Marisangila Alves, MSc
marisangila.alves@udesc.br
marisangila.com.br

UDESC
UNIVERSIDADE DO ESTADO DE SANTA CATARINA
JOINVILLE
CENTRO DE CIÊNCIAS TECNOLÓGICAS

UDESC
Universidade do Estado de Santa Catarina

2025/2

Segurança da Informação

Terminologias

Sumário

Terminologias

Figura 1: Terminologias (Internet Engineering Task Force (IETF), 2000).

Ativos

Ativos I

- Dados contidos em um sistema de informação; serviço provido por um sistema; capacidade do sistema, como poder de processamento ou largura de banda de comunicação; item de equipamento do sistema; instalação que abrigue operações e equipamentos de sistema.
- *Hardware*;
- *Software*;
- Dados;
- Instalações e redes de comunicações.

As **Vulnerabilidades** desses ativos podem ser corrompidos, vazados ou se tornar indisponíveis.

Ameaça

Ameaça I

- Um **potencial** para violação de segurança, que existe quando há circunstância, capacidade, ação ou evento que poderia infringir a segurança e causar dano.
- Isto é, uma ameaça é um perigo possível que poderia explorar uma vulnerabilidade.

Ataque I

- Tentativa de violação da segurança do sistema que deriva de ameaça inteligente, isto é, um ato inteligente que é uma tentativa deliberada para burlar serviços de segurança e violar a política de segurança de um sistema.

Um ataque é uma ameaça que é executada. Tentativa de descobrir

ou fazer uso de informações advindas do sistema que não afeta ativos do sistema.

Ataque Passivo

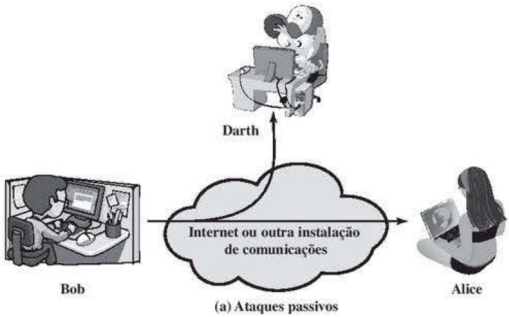


Figura 2: Ataque Passivo (Stallings, 2020).

Ataque Ativo

Tentativa de alterar ativos de sistemas ou afetar sua operação.

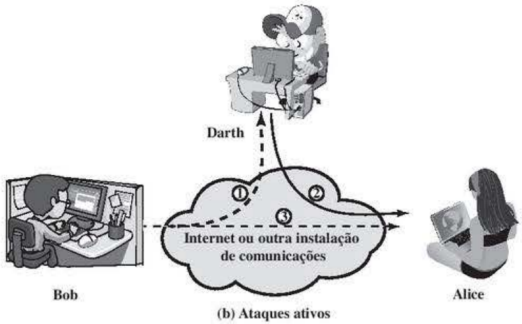


Figura 3: Ataque Ativo (Stallings, 2020).

Ataque IV

Origem de Ataque

Ataque Interno:

- Iniciado por uma entidade que está dentro do perímetro de segurança (um "usuário interno legítimo" ou *"insider"*)
- O insider está autorizado a acessar ativos de sistema, mas os usa de modo não aprovado por quem concedeu a autorização.

Ataque Externo:

- Iniciado de fora do perímetro por um usuário não autorizado ou ilegítimo do sistema (um *"outsider"*).
- Na Internet, atacantes externos potenciais vão de amadores curiosos a criminosos organizados, terroristas internacionais e governos hostis

Sniffing (Captura de Tráfego)

- Interceptação passiva (ou ativa) do tráfego de rede para capturar informações (cleartext, sessões, tokens).
  - Ataque passivo em rede local ou ativa (ARP spoofing / MITM) para redirecionar tráfego.
- **Mitigações:**
  - Uso obrigatório de criptografia de transporte (TLS) e de ponta a ponta onde aplicável.
  - Segmentação de rede, switches com segurança de porta, uso de VPNs para redes públicas.
  - Deteção de ARP spoofing (IDS/IPS), monitoramento de ARP e inspeção de certificados.
  - Uso de HSTS: forçar o uso do protocolo HTTPS em vez de HTTP.

- Engenharia social que induz usuários a revelar credenciais ou executar ações (link malicioso, anexo).
  - Ataque via e-mail/SMS/mensagem → link para site falso ou anexo com malware → captura de credenciais.
- **Exemplos:** whaling (diretoria), vishing (voz), smishing (SMS).
- **Sinais / Indicadores:** URLs suspeitas, erros de grafia, remetente externo não esperado, pedido urgente de ação.
- **Mitigações:**
  - Autenticação multifator (MFA) obrigatória.
  - Filtro de e-mail e anexos.
  - Treinamento contínuo com funcionários.

Brute Force (Força Bruta)

- Tentativa automatizada e exaustiva de adivinhar credenciais (senha/Chave).
- **Como funciona:**
  - Script/robot tenta combinações (dicionário, ataques por força bruta pura, credenciais vazadas).
- **Mitigações:**
  - Bloqueio temporário após X tentativas, rate limiting e CAPTCHA.
  - Políticas de senha fortes, MFA e uso de gestores de senha.
  - Monitoramento e bloqueio de IPs maliciosos; uso de WAF para aplicações web.

OWASP

OWASP I

- **OWASP** significa *Open Web Application Security Project*.
- Fundação sem fins lucrativos dedicada a melhorar a segurança de software.
- Produz guias, ferramentas, metodologias e projetos de código aberto para auxiliar desenvolvedores e empresas.
- Amplamente reconhecida pelo **OWASP Top 10**, lista dos dez principais riscos de segurança em aplicações web 🔗 OWASP Top 10 - 2021.
- Oferece base de conhecimento sobre táticas e técnicas usadas por atacantes, em complemento ao 🔗 MITRE ATT&CK.

OWASP Top 10 (2021) - Parte 1 I

#	Vulnerabilidade	Exemplo prático	Mitigação
A01	Broken Access Control	Usuário comum acessa `/admin/painel` mudando a URL	Verificação de permissões no servidor; RBAC/ABAC
A02	Cryptographic Failures	Senhas salvas em texto puro no banco	Hashing seguro (bcrypt, Argon2), TLS bem configurado
A03	Injection	Login: `' OR '1'='1` $\rightarrow$ acesso sem senha	Queries parametrizadas (prepared statements), ORM seguro
A04	Insecure Design	Carrinho de compras aceita preço enviado pelo cliente	Validar lógica de negócio no servidor; modelagem de ameaças
A05	Security Misconfiguration	Servidor com página de debug ativa (`/phpinfo.php`)	Desativar debug em produção, hardening de configs

#	Vulnerabilidade	Exemplo prático	Mitigação
A06	Vulnerable/Outdated Components	Uso de jQuery 1.x vulnerável a XSS	Atualizar dependências; scanners de vulnerabilidade
A07	Identification/Authentication Failures	Login sem limite de tentativas → brute force	Bloqueio após falhas, MFA, tokens seguros
A08	Software/Data Integrity Failures	Atualização via .zip sem checar assinatura	Verificação de integridade, CI/CD confiável
A09	Logging/Monitoring Failures	Ataque ocorre mas nenhum log é gerado	Configuração de logs, SIEM, alertas de eventos suspeitos
A10	Server-Side Request Forgery (SSRF)	App acessa `http://127.0.0.1/admin` via input do usuário	Validar entradas, bloquear IPs internos, allowlist de domínios

Atacante

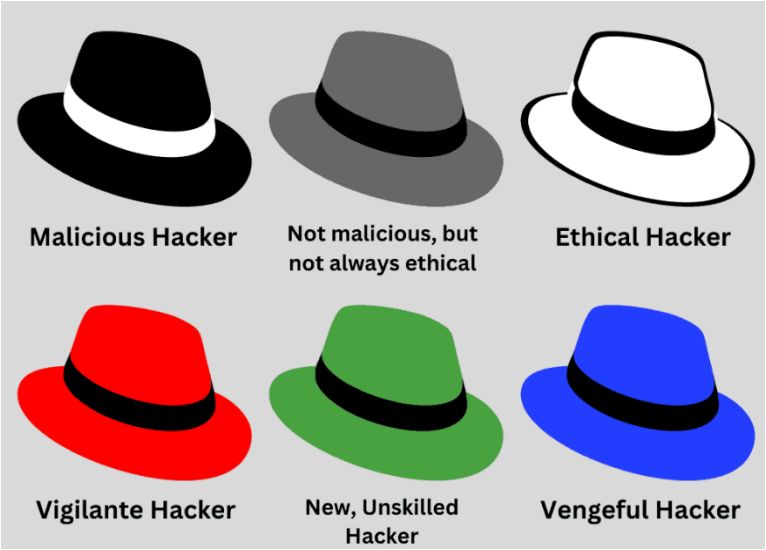
> *O hacker criminoso condenado Kevin Mitnick testemunhou perante o Congresso. Ele disse que a engenharia social é uma grande vulnerabilidade na segurança: ele normalmente cnosegue apanhar senhas e outros segredos simplesmente fingindo ser outra pessoa ou perguntando.*
>
> (SCHNEIER, 2001)

Adversário ou Atacante I

- Entidade que ataca um sistema ou é uma ameaça para ele.

O agente que executa o ataque é denominado atacante ou agente fonte de ameaça.

Tipos de Atacante I



Tipos de Atacante II

- **Chapéu Preto (Black Hat):** Crackers mal-intencionados que invadem sistemas para roubar dados ou causar danos.
- **Chapéu Branco (White Hat):** Hackers éticos que testam sistemas para melhorar a segurança.
- **Chapéu Cinza (Gray Hat):** Crackers que agem entre o ético e o malicioso, muitas vezes sem permissão clara.
- **Chapéu Vermelho (Red Hat):** Crackers vigilantes que combatem os black hats ofensivamente.
- **Chapéu Azul (Blue Hat):** Crackers contratados para testes específicos.
- **Chapéu Verde (Green Hat):** Crackers iniciantes aprendendo e desenvolvendo suas habilidades.

Tipos de Atacante III

- **Hacker**: alguém que possui profundo conhecimento em uma determinada área, tem iniciativa, é autodidata e está sempre buscando aprender mais.
- **Cracker**: um hacker que utiliza seu conhecimento para obter vantagem própria.
- **Script Kiddie:** Usuários inexperientes que usam ferramentas prontas sem compreender profundamente.
- **Lammer**: alguém que está tentando adquirir conhecimento/experiência para se tornar um hacker ou cracker.
- **Phreaker**: um hacker de sistemas de telecomunicações.

Contramedida

- Ação, dispositivo, procedimento ou técnica que reduz uma ameaça, uma vulnerabilidade ou um ataque, eliminando-o ou prevenindo-o, minimizando o dano que ele pode causar ou descobrindo-o e relatando-o de modo a possibilitar uma ação corretiva.

- Sistema ou serviço deliberadamente vulnerável/atrativo para atrair atacantes e estudar seu comportamento.
- **Objetivos:**
  - Detectar atacantes, coletar TTPs (técnicas/táticas/procedimentos), retardar intrusão e proteger ativos reais.
- **Boas práticas:**
  - Isolamento em VLANs/segurança de rede.
  - Integração com IDS para alertas.

Política

- Conjunto de regras e práticas que especificam ou regulamentam como um sistema ou organização provê serviços de segurança para proteger ativos sensíveis e críticos de um sistema.

Risco

- Expectativa de perda de segurança expressa como a probabilidade de que uma ameaça particular explorará uma vulnerabilidade particular com resultado danoso particular.

Vulnerabilidade

Vulnerabilidade I

- Falha, defeito ou fraqueza no projeto, implementação ou operação e gerenciamento de um sistema que poderia ser explorada para violar a política de segurança do sistema.

O que é CVE?

- **CVE** significa *Common Vulnerabilities and Exposures* (Vulnerabilidades e Exposições Comuns).
- É um catálogo público que lista vulnerabilidades conhecidas em *softwares* e *hardwares*.
- Cada vulnerabilidade recebe um identificador único, como `CVE-2024-12345`.
- Criado e mantido pela **MITRE Corporation**, desde 1999.
- Objetivo: padronizar a comunicação de vulnerabilidades para facilitar correções e defesa.
- Profissionais usam o CVE para priorizar riscos e proteger sistemas.

Bases :

- 🔗 CVE Oficial - catálogo oficial mantido pela MITRE.

- Vulnerabilidade desconhecida pelo fornecedor e sem correção disponível; explorada antes de existir *patch*.
- **Como funciona:**
  - Atacante encontra/compra a falha e realiza um ataque direcionado.

> *Open-source intelligence (OSINT) é uma inteligência produzida a partir de informações publicamente disponíveis, coletadas, exploradas e disseminadas de forma oportuna para o público apropriado, com o propósito de atender a uma necessidade específica de inteligência.*
>
> OSINT

Projeto OSINT Brazuca

> *(Mell; Kent; Nusbaum, 2005) um programa que é inserido em um sistema, usualmente às escondidas, com a intenção de comprometer a confidencialidade, a integridade ou a disponibilidade dos dados, aplicações ou sistema operacional da vítima ou, possivelmente, apenas aborrecer ou perturbar a vítima.*

Adware: propaganda que é integrada ao software. Pode resultar em pop-ups de propaganda ou no redirecionamento de um navegador para um site comercial.

Kit de ataque: conjunto de ferramentas para gerar um novo malware automaticamente, usando uma variedade de mecanismos de propagação e cargas úteis fornecidos.

Auto-rooter: ferramentas maliciosas usadas por hackers para invadir remotamente novas máquinas, automatizando a obtenção de acesso privilegiado.

Backdoor (trapdoor): qualquer mecanismo que burle uma verificação de segurança normal; pode permitir acesso não autorizado a funcionalidades em um programa ou a um sistema comprometido.

Downloaders: códigos que instalam outros componentes maliciosos em uma máquina sob ataque. Normalmente são incluídos no malware inicial para depois importar um pacote maior.

Drive-by Download: ataque que usa código em um site comprometido para explorar vulnerabilidades de navegadores, atacando um sistema cliente assim que o site é visitado.

Exploits (Explorações): códigos específicos que exploram uma única vulnerabilidade ou um conjunto de vulnerabilidades para comprometer sistemas.

Flooders (cliente de DoS)

Flooders (cliente de DoS): ferramentas usadas para gerar alto volume de tráfego a fim de atacar sistemas em rede, executando ataques de negação de serviço (DoS).

Keyloggers

Keyloggers: programas que capturam as teclas digitadas em um teclado de um sistema comprometido, frequentemente usados para roubo de credenciais.

Bomba lógica: código inserido por um intruso que permanece inativo até que uma condição predefinida ocorra; então executa uma ação não autorizada.

Vírus de macro: tipo de vírus que usa código de macro ou script embutido em documentos; é ativado ao visualizar/editar o documento e se reproduz em outros documentos do mesmo tipo.

Código móvel: software (script, macro ou outra instrução portável) que pode ser distribuído sem alterações para diversas plataformas e executado com semântica idêntica.

Rootkit: conjunto de ferramentas utilizadas após o invasor obter acesso de nível root, projetadas para ocultar presença e manter controle do sistema comprometido.

Spammers: programas usados para enviar grande volume de e-mail indesejado (spam), muitas vezes com objetivos comerciais ou maliciosos.

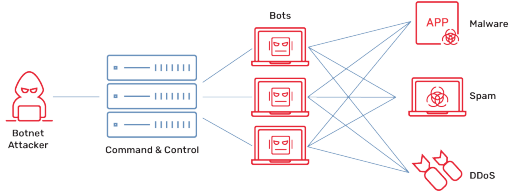
Spyware: software que coleta informações de um computador e as transmite a outro sistema — por exemplo, monitoramento de teclas, captura de tela, tráfego de rede ou escaneamento de arquivos por dados sensíveis.

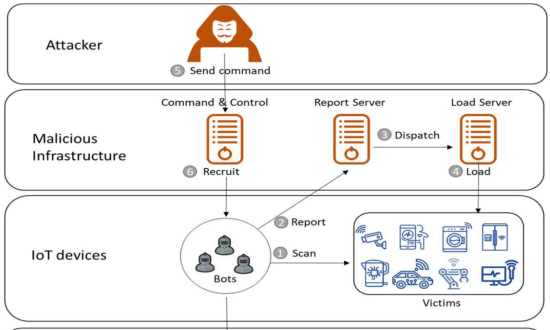
Cavalo de Troia: programa que aparenta ter função útil, mas contém uma função oculta e potencialmente maliciosa que escapa aos mecanismos de segurança, por vezes explorando autorizações legítimas.

Vírus: malware que, quando executado, tenta se reproduzir inserindo-se em outro código executável ou script. O código infectado propaga o vírus quando executado.

Verme: programa que pode ser executado independentemente e propagar cópias completas de si mesmo para outras máquinas em rede, geralmente explorando vulnerabilidades de software.

Zumbi (bot): programa ativado em uma máquina infectada que é controlado remotamente para lançar ataques contra outras máquinas ou executar tarefas maliciosas em rede.





Capítulo 1 (SCHNEIER, 2001)

Leitura Recomendada

Capítulo 1 (Brown, 2013)

Bibliografia

BRASIL. **Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet)**. [*S. l.: s. n.*], 2014. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais)**. [*S. l.: s. n.*], 2018. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais.

BROWN, L. L. **Segurança de Computadores - Princípios e Práticas**. 1. ed. São Paulo: GEN LTC, 2013.

FOROUZAN, Behrouz; MOSHARRAF, Firouz. **Redes de Computadores: Uma abordagem Top-Down**. São Paulo: McGraw Hill, 2014.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **NBR ISO/IEC 27000, 27001 e 27002**. Genebra, 2022. Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação.

SCHNEIER, Bruce. **Secrets and Lies: Digital Security in a Networked World**. 15th Anniversary Edition. Indianapolis, IN: Wiley, 2015. p. 448.

UNION, European. **General Data Protection Regulation (Regulation EU 2016/679)**. [*S. l.: s. n.*], 2016. `https://eur-lex.europa.eu/eli/reg/2016/679/oj`. Regulation on the protection of natural persons with regard to the processing of personal data.

Bibliografia Complementar I

BISHOP, Matt. **Computer Security: Art and Science**. 2. ed. Boston, MA: Addison-Wesley, 2018.

DIAS, Claudia. **Segurança e Auditoria da Tecnologia da Informação**. São Paulo: Axcel Books, 2000.

HINTZBERGEN, J. *et al.* **Fundamentos de Segurança da Informação: com Base na ISO 27001 e na ISO 27002**. 1. ed. Rio de Janeiro: Brasport, 2018.

MCCLURE, Stuart. **Hackers Expostos: Segredos e Soluções Para a Segurança de Redes**. 7. ed. Porto Alegre: Bookman, 2013.

SCHNEIER, Bruce. **Segurança.com**. 1. ed. São Paulo: Campus, 2001.

ZWICKY, Elizabeth D. **Construindo Firewalls para a Internet**. 2. ed. Rio de Janeiro: Editora Campus, 2000.

Estes slides estão protegidos por uma licença Creative Commons

Este modelo foi adaptado de Maxime Chupin.

Marisangila Alves, MSc
marisangila.alves@udesc.br
marisangila.com.br

UDESC
UNIVERSIDADE DO ESTADO DE SANTA CATARINA
JOINVILLE
CENTRO DE CIÊNCIAS TECNOLÓGICAS

UDESC
Universidade do Estado de Santa Catarina

2025/2

Segurança da Informação

Terminologias