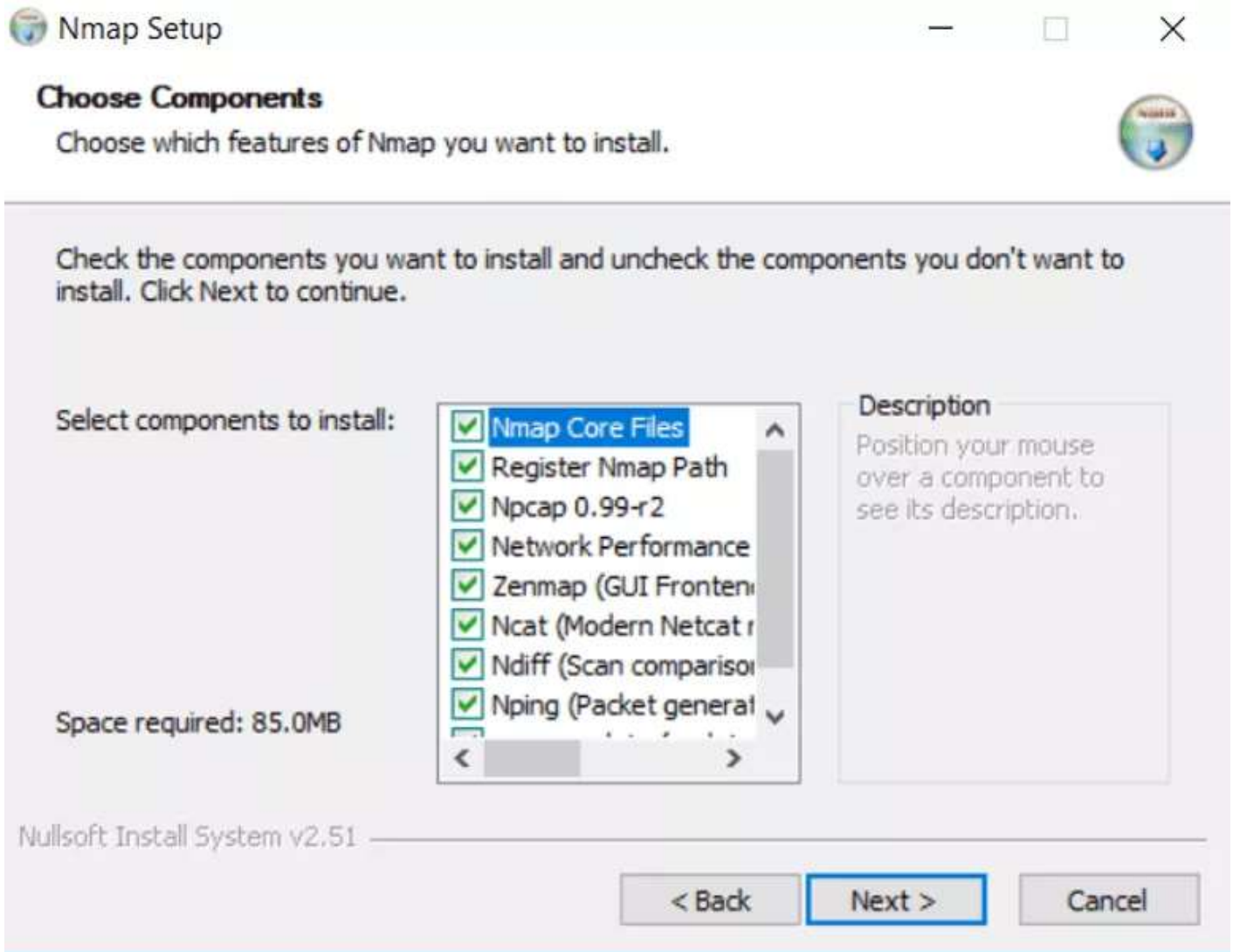
Note: The version of Npcap included in our installers may not always be the latest version. It install [the latest Npcap release](#).

The Nmap **executable Windows installer** can handle Npcap installation, registry performance location. It also includes the Zenmap graphical frontend. Skip all the complexity of the Wind

Latest stable release self-installer: [nmap-7.70-setup.exe](#)
Latest Npcap release self-installer: [npcap-0.99-r7.exe](#)

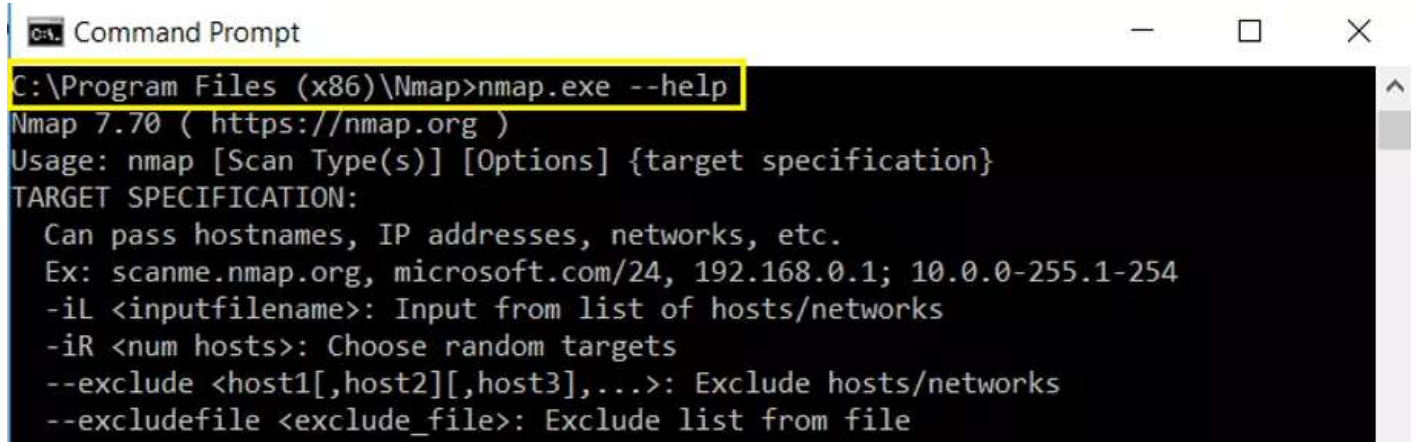
Şekil 2.2.1 – Windows Ortamı için İndirme İşlemi

Daha sonra indirilen .exe uzantılı nmap setup'ı yönetici olarak çalıştırılmaktadır.



Şekil 2.2.2 – Windows Kurulum Gösterimi

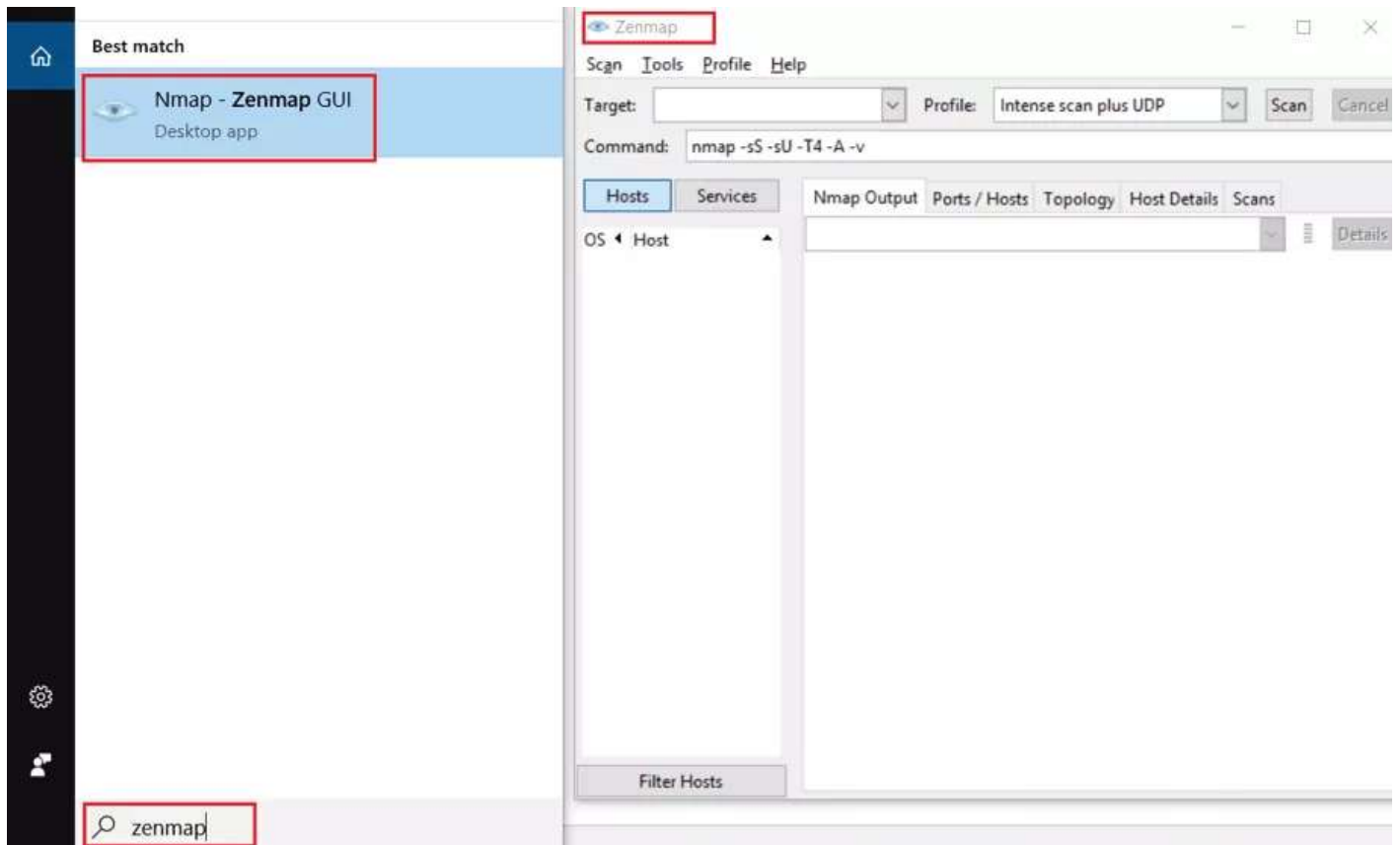
Kurulum işlemi bittikten sonra **Program Files(x86)\Nmap** dizinin altındaki **nmap.exe** uygulaması çalıştırılabilir. Ayrıca bu kurulumla birlikte Nmap'in grafik kullanıcı arayüzlü hali olan **zenmap** uygulaması da yüklenecektir.



```
C:\Program Files (x86)\Nmap>nmap.exe --help
Nmap 7.70 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
```

Şekil 2.2.3 – Command Prompt Ekranında Nmap

Şekil 2.2.3'te Command Prompt ekranı üzerinde nmap.exe çalıştırılmıştır.



Şekil 2.2.4 – Windows Ortamında ZenMap Uygulamasının Çalıştırılması

Şekil 2.2.3 ve Şekil 2.2.4'te gösterildiği gibi Nmap ve Zenmap araçları Linux ortamında da mevcuttur. Terminal üzerinden **nmap** ve **zenmap** komutu çalıştırılarak görüntülenebilir.

Host Keşif İşlemleri

Host keşfi, ağda bulunan sistemlere ping atılarak gerçekleştirilir. Fakat bu işlemler geniş ağlara yönelik yapıldığında veya var olan ağ üzerinde ICMP paketlerine yönelik cevap vermeyen bazı makineler olduğunda farklı yöntemler kullanılarak host keşfi yapılabilir. Hedef ağ üzerinde ping atmadan tarama işlemleri gerçekleştirilebilir. Ayrıca TCP, SYN/ACK, UDP gibi protokoller isteğe bağlı olarak kullanılabilir. Bu protokollerin amacı, türüne göre protokoller gönderildikten sonra, alınan yanıt doğrultusunda verilen IP adresine sahip makinenin gerçekten açık olup olmadığını tespit etmektir.

Hedef Hostları ve Ağları Belirlemek

Hedef hostları belirlemek için Nmap'e hedef ağın IP adresi veya Hostname bilgisi girilmelidir. Bir IP adresinin yerine IP adresi aralığı verilebilir. Ayrıca, Nmap uygulaması CIDR adreslemeyi desteklemektedir. CIDR, ip adresinden veya hostname'den sonra gelen /24, /18 vb. değerlerdir. Bu değerler sonucunda Nmap uygulaması kendi içerisinde bunun işlemlerini yaparak kaç hostun taranması gerektiğini hesaplayıp otomatik olarak tarama işlemini gerçekleştirmektedir. Örneğin, 192.168.10.0/24 IP adresini girdiğimizde 256 tane hostu taramaktadır. Ayrıca hostname adını belirterek tarama aynı şekilde gerçekleştirilmektedir. Örneğin, priviasecurity.com/24 diyerek de bir tarama başlatılabilir.

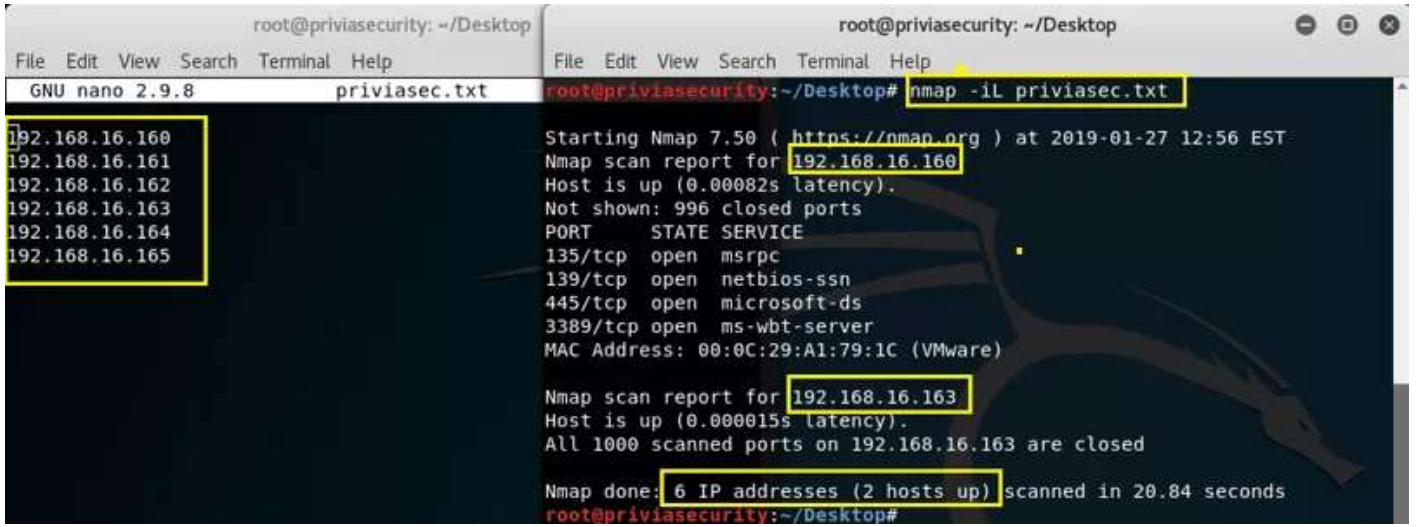

```
root@priviasecurity: ~  
File Edit View Search Terminal Help  
root@priviasecurity:~# nmap 192.168.16.160-167  
  
Starting Nmap 7.50 ( https://nmap.org ) at 2019-01-27 12:40 EST  
Stats: 0:00:36 elapsed; 6 hosts completed (1 up) 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 99.99% done; ETC: 12:41 (0:00:00 remaining)  
Nmap scan report for 192.168.16.160 Hedef makina IP adresi  
Host is up (0.00031s 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 scan report for 192.168.16.163 Benim makina IP adresi  
Host is up (0.000014s latency).  
All 1000 scanned ports on 192.168.16.163 are closed  
  
Nmap done: 8 IP addresses (2 hosts up) scanned in 43.29 seconds  
root@priviasecurity:~#
```

Şekil 3.1 – Örnek Host Keşif Sorgusu

Şekil 3.1’de gösterildiği gibi nmap uygulaması üzerinden bir IP aralığı verilmektedir. Bu tarama sonucunda verilen IP aralığında da tarama gerçekleştirilmektedir.

IP Listesi Belirtmek

Bu tür tarama işlemleri genellikle geniş ağ taramalarında gerçekleştirilmektedir. Verilen yüzlerce veya binlerce IP adresini bir dosyaya kaydettikten sonra -iL parametresi kullanılarak tarama işlemleri başlatılabilir.



```
root@priviasecurity: ~/Desktop
File Edit View Search Terminal Help
GNU nano 2.9.8 priviasec.txt
192.168.16.160
192.168.16.161
192.168.16.162
192.168.16.163
192.168.16.164
192.168.16.165

root@priviasecurity: ~/Desktop# nmap -iL priviasec.txt
Starting Nmap 7.50 ( https://nmap.org ) at 2019-01-27 12:56 EST
Nmap scan report for 192.168.16.160
Host is up (0.00082s 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 scan report for 192.168.16.163
Host is up (0.000015s latency).
All 1000 scanned ports on 192.168.16.163 are closed

Nmap done: 6 IP addresses (2 hosts up) scanned in 20.84 seconds
root@priviasecurity: ~/Desktop#
```

Şekil 3.1.1 – Nmap Uygulaması ile Liste Taraması Gerçekleştirmek

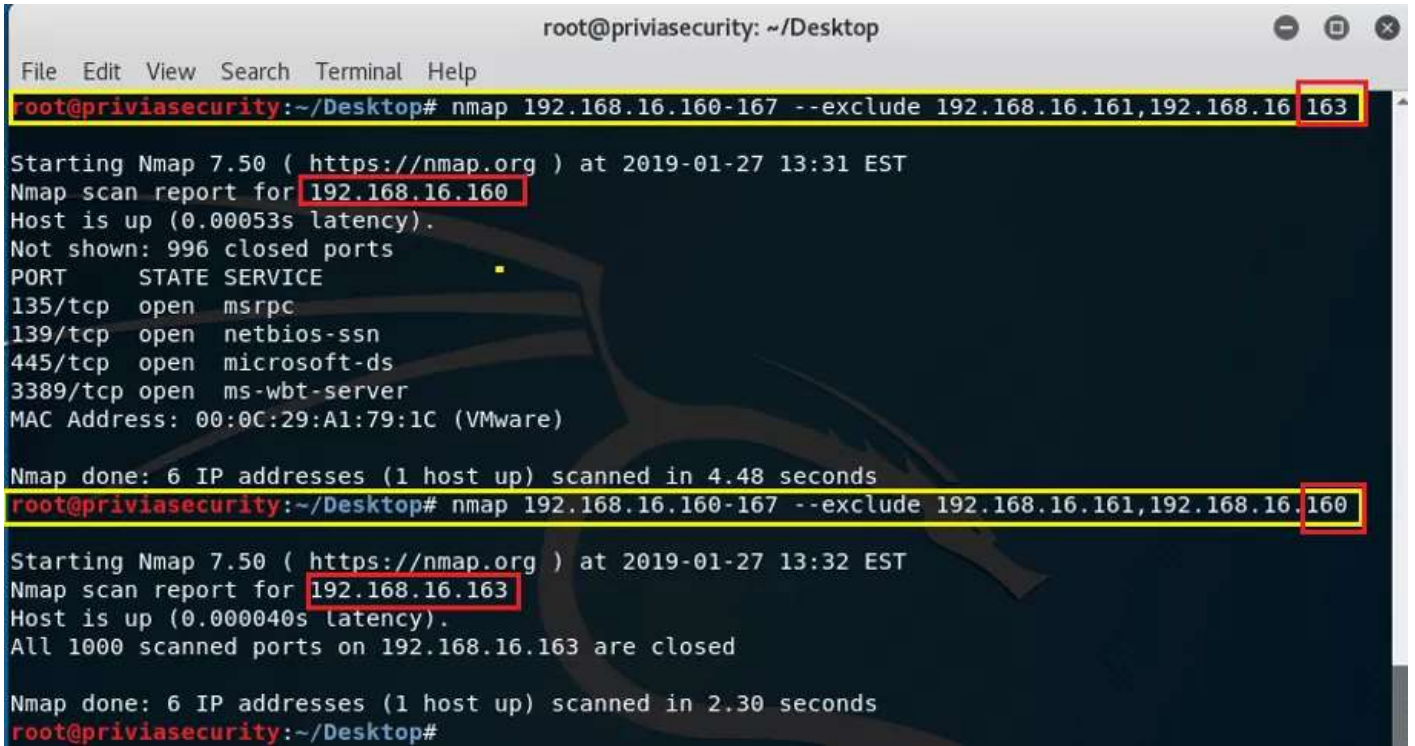
Şekil 3.1.1’de gösterildiği gibi nmap komutundan sonra -iL parametresi kullanılarak içerisinde IP adresleri bulunan bir dosya belirtilir ve tarama işlemi gerçekleştirilir.

Rastgele Hedef Seçmek

Nmap aracı ile rastgele IP adreslerinin taranması için -iR parametresi kullanılarak yapılmaktadır.

Kapsam Dışı Hedefleri Belirlemek

Genellikle gözden kaçan durumlardan biri olan kapsam dışı hedefleri belirleme işlemleri, riskli işlemleri önlemektedir. Tarama yapılacak ağda, taranması istenmeyen IP adresleri -exclude parametresi ile belirtilir. Birçok IP adresi olduğu durumlarda, IP adresleri bir dosyaya kaydedildikten sonra -excludefile parametresi ile bu işlemler gerçekleştirilmektedir.



```
root@priviasecurity: ~/Desktop
File Edit View Search Terminal Help
root@priviasecurity:~/Desktop# nmap 192.168.16.160-167 --exclude 192.168.16.161,192.168.16.163

Starting Nmap 7.50 ( https://nmap.org ) at 2019-01-27 13:31 EST
Nmap scan report for 192.168.16.160
Host is up (0.00053s 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: 6 IP addresses (1 host up) scanned in 4.48 seconds
root@priviasecurity:~/Desktop# nmap 192.168.16.160-167 --exclude 192.168.16.161,192.168.16.160

Starting Nmap 7.50 ( https://nmap.org ) at 2019-01-27 13:32 EST
Nmap scan report for 192.168.16.163
Host is up (0.000040s latency).
All 1000 scanned ports on 192.168.16.163 are closed

Nmap done: 6 IP addresses (1 host up) scanned in 2.30 seconds
root@priviasecurity:~/Desktop#
```

Şekil 3.1.3 – Exclude Parametresinin Kullanılması

Şekil 3.1.3’de gösterildiği gibi **–exclude** parametresinden sonra belirtilen IP adresleri tarama dışında tutulmaktadır. Ayrıca taranması istenmeyen IP adresleri birden fazla olduğunda **–excludefile** parametresi kullanılabilir.

Şekil 3.14’te, taranacak bir ağdaki IP adreslerinin listelenmesi için **–sL** parametresi kullanılır.

Şekil 3.1.4 – Nmap ile -sL Parametresinin Kullanılması

Eğer birbirinden farklı hedeflerin IP adresleri veya hostnameleri taranmak istenirse IP adresleri arasında boşluk bırakılarak tarama işlemi gerçekleştirilebilir. Şekil 3.1.5’de gösterilmiştir.

Şekil 3.1.5 – Nmap ile Farklı Hedeflerin Bir Anda Taranması

Hedef Kuruluşun IP Adresinin Bulunması

Genellikle bir taramadan önce ana domain bilgisi verilmektedir. Verilen domain adresinin IP bilgileri üzerinden tarama işlemleri gerçekleştirilebilir.

DNS Bilgilerinin Elde Edilmesi

DNS’in birincil amacı, domain adlarını IP adreslerine çözümlenektir. Bu nedenle DNS bilgilerini araştırılması gerekmektedir. Şekil 3.2.1’de gösterilmiştir.

Şekil 3.2.1 – DNS Kayıt Türlerinin Sorgulanması

Şekil 3.2.1’de gösterildiği gibi linux ortamında DNS kayıt türlerinin öğrenilmesi için host yardımcı uygulaması kullanılarak nameserver’lar hakkında bilgi elde edilmektedir. Ayrıca zone transferi ile ilgili işlemler Şekil 3.2.2’de gösterilmektedir.

Şekil 3.2.2 – Zone Transfer İşleminin Kontrolü

Şekil 3.2.2 ‘de gösterildiği gibi zone transfer işleminin başarılı veya hatalı olduğu gösterilmektedir. Bir domainin IP adresi var olan kapsam içerisinde var mı yok mu gibi işlemleri öğrenmek için DNS çözümlemesi, traceroute ve ilgili IP adresi için kayıtları için whois kullanılmaktadır.

Şekil 3.2.3 – Nmap ile Traceroute Kullanımı

Şekil 3.2.3'te gösterildiği gibi hedef domaine yönelik tarama gerçekleştirildiğinde `-tracetoute` parametresi kullanılarak hedef IP adresine kadarki ara IP adresleri gösterilecektir. Ayrıca bir IP adresini kullanarak bilgi toplama işlemi Şekil 3.2.4'te de gösterilmektedir.

Şekil 3.2.4 – Hedef Hakkında Bilgi Toplama

Şekil 3.2.4'te gösterildiği gibi whois ile hedef IP adresi hakkında bilgiler getirmektedir.

DNS Çözümlemesi

Host keşiflerinde DNS çözümlemesi işleminin kullanılması büyük önem taşımaktadır. Nmap, host keşif problemlerine yanıt veren her IP adresi için DNS çözümlemesi gerçekleştirmektedir. DNS çözümlemesini kontrol etme işleminde 4 parametre kullanılmaktadır. Bu parametreler aşağıdaki gibidir:

(-n) Parametresi: Nmap uygulamasının bulduğu IP adreslerine yönelik Reverse DNS çözümlemesi yapmamasını sağlamaktadır. Bu parameter genellikle tarama süresini azaltmaktadır.

(-R) Parametresi: Nmap uygulamasının elde ettiği bütün IP adreslerine yönelik Reverse DNS çözümlemesi yapmasını sağlamaktadır. Varsayılan olarak Reverse DNS çözümlemesi yalnızca açık hostlara karşı gerçekleştirilmektedir.

(-system-dns) Parametresi: Nmap uygulaması, varsayılan olarak makinemizde yapılandırılmış name server'lara sorgu gönderip yanıtları dinleyerek IP adreslerini çözümlemektedir. Performansı arttırmak için birçok istek parallel olarak yapılmaktadır. Bunun yerine ise bu parameter kullanılmaktadır. -system-dns parametresi IPv6 için kullanılmaktadır.

(-dns-server) Parametresi: Nmap uygulaması, varsayılan olarak DNS sunucuları resolv.conf(Unix) dosyasından veya registry(Win32)'den belirtmektedir. Birden çok DNS sunucusu kullanıldığında daha hızlıdır. İstekler internetteki özyinelemeli DNS sunucusundan hemen hemen ayrılabilceği için gizliliği de arttırabilmektedir.

Şekil 3.3'te DNS çözümlemesine yönelik uygulanmıştır.

Şekil 3.3 – Nmap ile -system-dns Parametresinin Kullanılması

Şekil 3.3'te gösterildiği gibi DNS çözümleme işlemi gerçekleştirilmiştir. Yukarıda belirtilen parametreler kullanılarak sonuçlar elde edilmiştir.

Host Keşif Kontrolleri

Host keşif kontrollerinde kullanılan parametreler sonucunda, hedeflerin açık/kapalı olma durumu tespit edilebilir. Makinelere gönderilen problemlerin yanıtlarının kontrol edilmesi gerekmektedir.

Liste Taraması (-sL)

Hedef IP adreslerinin kontrolünü sağlamak amacıyla kullanılır. Hedef makinelere herhangi bir paket gönderilmeden belirtilen ağ üzerindeki hostların listelenmesini sağlayan bir host keşif şeklidir.

Şekil 3.4.1 – Nmap ile Liste Taramasının Gerçekleştirilmesi

Şekil 3.4.1’de gösterildiği gibi -sL parametresi ile liste taraması gerçekleştirilmektedir. Ayrıca -Pn parametresi kullanılarak ping tarama yapıp taramadaki işlevselliğin devam etmesi sağlanılacaktır.

Bir ön liste taraması, hangi hedeflerin tarandığını doğrulamaya yardımcı olmaktadır. Gelişmiş bir liste taramasının nedenlerinden biri gizliliklerdir. Bazı

durumlar IDS sistemlerin tetiklenmesine neden olmaktadır. Liste taraması bu tür tetiklenmelere sebep vermeden hangi makinelerin hedef makine olacağı konusunda bilgi sağlamaktadır. Hedeflerin Reverse DNS çözümleme isteklerini fark etmeleri durumunda –dns-server parametresini kullanarak isimsiz özyinelemeli DNS sunucuları arasında geçiş yapılabilir.

Port Taramasını Devre Dışı Bırakmak (-sn)

Nmap, bir ağ üzerinde aktif hostların hızlı bir şekilde tespit edilmesi için –sn parametresini kullanır. Tespit edilen hostların IP adresleri belirtilmektedir. Bu işleme “ping scan” denir. Port taraması gerçekleştirilmeden Nmap uygulamasının içerisindeki scriptlerden ve traceroute problemlerinden faydalanılmaktadır. Ping Scan, liste taramasına göre daha aktif bir tarama türüdür. Bu tarama türü ile hedeflerin IP adresleri ve hostname bilgileri elde edilir. Şekil 3.4.2’de Nmap ile ping taraması gösterilmektedir.

Şekil 3.4.2 – Nmap Uygulaması ile Ping Scan İşlemi

Şekil 3.4.2’de –sn parametresi kullanılarak ping taraması gerçekleştirilmiştir. Ekran görüntüsünde görüldüğü gibi port taraması yapılmamıştır.

Ping Devre Dışı Bırakmak (-Pn)

Nmap uygulaması ile pingsiz tarama gerçekleştirilmesi, host keşfinin yapılmasının istenmemesi anlamına gelmektedir. Bir ağdaki bütün makineleri sırasıyla diğer işlemlere tabi tutulmaktadır. Host keşfi atlanılmaktadır. Bir ağda verilen IP adresleri üzerinde host keşfi yapıldığında pingsiz taramaya göre zaman kaybı meydana gelecektir. Ayrıca nmap ile –Pn parametresi kullanıldığında pingsiz tarama işlemleri gerçekleştirilmektedir. Şekil 3.4.4’te gösterilmiştir.

Bazı Parametreler

(–disable-arp-ping) Parametresi: Genellikle host keşfinde ARP paketleri gönderilip alınan yanıtlar doğrultusunda hostun aktif olup olmadığı tespit edilmektedir. Bu seçenek, bir yönlendiricinin bütün ARP isteklerine özel olarak yanıt verdiği ve hedefin ARP taraması yapıyormuş gibi görünmesini sağlayan ağlarda kullanılmaktadır. Varsayılan ARP taramasını devre dışı bırakmaktadır. Şekil 3.4.4’te gösterilmektedir.

Şekil 3.4.4 – Nmap ile ARP ve ND Ping Taramasını Pasif Tutarak Tarama

(-resolve-all) Parametresi: Bir hostname hedefi birden fazla adrese çözümlenirse, hepsi taranmaktadır. Varsayılan olan, yalnızca ilk çözülen adresi taramaktır.

(-traceroute) Parametresi: Hedefe ulaşması en uygun portu ve protokolü belirlemek için tarama sonuçlarından gelen bilgileri kullanarak tarama sonrasında gerçekleştirilmektedir. Bağlantı taramaları (-sT) ve boşta taramalar (-sl) dışındaki bütün tarama türleriyle çalışmaktadır. Traceroute, ICMP zamanını aşmak için tarayıcı ve hedef host arasındaki ara atlama noktalarından aşılmış mesajları almak için düşük TTL (yaşam süresi) sürüme sahip paketler göndererek çalışmaktadır. Standart traceroute uygulamaları 1 TTL ile başlayıp hedef hosta ulaşana kadar arttırmaktadır. Bu TTL işlemleri, Nmap uygulaması üzerinde geriye doğru yapıldığında sürecin hızlandırılması için akıllı önbellek algoritması kullanılmıştır.

Host Keşif Teknikleri

Genellikle bir  üzerinde bulunan makinelerin aktif olup olmadığını tespit edilmek açacıyla makinelere ICMP echo isteęi gönderilmektedir. Daha sonra yapılan istek sonucunda bir yanıt alınmaktadır. Alınan yanıt sonucunda makinenin aktif veya pasif olduęu tespit edilmektedir. Güvenlik duvarları bu istekleri nadiren engellemektedir. Bundan dolayı host keşif çalışmaları için kullanılan bir tekniktir. Şekil 3.5’de –sn –PE parametreleri ICMP ping taramasını belirtmektedir. –R parametresi ise tüm makinelere yönelik reverse DNS çözümlemesi yapmasını istemektedir.

Şekil 3.5 – Nmap Host Keşif Teknikleri

TCP SYN Ping

-PS parametresi kullanılarak, SYN bayraklı boş bir TCP paketi gönderilmektedir. Varsayılan olarak 80. port hedef alınmaktadır. Bu bayrak uzak bir sistem ile bağlantı kurulmak istendiğini göstermektedir. Port açık olursa SYN/ACK paketiyle yanıt verilecektir. Üç el sıkışma tamamlayıp bir ACK paketi yerine RST paketini göndererek bağlantıyı düşürecektir. Alınan RST ve SYN/ACK yanıt makinenin açık olduğunu belirtmektedir.

Şekil 3.5.1 – TCP SYN probu ile host keşfi

TCP ACK Ping

-PA parametresi kullanılarak gerçekleştirilen bir host keşif tekniğidir. SYN ping'e benzemektedir. Tek fark bayrakların değişik olmasıdır. Hedef sisteme ACK bayraklı TCP paketi gönderilir. Eğer hedef sistem açıksa RST paketi ile yanıt verir. 80. port hedef alınarak yapılmaktadır. -PS parametresi ile yapılan taramalar engellendiğinde kullanılmaktadır.

Şekil 3.5.2 – Nmap ile TCP ACK Ping tekniğinin kullanımı

UDP Ping

UDP paketleri kullanılarak sistemlerin aktif olup olmadığı tespit edilir. –PU parametresi kullanılarak gerçekleştirilmektedir. –PS ve –PA parametreleri ile aynı formattadır. Varsayılan olarak 40. Ve 125. Portlar kullanılmaktadır. Genellikle gönderilen paketler boştur. Fakat 53. Ve 161. Portlar genel bağlantı noktaları olduğu için özel payload gönderilmektedir. **–data-length** parametresi, tüm portlar için rastgele payload göndermektedir. Bu tarama türünün en önemli avantajı güvenlik duvarını atlatması ve TCP portlarını tarayan filtreleri olmasıdır.

ICMP Ping Türleri

Nmap, host keşiflerinde ICMP paketlerini kullanır. Hedef hostlara ICMP type 8 (Echo isteği) gönderip ICMP type 0(Echo yanıtı) beklemektedir. Fakat birçok güvenlik duvarı bu isteği engellemektedir. -PE parametresi kullanılarak ICMP echo isteği gerçekleştirilir. Bu işlem ICMP ping sorgusu olarak bilinmektedir. Ayrıca açık hostların keşfi zaman damgası ve adres damgası üzerinden de tespit edilebilmektedir. Bu işlemler –PP ve –PM parametreleri kullanılarak gerçekleştirilir.

IP Protocol Ping

IP paketlerinin içerisindeki IP başlığında belirtilen protokol numarası ile yapılan bir tarama türüdür. Herhangi bir protokol belirtilmediği zaman ICMP, IGMP, IP-inIP protokolleri için birden fazla IP paketi gönderilmektedir. Bu yöntemde kullanılan prob ile aynı protokolü kullanan yanıtlar üzerinde veya hedef hosta yönelik erişilemediğini belirten ICMP paketlerine bakılarak bir makinenin çalışıp çalışılmadığı tespit edilmektedir.

ARP Ping

En yaygın kullanılan taramalardan biridir. Bu tarama işlemi `-PR` parametresi kullanılarak gerçekleştirilir. Bu tarama ham bir IP paketi gönderilerek gerçekleştirilmektedir. Böylece hedef IP adresine karşılık gelen makinenin fiziksel adresi tespit edilir.

Şekil 3.5.6 – Çevrimdışı hedefe yönelik IP Ping Taraması ve ARP Ping Taraması

Şekil 3.5.6'da gösterildiği gibi tarama örnekleri gerçekleştirilmiştir. Bu tarama örneğinin ilkinde **`-send-ip`** parametresi kullanılmasıyla, yerel ağ olmasına rağmen IP seviyesinde paketler gönderilmektedir. İlk örnek 3.09 saniye

sürmüştür. Yalnızca bir hedefe yönelik yapılan bir tarama olduğu için taramanın sonuçlanması kısa sürmüştür. Fakat kurumsal bir yerel ağdaki makine sayısının fazlalığı bu süreyi arttırmaktadır. İşletim sistemi hosttan vazgeçmediği için bir saniye arayla üç ARP isteği göndermektedir. İkinci örnekte ise ARP taraması 0.47 saniyede gerçekleştirilmiştir. Ağ yöneticileri normal şartlarda ping paketlerini engellemektedir. Fakat ARP istekleri veya yanıtları genellikle engellenmemektedir. Ayrıca bu taramalar gerçekleştirildiğinde **-spoof-mac** parametresini kullanılarak tarama yapan makinenin MAC adresi gizlenebilmektedir.

SCTP INIT Ping

Bu tarama türü -PY kullanılarak gerçekleştirilmektedir. Bu parametre kullanılarak içerisinde INIT öbeği bulunan bit SCTP paketi gönderilmektedir. Varsayılan olarak 80. portu hedef almaktadır. Örnek olarak "-PY22,80" gibi bir parametre ile 22. ve 80. portlar ile bağlantı kurulacaktır. Portlar açık ise INIT-ACK yanıtı dönmektedir. Nmap, bu yanıtı işlevsel bir SCTP paketi göndermek yerine ABORT yanıtını vererek bağlantıyı bitirmektedir. Böylece bu iki yanıt ile hedef makine üzerindeki portların açık olduğu tespit edilmektedir.

Host Keşif Stratejileri

Nmap aracı, host keşiflerini daha iyi şekilde tespitinin sağlanması için belirli parametreleri kullanmaktadır. Bu parametreler host keşiflerinde kullanıcının yapmak istediği tarama türlerine göre kullanılmaktadır. Bu parametreler aşağıda belirtilmiştir.

(-v/-verbose) Parametresi

Nmap aracında bulunan bu parametre, tarama sonucunda gelen çıktının ayrıntılı bir şekilde gelmesini sağlamaktadır. Bu doğrultuda host hakkında ek

bilgiler verilmektedir.

Şekil 3.6.1 – Verbose Parametresinin Kullanımı

(-source-port <port no>) Parametresi

Firewall yöneticileri, DNS ve FTP portlarını açık tutmak için firewall üzerinden özel kurallar oluşturmaktadır. Fakat firewall bypass işlemlerinden biri de source port manipülasyon işlemidir.

(-data-length <length>) Parametresi

Bu parametre ile her pakete rastgele olarak veri eklenmektedir. Ayrıca TCF UDP ve ICMP gibi tarama türleriyle birlikte kullanılabilir. Birçok IDL

sistemini atlatmak için kullanılan yöntemlerden biridir. Örneğin, data değeri 56 olan bir echo istek paketine rastgele olarak 32 değeri atanırsa, IDS sistemi paketin bir Windows işletim sistemine sahip bir makineden geldiğini işaretler. Fakat gelen istek paketindeki gerçek data değerinin 56 olması isteğin bir Linux işletim sistemine sahip makineden geldiğini gösterebilir.

Şekil 3.6.3 – (-data-length) Parametresinin Kullanımı

(-ttl <value>) Parametresi

Giden TTL değerinin ayarlanması, IPv4 düzeyindeki ping taramalarında kullanılmaktadır. Yapılan taramanın yerel ağ sınırları içerisinde yapılmasını sağlamayı hedeflemektedir. Giden -ttl değeri azaltılarak, herhangi bir döngü ile karşılaşıldığında yönlendirici CPU'sunun işlem yükünün azaltılması hedeflenmektedir.

Şekil 3.6.4 – TTL Parametresinin Kullanımı

Hazır Zamanlama Parametreleri

Ping taramasını hızlandırıp sonuçların alınmasına yönelik yapılmış bir parametre düzenlemesidir. -T parametresi ile kullanılır. Hazır zamanlama şablonları, **paranoid(0)**, **sneaky(1)**, **polite(2)**, **normal(3)**, **aggressive(4)** ve **insane(5)** olarak 6 tanedir.

Şekil 3.6.5 – Zamanlama Parametresinin Kullanılması

(-max/min-parallelism <value>) Parametreleri

Yapılan taramalarda taranacak makinelerin paralel bir şekilde taramasını sağlamak için düzenlenmiş bir parametredir. Parametreyi kullanarak <value> değeri olarak makine sayısı belirtilmektedir.

(-min/max/initial-rtt-timeout <time>) Parametreleri

Bu parametreler, Nmap aracının yaptığı istek sonucunda gelecek yanıt paketinin ne kadar bekleyeceğini kontrol etmektedir.

Çıktı Parametreleri

-oA, -oN, -oG, -oX vb. parametrelerden oluşur. Örneğin, -oX parametresinin kullanılması ile Nmap çıktıları XML formatında oluşturulur.

(-randomize-hosts) Parametresi

Ağda bir tarama yapılırken, `-randomize-hosts` parametresinin kullanılması taramayı belirsizleştirir. Bu yöntem IDS ve IPS sistemlerinden kaçınmak için kullanılır. Nmap, varsayılan olarak bir ağdaki makineleri ardışık olarak tarar. Bazı IDS ve IPS sistemleri ise, yapılan taramayı tespit edip engelleyebilir.

(-reason) Parametresi

Varsayılan taramalar sonucunda gelen çıktıda hedef portun çalışır durumda olup olmadığını göstermektedir. Bu parametre ile nmap taramasında hedef makinesinin hangi keşif testlerine yanıt verdiğini açıklamaktadır. Nmap çalışma sırasında yanıt paketi olarak bir ICMP echo paketi yanıtı rapor edilebilir. Fakat ikinci bir tarama sonucunda önce bir RST paketi alınabilir ve Nmap aracının bunu bildirmesine neden olabilir. Bundan dolayı detaylı olarak hedef makinenin ne tür yanıtlar verip vermediğini görebilmek için bu parametrenin kullanılması fayda sağlamaktadır.

Şekil 3.6.10 – Reason Parametresinin Kullanılması

(-packet-trace) Parametresi

Nmap, -packet-trace parametresini kullanarak tarama süresince neler yapıldığını detaylı olarak gösterir. -packet-trace parametresi, Sıra numaraları, TTL değerleri ve TCP bayrakları gibi ayrıntılar dâhil olmak üzere, alınan ve gönderilen her paketin gösterilmesini sağlar.

(-D <decoy1, decoy2,,,) Parametresi

Decoy olarak tanımlanan IP adresleri, saldırgan IP adresini gizlemek için kullanılan sahte IP adresleri olarak tanımlanabilir. Resim 3.6.12'deki saldırgan IP adresi, 192.168.16.163'tür. Fakat, -D parametresi ile verilen 192.168.16.138, 192.168.16.2 gibi sahte IP adresleri kullanılarak saldırgan IP ile tarama yapılmıştır. Böylelikle ağı izleyen yetkililerin saldırganı tespit etmesi zorlaşır.

Şekil 3.6.12 – Decoy Parametresinin Kullanılması

(-6) Parametresi

Taramalarda ipv4 adresi yerine ipv6 kullanmayı sağlar.

(-S <source IP address>, -e <sending device name>) Parametreleri

Kaynak IP adresini ve gönderen cihazın adını belirterek yapılan tarama türleridir.

Ping Parametrelerini Seçmek ve Birleştirmek

Hedefi daha etkili bir şekilde tarama için parametrelerin tümünü bilmekten daha fazlası gerekebilir. Bu parametreleri bir arada belirterek ve birleştirerek başarı oranları farklılık göstermektedir. Bu farklılık Şekil 3.7’de gösterilmektedir.

Şekil 3.7.a – Taramada Kullanılacak Olan Probların Başarı Yüzdeleri

Şekil 3.7.b – Taramada Kullanılacak Birleştirilmiş Problar ve Başarı Yüzdeleri

- < **Internet Explorer Üzerinde RCE Zafiyeti Keşfedildi #39**
- > **Nmap Nedir? – Temel ve İleri Seviye – Part 2**

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