Relatório de incidente de segurança cibernética

Análise de tráfego de rede

Introdução

Objetivo desse projeto é analisar o **relatório** apresentado pelo curso e atribuir os problemas e soluções. A primeira parte é fornecer um resumo do problema encontrado no DNS e no ICMP registro de tráfego, E uma segunda parte que serve para explicar sua análise dos dados e forneça pelo menos uma causa do incidente.

Cenário

Analise o cenário abaixo. Em seguida, conclua as instruções passo a passo.
Você é um analista de segurança cibernética que trabalha em uma empresa especializada na prestação de serviços de TI para clientes. Vários clientes de clientes relataram que não conseguiram acessar o site da empresa cliente www.yummyrecipesforme.com, e viram o erro "porta de destino inacessível" depois de esperar que a página carregasse.
Você tem a tarefa de analisar a situação e determinar qual protocolo de rede foi afetado durante esse incidente. Para começar, você tenta visitar o site e também recebe o erro "porta de destino inacessível". Para solucionar o problema, carregue a ferramenta do analisador de rede, tcpdump, e tente carregar a página da Web novamente. Para carregar a página da Web, seu navegador envia uma consulta a um servidor DNS por meio do protocolo UDP para recuperar o endereço IP do nome de domínio do site; isso faz parte do protocolo DNS. Seu navegador, em seguida, usa esse endereço IP como o IP de destino para enviar uma solicitação HTTPS para o servidor Web para exibir a página da Web O analisador mostra que, quando você envia pacotes UDP para o servidor DNS, você recebe pacotes ICMP contendo a mensagem de erro: "udp porta 53 inacessível".

Mateus Breno Soares Silva

Relatório de incidente de segurança cibernética

Análise de tráfego de rede

```
13:24:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:24:36.098564 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 254

13:26:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:27:15.934126 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 320

13:28:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:28:50.022967 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 150
```

No log tcpdhum, você encontra as seguintes informações:

- As duas primeiras linhas do arquivo de log mostram a solicitação de saída inicial do computador para o servidor DNS solicitando o endereço IP de yummyrecipesforme.com. Essa solicitação é enviada em um pacote UDP.
- A terceira e a quarta linhas do log mostram a resposta ao pacote UDP. Nesse caso, a linha ICMP 203.0.113.2 é o início da mensagem de erro indicando que o pacote UDP não foi entregue à porta 53 do servidor DNS.
- Na frente de cada solicitação e resposta, você encontra carimbos de data/hora que indicam quando o incidente aconteceu. No log, esta é a primeira sequência de números exibida: 13:24:32.192571. Isso significa que o tempo é 13h24, 32,192571 segundos.

Mateus Breno Soares Silva

Relatório de incidente de segurança cibernética

Análise de tráfego de rede

- Após os carimbos de data/hora, você encontrará os endereços IP de origem e destino. Na primeira linha, onde o pacote UDP viaja do seu navegador para o servidor DNS, essas informações são exibidas como: 192.51.100.15 > 203.0.113.2.domain. O endereço IP à esquerda do símbolo maior que (>) é o endereço de origem, que neste exemplo é o endereço IP do computador. O endereço IP à direita do símbolo maior que (>) é o endereço IP de destino. Nesse caso, é o endereço IP do servidor DNS: 203.0.113.2.domain. Para a resposta de erro ICMP, o endereço de origem é 203.0.113.2 e o destino é o endereço IP do computador 192.51.100.15.
- Após os endereços IP de origem e destino, pode haver uma série de detalhes adicionais, como o protocolo, o número da porta da origem e os sinalizadores. Na primeira linha do log de erros, o número de identificação da consulta aparece como: 35084. O sinal de adição após o número de identificação da consulta indica que há sinalizadores associados à mensagem UDP. O "A?" indica um sinalizador associado à solicitação DNS para um registro A, onde um registro A mapeia um nome de domínio para um endereço IP. A terceira linha exibe o protocolo da mensagem de resposta para o navegador: "ICMP", que é seguido por uma mensagem de erro ICMP.
- A mensagem de erro, "udp porta 53 inacessível" é mencionada na última linha. A porta 53 é uma porta para o serviço DNS. A palavra "inacessível" na mensagem indica que a mensagem UDP solicitando um endereço IP para o domínio "www.yummyrecipesforme.com" não passou para o servidor DNS porque nenhum serviço estava escutando na porta DNS de recebimento.
- 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 analisador de rede, é seu trabalho identificar qual protocolo de rede e serviço foram afetados por esse incidente. Em seguida, você precisará escrever um relatório de acompanhamento.

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

Esse evento, enquanto isso, está sendo tratado por engenheiros de segurança depois que você e outros analistas relataram o problema ao seu supervisor direto.

Mateus Breno Soares Silva

Relatório de incidente de segurança cibernética

Análise de tráfego de rede

Primeira parte

Deve-se fornecer um resumo do problema encontrado no DNS e no ICMP registro de tráfego:

O protocolo UDP, no caso desse cenário faz parte do DNS **www.yummyrecipesforme.com**, como mostra a imagem acima, o protocolo ICMP respondeu todas as solicitações UDP com uma mensagem de erro. Essa resposta indaca erro ao manter contato com o servidor DNS.
Essa resposta pode ser vista na terceira linha de cada verificação da imagem acima. O *UDP port 53 unreachable length 254*, ou seja, o *unreacheble* é a resposta *inacessível* da comunicação.
Pode-se determinar que o erro parte do DNS, pois, no seu lado da comunicação, após o seu ip.domain seu identificador de consulta, o 35084+, e o “A?” que indica sinalizadores com a execução de operações de protocolo DNS.

Mateus Breno Soares Silva

Relatório de incidente de segurança cibernética

Análise de tráfego de rede

Segunda parte

Explique sua análise dos dados e forneça pelo menos uma causa do incidente:

O incidente foi registrado por volta da 13:24, sem embasando a imagem mostrada acima. Com isso, e as notificações dos clientes, devido a porta 53 estar inacessível quando tentam acessar o **www.yummyrecipesforme.com**, segundo o Cenário, a equipe de segurança está investigando o caso.
Como citado acima, ao utilizar o tcpdump para verificar mais a fundo o problema, assim, pode-se identificar se o problema é oriundo da porta 53 ou do servidos DNS, pois, nesse caso, a melhor hipótese, sem maiores dados, é que estejam sofrendo um ataque DoS.

Mateus Breno Soares Silva