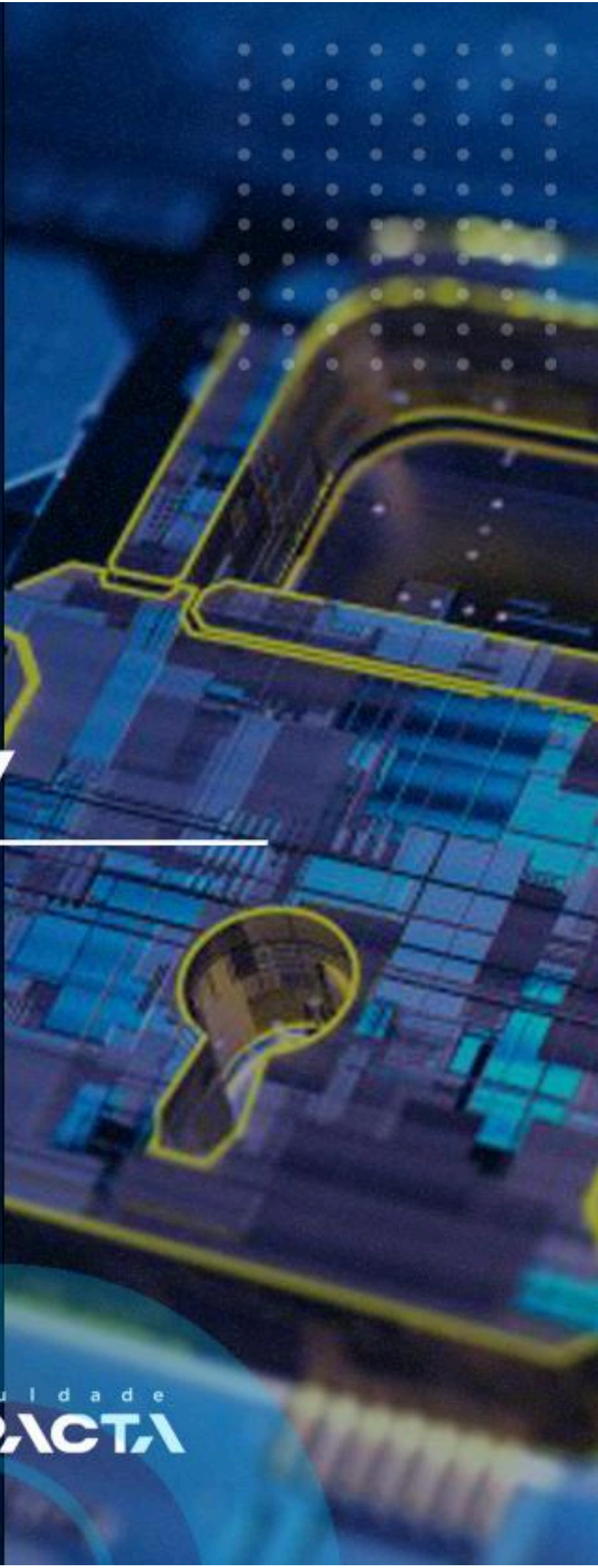
NEaD
Núcleo de Educação a Distância

CYBER SECURITY



Faculdade IMPACTA

7

Como as Redes de Computadores são Atacadas

Alex Sandro da Silva Feitosa

Resumo

Esta aula abordará tópicos fundamentais da segurança da informação, incluindo malwares, tráfego de redes, defesa da rede, controle de acesso, fontes de inteligência cibernética e criptografia. Serão discutidos os principais tipos de ameaças, suas formas de atuação e os mecanismos de defesa utilizados para proteger sistemas e dados. A abordagem visa fornecer uma visão geral dos principais conceitos e práticas de segurança, importantes para a proteção de ambientes computacionais.

Introdução

A segurança da informação é um campo cada vez mais relevante diante do crescimento das ameaças cibernéticas. Nesta aula, serão tratados aspectos fundamentais desse tema, começando pelos malwares — seus tipos, modos de propagação e impactos. Em seguida, será discutido o monitoramento do tráfego de rede como ferramenta para detectar comportamentos anômalos e ataques em andamento. Serão exploradas também estratégias de defesa, como firewalls, antivírus e sistemas de detecção e prevenção de intrusões. O controle de acesso será abordado com foco em garantir que apenas usuários autorizados tenham acesso a recursos específicos. Fontes de inteligência cibernética serão apresentadas como suporte à resposta a incidentes. Por fim, serão introduzidos os conceitos e técnicas de criptografia, fundamentais para proteger dados tanto em trânsito quanto em repouso.

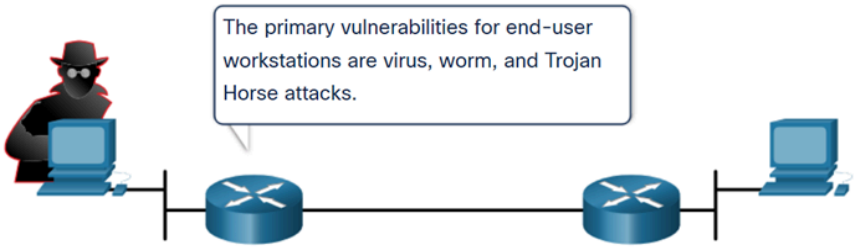
1.1. Evolução das Ameaças

1.1.1 Tipos de malwares

Malware é um código ou software malicioso desenvolvido com o objetivo de danificar, interromper, roubar informações ou realizar outras ações ilegítimas em dados, dispositivos ou redes. Entre os tipos mais comuns de malware, destacam-se os vírus, os

worms e os cavalos de Troia, cada um com características e métodos de propagação específicos.

Figura 1.1 Simbologias



Fonte: CCNA Cyber OPS Associate v1, 2020.

Vírus

Um vírus é um tipo de malware que se propaga ao inserir cópias de si mesmo em outros programas executáveis. Quando o programa infectado é executado, o vírus se ativa e pode se espalhar para outros computadores, comprometendo novos sistemas. Em sua forma mais simples, um vírus pode ser inserido logo na primeira linha de código de um arquivo executável. Seus efeitos variam: alguns são inofensivos, limitando-se a exibir mensagens ou imagens na tela, enquanto outros são altamente destrutivos, podendo modificar ou excluir arquivos armazenados no disco rígido. Os vírus costumam se disseminar por meio de mídias removíveis, como unidades USB, CDs e DVDs, além de compartilhamentos de rede e mensagens de e-mail — sendo os vírus transmitidos por e-mail uma das formas mais comuns de infecção.

Trojan

O malware Cavalo de Troia é um tipo de software que aparenta ser legítimo, mas contém código malicioso projetado para explorar os privilégios do usuário que o executa. Comumente, esses malwares são encontrados anexados a jogos online ou outros programas atrativos, nos quais os usuários são induzidos a fazer o download e executá-los em seus sistemas. O conceito de Cavalo de Tróia é bastante flexível: ele pode causar danos imediatos, permitir acesso remoto ao sistema ou abrir uma porta traseira (backdoor) para futuras invasões. Cavalos de Tróia desenvolvidos sob medida para alvos específicos tendem a ser difíceis de detectar. Em geral, eles são classificados com base nos danos que causam ou no método utilizado para comprometer o sistema.

Tabela 1.1 Os tipos de cavalos de Troia são os seguintes:

Tipo do Cavalo de Troia	Descrição
Acesso remoto	Permite acesso remoto não autorizado.
Envio de dados	Fornece ao agente da ameaça dados confidenciais, como senhas.
Destrutivo	Corrupta ou exclui arquivos.
Proxy	Usa o computador da vítima como dispositivo de origem para lançar ataques e realizar outras atividades ilegais.

FTP	Habilita serviços de transferência de arquivos não autorizados em dispositivos finais.
Desativador do software de segurança	Impede o funcionamento de programas antivírus ou firewalls.
Negação de Serviço (DoS)	Retarda ou interrompe a atividade da rede.
Agentes de log de digitação	Tenta ativamente roubar informações confidenciais, como números de cartão de crédito, gravando as teclas digitadas em um formulário da web.

Fonte: CCNA Cyber OPS Associate v1, 2020.

Worms Comuns

Worms de computador, ou vermes, são semelhantes aos vírus por também possuírem a capacidade de se replicar. No entanto, diferenciam-se por se propagarem de forma autônoma, explorando vulnerabilidades em redes, sem a necessidade de um programa hospedeiro. Essa capacidade faz com que possam se espalhar rapidamente entre sistemas, muitas vezes causando lentidão e sobrecarga nas redes. Um exemplo notável ocorreu em 2001, quando o worm Code Red infectou inicialmente 658 servidores e, em apenas 19 horas, já havia comprometido mais de 300.000 sistemas.

Outro caso emblemático foi o do SQL Slammer, apelidado de “o worm que comeu a internet”. Esse worm realizou um ataque de Negação de Serviço (DoS) explorando uma falha de estouro de buffer no Microsoft SQL Server. O número de servidores infectados dobrava a cada 8,5 segundos, comprometendo gravemente a estabilidade da rede global. A maioria dos sistemas afetados não possuía o patch de segurança que havia sido disponibilizado seis meses antes do ataque. Esse cenário evidencia a importância crítica de que organizações adotem políticas de segurança eficazes, garantindo a aplicação tempestiva de atualizações e correções de segurança.

Os três componentes do worm são os seguintes:

- Habilitando vulnerabilidade: Um worm se instala usando um mecanismo de exploração, como um anexo de e-mail, um arquivo executável ou um cavalo de Tróia, em um sistema vulnerável.
- Mecanismo de propagação: Depois de obter acesso a um dispositivo, o worm se replica e localiza novos alvos.
- Payload: Qualquer código malicioso que resulte em alguma ação é uma carga útil. Na maioria das vezes, isso é usado para criar um backdoor que permite que um ator de ameaça acesse o host infectado ou crie um ataque DoS.

Worms são programas autônomos projetados para explorar vulnerabilidades conhecidas em sistemas. Após uma exploração bem-sucedida, o worm se replica a partir do host de origem para o novo sistema comprometido, reiniciando o ciclo de infecção. Esse processo de propagação costuma ser executado de maneira furtiva, dificultando sua detecção por mecanismos de segurança convencionais.

Observação: Uma vez liberados na internet, os worms tendem a se espalhar indefinidamente. Eles continuam a propagar-se até que todos os sistemas vulneráveis tenham sido devidamente atualizados ou corrigidos.

Ransomware

Ransomware é um tipo de malware que bloqueia o acesso ao sistema infectado ou aos seus dados, geralmente exigindo um resgate (ransom) para restaurar o acesso. Esse bloqueio costuma ser realizado por meio de algoritmos de criptografia que codificam arquivos e informações armazenadas no dispositivo. Os vetores mais comuns para campanhas de ransomware incluem e-mails maliciosos e publicidade comprometida (conhecida como malvertising). Além disso, técnicas de engenharia social também são utilizadas: cibercriminosos se passam por técnicos de suporte e, por meio de ligações aleatórias, convencem usuários a acessar sites fraudulentos que instalam o ransomware no computador.

Outros malwares

Alguns exemplos de malware moderno são:

Scareware é um software fraudulento que utiliza técnicas de engenharia social para induzir medo ou ansiedade no usuário, criando a falsa percepção de que o sistema está sob ameaça. O objetivo é enganar usuários desavisados, persuadindo-os a tomar ações que, na verdade, resultam na instalação de malware ou na exposição do sistema a riscos reais.

Phishing é uma técnica que visa enganar pessoas para que revelem informações confidenciais, como senhas, números de cartão ou dados bancários. Um exemplo comum é o envio de e-mails que se passam por comunicações oficiais de instituições financeiras, solicitando que o usuário forneça seus dados de acesso ou PIN.

Rootkits são instalados em sistemas comprometidos e têm como principal função ocultar a presença de outros malwares, garantindo acesso privilegiado ao invasor. Uma vez instalado, o rootkit é extremamente difícil de detectar e permite que o atacante mantenha o controle do sistema de forma sigilosa.

Spyware é um tipo de malware projetado para coletar informações sobre o comportamento ou os dados de um usuário, enviando essas informações para terceiros sem o conhecimento ou consentimento da vítima. Ele pode se manifestar como monitor de sistema, cavalo de Troia, adware, cookies de rastreamento ou keyloggers — programas que registram tudo o que é digitado.

Adware é um software que exibe anúncios indesejados, como pop-ups, com o objetivo de gerar receita para seus criadores. Em alguns casos, esse malware também rastreia a atividade de navegação do usuário para exibir anúncios personalizados com base em seus interesses e sites visitados.

Comportamentos dos malwares:

Os computadores infectados com malware geralmente apresentam um ou mais dos seguintes sintomas:

- Aparência de arquivos, programas ou ícones da área de trabalho estranhos;

- Programas antivírus e de firewall estão desativando ou reconfigurando configurações;
- A tela do computador está congelando ou o sistema está travando;
- E-mails são enviados espontaneamente sem o seu conhecimento para a sua lista de contatos;
- Os arquivos foram modificados ou excluídos;
- Maior uso da CPU e/ou da memória;
- Problemas de conexão a redes;
- Velocidade lenta do computador ou do navegador da Web;
- Processos ou serviços desconhecidos em execução;
- Portas TCP ou UDP desconhecidas abertas;
- Conexões são feitas para hosts na Internet sem ação do usuário;
- Comportamento estranho do computador.

Observação: O comportamento de malware não se limita à lista acima.

1.1.2 Ataques comuns de reconhecimento, acesso e engenharia social

Malware é frequentemente utilizado como meio para entregar uma carga útil maliciosa (payload) a um sistema. Quando essa carga útil é instalada com sucesso, ela pode causar diversos danos à infraestrutura da rede de computadores, afetando tanto sistemas internos quanto externos da organização.

Os ataques a redes de computadores podem ser classificados em três categorias principais:

- Ataques de Reconhecimento
- Ataques de Acesso
- Ataques de DoS

Reconhecimento é a coleta de informações.

> Os autores de ameaças usam ataques de reconhecimento (ou recon) para fazer descobertas e mapeamentos não autorizados de sistemas, serviços ou vulnerabilidades.
> Os ataques Recon precedem ataques de acesso ou ataques DoS.
> As técnicas usadas por agentes de ameaças maliciosas para realizar ataques de reconhecimento são as seguintes (Cisco NetAcademy CCNA Cyber OPS Associate v1, 2021):

Tabela 1.2 Técnicas usadas por agentes de ameaças:

Técnicas	Descrição
Executar uma consulta de informações de um alvo	O agente da ameaça está procurando informações iniciais sobre um alvo. Várias ferramentas podem ser usadas, incluindo a pesquisa no Google, o site das organizações, whois e muito mais.
Iniciar uma varredura de ping da rede de destino	A consulta de informações geralmente revela o endereço de rede do alvo. O agente de ameaça agora pode iniciar uma varredura de ping para determinar quais endereços IP estão ativos.

Iniciar uma verificação de porta nos endereços IP ativos	Isso é usado para determinar quais portas ou serviços estão disponíveis. Exemplos de scanners de portas incluem Nmap, SuperScan, Angry IP Scanner e NetScanTools.
Execute o scanner de vulnerabilidades	Isso é para consultar as portas identificadas para determinar o tipo e a versão do aplicativo e do sistema operacional que está sendo executado no host. Exemplos de ferramentas incluem Nipper, Secuna PSI, Core Impact, Nessus v6, SAINT e Open VAS.
Execute ferramentas de exploração	O agente de ameaças agora tenta descobrir serviços vulneráveis que podem ser explorados. Existe uma variedade de ferramentas de exploração de vulnerabilidades, incluindo Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit e Netsparker.

Fonte:CCNA Cyber OPS Associate v1, 2020.

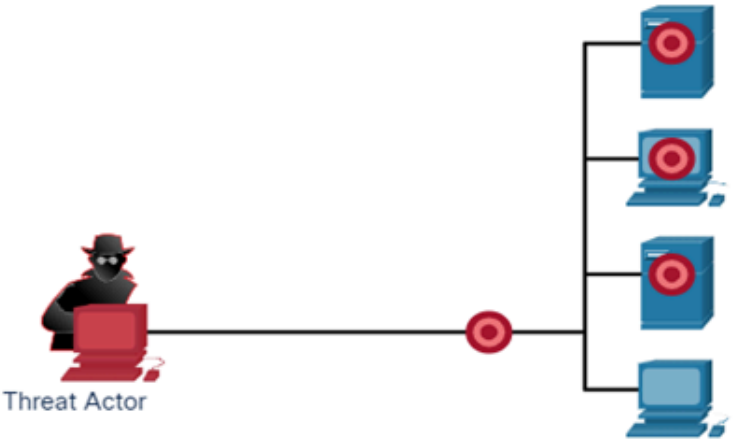
Consultas de informações da Internet:

Figura 1.2 Consultas

Fonte: CCNA Cyber OPS Associate v1, 2020.

Execução da varredura de ping:

Figura 1.3 Varredura de ping



Fonte: CCNA Cyber OPS Associate v1, 2020.

Executando a varredura da porta:

Figura 1.4 Varredura de porta

Fonte: CCNA Cyber OPS Associate v1, 2020.

Os ataques de acesso exploram vulnerabilidades conhecidas em serviços de autenticação, serviços de FTP e serviços da web para obter acesso a contas da web, bancos de dados confidenciais e outras informações confidenciais.

Ataques de senha

O ator da ameaça tenta descobrir senhas críticas do sistema usando uma variedade de ferramentas de quebra de senha (Cisco NetAcademy CCNA Cyber OPS Associate v1, 2021).

Ataques de falsificação (spoofing)

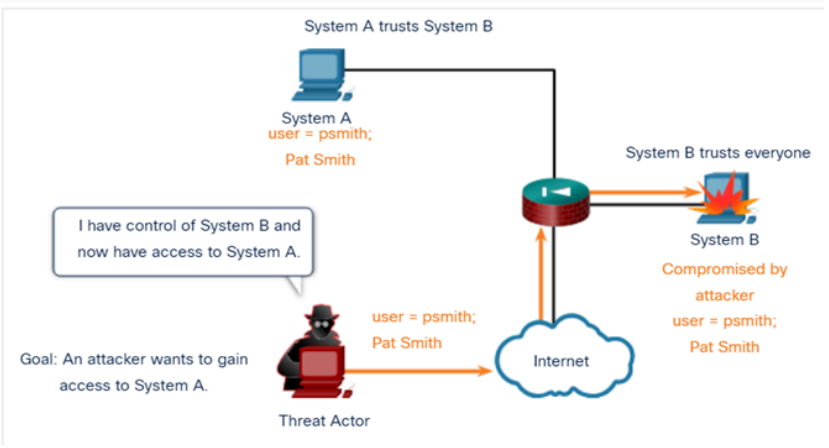
O equipamento utilizado por um ator da ameaça pode tentar se passar por um dispositivo legítimo por meio da falsificação de dados. Esse tipo de ataque visa enganar sistemas e dispositivos da rede, explorando falhas de autenticação e confiança.

Alguns dos ataques mais comuns incluem:

- Falsificação de IP (IP Spoofing): o invasor altera o endereço IP de origem em pacotes para parecer que vêm de uma fonte confiável.
- Falsificação de MAC (MAC Spoofing): o atacante modifica o endereço MAC de seu dispositivo para se passar por outro na rede.
- Falsificação de DHCP (DHCP Spoofing): envolve o envio de respostas DHCP falsas para redirecionar o tráfego de rede ou conceder configurações maliciosas aos dispositivos.
- Exploração de Confiança: o atacante se aproveita de relações de confiança entre sistemas para obter acesso não autorizado.
- Redirecionamento de Porta (Port Redirection): técnica usada para encaminhar o tráfego de uma porta de rede para outra, redirecionando informações para sistemas controlados pelo invasor.
- Ataque Man-in-the-Middle (MitM): o invasor intercepta e possivelmente altera comunicações entre duas partes sem que elas percebam.

- Ataque de Esgotamento de Buffer (Buffer Overflow): consiste em inserir mais dados do que um buffer pode suportar, sobrescrevendo áreas da memória e potencialmente executando código malicioso.

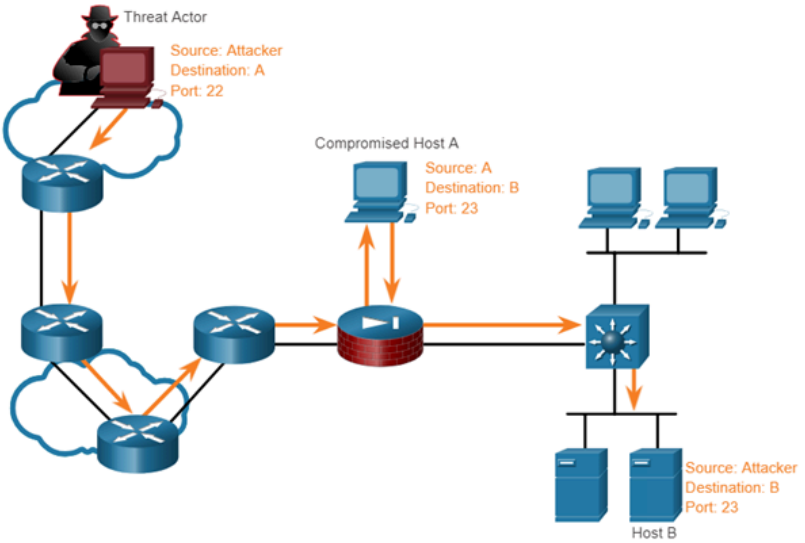
Figura 1.5 Exemplo de exploração de confiança



Fonte: CCNA Cyber OPS Associate v1, 2020.

Redirecionamento de porta Exemplo: O exemplo mostra um agente de ameaça usando SSH (porta 22) para se conectar a um Host A comprometido confiável pelo Host B. Portanto, o agente de ameaça pode usar Telnet (porta 23) para acessá-lo (Cisco NetAcademy CCNA Cyber OPS Associate v1, 2021).

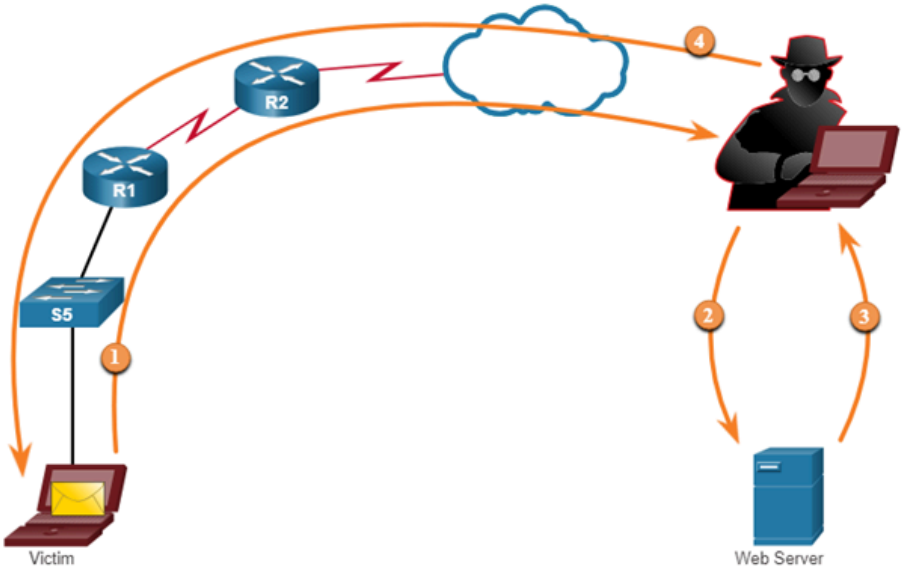
Figura 1.6 Redirecionamento de porta



Fonte: CCNA Cyber OPS Associate v1, 2020.

A figura mostra um exemplo de ataque man-in-the-middle.

Figura 1.7 Man-in-the-Middle



Fonte: CCNA Cyber OPS Associate v1, 2020.

Ataques de engenharia social

Engenharia Social é um ataque de acesso que tenta manipular os indivíduos para que realizem ações ou divulguem informações confidenciais.

Algumas técnicas de engenharia social são realizadas pessoalmente ou por telefone ou internet.

Técnicas de engenharia social são explicadas na tabela abaixo (Cisco NetAcademy CCNA Cyber OPS Associate v1, 2021).

Tabela 1.3 Técnicas de engenharia social:

Ataques de engenharia social	**Descrição**
Pretexting	Um ator de ameaça finge precisar de dados pessoais ou financeiros para confirmar a identidade do destinatário.
Phishing	Um agente de ameaças envia e-mails fraudulentos, disfarçados de fontes legítimas e confiáveis, para induzir o destinatário a instalar malware em seu dispositivo ou compartilhar informações pessoais ou financeiras.
Spear phishing	Um agente de ameaça cria um ataque de phishing direcionado, personalizado para um indivíduo ou organização específico.
Spam	Também conhecido como lixo eletrônico, este é um e-mail não solicitado que geralmente contém links prejudiciais, malware ou conteúdo enganoso.
Algo por Algo	Às vezes chamado de “quid pro quo”, é quando um ator de ameaça solicita informações pessoais de uma parte em troca de algo como um presente.
Iscas	Um agente de ameaça deixa uma unidade flash infectada por malware em um local público. Uma vítima encontra a unidade e a insere inconscientemente em seu laptop, instalando involuntariamente malware.
Representação	Nesse tipo de ataque, um ator de ameaça finge ser outra pessoa para ganhar a confiança da vítima.

Tailgating	É aqui que um agente de ameaças segue rapidamente uma pessoa autorizada para um local seguro para obter acesso a uma área segura.
Navegação bisbilhoteira	É aqui que um ator de ameaça olha discretamente por cima do ombro de alguém para roubar suas senhas ou outras informações.
Busca de informações na lixeira	É aqui que um ator de ameaças vasculha latas de lixo para descobrir documentos confidenciais.

Fonte:CCNA Cyber OPS Associate v1, 2020.

O Social Engineer Toolkit (SET) foi projetado para ajudar hackers de chapéu branco e outros profissionais de segurança de rede a criar ataques de engenharia social para testar suas próprias redes.
As empresas devem educar seus usuários sobre os riscos da engenharia social e desenvolver estratégias para validar identidades por telefone, via email ou pessoalmente (Cisco NetAcademy CCNA Cyber OPS Associate v1, 2021).

Figura 1.8 Práticas de proteção de Engenharia Social

Fonte: CCNA Cyber OPS Associate v1, 2020.

A segurança cibernética é tão robusta quanto o seu elo mais fraco — e, frequentemente, esse elo é representado pelas pessoas dentro da própria organização. A engenharia social continua sendo uma das maiores ameaças, explorando a confiança, o

erro humano e a falta de conscientização dos usuários para obter acesso não autorizado a sistemas e dados.

Uma das medidas de segurança mais eficazes que uma organização pode adotar é investir na capacitação de seus colaboradores, promovendo uma cultura organizacional voltada para a segurança da informação. Isso inclui treinamentos regulares, simulações de ataques, campanhas de conscientização e políticas claras sobre o uso seguro dos recursos digitais.

1.2. Vamos praticar

1.2.1 Pesquise e analise malware.

Histórico/Cenário

Malware, ou software malicioso, é um termo que abrange diversos tipos de programas desenvolvidos para causar danos a sistemas de computador, roubar dados ou contornar mecanismos de segurança. Além de comprometer dispositivos individuais, o malware pode atingir infraestruturas críticas, resultando em consequências graves, como a desativação de serviços de emergência, a produção de bens defeituosos em linhas de montagem, a paralisação de geradores elétricos ou a interrupção de sistemas de transporte.

Especialistas em segurança estimam que mais de um milhão de novas ameaças de malware são lançadas diariamente. O Relatório de Ameaças do McAfee Labs 2019 destacou tendências preocupantes, como o surgimento de novas técnicas de ransomware, vazamentos em massa de dados contendo bilhões de contas, exploração de vulnerabilidades em conexões HTTP, falhas em plataformas amplamente utilizadas como Windows, Microsoft Office e Apple iOS, além de ataques direcionados a dispositivos IoT pessoais.

Para acessar os dados mais recentes, recomenda-se buscar na internet pela versão atualizada do Relatório de Ameaças do McAfee Labs.

Recursos necessários

Um computador ou dispositivo móvel com acesso à internet.

Instruções

Faça uma pesquisa de malware recente:

a. Usando seu mecanismo de pesquisa favorito, realize uma pesquisa sobre malwares recentes. Durante a pesquisa, escolha quatro exemplos de malware, sendo cada um de um tipo diferente, e esteja preparado para discutir os seguintes aspectos de cada um:

- O que o malware faz;
- Como ele é transmitido;
- Qual o impacto que ele causa.

Exemplos de tipos de malware incluem: Ransomware, Trojan, Hoax, Adware, Malware em geral, PUP (Programas Potencialmente Indesejados), Exploit, Exploit Kit e Vulnerability (Vulnerabilidade explorada).

Você pode encontrar informações úteis sobre malware visitando os seguintes sites, utilizando os termos de pesquisa sugeridos:

- Painel do Cenário de Ameaças do McAfee Threat Center
- Centro de Ameaças do Malwarebytes Labs – "10 Principais Malwares"
- SecurityWeek.com > Ameaças de Vírus > Malware
- TechNewsworld.com > Segurança > Malware

b. Leia as informações sobre o malware encontrado em sua pesquisa escolha um dos malwares identificados e escreva um breve resumo explicativo, abordando:

- Suas funcionalidades maliciosas;
- Seu método de propagação
- E os danos ou consequências causadas ao sistema ou à organização.

1.2.2 Pesquise e identifique ataques de engenharia social

Histórico/Cenário

A engenharia social é um tipo de ataque cujo objetivo é induzir a vítima a fornecer informações pessoais ou confidenciais. Esse ataque pode ser realizado por um invasor por meio de ferramentas como keyloggers, e-mails de phishing ou até mesmo através de abordagens diretas e pessoais. Este laboratório exige a pesquisa sobre engenharia social, bem como a identificação de formas de reconhecê-la e preveni-la.

Recursos necessários

Um computador ou dispositivo móvel com acesso à internet.

Instruções

Usando um navegador da web, localize o artigo "Métodos para entender e reduzir ataques de engenharia social" no site do SANS Institute. O artigo deve ser facilmente encontrado por meio de um motor de busca.

O SANS Institute é uma organização cooperativa de pesquisa e educação que oferece treinamento e certificação em segurança da informação. O SANS Reading Room possui diversos artigos relevantes para a prática da análise em segurança cibernética. Você pode participar da comunidade SANS criando uma conta gratuita para acessar os artigos mais recentes, ou acessar artigos mais antigos sem a necessidade de cadastro.

Leia o artigo indicado ou escolha outro artigo relacionado à engenharia social. Após a leitura, responda às seguintes perguntas:

Perguntas:

a) Quais são os três métodos usados em engenharia social para obter acesso às informações?

As respostas devem incluir: acesso eletrônico, acesso físico e mídias sociais.

b) Quais são três exemplos de ataques de engenharia social relacionados aos dois primeiros métodos citados na pergunta anterior?

As respostas podem incluir, por exemplo: spear phishing por e-mail, isca com conteúdo desejado ou utilização não autorizada.

c) Por que as redes sociais representam uma ameaça no contexto da engenharia social?

As respostas devem incluir que as redes sociais incentivam as pessoas a compartilhar informações pessoais, interesses e hábitos, como nome completo, data de nascimento, cidade natal, entre outros.

d) Como uma organização pode se proteger contra ataques de engenharia social?

As respostas devem mencionar a criação e a implementação de treinamentos de conscientização em segurança.

e) O que é o SANS Institute, autor deste artigo?

As respostas devem ser baseadas no conteúdo do site https://www.sans.org, destacando que o SANS Institute é um fornecedor de treinamento e certificação em segurança da informação.

Conclusão

A engenharia social é uma ameaça significativa à segurança cibernética, pois explora a confiança e o comportamento humano para obter acesso a informações sensíveis. Métodos variados, como ataques eletrônicos, invasões físicas e o uso de mídias sociais, demonstram como os invasores podem se aproveitar de diferentes vetores para alcançar seus objetivos. As redes sociais, em particular, amplificam os riscos ao incentivar o compartilhamento de dados pessoais, facilitando o trabalho dos agentes mal-intencionados. Para mitigar esses riscos, é fundamental que as organizações invistam em treinamentos de conscientização em segurança, fortalecendo a cultura de prevenção entre seus colaboradores. Instituições como o SANS Institute desempenham um papel essencial ao fornecer recursos educacionais e certificações que capacitam profissionais para enfrentar esses desafios. Assim, a combinação de conhecimento, vigilância e práticas de segurança torna-se imprescindível para reduzir os impactos dos ataques de engenharia social.

Referências

Cisco Systems. **Cisco Networking Academy Program CCNA CyberOps Associate** v1, 2020. Disponível em: <https://www.netacad.com>.

SÊMOLA, Marcos. **Gestão da segurança da informação**. Rio de Janeiro: Campus, 2003.

NAKAMURA, Emilio Tissato. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec, 2007.

THOMAS, Tom. **Segurança de redes**: primeiros passos. Tradução de Flávio MORGADO. Rio de Janeiro: Ciência Moderna, 2007.

BEAL, A. **Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações**. São Paulo: Atlas, 2005.

STALLINGS, W. **Network security**: applications and standards. 3.nd. New Jersey: Prentice Hall, 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001 E 27002** Tecnologia da informação.

WADLOW, Thomas A. **Segurança de redes**: projeto e gerenciamento de redes seguras. Rio de Janeiro: Campus, 2000.