

Alternatif Port Tarama Araçları

Bilgi Güvenliği AKADEMİSİ

Bölüm İçeriği

Hping Kullanarak Port Tarama

- Hatırlatmalar:
 - Hping istenilen türde paket oluşturmak için kullanılan bir uygulamadır.
 - Port taramaları TCP/IP paketleri üzerinde oynamalarla gerçekleştirilir.
- Port Tarama Konusunda Hping:
 - Nmap kadar kolay ve esnek olmasa da Nmap'in yaptığı her tür taramayı kolaylıkla gerçekleştirebilir.
 - SYN SCAN, XMASs, FIN, NULL, Traceroute, UDP, ICMP vb

Hping ile SYN Port Tarama

```
# hping -S 192.168.1.1 -p ++22
```

```
HPING 192.168.1.1 (eth0 192.168.1.1): S set, 40 headers + 0 data bytes
```

```
len=46 ip=192.168.1.1 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=5840 rtt=6.2 ms
```

```
len=46 ip=192.168.1.1 ttl=64 DF id=0 sport=23 flags=SA seq=1 win=5840 rtt=0.9 ms
```

```
len=46 ip=192.168.1.1 ttl=255 DF id=0 sport=24 flags=RA seq=2 win=0 rtt=0.8 ms
```

```
len=46 ip=192.168.1.1 ttl=255 DF id=0 sport=25 flags=RA seq=3 win=0 rtt=0.8 ms
```

```
len=46 ip=192.168.1.1 ttl=255 DF id=0 sport=26 flags=RA seq=4 win=0 rtt=0.7 ms
```

```
len=46 ip=192.168.1.1 ttl=255 DF id=0 sport=27 flags=RA seq=5 win=0 rtt=0.7 ms
```

```
--- 192.168.1.1 hping statistic ---
```

```
13 packets tramitted, 13 packets received, 0% packet loss
```

```
round-trip min/avg/max = 0.7/1.2/6.2 ms
```

Hping Taramalarında Çıktı Okuma

- Hping çıktıları çok okunur değildir.
- Özellikle port tarama çıktıları uzman gözü gerektirir.
- Port tarama çıktılarının daha okunabilir olması için `--scan` parametresi kullanılır.

```
# hping --scan 21,22,23,80,110,130-143 -S 1.2.3.488

Scanning 1.2.3.488 (1.2.3.488), port 21,22,23,80,110,130-143

19 ports to scan, use -V to see all the replies

+---+-----+-----+---+---+-----+-----+
|port| serv name | flags |ttl| id  | win | len |
+---+-----+-----+---+---+-----+-----+

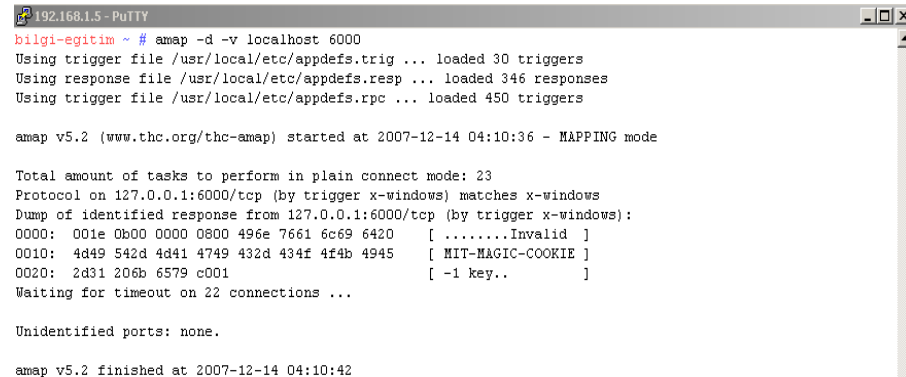
 21 ftp      : .S..A... 56 52428 65535 46
 22 ssh      : .S..A... 56 52684 65535 46
 80 http     : .S...A... 56 52940 65535 46
110 pop3     : .S...A... 56 53196 65535 46

All replies received. Done.

Not responding ports: (130 cisco-fna) (131 cisco-tna) (132 cisco-sys) (133 statsrv) (134
ingres-net) (135 loc-srv) (136 profile) (137 netbios-ns) (138 netbios-dgm) (139 netbios-
ssn) (140 emfis-data) (141 emfis-ctrl) (142 bl-idm) (143 imap)
```

Thc-Amap İle Port Tarama

- Amap bir port tarama aracının ötesinde servis tanıma/belirleme aracıdır.
- Klasik port tarama araçları bir portu tararken o porttaki servisi default değerlere göre değerlendirir(/etc/services).
- Amap ise portun default değerini değil kendi yapıtğı değerlendirmeleri sonucu servisin ne olduğuna karar verir.
- Nmap'deki -sV parametresi benzeri.
- Amap bu özelliği sağlayan ilk tarama programlarındanıdır.



```
192.168.1.5 - PuTTY
bilgi-egitim ~ # amap -d -v localhost 6000
Using trigger file /usr/local/etc/appdefs.trig ... loaded 30 triggers
Using response file /usr/local/etc/appdefs.resp ... loaded 346 responses
Using trigger file /usr/local/etc/appdefs.rpc ... loaded 450 triggers

amap v5.2 (www.thc.org/thc-amap) started at 2007-12-14 04:10:36 - MAPPING mode

Total amount of tasks to perform in plain connect mode: 23
Protocol on 127.0.0.1:6000/tcp (by trigger x-windows) matches x-windows
Dump of identified response from 127.0.0.1:6000/tcp (by trigger x-windows):
0000: 001e 0b00 0000 0800 496e 7661 6c69 6420 [ .....Invalid ]
0010: 4d49 542d 4d41 4749 432d 434f 4f4b 4945 [ MIT-MAGIC-COOKIE ]
0020: 2d31 206b 6579 c001 [ -1 key.. ]
Waiting for timeout on 22 connections ...

Unidentified ports: none.

amap v5.2 finished at 2007-12-14 04:10:42
```

Unicornscan İle Port Tarama

- Unicornscan geniş ağları taramak için geliştirilmiş hızlı bir port tarama aracıdır.
- Geniş ağlar için düşünüldüğünden taranacak sistemleri belirtirken CIDR notasyonu kullanılır.
 - Mesela 192.168.1.0 ağını taramak için 192.168.1.0/24 değeri kullanılır.
 - Tek bir hostu taramak için 10.0.1.3/32 şeklinde bir tanım kullanılır.
- -r ile ne tarama işleminde ne kadarlık paket gönderileceği belirtilir.
 - -r 10000 gibi bir parametre ile çoğu ağ cihazı devre dışı bırakılabilir.
 - Bu sebeple bu parametre ile kullanılırken dikkatli olunmalıdır.

TCP Tarama Çeşitleri

- unicornscan öntanımlı olarak TCP SYN tarama yapar.
- İstenirse parametrelerle diğer TCP taramaları da yapılabilir.

```
home-labs ~ # unicornscan -r 500 -mT vpn.lifeoverip.net
TCP open      smtp[ 25]      from 80.93.212.86  ttl 55
TCP open      domain[ 53]    from 80.93.212.86  ttl 55
TCP open      pop3[ 110]     from 80.93.212.86  ttl 55
TCP open      imap[ 143]     from 80.93.212.86  ttl 55
TCP open      https[ 443]    from 80.93.212.86  ttl 55
TCP open      pop3s[ 995]    from 80.93.212.86  ttl 55
TCP open      mysql[ 3306]   from 80.93.212.86  ttl 55
```


UDP Tarama Çeşitleri

- Unicornscan'in en önemli ve ayırt edici özelliklerinden biri UDP taramalarındaki davranışıdır.
- Normal tarama programları(Nmap dahil) udp portlarını tararken portun durumunu gelen/gelmeyen cevaba göre açıklar.
- Normal tarama programları udp taraması yaparken hedef udp portuna boş udp paketleri gönderir
 - Eger cevap gelmezse portun açık olduğunu -ya da filtrelenmiş olduğunu- kabul eder.
 - Cevap olarak icmp paketi alırsa portun kapalı -ya da filtrelenmiş olduğunu- varsayar.
- Unicornscan belirlenen udp portuna özel sorgular göndererek cevap bekler. Böylece karşı tarafta çalışan servisin gerçekten durumu ve üzerinde çalışan yazılım bilgisi anlaşılabilir.

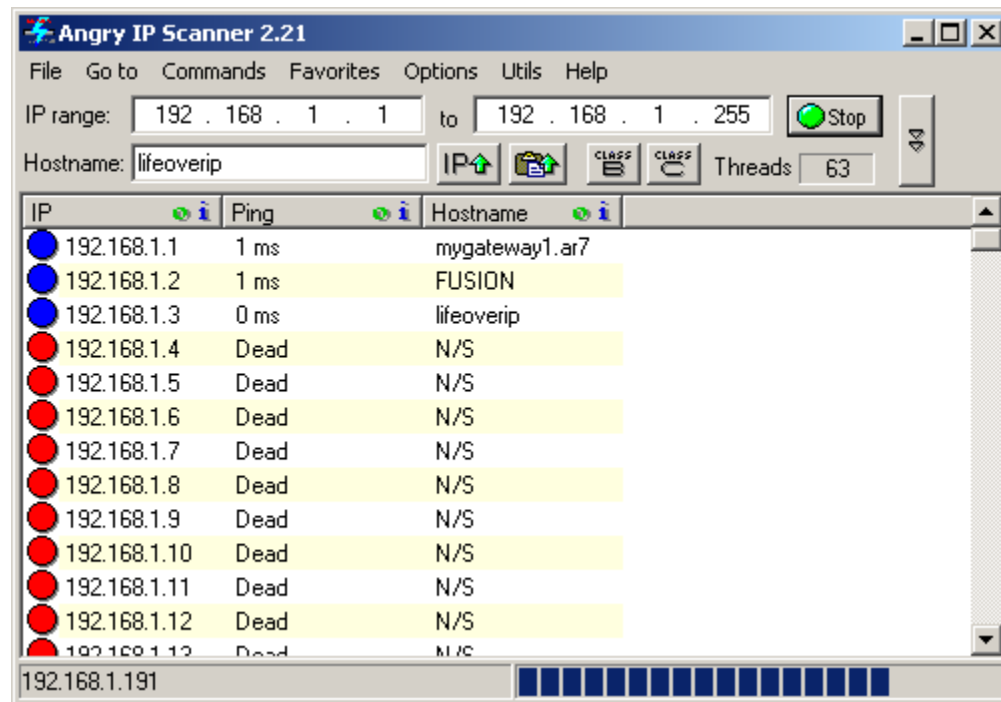
Taramalarda Veri ekleme

- Unicornscan, yapılan taramaların sonuçlarının sağlıklı olması için ilgili portlara uygun veri parçaları gönderir.
- UDP taramalarda payload kısmı otomatik eklenirken TCP protokolü kullanılarak yapılan taramalarda payload kısmı öntanımlı olarak eklenmez.
- TCP taramalarda payload eklenmesi için -msf parametresi kullanılır.

Scanrand

Angry IP Scanner

- Windows için basit, hızlı port tarama aracı



SuperScan

