

Segurança de Computadores e Redes

Universidade Estadual Paulista Júlio de Mesquita Filho

Prof. Dr. Kelton Augusto Pontara da Costa

Aula 1

Sumário

- 1 Abordagem da aula 1
 - Introdução à segurança
 - Ameaças à segurança
 - Etapas de um ataque
 - Tipos de ataques
 - Classificação de ataques

- A dependência da sociedade pela infraestrutura computacional acarreta a preocupação com a segurança envolvida;
- Dessa forma, várias técnicas vêm sendo aplicadas e aprimoradas no intuito de reduzir os riscos com vazamentos, erros, fraudes, sabotagens, uso indevido, roubo de informações e diversos outros problemas;
- Apesar de vários esforços no sentido de prover segurança em ambientes computacionais, o número, a variedade e complexidade dos incidentes relacionados à segurança tem crescido significativamente.

- Os sistemas computacionais estão constantemente sujeitos a vários tipos de ameaças, sejam elas acidentais, maliciosas, internas ou externas, que podem desencadear intrusões explorando vulnerabilidades do sistema.
- As explorações dessas vulnerabilidades são motivadas por objetivos específicos que podem variar desde simples atos de vandalismo até sofisticadas técnicas de espionagem industrial.

- Em um relatório técnico gerado pelo Sandia National Laboratories é discutida uma taxonomia que se baseia em ações para classificar ameaças à segurança. Tal aplicação aborda sobre informações que estão em trânsito e que podem ser visualizadas pela figura a seguir:

■ Taxonomia baseada em ações

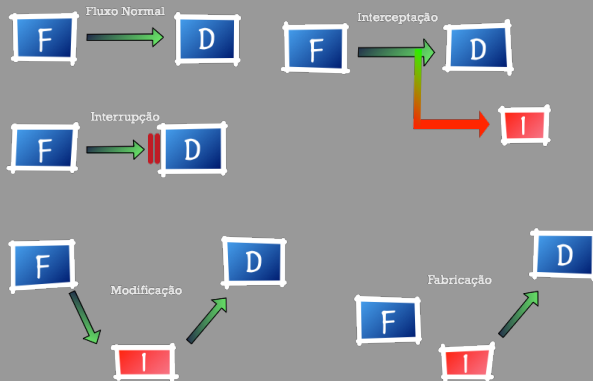


Figura 1: (F)onte de informação; (D)estino da informação; (I)ntroso

INTERRUPÇÃO: as informações em trânsito são interrompidas, impossibilitando que as mesmas cheguem até seu destino e prejudicando a questão da disponibilidade dos recursos.

INTERCEPTAÇÃO: as informações são interceptadas durante a transmissão, comprometendo a confidencialidade da mensagem.

MODIFICAÇÃO: as informações são interceptadas e alteradas durante a transmissão, afetando não só a confidencialidade como a integridade da mensagem.

FABRICAÇÃO: trata-se da inserção de informações em determinada comunicação, comprometendo a autenticidade das informações recebidas.

- A preocupação com a segurança em redes de computadores ocasionou o surgimento de várias técnicas voltadas à prevenção de ataques;
- Não há possibilidade de prevenção total para todos os tipos de quebras de segurança, pois novas vulnerabilidades são descobertas constantemente;
- Possibilidade de identificação de tentativas ou violações e gerar respostas para minimizar danos;

- A detecção é realizada através de conjuntos de hardware e software que cooperam de forma a analisar e identificar eventos considerados ataques ou atividades maliciosas;
- Grande parte das abordagens de D.I.¹ ainda são realizadas através da comparação das atividades correntes com ações esperadas de um intruso;

¹D.I. - detecção de intrusão

- Os SDIs² possuem componentes que desempenham funções específicas como sensores, analisadores de eventos e unidades de respostas, que juntos oferecem a capacidade de detectar, analisar e responder aos eventos.

²S.D.I. - sistemas de detecção de intrusão

- Para um sistema atacado com sucesso, observa-se a presença de atividades sucessivas que caracterizam etapas do ataque.

- Ataques caracterizados por busca de informações sobre recursos e vulnerabilidades no host (investigações de reconhecimento);
- Varreduras devem ser detectadas para evitar tal exploração e posterior efetivação de uma intrusão;

- EXEMPLO DE TÉCNICAS DE RECONHECIMENTO:
- envio de pacotes mal formados (crafted packets) com estímulo de respostas;
- permite identificar o S.O.³ ;
- permite definir as vulnerabilidades a serem exploradas;
- permite definir as respectivas ferramentas a serem utilizadas;

³S.O. - sistema operacional

- EXEMPLO DE TÉCNICAS DE RECONHECIMENTO: (cont.)
- após explorar o atacante passa a preocupar-se em eliminar indícios de sua presença ou atividades no sistema;
- garante acesso futuro ao host;
- coordena utilização das ferramentas intrusivas implantadas.

- EXEMPLO DE TÉCNICAS DE RECONHECIMENTO: (cont.)
- para isso manipula logs e registros de atividades;
- implanta backdoors;
- instala rootkit's⁴.

⁴Rootkit - conjunto de softwares para substituir aplicativos do sistema operacional, podem omitir processos, conexões, arquivos, logs, etc.

Um ataque é uma ação maliciosa que viola as políticas de segurança⁵ e que compromete a integridade ou a disponibilidade dos recursos em um sistema.

⁵ABNT NBR ISO/IEC 17799; ABNT NBR ISO/IEC 27002

- O princípio básico é a exploração das vulnerabilidades encontradas nas investigações realizadas (nos sistemas e/ou protocolos);
- É caracterizado efetivamente como invasão caso ocasione indisponibilidade dos serviços.

Os ataques podem ser classificados de acordo com as formas que atuam sobre os sistemas:

i. Denial of Service - caracterizada pelo uso anormal do sistema de forma a exaurir os recursos disponíveis.

ii. Malicious Use - trata da execução de atividade maliciosa fazendo uso de privilégios concedidos e normalmente está relacionado a usuários legítimos do sistema.

iii. Attempted Breack-Inn⁶ - executadas através de ações atípicas e que infringem as regras de segurança do sistema.

⁶Attempted Breack-Inn - tentativas de invasão

iv. Masquerade Attack⁷ - tentativas de invasão executadas de forma a se passarem por atividades de usuários válidos ou por máquinas confiáveis do domínio.

⁷Masquerade Attack - tentativas de personificação

v. Penetration⁸ - geralmente são detectados por monitoração de padrões específicos das atividades ocorridas e reportadas pelo sistema.

⁸Penetration - invasão no controle de segurança

vi. Leakage⁹ - ataques são detectados pelo uso anormal de recursos de entrada e saída dos sistemas e variações no padrão de utilização dos mesmos.

⁹Leakage - vazamento

vii. Scanning¹⁰ - mais comuns dos ataques, consiste no envio de diversos tipos de pacotes no intuito de se conhecer mais sobre o nó alvo ou a rede em questão.

¹⁰Scanning - varredura