Packet Tracer - Investigue um cenário de ameaças

# Objetivos

Parte 1: Investigar uma vulnerabilidade de configuração de rede

Parte 2: Investigue uma vulnerabilidade de malware de phishing

Parte 3: Investigar uma vulnerabilidade de rede sem fio e DNS

# Histórico/Cenário

O cenário de ameaças consiste em todas as vulnerabilidades que podem ser exploradas pelos agentes de ameaças. Cada incidente de segurança digital envolve a exploração de vulnerabilidades por diferentes tipos de agentes de ameaça. Alguns agentes de ameaças querem dinheiro, outros querem ser famosos e outros querem destruir informações e infraestrutura.

Nesta atividade, você investigará três vulnerabilidades que podem ser exploradas por agentes de ameaças.

**Observação**: nessa atividade, os **Data Centers** e sites de **ISP/Telco** estão bloqueados.

# Instruções

## Parte 1: Investigar uma vulnerabilidade de configuração de rede

Às vezes, as vulnerabilidades de segurança da rede podem acontecer por acidente. Por exemplo, esquecer de atualizar o software do servidor ou host pode expor vulnerabilidades conhecidas que poderiam ser facilmente mitigadas com uma atualização simples. Da mesma forma, vulnerabilidades podem ser introduzidas quando um dispositivo de rede não está configurado corretamente ou um dispositivo está com defeito. Nesta parte, você explorará uma vulnerabilidade resultante de um dispositivo que não está configurado corretamente com as melhores práticas de segurança.

### Etapa 1: usar uma rede de convidados para obter acesso a outros dispositivos na rede.

a.     Em Greenville, localize o Smartphone 3 fora da localidade Home.

Maria é a proprietária do smartphone. Ela é uma amiga de Bob que mora na casa. Mary está estudando para conseguir um emprego na defesa de segurança digital e está familiarizada com o teste de penetração de rede. Ela percebeu que uma rede sem fio de convidado é aberta e acessível por qualquer pessoa. Ela se conectou à rede de convidados e usou o Nmap para executar uma verificação, que pode identificar e descobrir detalhes sobre todos os dispositivos ativos. Um dos dispositivos parece ser uma webcam. O endereço IP é 192.168.100.101.

b.     Clique em Smartphone 3 e, em seguida, clique em Prompt de comando. Digite o comando ping **192.168.100.101**. Após uma ou duas mensagens de "Solicitação expirarem", os pings restantes devem ser bem-sucedidos.

Mary informa Bob que a rede está muito vulnerável a ataques. Alguém pode assumir o controle da webcam, por exemplo, e assistir o vídeo de dentro da casa. Bob convida Mary para entrar, investigar o problema e propor uma solução.

### Etapa 2: Explore a rede doméstica para identificar a vulnerabilidade.

a.     Clique em Início. Sabendo que os roteadores domésticos normalmente controlam as redes sem fio domésticas, Mary vai direto para o escritório e fica atrás da mesa. Ela usará o PC do Home Office para se conectar ao roteador. Mas primeiro ela precisa determinar o endereço IP.

b.     Clique em Home Office PC > Desktop > Prompt de comandoe digite o comando ipconfig.

O gateway padrão é o endereço IP do Roteador sem fio doméstico.

#### Pergunta:

Qual é o endereço IP usado?

Digite suas respostas aqui.

c.     Em seguida, Mary usa o Navegador da Web para se conectar ao Roteador sem fio doméstico. Feche o Prompt de Comando e clique em Navegador da Web. Insira o endereço IP do gateway padrão.

d.     Bob não tem a documentação para o roteador nem conhece as credenciais de login. Mary consulta o modelo de roteador na Internet e descobre que as credenciais padrão usam admin para nome de usuário e senha. Faça login no Roteador sem fio doméstico.

e.     Clique em Conexão sem fio. Analise as configurações básicas da rede sem fio para cada um dos três rádios que fazem parte do roteador sem fio.

#### Perguntas:

Quais das bandas estão ativas?

Digite suas respostas aqui.

Quais são os SSIDs atribuídos a esses rádios?

Digite suas respostas aqui.

f.      Clique no submenu Segurança sem fio

#### Pergunta:

A segurança está ativada para cada um dos rádios? As senhas estão definidas?

Digite suas respostas aqui.

g.     Mary conseguiu acessar a rede de fora sem fazer login; portanto, ela investiga mais. Clique no submenu Guest Network (Rede de convidados) e investigue as configurações.

#### Pergunta:

A rede Guest está ativa? Em caso afirmativo, em qual rádio?

Digite suas respostas aqui.

Uma rede sem fio Guest deve fornecer acesso à Internet apenas para convidados. Ele não deve permitir que os convidados acessem os dispositivos na rede local dentro de casa. Nesse caso, os convidados podem acessar a rede local. Isso indica que o roteador doméstico está configurado incorretamente.

#### Pergunta:

O que você sugeriria que Bob fizesse para proteger essa rede?

Digite suas respostas aqui.

## Parte 2: Investigue uma vulnerabilidade de malware de phishing

Phishing é um tipo de ataque de engenharia social em que um agente de ameaças se disfarça como uma fonte legítima e confiável para induzi-lo a instalar malware no dispositivo ou compartilhar informações pessoais ou financeiras. Os ataques de phishing normalmente ocorrem por e-mails ou telefonemas. Ao contrário de outras vulnerabilidades de rede, a principal vulnerabilidade em ataques de phishing são os usuários da rede. Por esse motivo, uma defesa importante contra o phishing é treinar os usuários sobre como evitar explorações de phishing.

Nesta parte, você simulará e investigará um ataque de phishing.

**Observação**: esta atividade é apenas para fins de demonstração. Escrever e enviar mensagens de e-mail de phishing é antiético e é considerado um ataque criminoso na maioria das jurisdições.

### Etapa 1: Agir como um agente de ameaças e criar um e-mail de phishing.

a.     Navegue até a rede Cafe.

b.     Clique na guia Cafe Hacker Laptop > Área de trabalho > E-mail.

c.     Clique em Escrever.

Use sua imaginação para escrever um e-mail de phishing. Seu objetivo é persuadir o usuário a copiar e colar uma URL da mensagem de e-mail no navegador. Inclua o link **pix.example.com** no e-mail. Você pode procurar, por exemplo, e-mails de phishing on-line para ver como agentes de ameaças gravam esse tipo de e-mail.

**Observação**: os links em e-mails de phishing normalmente são ativos ou "ativos". Tudo o que a vítima precisa fazer é clicar. No entanto, o Packet Tracer não é compatível com o uso de links ativos dentro do cliente de e-mail.

d.     Envie seu e-mail para três pessoas dentro da rede Filial. Seus endereços de e-mail são os seguintes:

o    user1@mail.isp.net

o    user2@mail.isp.net

o    user3@mail.isp.net

### Etapa 2: abrir os e-mails recebidos do agente de ameaças.

a.     Navegue até a rede Filial.

b.     Clique em um dos dispositivos, PC-BR1, Laptop BR-1 ou Laptop BR-2.

c.     Clique na guia Desktop (Área de Trabalho)e depois clique em E-mail e clique em Receber. Você deve receber o e-mail que acabou de enviar.

**Observação**: o Packet Tracer pode levar vários segundos para convergir. Você pode precisar clicar em Receber várias vezes se o e-mail não for recuperado.

d.     Opcional: acesse outros dispositivos da vítima, abra o cliente de E-mail e clique em Receber para verificar se eles também receberam seu e-mail de phishing.

### Etapa 3: Se passar por vítima e seguir as instruções de phishing.

a.     Leia o e-mail e copie o endereço do site.

b.     Feche a janela Navegador de email e clique em Navegador da Web.

c.     Cole a URL no campo URL e, em seguida, clique em Ir.

**Observação**: o Packet Tracer pode levar vários segundos para convergir. Você pode clicar em Fast Forward Time para acelerar o processo.

#### Perguntas:

O que aconteceu quando a página da Web foi carregada?

Digite suas respostas aqui.

Que tipo de ataque é esse?

Digite suas respostas aqui.

Em uma situação do mundo real, esse e-mail é normalmente espalhado por um vírus que envia automaticamente e-mails mal-intencionados para todos os endereços na sua lista de contatos.

#### Pergunta:

Descreva os danos que esse tipo de ataque pode causar em uma empresa?

Digite suas respostas aqui.

Os funcionários devem ser treinados para identificar e-mails de phishing e as ações que devem ser tomadas para evitar danos. Além disso, as empresas podem configurar firewalls, sistemas de prevenção contra invasões e outros dispositivos de segurança e software para bloquear e-mails de phishing antes de entrar na rede. Algumas empresas assinam serviços que compilam e mantêm listas de sites mal-intencionados. Os dispositivos de segurança da empresa podem, então, usar essas listas para atualizar automaticamente os filtros para bloquear o tráfego mal-intencionado.

## Parte 3: Investigar uma vulnerabilidade de rede sem fio e DNS

O usuário médio de rede tende a confiar em redes Wi-Fi abertas em locais públicos. Ao usar o Wi-Fi, os serviços de dados por celular podem proporcionar taxas de dados mais rápidas e ser mais econômicos. No entanto, os agentes de ameaças podem configurar um laptop com uma interface Wi-Fi que possa atuar como um ponto de acesso Wi-Fi e um cliente Wi-Fi. Isso significa que os agentes de ameaças podem criar suas próprias redes sem fio e transmitir um SSID convincente para possíveis vítimas em locais públicos. Os agentes de ameaças usam esses access points não autorizados para criar ataques de interferência principal. Nesse ataque, os agentes de ameaças podem capturar e ler todo o tráfego sem fio de dispositivos que se associam ao access point não autorizado, potencialmente aprendendo nomes de usuário, senhas e outras informações confidenciais.

Nesta parte, você investigará como um access point não autorizado pode ser usado para motivar usuários a se conectarem a uma rede sem fio falsa. Quando combinados com serviços de rede como DHCP e DNS, os usuários podem se tornar vítimas de ataques mal-intencionados a sites por meio de sequestro de DNS.

### Etapa 1: Conectar-se à rede sem fio do agente de ameaças.

a.     Navegue até a rede Cafe. Observe o agente de ameaças sentado no canto.

b.     Clique na Hacker Backpack e investigue o conteúdo. Ele tem um roteador sem fio e um sniffer de rede. Seu objetivo é interceptar o tráfego de usuários e direcioná-lo para um servidor mal-intencionado.

c.     Volte para o Café e clique no laptop Café do cliente > Desktop> aplicativo PC Wireless.

d.    Clique na guia Connect. Talvez seja necessário clicar em Atualizar para ver a lista de redes sem fio disponíveis.

#### Pergunta:

Se você estivesse no Café, a qual rede sem fio você escolheria se conectar? Explique.

Digite suas respostas aqui.

e.     Clique em qualquer um dos nomes de rede Cafe\_WI-FI\_FAST e clique em **Connect**.

### Etapa 2: Visite seu site de mídia social favorito.

a.     Feche o aplicativo PC Wireless e clique em Navegador da Web.

b.     No campo URL, digite friends.example.com e clique em Ir. Este site é uma rede social legítima nessa simulação.

#### Perguntas:

O que aconteceu?

Digite suas respostas aqui.

Qual era a URL do servidor de malware usada no cenário de ataque de phishing? É a mesma coisa?

Digite suas respostas aqui.

### Etapa 3: Investigar a origem do ataque.

a.     Feche o navegador da Web e clique em Configuração de IP.

b.     No Café, clique em VPN Laptop > Desktop > Configuração de IP.

c.     Clique em Café do cliente na barra de tarefas para trazê-lo de volta à vista e, em seguida, organizar as duas janelas de Configuração de IP lado a lado. Compare os valores entre os dois dispositivos.

#### Perguntas:

Quais são as diferenças entre os endereços dos dois notebooks?

Digite suas respostas aqui.

d.     Investigue o laptop Cafe Hacker.

#### Pergunta:

Qual é o seu endereço IP? Por que isso é significativo?

Digite suas respostas aqui.

No laptop Cafe Hacker, clique na guia Serviços > DNS.

e.     Localize o nome do site friends.example.com. Observe que o endereço IP é o mesmo endereço IP associado a pix.example.com do ataque de phishing anteriormente.

f.      Em Serviços, clique em DHCP. Observe que o endereço do servidor DNS distribuído para os hosts pelo DHCP é o mesmo atribuído ao cliente do Cafe.

#### Pergunta:

Quais são as etapas desse ataque?

Digite suas respostas aqui.

# Resumo

Nesta atividade, analisamos três maneiras diferentes pelas quais as vulnerabilidades podem gerar explorações. Como um usuário de rede ou profissional de segurança digital informado, é de sua responsabilidade pensar nas diferentes maneiras pelas quais essas vulnerabilidades podem ser detectadas e mitigadas antes que ocorra um ataque digital.

Fim do documento