Network Sweeping

+ O objetivo aqui é fazer um mapeamento mais eficiente de uma rede grande escolhendo bem as portas que serão testadas pelo nmap

+ Primeiro, devemos ter a noção de quais hosts estão ou não ativos
→ Isso pode ser feito pelo seguinte comando

```
nmap -v -sn 172.16.1.0/24 -oG ativos.txt
```

-v de verbose
-sn para que ele verifique se estão ativos
-oG para que a sáida (output) seja grepable (grepável kkk)
ativos.txt será o arquivo em que as respostas serão guardadas

+ Quando analisarmos a varredura do comando passado com o

```
cat ativos.txt
```

veremos que ela exibe o estado de cada host como "up" ou "down".
Obviamente, faaremos um filtro pelos "up"

```
grep "Up" ativos.txt
```

Em seguida, faremos um filtro só pelos endereços de IP

```
grep "Up" ativos.txt | cut -d " " -f 2 > hosts
```

+ Faremos agora uma varredura nas principais portas desses hosts

```
nmap -sSV -p 80 --open -Pn -iL hosts -oG web.txt
```

→ Esse filtro varre apenas a porta 80
-sSV para que seja capturado o Banner Grab e possamos identificar a tecnologia em que o serviço está funcionando
-Pn para não verificar se está ativo ou não (já sabemos que está)
-iL para carregar uma lista, no caso a hosts

+ Em seguida, se queremos, por exemplo, os hosts que rodam Ubuntu, podemos executar

```
grep "Ubuntu" web.txt
```

+ Se quisermos fazer testes em outras portas, podemos ver qual o serviço de nosso interesse e fazer a pesquisa no kali mesmo
→ Exemplo, queremos as portas que rodam serviço ftp para que possamos passar como parâmetro de pesquisa no nmap
Executamos então

```
cat /etc/services | grep "ftp"
```

+ Ou, na hora da pesquisa com o nmap, podemos declarar direto o serviço desejado:

```
nmap -sS -p http* --open -Pn -iL hosts
```

→ Ele fará os testes nas portas mais comuns para o http