Network Mapper - NMAP

~~~~~~
NMAP
~~~~~~

+ Uma das ferramentas mais conhecidas para realizar scan

+ Já existe a mais de 20 anos

+ Sugestão de livro: Exame de redes com o nmap

+ Quando executamos somente nmap no terminal, podemos visualizar as ferramentas dele que podemos usar, como
→ Especificação de portas
→ Endereços IP
→ Redes
→ Técnicas de scanneamento
→ Detecção de Sistemas Operacionais
→ Tempo e perfomance de execução do mapeamento
→ Evasão de Firewalls
→ E muitas outras

+ Exemplo:

```
nmap -v -p 21-25,80,8080 -Pn 172.16.1.5
```

-v de verbose (que dá a saída que possamos ler)
-p especifica as portas, no caso da 21 à 25, a 80 e a 8080
-Pn para que não haja verificação de se o host está ativo ou não
- no final, o endereço de ip

```
nmap -v -sS --top-port=5 -Pn 172.16.1.5
```

-sS de SYN Scan
--top-port=5 para escanear as 5 principais portas. Caso n fosse declarado esse parâmetro, ele faria o scan nas 1000 principais (melhor do que fazer nas 65535)
→ Se quisesse varrer toda a rede, poderíamos declarar o ip como 172.16.1.0/24

+ Há também um modo de ter acesso aos scripts de scan do nmap, que é chegar no diretório onde eles estão guardados:

```
cd /usr/share/nmap/scripts
```