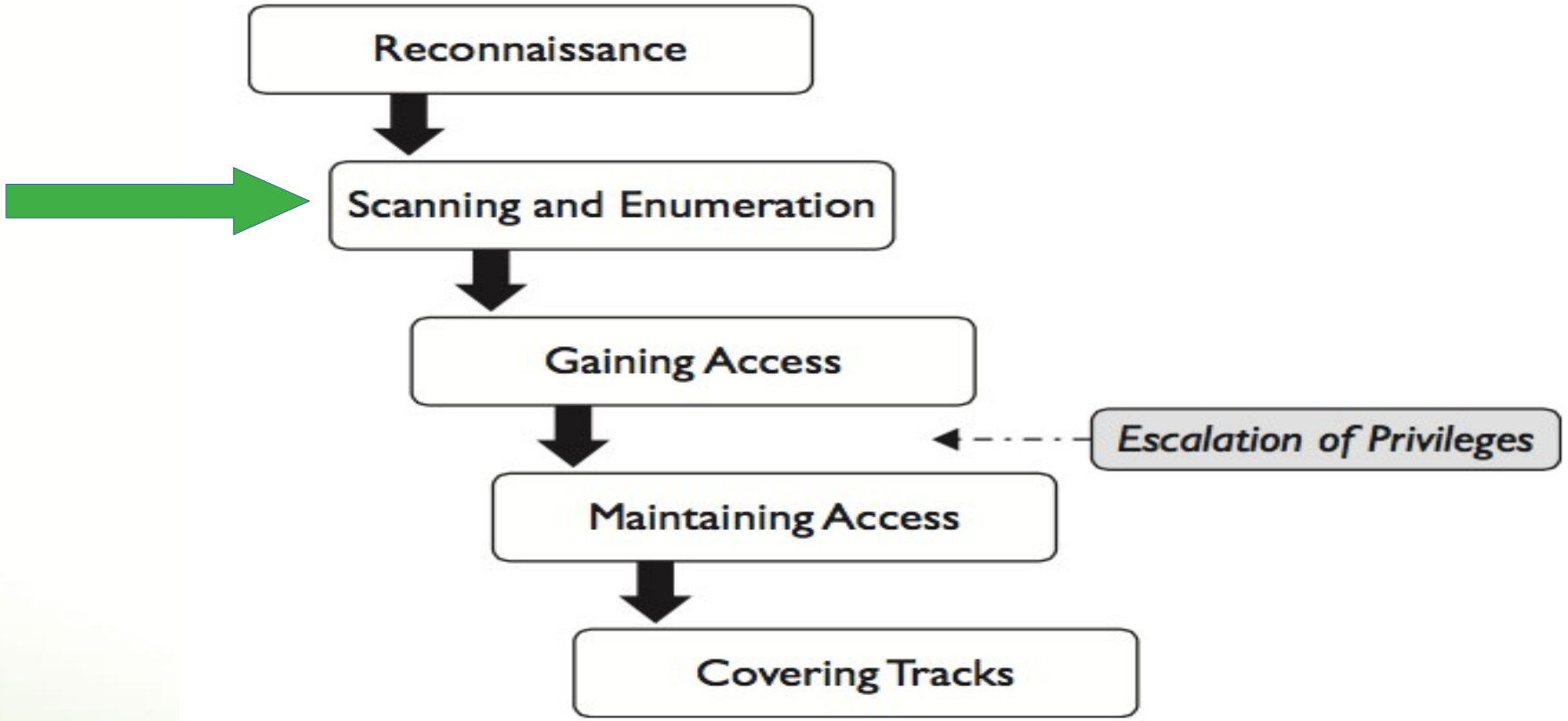
INSTITUTO FEDERAL
São Paulo
Câmpus Barretos

Segurança da Informação

Aula 5

Prof. Lucas

Fases


Reconnaissance
Scanning and Enumeration
Gaining Access
Escalation of Privileges
Maintaining Access
Covering Tracks

nmap

- Sintaxe
  - `nmap <scan options> <target>`

- O `<target>` pode ser um único IP, múltiplos Ips (separados por espaços) ou uma rede inteira (notação por prefixo)

Nmap - exemplos

- `nmap 192.168.1.100`
- `nmap 192.168.1.100 192.168.1.101`
- `nmap 192.168.1.0/24`

- Ao executar o nmap sem nenhum parâmetro, a opção *default* será um scan “regular”

Nmap - exemplos

- Time number
- T0: scan mais lento
- T4: mais rápido (pode sobrecarregar sua interface de rede e gerar resultados estranhos)
- Por padrão, o valor de T sempre será 2 (normal)

nmap

Nmap Switch	Description	Nmap Switch	Description
-sA	ACK scan	-Pl	ICMP ping
-sF	FIN scan	-Po	No ping
-sI	IDLE scan	-PS	SYN ping
-sL	DNS scan (a.k.a. List scan)	-PT	TCP ping
-sN	NULL scan	-oN	Normal output
-sO	Protocol scan	-oX	XML output
-sP	Ping scan	-T0	Serial, slowest scan
-sR	RPC scan	-T1	Serial, slowest scan
-sS	SYN scan	-T2	Serial, normal speed scan
-sT	TCP Connect scan	-T3	Parallel, normal speed scan
-sW	Windows scan	-T4	Parallel, fast scan
-sX	XMAS scan		

nmap

- “s” determina o tipo de scan
- “P” opções do ping sweep
- “o” lida com a saída
- “T” lida com a velocidade

nmap

- Um scan é definido por 3 características: Quais flags serão setadas; tipo de resposta aguardada e quão silencioso será o scan

- Genericamente falando, existem 7 tipos de scan

nmap

- **Full Connect (TPC connect)**: Executa o 3 *way handshake* em todas as portas. Fácil de detectar porém o mais confiável. Portas abertas responderão com as flags SYN/ACK e portas fechadas responderão com o RST/ACK

- **SYN**: Apenas pacotes SYN são enviados e não é completado o 3 way handshake. Respostas iguais a do full connect

nmap

- **FIN**: Processo reverso do scan SYN. Portas abertas não responderão e portas fechadas responderão com a flag RST

- **XMAS**: Todas as flags são ligadas. Respostas iguais a do FIN scan

- **ACK**: Usados principalmente em Unix. Utiliza mensagens ICMP (destination unreachable) para determinar quais portas estão abertas no firewall. **Portas fechadas não responderão!!!**

nmap

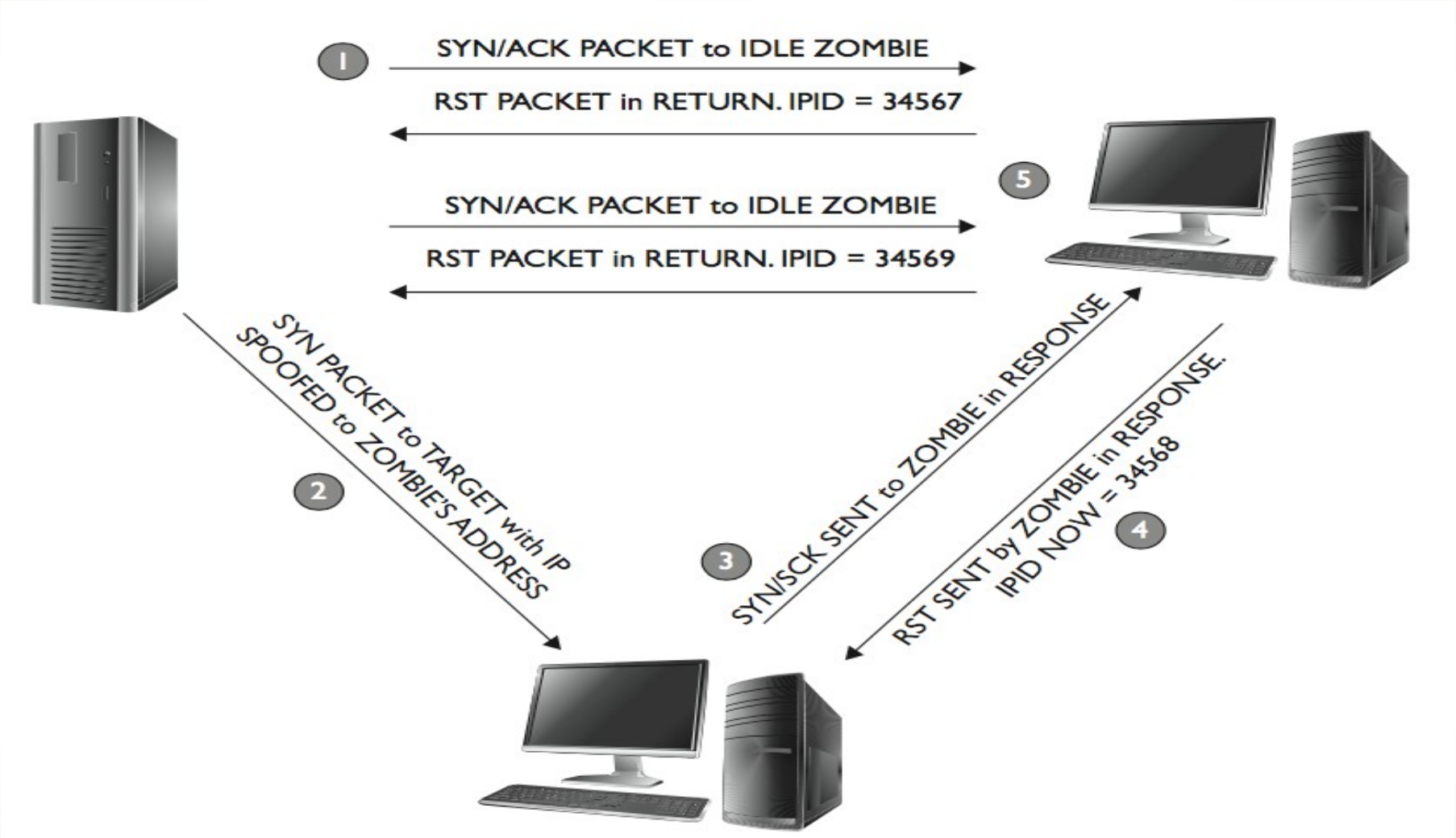
- **IDLE**: Utiliza a técnica de *sfoofed* IP. Utiliza a flag SYN e monitora as respostas de acordo com o SYN scan

- **NULL**: Contrário do XMAS scan. Nenhuma flag é setada. Respostas podem varia de acordo com o SO. Mais utilizado em sistemas Unix.

Nmap - IDLE

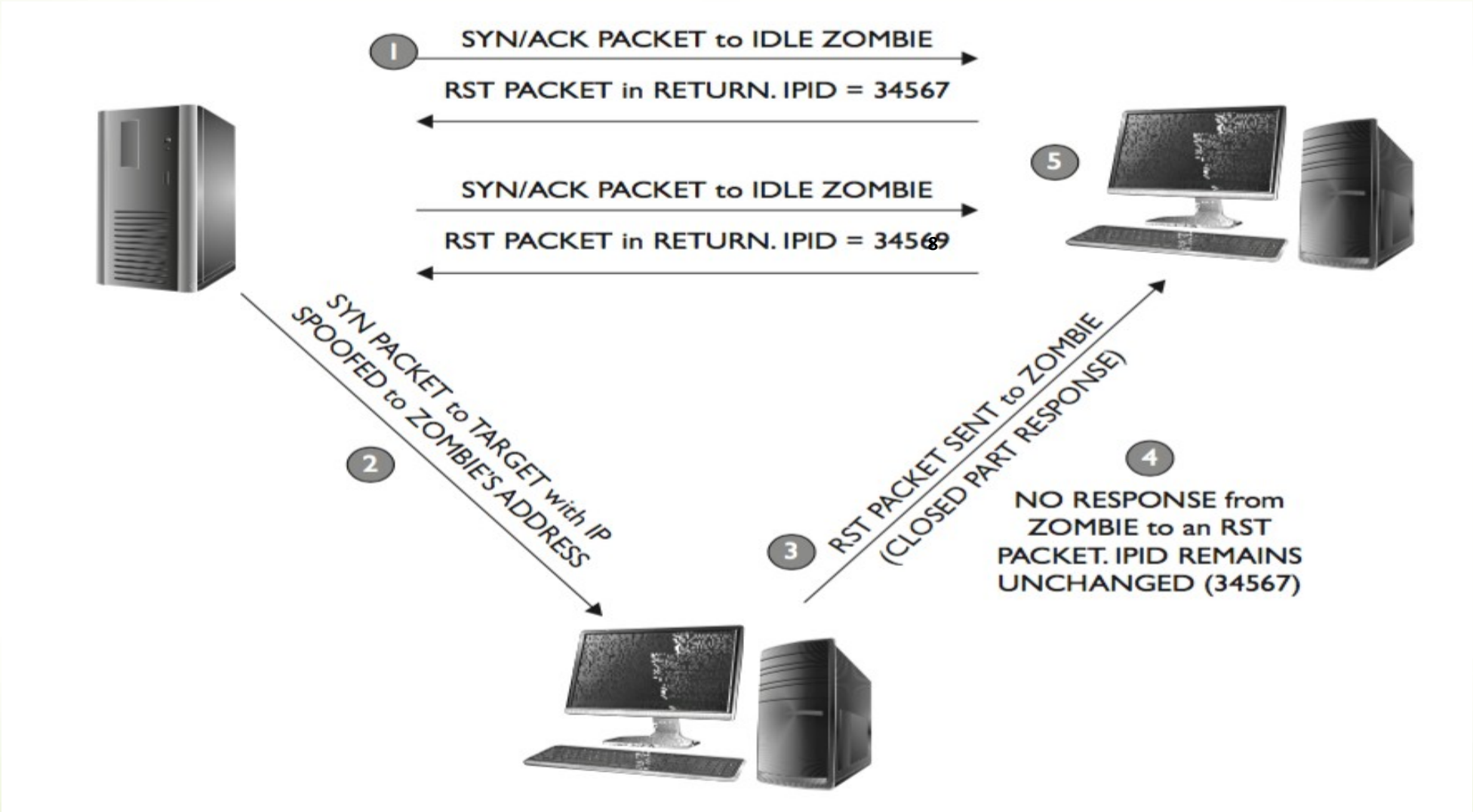
- Cada pacote IP possui um campo chamado de IPID (IP identifier)
- Utilizado para fragmentação
- Cada pacote é incrementado por 1
- O processo é feito da seguinte forma:
  - O atacante envia um SYN/ACK para uma máquina IDLE e anota na resposta o IPID
  - Com o IPID e o IP em mãos ele manda um SYN para o alvo
  - Se a porta estiver aberta, o 3 way handshake acontece, caso contrário é enviado um RST
  - O atacante envia outro SYN/ACK para o IDLE e compara o IPID.
  - Se estiver incrementado de 2, a porta está aberta
  - Caso contrário (incremento de 1) a porta está fechada

Nmap – IDLE – situação porta aberta



Todas as respostas são RST para portas fechadas com exceção do ACK scan que não responde nada

Nmap – IDLE – situação porta fechada



Nmap-resumo

Scan Type	Initial Flags Set	Open Port Response	Closed Port Response	Notes
Full (TCP Connect)	SYN	SYN/ACK	RST	Noisiest but most reliable*
Half open (Stealth or SYN Scan)	SYN	SYN/ACK	RST	No completion of three-way hand-shake; designed for stealth but may be picked up on IDS sensors
XMAS	FIN/URG/ PSH	No response	RST/ACK	Doesn't work on Windows machines
FIN	FIN	No response	RST/ACK	Doesn't work on Windows machines
NULL	No flags set	No response	RST/ACK	Doesn't work on Windows machines
ACK	ACK	RST	No response	Used in firewall filter tests

Obs.: No google: "*Ip Addresses You shouldn't scan*"

Outros exemplos:

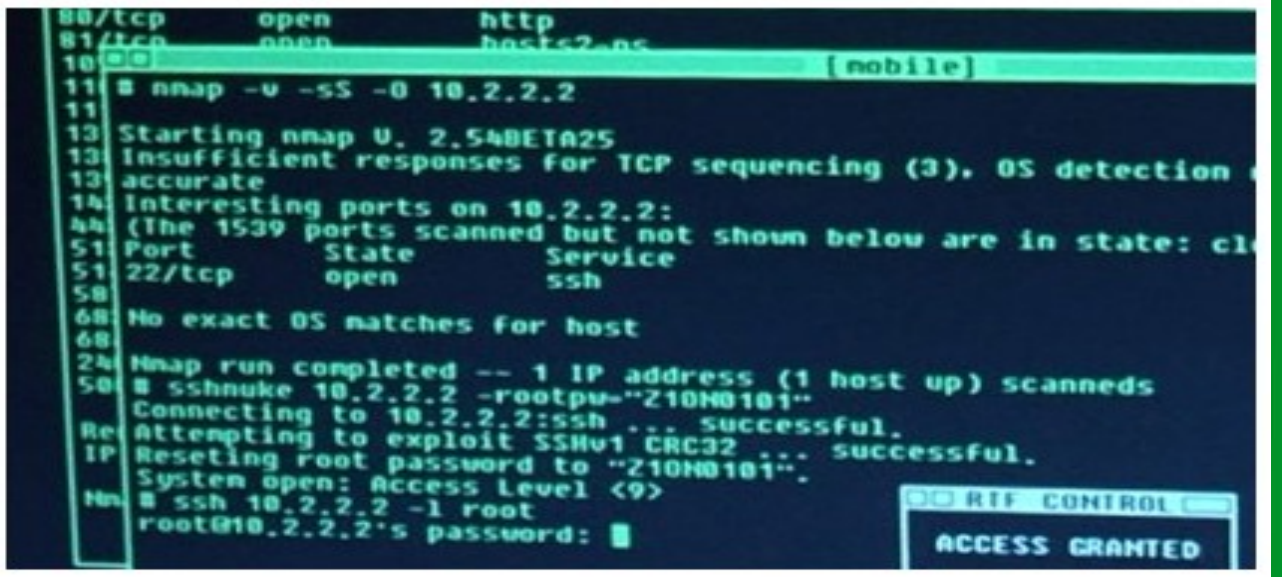
- `nmap -sP [ip]` => scan usando somente ping
- `nmap -P0 [ip]` => força o scan mesmo sem resposta por ping
- `nmap -PR [ip]` => “ping” usando ARP (mais rápido em rede)
- `nmap -F [ip]` => portas mais comuns
- `nmap -O [ip]` => tenta detectar SO
- `nmap -sV [ip]` => detecção de serviços e versões (grab banner)

INSTITUTO FEDERAL
São Paulo

Curiosidades....

- Nmap em filmes:

- https://nmap.org/movies/



Outras ferramentas

- SolarWinds
- NetCraft
- HTTrack
- SuperScan
- hping

- Port sweeping é também conhecido com *fingerprint*

Outros comandos

- UDP Scan
  - `nmap -sU 192.168.1.100`
- Fingerprint em um SO
  - `nmap -sS -O 192.168.1.100`
- Executar um TCP full connect em um host e armazenar o resultado em um arquivo
  - `nmap -sT -oN resultado.txt 192.168.1.100`
- Testar os comandos!

Usando descrição

- Objetiva disfarçar quem você é!
  - Proxies
  - Fragmentação de pacotes
  - Spoofing de endereço IP

Proxy

- Sistema intermediário entre você e o alvo
- Controla o tráfego e segurança adicional
- Alguns exemplos:
  - ProxyChains (http://proxychains.sourceforge.net)
  - SoftCab's Proxy Chain Builder
  - Proxifier
  - Tor

Spoofing ip

- hping
- Scapy
- Komodia
- Ettercap
- Cain
- nmap

Exercícios

- Responder o questionário disponível no moodle!

INSTITUTO FEDERAL
São Paulo