UDP Host Scan

+ O UDP Host Scan pode ser mais difícil de executar, dadas as ambiguidades oferecidas pelas respostas de mapeamento, como se segue:

RESPOSTAS	
PORTA ABERTA	SEM RESPOSTA
PORTA FECHADA	PORT UNREACHABLE
PORTA COM FILTRO DE FIREWALL EM DROP	SEM RESPOSTA
PORTA COM FILTRO DE FIREWALL EM REJECT	PORT UNREACHABLE

+ Resposta apresentada pelo escaneamento de uma porta aberta

```
root@pentest:~/Desktop# hping3 --udp -p 69 -c 1 172.16.1.5
HPING 172.16.1.5 (tun0 172.16.1.5): udp mode set, 28 headers + 0 data bytes

--- 172.16.1.5 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

+ Resposta apresentada pelo escanemento de uma porta fechada

```
root@pentest:~/Desktop# hping3 --udp -p 161 -c 1 172.16.1.5
HPING 172.16.1.5 (tun0 172.16.1.5): udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from ip=172.16.1.5 name=UNKNOWN
status=0 port=2804 seq=0

--- 172.16.1.5 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 359.6/359.6/359.6 ms
```

→ Port Unreachable

+ Agora, com o iptables, vamos por a configuração de DROP na porta 69:

```
iptables -A INPUT -p udp --dport 69 -j DROP
```

```
root@pentest:~/Desktop# hping3 --udp -p 69 -c 1 172.16.1.5
HPING 172.16.1.5 (tun0 172.16.1.5): udp mode set, 28 headers + 0 data bytes

--- 172.16.1.5 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

→ Agora não houve resposta ao nosso ping, o que traz a dúvida se ela
→ está aberta ou protegida por um Firewall. Isso é justamento o que conclui
→ o nmap:

```
root@pentest:~/Desktop# nmap -sU -p 69 -Pn 172.16.1.5
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-20 17:40 -03
Nmap scan report for 172.16.1.5
Host is up.

PORT   STATE         SERVICE
69/udp open|filtered tftp

Nmap done: 1 IP address (1 host up) scanned in 2.22 seconds
```

→ A resposta dele é que ou está aberta, ou filtrada

\+ Colocaremos agora a configuração de REJECT

```
iptables -F
iptables -A INPUT -p udp --dport 69 -j DROP
```

→ a porta não está fechada, apenas com a configuração reject,
→ mas a resposta ao ping é igual à de quando está fechada

```
root@pentest:~/Desktop# hping3 --udp -p 69 -c 1 172.16.1.5
HPING 172.16.1.5 (tun0 172.16.1.5): udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from ip=172.16.1.5 name=UNKNOWN
status=0 port=1153 seq=0

--- 172.16.1.5 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 326.0/326.0/326.0 ms
```

\+ Para ajudar nessa situação, vamos executar o

```
nmap -v -sUV -p 161 172.16.1.4
```

→ serão executados testes de conexão com a porta (banner grabbing, por exemplo)
para se verificar o caso de ela estar aberta ou não

```
root@pentest:~/Desktop# nmap -v -sUV -p 161 172.16.1.4
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-20 17:42 -03
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 17:42
Scanning 172.16.1.4 [4 ports]
Completed Ping Scan at 17:42, 0.35s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:42
Completed Parallel DNS resolution of 1 host. at 17:42, 0.02s elapsed
Initiating UDP Scan at 17:42
Scanning 172.16.1.4 [1 port]
Completed UDP Scan at 17:42, 3.24s elapsed (1 total ports)
Initiating Service scan at 17:42
Scanning 1 service on 172.16.1.4
Discovered open port 161/udp on 172.16.1.4
Discovered open|filtered port 161/udp on 172.16.1.4 is actually open
Completed Service scan at 17:42, 0.28s elapsed (1 service on 1 host)
NSE: Script scanning 172.16.1.4.
Initiating NSE at 17:42
```

→ Veja que ele executará 45 scripts para fazer esse teste