Capítulo 5

Técnicas de Varreduras

O que é uma varredura ?

Técnicas de Varredura

- **Baseadas em portas**:

  Em que o scanner se comporta como um pseudo-cliente, identificando as **portas de serviços** ativos (**portas abertas**) em um determinado host.

Técnicas de Varredura

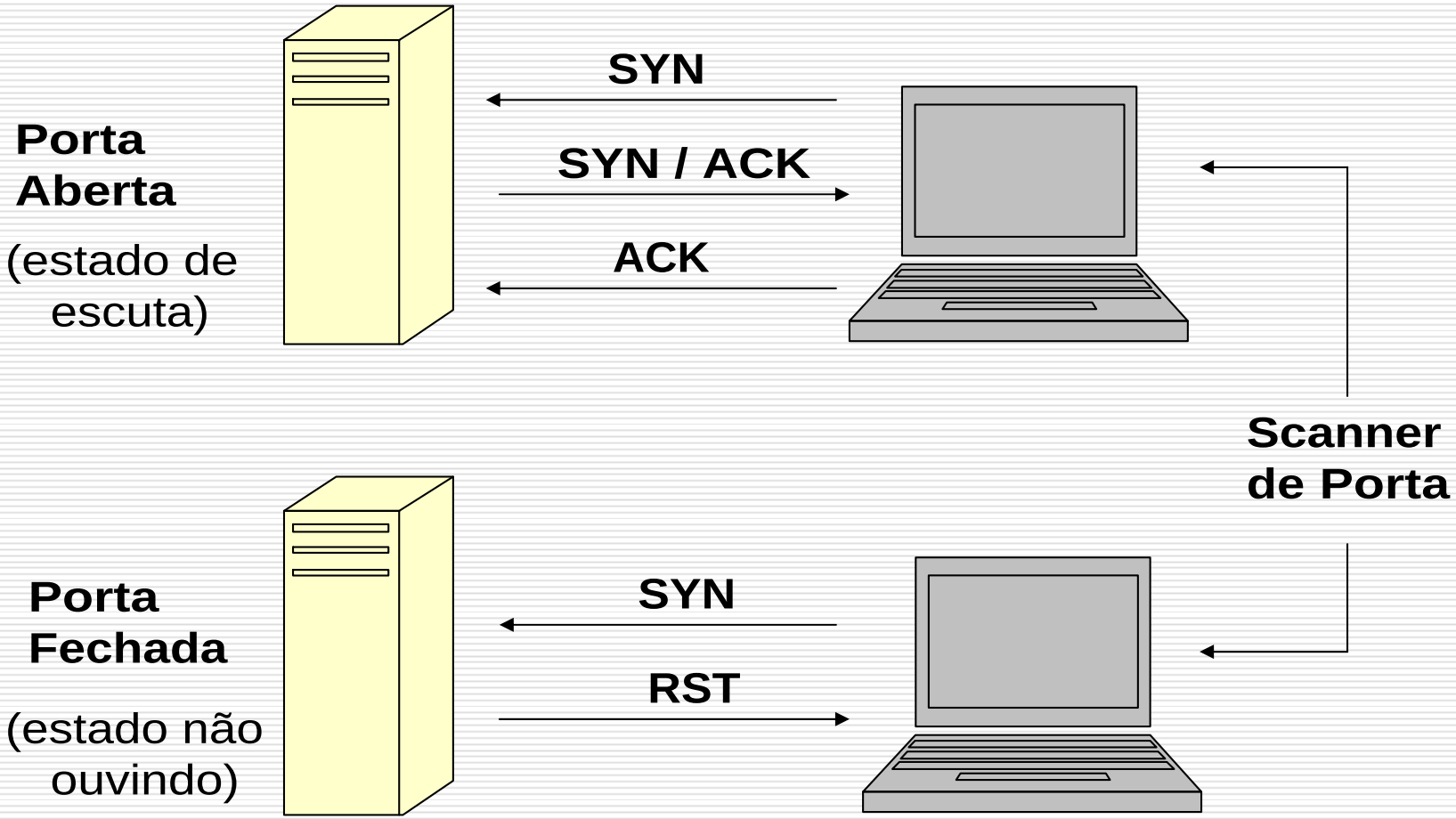
- **Baseadas nos serviços**

  Para levantamento de dados mais específicos.

Varreduras de portas clássicas

- TCP connect
- TCP syn (conexão semi-aberta)
- Baseadas na RFC 793 (não Microsoftware)
- TCP Xmas Tree (árvore de natal)
- TCP null (varreduras nulas)
- Microsoftware e RFC 793
- UDP
- ACK
- TCP window
- TCP fin/ack (fim de conexão)

TCP Connect


Porta Aberta
(estado de escuta)
SYN
SYN / ACK
ACK
Scanner de Porta
Porta Fechada
(estado não ouvindo)
SYN
RST

TCP Connect

- Quase todos scanners de portas usam esse recurso.
- Na prática, é um *handshake* para cada porta definida na varredura.
- Um *handshake* demanda duas mensagens TCP por porta.
- A varredura é facilmente detectável.
- Não é preciso nenhum privilégio especial.

TCP Connect

- Uma mensagem SYN é enviada.
- Se a **porta estiver (aberta) ouvindo com um serviço**, a conexão se sucederá.
- Um **SYN é retornado** estabelecendo **o número de sequência inicial**. Um **ACK** considera o **campo numérico de confirmação válido**.

TCP Connect

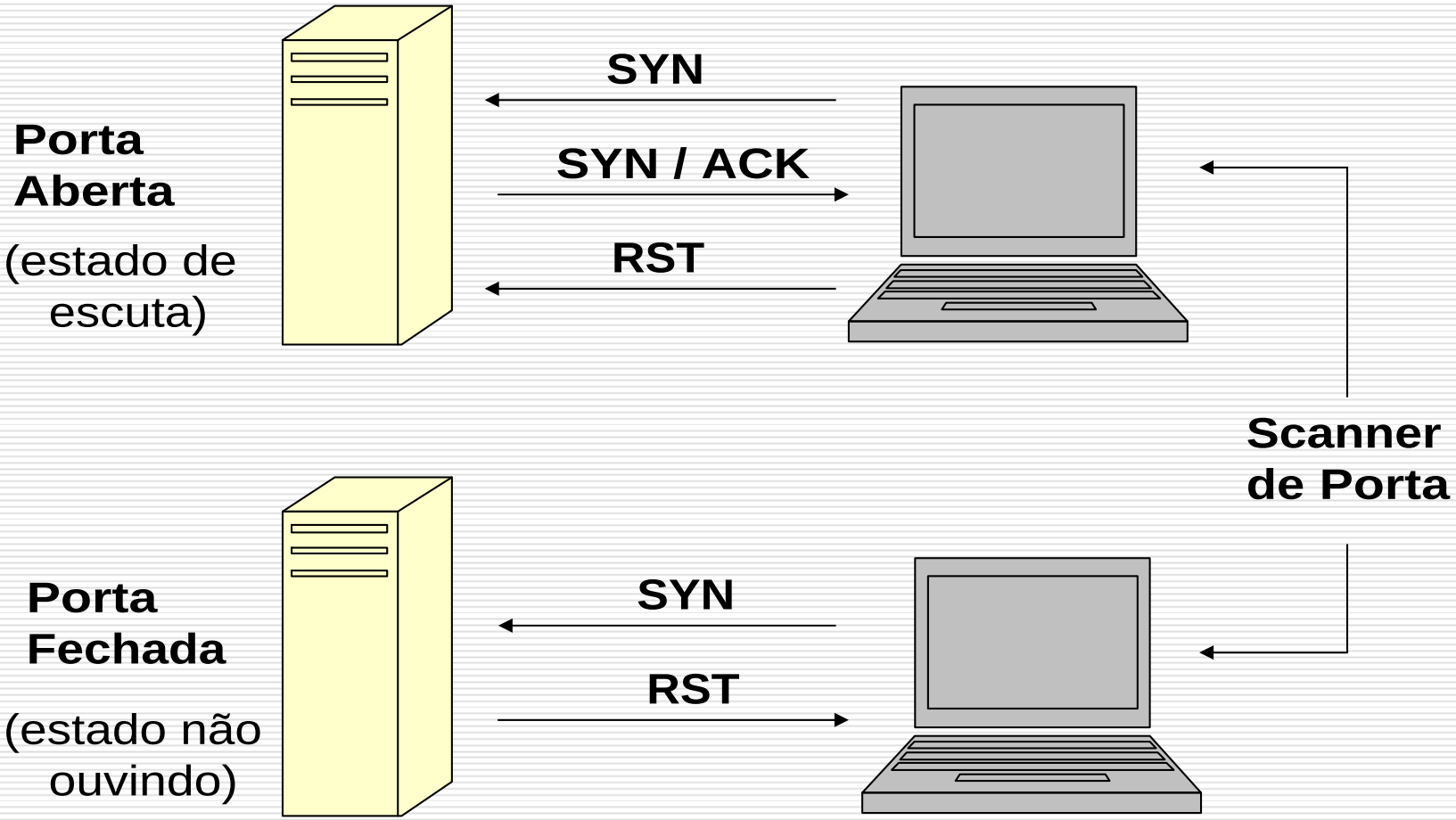
- Se a **porta estiver (fechada) sem serviço ouvindo**, uma mensagem **RST é retornada**, para **reiniciar o pedido de conexão**.

- A máquina-alvo mostrará uma conexão que falhou, porque a porta não está ouvindo, em estado de conexão.

TCP Connect

- Port Scanners
  - Nmap
  - Amap
  - Blaster

TCP SYN


Porta Aberta
(estado de escuta)
SYN
SYN / ACK
RST
Scanner de Porta
Porta Fechada
(estado não ouvindo)
SYN
RST

TCP SYN

- Técnica muito usada.
- O scanner envia uma mensagem SYN, como se estivesse pedindo uma conexão.
- Uma resposta da máquina-alvo com SYN/ACK indica que a porta se encontra ouvindo, através de um serviço.

TCP SYN

- Um RST indica que a porta não está ouvindo. O *handshake* é cancelado.
- A técnica ser conhecida como conexão semi-aberta, pois a exploração não demanda um *handshake* completo.

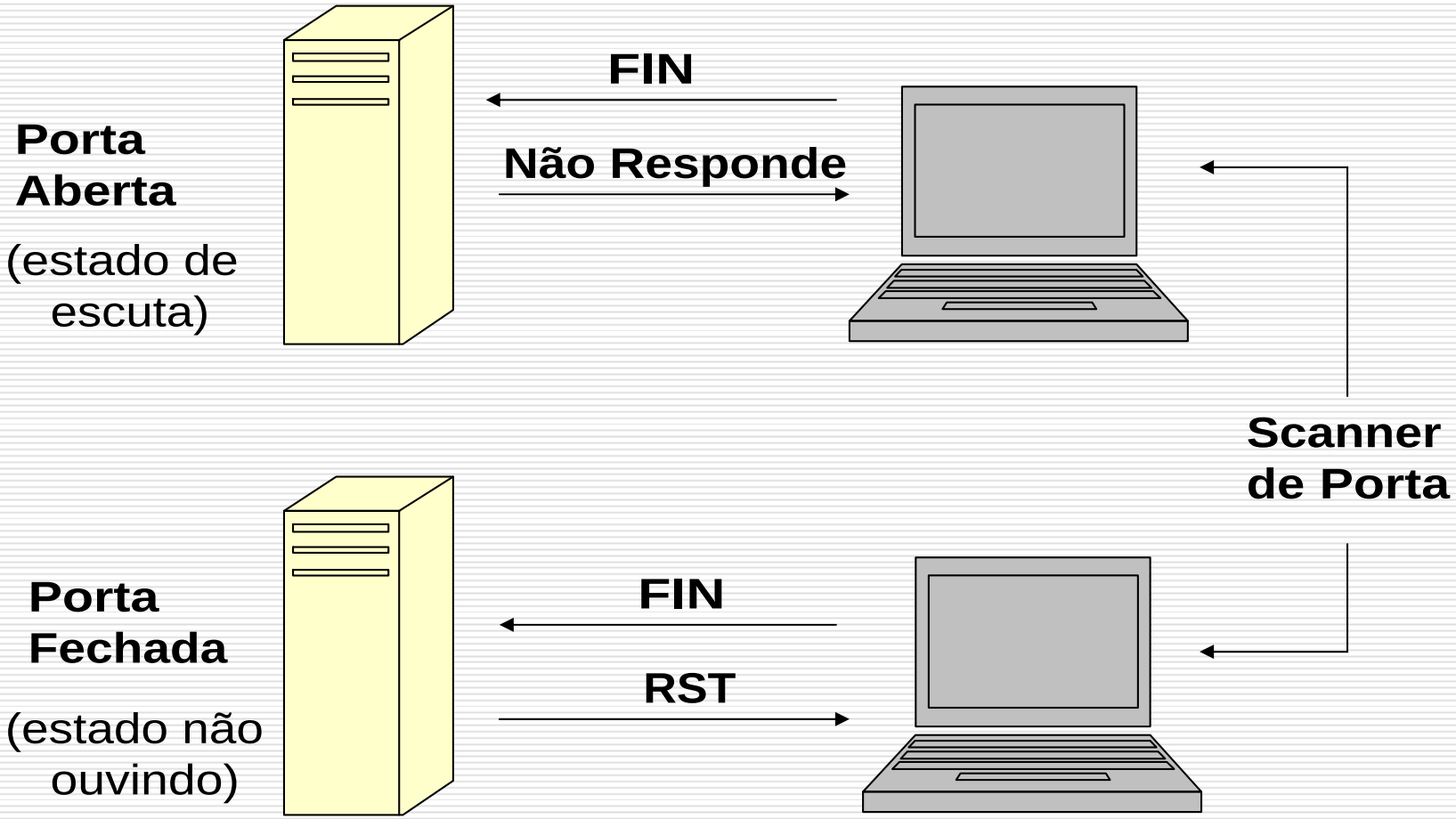
TCP SYN

- **Nmap** usa essa lógica.
- Mas, é comum encontrarmos scanners mal escritos que não enviam o RST após o SYN/ACK.
- É como se o scanner não tivesse recebido o SYN/ACK.
- Isto motiva o scanner a realizar uma segunda mensagem RST.
- Demanda privilégio de *root*.

TCP SYN

- Port Scanners
  - **Netstat** (Windows)
  - **Netcat**
  - **Amap** (ideal para leitura de *banners*)
  - **Blaster**
  - **Hping2**
  - **Nmap** (pode ser combinado com o **Amap**)

Varreduras baseadas na RFC 793



Varreduras baseadas na RFC 793

- Com **portas fechadas** (sem serviço), ao receberem **TCP FIN**, ou mensagem com prioridade **TCP FIN/ URG/ PSH**, ou mensagem **TCP NULL** (sem nenhum flag ativo), o host-alvo responde com um **TCP RST**.

Varreduras baseadas na RFC 793

- Quando a **porta estiver aberta (existe serviço)**, eles são ignorados. **O hos-alvo não responde**.

- O scanner não recebe nenhuma resposta, **pois não podem pertencer a nenhuma conexão estabelecida**.

Varreduras baseadas na RFC 793

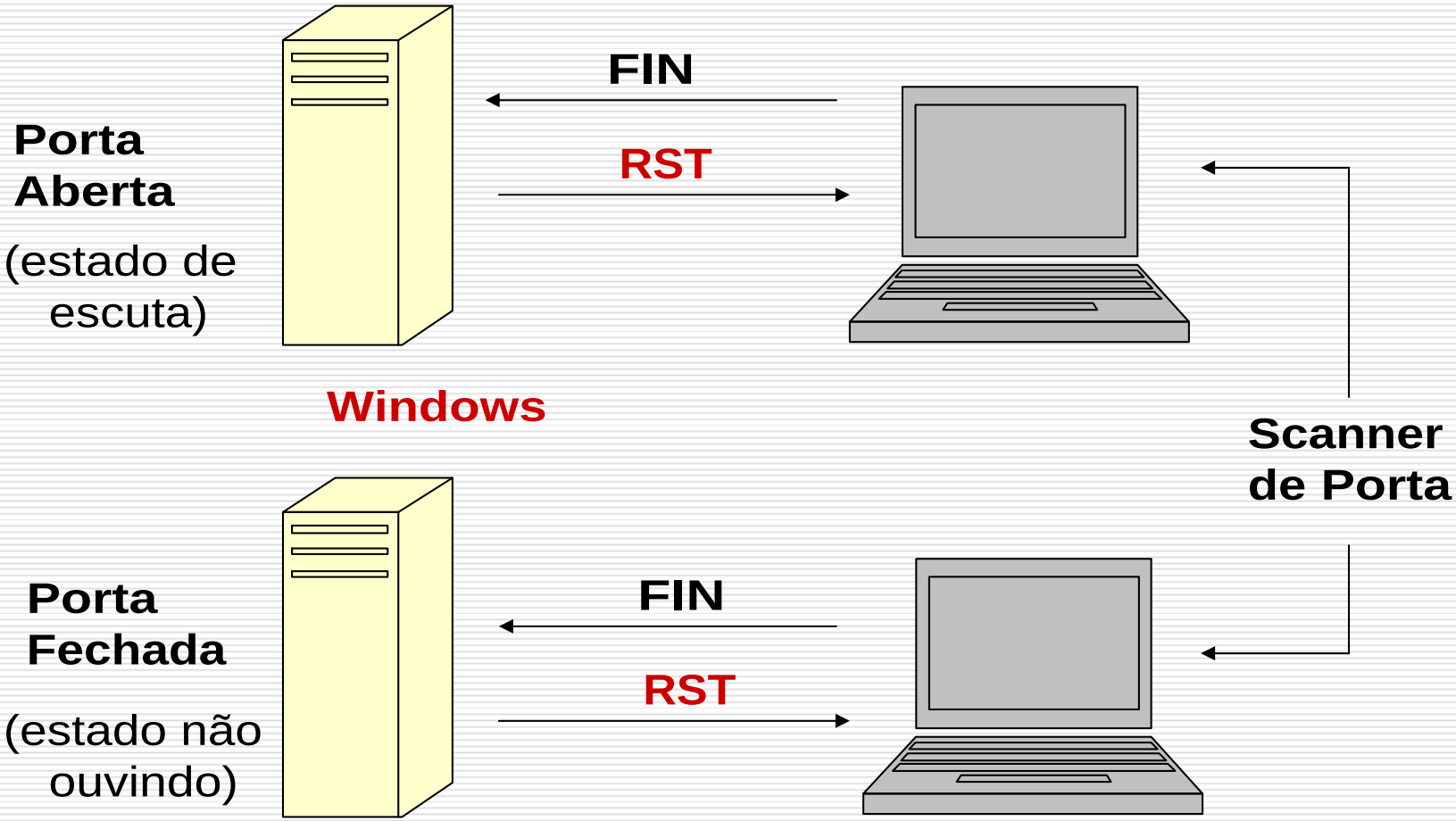
- Convém que um IDS na máquina-alvo, possa identificar varreduras baseadas na RFC 793.
- Se um IDS só identifica varreduras de início de conexão (TCP Connect e TCP SYN), a técnica RFC 793 passa despercebida.

Varreduras baseadas na RFC 793

- Não funcionam em pilhas TCP/IP Microsoftware, pois essas não seguem a RFC 793.

- Pilhas **TCP/ IP Microsoftware respondem com TCP RST** , tanto para **portas abertas**, como para **portas fechadas**, como segue:

Varreduras baseadas na RFC 793 em pilhas TCP/IP Microsoftware

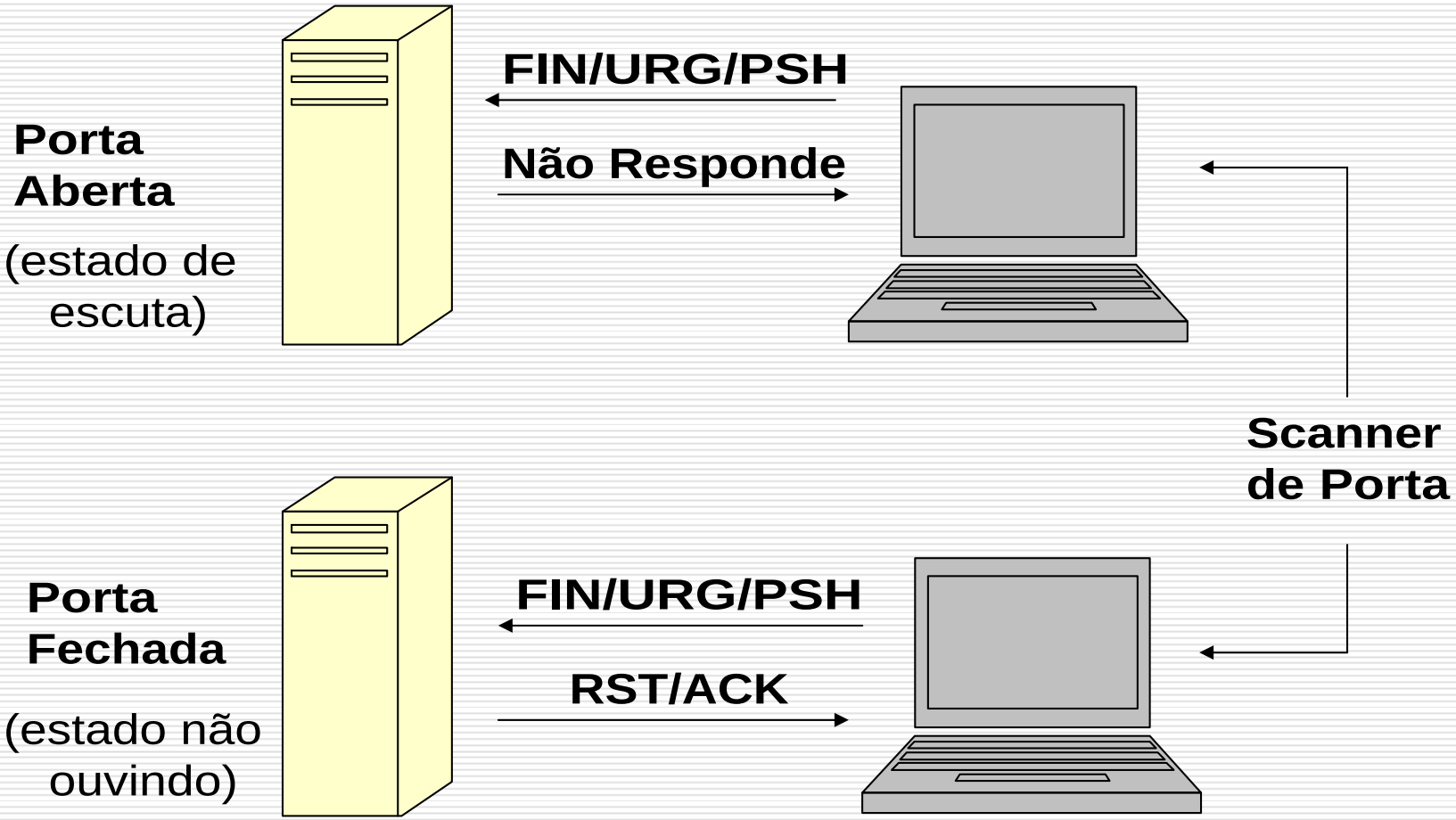


Varreduras baseadas na RFC 793

- Port Scanners

  - Hping2
  - Nmap

Varredura Xmas Tree



Varredura Xmas Tree

- Equivale a TCP FIN.
- Com **portas abertas** (com serviço), e mensagem com prioridade **TCP FIN/ URG/ PSH**, o host-alvo **não responde**.

Varredura Xmas Tree

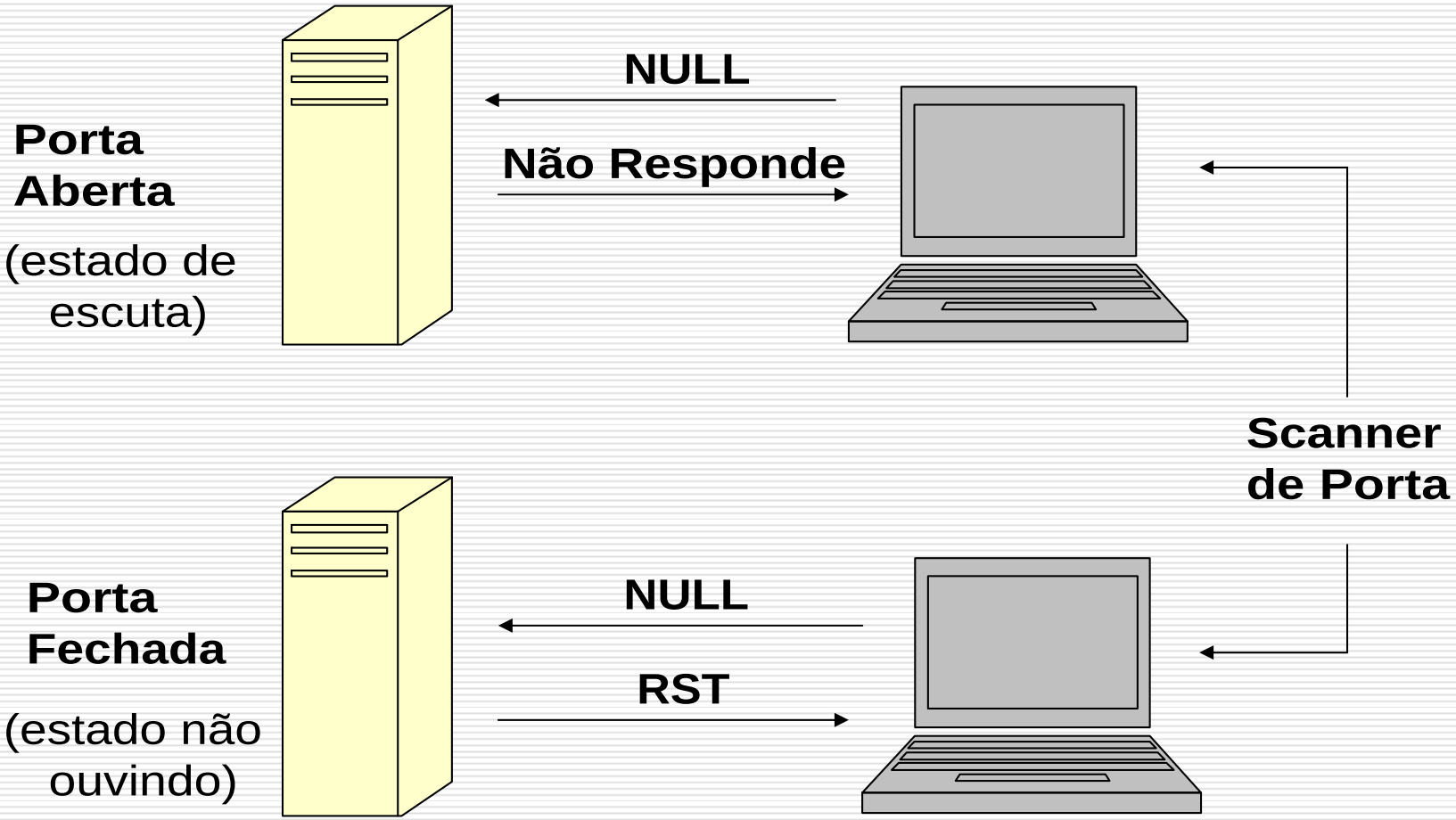
- Com **portas fechadas** (sem serviço), e mensagem com prioridade **TCP FIN/ URG/ PSH**, o host-alvo responde com um **TCP RST**.

Varredura Xmas Tree

- Port Scanners

  - Hping2
  - Netstat
  - Nmap

TCP Null (sem flags ativos)



TCP Null (sem flags ativos)

- Equivalente a TCP FIN.
- Tem-se resposta **TCP RST** para **portas fechadas**.
- **Não se tem resposta** para **portas abertas**.

TCP Null (sem flags ativos)

- Port Scanners

  - Hping2
  - Netstat
  - Nmap

Microsoftware e a RFC 793

Varredura ACK

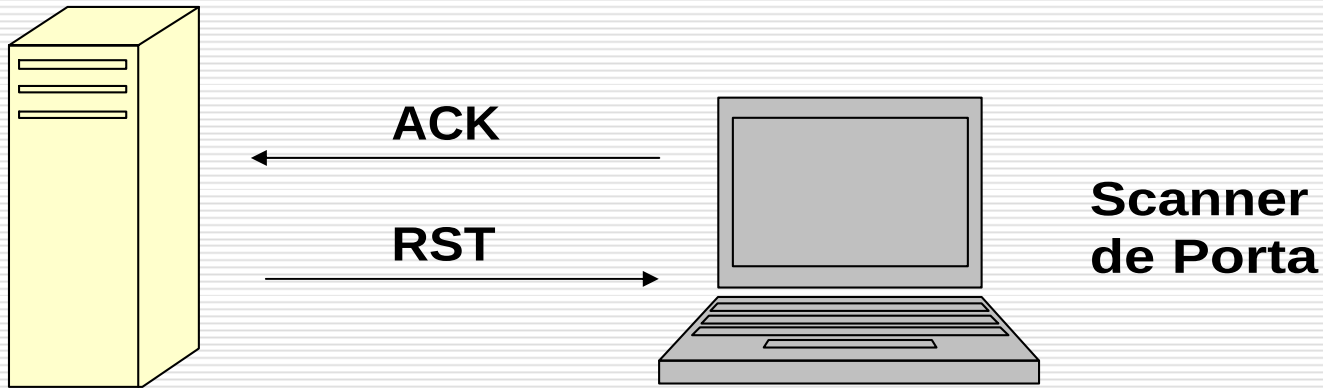
Porta Aberta

(estado de escuta)

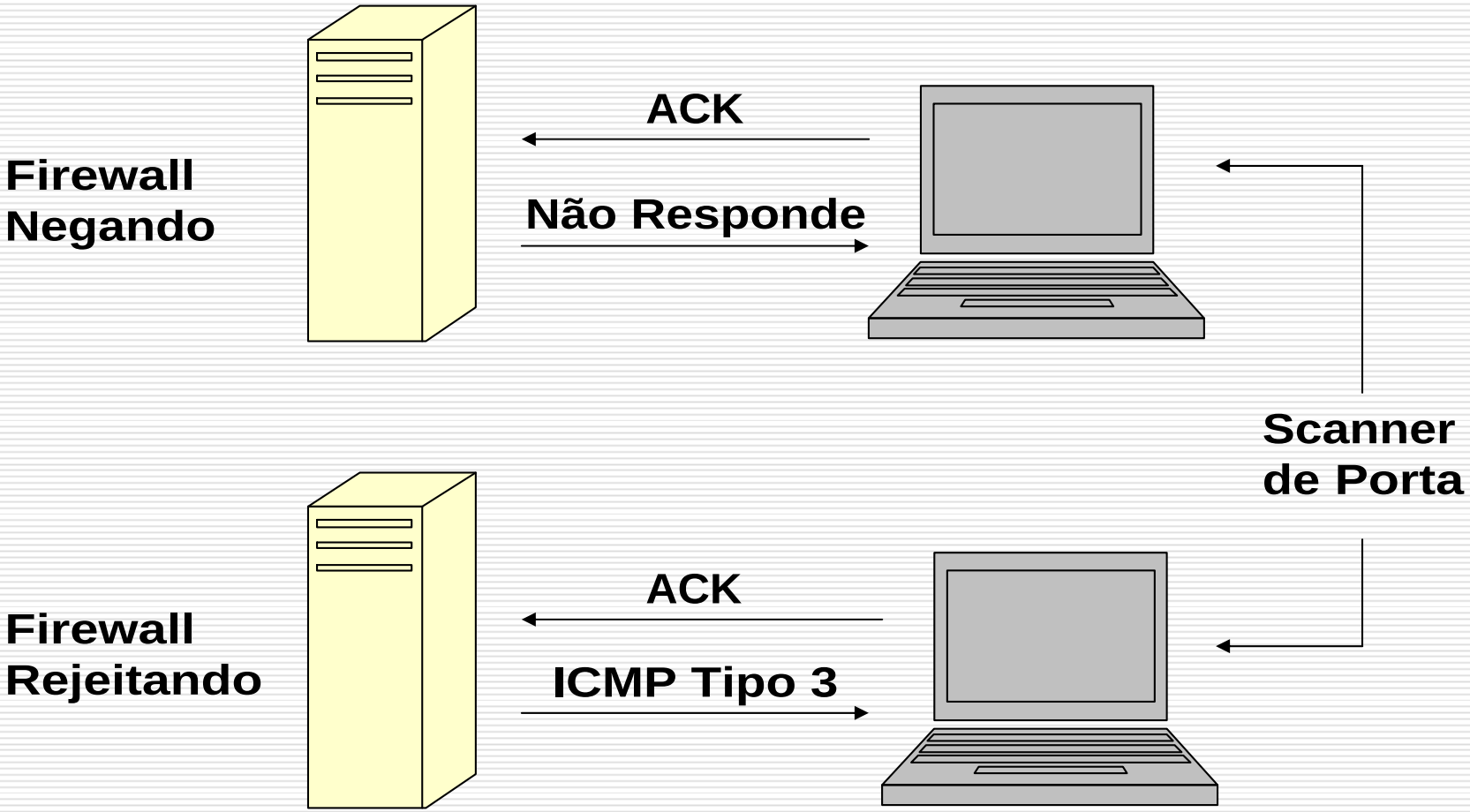
ou

Porta Fechada

(estado não ouvindo)



Varreduras ACK (continuação)



Varreduras ACK

- Técnica usada para identificar Firewalls.
- Um TCP ACK, que não pertença a nehuma conexão estabelecida, é gerado pelo scanner.
- Se um RST é devolvido pela máquina-alvo, tanto em uma porta aberta com em uma fechada, as portas são classificadas como não tendo Firewalls.

Varreduras ACK

- Sendo um ICMP 3 ou nenhuma resposta é devolvida, é assumido que as portas são filtradas, ou seja existe Firewall.

- Port Scanner

  Hping2

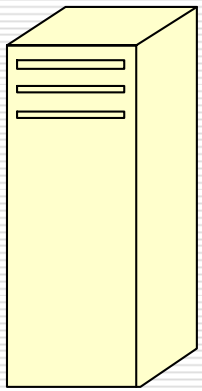
- Exemplo:

  > hping2 ip.ip.ip.ip **–ack** –p <porta aberta ou fechada> -c 3

Varredura TCP Window

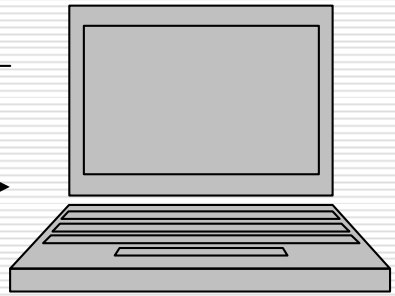
Porta Aberta

(estado de escuta)



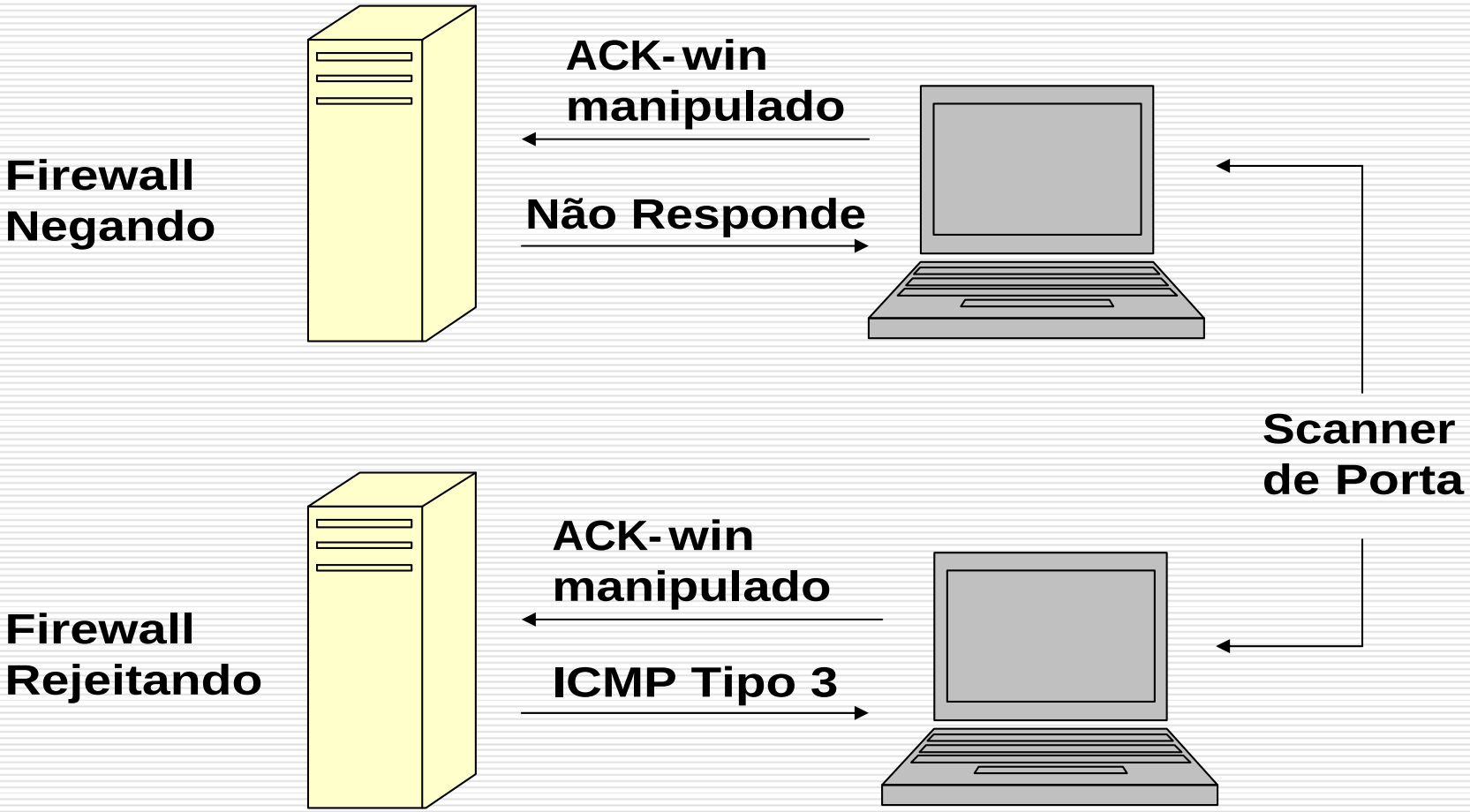
ACK-win

RST



Scanner de Porta

Varredura TCP Window (continuação)



Varredura TCP Window

- Técnica avançada.
- Tem como objetivo identificar portas protegidas por Firewall, e não portas abertas com outros serviços.
- Nmap envia ACK-win. Voltando **RST**, **a porta não está filtrada**.

Varredura TCP Window

- **Não tendo resposta** ou **voltando ICMP 3**, a porta está filtrada e assim existe Firewall.

- Por Scanner
  - Nmap

- Exemplo: > nmap **–sW** ip.ip.ip.ip

Varredura FIN/ACK

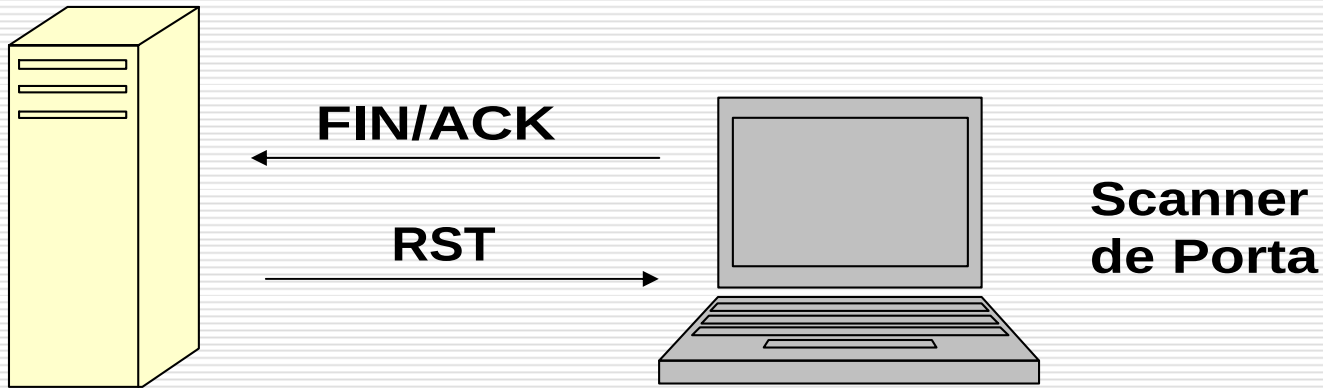
Porta Aberta

(estado de escuta)

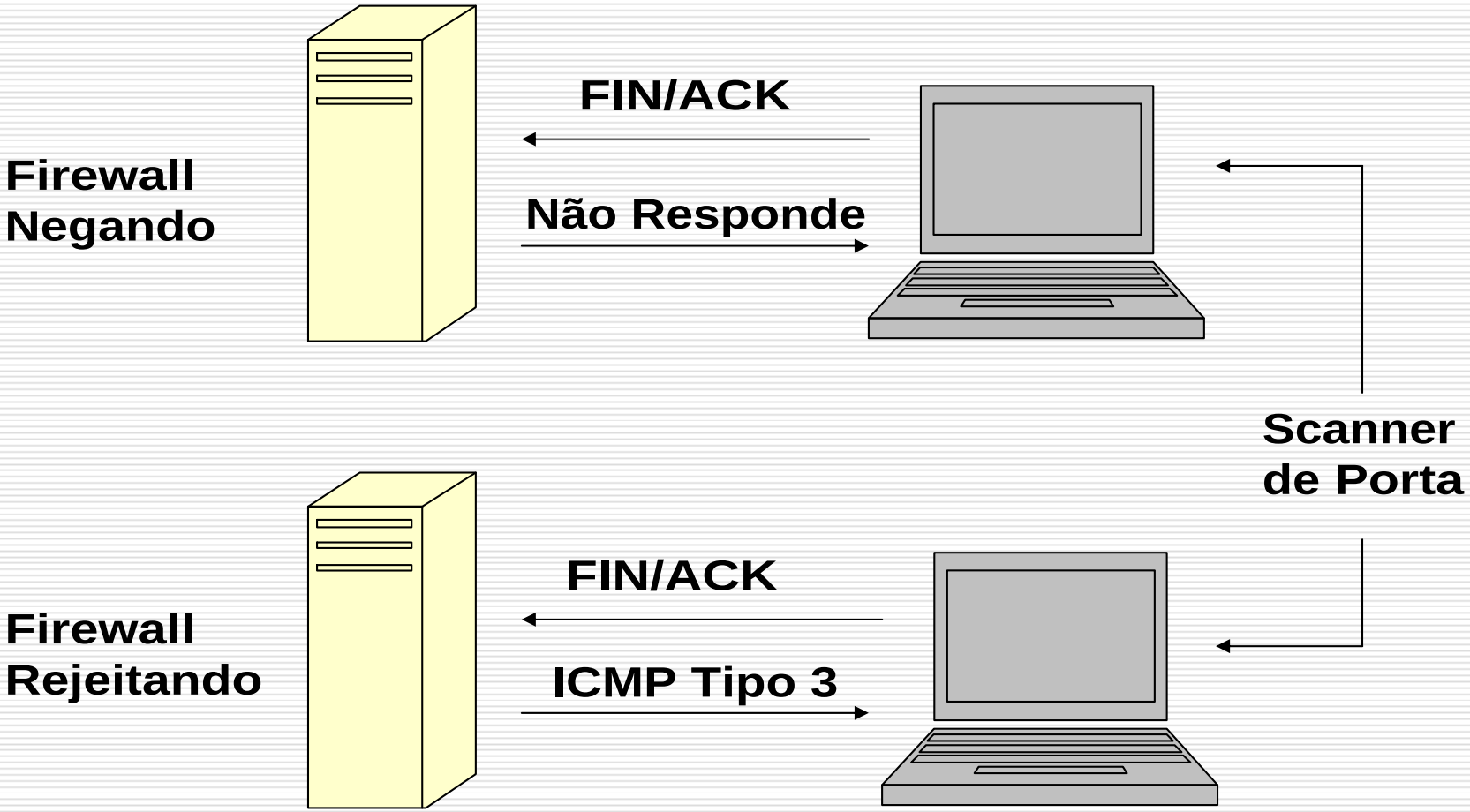
ou

Porta Fechada

(estado não ouvindo)



Varreduras FIN/ACK (continuação)



Varreduras FIN/ACK

- Forma de identificar um Firewall.
- Bit FIN ativo.
- Comportamento similar à varredura ACK.
- Port Scanners
  - Hping2
  - Nmap
- Exemplos:

  hping2 ip.ip.ip.ip –fin –ack –p <porta aberta ou fechada> -c 3

  nmap –sM ip.ip.ip.ip

Escondendo um Firewall

- Enganar um scanner como o Nmap.
- Se **Nmap receber um TCP RST** como resposta, ele envia dois pacotes.
- Para esses dois pacotes enviados, **Nmap assume que a porta não está filtrada**.

Escondendo um Firewall

- Se **Nmap recebe ICMP 3** como resposta, ele **assume que a porta é filtrada por um Firewall** que rejeita pacotes.

Escondendo um Firewall

- Se **Nmap não recebe nenhuma resposta**, ele envia mais quatro pacotes e, não obtendo nenhuma resposta, **ele assume a porta como filtrada**.

Escondendo um Firewall

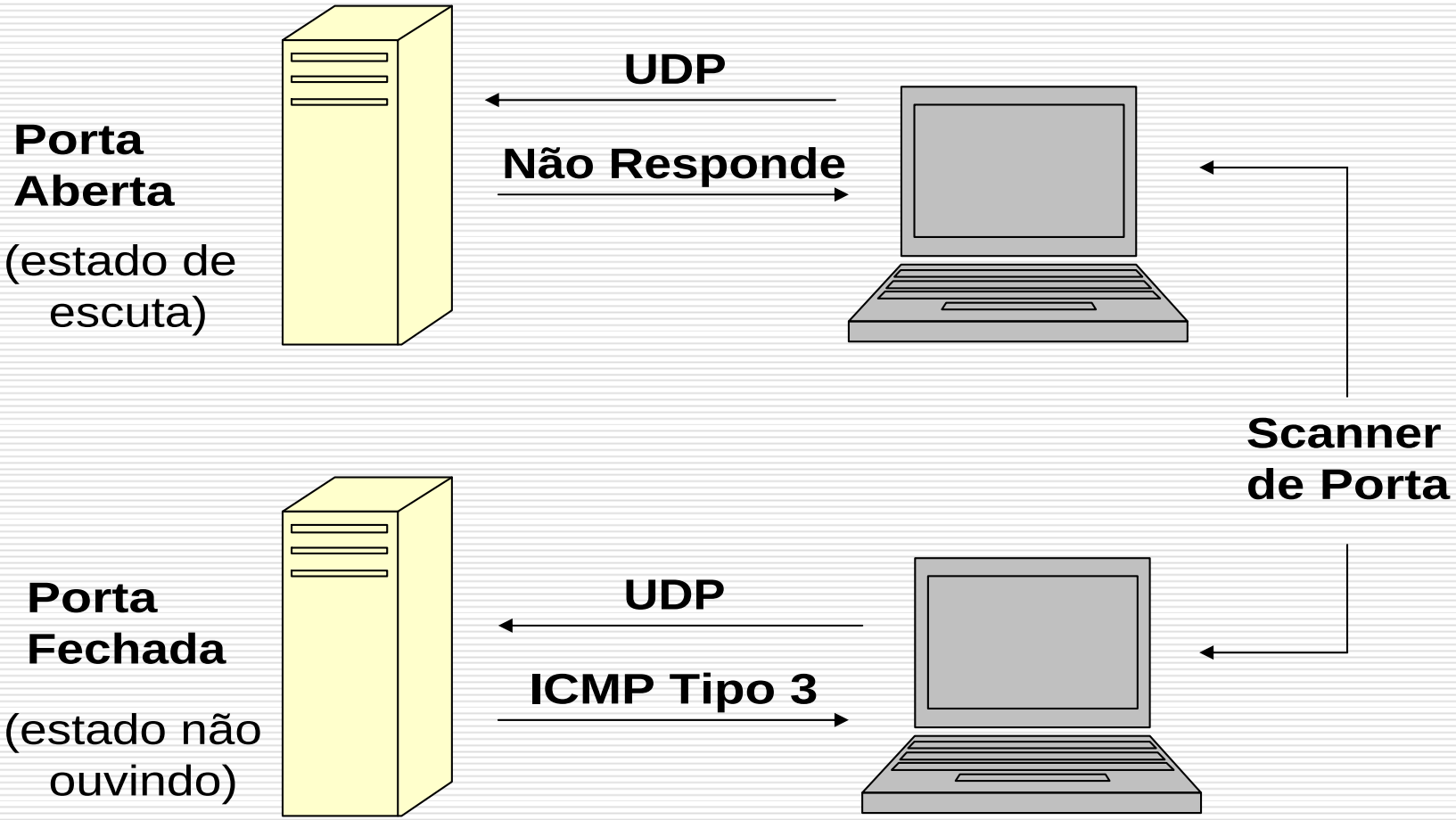
- Definindo-se uma **política para o firewall**, em que a porta 22 somente aceite conexões IP já pré-definidas, qualquer outro pacote IP será rejeitado.

- Na política, definimos **o firewall não rejeitar pacotes com ICMP** (não responder com ICMP), **mas com TCP RST**.

Escondendo um Firewall

- Isto, faz com que seja gerado um **falso negativo**, ou seja, uma informação tal que, a ocorrência existe, mas não é identificada (**o Firewall existe, mas o Nmap não o vê**).

Varreduras UDP



Varreduras UDP

- Técnica que descobre os serviços UDP ativos, ou seja, as portas UDP abertas em um host.
- Datagramas de 0 bytes são emitidos a cada porta da máquina-alvo.
- Se um datagrama chega em uma porta fechada, a máquina-alvo devolve uma mensagem de erro ICMP 3. Caso não retorne nada, supõe-se que a porta é aberta.

Varreduras UDP

- Port Scanners
  - Netstat
  - Hping2
  - Nmap

Varreduras RPC

- Varredura baseada em serviço.
- Lavantando dados de RPC com Nmap:

```
nmap –sR  ip.ip.ip.ip
```

Varredura Bounce

- Técnica que consiste em utilizar um serviço de um determinado host para levantar informações sobre outros serviços.

Varreduras baseadas no Cabeçalho do Protocolo IP

Varreduras ICMP e Discovery

Formas de Furtivas de Varreduras

Varreduras Furtiva Temporizadas

- Também conhecida como “Slow Scan”.
- **Temporiza** o envio de pacotes.
- Obtidas através do **Nmap** com a opção -T.
- Tipos de Varredura:

Métodos de Varreduras Furtivas

- **FTP Bounce / Proxy Bounce**
- **IP Decoy**
- Port Decoy
- Randon Port
- Slow Scan
- Coordinated
- Fragmenting
- **Spoofing / Sniffer**
- Multiprocessing
- Stateless

- **Servem para Intrusões.**

Varreduras Furtiva Temporizadas

- Tipos de Varredura:

Enumeração de informações em serviços

- SMTP scan
- SNMP scan
- SMB scan
- Reverse Ident
- RPC scan

Ferramentas de Ataque

- Constrói-se ou escolhe-se as ferramentas para a invasão.

- Rootkits:
  - Sniffer
  - Trojan
  - Backdoor
  - LogClean

Para concretizar um Ataque

- Instalação de **Sniffers**.
- Técnicas de **Backdoor**.
- **Apagamento de rastros ou forjar logs**, eliminando o rastro do invasor ou dificultando a auditoria (CleanLogs).
- **Ataques DoS**,
- **Ataques DDoS**, **DRDoS**

Ataques sem intrusão

- Existem formas de ataque que não têm objetivos de intrusão.

- Exemplos:
  - Spam em servidores que permitem ***relay*** (retrasmissão).

  - DoS, DDoS, DRDoS

Ataques sem intrusão

- Algumas supostas invasões ocorrem sem nenhuma intrusão no sistema.
- Como nos casos de ataques de **entrada inesperada**.

Para Auto-Monitoramento

- Verificadores de Senha (**John the Ripper**),
- Auditoria de Segurança de Sistemas (**Nmap**),
- Scanner de Segurança para identificar vulnerabilidades (**Nessus**).
- Firewalls, Web Proxy
- IDS de Host (**Tripware**),
- IDS de rede (**Snort**)

Melhor Proteção

- Estabelecimento de Políticas de Segurança.
- Informações Criptografadas em protocolos (S/MIME, SSH, SSL, TSL, IPSec...).
- Redes Privadas Virtuais (VPN com SSL, IPSec)