Segurança em Redes e Sistemas

Segurança da Informação

Rafael Roque
rra@cin.ufpe.br

Eduardo Feitosa
elf@cin.ufpe.br

Djamel Sadok
jamel@cin.ufpe.br

Agenda

- Conceitos
- Gerenciamento e Avaliação de Riscos
- Políticas de Segurança
- Detecção de Vulnerabilidades
- Ataque

Conceitos

Segurança da Informação

- Segurança da Informação (SI) é a proteção de sistemas de informação contra desastres, erros e manipulação de modo a minimizar a probabilidade e impacto de incidentes
- Req

Requisitos de Segurança

- Confidencialidade
  - ➔Garantia de que a informação é acessível somente por pessoas autorizadas
  - ➔Não deve acontecer divulgação intencional (ou não) de informações reservadas
  - ➔Questões de confidencialidade surgem porque processos e informação sensíveis do negócio só devem ser divulgados para pessoal / programas autorizados
  - ➔Necessidade de controlar acesso

Requisitos de Segurança

- Integridade
  - ➔Garantia da exatidão e completude da informação e dos métodos de processamento
    - ➔Informações não devem ser modificadas por pessoas/processos desautorizados
    - ➔Modificações desautorizadas não sejam feitas por pessoas/processos autorizados
    - ➔Informações não devem ser inconsistentes
  - ➔Necessidade de garantir que as informações são precisas e completas

Requisitos de Segurança

- Disponibilidade
  - ➔Garantia que usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário
  - ➔Informação e serviços do negócio devem estar disponíveis quando necessários
    - ➔Necessidade de controles para garantir confiabilidade dos serviços

Requisitos de Segurança

- Autenticidade
  - ➔Garantia da origem dos dados e da identidade da pessoa ou sistema
  - ➔O serviço de autenticação deve informar se a mensagem é realmente procedente da origem indicada em seu conteúdo
    - ➔Normalmente isso é obtido através de mecanismos como senhas e assinaturas digitais

Requisitos de Segurança

- Controle de Acesso
  - ➔Usuários não autorizados são mantidos à distância

Requisitos de Segurança

- Não Repúdio
  - ➔Segurança Forte – O significado de autenticação não pode ser contestado posteriormente
    - ➔O usuário não pode negar posteriormente que efetuou alguma operação no sistema

Segurança da Informação

- Como a SI pode ser obtida?
  - ➔Implementando controles para garantir que os objetivos de segurança sejam alcançados
- Porque SI é necessária?
  - ➔A informação, processos, sistemas e redes são importantes ativos para os negócios
  - ➔As informações são constantemente "ameaçadas"
  - ➔Dependência dos SIs gera vulnerabilidades
  - ➔Quase nada é projetado para ser seguro

Normas para SI

- BS-7799-1:2000 – Primeira parte
- BS-7799-2:2002 – Segunda parte
- ISO/IEC 17799
- NBR 17799

Gerenciamento e Avaliação de Riscos

Terminologia (1 # 2)

- Risco
  - ➔Possibilidade de sofrer perda ou dano; perigo
- Ataque
  - ➔Acesso a dados ou uso de recursos sem autorização
  - ➔Violação de uma política de segurança, etc
  - ➔Ativo - Altera o conteúdo da informação
  - ➔Passivo - Observação
- Vulnerabilidade
  - ➔É uma falha que pode permitir a condução de um ataque

Terminologia (2 # 2)

- Incidente
  - ➔A ocorrência de um ataque; exploração de vulnerabilidades
- Ameaça
  - ➔Qualquer evento que pode causar dano a um sistema ou rede
  - ➔A existência de uma vulnerabilidade implica em uma ameaça
- Exploit code
  - ➔Um código preparado para explorar uma vulnerabilidade conhecida

Exemplos de Ameaças

- Pessoas chaves para uma organização
  - ➔Ferimento, morte
- Servidores de arquivos
  - ➔Ataques DoS
- Dados dos alunos
  - ➔Acesso interno não autorizado
- Equipamentos de produção
  - ➔Desastre natural

Exemplos de Vulnerabilidades

- Pessoas chaves para uma organização
  - ➔Sem controle de acesso
- Servidores de arquivos
  - ➔Aplicação incorreta de correções (patches)
- Dados dos alunos
  - ➔Terceirizados não averiguados
- Equipamentos de produção
  - ➔Controles fracos de acesso físicos

Identificação de Riscos

- Conhecimento do Ambiente
  - ➔Identificar, examinar e compreender como a informação é processada, armazenada e transmitida
  - ➔Iniciar um programa detalhado de gerenciamento de riscos
- Conhecimento do inimigo
  - ➔Identificar, examinar e compreender as ameaças
  - ➔Gestores devem estar preparados para identificar as ameaças que oferecem riscos para a organização e a segurança dos seus

Identificação de Riscos

- Estimativa de Riscos
  - ➔Passo 1: Caracterização do sistema
    - ➔O que há para gerenciar?
  - ➔Passo 2: Identificação das ameaças
    - ➔Quais fontes de ameaças devem ser consideradas?
  - ➔Passo 3: Identificação de vulnerabilidades
    - ➔Quais falhas/fraquezas podem ser exploradas?
  - ➔Passo 4: Análise de controles
    - ➔Quais são os controles atuais e planejados?

Identificação de Riscos

- Estimativa de Riscos
  - Passo 5: Determinação das possibilidades
    - Alta, Média e Baixa
  - Passo 6: Análise de Impacto
    - O que a exploração da vulnerabilidade pode resultar?
  - Passo 7: Determinação dos riscos
    - Possibilidade x Impacto
  - Passo 8: Recomendações de controles
  - Passo 9: Documentação

Políticas de Segurança da Informação

Tipos de políticas

1. Programa de Política (organizacional)
   - ➔ Diretrizes da diretoria para criar um "programa" de segurança, estabelecer os seus objetivos e atribuir responsabilidades
2. Políticas de sistemas
   - ➔ Regras de segurança específicas para proteger sistemas (redes, máquinas, software) específicos

Implementação de Políticas

- Padrões
  - ➔Uniformidade de uso de tecnologias, parâmetros ou procedimentos, para beneficiar a organização
    - ➔Ex: Uso de Windows 2000 (mesmo existindo XP)
- Diretrizes
  - ➔Em alguns casos, a aplicação de padrões não é possível, conveniente ou acessível (custos)
    - ➔Ex: auxílio no desenvolvimento de procedimentos
- Procedimentos
  - ➔Passos detalhados para serem seguidos pelos funcionários
    - ➔ Ex: Cuidados na criação de contas de e-mail

Política (componentes)

- Objetivo
  - ➔Por que a política?
- Escopo
  - ➔Toda a organização ou parte dela?
- Responsabilidades
  - ➔Quem são as pessoas? Estrutura formal?
- Conformidade
  - ➔Como fiscalizar”?
  - ➔O que acontece para quem não cumprir?
    - ➔Intencional, não-intencional (falta de treinamento?)

Exemplo: SANS Institute para roteador

- Objetivo
  - Este documento descreve uma configuração mínima de segurança para todos os roteadores e switches conectados na rede de produção da <organização>
- Escopo
  - Todos os roteadores e switches conectados na rede de produção da <organização> são afetados.
  - Roteadores em laboratórios internos/seguros são excluídos
  - Roteadores dentro da DMZ devem seguir

Exemplo: SANS Institute para roteador

- Política: padrões de configuração
  1. Contas locais não devem ser configuradas nos roteadores. Roteadores devem usar TACACS+ (AAA) para todas as autenticações de usuários
  2. A senha de “enable” deve ser criptografada
  3. Deve ser desabilitado
     - Broadcast IP direcionado (sub-redes que o host não está)
     - Recepção de pacotes com endereços inválidos (ex: RFC1918)
     - Serviços “pequenos” TCP e UDP (echo, chargen, daytime, discard)
     - Roteamento pela fonte (source routing)
     - Serviços web rodando no roteador
  4. Não usar comunidade SNMP public (criar padrões)
  5. Regras de acesso devem ser definidas pela necessidade
  6. ...

Vulnerabilidades

Terminologia

- RFC 2828 – Glossário de segurança da Internet
  - ➔Uma falha ou fraqueza em um sistema
  - ➔Que pode ocorrer
    - ➔No projeto
    - ➔Na implementação
    - ➔Na operação ou gerenciamento
  - ➔Que pode ser explorada para violar a política de segurança do sistema
- Livro do Nessus
  - ➔Erro de programação ou configuração errada que pode permitir que um intruso tenha acesso não autorizado a algum ativo

Tipos de Vulnerabilidades

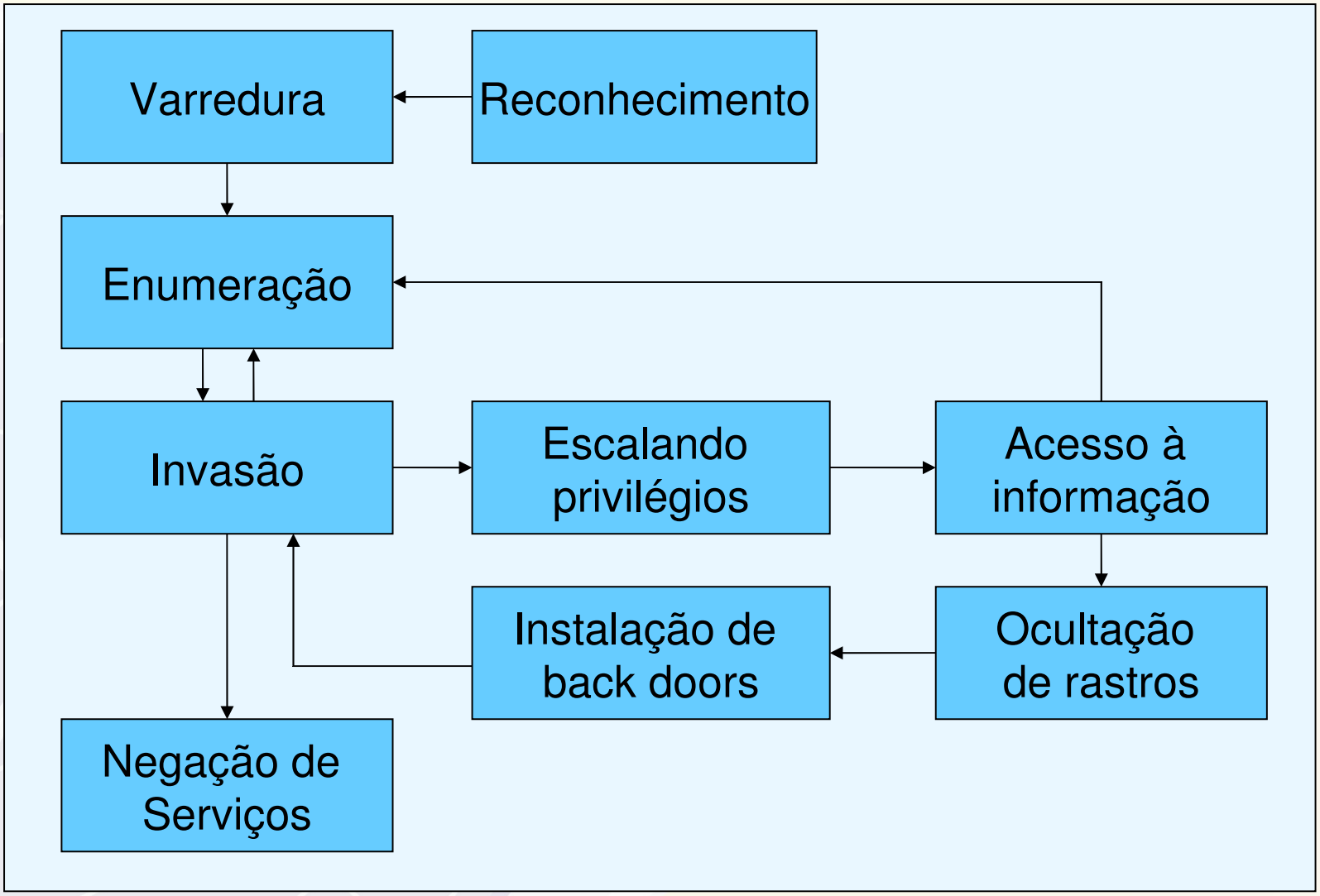
- Não existe ainda consenso sobre classificação e/ou taxonomia para vulnerabilidades
  - ➔Por serviço afetado
  - ➔Por gravidade
  - ➔Por sistema operacional alvo
- Classificação por impacto potencial (Nessus)
  - ➔Vulnerabilidades Críticas
  - ➔Vazamento de informações
  - ➔Negação de serviços

Anatomia de um ataque

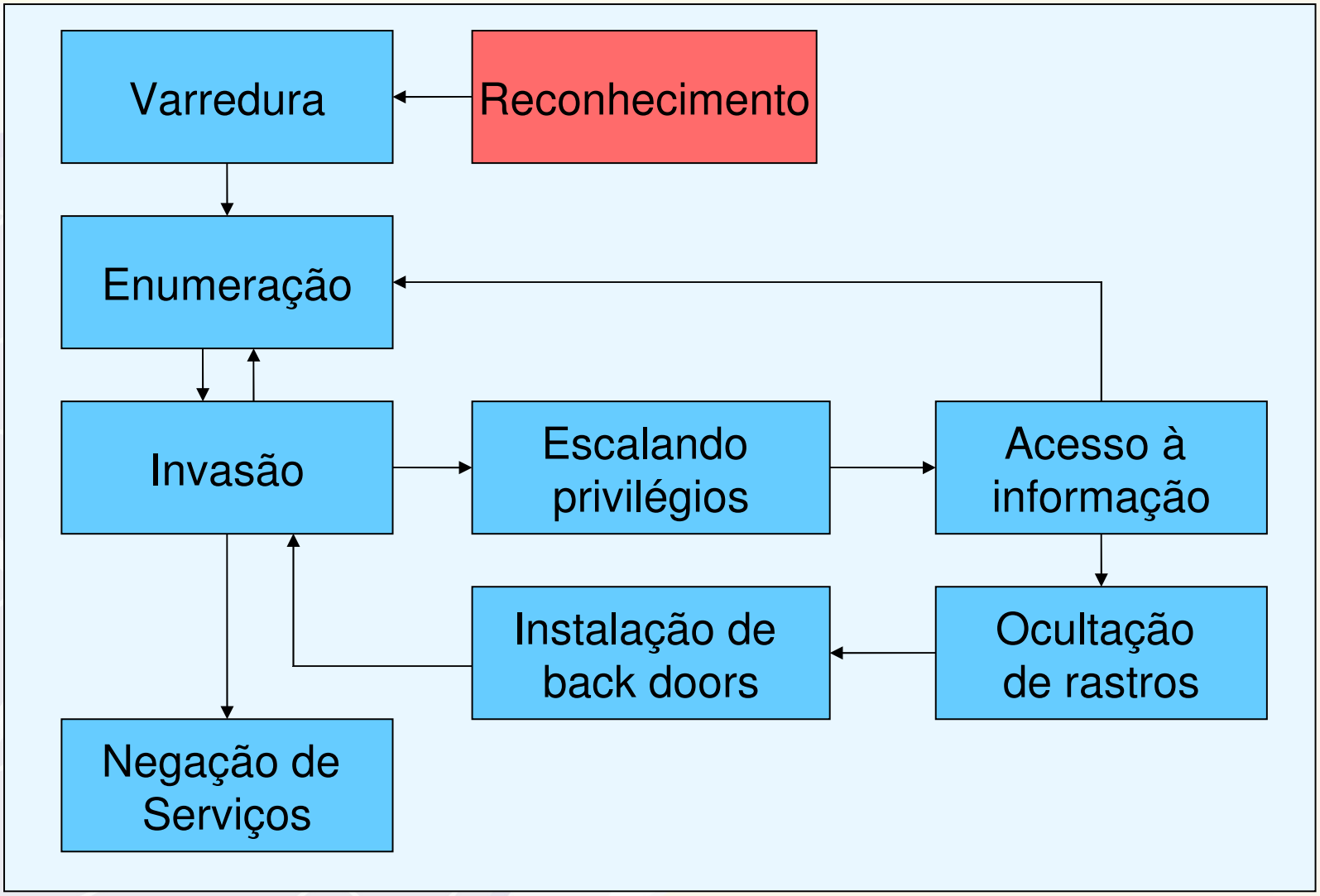
Etapas de um Ataque

1. Footprinting (reconhecimento)
2. Scanning (varredura)
3. Enumeration (enumeração)
4. Ganhando acesso (invasão)
5. Escalada de privilégios
6. Acesso à informação
7. Ocultação de rastros
8. Instalação de Back doors (portas de entrada)
9. Denial of Service (negação de serviço)

Anatomia de um ataque



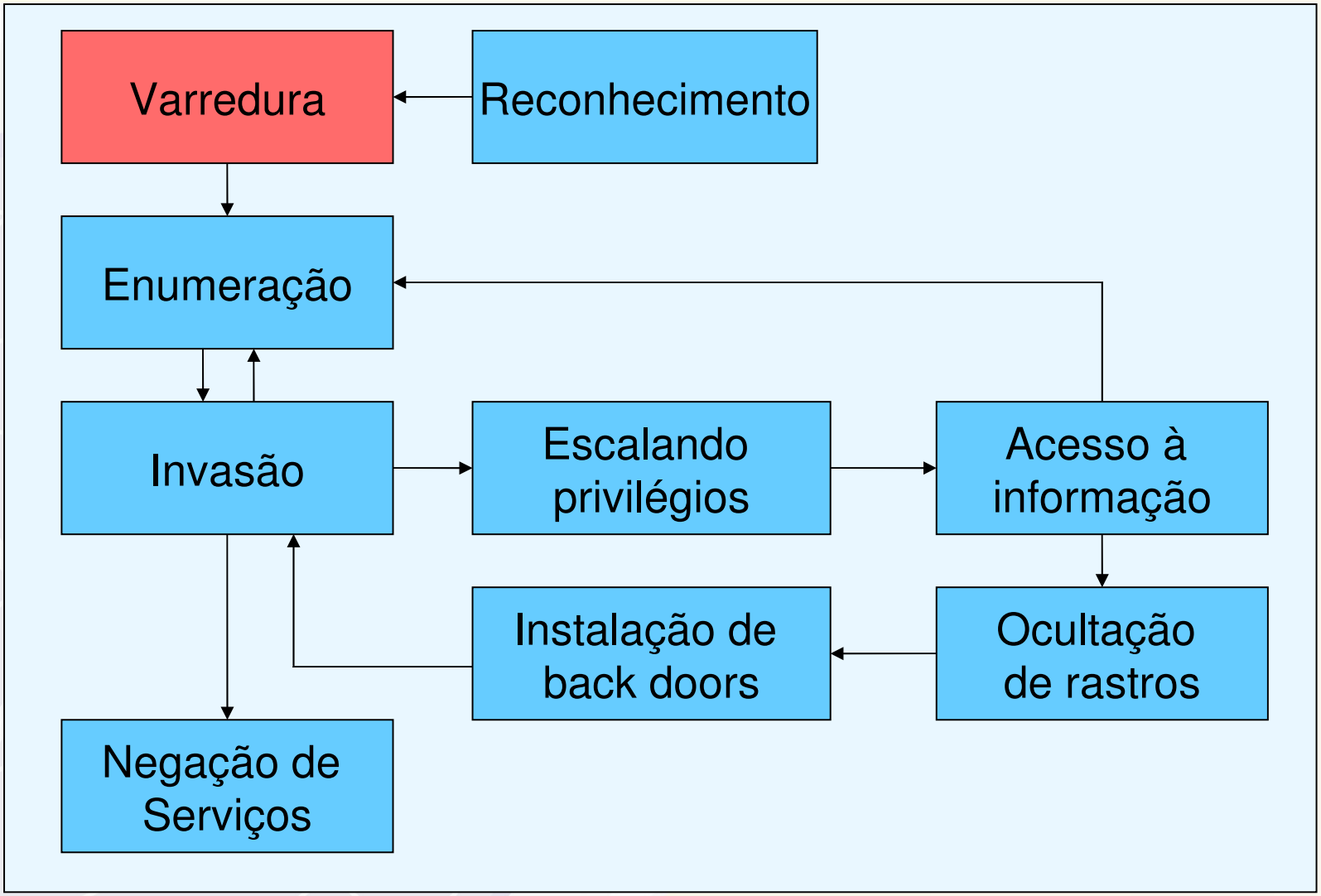
Anatomia de um ataque



1. Footprinting (reconhecimento)

- Informações básicas podem indicar a postura e a política de segurança da empresa
- Coleta de informações essenciais para o ataque
  - ➔ Nomes de máquinas, nomes de login, faixas de IP, nomes de domínios, protocolos, sistemas de detecção de intrusão
- São usadas ferramentas comuns da rede
- Engenharia Social
  - ➔ Qual o e-mail de fulano?
  - ➔ Aqui é Cicrano. Poderia mudar minha senha?
  - ➔ Qual o número IP do servidor SSH? e o DNS?

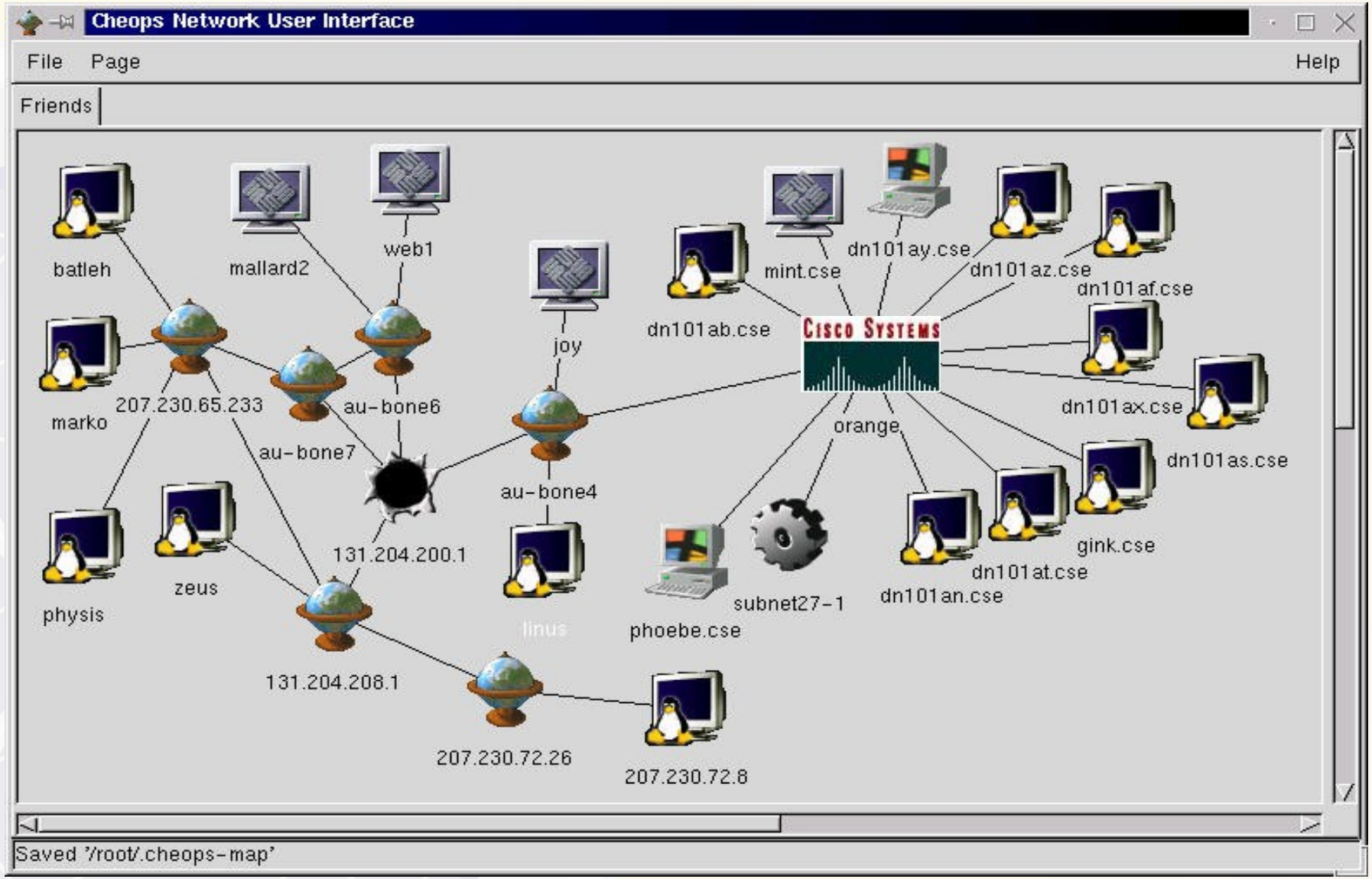
Anatomia de um ataque



2. Scanning (varredura ou mapeamento)

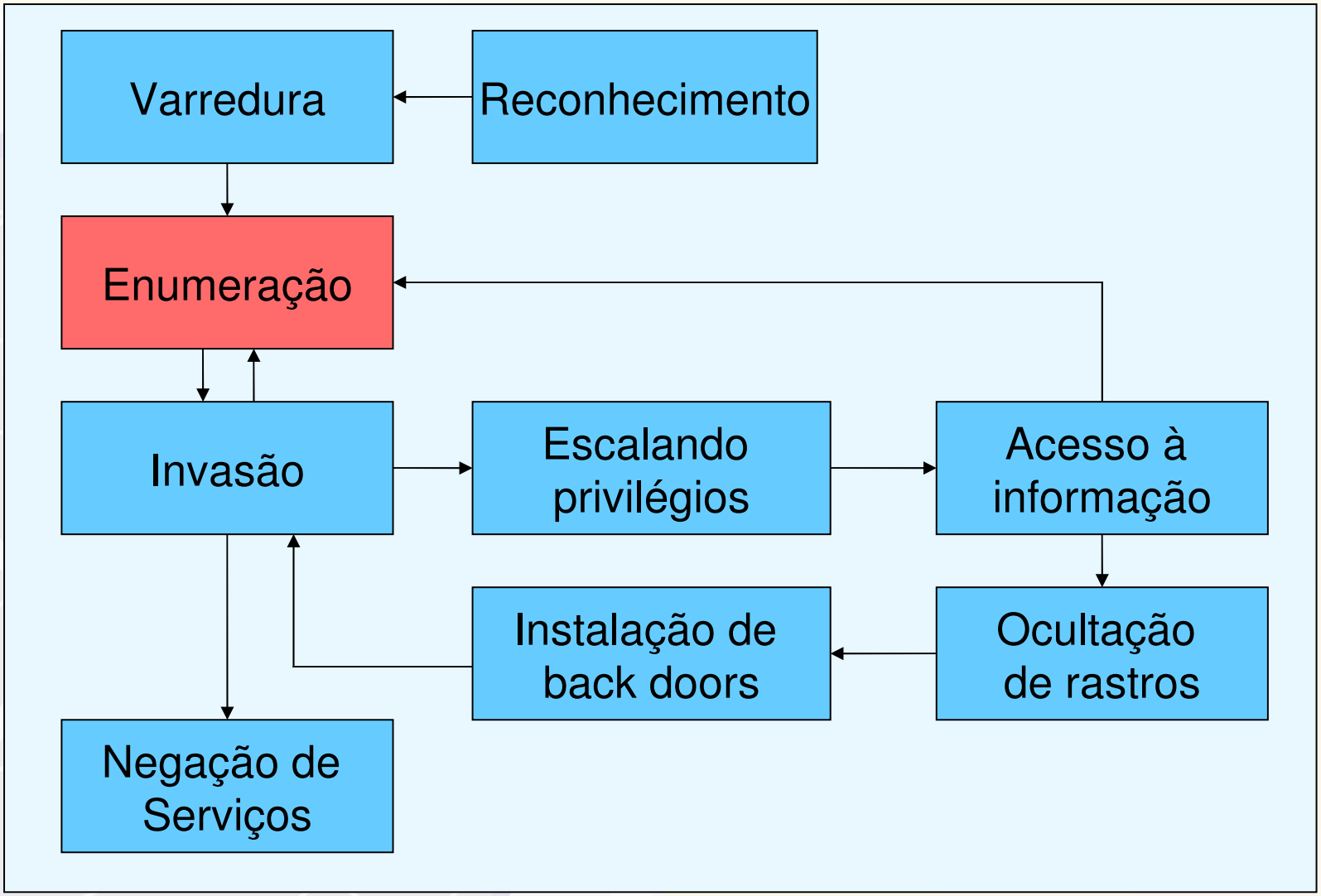
- De posse das informações coletadas, determinar
  - ➔Quais sistemas estão ativos e alcançáveis
  - ➔Portas de entrada ativas em cada sistema
- Ferramentas
  - ➔Nmap, system banners, informações via SNMP
- Descoberta da Topologia
  - ➔Automated discovery tools: cheops, ntop, ...
  - ➔Comandos usuais: ping, traceroute, nslookup
- Detecção de Sistema Operacional
  - ➔Técnicas de fingerprint (nmap)
- Busca de senhas contidas em pacotes (sniffing)
  - ➔Muitas das ferramentas são as mesmas usadas para gerenciamento e administração da rede

Mapeamento de rede



Tela do Cheops (http://cheops-ng.sourceforge.net)

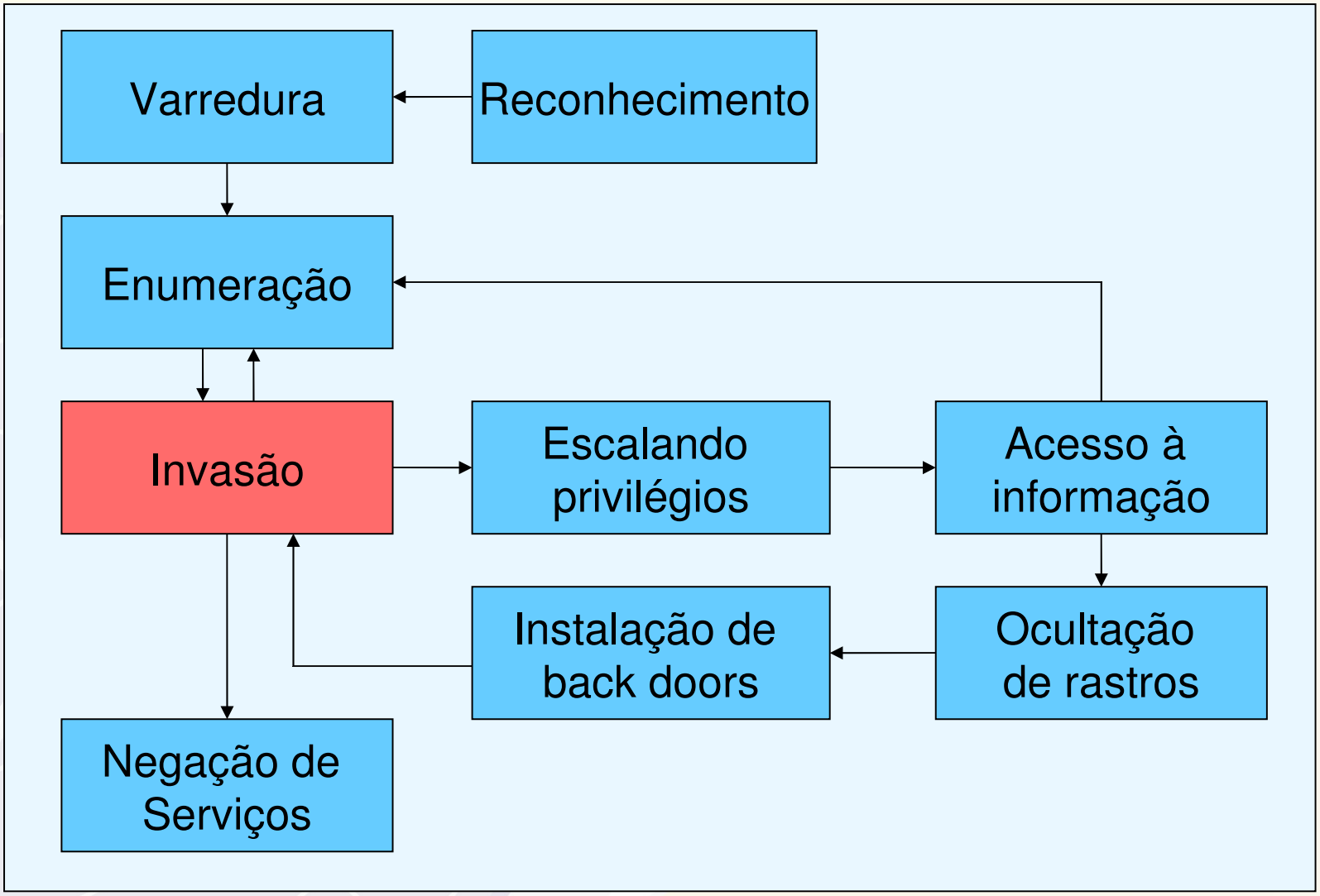
Anatomia de um ataque



3. Enumeration (enumeração)

- Coleta de dados intrusiva
  - ➔Consultas diretas ao sistema
  - ➔Está conectado ao sistema e pode ser notado
- Identificação de logins válidos
- Banners identificam versões de HTTP, FTP servers
- Identificação de recursos da rede
  - ➔Compartilhamentos (windows) - Comandos net view, nbstat
  - ➔Exported filesystems (unix) - Comando showmount
- Identificação de Vulnerabilidades comuns
  - ➔Nessus, SAINT, SATAN, SARA, TARA, ...
- Identificação de permissões

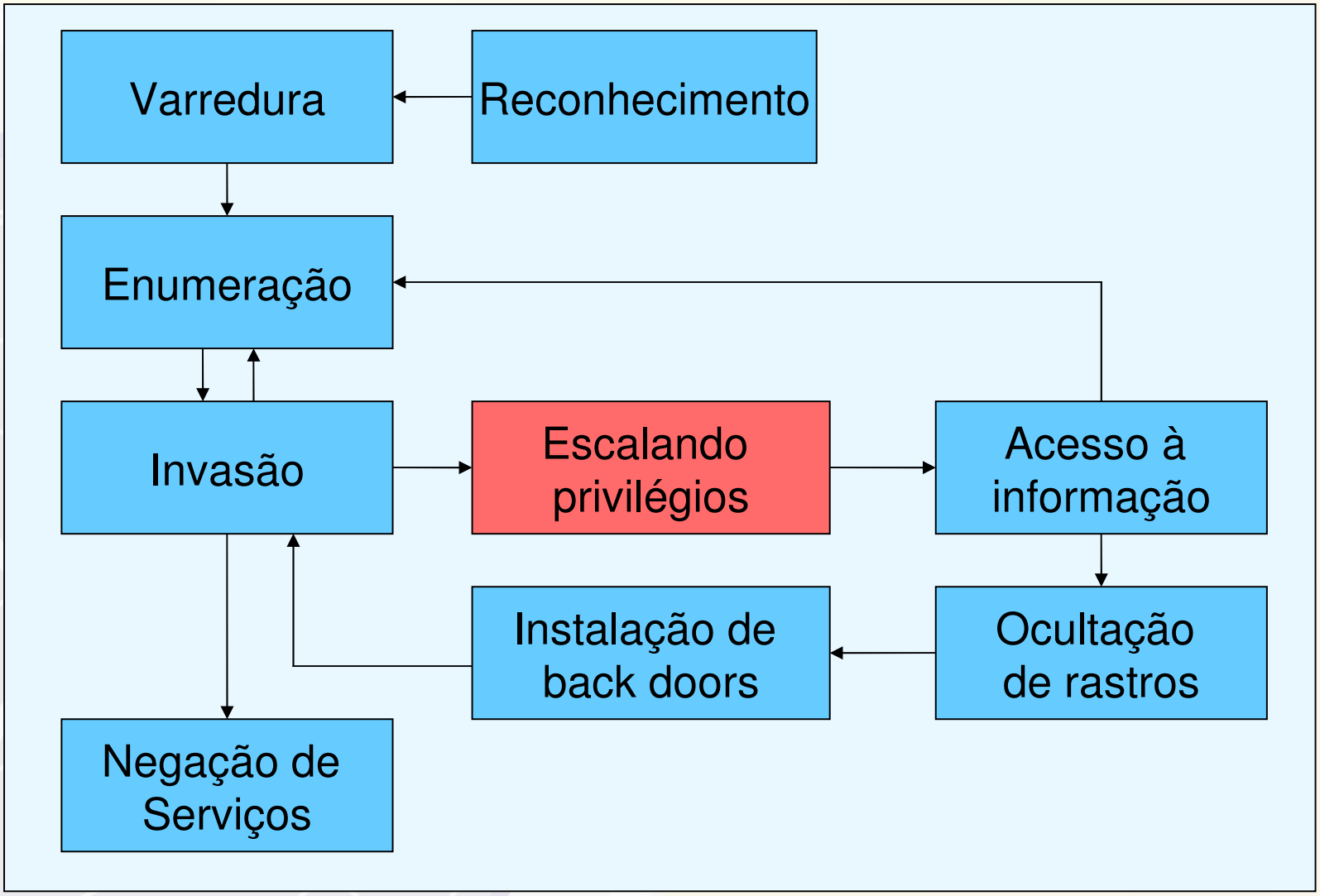
Anatomia de um ataque



4. Ganhando acesso (invasão)

- Informações coletadas norteiam a estratégia de ataque
- Invasores tem uma “base” de vulnerabilidades
  - ➔ Bugs de cada SO, kernel, serviço, aplicativo – por versão
  - ➔ Tentam encontrar sistemas com falhas conhecidas
- Busca privilégio de usuário comum (pelo menos)
- Técnicas
  - ➔ Password sniffing, password crackers, password guessing
  - ➔ Session hijacking (sequestro de sessão)
  - ➔ Ferramentas para bugs conhecidos (buffer overflow)
- Hackers constróem suas próprias ferramentas

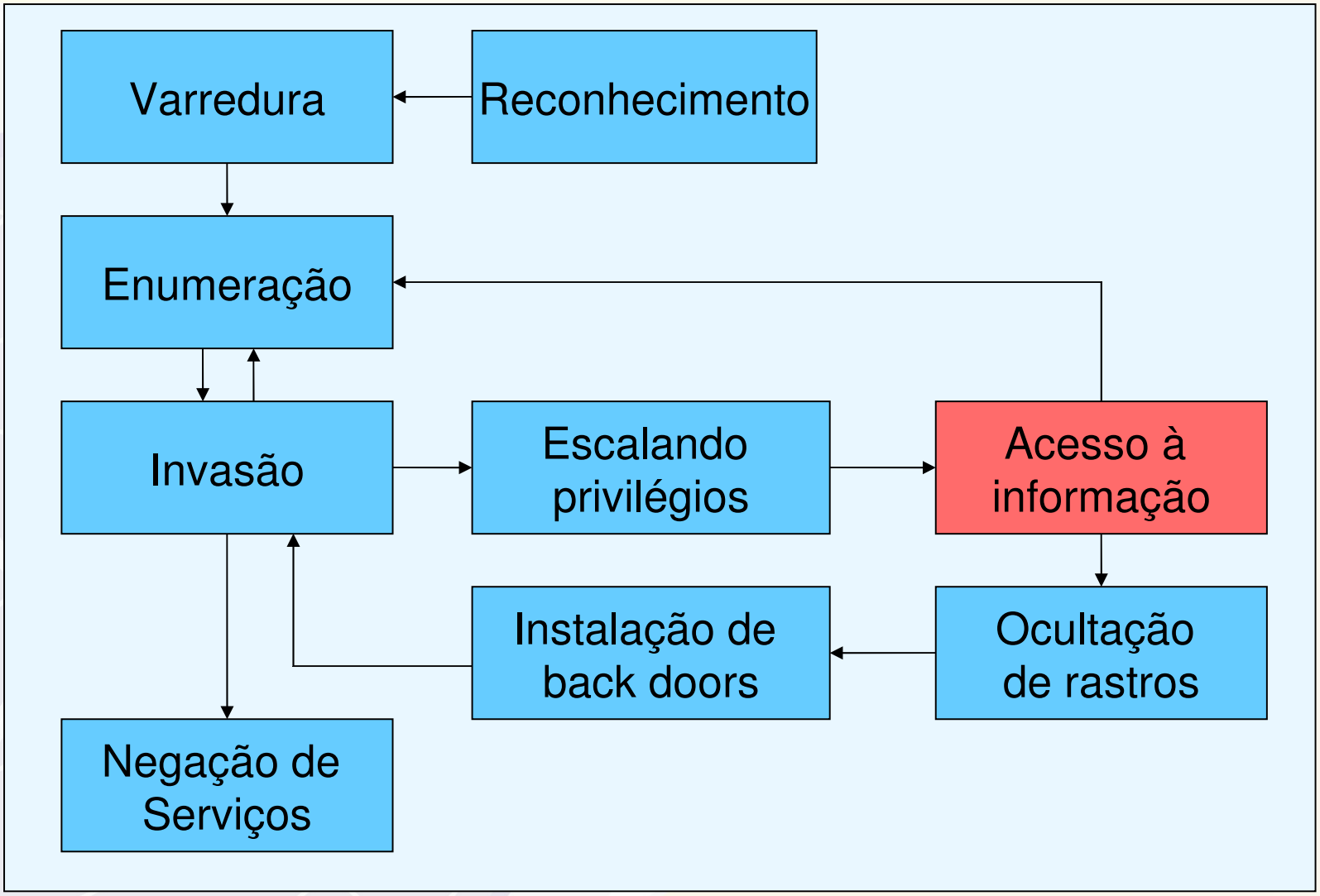
Anatomia de um ataque



5. Escalada de privilégios

- Uma vez com acesso comum, busca acesso completo ao sistema (administrator, root)
- Ferramentas específicas para bugs conhecidos
  - ➔"Exploits"
- Técnicas
  - ➔Password sniffing, password crackers, password guessing
  - ➔Session hijacking (sequestro de sessão)
  - ➔Replay attacks
  - ➔Buffer overflow
  - ➔Trojans

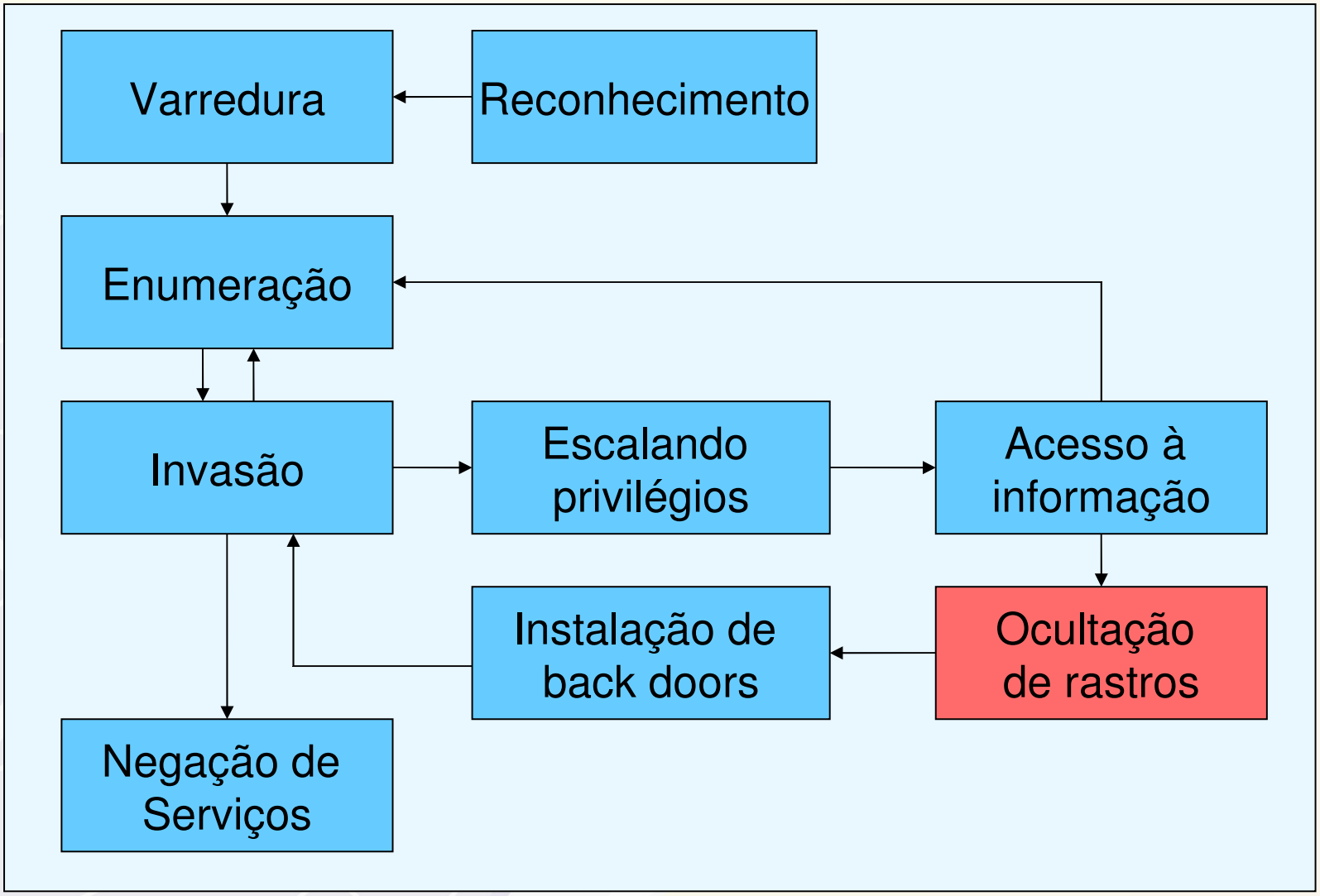
Anatomia de um ataque



6. Acesso a informação

- Alguns conceitos relacionados à “informação”
  - ➔Confidencialidade – trata do acesso autorizado
  - ➔Integridade – trata da alteração autorizada
  - ➔Autenticidade – trata da garantia da autoria da informação
  - ➔Disponibilidade – disponível quando desejada, sem demora excessiva (com autorização)
  - ➔Auditoria – trata do registro do acesso
- Invasor pode atuar contra todos os

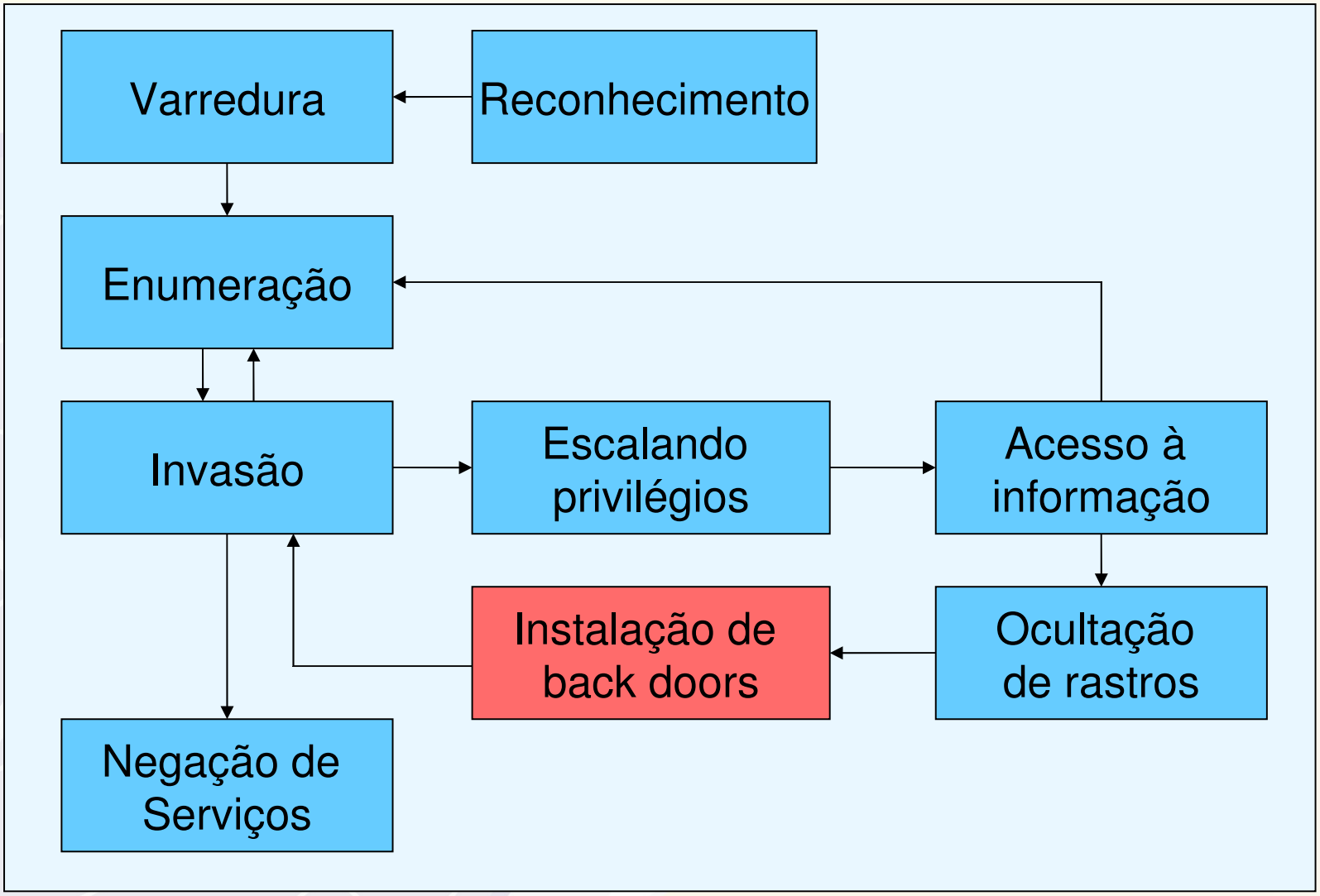
Anatomia de um ataque



7. Ocultação de rastros

- Invasor usa tenta evitar detecção da presença
- Usa ferramentas do sistema para desabilitar auditoria
- Toma cuidados para não deixar “buracos” nos logs
  - ➔excessivo tempo de inatividade vai denuciar um ataque
- Existem ferramentas para remoção seletiva do Event Log
- Esconde arquivos “plantados” (back doors)

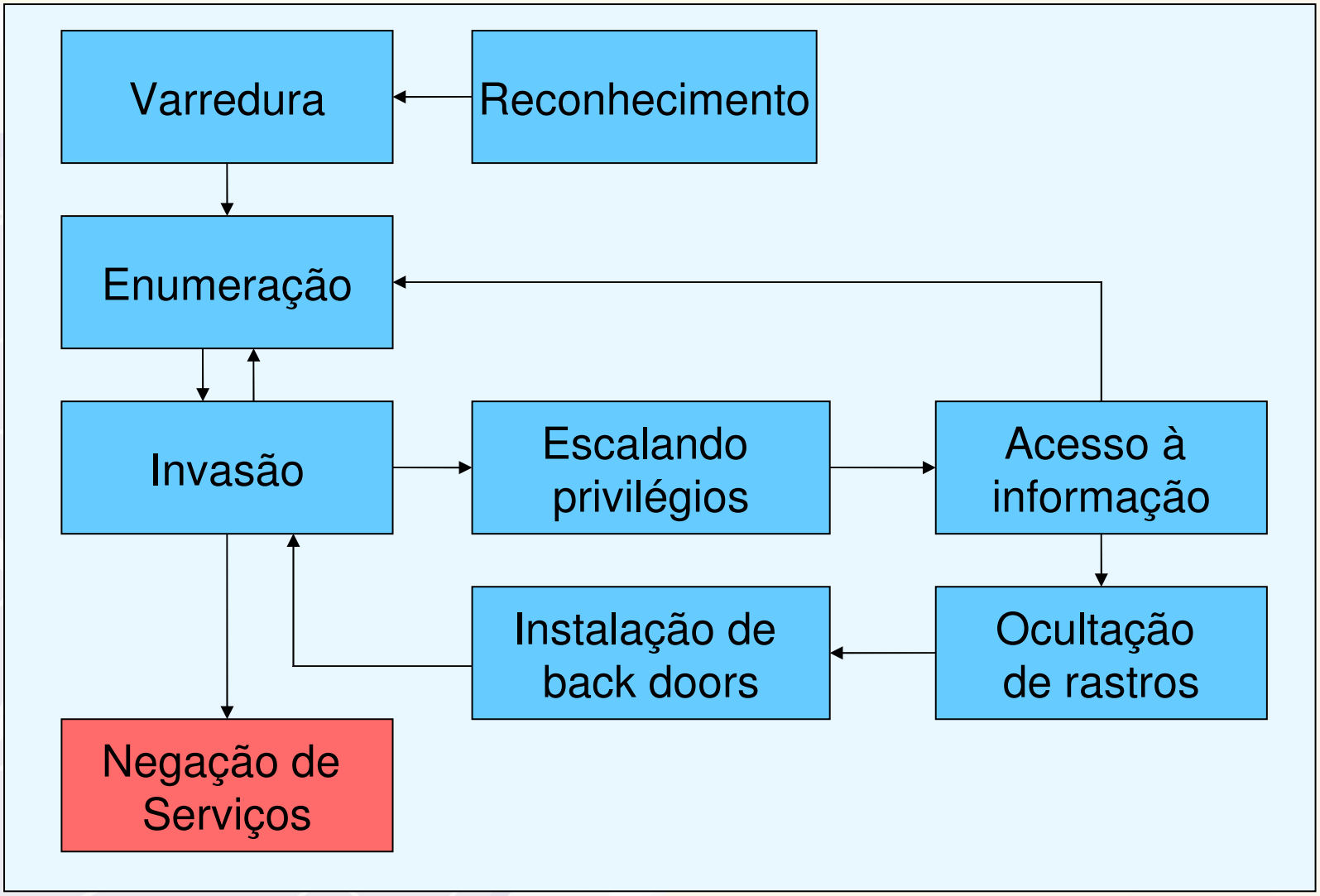
Anatomia de um ataque



8. Instalação de Back doors

- Objetivo é a manutenção do acesso
  - ➔Rootkits – ferramentas ativas, mas escondidas
  - ➔Trojan horses – programas falsificados
  - ➔Back doors – acesso/controle remoto sem autenticação
- Trojans podem mandar informação para invasor
  - ➔Captura teclado
  - ➔Manda um e-mail com a senha
- Rootkits se confundem com o sistema
  - ➔Comandos modificados para não revelar o invasor
- Back doors
  - ➔Sistemas cliente/servidor
  - ➔Cliente na máquina invasora controlando Servidor na máquina remota
  - ➔Não aparecem na "Task List" do Windows NT/2k

Anatomia de um ataque



9. Denial of Service (negação de serviço)

- Ataques com objetivo de bloquear serviços, através de:
  - ➔Consumo de banda de rede
  - ➔Esgotamento de recursos
  - ➔Exploração de falhas de programação (ex: ping da morte)
  - ➔Sabotagem de Roteamento
  - ➔Sabotagem no DNS
- DDoS ➔Distributed Denial of Service
  - ➔Ataques coordenados de múltiplas fontes

Trabalho

Atividades