



Redes de Computadores II

C.T. Informática para Internet
Prof. Vinícius Alves Hax



Antes

- Auditoria



Hoje

- Auditoria (um pouco de prática)



Entendendo a rede

- Cálculo da máscara de rede
\$ netmask 10.0.2.2/16 -r



Descobrimos hosts

```
$ fping -g 10.0.2.0/24 > /tmp/saida
```

```
$ cat /tmp/saida | grep alive
```

```
$ sudo netdiscover -r 10.0.2.0/24
```



Tentando descobrir o SO

```
$ sudo nmap 10.0.2.2 -O
```



Descobrimo portas abertas

```
$ sudo masscan 10.0.2.2 --ports 0-65535
```

```
$ spiderfoot -s 10.0.2.2
```



Escaneando servidor web

```
$ nikto -host 10.0.2.2
```




Elevação de privilégios

\$ unix-privesc-check standard



Dúvidas?