Portscan e NMAP

1. NMAP

- É uma ferramenta de código aberto, utilizada para exploração de rede e auditoria de segurança.
- Ela foi desenhada para identificar as portas de serviço que estão abertas na máquina-alvo ou em um conjunto de máquinas.
- Resultado final:
  - Versão do Sistema Operacional
  - Versão dos serviços em execução.

2. Visual do NMAP

```
C:\Users\valerio.martins>nmap 172.16.5.73
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-11 10:49 Hora oficial do Brasil
Nmap scan report for 172.16.5.73
Host is up.
All 1000 scanned ports on 172.16.5.73 are filtered

Nmap done: 1 IP address (1 host up) scanned in 205.63 seconds

C:\Users\valerio.martins>nmap -v 172.16.5.73
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-11 10:56 Hora oficial do Brasil
Initiating Parallel DNS resolution of 1 host. at 10:56
Completed Parallel DNS resolution of 1 host. at 10:56, 0.01s elapsed
Initiating SYN Stealth Scan at 10:56
Scanning 172.16.5.73 [1000 ports]
SYN Stealth Scan Timing: About 15.50% done; ETC: 10:59 (0:02:49 remaining)
SYN Stealth Scan Timing: About 30.50% done; ETC: 10:59 (0:02:19 remaining)
SYN Stealth Scan Timing: About 44.55% done; ETC: 10:59 (0:01:53 remaining)
SYN Stealth Scan Timing: About 59.55% done; ETC: 10:59 (0:01:22 remaining)
SYN Stealth Scan Timing: About 74.55% done; ETC: 10:59 (0:00:52 remaining)
Completed SYN Stealth Scan at 10:59, 202.08s elapsed (1000 total ports)
Nmap scan report for 172.16.5.73
Host is up.
All 1000 scanned ports on 172.16.5.73 are filtered
```

3. NMAP – Parâmetros Básicos

- -O : Realiza uma tentativa de detectar o sistema operacional da máquina analisada.
- -PO: realiza a varredura da máquina mesmo que ela não responda ao ping, sendo útil em servidores que estão sendo filtrados por firewalls.
- -v : aumenta a quantidade de informação apresentada.
- -s <tipo>: Varreduras com flags específicos.

S (SYN)	N (Null)
S (SYN)	F (FIN)
T (Connect)	X (Xmas)
A (ACK)	I (Idle)
W (Window)	Y (SCTP)
M (Maimon)	O (IP Protocol)
U (UDP)	

4. NMAP – Resultados da Varredura de Portas

- OPEN: uma aplicação está ativa e escutando os pacotes na porta
- CLOSED: nenhuma aplicação está ativa e escutando os pacotes na porta
- FILTERED: um firewall está bloqueando a porta, logo não é possível dizer se ela está ativa ou não.

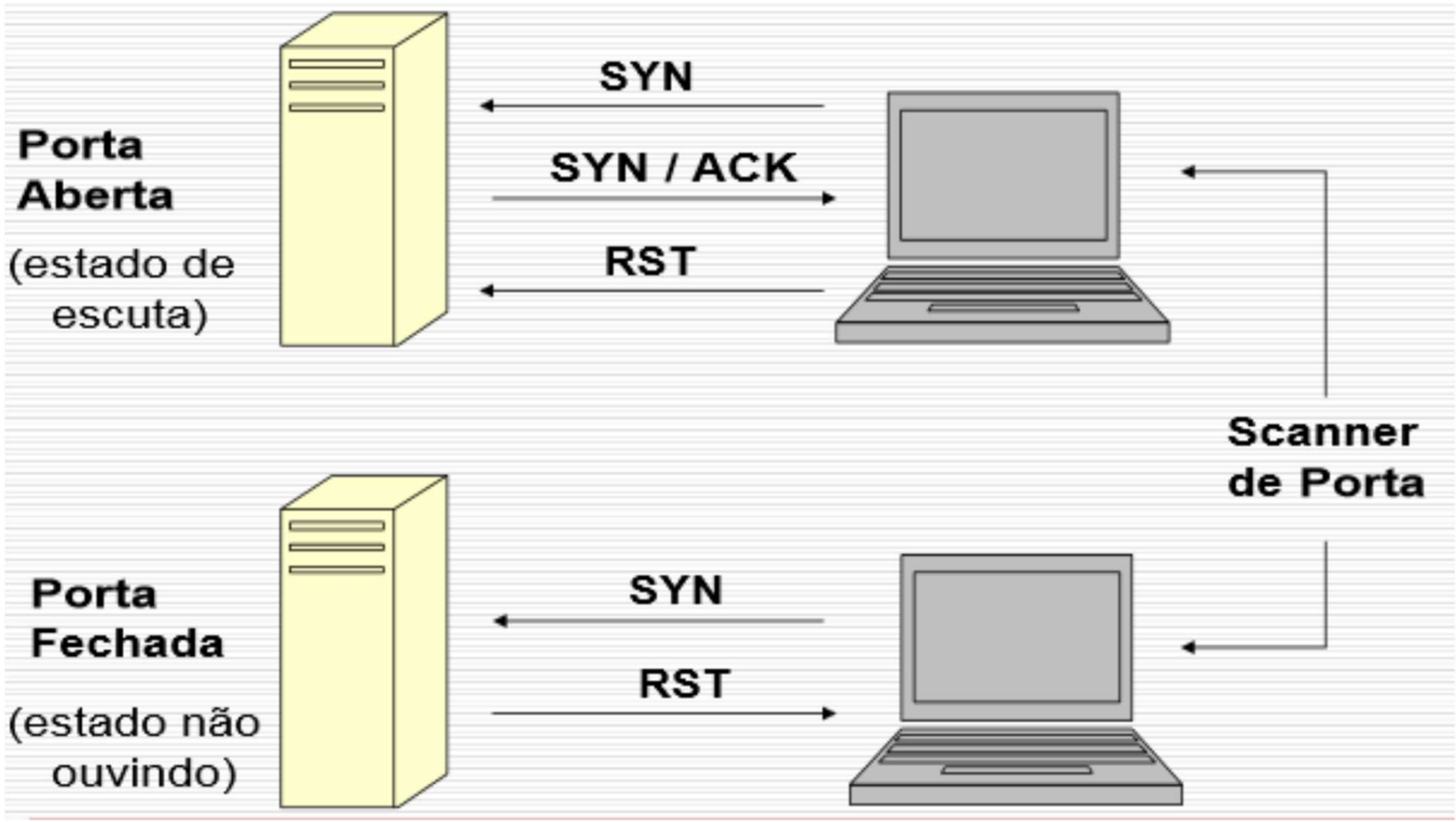
- Descubra se o alvo é protegido por um firewall

  sudo nmap -sA 172.16.5.254
- Scan quando o host é protegido por um firewall

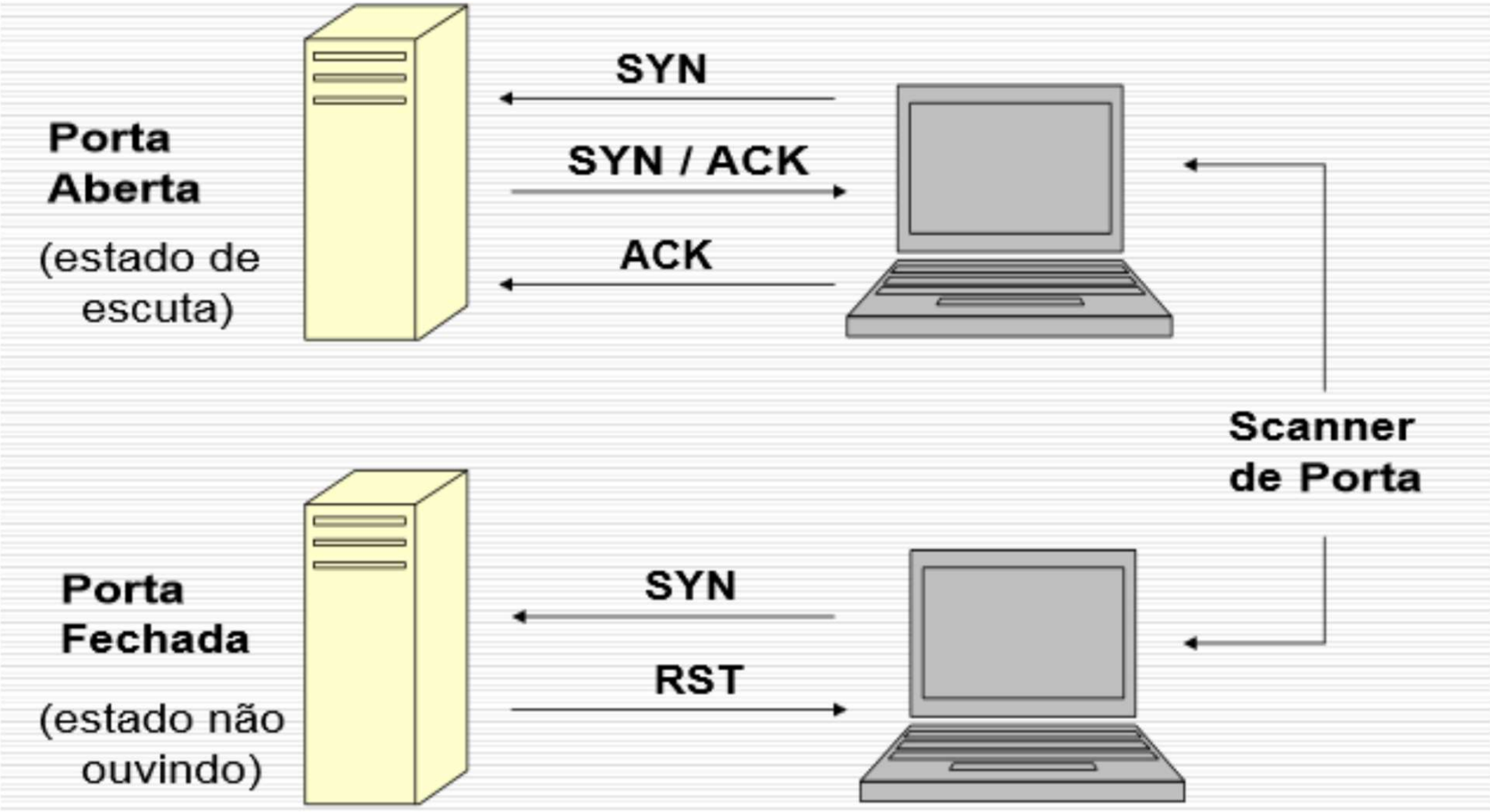
  sudo nmap -PN 172.16.5.1
- Scan de firewall com falha de segurança (TCP Null engana o firewall) para obter uma resposta

  sudo nmap -sN 172.16.5.254

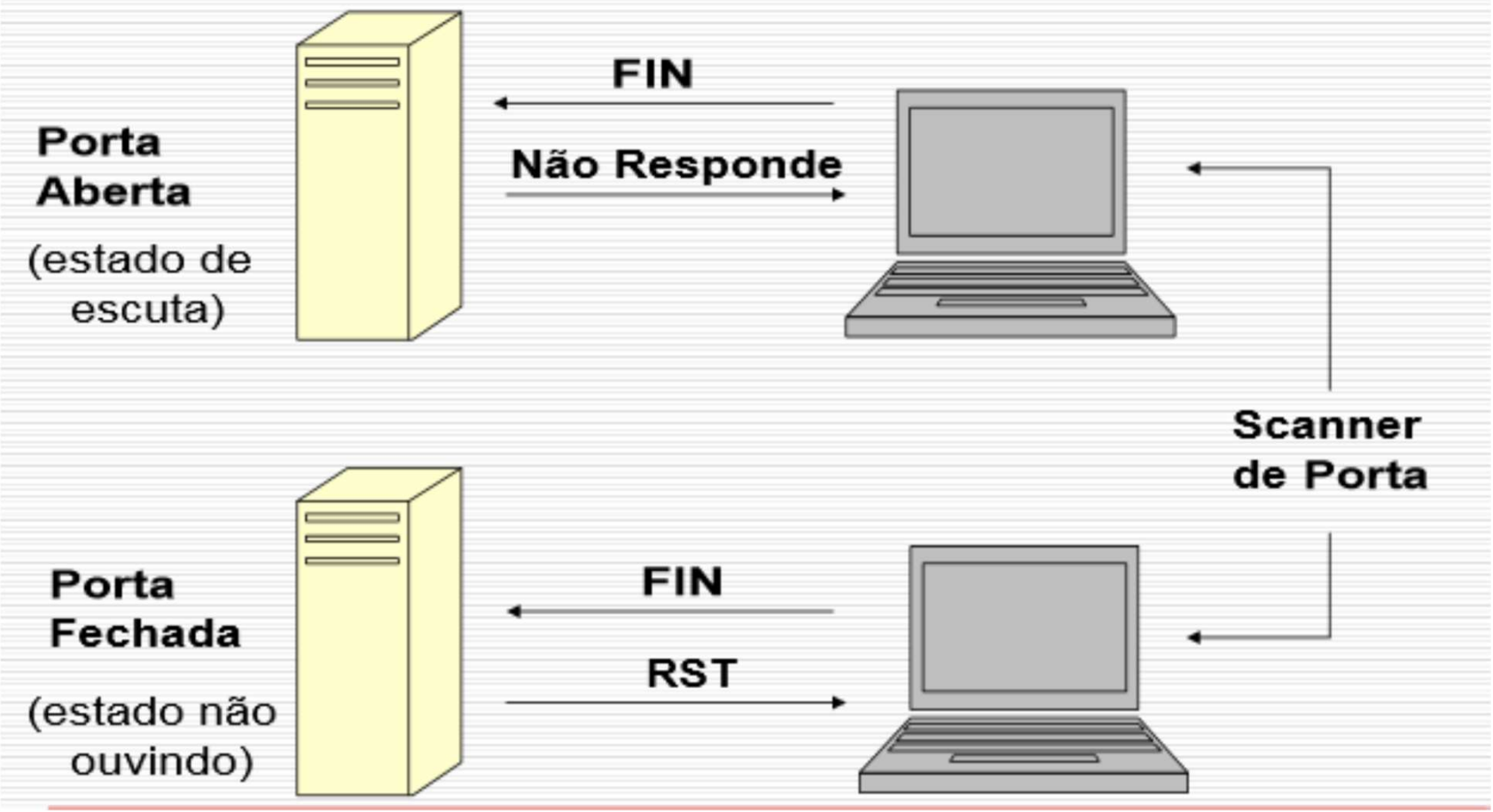
5. Varredura TCP (TCP SYN)



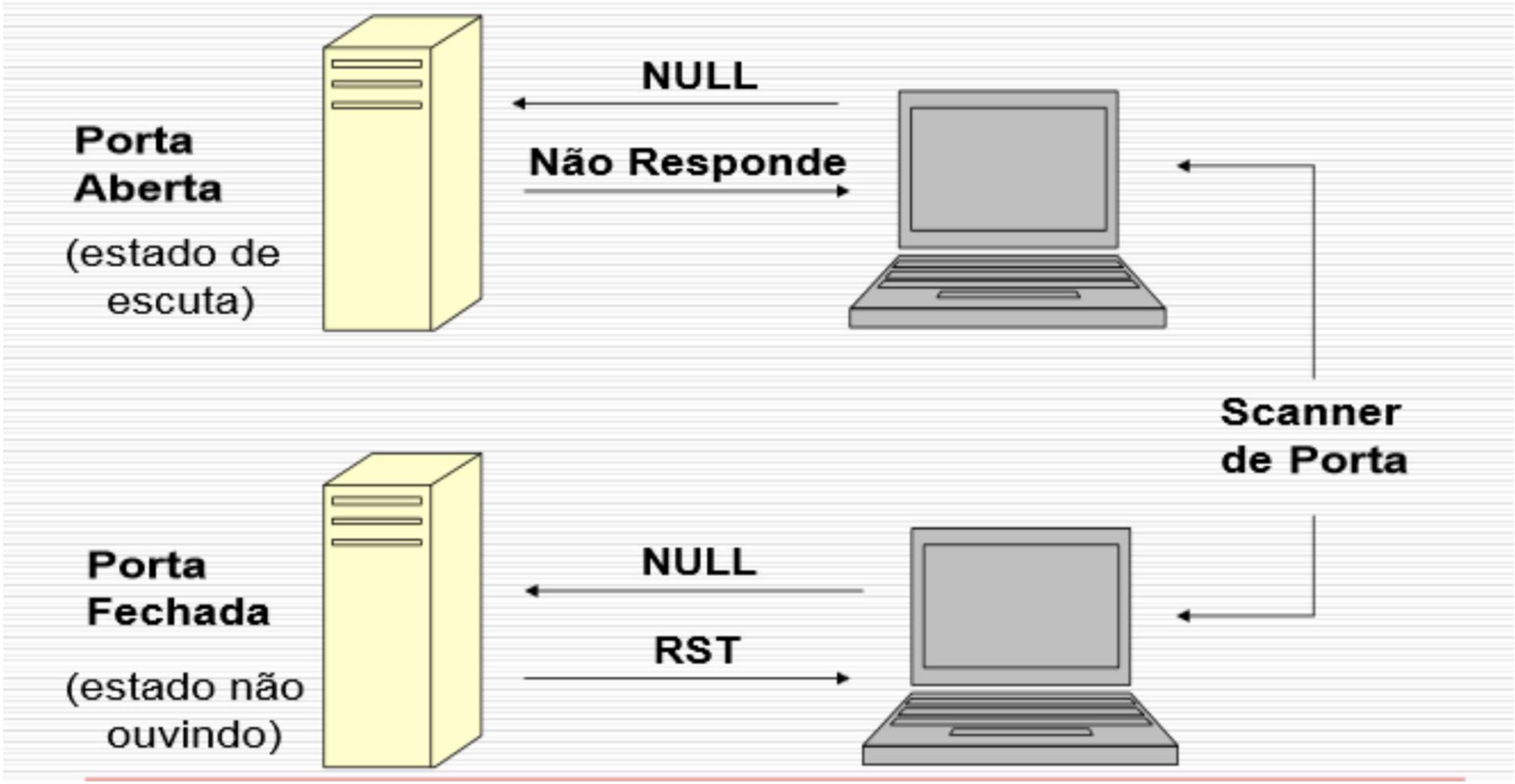
5. Varredura TCP (TCP Connect)



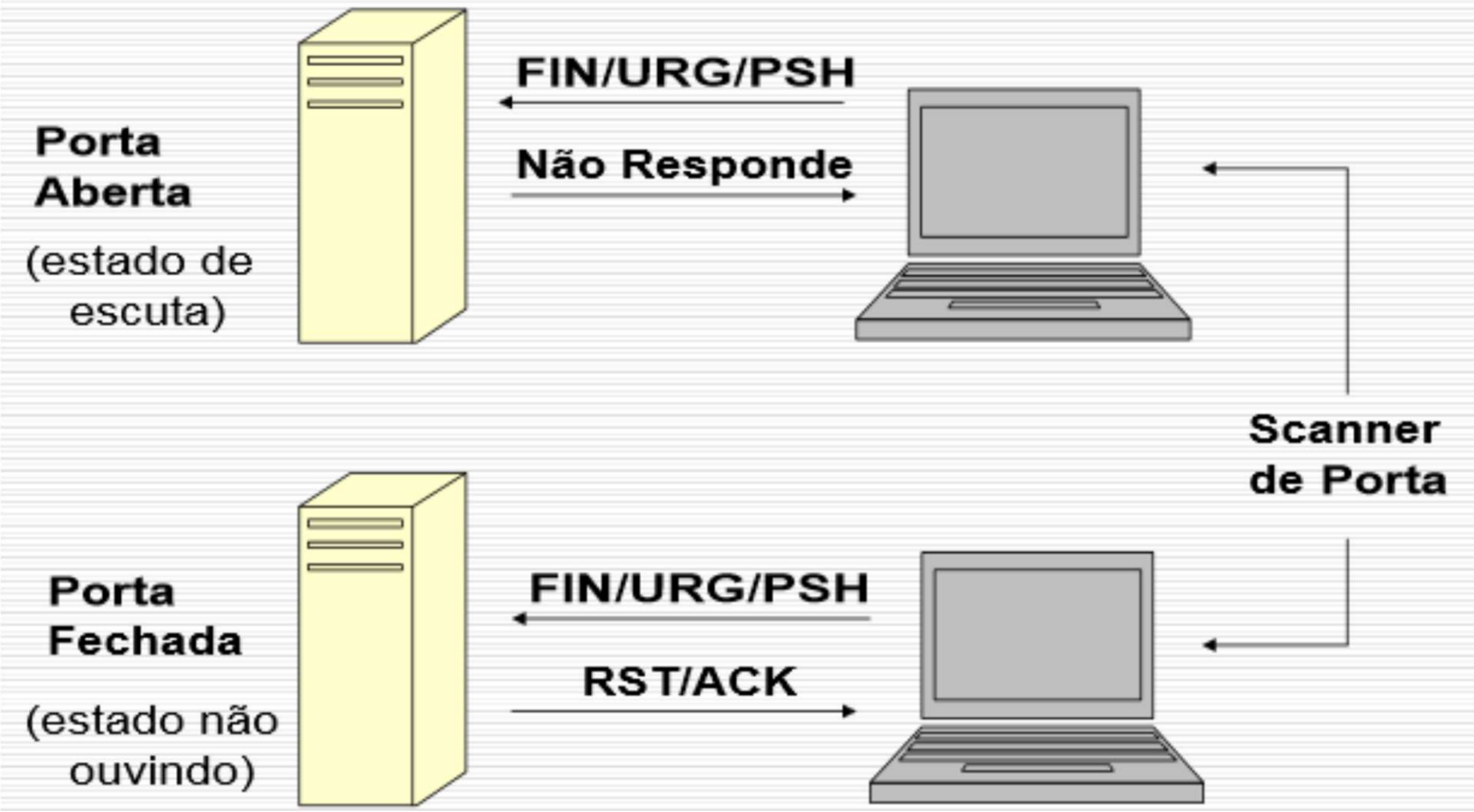
5. Varredura TCP (TCP FIN)



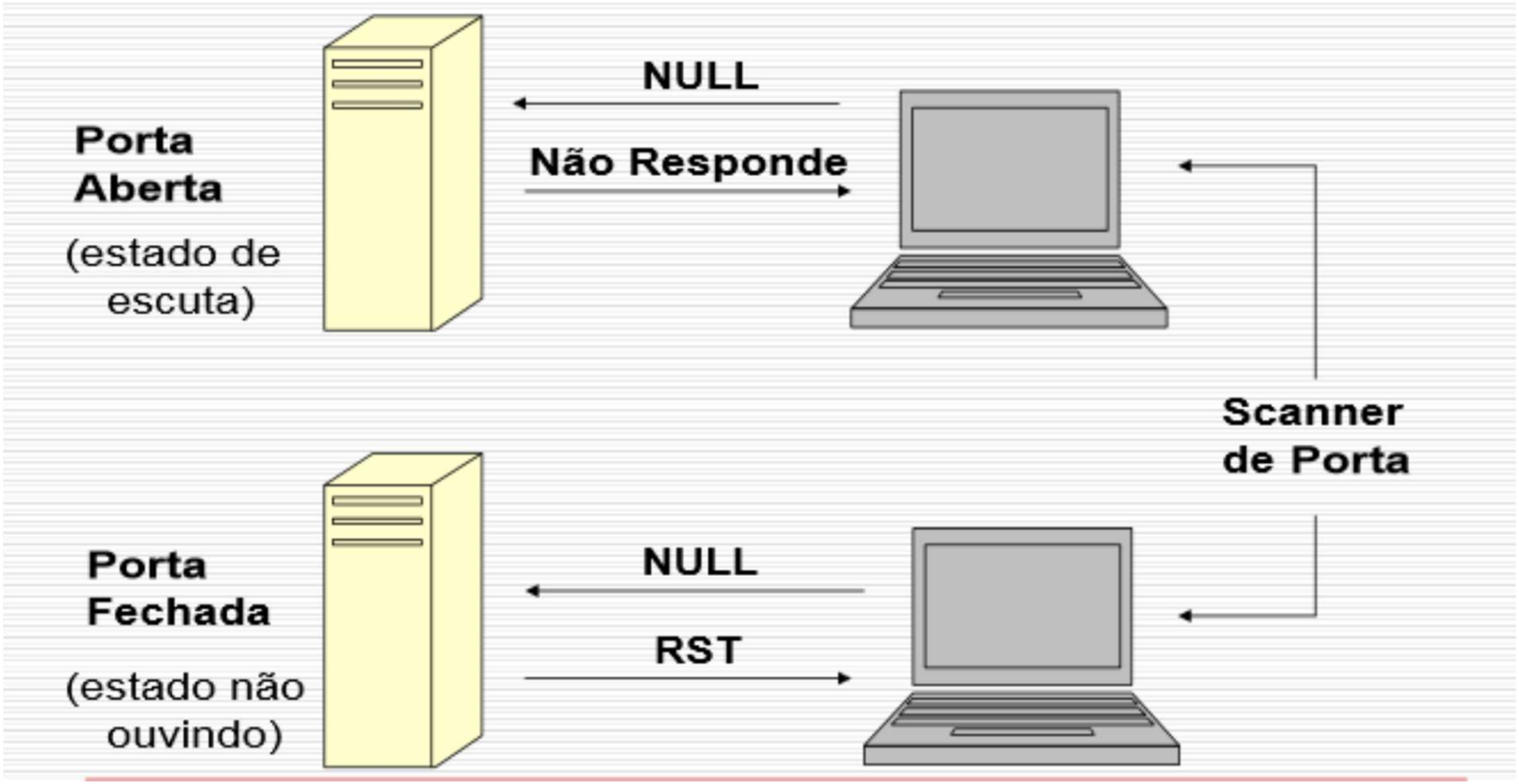
5. Varredura TCP (TCP Null)



5. Varredura XMAS (TCP XMAS)



5. Varredura UDP



6. Texto Varredura TCP (TCP SYN e TCP Connect)

Técnica	Explicação	Exemplo
Varredura TCP SYN	Tipo de varredura mais comumente utilizada, facilmente detectável. O atacante envia para o alvo pacote com a flag SYN setada: se receber SYN/ACK, a porta está aberta; se receber RST, a porta está fechada.	`#Nmap -sS <ip_alvo>`
Varredura TCP Connect	Tipo de varredura padrão do Nmap, também facilmente detectável. O Nmap procura realizar uma conexão normal com a máquina-alvo, emitindo no final o comando *connect*.	`#Nmap -sT <ip_alvo>`

- TCP SYN: não completa a conexão
- TCP Connect: completa a conexão

6. Texto Varredura TCP (TCP FIN)

Técnica	Explicação	Exemplo
Varredura TCP FIN, XMAS (Árvore de Natal) e TCP Nula	Essa varredura explora uma falha sutil na implementação do TCP/IP na máquina-alvo. Um atacante envia para o alvo pacote com a flag FIN, sem flag (TCP Null) ou com todas as flags setadas (XMAS). Se receber RST, a porta está fechada. Se não receber nada ou um pacote qualquer, a porta está aberta.	#Nmap -sF <ip_alvo> #Nmap -sX <ip_alvo> #Nmap -sN <ip_alvo>
Varredura UDP	Embora os serviços mais populares na internet utilizem o protocolo TCP, serviços como DNS, SNMP e DHCP utilizam o protocolo UDP. Essa varredura permite identificar serviços UDP em execução na máquina. Seu modo de funcionamento é bastante simples: o atacante envia para o alvo um pacote UDP. Se receber a mensagem ICMP Port Unreachable, a porta está fechada. Se não receber nada ou um pacote qualquer, a porta está aberta.	#Nmap -sU ip_alvo

7. Varredura com Decoy (-D)

Varreduras Decoy	Realiza varreduras em um alvo utilizando endereços falsos. O objetivo é "esconder" o verdadeiro alvo de sistemas de detecção de intrusos (IDS).	`# Nmap -s S -D 101.102.103.104, 1.1.1.1, 2.2.2.2, 3.3.3.3 ip_alvo`

Para cada pacote, envia outro "spoofado" para cada decoy

- ✓ Gera MUITO ruído, mas dificulta a definição da origem
- ✓ Eficaz no contorno de ferramentas de gerência automatizada de logs

Existem outras técnicas como:

- Varredura TCP Idle (-sI)
- Varredura FTP Bounce (-b)
- Varredura com spoofing IP (-S)
- Varredura com spoofing MAC (--spoof-mac)

- Controle de Desempenho (-T)
- Pacotes fragmentados (-f)
- Definição da porta de origem (-g)

7. Para uma leitura detalhada

https://nmap.org/man/pt_BR/man-port-scanning-techniques.html