



Módulo 13:Atacantes e suas ferramentas



CyberOps Associate v1.0

Prof. Clemilson Oliveira

clemilson.oliveira@edu.sc.senai.br

Objetivos do módulo

- **Título do Módulo:** Atacantes e suas ferramentas
- **Objetivo do Módulo:** Explique como as redes são atacadas.

Título do Tópico	Objetivo do Tópico
Quem está atacando nossa rede	Explicar como as ameaças à rede evoluíram.
Ferramentas do agente da ameaça	Descrever os vários tipos de ferramentas de ataque usadas pelos agentes de ameaças.

13.1 Quem está atacando nossa rede?

Ameaça, vulnerabilidade e risco

- Os atacantes querem acessar nossos ativos, como dados e outras propriedades intelectuais, servidores, computadores, smartphones, tablets e assim por diante.



Ameaça, Vulnerabilidade e Risco (Cont.)

- Para entender a segurança da rede, é importante conhecer os seguintes termos:

TERM	EXPLICAÇÃO
Ameaça	Um perigo potencial para um ativo, como dados ou a própria rede.
Vulnerabilidade	Uma fraqueza em um sistema ou em seu design que pode ser explorada por uma ameaça.
Superfície de ataque	Uma superfície de ataque é a soma total das vulnerabilidades em um determinado sistema que são acessíveis a um invasor. A superfície de ataque descreve diferentes pontos em que um invasor pode entrar em um sistema e onde ele pode obter dados do sistema.
Exploit	O mecanismo que é usado para alavancar uma vulnerabilidade para comprometer um ativo. As explorações podem ser remotas ou locais. Uma exploração remota é aquela que funciona através da rede sem qualquer acesso prévio ao sistema de destino. Em uma exploração local, o ator de ameaça tem algum tipo de acesso administrativo ou de usuário ao sistema final. Isso não significa necessariamente que o invasor tenha acesso físico ao sistema final.
Risco	A probabilidade de uma determinada ameaça explorar uma vulnerabilidade específica de um ativo e resultar em uma consequência indesejável.

Ameaça, Vulnerabilidade e Risco (Cont.)

- A gestão de riscos é o processo que equilibra os custos operacionais de provisão de medidas de proteção com os ganhos obtidos através da proteção do ativo.

Quatro maneiras de gerenciar o risco:

Estratégia de gestão de riscos	Explicação
Aceitação de riscos	Quando o custo das opções de gerenciamento de risco supera o custo do risco, o risco é aceito e nenhuma ação é tomada.
Prevenção de riscos	Isto significa evitar qualquer exposição ao risco, eliminando a atividade, resultando em perda de quaisquer benefícios da atividade.
Redução de risco	Isso reduz a exposição ao risco. É a estratégia de mitigação de riscos mais utilizada. Essa estratégia requer uma avaliação cuidadosa dos custos de perda, da estratégia de mitigação e dos benefícios obtidos com a operação ou atividade que está em risco.
transferência de risco	Parte ou todo o risco é transferido para um terceiro disposto, como companhia de seguros.

Ameaça, Vulnerabilidade e Risco (Cont.)

- **Termos comuns de segurança de rede:**

- Contramedida — Ações tomadas para proteger ativos, atenuando uma ameaça ou reduzindo o risco.
- Impacto - O potencial dano à organização causado pela ameaça
- **Observação:** uma exploração local requer acesso interno à rede, como um usuário com uma conta na rede. Não requer uma conta na rede para explorar a vulnerabilidade dessa rede.

Hacker vs. Agente de Ameaça

‘Hacker’ é um termo comum usado para descrever um agente de ameaça. Hacker tem uma variedade de significados que são os seguintes:

- Um programador inteligente capaz de desenvolver novos programas e fazer alterações de codificação em programas existentes para torná-los mais eficientes.
- Um profissional de rede que usa habilidades sofisticadas de programação para garantir que as redes não sejam vulneráveis a ataques.
- Um indivíduo que executa programas para impedir ou corromper dados em servidores.

Tipos de hackers:

- Hackers White Hat
- Hackers Gray Hat
- Hackers Black Hat

Hacker vs. Ator de Ameaças (Cond.)

Hackers White Hat:

- Hackers de White Hat são hackers éticos que usam suas habilidades de programação para propósitos bons, éticos e legais.

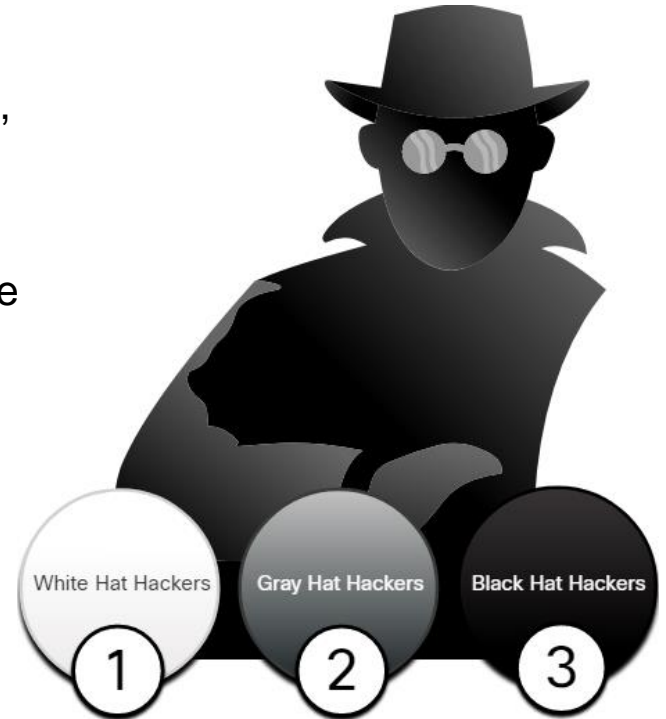
Hackers Gray Hat:

- Hackers Gray Hat são indivíduos que cometem crimes e coisas antiéticas, mas não para ganho pessoal ou para causar danos.

Hackers Black Hat::

- Os hackers Black Hat são criminosos antiéticos que violam a segurança do computador e da rede para ganho pessoal.

Observação: o termo “agente de ameaça” é usado quando se refere a indivíduos ou grupos que podem ser classificados como hackers cinza ou black hat.



Evolução dos atores de ameaças

- O hackeamento começou na década de 1960 com a *freaking* por telefone, que se refere ao uso de várias frequências de áudio para manipular sistemas telefônicos.
- No início da década de 1960, os agentes de ameaças perceberam que, imitando um tom com um apito, eles poderiam explorar os interruptores do telefone para fazer chamadas de longa distância gratuitas.
- Em meados da década de 1980, os agentes de ameaças escreveram programas de "discagem de guerra" que discavam cada número de telefone em uma determinada área em busca de computadores, sistemas de boletim informativo e máquinas de fax.
- Quando um número de telefone era encontrado, programas de quebra de senha eram usados para obter acesso.

Evolução dos Atores da Ameaça (Cont.)

Tipos de agente de ameaça:

- **Script kiddies** - Refere-se a adolescentes ou atores de ameaças inexperientes executando scripts, ferramentas e explorações existentes para causar danos, mas normalmente sem fins lucrativos.
- **Corretores de vulnerabilidade**- Refere-se a hackers Gray Hat que tentam descobrir exploits e relatá-los aos fornecedores, por prêmios ou recompensas.
- **Hacktivistas** - Refere-se a hackers Gray Hat que se manifestam e protestam contra diferentes ideias políticas e sociais.
- **Cibercriminosos** -Refere-se a hackers Black Hat que são autônomos ou trabalham para grandes organizações do crime cibernético.
- **Patrocinados pelo Estado** - Os hackers patrocinados pelo Estado são atores de ameaças que roubam segredos do governo, coletam informações e sabotam redes de governos estrangeiros, grupos terroristas e corporações.

Cybercriminals

- Os cibercriminosos são agentes de ameaça que estão motivados a ganhar dinheiro usando todos os meios necessários.
- Às vezes, os cibercriminosos trabalham de forma independente ou são financiados e patrocinados por organizações criminosas.
- Eles roubam bilhões de dólares de consumidores e empresas todos os anos.
- Operam na economia subterrânea e compram e vendem informações pessoais e propriedade intelectual que roubam das vítimas.
- Eles têm como alvo pequenas empresas e consumidores, bem como grandes empresas e indústrias.



Tarefas de cibersegurança

- Os atores de ameaças visam os usuários domésticos, empresas de pequeno a médio porte, bem como grandes organizações públicas e privadas.
- Por conseguinte, a cibersegurança é uma responsabilidade partilhada que todos os utilizadores devem praticar para tornar a Internet e as redes mais seguras e seguras.
- As organizações devem agir e proteger seus ativos, usuários e clientes. Eles devem desenvolver e praticar tarefas de segurança cibernética, como as mencionadas na figura.



Indicadores de ameaças cibernéticas

Indicadores de compromisso (IOC)

- IOCs são a evidência de que um ataque ocorreu e cada ataque tem atributos identificáveis únicos.
- Os IOCs podem ser recursos que identificam arquivos de malware, endereços IP de servidores que são usados em ataques, nomes de arquivos e alterações características feitas no software final do sistema, entre outros.
- Os IOCs ajudam o pessoal de segurança cibernética a identificar o que aconteceu em um ataque e desenvolver defesas contra o ataque.

```
Malware File - "studiox-link-standalone-v20.03.8-stable.exe"
sha256 6a6c28f5666b12beecd56a3d1d517e409b5d6866c03f9be44ddd9efffa90f1e0
sha1   eb019ad1c73ee69195c3fc84ebf44e95c147bef8
md5    3a104b73bb96dfed288097e9dc0a11a8

DNS requests
domain log.studiox.link
domain my.studiox.link
domain _sips._tcp.studiox.link
domain sip.studiox.link

Connections
ip      198.51.100.248
ip      203.0.113.82
```

Resumo do COI para um pedaço de malware

Indicadores de ameaças cibernéticas (Cont.)

Indicadores de ataque (IOA)


- O IOA concentra-se mais na motivação e nas estratégias por trás de um ataque e nos atacantes para obter acesso a ativos.
- Os IOAs ajudam a gerar uma abordagem de segurança proativa que pode ser reutilizada em vários contextos e ataques múltiplos. Defender contra uma estratégia pode, portanto, evitar ataques futuros.

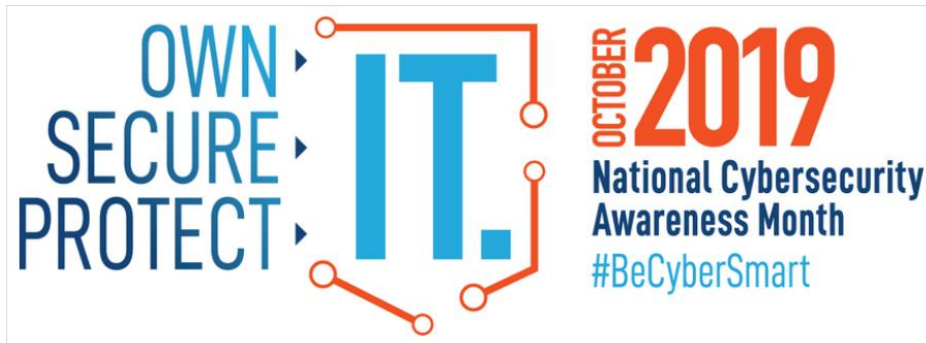
Compartilhamento de ameaças e criação de conscientização de cibersegurança

- Os governos estão agora promovendo ativamente a segurança cibernética.
- A Agência de Infraestrutura e Segurança Cibernética dos EUA (CISA) está liderando esforços para automatizar o compartilhamento de informações de segurança cibernética com organizações públicas e privadas sem nenhum custo.
- A CISA usa um sistema chamado Automated Indicator Sharing (AIS) que permite o compartilhamento de indicadores de ataque entre o governo dos EUA e o setor privado assim que as ameaças são verificadas.
- A Agência da União Europeia para a Cibersegurança (ENISA) presta aconselhamento e soluções para os desafios da cibersegurança dos Estados-Membros da UE.
- A CISA e a National Cyber Security Alliance (NCSA) têm uma campanha anual em outubro chamada National Cybersecurity Awareness Mês (NCASM) para aumentar a conscientização sobre segurança cibernética.

Compartilhamento de ameaças e criação de consciência de segurança cibernética (Cont.)

- O tema para o NCASM para 2019 foi **a TI Própria. TI Segura. Proteja a TI.**
- Tópicos de segurança fornecidos por meio da campanha:
 - Segurança das redes sociais
 - Atualizando configurações de privacidade
 - Reconhecimento da segurança de aplicativos de dispositivos
 - Manter o software atualizado
 - Compras online seguras
 - Segurança Wi-Fi

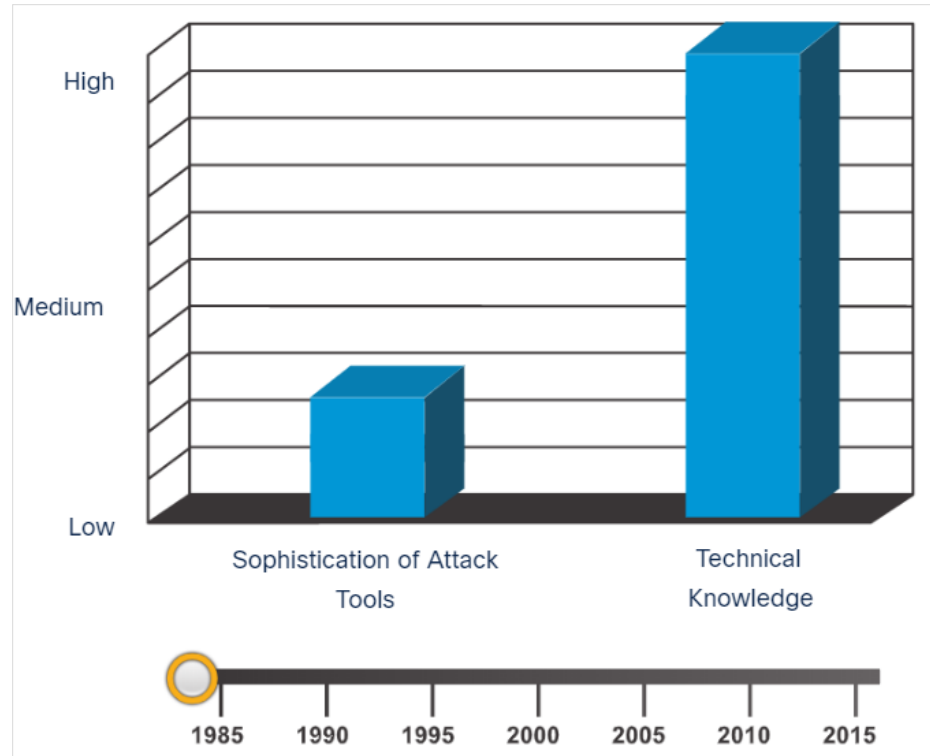
 Protegendo os dados do cliente



13.2 Ferramentas dos agentes de ameaças

Introdução de ferramentas de ataque

- Para explorar a vulnerabilidade, um ator de ameaça deve ter uma técnica ou ferramenta.
- Ao longo dos anos, as ferramentas de ataque tornaram-se mais sofisticadas e altamente automatizadas.
- Essas novas ferramentas requerem menos conhecimento técnico para serem implementadas.
- Na figura, arraste o círculo branco pela linha do tempo para visualizar o relacionamento entre a sofisticação das ferramentas de ataque e o conhecimento técnico necessário para usá-las.



Evolução das ferramentas de segurança

- O hacking ético envolve o uso de muitos tipos diferentes de ferramentas para testar a rede e os dispositivos finais.
- Para validar a segurança de uma rede e seus sistemas, muitas ferramentas de teste de penetração de rede foram desenvolvidas e muitas dessas ferramentas também podem ser usadas por agentes de ameaça para exploração.
- Atores de ameaças também criaram várias ferramentas de hacking. O pessoal de segurança cibernética também deve saber como usar essas ferramentas ao realizar testes de penetração na rede.

Observação: *a maioria dessas ferramentas é baseada em UNIX ou Linux; portanto, um profissional de segurança deve ter uma sólida experiência em UNIX e Linux.*

Evolução das ferramentas de segurança (cont.)

A tabela a seguir lista algumas das categorias de ferramentas comuns de teste de penetração de rede.

Categorias de Ferramentas	Descrição
Quebradores de senha	Usado para quebrar ou recuperar a senha. Exemplo: John the Ripper, Ophcrack
Ferramentas de hacking sem fio	Usado para invadir intencionalmente uma rede sem fio para detectar vulnerabilidades de segurança. Exemplo:Aircrack-ng, Kismet
Ferramentas de varredura de rede e hacking	Usado para sondar dispositivos de rede, servidores e hosts para portas TCP ou UDP abertas. Por exemplo: Nmap, SuperScan
Ferramentas de criação de pacotes	Usado para sondar e testar a robustez de um firewall. Por exemplo: Hping, Scapy
Sniffers de pacotes	Usado para capturar e analisar pacotes dentro de LANs Ethernet ou WLANs tradicionais.Por exemplo: Wireshark, Tcpdump
Detectores de rootkit	É um verificador de integridade de diretório e arquivo usado por white hats para detectar root kits instalados. Por exemplo: AIDE, Netfilter
Fuzzers para pesquisar vulnerabilidades	Usado por agentes de ameaça ao tentar descobrir vulnerabilidades de segurança de um sistema de computador. Por exemplo: Skipfish, Wapiti

Evolução das ferramentas de segurança (cont.)

Categorias de Ferramentas	Descrição
Ferramentas forenses	Os hackers White Hat usam essas ferramentas para encontrar qualquer vestígio de evidência existente em um sistema de computador específico. Por exemplo: Sleuth Kit, Helix
Depuradores	Usado por Black Hats para fazer engenharia reversa de arquivos binários ao escrever exploits e usado por White Hats ao analisar malware. Exemplo: Gdb, WinDbg
Sistemas operacionais para hacking	Estes são pré-carregados com ferramentas e tecnologias otimizadas para hacking. Por exemplo: Kali Linux, SELinux
Ferramentas de criptografia	Essas ferramentas usam esquemas de algoritmo para codificar os dados e evitar o acesso não autorizado aos dados. Por exemplo: VeraCrypt, CipherShed
Ferramentas de exploração de vulnerabilidade	Essas ferramentas identificam se um host remoto é vulnerável a um ataque de segurança. Por exemplo: Metasploit, Core Impact
Scanners de vulnerabilidade	Essas ferramentas examinam uma rede ou sistema para identificar portas abertas. Eles também podem ser usados para verificar vulnerabilidades conhecidas e verificar VMs, dispositivos BYOD e bancos de dados do cliente. Por exemplo: Nipper, Securia PSI

Categorias de ataques

- Os agentes de ameaças usam as ferramentas mencionadas anteriormente ou uma combinação de ferramentas para criar vários ataques.
- É importante entender que os agentes de ameaças usam uma variedade de ferramentas de segurança para realizar esses ataques.
- A tabela a seguir exhibe tipos comuns de ataques.

Categoria de Ataque	Descrição
Ataque de escuta	Um ataque de escuta ocorre quando um agente de ameaça captura e escuta o tráfego da rede. Isso também é chamado de sniffing ou snooping.
Ataque de modificação de dados	Ataques de modificação de dados ocorrem quando um agente de ameaça capturou o tráfego da empresa e alterou os dados nos pacotes sem o conhecimento do remetente ou receptor.
Ataque de Falsificação de Endereços IP	Um ataque de falsificação de endereço IP ocorre quando um ator de ameaça constrói um pacote IP que parece se originar de um endereço válido dentro da intranet corporativa.

Categorias de Ataques (Cont.)

Categoria de Ataque	Descrição
Ataques baseados em senha	Ataques baseados em senha ocorrem quando um ator de ameaça obtém as credenciais para uma conta de usuário válida.
Ataque de negação de serviço (DoS)	Um ataque de DoS impede o uso normal de um computador ou rede por usuários válidos. Este ataque pode bloquear o tráfego, o que resulta na perda de acesso aos recursos da rede.
Ataque man-in-the-middle (MiTM)	Um ataque MiTM ocorre quando os agentes da ameaça se posicionam entre a origem e o destino.
Ataque de chave comprometida	Um ataque de chave comprometida ocorre quando um ator ameaça obtém uma chave secreta. Uma chave comprometida pode ser usada para obter acesso a uma comunicação segura sem o remetente ou receptor.
Ataque Sniffer	Um sniffer é um aplicativo ou dispositivo que pode ler, monitorar e capturar trocas de dados de rede e ler pacotes de rede. Se os pacotes não estiverem criptografados, um sniffer fornece uma visão completa dos dados dentro do pacote.

13.3 Resumo dos invasores e suas ferramentas

O que aprendi neste módulo?

- Para compreender a segurança da rede, é importante compreender os termos como ameaça, vulnerabilidade, superfície de ataque, exploração e risco.
- A gestão de riscos é o processo de fornecer medidas de proteção através da proteção do ativo.
- Quatro formas comuns de gerenciar riscos são a aceitação de riscos, a prevenção de riscos, a redução de riscos e a transferência de riscos.
- Hacker é um termo usado para descrever um ator de ameaça. Os hackers White Hat são hackers éticos que usam suas habilidades para propósitos bons, éticos e legais.
- Hackers de Gray Hat são indivíduos que cometem crimes e fazem coisas antiéticas, mas não para ganho pessoal.
- Os hackers Black hat são criminosos que violam a segurança do computador e da rede para ganho pessoal ou por motivos maliciosos, como ataques a redes.

O que aprendi neste módulo? (Continuação)

- Muitos ataques de rede podem ser evitados compartilhando informações sobre Indicadores de Compromisso (IOC). CISA e NCSA são exemplos de organizações promotoras de segurança cibernética.
- As ferramentas de ataque se tornaram mais sofisticadas e altamente automatizadas.
- Muitas das ferramentas são baseadas em Linux ou UNIX e o conhecimento delas é útil para um profissional de segurança cibernética.
- As ferramentas incluem crackers de senhas, ferramentas de hacking sem fio, ferramentas de varredura e hacking de segurança de rede, ferramentas de criação de pacotes, ferramentas de criação de pacotes, sniffers de pacotes, detectores de rootkit, fuzzers para pesquisar vulnerabilidades, ferramentas forenses, depuradores, sistemas operacionais de hacking, ferramentas de criptografia, vulnerabilidade ferramentas de exploração e scanners de vulnerabilidade.
- As categorias de ataques incluem ataques de espionagem, ataques de modificação de dados, ataques de falsificação de endereços IP, ataques baseados em senha, ataques de negação de serviço, ataques de man-in the-middle, ataques de chave comprometidos e ataques de farejador.

