

# Identificando o Escopo na Rede

+ Iremos identificar o escopo em uma possível rede muito grande

+ Como foi determinado no escopo, devemos encontrar o hosts do domínio local **ORIONSCORP2**

+ O objetivo aqui é fazer uma varredura mais otimizada

+ Primeira atitude é rodar um nmap em cima da porta 445 (SMB), pois como nosso objetivo é comprometer um domínio local, um AD, sabemos que teremos 445 aberta

+ Faremos uma saída do tipo "grepable"

```
nmap --open -v -sS -p 445 -Pn 172.16.1.0/24 -oG smb.txt
```

+ Para fazer um filtro pelos hosts encontrados, usamos

```
cat smb.txt | grep "Up" | cut -d " " -f 2 > targets
```

+ Usaremos então o nosso querido canivete suíço do pentest

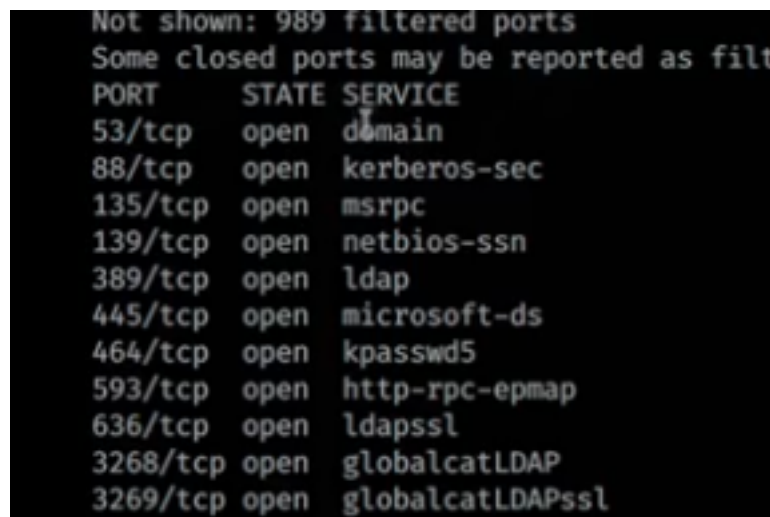
```
crackmapexec smb targets
```

+ E aí identificamos os host da tal da ORIONSCORP2

→ Um deles era o 172.16.1.243

+ Fizemos uma varredura nele mais aprofundada com o nmap

```
nmap -v --open -Pn 172.16.1.243
```

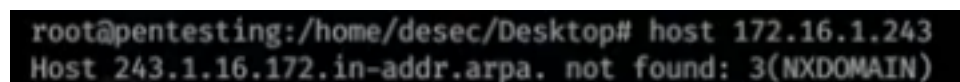


```
Not shown: 989 filtered ports
Some closed ports may be reported as filtered
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldaps
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
```

→ essas portas abertas indicam que ele mesmo é o AD

+ Ao tentarmos fazer a resolução DNS desse host, ela não é concluída pois estaríamos fazendo pelo nosso servidor dns. Para que consigamos, usaremos o host do AD:

```
host 172.16.1.243
```



```
root@pentesting:/home/desec/Desktop# host 172.16.1.243
Host 243.1.16.172.in-addr.arpa. not found: 3(NXDOMAIN)
```

```
host 172.16.1.243 172.16.1.243
```

```
root@pentesting:/home/desec/Desktop# host 172.16.1.243 172.16.1.243
Using domain server:
Name: 172.16.1.243
Address: 172.16.1.243#53
Aliases:

243.1.16.172.in-addr.arpa domain name pointer SERVAD02.ORIONSCORP2.LOCAL.
root@pentesting:/home/desec/Desktop# host 172.16.1.241 172.16.1.243
Using domain server:
Name: 172.16.1.243
Address: 172.16.1.243#53
Aliases:

241.1.16.172.in-addr.arpa domain name pointer CORPPC01.ORIONSCORP2.LOCAL.
```

→ Usando o 172.16.1.243 como servidor dns, podemos visualizar a resposta da consulta dns

+ Info capturadas

```
Warning, you are using the root account, you may harm your system.
SMB      172.16.1.243      445      SERVAD02      [*] Windows 10.0 Build 17763 x64 (name:SERVAD02) (domain:ORIONSCORP2) (signing
SMB      172.16.1.253      445      CORPC02      [*] Windows 10.0 Build 18362 x64 (name:CORPC02) (domain:ORIONSCORP2) (signing
SMB      172.16.1.241      445      CORPPC01      [*] Windows 10.0 Build 18362 x64 (name:CORPPC01) (domain:ORIONSCORP2) (signing

SERVAD02.ORIONSCORP2.LOCAL - 172.16.1.243 - Servidor AD
CORPPC01.ORIONSCORP2.LOCAL - 172.16.1.241 - Estacao 1
CORPPC02.orionscorp2.local - 172.16.1.253 - Estacao 2
```

+ Primeiramente, vamos configurar o responder da nossa máquina de acesso

→ primeiro acessamos a raiz (sudo su)

depois:

```
cd /etc/responder
```

```
nano responder.conf
```

```
; Dump Responder Config log:
ResponderConfigDump = Config-Responder.log

; Specific IP Addresses to respond to (default = All)
; Example: RespondTo = 10.20.1.100-150, 10.20.3.10
RespondTo = 172.16.1.243, 172.16.1.241, 172.16.1.253
```

→ Faremos essa modificação para que ao invés de responder a todos, nossa máquina interaja somente com as máquinas que queremos

