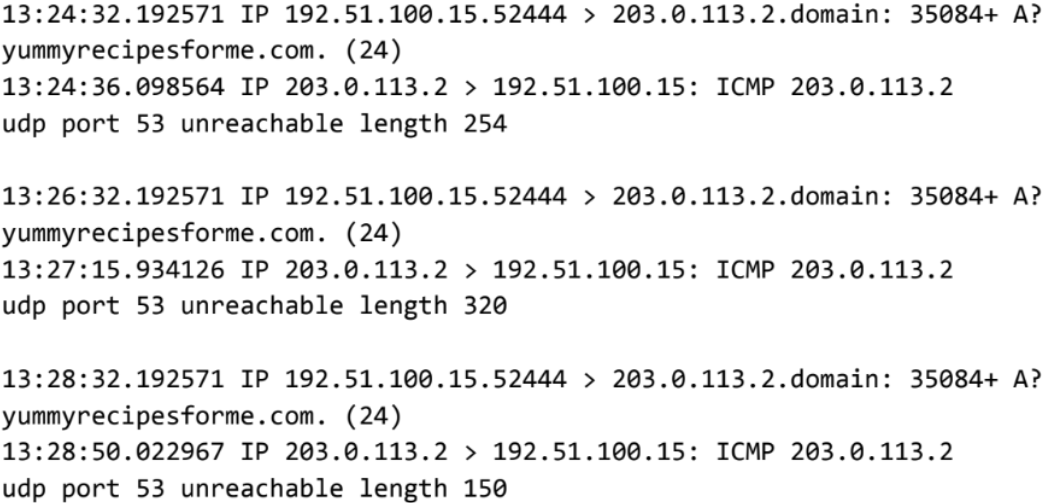
**Atividade: Analisar a comunicação da camada de rede**

**Cenário**

Você é analista de segurança cibernética e trabalha em uma empresa especializada na prestação de serviços de consultoria de TI. Vários clientes entraram em contato com sua empresa para relatar que não conseguiram acessar o site da empresa *www.yummyrecipesforme.com* e viram o erro de porta de destino inacessível após aguardar o carregamento da página.

Você tem a tarefa de analisar a situação e determinar qual protocolo de rede foi afetado durante o incidente. Para começar, você visita o site e também recebe o erro de porta de destino inacessível. Em seguida, você carrega sua ferramenta de análise de rede, **tcpdump**, e carrega a página da web novamente. Desta vez, você recebe muitos pacotes no seu analisador de rede. O analisador mostra que quando você envia pacotes UDP e recebe uma resposta ICMP retornada ao seu host, os resultados contêm uma mensagem de erro: “*udp port 53 unreachable*”.



No log DNS e ICMP, você encontra as seguintes informações:

1. Nas duas primeiras linhas do arquivo de log, você vê a solicitação inicial de saída do seu computador para o servidor DNS solicitando o endereço IP de *yummyrecipesforme.com*. Esta solicitação é enviada em um pacote UDP.
2. A seguir você encontra carimbos de data/hora que indicam quando o evento aconteceu. No log, esta é a primeira sequência de números exibida. Por exemplo: 13:24:32.192571. Isso exibe a hora 13h24, 32,192571 segundos.
3. O endereço IP de origem e destino é o próximo. No log de erros, essas informações são exibidas como: 192.51.100.15.52444 > 203.0.113.2.domain. O endereço IP à esquerda do símbolo de maior que (>) é o endereço de origem. Neste exemplo, a fonte é o endereço IP do seu computador. O endereço IP à direita do símbolo maior que (>) é o endereço IP de destino. Neste caso, é o endereço IP do servidor DNS: 203.0.113.2.domain
4. A segunda e terceira linhas do log mostram a resposta à sua solicitação inicial do pacote ICMP. Nesse caso, a linha ICMP 203.0.113.2 é o início da mensagem de erro indicando que o pacote ICMP não pôde ser entregue à porta do servidor DNS.
5. A seguir estão o protocolo e o número da porta, que exibe qual protocolo foi usado para lidar com as comunicações e para qual porta foi entregue. No log de erros, isso aparece como: porta udp 53 unreachable. Isso significa que o protocolo UDP foi usado para solicitar uma resolução de nome de domínio usando o endereço do servidor DNS na porta 53. A porta 53, que se alinha à extensão .domain em 203.0.113.2.domain, é uma porta bem conhecida para serviço DNS. A palavra “unreachable” na mensagem indica que a mensagem não foi enviada para o servidor DNS. Seu navegador não conseguiu obter o endereço IP de yummyrecipesforme.com, necessário para acessar o site porque nenhum serviço estava executando na porta DNS de recebimento, conforme indicado pela mensagem de erro ICMP “udp port 53 unreachable”.
6. As linhas restantes no log indicam que os pacotes ICMP foram enviados mais duas vezes, mas o mesmo erro de entrega foi recebido nas duas vezes.

Agora que você capturou pacotes de dados usando uma ferramenta de análise de rede, é sua tarefa identificar quais protocolos e serviços de rede foram afetados por esse incidente. Em seguida, você precisará escrever um relatório de acompanhamento.

Como analista, você pode inspecionar o tráfego e os dados da rede para determinar o que está causando problemas relacionados à rede durante incidentes de segurança cibernética. Posteriormente neste curso, você demonstrará como gerenciar e resolver incidentes. Por enquanto, basta analisar a situação.

Enquanto isso, esse incidente está sendo tratado por engenheiros de segurança depois que você e outros analistas relataram o problema ao seu supervisor direto.

**Passo 1: Acesse o modelo**

Use os iniciadores de frases e instruções fornecidas no modelo para apoiar seu pensamento e garantir que você inclua todos os detalhes relevantes sobre o incidente.

Arquivo “*Relatório de incidentes de segurança cibernética*”

**Passo 2: Acesse materiais de apoio**

Os seguintes materiais de apoio irão ajudá-lo a completar esta atividade. Mantenha-os abertos enquanto avança para as próximas etapas.

Arquivo “*2* *EXEMPLO Relatório de incidentes de segurança cibernética*”

**O que incluir em sua resposta**

Certifique-se de abordar os seguintes itens em sua atividade concluída:

* Forneça um resumo do problema encontrado no log de tráfego DNS e ICMP
* Explique sua análise dos dados e forneça uma possível causa do incidente

**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 exemplo oferece uma abordagem possível para investigar e analisar um possível evento de segurança. 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.

Escrever um relatório de análise de segurança cibernética eficaz pode ajudar a solucionar problemas e vulnerabilidades de rede de maneira mais rápida e eficaz. Quanto mais prática você tiver na análise do tráfego de rede em busca de tendências e atividades suspeitas, mais eficazes você e sua equipe serão no gerenciamento e na resposta aos riscos presentes em sua rede.

**Principais conclusões**

Como analista de segurança, você nem sempre sabe exatamente o que está na origem de um problema de rede ou de um possível ataque. Mas ser capaz de analisar os pacotes IP envolvidos ajudará você a adivinhar melhor o que aconteceu ou potencialmente impedir que um ataque invada a rede. O protocolo de rede e os logs de tráfego se tornarão o ponto de partida para investigar mais a fundo o problema e resolver o ataque.