PENTEST EĞİTİMİ
UYGULAMA KİTABI

BÖLÜM - 2

İÇİNDEKİLER

2. PORT TARAMA ve KEŞİF ÇALIŞMALARI

BU KATEGORİDEKİ LAB UYGULAMA LİSTESİ

2.1. Nmap Kullanarak Açık Sistemlerin Belirlenmesi

Amaç: Çeşitli metotlar (ARping, UDPing, TCPing) kullanarak hedef sistemlerin ayakta olup olmadığının belirlenmesi.

Kullanılan Araçlar:

● Nmap

Adımlar:

1. Adım: Hedef sistemin (cnn.com) 21 portuna TCP SYN paketi göndererek hedefin ayakta olup olmadığını görelim. Hedef sistemin 21 portuna erişim olmadığı için hedefin "down" olduğunu görmemiz beklenmektedir.

```
root@pentest09:/home/celal# nmap -sP -PS21 cnn.com
Starting Nmap 6.01 ( http://nmap.org ) at 2012-12-09 01:46 EET
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.09 seconds
```

2. Adım: Hedef sistemin(cnn.com) 80 portuna TCP SYN paketi göndererek hedefin ayakta olup olmadığı tespit edilebilir. Hedef sistemin 80 portuna erişim olduğu için hedefin "up" olduğunun görülmesi beklenmektedir.

```
root@pentest09:/home/celal# nmap -sP -PS80 cnn.com
Starting Nmap 6.01 ( http://nmap.org ) at 2012-12-09 01:46 EET
Nmap scan report for cnn.com (157.166.255.19)
Host is up (0.26s latency).
Other addresses for cnn.com (not scanned): 157.166.226.25 157.166.226.26 157.166.255.18
Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
```

3. Adım: Yine, hedef sistemin(cnn.com) 22 portuna TCP ACK paketi göndererek hedefin ayakta olup olmadığı tespit edilebilir. Hedef sistemin 22 portuna erişim olmadığı için hedefin "down" olduğunun görülmesi beklenmektedir.

```
root@pentest09:/home/celal# nmap -sP -PA22 cnn.com
Starting Nmap 6.01 ( http://nmap.org ) at 2012-12-09 01:49 EET
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.09 seconds
```

4. Adım: Hedef sistemin(cnn.com) 80 portuna TCP ACK paketi göndererek hedefin ayakta olup olmadığı tespit edilebilir. Hedef sistemin 80 portuna erişim olduğu ve ACK paketlerine cevap verdiği için hedefin "up" olduğunun görülmesi beklenmektedir.

```
root@pentest09:/home/celal# nmap -sP -PA80 cnn.com
Starting Nmap 6.01 ( http://nmap.org ) at 2012-12-09 01:51 EET
Nmap scan report for cnn.com (157.166.226.26)
```

```
Host is up (0.24s latency).
Other addresses for cnn.com (not scanned): 157.166.255.18 157.166.255.19 157.166.226.25
rDNS record for 157.166.226.26: www.cnn.com
Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

5. Adım: UDP ping genelde sistemin ayakta olup olmadığını tespit etmede başarılı değildir. Bu nedenle tercih edilmemektedir. UDP ping için ilgili nmap parametresi -PU şeklindedir.

Ek Kaynaklar:

- www.insecure.org

2.2. Nmap Kullanarak Belirli Ip Aralığındaki Belirli Port Aralığını Tarama

Amaç: Sadece belirli IP adreslerinin istenilen portlarına yönelik taramalar yapıp sonuçlarını gözlemleme.
Kullanılan Araçlar:

- Nmap

Adımlar:
1. Adım: Nmap aracı kullanılarak, hedef olarak seçilen 192.168.21.141 adresinin 1-3389 arasındaki TCP portlarını taranacaktır. Gerçek sistemlerde taramalar zaman almaktadır. Taranmak için seçilen sistemin ayakta olup olmadığı tespit edilmeden taranmaya başlanması durumunda yapılan çalışmalar boşa gidebilmektedir. Bu olası zaman kaybını önlemek adına önce sistemin ayakta olup olmadığı test edilmelidir.

Nmap ön tanımlı olarak taramaya geçmeden önce hedefin ayakta olup olmadığı test edilmelidir.

```
root@kali:~# nmap 192.168.21.141 -sn

Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-17 10:21 EST
Nmap scan report for 192.168.21.141
Host is up (0.00026s latency).
MAC Address: 00:0C:29:BF:F5:B9 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

Görüldüğü üzere hedef sistem hakkında "**Host is up" bilgisi alınmıştır**. Nmap taramaları çok çeşitlidir ve çeşitleri ihtiyaç ile birlikte ortaya çıkmıştır. Bu tarama yönteminde kullanılan "**-sn**" parametresi sistemin ayakta olup olmadığını sisteme SYN paketleri göndererek tespit etmektedir. Bu tarama yöntemi çok hızlı bir tarama yöntemidir. Fakat sistem bir güvenlik duvarı tarafından korunuyor ise bu tarama yöntemi ile hedef sistem hakkında bilgi almak zor olacaktır. Bu durumda "**-Pn**" parametresi kullanılmalıdır. Fakat güvenlik önlemleri tam olarak alınmış sistemler hakkında bilgi almak çok zor olabilir.

1. Adım: Ayakta olduğu tespit edilen sisteme ait belirli port aralığının taranması;

```
root@kali:~# nmap 192.168.21.141 -Pn --open -p1-3389

Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-17 10:30 EST
Nmap scan report for 192.168.21.141
Host is up (0.00011s latency).
Not shown: 3385 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:BF:F5:B9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 3.36 seconds
```

Bu örnekte kullanılan:
--open: Parametresi sadece açık olan portları raporlamaktadır.
-Pn: Parametresi hedef sistemde yapılan port taramalarında ping paketlerini kullanılmaması gerektiğini vurgulamaktadır(Hedef sistemlerin güvenlik duvarları tarafından korunduğu durumlarda kullanılmaktadır).
-p: Parametre ile hedef sistem üzerinde taranmak istenen portların belirtilmeksi için kullanılır.
Tarama sonucunda görüldüğü üzere hedef sistemde 135, 139, 445, 3389 portları açıktır.

2.3. Nmap Kullanarak Çalışan Servis Sürümlerini Belirleme

Amaç: Açık olan portu kullanan servisin ismini ve sürümünü tespit etme.
Kullanılan Araçlar:

- Nmap

Adımlar:

1. **Adım:** Nmap kullanılarak google.com domainin TCP/80 portunda çalışan servis belirlenecektir.

```
root@kali:~# nmap google.com -sV -p 80

Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-17 10:55 EST
Nmap scan report for google.com (216.58.209.14)
Host is up (0.025s latency).
rDNS record for 216.58.209.14: sof01s12-in-f14.1e100.net
PORT   STATE SERVICE VERSION
80/tcp open  http    Google httpd 2.0 (GFE)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.34 seconds
```

Görüldüğü gibi google web server olarak kendisine ait olan Google httpd kullanmaktadır. Ve kullandığı versiyonu 2.0'dır. **-sV** parametresi ile açık bulunan portlarda çalışan servis bilgisi ve versiyonu öğrenilebilir.

2.4. Nmap Kullanarak İşletim Sistemi Belirleme

Amaç: Hedef sistem üzerinde çalışan işletim sistemini tespit etmek.
Kullanılan Araçlar:

- Nmap

Adımlar:

1. **Adım:** Nmap -O parametresi ile uzak sistemde çalışan işletim sistemini tespit edelim. Nmap işletim sistemini tespit işleminde 1 açık port 1 kapalı port bulduğu durumlarda en sağlıklı bilgi verir. Aksi durumda kendi işletim sistemini ekrana basar.

```
root@bt:~# nmap 10.10.10.5 -O -n
Starting Nmap 6.00 ( http://nmap.org ) at 2012-11-10 22:32 EET
Nmap scan report for 85.95.238.171
Host is up (0.00014s latency).
Not shown: 994 closed ports
PORT STATE SERVICE
53/tcp open domain
135/tcp open msrpc
139/tcp open netbios-ssn
443/tcp open https
1027/tcp open IIS
1029/tcp open ms-lsa
MAC Address: 00:0C:29:3A:AE:DD (VMware)
Device type: general purpose
Running: Microsoft Windows 2003
OS CPE: cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2
OS details: Microsoft Windows Server 2003 SP1 or SP2
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 2.81 seconds
```

Nmap hedefin işletim sistemini belirlerken öncelikle sistem üzerinde bir açık bir kapalı port bulması gerekir. Aksi halde sağlıklı sonuç bulamayabilir. Açık ve kapalı porta gönderdiği paketlere dönülen cevaplardaki TTL değerlerinden hedef sistemi tespit eder.

2.5. Bir Ağda Yer Alan Tomcat Sunucularının Tespiti

Amaç: Nmap aracı ile hedef sistemlerde tomcat sunucularının varlığının tespit edilmesi.
Kullanılan Araçlar: nmap
Uygulama: Tomcat sunucuları ön tanımlı olarak 8080 portunda hizmet vermektedir. Ancak düzenlemeler ile başka portlarda hizmet verebilmesi de sağlanabilmektedir. Bu yüzden hedef sistemler bilinen web sunucu portlarının servis tespiti yapacak şekilde taranması gerekmektedir.
Bilinen web sunucu portları: 80, 443, 8080, 8081, 8090, 8091.
Tomcat tespiti için nmap'de işlenmesi gereken komut;

```
root@kali:~# nmap 192.168.1.0/24 -p 80,443,8080,8081,8090,8091 -sV --open -n

Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-05 07:48 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00056s latency).
Not shown: 4 closed ports
PORT    STATE SERVICE  VERSION
80/tcp  open  http?
443/tcp open  ssl/http micro_httpd
MAC Address: 4C:9E:FF:39:09:5C (ZyXEL Communications)

Nmap scan report for 192.168.1.37
Host is up (0.000098s latency).
Not shown: 5 closed ports
PORT    STATE SERVICE  VERSION
443/tcp open  ssl/http VMware VirtualCenter Web service
MAC Address: 44:8A:5B:EC:5E:48 (Micro-Star INT'L CO.)

Nmap scan report for 192.168.1.45
Host is up (0.00013s latency).
Not shown: 3 closed ports
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Apache httpd 2.2.22 ((Ubuntu))
443/tcp  open  ssl/http Apache httpd 2.2.22 ((Ubuntu))
8080/tcp open  http     Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:B0:8F:7C (VMware)

Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 256 IP addresses (7 hosts up) scanned in 22.53 seconds
```

Kullanılan parametrelerin açıklamaları:
-p: Taranacak port adresleri
-sV: Hedef portlarda çalışan servislerin versiyon bilgileri
--open: Hedef portların sadece açık olanların ekrana basılması
-n: Dns ismi çözülmesinin engellenmesi(Daha hızlı bir tarama için önerilmektedir)
Görüldüğü üzere hedef sistemlerden 192.168.1.45 adresinde 8080 portunda bulunan bir Tomcat sunucusu tespit edilmiştir.

2.6. Nmap Kullanarak TCP/UDP Port Tarama

Amaç: Hedef sistemler üzerindeki portların durumlarını(open, closed, filtered) öğrenme.

Kullanılan Araçlar:
Adımlar:

1. **Adım:** Nmap kullanarak bga.com.tr sitesinin TCP 21, 80, 443 portları taranacaktır;

```
root@pentest09:~# nmap bga.com.tr -p 80,21,443 -sS

Starting Nmap 6.01 ( http://nmap.org ) at 2012-11-29 00:35 EET
Nmap scan report for bga.com.tr (50.22.202.162)
Host is up (0.17s latency).
rDNS record for 50.22.202.162: 50.22.202.162-static.reverse.softlayer.com
PORT    STATE  SERVICE
21/tcp  closed ftp
80/tcp  open   http
443/tcp open   https

Nmap done: 1 IP address (1 host up) scanned in 2.10 seconds
```

sS parameteresi hedefe TCP Syn scan yapılacağını gösterir.

2. **Adım:** Nmap kullanarak 8.8.8.8 IP adresinin UDP 53 portunu tarayalım
3. **Adım**: Port durumunun açık mı filtreli mi olduğundan emin olamadığı için open|filtered dönmektedir. Fakat emin olmak için -sV komutu ile çalıştırılmalıdır.

```
root@pentest09:~# nmap 8.8.8.8 -p 53 -sU -sV

Starting Nmap 6.01 ( http://nmap.org ) at 2012-11-29 00:39 EET
Nmap scan report for google-public-dns-a.google.com (8.8.8.8)
Host is up (0.061s latency).
PORT   STATE SERVICE VERSION
53/udp open  domain  NetWare dnsd

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.97 seconds
root@pentest09:~#
```

Portun açık olduğu böylece tespit edilmiştir.

2.7. Nmap NSE ile SMB Dosya Paylaşımlarını Tespit Etmek

Amaç: Hedef ağdaki tüm sistemlerin üzerinde genele açık paylaşım dosyalarını tespit etmek, hassas verilere ulaşmak.
Lab senaryosu: Bu uygulama internet erişimine sahip Backtrack Linux dağıtımı kullanılarak hazırlanmıştır.
Kullanılan Araçlar:

- Nmap

Adımlar:

1. **Adım:** 6.6.6.90-99 IP aralığındaki sistemlere yönelik smb paylaşım taraması yapılacaktır;

```
root@bt:~# nmap 6.6.6.90-99 --script=smb-enum-shares -PN -p 139,445 -n
Starting Nmap 6.01 ( http://nmap.org ) at 2012-11-29 10:28 EET
Nmap scan report for 6.6.6.97
Host is up (0.016s latency).
PORT STATE SERVICE
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 00:0C:29:6E:1B:8F (VMware)
Host script results:
| smb-enum-shares:
| ADMIN$
| Anonymous access: <none>
| C$
| Anonymous access: <none>
| IPC$
|_ Anonymous access: READ
Nmap done: 10 IP addresses (6 hosts up) scanned in 6.42 second
```

2. **Adım:** Read/Write haklara sahip paylaşımlar bulunacaktır;

```
root@bt:~# nmap 6.6.6.100-150 --script=smb-enum-shares -PN -p 139,445 -n
Nmap scan report for 6.6.6.110
Host is up (0.0035s latency).
PORT STATE SERVICE
139/tcp open netbios-ssn
445/tcp open microsoft-ds
Host script results:
| smb-enum-shares:
```

```
| ADMIN$
| Anonymous access: <none>
| Current user ('guest') access: <none>
| C$
| Anonymous access: <none>
| Current user ('guest') access: <none>
| Com Printers
| Anonymous access: <none>
| Current user ('guest') access: READ
| D$
| Anonymous access: <none>
| Current user ('guest') access: <none>
| IPC$
| Anonymous access: READ <not a file share>
| Current user ('guest') access: READ <not a file share>
| PaylasılanDosya
| Anonymous access: <none>
|_ Current user ('guest') access: READ/WRITE
```

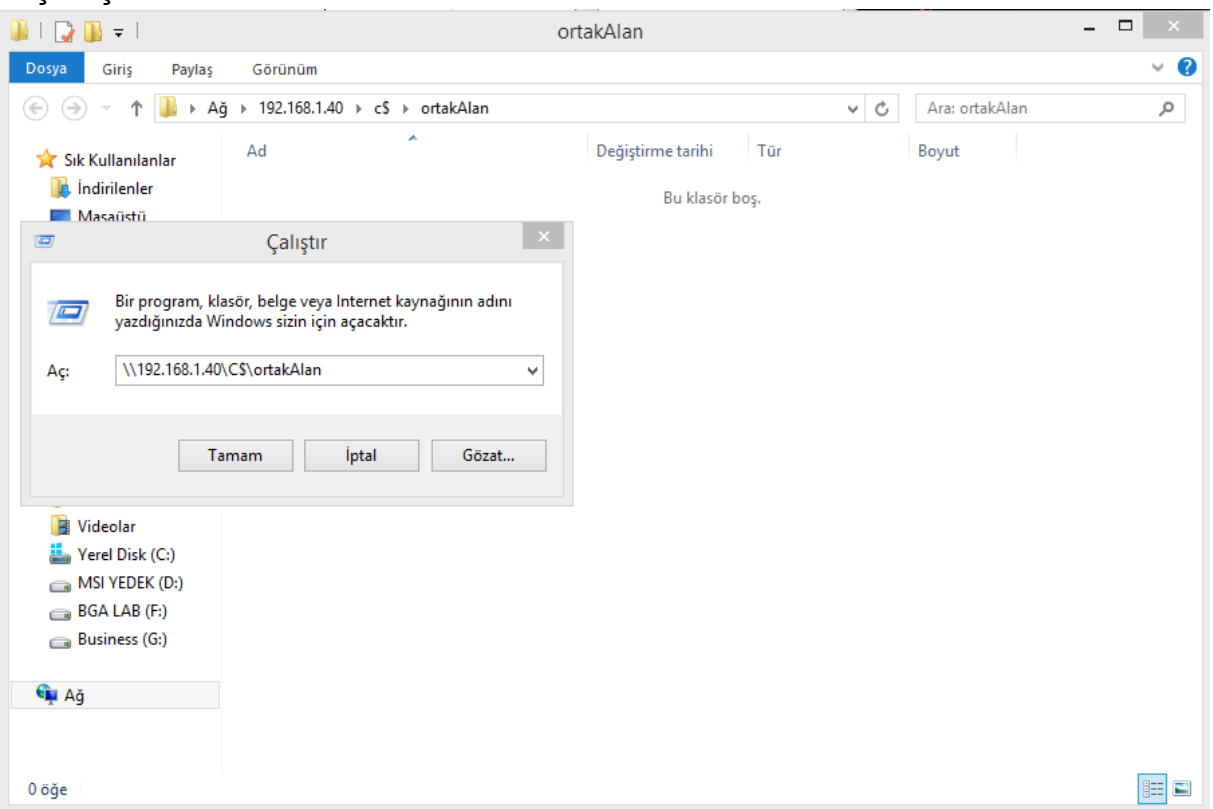
2.8. Nmap NSE Kullanarak Genele Açık Paylaşımların Tespiti

Amaç: Nmap scriptleri yardımıyla bir ağda bulunan ve yetkisiz erişime izin verilmiş paylaşımların tespit edilmesi.

Kullanılan Araçlar: nmap
Uygulama: Bir ağdaki paylaşımlar güvenli ve kontrollü bir şekilde paylaşılmaması halide, yetkisiz kişiler bu paylaşımlara erişebilirler. Yazma haklarının bulunması durumunda verileri değiştirme imkanı oluşabilir. Bu durum güvenlik ihlali oluşturur.
nmap scriptleri aracılığıyla, hedef sistemlerde yetkisiz paylaşımların tespit edilebilmesi mümkündür.
Yetkisiz paylaşımların tespit edebilmek için kullanılacak script “sbm-enum-shares” tir.

```
root@kali:~# nmap --script smb-enum-shares 192.168.1.40 -p 139

Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-05 09:03 EDT
Nmap scan report for 192.168.1.40
Host is up (0.00020s latency).
PORT    STATE SERVICE
139/tcp open  netbios-ssn
MAC Address: 00:0C:29:75:90:01 (VMware)

Host script results:
| smb-enum-shares:
|   ADMIN$
|     Anonymous access: <none>
|     Current user ('guest') access: <none>
|   C$
|     Anonymous access: <none>
|     Current user ('guest') access: <none>
|   IPC$
|     Anonymous access: READ <not a file share>
|     Current user ('guest') access: READ <not a file share>
|   Users
|     Anonymous access: <none>
|     Current user ('guest') access: READ
|   ortakAlan
|     Anonymous access: <none>
|     Current user ('guest') access: READ/WRITE
|   ortakAlan-Herkes
|     Anonymous access: <none>
|_    Current user ('guest') access: READ/WRITE

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

Görüldüğü üzere hedef sistemde “ortakAlan” ve “ortakAlan-Herkes” paylaşımları herkese açıktır. Bunu doğrulamak için hedef sistemde adı verilen paylaşımlara erişilmiştir.



2.9. Nmap NSE Kullanarak Güvenlik Açığı Tespit Etme

Amaç: Hedef sistemde 21 nolu portta açık olarak bulunan FTP servisinin, Anonymous FTP zafiyetine sahip olup olmadığının tespit edilmesi.

Kullanılan Araçlar:

- Nmap NSE

Adımlar:

1. Adım: Nmap Script Engine(NSE) kullanarak FTP hizmetinin Anonymous kullanıcısının parolası boş ise bunun tespit edilecektir.

```
root@bt:/usr/local/share/nmap/scripts# nmap 10.10.15.12 -p 21 --script=ftp-anon -PN -n
Starting Nmap 6.00 ( http://nmap.org ) at 2012-11-10 21:56 EET
Nmap scan report for 10.10.15.12
Host is up (0.0048s latency).
PORT STATE SERVICE
21/tcp open ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x 2 0 0 4096 Mar 10 2011 pub
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

Tüm NSE scriptlerini görmek için **/usr/local/share/nmap/scripts** dizinine bakılabilir.

2. Adım: NSE kullanarak belli bir IP aralığındaki MS08-067 açıklığı ve Conficker virüsüne sahip sunucuları bulalım. Bu taramayı smb-check-vulns.nse isimli script ile aşağıda gösterildiği şekilde gerçekleştirebiliriz.

```
root@bt:~# nmap 6.6.6.90-99 --script=smb-check-vulns -PN -p 139,445 -n
Starting Nmap 6.01 ( http://nmap.org ) at 2012-11-29 09:32 EET
Nmap scan report for 6.6.6.97
Host is up (0.0057s latency).
PORT STATE SERVICE
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 00:0C:29:6E:1B:8F (VMware)
Host script results:
| smb-check-vulns:
| MS08-067: VULNERABLE
| Conficker: Likely CLEAN
| regsvc DoS: CHECK DISABLED (add '--script-args=unsafe=1' to run)
| SMBv2 DoS (CVE-2009-3103): CHECK DISABLED (add '--script-args=unsafe=1' to run)
| MS06-025: CHECK DISABLED (remove 'safe=1' argument to run)
```

```
|_ MS07-029: CHECK DISABLED (remove 'safe=1' argument to run)
Nmap done: 10 IP addresses (5 hosts up) scanned in 0.80 seconds
```

2.10. İleri Seviye Nmap Kullanımı

Amaç: Nmap aracının kullanılarak hedef sistemlere yönelik yapılan testlerin ağda trafik oluşturup dikkat çekmesini önlemek için tarama hızının düşürülmesi.

Kullanılan Araçlar: nmap
Uygulama: Tarama işleminin yerel ağlarda dikkat çekici trafik oluşturmaması ve farklı güvenlik cihazları tarafından tespit edilmemesi için farklı özelliklerle taranması gerekebilmektedir. Bu özelliklerden bir tanesi hızdır. Nmap ile tarama hızını düşürmek mümkündür.
Herhangi bir düzenlemeye gidilmeden taranmış bir hedefe ait çıktı;

```
root@kali:~# nmap 192.168.1.45

Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-04 19:17 EDT
Nmap scan report for 192.168.1.45
Host is up (0.000072s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
8080/tcp open  http-proxy
MAC Address: 00:0C:29:B0:8F:7C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

Şimdi ise saniyede 20 paket olacak şekilde bir tarama yapılması ile elde edilen tarama;

```
root@kali:~# nmap 192.168.1.45 --max-rate 20

Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-04 18:45 EDT
Nmap scan report for 192.168.1.45
Host is up (0.00034s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
```

```
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
8080/tcp open  http-proxy
MAC Address: 00:0C:29:B0:8F:7C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 50.01 seconds
```

Görüldüğü gibi aynı tarama çok daha yavaş gerçekleştirilmiştir.

2.11. Parçalanmış Paketlerle Port Tarama

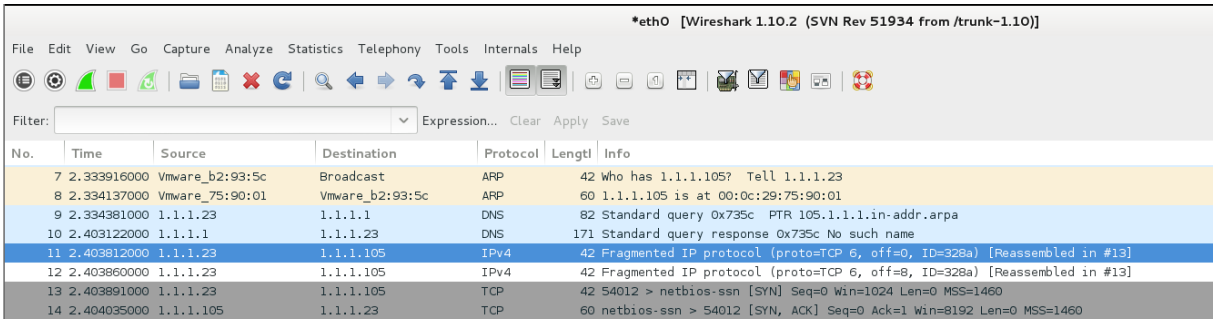
Amaç: nmap ile port taramalarını güvenlik duvarı ve IDS sistemlere takılmadan gerçekleştirmek.

Kullanılan Araçlar: nmap
Uygulama: Nmap ile yapılan bazı taramalar güvenlik duvarları ve IDS sistemleri tarafından tespit edilebilmekte ve log altına alınabilmektedir. Bu cihazlara takılmadan taramaların gerçekleştirilmesi için taramalar küçük paketlere bölünerek gönderilebilir. Güvenlik duvarı ve IDS sistemeler bu paketleri incelediklerinde anlam veremeyecekleri için bunun bir port tarama işlemi olduğunu da anlayamacaklardır.
nmap ile paketlerin parçalanarak gönderilmesi için kullanılması gereken parametreler: **-f** ve **–mtu** parametreleridir.
-f parametresi tek başına kullanıldığında 20 byte'lık IP başlıklarını 16 byte'lık parçalara böler, yani bir paketi 3 parçaya bölmüş olur. Gönderilen paketlerin offset değerlerini manuel olarak ayarlayıp boyutu değiştirmek içinse **mtu** parametresi kullanılabilir. **MTU** parametresine atanacak değer 8 ve katları olmalıdır.
-f parametresi ile birlikte kullanılmış bir örnek tarama sonucu aşağıda verilmiştir.

```
root@kali:~# nmap --script smb-enum-shares 1.1.1.105 -p 139 -f

Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-05 10:52 EDT
Nmap scan report for 1.1.1.105
Host is up (0.00023s latency).
PORT    STATE SERVICE
139/tcp open  netbios-ssn
MAC Address: 00:0C:29:75:90:01 (VMware)

Host script results:
| smb-enum-shares:
|   ADMIN$
|     Anonymous access: <none>
|     Current user ('guest') access: <none>
|   C$
|     Anonymous access: <none>
|     Current user ('guest') access: <none>
|   IPC$
|     Anonymous access: READ <not a file share>
|     Current user ('guest') access: READ <not a file share>
|   Users
|     Anonymous access: <none>
```

```
|     Current user ('guest') access: READ
|   ortakAlan
|     Anonymous access: <none>
|     Current user ('guest') access: READ/WRITE
|   ortakAlan-Herkes
|     Anonymous access: <none>
|_    Current user ('guest') access: READ/WRITE

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

Bir paket sniffer aracılığı ile ortam dinlenip değerler incelenecek olunursa elde edilecek sonuç:



Görüldüğü üzere fragmented paketler şeklinde görülecektir.

MTU parametresi ile örnek bir kullanım örneği;

```
root@kali:~# nmap --script smb-enum-shares 1.1.1.105 -p 139 --mtu 8

Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-05 10:55 EDT
Nmap scan report for 1.1.1.105
Host is up (0.00024s latency).
PORT    STATE SERVICE
139/tcp open  netbios-ssn
MAC Address: 00:0C:29:75:90:01 (VMware)

Host script results:
| smb-enum-shares:
|   ADMIN$
|     Anonymous access: <none>
|     Current user ('guest') access: <none>
|   C$
|     Anonymous access: <none>
|     Current user ('guest') access: <none>
|   IPC$
|     Anonymous access: READ <not a file share>
|     Current user ('guest') access: READ <not a file share>
```

```
|   Users
|     Anonymous access: <none>
|     Current user ('guest') access: READ
|   ortakAlan
|     Anonymous access: <none>
|     Current user ('guest') access: READ/WRITE
|   ortakAlan-Herkes
|     Anonymous access: <none>
|_    Current user ('guest') access: READ/WRITE

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

Yine ortam bir sniffer ile dinlendiğinde elde edilen trafik şu şekildedir:

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Lengtl	Info
1	0.000000000	Vmware_b2:93:5c	Broadcast	ARP	42	Who has 1.1.1.105? Tell 1.1.1.23
2	0.000212000	Vmware_75:90:01	Vmware_b2:93:5c	ARP	60	1.1.1.105 is at 00:0c:29:75:90:01
3	0.000462000	1.1.1.23	1.1.1.1	DNS	82	Standard query 0xc528 PTR 105.1.1.1.in-addr.arpa
4	0.060984000	1.1.1.1	1.1.1.23	DNS	171	Standard query response 0xc528 No such name
5	0.061615000	1.1.1.23	1.1.1.105	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID=d2c1) [Reassembled in #7]
6	0.061676000	1.1.1.23	1.1.1.105	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=8, ID=d2c1) [Reassembled in #7]
7	0.061707000	1.1.1.23	1.1.1.105	TCP	42	52590 > netbios-ssn [SYN] Seq=0 Win=1024 Len=0 MSS=1460
8	0.061884000	Vmware_75:90:01	Broadcast	ARP	60	Who has 1.1.1.23? Tell 1.1.1.105
9	0.061897000	Vmware_b2:93:5c	Vmware_75:90:01	ARP	42	1.1.1.23 is at 00:0c:29:b2:93:5c
10	0.061997000	1.1.1.105	1.1.1.23	TCP	60	netbios-ssn > 52590 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460

2.12. Sahte IP/Tuzak Sistemler Kullanarak Port Tarama

Amaç: Kimliğimizi gizleyerek hedef sistem üzerinde taramalar gerçekleştirme

Kullanılan Araçlar:

- Nmap

Adımlar:

1.Adım: Nmap aracı kullanılarak bir sahte IP havuzu oluşturulacaktır. Saldırganın IP adresi bu oluşturulan IP havuzunda bulunmaktadır. Havuz istenilen IP'lerden veya rastgele seçilecek IP adreslerinden oluşabilir. Bu havuzdaki IP adreslerinden hedefe yönelik aynı anda port taraması yapılacaktır. Bu şekilde hedef sistem şaşırtılacaktır.
İstenilen IP adresleri ile hedefe yönelik port taraması (-D IP1,IP2,IP3...):

```
sh-3.2# nmap bga.com.tr -D 212.23.23.145,11.12.45.6,5.5.5.5 -p 80 -sV -n

Starting Nmap 6.01 ( http://nmap.org ) at 2012-12-01 18:50 EET
Nmap scan report for bga.com.tr (50.22.202.162)
Host is up (0.25s latency).
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd

Service detection performed. Please report any incorrect results at http://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.55 seconds
```

Aynı anda tcpdump ile oluşan trafik incelenecek olduğunda input olarak verilen kaynak IP adreslerinden hedefe doğru SYN(S) bayrakları set edilmiş TCP paketlerinin gittiği görülebilecektir;

```
silent-root-2:~ fcelalerdik$ tcpdump -i en1 -nn -t
IP 192.168.1.101.47986 > 50.22.202.162.443: Flags [S], seq 1404471153, win 1024,
IP 212.23.23.145.47986 > 50.22.202.162.443: Flags [S], seq 1404471153, win 1024,
IP 11.12.45.6.47986 > 50.22.202.162.443: Flags [S], seq 1404471153, win 1024, opt
IP 5.5.5.5.47986 > 50.22.202.162.443: Flags [S], seq 1404471153, win 1024, option
```

2. Adım: Rastgele IP adresleri ile bir 10 IP adresine sahip havuz oluşturup bu havuz IP adresleri ile hedefe yönelik port taraması yapılacaktır;

```
sh-3.2# nmap bga.com.tr -D RND:10  -p 80 -sV -n

Starting Nmap 6.01 ( http://nmap.org ) at 2012-12-01 19:04 EET
Nmap scan report for bga.com.tr (50.22.202.162)
Host is up (0.18s latency).
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.88 seconds
```

Sonuçların tcpdump ile incelendiğinde:

```
silent-root-2:~ fcelalerdik$ tcpdump -i en1 -nn -t
```

```
IP 192.168.1.101.39067 > 50.22.202.162.443: Flags [S], seq 2331156151, win 1024,
IP 148.138.95.213.39067 > 50.22.202.162.443: Flags [S], seq 2331156151, win 1024
IP 161.39.202.88.39067 > 50.22.202.162.443: Flags [S], seq 2331156151, win 1024,
IP 81.85.139.109.39067 > 50.22.202.162.443: Flags [S], seq 2331156151, win 1024,
IP 67.232.48.36.39067 > 50.22.202.162.443: Flags [S], seq 2331156151, win 1024,
IP 74.167.72.193.39067 > 50.22.202.162.443: Flags [S], seq 2331156151, win 1024,
IP 133.203.207.37.39067 > 50.22.202.162.443: Flags [S], seq 2331156151, win 1024
IP 208.140.24.110.39067 > 50.22.202.162.443: Flags [S], seq 2331156151, win 1024
IP 28.203.195.139.39067 > 50.22.202.162.80: Flags [.], ack 2331156151, win 1024,
IP 142.113.250.145.39067 > 50.22.202.162.80: Flags [.], ack 2331156151, win 1024
IP 37.5.36.56.39067 > 50.22.202.162.80: Flags [.], ack 2331156151, win 1024, len
```

2.13. SYN Proxy Kullanılan Sistemlere Yönelik Port Tarama

Amaç: SYN proxy kullanımından dolayı saldırganlara karşı alınmış önlemleri atlatarak hazırlanmış aldatmacayı düzenli bir şekilde atlatma.

Kullanılan Araçlar:

- Nmap

Adımlar:

1. **Adım:** SYN Proxy kullanan hedefe yönelik port taramasında SYN Proxy'lik yapan cihaz her gönderilen SYN bayrağı set edilmiş TCP paketine SYN+ACK döneceğinden tüm portlar açık görünür;

```
root@bt:/usr/local/share/nmap/scripts# nmap 10.10.10.5 -p 78-82
Starting Nmap 6.00 ( http://nmap.org ) at 2012-11-10 22:20 EET
Nmap scan report for 10.10.10.5
Host is up (0.0091s latency).
PORT STATE SERVICE
78/tcp open unknown
79/tcp open finger
80/tcp open http
81/tcp open hosts2-ns
82/tcp open xfer
```

2. **Adım:** SYN proxy kullanan sistemlerde hangi portların gerçekte açık olduğunu tespit etmek için nmap'in -sV komutu ile portlarda çalışan servis tespitinin yapılması gerekmektedir.

```
root@bt:/usr/local/share/nmap/scripts# nmap 10.10.10.5 -p 78-82 -sV
Nmap scan report for 10.10.10.5
Host is up (0.0087s latency).
PORT STATE SERVICE VERSION
78/tcp open unknown
79/tcp open finger?
80/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
81/tcp open hosts2-ns?
82/tcp open xfer?
```

Görüldüğü gibi port taraması yaptığımız aralıkta gerçekte yalnızca 80 portunun açık olduğunu görebilirsiniz.

2.14. Nmap NSE Kullanarak Openssl Heartbleed Zafiyeti Tespiti

Amaç: Nmap aracının kullanılarak hedef sistemlerde OpenSSL Heartbleed zafiyeti varlığı tespit edilmesi.

Kullanılan Araçlar: nmap(ssl-heartbleed.nse)
Uygulama: Nmap aracı "script engine" adında bir alt araca sahiptir. Bu araç sayesinde hedef sistemlerde bazı zafiyet ve özel taramalar gerçekleştirilebilmektedir.
Nmap ile bir script kullanarak, aşağıda gösterildiği şekilde tarama yapabilir:

```
nmap hedef_IP -p hedef_PORT --script=script_ADI
```

nmap için hazırlanmış yeni scriptleri edinmek için nmap script veri tabanının güncellenmesi gerekmektedir.
Nmap script veritabanının güncellenmesi için aşağıdaki komutun çalıştırılması gerekmektedir.

```
nmap --script-updatedb
```

Hedef sistemde openssl-heartbleed zafiyetinin varlık tespiti için;

```
root@kali:~# nmap 192.168.1.45 -p 443 --script=ssl-heartbleed.nse

Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-04 17:24 EDT
Nmap scan report for 192.168.1.45
Host is up (0.00016s latency).
PORT    STATE SERVICE
443/tcp open  https
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows for stealing information intended to be protected by SSL/TLS encryption.
|     State: VULNERABLE
|     Risk factor: High
|     Description:
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for reading memory of systems protected by the vulnerable OpenSSL versions and could allow for disclosure of otherwise encrypted confidential information as well as the encryption keys themselves.
|
|     References:
```

```
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
|       http://www.openssl.org/news/secadv_20140407.txt
|_      http://cvedetails.com/cve/2014-0160/
MAC Address: 00:0C:29:B0:8F:7C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

Görüldüğü üzere hedef sistemde zafiyet varlığı tespit edilmiştir.

2.15. Port Tarama Sistemlerini Şaşırtma

Amaç: Port tarama sistemlerinin, mevcut sistemin port durumu hakkında bilgi almasını önlemek için tüm portlarının yapılandırılması.

Kullanılan Araçlar: portspoof
Uygulama: Saldırganlar bir sistemi hedef aldıklarında ilk yaptığı işlerden biri hedef sistemin açık portlarını tespit etmek ve portlar üzerinde koşan servisleri belirlemektir. Fakat sistemin tüm portlarının açıkmış gibi gösterilmesi durumunda saldırganlar gerçekten hangi portların açık olduğunu tespit edebilmek için full TCP bağlantısı gerçekleştirmesi gerekmektedir. Bu işlem herhangi bir synproxy aracı ile de gerçekleştirilebilmektedir.
Portspoof aracının çalışma prensibi; portspoof kullanım dışında olan tüm portların **nat** kuralı ile 4444 portuna yönlendirilmesini sağlar, önceden açılmış olan 4444 portuna tüm bağlantılar yönlendirilmiş olur. Fakat kullanımda olan portlar nat kuralı dâhilinde yönlendirilmemelidir.

1. **Adım:** Portspoof aracının indirilip derlenmesi;

Aracı aşağıda verilen linkte bulunan download sekmesinden indirmek mümkün.

```
http://portspoof.org/
```

İndirilen zip dosyasının açılması ve açılan dizine gidilmesi;

```
unzip portspoof-master.zip
root@kali:~ cd portspoof-master/
```

Programın derlenmesi;

```
root@kali:~/portspoof-master# ./configure
root@kali:~/portspoof-master# make
root@kali:~/portspoof-master# make install
```

2. **Adım:** Portspoof aracının yapılandırılması;

Bu yapılandırma örneğinde sistemde ssh hizmeti verilmektedir, diğer tüm portlar 4444 portuna yönlendirilecek ve portspoof aracı çalıştırılacaktır.

```
iptables -t nat -A PREROUTING -i eth0 -p tcp -m tcp --dport 1:21 -j REDIRECT --to-ports 4444
iptables -t nat -A PREROUTING -i eth0 -p tcp -m tcp --dport 23:65535 -j REDIRECT --to-ports 4444
portspoof -D
```

3. **Adım:** Sistemin Nmap ile taranması;

```
root@kali:~# nmap 192.168.20.235 -n -p1-65535 --open

Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-07 07:34 EDT
Nmap scan report for 192.168.20.235
Host is up (0.00019s latency).
PORT      STATE SERVICE
1/tcp     open  tcpmux
2/tcp     open  compressnet
3/tcp     open  compressnet
4/tcp     open  unknown
5/tcp     open  unknown
6/tcp     open  unknown
7/tcp     open  echo
8/tcp     open  unknown
9/tcp     open  discard
10/tcp    open  unknown
11/tcp    open  systat
12/tcp    open  unknown
13/tcp    open  daytime
14/tcp    open  unknown
15/tcp    open  netstat
16/tcp    open  unknown
17/tcp    open  qotd
18/tcp    open  unknown
19/tcp    open  chargen
20/tcp    open  ftp-data
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
24/tcp    open  priv-mail
25/tcp    open  smtp
26/tcp    open  rsftp
27/tcp    open  nsw-fe
```

Görüldüğü üzere tüm portlarda hizmet varmış gibi görünmektedir, Böyle sistemlerin saldırganlar tarafından analiz edilmesi çok daha zordur.

2.16. Nmap GUI/Zenmap Kullanarak Port Tarama

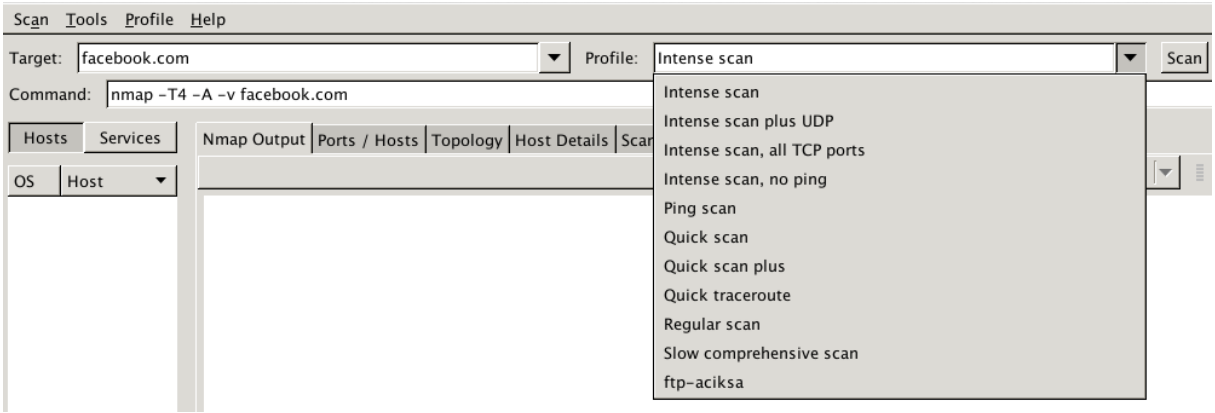
Amaç: Hedef sistemin üzerinde açık olan portları bir grafik arabirim kullanarak taramak.

Kullanılan Araçlar:

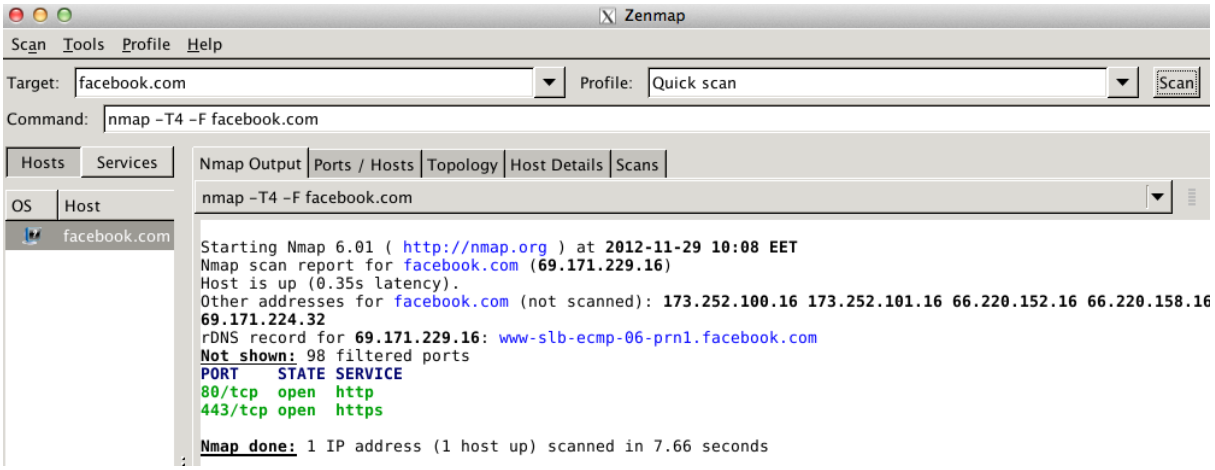
- Zenmap

Adımlar:

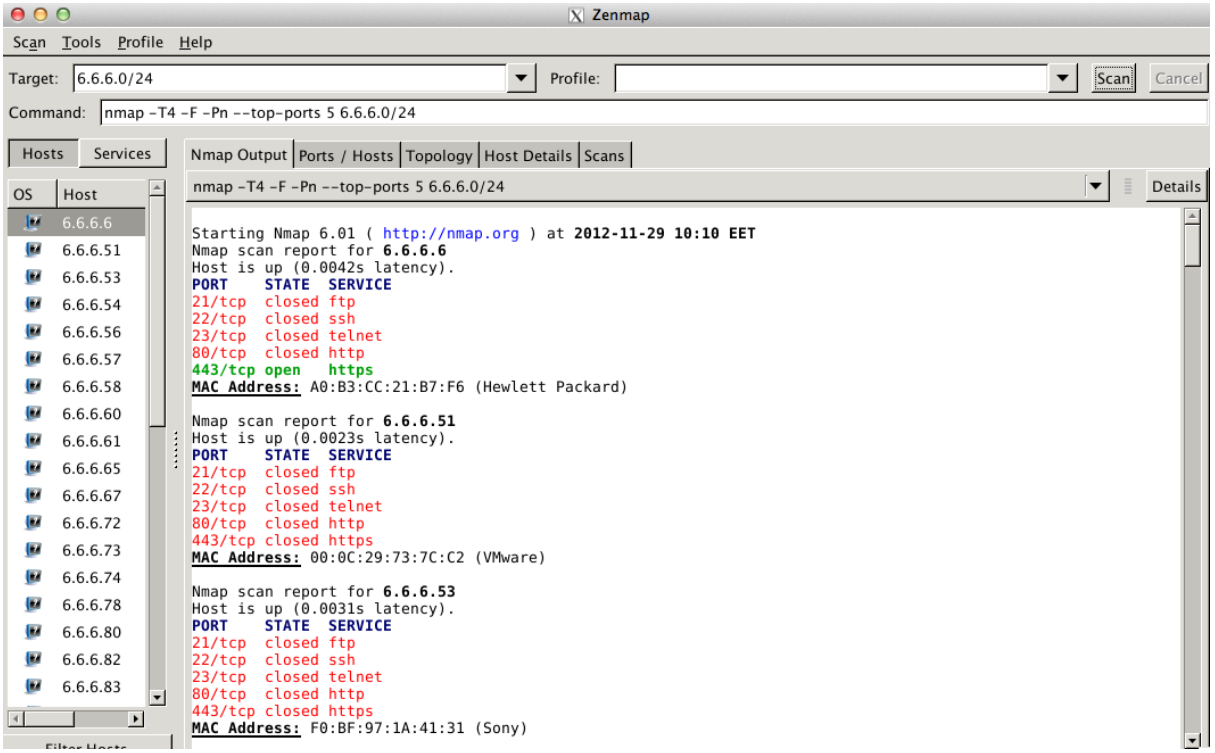
1. **Adım**: Zenmap hedef sistemleri tespit noktasında kullanılabilecek farklı yöntemleri hazır olarak görsel bir şekilde barındırmaktadır. Bu tarama modları "**Profile**" aşağı açılır menüsünden görüntülenebilmektedir.



2. **Adım**: Örnek olması açısından "**Quick scan**" kullanarak facebook.com domain adresinin portlarını taranabilir.



3. **Adım**: 6.6.6.0/24 subnetinde bulunan cihazların en sık kullanılan 5 portu zenmap ile taranacaktır. En popüler portları taramak için "**--top-ports**" parametresi kullanılmaktadır.



2.17. TOR Networkü Üzerinden Port Tarama

Amaç: Hedef sistemleri tarama esnasında iz bırakmamak için tor networkünün kullanılması.

Kullanılan Araçlar: tor, proxychains, nmap
Uygulama: Hedef sistemlerin tarama işlemi mevcut ip adresinin ifşa edilmemesi için tor networkü üzerinden çıkılacaktır.

1. **Adım:** tor kurulumu

```
apt-get install tor
```

2. **Adım:** proxychains kurulumu

Proxychain, trafiğin tora yönlendirilecek şekilde yapılandırılmış bir halde gelmektedir.

```
apt-get install proxychains
```

3. **Adım:** nmap ile hedef sistemin taranması;

```
root@kali:~# proxychains nmap -p 53 -sT 8.8.8.8
ProxyChains-3.1 (http://proxychains.sf.net)

Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-07 08:40 EDT
|S-chain|-<>-127.0.0.1:9050-<><>-8.8.8.8:53-<><>-OK
Nmap scan report for google-public-dns-a.google.com (8.8.8.8)
Host is up (0.024s latency).
PORT   STATE SERVICE
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 3.37 seconds
```

Hedef sistemin logları incelendiğinde saldırganın asıl ip adresi görülmeyecektir.

2.18. Alternatif Port Tarama ve Keşif Araçları-Masscan

Amaç: Alternatif port tarama araçlarından olan masscan kullanımını öğrenmek ve hedef sistemlerin port durumlarını tespit etmek.

Kullanılan Araçlar: masscan
Uygulama: masscan aracının tanıtımı yapıldıktan sonra kullanım örnekleri verilecektir.

1. **Adım:** Masscan aracının tanıtımı;

Masscan aracı nmap benzeri bir araçtır, nmap kadar gelişmiş olmamakla birlikte temelde hedef sistemlerin port durumlarının tespit edilebileceği ve tarama işlemlerinin hızlarının düzenlenebildiği bir araçtır.
Aracın kullanım şu şekildedir:

```
masscan <ip adresi/aralığı> -p port_numarası tarama_seçenekleri
```

Belli başlı seçenekleri:
<ip/range>: Taranacak olan ip adres aralığı
-p <ports>: Hedef sistemde taranacak port numaraları
--banners: Hedef sistemden elde edilecek başlık bilgileri, örneğin http sunucu versiyonu
--rate: Tarama esnasında gönderilecek paket/saniye oranı, ön tanımlı olarak 100 paket/saniyedir.

2. **Adım:** Örnek masscan taramaları.

192.168.1.42 adresinin sadece 22. portunun taranması;

```
root@kali:~# masscan 192.168.1.42 -p 22

Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2015-04-04 10:58:50 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [1 port/host]
Discovered open port 22/tcp on 192.168.1.42
```

192.168.1.42 adresinin ilk 1000 portunun rate değerini 500 paket/saniye değeri ile taranması;

```
root@kali:~# masscan 192.168.1.42 -p1-1000 --rate 500

Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2015-04-04 11:05:17 GMT
```

```
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [1000 ports/host]
Discovered open port 22/tcp on 192.168.1.42
```

Daha detaylı bir bilgi edinmek ve diğer seçeneklerin kullanımını öğrenmek için aracın manuelinin incelenmesi önerilmektedir.

Not: Bu doküman BGA Bilgi Güvenliği A.Ş için Mesut Türk tarafından hazırlanmıştır.