ASSIST

# CIBERSEGURANÇA
# GLOSSÁRIO

100 Termos Essenciais de Cibersegurança

Projeto Erasmus+ KA210-ADU
2023-1-TR01-KA210-ADU-000165733

Erasmus+

# AMEAÇAS - Software Malicioso

1. **Vírus** - Software malicioso que infecta computadores e se replica para danificar arquivos.
2. **Worm** - Malware que se auto-replica e se espalha automaticamente pelas redes.
3. **Cavalo de Troia** - Malware disfarçado de software legítimo que executa ações prejudiciais.
4. **Ransomware** - Malware que criptografa arquivos e exige pagamento para descriptografar.
5. **Spyware** - Software que coleta secretamente informações e atividades do usuário.
6. **Adware** - Software que exibe anúncios indesejados e torna os navegadores lentos.
7. **Rootkit** - Malware oculto profundamente no sistema para obter controle total.
8. **Keylogger** - Software que registra teclas digitadas para roubar senhas e dados.
9. **Botnet** - Rede de computadores infectados controlados remotamente por hackers.
10. **Malware** - Termo geral para software malicioso como vírus, worms, trojans.
11. **Zero-Day** - Vulnerabilidade de segurança recém-descoberta sem patch disponível.
12. **Exploit** - Código ou técnica que explora vulnerabilidades de segurança.
13. **Backdoor** - Ponto de acesso oculto que permite entrada não autorizada ao sistema.
14. **RAT** - Trojan de Acesso Remoto. Permite controle remoto completo do computador.
15. **Cryptojacking** - Uso não autorizado do computador de alguém para mineração de cripto.
16. **Scareware** - Alertas de segurança falsos para assustar usuários e pedir dinheiro.
17. **Logic Bomb** - Código malicioso que ativa quando condições específicas são atendidas.
18. **Fileless Malware** - Malware que opera na memória sem deixar arquivos no disco.
19. **Dropper** - Programa projetado para baixar e instalar outros malwares.

20 **Wiper** - Malware que destrói dados permanentemente sem possibilidade de recuperação.

## ATAQUES - Técnicas de Ataque Cibernético

21 **Phishing** - Tentativas fraudulentas de roubar informações via e-mails ou sites falsos.

22 **Smishing** - Ataque de phishing realizado por mensagens SMS.

23 **Vishing** - Ataque de phishing por voz realizado por telefone.

24 **Spear Phishing** - Ataque de phishing direcionado a pessoas ou organizações específicas.

25 **Whaling** - Ataque de phishing direcionado especificamente a executivos de alto nível.

26 **DDoS** - Negação de Serviço Distribuída. Ataque de múltiplas fontes.

27 **DoS** - Negação de Serviço. Ataque que torna um sistema indisponível.

28 **Man-in-the-Middle** - Ataque que intercepta secretamente comunicação entre duas partes.

29 **SQL Injection** - Ataque que insere código SQL malicioso em consultas de banco de dados.

30 **XSS** - Cross-Site Scripting. Injeção de scripts maliciosos em sites.

31 **Brute Force** - Ataque que tenta todas as combinações de senha sistematicamente.

32 **Dictionary Attack** - Ataque usando lista de senhas comuns para adivinhar credenciais.

33 **Credential Stuffing** - Usar credenciais roubadas para tentar acesso em outros sites.

34 **Session Hijacking** - Assumir uma sessão ativa para obter acesso não autorizado.

35 **DNS Spoofing** - Manipular registros DNS para redirecionar usuários a sites falsos.

36 **ARP Spoofing** - Manipular tabelas ARP para interceptar tráfego de rede.

37 **Pharming** - Redirecionar usuários para sites fraudulentos via manipulação de DNS.

38 **Engenharia Social** - Manipular pessoas psicologicamente para revelar informações.

39 **Baiting** - Atrair vítimas com promessas de itens grátis ou recompensas.

40 **Pretexting** - Criar cenário falso para ganhar confiança e extrair informações.

## PROTEÇÃO - Medidas de Segurança

41 **Antivírus** - Software de segurança que detecta e remove programas maliciosos.

42 **Firewall** - Sistema de segurança que monitora e controla o tráfego de rede.

43 **2FA** - Autenticação de Dois Fatores. Camada extra de verificação de segurança.

44 **MFA** - Autenticação Multifator. Múltiplos métodos de verificação.

45 **Criptografia** - Converter dados em código ilegível para proteção. Encryption.

46 **SSL/TLS** - Protocolos que criptografam tráfego de internet para conexões seguras.

47 **HTTPS** - Protocolo HTTP seguro com conexões web criptografadas.

48 **VPN** - Rede Privada Virtual. Criptografa e anonimiza o tráfego de internet.

49 **Backup** - Criar cópias de dados para proteção contra perda.

50 **Atualização** - Manter software atualizado para corrigir vulnerabilidades.

51 **Gerenciador de Senhas** - Aplicativo que armazena e gerencia senhas com segurança.

52 **Sandbox** - Ambiente isolado para testar arquivos suspeitos com segurança.

53 **IDS** - Sistema de Detecção de Intrusão. Monitora atividades suspeitas.

54 **IPS** - Sistema de Prevenção de Intrusão. Detecta e bloqueia ataques.

55 **WAF** - Web Application Firewall. Protege aplicações web.

56 **Endpoint Security** - Proteção para computadores e dispositivos em uma rede.

57 **Zero Trust** - Abordagem de segurança: nunca confiar, sempre verificar.

58 **Patch** - Atualização de software que corrige bugs e falhas de segurança.

59 **Whitelist** - Permitir apenas aplicativos ou endereços aprovados.

60 **Blacklist** - Bloquear sites ou softwares maliciosos conhecidos.

## FERRAMENTAS - Tecnologia e Infraestrutura

61 **Endereço IP** - Identificador numérico único para dispositivos na internet.

62 **Endereço MAC** - Endereço físico único de uma placa de interface de rede.

63 **DNS** - Sistema de Nomes de Domínio. Traduz nomes de domínio para IPs.

64 **Roteador** - Dispositivo que direciona o tráfego de rede entre redes.

65 **Proxy** - Servidor intermediário que encaminha solicitações de internet.

66 **Porta** - Ponto de conexão virtual para comunicações de rede.

67 **Protocolo** - Regras para comunicação entre dispositivos. HTTP, FTP, TCP.

68 **Cookie** - Pequenos arquivos de dados armazenados por sites no navegador.

69 **Cache** - Armazenamento temporário de dados para acesso mais rápido.

70 **Token** - Chave digital usada para fins de autenticação.

71 **Hash** - Valor de comprimento fixo gerado a partir de dados. Impressão digital.

72 **API** - Interface de Programação de Aplicativos. Permite comunicação entre softwares.

73 **Nuvem** - Serviços de servidor remoto acessíveis pela internet. Cloud.

74 **Metadados** - Dados que fornecem informações sobre outros dados.

75 **Largura de Banda** - Capacidade de transferência de dados de uma conexão de rede.

76 **Latência** - Tempo de atraso na transmissão de dados.

77 **Ping** - Comando para testar a conectividade de rede.

78 **Traceroute** - Ferramenta que mostra o caminho que os pacotes de dados percorrem.

79 **Tor** - Rede que permite navegação anônima na internet.

80 **Dark Web** - Parte oculta da internet acessível com software especial.

## CONCEITOS - Conhecimento Fundamental

81 **Cibersegurança** - Prática de proteger sistemas digitais e dados contra ameaças.

82 **Vazamento de Dados** - Acesso não autorizado a dados sensíveis ou confidenciais.

83 **Roubo de Identidade** - Roubar informações pessoais de alguém para uso fraudulento.

84 **Spam** - E-mails ou mensagens em massa não solicitados.

85 **CAPTCHA** - Teste para distinguir humanos de bots automatizados.

86 **Privacidade** - Proteção de informações pessoais contra acesso não autorizado.

87 **Anônimo** - Ter uma identidade desconhecida ou oculta online.

88 **Código Aberto** - Software com código-fonte disponível publicamente. Open source.

89 **Teste de Penetração** - Ataque simulado autorizado para testar segurança. Pentest.

90 **Vulnerabilidade** - Fraqueza em um sistema que pode ser explorada.

91 **Risco** - Avaliação de ameaças potenciais e seu impacto.

92 **Conformidade** - Adesão a padrões de segurança e regulamentações. Compliance.

93 **GDPR** - Regulamento Geral de Proteção de Dados. Lei de privacidade da UE.

94 **Ataque Cibernético** - Tentativa deliberada de danificar ou interromper sistemas digitais.

95 **Hacker** - Pessoa que invade sistemas de computador. Ético ou malicioso.

96 **White Hat** - Hacker ético que testa segurança com permissão.

97 **Black Hat** - Hacker malicioso que invade sistemas ilegalmente.

98 **Bug Bounty** - Programa que recompensa pessoas por encontrar vulnerabilidades.

99 **Pegada Digital** - Rastros e dados deixados pelas atividades na internet.

100 **Higiene Cibernética** - Melhores práticas para manter a segurança digital.



O apoio da Comissão Europeia à produção desta publicação não constitui um aval do seu conteúdo, que reflete apenas as opiniões dos autores, e a Comissão não pode ser responsabilizada por qualquer utilização que possa ser feita das informações nela contidas.