**Introdução**

1.0.1

**Primeira Vez neste Curso**



CyberOps Associate v1.0 cobre o conhecimento e as habilidades necessárias para lidar com sucesso com as tarefas, deveres e responsabilidades de um Analista de Segurança de nível associado trabalhando em um Centro de Operações de Segurança (SOC).

Depois da conclusão do curso CyberOps Associate v1.0 , os alunos serão capazes de realizar as seguintes tarefas:

* Instalar máquinas virtuais para criar um ambiente seguro para implementar e analisar eventos de ameaças à segurança cibernética.
* Explicar a função do analista de operações de segurança cibernética na empresa.
* Explicar os recursos e as características do sistema operacional Windows necessários para oferecer suporte às análises de segurança cibernética.
* Explicar os recursos e as características do sistema operacional Linux.
* Analisar a operação de protocolos e serviços de rede.
* Explicar a operação da infraestrutura de rede.
* Classificar os vários tipos de ataques à rede.
* Usar ferramentas de monitoramento de rede para identificar ataques contra protocolos e serviços de rede.
* Explicar como evitar o acesso mal-intencionado a redes, hosts e dados de computadores.
* Explicar os impactos da criptografia no monitoramento de segurança de rede.
* Explicar como investigar vulnerabilidades e ataques de endpoints.
* Avaliar os alertas de segurança de rede.
* Analisar dados de invasão de rede para identificar hosts e vulnerabilidades comprometidos.
* Aplicar modelos de resposta a incidentes para gerenciar incidentes de segurança de rede.

1.0.2

**Recursos dos alunos**



Há uma série de ferramentas e recursos disponíveis para você que o ajudarão em sua jornada à medida que você desenvolve suas habilidades em CyberOps e se prepara para oportunidades de emprego.

**Ambiente de Laboratório**

Neste curso, duas máquinas virtuais (VM) são usadas: CyberOps Workstation e Security Onion. Essas VMs fornecem todos os aplicativos e os recursos mais recentes de monitoramento de segurança e análise de intrusão de rede necessários para o curso.

O requisito mínimo de memória RAM para executar máquinas virtuais CyberOps Workstation é de 1 GB. No entanto, para a máquina virtual Security Onion, recomenda-se 4 GB de RAM. A recomendação de memória RAM na VM Security Onion permite que os serviços, como o monitoramento de segurança de rede (NSM), funcionem corretamente.

Os laboratórios de instalação estão disponíveis no curso e fornecem etapas detalhadas para configurar adequadamente suas VMs e o ambiente de laboratório.

**Sobre o Security Onion**

Security Onion é desenvolvido pela Security Onion Solutions. [Security Onion] (<https://securityonion.net/>) é disponibilizado sob licença GPL. Este curso usa fornece treinamento básico no uso de Security Onion para validar os objetivos deste curso. Para mais necessidades de treinamento, visite o site do desenvolvedor Security Onion Solutions.

**Packet Tracer**

O Packet Tracer simula o funcionamento interno de uma rede e é usado neste curso. Baixe e instale a versão mais recente do Packet Tracer aqui: [Packet Tracer Resources] (<https://www.netacad.com/portal/resources/packet-tracer>).

Se você é novo no Packet Tracer, faça este curso gratuito, curto e online agora: [Introdução ao Packet Tracer Course] (<https://www.netacad.com/courses/packet-tracer/introduction-packet-tracer>).

Você pode usar seu smartphone, tablet ou desktop para acessar seu curso ; entretanto, as atividades do Packet Tracer, bem como algumas outras atividades, questionários e exames, são mais bem experimentadas usando um PC.

**Participe de Nossas Comunidades**

Conecte-se e obtenha ajuda de outros alunos da Networking Academy de todo o mundo com nossa [página do Facebook da Cisco Networking Academy] ([https://www.facebook.com/cisconetworkingacademy).Você](https://www.facebook.com/cisconetworkingacademy).Voc%C3%AA) pode usar seu smartphone, tablet ou desktop para acessar seu curso;

Faça contato com seus colegas em nossa página [Cisco Networking Academy LinkedIn] (<https://www.linkedin.com/school/cisco-networking-academy1/>).

**Ganhe um emprego!**

Acesse [Recursos de carreira] (<https://www.netacad.com/careers/career-advice>) adaptado especificamente para ajudar os alunos da NetAcad a ter sucesso no local de trabalho.

Encontre grandes oportunidades de emprego com parceiros Cisco e Cisco. Registre-se agora na [Talent Bridge] (<https://www.netacad.com/portal/careers/talent-bridge-program>).

Obter a certificação do setor é uma garantia para os empregadores de que você possui as habilidades técnicas para fazer o trabalho. Confira nossa página [Certificações e Vouchers] (<https://www.netacad.com/careers/career-advice/certification-advice/qualify-receive-discount-your-certification-exam?utm_source=netacad&utm_medium=course&utm_campaign=student&utm_content=voucher>).

**Mais cursos**

Escolha um curso, pratique o que você sabe e torne-se um profissional de TI. Confira nosso [Catálogo de Cursos] (<https://www.netacad.com/courses/all-courses>).

1.0.3

**Declaração de hackers éticos**

O programa Cisco Networking Academy está focado na criação dos solucionadores de problemas globais necessários para criar, dimensionar, proteger e defender as redes que são usadas em nossos negócios e na vida diária. A necessidade de especialistas em segurança cibernética bem treinados continua a crescer a uma taxa exponencial. O treinamento para se tornar um especialista em segurança cibernética requer compreensão profunda e exposição a como ocorrem ataques cibernéticos, bem como eles são detectados e prevenidos. Essas habilidades também incluirão, naturalmente, o aprendizado das técnicas que os atores ameaçam usam para comprometer dados, privacidade e segurança de computadores e redes.

Neste curso, os alunos usarão ferramentas e técnicas em um ambiente de máquina virtual “sandbox” que lhes permite criar, implementar, monitorar e detectar vários tipos de ataques cibernéticos. O treinamento prático é realizado neste ambiente para que os alunos possam adquirir as habilidades e conhecimentos necessários para frustrar esses e futuros ataques cibernéticos. As falhas de segurança e vulnerabilidades criadas neste curso só devem ser usadas de forma ética e somente neste ambiente virtual “sandbox”. A experimentação com essas ferramentas, técnicas e recursos fora do ambiente virtual em área restrita fornecido fica a critério do instrutor e da instituição local. Se o aluno tiver alguma dúvida sobre quais sistemas e redes de computadores fazem parte do ambiente virtual em área restrita, ele deve entrar em contato com seu instrutor antes de qualquer experimentação.

O acesso não autorizado a dados, computadores e sistemas de rede é um crime em muitas jurisdições e geralmente é acompanhado por graves consequências, independentemente das motivações do agressor. É responsabilidade do aluno, como usuário deste material, conhecer e cumprir as leis de uso do computador.

1.0.4

**Por que devo fazer este módulo?**

Alguma vez roubaram alguma coisa? Talvez você tenha uma carteira roubada ou sua casa tenha sido roubada. Você não só precisa proteger sua propriedade física, como também proteger suas informações! Quem está roubando informações e por que eles estão fazendo isso? Talvez seja um indivíduo apenas vendo se é capaz de hackear as informações. Muitas vezes é para ganho financeiro. Há muitas razões. Continue lendo este módulo para saber mais sobre as ameaças e os atores responsáveis por esses ataques.

1.0.5

**O que vou aprender neste módulo?**

**Título do módulo:** O perigo  
**Objetivo do módulo:** Explicar por que redes e dados são atacados.

| **Título do Tópico** | **Objetivo do Tópico** |
| --- | --- |
| Histórias de guerra | Explicar por que as redes e os dados são atacados. |
| Agentes da ameaça | Explicar as motivações dos agentes de ameaças por trás de incidentes de segurança específicos. |
| Impacto de ameaça | Explicar o possível impacto dos ataques de segurança de rede. |

1.0.6

**Atividade de Classe - O Top Hacker nos mostra como é feito**

Nesta atividade de classe, você verá um vídeo TED Talk que discute várias vulnerabilidades de segurança. Você também pesquisará uma das vulnerabilidades mencionadas no vídeo.

# Histórias de guerra

1.1.1

## Pessoas Sequestradas

Sarah passou no seu café favorito para pegar sua bebida da tarde. Ela fez o pedido, pagou ao balconista e esperou enquanto os baristas trabalhavam furiosamente para cumprir o atendimento dos pedidos. Sarah pegou o celular, abriu o cliente sem fio, e se conectou ao que ela presumiu ser a rede sem fio gratuita da cafeteria.

No entanto, sentado em um canto da loja, um hacker tinha acabado de configurar um hotspot sem fio “desonesto” aberto posando como a rede sem fio da cafeteria. Quando Sarah entrou no site do banco, o hacker sequestrou sua sessão e teve acesso às contas bancárias dela. Outro termo para hotspots sem fio desonestos são hotspots “gêmeos malvados”.

Pesquise na internet em “pontos de acesso gêmeos malvados” para saber mais sobre essa ameaça à segurança.



1.1.2

## Empresas resgatadas

Rashid, um funcionário do departamento financeiro de uma grande corporação pública, recebe um e-mail de seu CEO com um PDF anexado. O PDF é sobre os ganhos do terceiro trimestre da empresa. Rashid não se lembra de seu departamento ter criado o PDF. Sua curiosidade é despertada, então ele abre o anexo.

O mesmo cenário se desenrola em toda a organização, já que dezenas de outros funcionários são atraídos com sucesso para clicar no anexo. Quando o PDF é aberto, o ransomware é instalado nos computadores dos funcionários e inicia o processo de coleta e criptografia de dados corporativos. O objetivo dos atacantes é o ganho financeiro, porque eles mantêm os dados da empresa para resgate até serem pagos.



1.1.3

## Nações-alvo

Alguns dos malwares atuais são tão sofisticados e caros para criar que especialistas em segurança acreditam que apenas um estado-nação ou grupo de nações poderia possivelmente ter a influência e o financiamento para criá-lo. Esse malware pode ser direcionado para atacar a infraestrutura vulnerável de uma nação, como o sistema de água ou a rede elétrica.

Este era o propósito do worm Stuxnet, que infectou unidades USB. Essas unidades foram transportadas por cinco fornecedores iranianos de componentes para uma instalação segura que eles apoiaram. O Stuxnet foi projetado para se infiltrar nos sistemas operacionais Windows e, em seguida, direcionar o software Passo 7. O passo 7 foi desenvolvido pela Siemens para seus controladores lógicos programáveis (PLCs). A Stuxnet estava à procura de um modelo específico dos PLCs da Siemens que controla as centrífugas em instalações de processamento de urânio. O worm foi transmitido dos drives USB infectados para os PLCs e, eventualmente, danificou muitas dessas centrífugas.

Zero Days, um filme lançado em 2016, documenta o que se sabe sobre o desenvolvimento e a implantação do ataque de malware alvo da Stuxnet. Procure Zero Days para encontrar o filme ou informações sobre o filme.



1.1.4

## Vídeo - Anatomia de um Ataque

Assista a este vídeo para ver detalhes de um ataque complexo.

1.1.5

## Laboratório - Instalando as Máquinas Virtuais

Neste laboratório, você instalará o VirtualBox em seu computador pessoal. Em seguida, você baixará e instalará o CyberOps Workstation Virtual Machine (VM).

1.1.6

## Laboratório - Estudos de caso de cibersegurança

Neste laboratório, você analisará os casos dados e responderá a perguntas sobre eles.

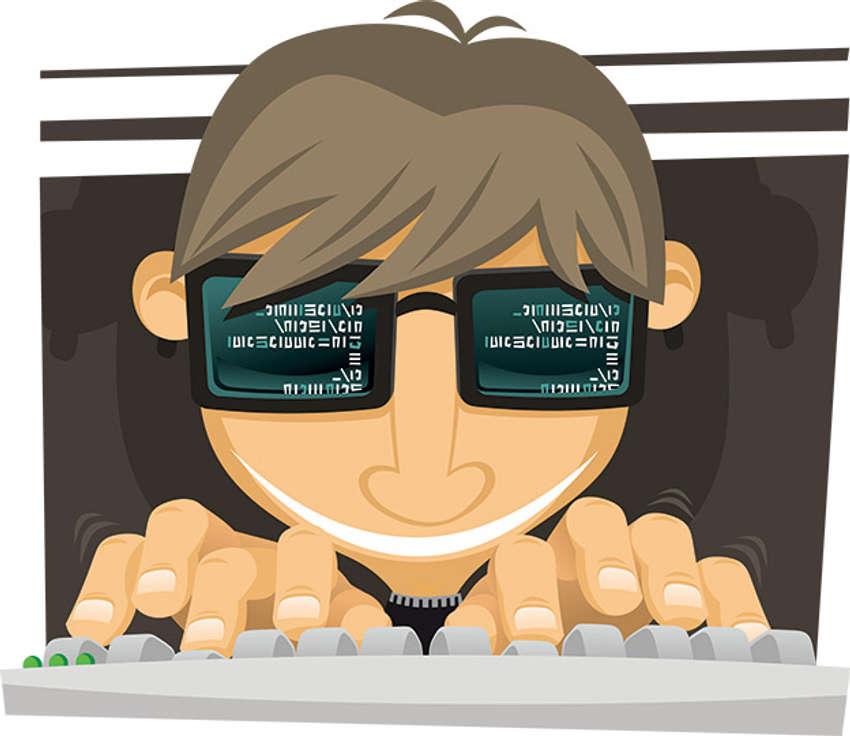
# Agentes da ameaça

1.2.1

## Agentes da ameaça

Os atores de ameaças incluem, entre outros, amadores, hacktivistas, grupos do crime organizado, patrocinados pelo Estado e grupos terroristas. Os atores de ameaças são indivíduos ou grupos de indivíduos que realizam ataques cibernéticos. Os ataques cibernéticos são atos maliciosos intencionais destinados a impactar negativamente outro indivíduo ou organização.

Amadores, também conhecidos como crianças de roteiro, têm pouca ou nenhuma habilidade. Eles costumam usar ferramentas existentes ou instruções encontradas na Internet para lançar ataques. Alguns são apenas curiosos, enquanto outros tentam demonstrar suas habilidades causando danos. Mesmo que eles estejam usando ferramentas básicas, os resultados ainda podem ser devastadores.



1.2.2

## Quão segura é a Internet das coisas?



A Internet das Coisas (IoT) está ao nosso redor e em rápida expansão. Estamos apenas começando a colher os benefícios da IoT. Novas formas de usar coisas conectadas estão sendo desenvolvidas diariamente. A IoT ajuda os indivíduos a conectar coisas para melhorar sua qualidade de vida. Por exemplo, muitas pessoas estão agora usando dispositivos vestíveis conectados para rastrear suas atividades de fitness. Quantos dispositivos você possui atualmente que se conectam à sua rede doméstica ou à Internet?

Quão seguros são esses dispositivos? Por exemplo, quem escreveu o firmware? O programador prestou atenção às falhas de segurança? Seu termostato doméstico conectado é vulnerável a ataques? E o seu gravador de vídeo digital (DVR)? Se forem encontradas vulnerabilidades de segurança, o firmware no dispositivo pode ser corrigido para eliminar a vulnerabilidade? Muitos dispositivos na internet não são atualizados com o firmware mais recente. Alguns dispositivos mais antigos nem foram desenvolvidos para serem atualizados com patches. Essas duas situações criam oportunidades para atores de ameaças e riscos de segurança para os proprietários desses dispositivos.

Em outubro de 2016, um ataque DDoS contra o provedor de nomes de domínio Dyn derrubou muitos sites populares. O ataque veio de um grande número de webcams, DVRs, roteadores e outros dispositivos IoT que tinham sido comprometidos por software malicioso. Esses dispositivos formaram um “botnet” controlado por hackers. Este botnet foi usado para criar um enorme ataque DDoS que desabilitou os serviços essenciais de internet. Dyn postou um blog para explicar o ataque e sua reação a ele. Pesquise em “Dyn Analysis Summary of Friday October 21 Attack” para saber mais sobre este ataque recorde.

Para obter uma explicação sobre os perigos de não proteger dispositivos IoT, procure a palestra TED de Avi Rubin, “Todos os seus dispositivos podem ser hackeados”. Dr. Rubin é professor de Ciência da Computação na Universidade Johns Hopkins.

1.2.3

## Laboratório - Aprendendo os detalhes dos ataques

# Impacto de ameaça

1.3.1

## PII, PHI e PSI

O impacto econômico dos ataques cibernéticos é difícil de determinar com precisão. No entanto, estima-se que as empresas percam mais de US$5 trilhões por ano até 2024 devido a ataques cibernéticos.

Informações de identificação pessoal (PII) são todas as informações que podem ser usadas para identificar positivamente um indivíduo. Exemplos de PII incluem:

* Nome
* Número da previdência social
* Data de nascimento
* Números de cartão de crédito
* Números de contas bancárias
* ID emitido pelo governo
* Informações de endereço (rua, e-mail, números de telefone)

Um dos objetivos mais lucrativos dos criminosos cibernéticos é obter listas de PII que podem ser vendidas na dark web. A dark web só pode ser acessada com software especial e é usada por cibercriminosos para proteger suas atividades. As PII roubadas podem ser usadas para criar contas financeiras falsas, como cartões de crédito e empréstimos de curto prazo.

Um subconjunto de PII são informações de saúde protegidas (PHI). A comunidade médica cria e mantém registros médicos eletrônicos (EMRs) que contêm PHI. Nos EUA, o tratamento de PHI é regulamentado pela Lei de Responsabilidade e Portabilidade de Seguro Saúde (HIPAA). Na União Europeia, o Regulamento Geral de Proteção de Dados (GDPR) protege uma ampla gama de informações pessoais, incluindo registros de saúde.

As informações de segurança pessoal (PSI) são outro tipo de PII. Essas informações incluem nomes de usuário, senhas e outras informações relacionadas à segurança que os indivíduos usam para acessar informações ou serviços na rede. De acordo com um relatório de 2019 da Verizon, a segunda maneira mais comum de que os atores ameaçadores violaram uma rede foi usando PSI roubado.

A maioria dos hacks em empresas e organizações que foram relatados nas notícias envolveu PII roubado ou PHI. Exemplos recentes são:

* Em 2019, um site de ferramentas de design gráfico on-line experimentou uma violação de dados em que as PII de aproximadamente 137 milhões de usuários foram visualizadas por hackers com detalhes de usuários para 4 milhões de contas aparecendo na internet.
* Em 2020, uma grande empresa chinesa de mídia social foi hackeada, resultando em roubo de PII, incluindo números de telefone, roubados de 172 milhões de usuários. O roubo não incluía senhas, então os dados estavam disponíveis por um preço baixo na internet.
* Em 2019, uma empresa que faz jogos que são jogados no Facebook foi hackeada e o PII de 218 milhões de usuários foi roubado.



1.3.2

## Vantagem Competitiva Perdida

As empresas estão cada vez mais preocupadas com a espionagem corporativa no ciberespaço. A perda de propriedade intelectual para os concorrentes é uma séria preocupação. Uma grande preocupação adicional é a perda de confiança que ocorre quando uma empresa é incapaz de proteger os dados pessoais de seus clientes. A perda de vantagem competitiva pode resultar dessa perda de confiança em vez de outra empresa ou país roubar segredos comerciais.

1.3.3

## Política e Segurança Nacional

Não são só as empresas que são hackeadas. Em fevereiro de 2016, um hacker publicou as informações pessoais de 20.000 funcionários do FBI (Federal Bureau of Investigation) dos EUA e 9.000 funcionários do Departamento de Segurança Interna (DHS) dos EUA. O hacker estava aparentemente motivado politicamente.

O worm Stuxnet foi projetado especificamente para impedir o progresso do Irã no enriquecimento de urânio que poderia ser usado em uma arma nuclear. Stuxnet é um excelente exemplo de um ataque de rede motivado por preocupações de segurança nacional. A guerra cibernética é uma possibilidade séria. Guerreiros hackers apoiados pelo Estado podem causar interrupção e destruição de serviços e recursos vitais dentro de uma nação inimiga. A Internet tornou-se essencial como meio de atividades comerciais e financeiras. A interrupção dessas atividades pode devastar a economia de uma nação. Controladores, semelhantes aos atacados por Stuxnet, também são usados para controlar o fluxo de água nas barragens e a troca de eletricidade na rede elétrica. Ataques a tais controladores podem ter consequências terríveis.

1.3.4

## Laboratório - Visualização dos Black Hats

Neste laboratório, você pesquisará e analisará incidentes de segurança cibernética para criar cenários como as organizações podem prevenir ou mitigar um ataque.

<https://shell.cloud.google.com/?pli=1&show=ide%2Cterminal>

# O Resumo do Perigo

1.4.1

## O que aprendi neste módulo?

**Histórias de guerra**

Os atores de ameaças podem sequestrar sessões bancárias e outras informações pessoais usando hotspots “gêmeos malvados”. Os atores de ameaças podem segmentar empresas, como no exemplo em que abrir um pdf no computador da empresa pode instalar ransomware. Nações inteiras podem ser alvo. Isso ocorreu no ataque de malware Stuxnet.

**Agentes da ameaça**

Os atores de ameaças incluem, entre outros, amadores, hacktivistas, grupos do crime organizado, patrocinados pelo Estado e grupos terroristas. O amador pode ter pouca ou nenhuma habilidade e muitas vezes usar informações encontradas na internet para lançar ataques. Hacktivistas são hackers que protestam contra uma variedade de ideias políticas e sociais. Grande parte da atividade de hacking é motivada pelo ganho financeiro. Os Estados-nação estão interessados em usar o ciberespaço para espionagem industrial. O roubo de propriedade intelectual pode dar a um país uma vantagem significativa no comércio internacional. À medida que a Internet das Coisas (IoT) se expande, webcams, roteadores e outros dispositivos em nossas casas também estão sob ataque.

**Impacto de ameaça**

Estima-se que as empresas percam mais de US$5 trilhões por ano até 2024 devido a ataques cibernéticos. As informações de identificação pessoal (PII), as informações de saúde protegidas (PHI) e as informações de segurança pessoal (PSI) são formas de informações protegidas que muitas vezes são roubadas. Uma empresa pode perder sua vantagem competitiva quando essas informações são roubadas, incluindo segredos comerciais. Além disso, os clientes perdem a confiança na capacidade da empresa de proteger seus dados. Os governos também foram vítimas de pirataria.