ÖN BİLGİ

Bu belge

- https://www.bgasecurity.com/makale/nmap-kullanim-kitapcigi/

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Nmap%20Kullan%C4%B1m%20Kitap%C3%A7%C4%B1%C4%9F%C4%B1.pdf

adresindeki makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

Nmap kullanarak taranan ağın haritası çıkarılabilir, ağda çalışan makinaların işletim sistemleri ve diğer yazılımlarının sürümleri tespit edilebilir, çalışan fiziksel aygıt tipleri, çalışma süreleri ve bilgisayarın firewall’a sahip olup olmadığı öğrenilebilir.

(Page 4)

2)

Nmap

- herhangi bir ağ hazırlanırken gerekli ayarların test edilmesinde,
- ağ envanteri tutulmasında, haritalanmasında, bakımında ve yönetiminde,
- bilinmeyen yeni sunucuları tanımlayarak güvenlik denetimlerinin yapılmasında

kullanılmaktadır.

(Page 4)

3)

Nmap çok güçlü bir uygulama olmasına ragmen yeni başlayanlar için anlaşılması zor bir uygulamadır. Nmap yaklaşık 15 farklı tarama yöntemine ve her tarama için yaklaşık 20 farklı seçeneğe sahiptir.

(Page 4)

4)

Nmap Çalışma Şekli

a. Eğer IP yerine domain girilmişse DNS Lookup işlemi yapılır.
b. Hedef makinaya bir ping atılır, fakat ICMP ping’i değil. Özel bir ping. –P0 ile bu iptal edilebilir.
c. Eğer IP belirtildiyse Reverse DNS Lookup işlemi yapılır. –n ile Reverse DNS Lookup işlemi önlenir.
d. Tarama gerçekleştirilir.

(Page 4)

5)

DNS Lookup işlemleri network trafiğinde göründüğünden log'lanır. Nmap'te bunu önlemenin yolu yok gibidir. Sadece eğer Nmap'in çalıştırıldığı makinanın DNS cache'inde IP-Domain kaydı varsa Nmap DNS Lookup işlemini yapmaz.

(Page 4)

6)

Hedef makinanının domain'i www.microsoft.com olarak belirtilirse DNS lookup sonucu gelecek olan IP 207.46.19.30 olacakken bu IP hedef makina IP'si olarak belirtilirse Reverse DNS Lookup sonucu gelecek olan domain www.microsoft.com olmayacaktır. Bunun yerine www.microsoft.com.nsatc.net olacaktır. Dolayısıyla IP->Domain sonuçları ile Domain->IP sonuçları farklı çıkabilir.

(Page 4-5)

7)

Host Discovery Parametreleri

- -iL <dosyaIsmi> : Hostların ve network'lerin belirtildiği dosyadan bilgileri alarak tarama yapar.
- -iR <hostSayisi> : Dünyadan rastgele hedef seçerek belirtilen sayıda host'u tarar (R = Random).
- --exclude <host1 [,host2][,host3],... > : Taranılması istenilmeyen hostların veya network'lerin belirtilmesi için kullanılır.
- --exclude <exclude_file> : Taranılması istenilmeyen hostların veya network'lerin bir dosya içerisinden alınarak belirtilmesinde kullanılır.

Hedef Belirtme Örnekleri;

192.168.1.10

192.168.1.10/24 : 192.168.1.0 – 192.168.1.255 aralığındaki subnet'i tarar.

192.168.1-2.* : 192.168.1.0 – 192.168.2.255 aralığındaki herşeyi tarar.

192.168.1,2.0-255 : 192.168.1.0 – 192.168.2.255 aralığındaki herşeyi tarar.

..1.5 : 1.0.1.6 – 255.255.1.5 aralığındaki herşeyi tarar.

nmap -iL hosts.txt : hosts.txt dosyasında her satırda bir host yer alır ve taranır.

nmap -iR 10 : Rastgele dünyadaki 10 tane hostu taramak için kullanılır.

nmap --exclude www.site.com,www.xyz.com 192.168.1.0/24 : 192.168.1.0 – 192.168.1.255 subnetindeki site.com ve xyz.com dışında herşeyi tarar.

nmap --excludefile riskli.txt 192.168.1.0/24 : 192.168.1.0 – 192.168.1.255 subnetindeki riskli.txt dosyasında belirtilen adresler haricinde herşeyi tarar. Not: riskli.txt dosyasında her satırda bir host yer alır.

(Page 6-7)

8)

Hedefleri Keşfetme

Keşfetme işlemi için birçok seçenek vardır. Ping Scan bunlardan biridir.

> nmap -sP 192.168.2.0/24

Output:

Host 192.168.2.1 appears to be up.

Host 192.168.2.3 appears to be up.

Host 192.168.2.4 appears to be up.

Nmap done: 256 IP addresses (3 hosts up) scanned in 1.281 seconds

Ping scan belirtilen hedef veya hedeflerin 80. Portuna ICMP echo request ve TCP ACK paketleri gönderir. Ping scan network envanterini çıkarma işlemi için idealdir.

9)

Diğer HOST Discovery Parametreleri

--dns-servers <serv1 [,serv2][,serv3],...>		: Özel DNS server'ı belirtmek için kullanılır.
-r		: Portları sırayla tarar. Rastgele tarama kullanılmaz.
--randomize_hosts	(-rH)	: Listede belirtilen hostları rastgele seçerek tarar.
--source_port	(-g)	: Taramayı yapacak olan makinanın kaynak portunu belirler.
-S <ip>		: Kaynak IP'yi değiştirmeye yarar (Ip Spoofing).
-e		: Network arayüzünü belirlemek amacıyla kullanılır.

(Page 7-8)

10)

Nmap varsayılan olarak ARP taraması (-PR) yapar. Bu özelliği iptal etmek için --send-ip seçeneği kullanılmalıdır.

(Page 7)

11)

Nmap'te protokol (TCP, UDP vb.) bazlı tarama yapılabileceği gibi belirli servisler bazlı tarama da yapılabilir.

(Page 8)

12)

Tarama Sonuçlarında Port'ları Tanımlayan İfadeler

- Open : Port açık. Yani aktif olarak TCP ve UDP bağlantılarını kabul eder.

- Closed : Port kapalı, ancak erişilebilirdir. Hedef sistem bu portu kullanmamaktadır.
- Filtered : Porta giden paketler filtreleme mekanizması tarafından engellenir. Dolayısıyla Nmap portun açık olup olmadığına karar veremez.
- Unfiltered : Port erişilebilirdir, ancak Nmap portun açık ya da kapalı olduğuna karar veremez. Sadece ACK Scan için bu sonuç çıkabilir.
- Open | Filtered : Nmap portların açık ya da filtrelenmiş olduğuna karar veremez. UDP, IP, Proto, FIN, Null, Xmas Scan için bu sonuç çıkabilir.
- Closed | Filtered : Nmap portun kapalı ya da filtreli olduğuna karar veremez. Sadece Idle Scan için bu sonuç çıkabilir.

(Page 8)

13)

Taramalar sırasında Nmap'in performansının düşmemesi ve çıktıların daha sıkı ekrana basılması için -v ya da -vv seçenekleri kullanılabilir. -vv kullanılırsa Nmap taraması başladığı andan bittiği ana kadarki Nmap'in yaptığı tüm işlem adımları ekrana basılır.

(Page 8)

14)

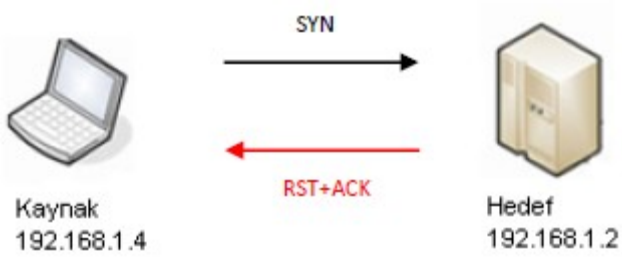
Tarama Türleri

Nmap Scan	Command Syntax	Requires Privileged Access	Identifies TCP Ports	Identifies UDP Ports
TCP SYN Scan	-sS	YES	YES	NO
TCP connect() Scan	-sT	NO	YES	NO
FIN Scan	-sF	YES	YES	NO
Xmas Tree Scan	-sX	YES	YES	NO
Null Scan	-sN	YES	YES	NO
Ping Scan	-sP	NO	NO	NO
Version Detection	-sV	NO	NO	NO
UDP Scan	-sU	YES	NO	YES
IP Protocol Scan	-sO	YES	NO	NO
ACK Scan	-sA	YES	YES	NO
Window Scan	-sW	YES	YES	NO
RPC Scan	-sR	NO	NO	NO
List Scan	-sL	NO	NO	NO
Idlescan	-sI	YES	YES	NO
FTP Bounce Attack	-b	NO	YES	NO

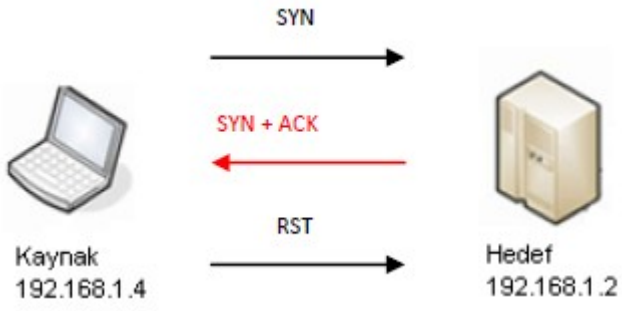
15)

TCP Syn Scan

Kaynak makinanın hedef makinaya SYN bayraklı TCP paketi göndererek başlattığı bu tarama türünde portların kapalı olması durumunda hedef makina SYN'e karşılık RST+ACK bayraklı TCP paketi gönderir.



Portun açık olduğu durumda ise hedef makina aldığı SYN paketine karşılık SYN + ACK paketi gönderecektir. Böylece kaynak makina portun açık olduğunu öğrenmiş olacaktır ve RST paketi göndererek TCP 3 yollu el sıkışmanın gerçekleşmesini önleyecektir.



TCP Syn Scan'ı gerçekleştirmek için aşağıdaki komut kullanılır:

```
> nmap -sS -v 192.168.0.14          // -v ile aşağıdaki detaylı bilgiler elde
                                    // edilmiştir.
```

Output:

```
at 2010-08-01 18:37 EEST            // Tarama başlama zamanı
Initiating ARP Ping Scan at 18:37   // ARP Broadcast
Scanning 192.168.1.2 [1 port]       // ARP Scanning
Completed ARP Ping Scan at 18:37, 0.04s elapsed (1 total hosts)
```

Initiating Parallel DNS resolution of 1 host. at 18:37 // DNS Çözümleme

Completed Parallel DNS resolution of 1 host. at 18:37, 0.02s elapsed

Initiating SYN Stealth Scan at 18:37 // TCP Syn Scan Taraması Hazırlığı

Scanning 192.168.1.2 [1000 ports] // TCP Syn Scan'ın Başlaması

Discovered open port 22/tcp on 192.168.1.2

Discovered open port 111/tcp on 192.168.1.2

Discovered open port 53/tcp on 192.168.1.2

Discovered open port 80/tcp on 192.168.1.2

Discovered open port 2049/tcp on 192.168.1.2

Completed SYN Stealth Scan at 18:37, 1.15s elapsed (1000 total ports)

Nmap scan report for 192.168.1.2 // Nmap Tarama Sonucu Rapor // Başlangıcı

Host is up (0.00097s latency). // Host'un online olduğunu söylüyor

Not shown: 995 closed ports

PORT STATE SERVICE

22/tcp open ssh

53/tcp open domain

80/tcp open http

111/tcp open rpcbind

2049/tcp open nfs

MAC Address: 00:0C:29:D7:D3:65 (VMware)

Read data files from: /usr/local/share/nmap

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds

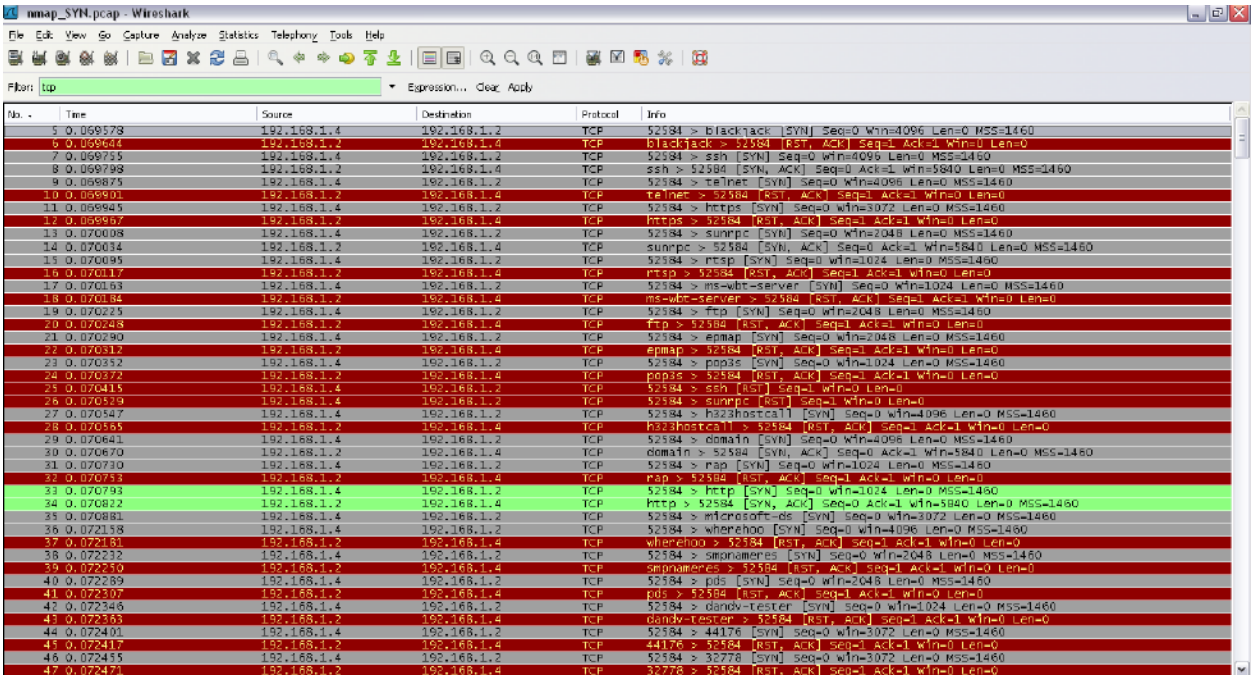
Raw packets sent: 1006 (44.248KB) | Rcvd: 1001 (40.048KB)

Daha önce bahsedilen ARP taramasının varsayılan olarak yapıldığı bilgisini tarama bildirimlerinde görebilirsin. Biz TCP Syn taraması yap emri vermis olmamıza ragmen Nmap önce ARP taraması yapmıştır. Ardından DNS çözümlemesi yapılmıştır. Ardından TCP Syn taraması yapmıştır. Ardından tarama raporunu sunmuştur.

a. ARP Taraması
b. DNS Çözümleme

c. TCP Syn Taraması
d. Rapor

Nmap tarama yaparken Wireshark ile eth0 dinlenilseydi gelen giden tüm TCP paketleri şekildeki gibi sıralanırdı.

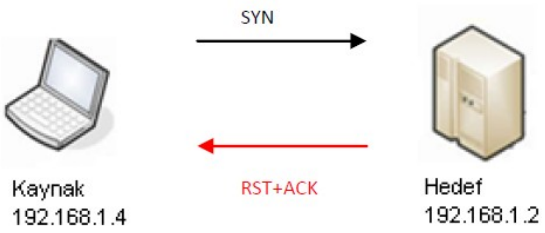


(Page 9-11)

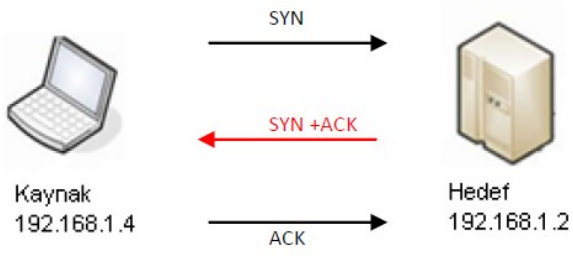
16)

TCP Connect Scan

Bu taramada da kaynak makine hedef makinenin portlarına SYN paketi gönderir ve buna hedef port kapalıysa RST+ACK paketi döner.



Eğer hedef port açıksa SYN+ACK paketi döner. Bu şekilde Nmap portun açık olduğunu anlar ve bunun ardından TCP Syn Scan'ın aksine kaynak makine ACK paketi göndererek bağlantıyı başlatır.



TCP Connect Scan'ın adından da belli olabileceği gibi TCP 3 yollu el sıkışma bu taramada gerçekleşir. Bu tarama aşağıdaki şekilde kullanılır.

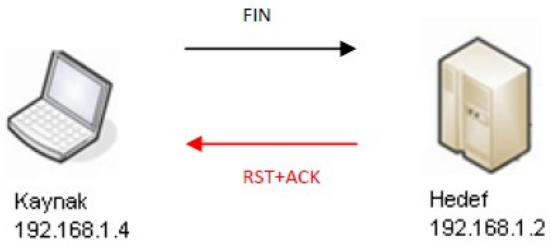
> nmap -sT -v 192.168.0.14

(Page 11-12)

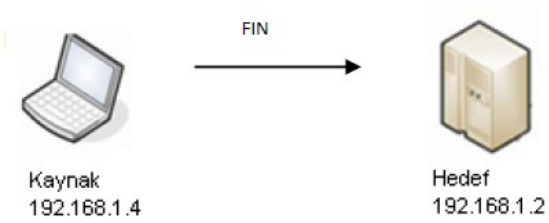
17)

FIN Scan

Kaynak makinenin hedef portlara göndereceği FIN bayraklı TCP paketlerine karşılık RST + ACK bayraklı TCP paketi dönerse port kapalı, hiçbir paket dönmezse port açık anlamına gelir.



Port Kapalı



Port Açık

FIN Scan şöyle gerçekleştirilir:

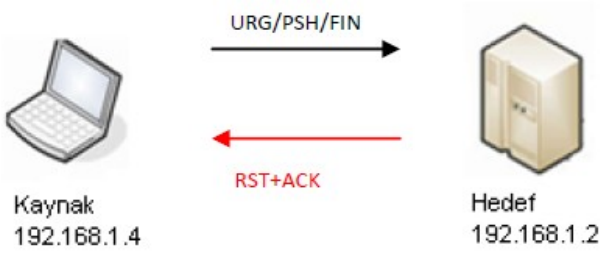
> nmap -sF -v 192.168.0.14

(Page 13)

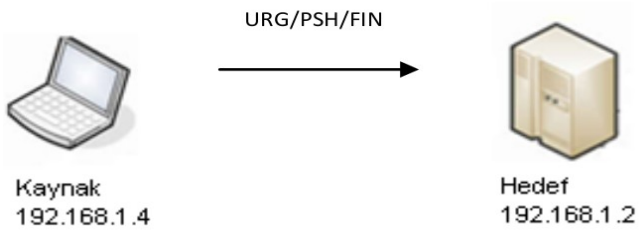
18)

Xmas Tree Scan

Kaynak makina göndereceği TCP paketi içerisine URG, PSH ve FIN bayraklarını ekler ve gönderir. Dönen yanıt eğer RST+ACK ise port kapalı, eğer hiçbir yanıt gelmezse port açık anlamına gelir.



Port Kapalı



Port Açık

Xmas Tree Scan şöyle gerçekleştirilir:

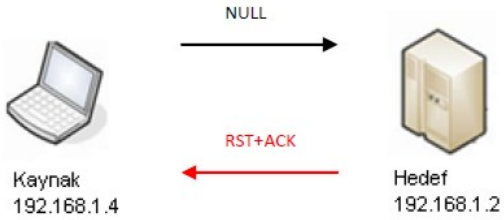
> nmap -sX -v 192.168.0.14

(Page 15)

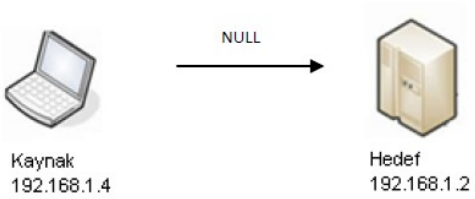
19)

Null Scan

Kaynak makinanın göndereceği bayraksız paketlere karşısında gelen cevaplar FIN Scan ile aynı şekilde değerlendirilir. Gönderilen bayraksız paket sonrası hedef porttan RST+ACK geliyorsa port kapalı, hiçbir şey gelmiyorsa port açıktır denir.



Port Kapalı



Port Açık

Null Scan şöyle gerçekleştirilir:

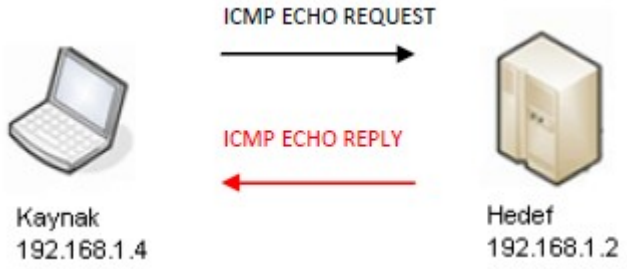
> nmap -sN -v 192.168.0.14

(Page 15-16)

20)

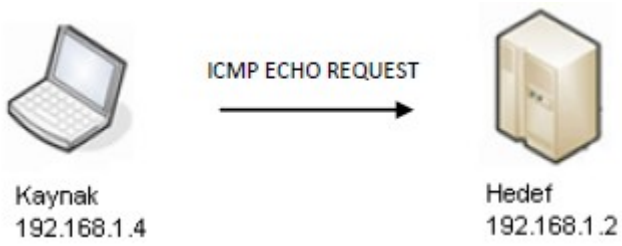
Ping Scan

Eğer hedef makina erişilebilir ise gönderilen ICMP Echo Request paketine karşılık ICMP Echo response paketi döner.



Host is up

Eğer hedef makine erişilebilir değilse ya da hedef makine ICMP paketlerini filtreleyecek (engelleyecek) şekilde ayarlanmışsa hedef makineden cevap dönmeyecektir.



Host is close or not accessible.

Ping Scan şöyle gerçekleştirilir:

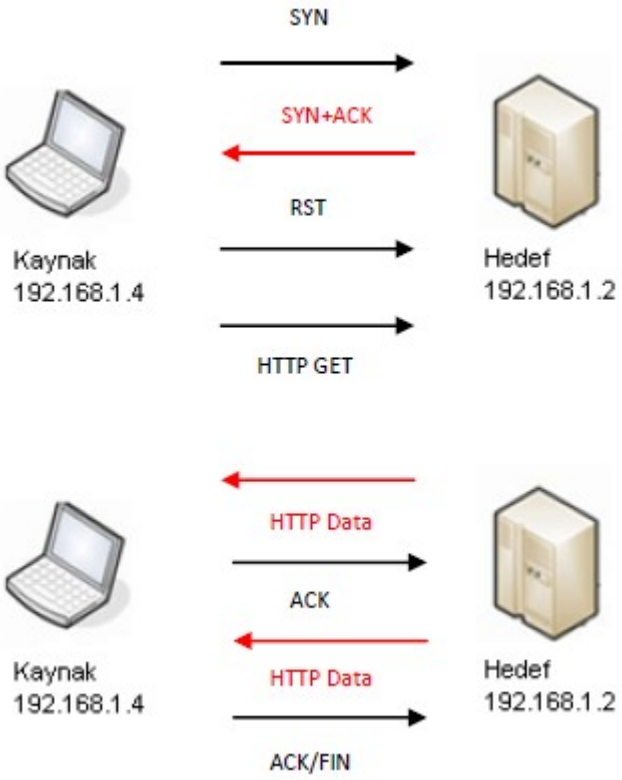
> nmap -sP -v 192.168.0.14

(Page 17-18)

21)

Version Detection Scan

Version Detection Scan eğer tarama türü belirtilmişse o tarama türünde önce açık portları arar, eğer tarama türü belirtilmemişse yetkili kullanıcılar için TCP Syn Scan, yetkisiz kullanıcılar için TCP Connect Scan ile açık portları arar. Eğer açık port bulunursa Version Detection Scan hedef makine üzerinde servis araştırması sürecini başlatır.



Version Detection Scan şöyle gerçekleştirilir:

> nmap -sV -v 192.168.0.14

Output:

at 2010-08-01 18:43 EEST
NSE: Loaded 6 scripts for scanning.
Initiating ARP Ping Scan at 18:43 // ARP Scan için hazırlanılır.
Scanning 192.168.1.2 [1 port] // ARP Scan başlatılır.
Completed ARP Ping Scan at 18:43, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:43 // DNS çözüm
// lemesi yapılır.
Completed Parallel DNS resolution of 1 host. at 18:43, 13.00s elapsed

```
Initiating SYN Stealth Scan at 18:43      // TCP Syn taraması hazırlanır.
Scanning 192.168.1.2 [1000 ports]      // TCP Syn Scan başlatılır.
Discovered open port 80/tcp on 192.168.1.2
Discovered open port 22/tcp on 192.168.1.2
Discovered open port 53/tcp on 192.168.1.2
Discovered open port 111/tcp on 192.168.1.2
Discovered open port 2049/tcp on 192.168.1.2
Completed SYN Stealth Scan at 18:43, 2.32s elapsed (1000 total ports)
Initiating Service scan at 18:43          // Service taraması hazırlanılır.
Scanning 5 services on 192.168.1.2      // Service taraması başlatılır.
Completed Service scan at 18:43, 6.02s elapsed (5 services on 1 host)
Initiating RPCGrind Scan against 192.168.1.2 at 18:43
Completed RPCGrind Scan against 192.168.1.2 at 18:43, 0.01s elapsed
(2 ports)
NSE: Script scanning 192.168.1.2.
NSE: Script Scanning completed.
Nmap scan report for 192.168.1.2        // Rapor sunulur.
Host is up (0.0017s latency).
Not shown: 995 closed ports
PORT  STATE SERVICE VERSION
22/tcp open ssh OpenSSH 5.2 (protocol 2.0)
53/tcp open domain dnsmasq 2.48
80/tcp open http Apache httpd 2.2.13 ((Fedora))
111/tcp open rpcbind
2049/tcp open nfs 2-4 (rpc #100003)
MAC Address: 00:0C:29:D7:D3:65 (VMware)
Read data files from: /usr/local/share/nmap
Service detection performed.
```

Tarama sonuçlarına bakacak olursan şöyle bir yol izlenmiştir:

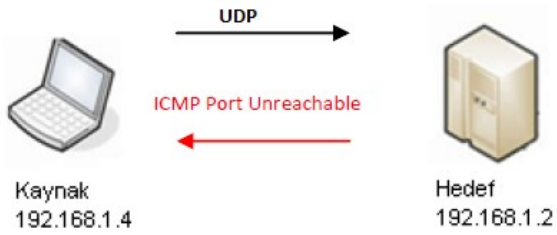
a. ARP scan yapılır (Varsayılan olarak)
b. DNS Çözümlemesi yapılır.
c. TCP Syn Scan yapılır.
d. Service Scan yapılır.
e. Rapor sunulur.

(Page 18-20)

22)

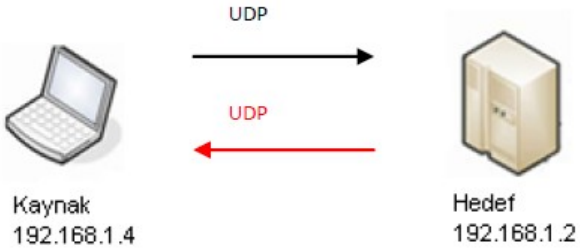
UDP Scan

Gönderilen UDP paketine karşılık ICMP Port Unreachable cevabı dönerse hedef port kapalı anlamına gelir.



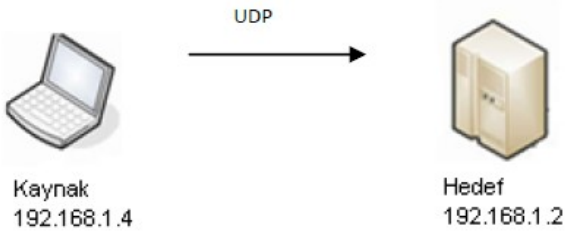
Port Kapalı

Gönderilen UDP paketine karşılık UDP cevabı dönerse port açık anlamına gelir.



Port Açık

Gönderilen UDP paketine karşılık herhangi bir paket dönmezse port open | filtered şeklinde kabul edilir. Yani ne açık olduğu ne de firewall tarafından engellenip engellenmediği tespit edilememiştir anlamına gelir.



Ne açık olduğu ne de filtered olup olmadığı belli

UDP Scan şöyle gerçekleştirilir:

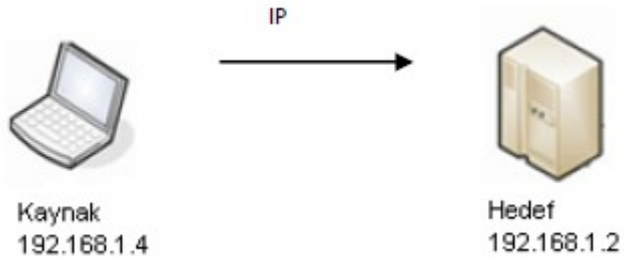
> nmap -sU -v 192.168.0.14

(Page 20-21)

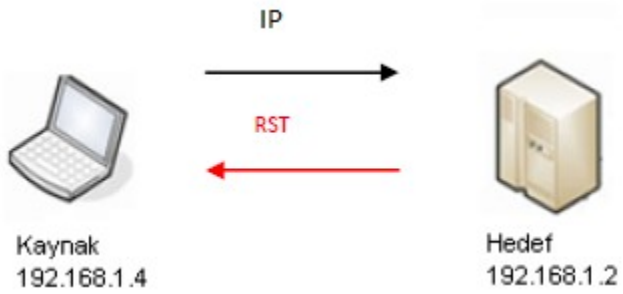
23)

IP Protocol Scan

Gönderilen IP paketine karşılık bir yanıt dönmezse hedef makina erişilemez durumda anlamına gelir.



Gönderilen IP paketine karşılık IP protokolüne mahsus RST bayraklı paket dönerse hedef makina erişilebilir durumda anlamına gelir.



IP Protocol Scan şöyle gerçekleştirilir:

> nmap -sO -v 192.168.0.14

(Page 22-23)

24)

ACK Scan

Gönderilen ACK bayraklı TCP paketlerine karşılık ICMP Destination Unreachable cevabı dönerse ya da herhangi bir cevap dönmezse port “filtered” kabul edilir. Yani bir firewall tarafından port korunuyor anlamına gelir.

Gönderilen ACK’ya karşılık RST bayraklı paket dönüyorsa port “unfiltered” kabul edilir. Yani port erişilebilirdir, fakat açık ya da kapalı olduğu tespit edilememiştir anlamına gelir.

ACK Scan şöyle gerçekleştirilir:

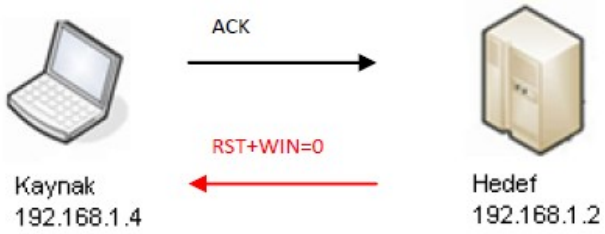
> nmap -sA -v 192.168.0.14

(Page 25-26)

25)

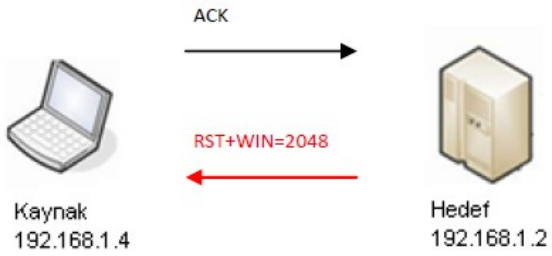
Window Scan

Gönderilen ACK’ya karşılık dönen RST’in window boyutu sıfır ise hedef port kapalı anlamına gelir.



Port Kapalı

Gönderilen ACK'ya karşılık dönen RST'in window boyutu sıfırdan farklı ise hedef port açık anlamına gelir.



Port Açık

Window Scan şöyle gerçekleştirilir:

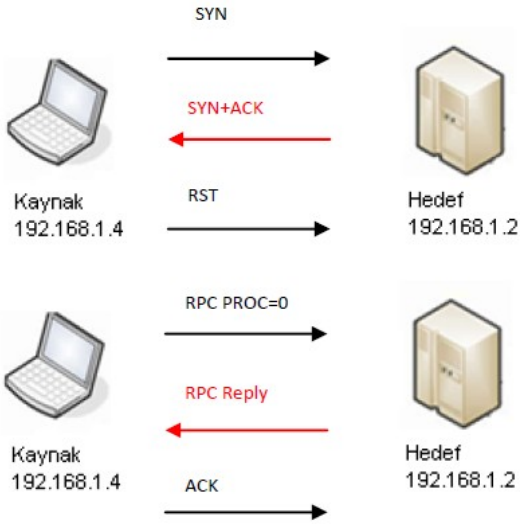
> nmap -sW -v 192.168.0.14

(Page 26-28)

26)

RPC Scan

Açık portlar keşfedildikten sonra gönderilen RPC null paketlerine karşılık RPC Reply paketi geliyorsa hedef portta çalışan bir RPC uygulaması var anlamına gelir.



TCP Syn ile açık portlar tespit edilir. Ardından açık portlara gönderilen RPC null paketlerine karşılık hangisinden RPC Reply geliyorsa o port RPC uygulaması kullanıyor demektir.

RPC Scan şöyle gerçekleştirilir:

> nmap -sR -v 192.168.0.14

Output:

...
PORT STATE SERVICE VERSION
80/tcp open unknown
111/tcp open unknown
2049/tcp open nfs (nfs V2-4) 2-4 (rpc #100003)
...

(Page 28-30)

27)

Active Hosts

Bu tarama türü network'teki aktif cihazları tespit etmek için kullanılır. Network'te online olan hedeflerin IP'sini sıralamaya yarar. Kullanım şekli şu şekildedir:

> nmap -sn 192.168.0.14/24 // -sP de aynı işi yapıyor.

Output:

Starting Nmap 6.47
Nmap scan report for 192.168.0.1
Host is up
Mac Address: 00:10:18:DE:AD:05 (Broadcom)
Nmap scan report for 192.168.0.10
Host is up
Mac Address: 3C:C2:43:5E:ED:C8 (Nokia)
Nmap scan report for 192.168.0.12
Host is up
Mac Address: B8:76:3F:EE:33:0D (Asustek Computer)
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.17 seconds.

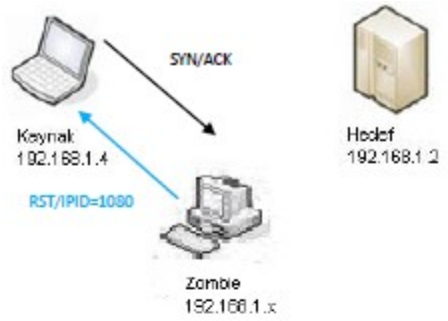
(Page 31)

28)

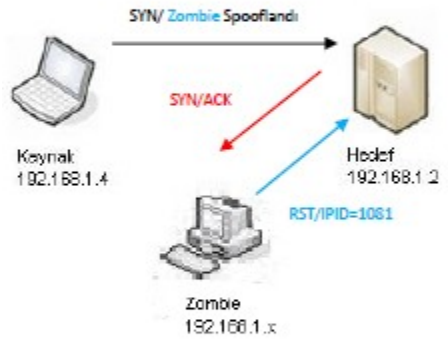
IdleScan

Kaynak makinanın “zombie” olarak adlandırılan aracı makinalar üzerinden hedef makinayı taramasına ve bilgi toplamasına IdleScan denir.

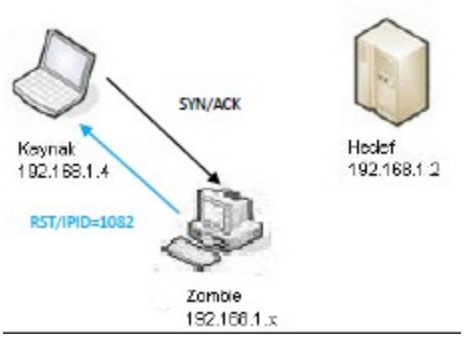
Hedef Portun Açık Olduğu Senaryo



Önce saldırgan kontrolü altındaki zombie’yi kendine SYN paketi göndermesini sağlar. Bunun karşılığında saldırgan zombie’ye SYN/ACK paketi yollar. Ardından zombie ise aldığı paket dolayısıyla 1080 numaralı RST paketi gönderir (1080 numarası referans noktamızdır).

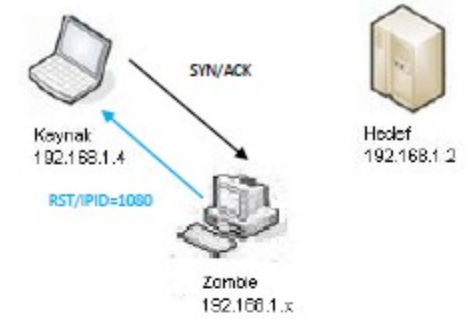


Yukarıdaki işlemlerden sonra saldırgan kaynak IP’si zombie olan bir SYN paketini hedefe yollar. Bunun üzerine hedef de zombie’ye SYN/ACK paketi yollar. SYN/ACK’yı gören zombie de 1081 numaralı bir RST paketi hedefe yollar. Böylece zombine’nin paket numarası 1081 olmuştur.

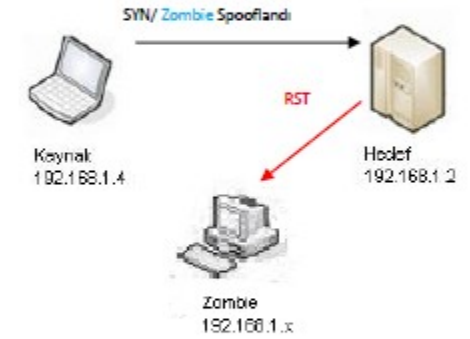


Saldırgan belli bir müddet sonra zombie’yi tekrar kendisine SYN paketi yollaması için tetikler. Ardından saldırgan aldığı SYN paketini SYN/ACK ile yanıtlar. Bunun üzerine zombie 1082 numaralı RST paketiyle noktayı koyar. 1082 numarasını gören saldırgan anlar ki zombie ile hedef arasındaki iletişim sağlıklı gerçekleşmiş, yani demek ki hedef’in portu açıkmış. Hedefin portu açık olmasaydı saldırgan 1082 değil 1081 numaralı RST paketi alırdı ki bu zombie ile hedef arasındaki iletişimin olamadığı, yani hedefin portunun kapalı olduğu anlamına gelirdi.

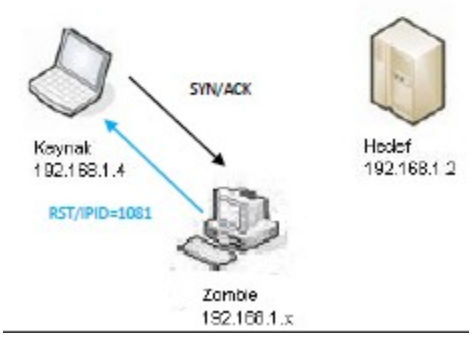
Hedef Portun Kapalı Olduğu Senaryo



Saldırgan 1080 numaralı paketi zombie'den alır.



Zombie hedeften RST paketi aldığı için tepki vermez. Bu yüzden sıradaki gönderilecek paketin numarası 1081 olarak kalmaya devam eder.



Saldırgan SYN/ACK ile zombie'yi yoklar ve zombie bunun üzerine sıradaki paket numarası olan 1081 ile yanıt yollar. 1081 numarasını gören saldırgan anlar ki zombie kendisine yolladığı 1080 nolu paketten beri hiç paket yollamamış ki bana 108**1** nolu paket gönderiyor. Demek ki hedefin portu açık değilmiş ki hedef ile zombie arasında paket alışverişi olmamış der. Böylece hedefin portunun açık mı kapalı mı olduğunu dolaylı yoldan anlamış olur.

Görüldüğü üzere IdleScan ile saldırgan hedefin portlarının açık mı kapalı mı olduğunu hedefte iz bırakmadan öğrenebilmektedir. Hedefe yolladığı paket iz bırakmamaktadır. Çünkü o paketin kaynak IP'si zombie'nin IP'si yapılmıştır. Saldırgan zombine'nin paket numaralarını ilk gelen paket ile son gelen paketten bakarak hedef ile zombie arasında paket alışverişi olup olmadığını anlar. Böylece hedef portun açık olup olmadığını anlar.

IdleScan şöyle gerçekleştirilir:

> nmap -sI -v zombiIP hedefIP

(Page 32)

29)

Nmap Ping Seçenekleri

Nmap taramaya başlamadan önce mutlaka hedef makinayı ping'ler. Nmap'te ping işlemi iki aşamalı gerçekleşir. Önce ICMP Echo isteği gönderilir. Eğer cevap alınmazsa ardından 80. Porta TCP ACK paketi gönderilir. Eğer hedef makina bu iki işleme de cevap vermezse Nmap diğer hedefe geçer. Eğer başka hedef yoksa tarama biter.

Network dünyasında bilinen ping işlemi ICMP Echo isteğinin gönderilip ICMP Echo cevabının dönmesine denir. Ancak Nmap'in ping işlemi biraz kendine özgüdür. Nmap dünyasında ping hedef makinanın döndürebileceği cevaplar (istekler) olarak adlandırılabilir. Nmap'teki ping seçenekleri şunlardır:

a. ICMP Echo Request ve TCP ACK Ping
   Aynı anda gönderilen ICMP Echo isteği ve TCP ACK bayraklı pakete karşılık

   • TCP RST ve
   • ICMP Echo Reply

   paketlerinin dönmesi beklenir. Paketlerin her ikisi de dönerse makina açık, dönmezse makina kapalı anlamına gelir. Bu ping işlemi şöyle gerçekleştirilir:
   > nmap -PB hedefIP

b. ICMP Echo Request Ping
   Gönderilen ICMP Echo isteğine karşılık cevap dönerse makina açık, cevap dönmezse makina kapalı ya da filtered kabul edilir. Bu ping işlemi şöyle gerçekleştirilir:
   > nmap -PE hedefIP

c. TCP ACK Ping

Gönderilen TCP ACK bayraklı pakete karşılık RST bayraklı paket gelirse hedef makina açık, hiçbir paket gelmezse hedef makina kapalı anlamına gelir. Bu ping işlemi şöyle gerçekleştirilir:

> nmap -PA hedefIP

d. TCP SYN Ping

Gönderilen TCP SYN bayraklı pakete karşılık SYN+ACK bayraklı paket gelirse makina açık, RST bayraklı paket gelirse makina kapalı anlamına gelir. Bu ping işlemi şöyle gerçekleştirilir:

> nmap -PS hedefIP

e. UDP Ping

Gönderilen UDP paketine karşılık ICMP Port Unreachable mesajı dönerse makina açık denir, eğer herhangi bir cevap dönmezse makina kapalı denir. Fakat çoğu UDP uygulamaları herhangi bir cevap dönmesine sebebiyet vermediğinden dolayı makinadan yanıt almayınca makina kapalıdır demek her zaman doğru olmayabilir. Bu yüzden hedef makinanın kapalı olduğu bilinen bir portuna bu ping işlemi uygulanarak önceki sonuç test edilmelidir. Bu ping işlemi şöyle gerçekleştirilir:

> nmap -PU hedefIP

f. ICMP Timestamp Ping

Gönderilen ICMP Get Timestamp isteğine karşılık ICMP Sent Timestamp paketi dönerse hedef makina açık demektir, eğer hiçbir paket dönmezse makina kapalı demektir. Bu ping işlemi şöyle gerçekleştirilir:

> nmap -PP hedefIP

g. ICMP Address Mask Ping

Gönderilen ICMP Address Mask isteğine karşılık ICMP Address Mask cevabı dönderse makina açık, dönmezse makina kapalı anlamına gelir. Bu ping işlemi şöyle gerçekleştirilir:

> nmap -PM hedefIP

h. Don’t Ping Before Scanning

Bu seçenek ile Nmap taramalarında yapılan ping işleminin gerçekleştirilmesi engellenir ve direct tarama işlemine geçiş sağlanır. Bu seçeneği kullanabilmek için -PO parametresi kullanılır:

> nmap -PO hedefIP

i. Require Reverse DNS

Reverse DNS işlemi taramalardaki ping işleminden sonra ve scan işleminden önce *zaman zaman* gerçekleştirilir. Bunu her daim yapmak için -R parametresi kullanılmalıdır:

> nmap -R hedefIP

j. Disable Reverse DNS

Reverse DNS işlemi taramalardaki ping işleminden sonra ve scan işleminden önce *zaman zaman* gerçekleştirilir. Taramalarda asla Reverse DNS yapılmaması isteniliyorsa -n parametresi kullanılmalıdır. Böylece ping işleminden sonra direct scan işlemine geçilir ve zaman kazanılmış olunur.

> nmap -n hedefIP

k. Ping Scan (Disable Port Scan)

Taranan makinaların hangisinin açık olduğunu tespit etmek için -sn parametresi kullanılır.

> nmap -sn hedefIP/24

l. Treat All Hosts as Online

Bu seçenek ile host discovery işlemi atlanır ve taranan her makina açıkmış gibi tarama işlemi gerçekleştirilir. Bunun için -Pn parametresi kullanılır.

> nmap -Pn hedefIP/24

Benim NOT: Ping scan'lardan her biri bir diğerinin bulamadığı host'u bulabiliyor. Dolayısıyla her biri denenip tüm açık hostlar not defterine kaydedilerek bulunabilir ya da en azından bulunması mümkün olan tüm host'lar elde edilebilmiş olur.

(Page 34-37)

30)

OS İzi Belirleme

> nmap -O 192.168.0.14

Output:

```
at 2010-08-01 20:01 EEST
Nmap scan report for 192.168.1.2
Host is up (0.0020s latency).              // Ping işlemi sonuçlanır.
Not shown: 995 closed ports                // Port taraması sonuçlanır.
PORT STATE SERVICE
22/tcp open ssh
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
2049/tcp open nfs
MAC Address: 00:0C:29:D7:D3:65 (VMware)
Device type: general purpose
Running: Linux 2.6.X                      // İşletim sistemi analizi sonuçlanır.
```

OS details: Linux 2.6.24 - 2.6.31
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at http://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 4.78 seconds

(Page 37-38)

31)

OS izi Belirleme Seçenekleri

a. --osscan-limit : En az bir açık ve bir kapalı portu bulunan hedeflerin OS izini belirlemeye çalışır.
b. --osscan-guess : Daha agresif bir şekilde OS izini belirlemeye çalışır.
c. --max-retries <sayi> : Belirtilen sayı miktarınca OS izi belirleme denemesi yapar.

(Page 38)

32)

Nmap Scripting Engine (NSE)

NSE var olan Nmap yeteneklerini geliştirmek için kullanılan bir yapıdır. NSE script'lerinin yapabildiklerine dair örnek olarak şunlar verilebilir:

a. Advanced Network Discovery
   Whois lookup sorguları ve ek protokol sorguları ile bilgi toplar. Ayrıca erişilebilir network paylaşımlarını dinleyen servisler için istemci gibi davranarak bilgi toplamaya çalışır.
b. Advanced Version Detection
   Karmaşık versiyon araştırmaları yapar ve servisleri brute force saldırısı düzenleyerek tespit etmeye çalışır.
c. Vulnerability Discovery
   Belirli zafiyetler hedef sistemde var mı yok mu diye araştırma yapar.
d. Malicious Software Discovery
   Virus, worm, Trojan gibi zararlı yazılımlar hedef sistemde var mı yok mu diye araştırma yapar.
e. Exploiting
   Bulunan zafiyetleri kullanarak sızma işlemini gerçekleştirmeye denir.

NSE script’leri Nmap’in kök dizinindeki scripts adlı klasörde depoludur. Bu script’ler script.db adlı bir veritabanı dosyasında Güvenli Giriş, Zorla Giriş, Zararlı Yazılım, Arka Kapı, Versiyon, Keşif, Zafiyet şeklinde sınıflandırılarak kayıt altına alınmıştır.

Default script’i hedef üzerinde denemek için -sC kullanılır:

```
> nmap -sC 192.168.1.0/24   // ya da nmap --script=default 192.168.1.0/24
```

Nmap’te var olan script’lerden birini çalıştırmak için --script= parametresi kullanılır. Örn;

```
> nmap --script=vulnerability 192.168.1.34
```

Belirli bir dizinin altındaki script’ler çalıştırılmak istenirse aşağıdaki seçenek kullanılmalıdır:

```
> nmap --script=/myScripts 192.168.1.0/24   // Klasörün nmap’in kök
                                            // dizininde yer aldığı
                                            // varsayılmıştır.
```

Bütün script’lerin çalışması istenirse aşağıdaki seçenek kullanılır:

```
> nmap --script=all 192.168.1.55
```

(Page 38-40)

33)

NSE Seçenekleri

- --script-updatedb : Script’lerin bulunduğu veritabanını günceller.
- --script-trace : Script’e ait bütün iç ve dış iletişimin çıktısını ekrana basmaya yarar.

(Page 40)

34)

Güvenlik Ürünleri Karşısında Nmap

Nmap taranılacak hedeflerin önünde bulunan güvenlik ürünlerinin kısıtlaması nedeniyle istenildiği şekilde çalışamayabilir. Günümüzdeki güvenlik ürünleri Nmap ve taramalarını rahatlıkla yakalayabilmektedir. Ancak Nmap kendi bünyesinde bulunan bazı seçenekler vasıtasıyla bu güvenlik ürünlerini atlatabilmektedir. Bu seçenekler Fragmentation, Spoofing ve Packet Manipulating olarak ayrılmaktadırlar. Bu seçenekler vasıtasıyla Nmap güvenlik ürünlerini atlatıp taramalarını daha rahat bir şekilde gerçekleştirebilmektedir.

Fragmentation

Eğer parçalanmak istenilen Nmap paketlerinin maksimum boyutu IP başlık bilgisi hariç 8 byte olması isteniyorsa -f parametresi kullanılır.

> nmap -f hedefIP

Eğer parçalanmak istenilen Nmap paketlerinin maksimum boyutu IP başlık bilgisi hariç 16 byte olması isteniyorsa -f -f şeklinde ardarda f kullanılır:

> nmap -f -f hedefIP

Eğer parçalanmak istenilen Nmap paketlerinin maksimum boyutunu IP başlık bilgisi hariç olmak kaydıyla elle belirlemek istiyorsak --mtu parametresi kullanılmalıdır:

> nmap --mtu <sayi> hedefIP

Spoofing

a. IP Spoofing

Nmap tarama paketlerinin başka bilgisayardan geliyormuş gibi yapmak için -D parametresi kullanılır. Ancak spoof niyetiyle kullanılacak IP’nin taramanın yapılacağı ortamla uyumlu olması çok önemlidir. Private IP kullanılan LAN ortamında Reel IP ile tarama yapılıyormuş gibi göstermek pek akıllıca bir iş olmayacaktır. Böylesi bir durumda direk spoofing yapıldığı anlaşılır.

> nmap -D spooflananIP hedefIP

Eğer spoof için IP belirtilmezse Nmap paketlerinin kaynak IP’sine rastgele bir IP koyacaktır. Bu yine duruma göre spoofing’in anlaşılmasına yol açabilmektedir.

b. Mac Spoofing

Nmap taramaları ile oluşturulan paketlere kaynak mac adresi olarak farklı mac adresi girilebilmektedir. Hatta mac adresi yerine vendor ismi ya da vendor ön eki girilebilir. Eğer mac adresi yerine 0 sayısı girilirse mac adresini Nmap kendisi belirler.

```
> nmap --spoof-mac 11:22:33:44:55:66  192.168.1.0/24
> nmap --spoof-mac D-Link  192.168.1.0/24
> nmap --spoof-mac 000D93  192.168.1.0/24
> nmap --spoof-mac 0  192.168.1.0/24
```

Packet Manipulating

Güvenlik cihazlarını atlatmak için Nmap çok sayıda packet manipüle etme seçenekleri barındırır. Aşağıda bu seçeneklerden bazısı ve açıklamaları verilmiştir:

a. --data-length <sayi> : Paket boyutunun sahip olması gereken uzunluğunu belirler.
b. --ttl <deger> : Paketin ne zaman düşürülebileceğini belirler (time to live).
c. --badsum : Yanlış checksum başlığına sahip TCP veya UDP paketleri gönderir.

(Page 40-42)