**Atividade: Analisar ataques de rede**

Nesta atividade, você considerará um cenário envolvendo um cliente da empresa para a qual você trabalha que enfrenta um problema de segurança ao acessar o site da empresa. Você identificará a causa provável da interrupção do serviço. A seguir, você explicará como ocorreu o ataque e o impacto negativo que teve no site.

**Cenário**

Você trabalha como analista de segurança em uma agência de viagens que anuncia vendas e promoções no site da empresa. Os funcionários da empresa acessam regularmente a página de vendas da empresa para pesquisar pacotes de férias de que seus clientes possam gostar.

Uma tarde, você recebe um alerta automático do seu sistema de monitoramento indicando um problema com o servidor web. Você tenta visitar o site da empresa, mas recebe uma mensagem de erro de tempo limite de conexão em seu navegador.

Você usa um sniffer de pacotes para capturar pacotes de dados em trânsito de e para o servidor web. Você percebe um grande número de solicitações TCP SYN provenientes de um endereço IP desconhecido. O servidor web parece estar sobrecarregado com o volume de tráfego de entrada e está perdendo a capacidade de responder ao número anormalmente grande de solicitações SYN. Você suspeita que o servidor esteja sob ataque de um atacante.

Você coloca o servidor off-line temporariamente para que a máquina possa se recuperar e retornar ao status operacional normal. Você também configura o firewall da empresa para bloquear o endereço IP que estava enviando o número anormal de solicitações SYN. Você sabe que sua solução de bloqueio de IP não durará muito, pois um invasor pode falsificar outros endereços IP para contornar esse bloqueio. Você precisa alertar seu gerente sobre esse problema rapidamente e discutir as próximas etapas para impedir esse invasor e evitar que esse problema aconteça novamente. Você precisará estar preparado para contar ao seu chefe o tipo de ataque que descobriu e como ele estava afetando o servidor web e os funcionários.

**Passo 1: Acesse o modelo**

Arquivo “*Cybersecurity Incident Report*”

**Passo 2: Acessar os materiais de suporte**

Arquivo “*2 SUPPORT How to read a Wireshark TCP\_HTTP log”*

Como ler um log TCP\_HTTP Wireshark

**Passo 3: Identificar o tipo de ataque que está causando a interrupção da rede**

Reflita sobre os tipos de ataques de intrusão de rede que você aprendeu neste curso até agora. Como analista de segurança, identificar o tipo de ataque à rede com base no incidente é o primeiro passo para gerenciar o ataque e prevenir ataques semelhantes no futuro.

Aqui estão algumas questões a serem consideradas ao determinar que tipo de ataque ocorreu:

* O que você entende atualmente sobre ataques de rede?
* Que tipo de ataque provavelmente resultaria nos sintomas descritos no cenário?
* Qual é a diferença entre negação de serviço (DoS) e negação de serviço distribuída (DDoS)?
* Por que o site está demorando muito para carregar e reportando um erro de tempo limite de conexão?

Revise a leitura do Wireshark na etapa 2 e tente identificar padrões no tráfego de rede registrado. Analise os padrões para determinar que tipo de ataque à rede ocorreu. Escreva sua análise na seção um do modelo de relatório de incidente de segurança cibernética fornecido.

**Passo 4: Explique como o ataque está causando o mau funcionamento do site**

Revise a leitura do Wireshark na etapa 2 e, em seguida, escreva sua análise na seção dois do modelo de relatório de incidente de segurança cibernética fornecido.

Ao escrever seu relatório, discuta os dispositivos de rede e as atividades envolvidas na interrupção. Inclua as seguintes informações em sua explicação:

* Descreva o ataque. Quais são os principais sintomas ou características deste tipo específico de ataque?
* Explique como isso afetou a rede da organização. Como esse ataque específico à rede afeta o site e como ele funciona?
* Descreva as consequências potenciais deste ataque e como ele afeta negativamente a organização.

Opcional: sugira possíveis formas de proteger a rede para que esse ataque possa ser evitado no futuro.

**O que incluir em sua resposta**

Certifique-se de abordar o seguinte em sua atividade concluída:

* O nome do ataque de intrusão de rede
* Uma descrição de como o ataque impacta negativamente o desempenho da rede

**Avaliação do Exemplo**

Compare o exemplar com sua atividade concluída. Revise seu trabalho usando cada um dos critérios do exemplar. O que você fez bem? Onde você pode melhorar? Use suas respostas a essas perguntas para orientá-lo à medida que avança no curso.

Nota: O exemplar representa uma possível explicação para os problemas que o usuário está enfrentando. O seu provavelmente será diferente em alguns aspectos. O importante é que você identificou os protocolos de rede envolvidos e criou um relatório. Em sua função como analista de segurança, você e sua equipe fariam uma estimativa melhor sobre o que aconteceu e, em seguida, investigariam mais a fundo para solucionar o problema e fortalecer a segurança geral de sua rede.

O exemplo identifica que a mensagem de tempo limite de conexão é resultado de um ataque DoS. Neste caso, o ataque DoS específico é um ataque de inundação SYN.

Para determinar isso, analise os dados apresentados no trecho do arquivo de log anexado a esta atividade. A seguir, reflita sobre seu entendimento atual sobre ataques de rede para identificar que tipo de ataque está ocorrendo com base nos dados disponíveis.

Depois de identificar um possível tipo de ataque à rede, explique como identificamos o ataque. Em seguida, documente como esse tipo específico de ataque pode ter afetado a rede e inclua uma descrição geral de como o invasor explorou a vulnerabilidade da rede.

Por último, descreva como esse ataque resultou na exibição do erro de tempo limite de conexão na página da web.

O exemplar fornece apenas um exemplo de explicação para o evento. Descrever um evento normalmente requer apresentar suas evidências e explicar como você tomou sua decisão. Todos os padrões que você observa nos logs e dados são essenciais para determinar a origem e o tipo de ataque à rede. Quanto mais prática você tiver na identificação desses padrões, mais fácil será detectar ataques à rede à medida que eles ocorrem. Isso permitirá que você responda a incidentes com mais rapidez e eficiência.