Capítulo 3

Anatomia dos Ataques às Redes TCP/IP

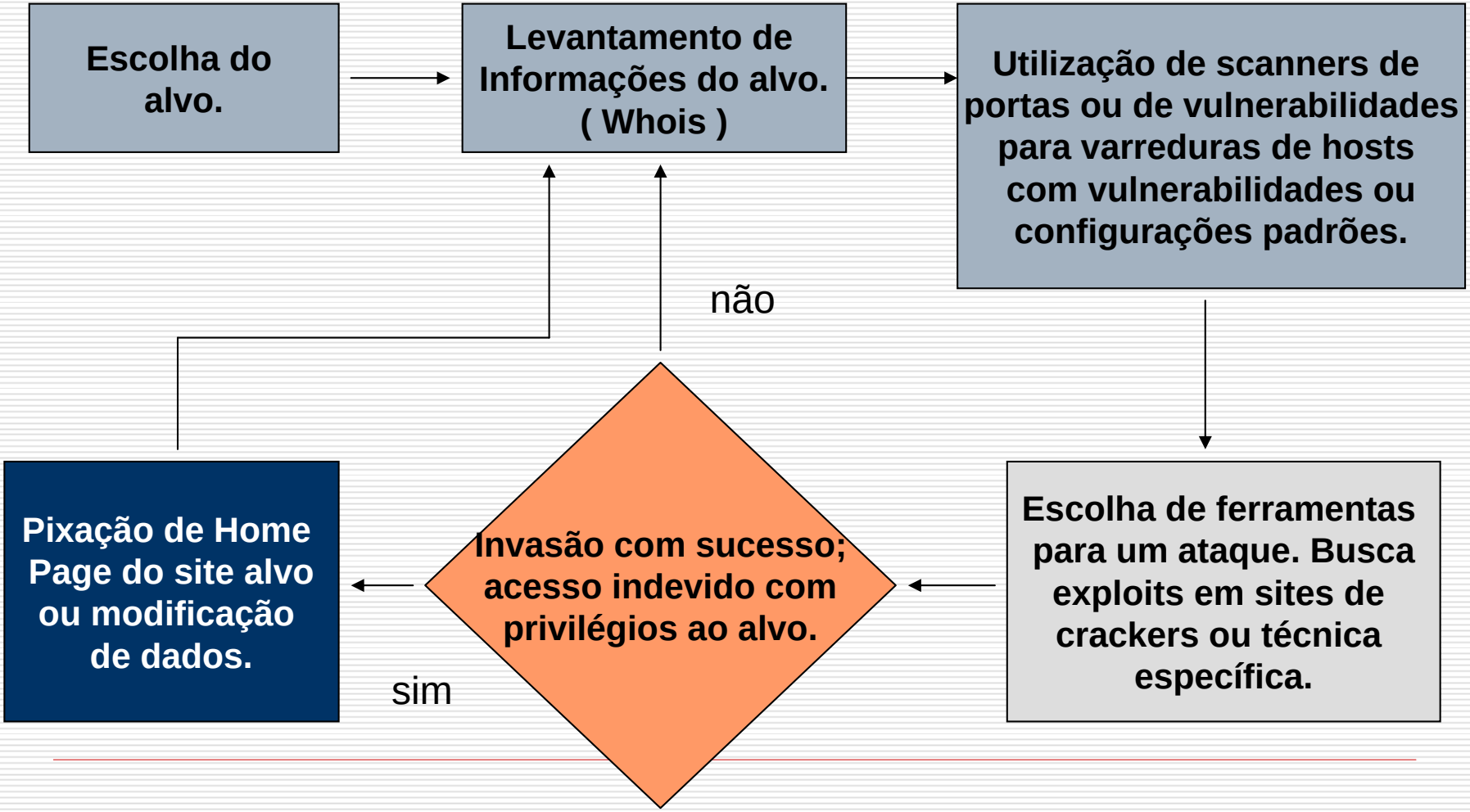
A construção de um ataque

- O primeiro passo para entender um ataque é entender sua anatomia, ou seja a forma como se pode construir um ataque.

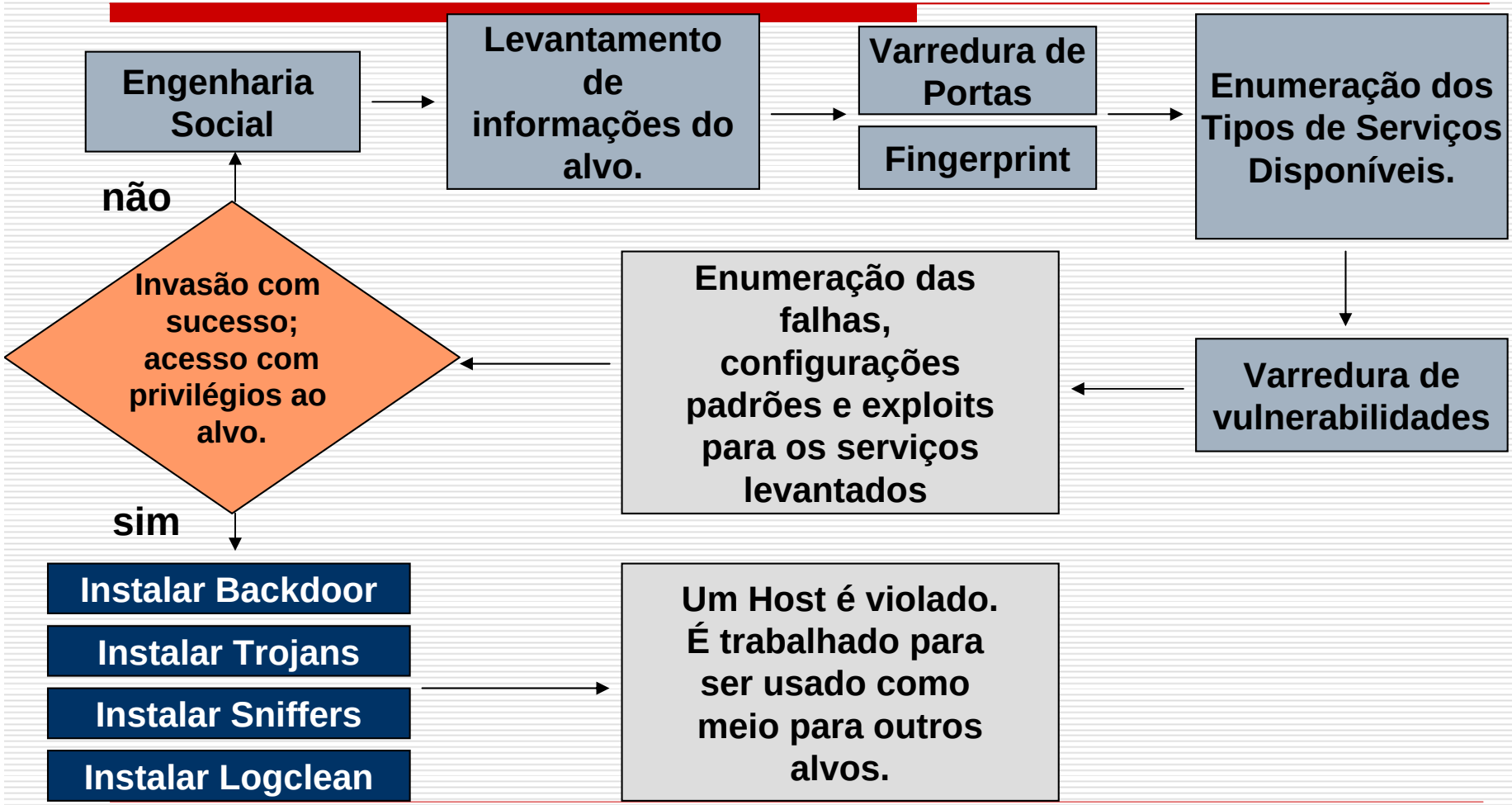
Anatomia de Ataques

- Um ataque é basicamente definido (com mais detalhes) em três etapas:
  - **Footprint**
  - **Fingerprint**
  - **Enumeração**

Anatomia de um Ataque Script Kiddie



Anatomia do Ataque Cracker



Rootkit

Ataque de Cracker

- “ ... a sua máquina nada tem de interessante ...”

- Máquina boa para ser “rooteda”
- Máquina boa para ser invadida e seus rastros serem apagados.
- O cracker consegue domínio total e usa a máquina para invadir outras.

Ataque de Cracker

- Caso o ataque seja detectado, tal máquina será identificada como a origem de ataques e seu administrador ,a priori, será responsável por possíveis danos.

- O cracker pode divulgar em canais IRC de crackers e script kiddies, as backdoors, a senha para se ter acesso à maquina comprometida.

Ataque de Cracker

- Com isso, o cracker além de ter apagado o seu rastro, chama a atenção do administrador para os “laranjas” que tenham acessado à máquina depois dele.

Etapas detalhadas de um Ataque

- Ver material impresso, distribuído em aula.

- Observações:

  - varreduras de portas
  - métodos de varreduras furtivas.
  - enumeração de informações em serviços.
  - ataques script kiddie ou cracker

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)