Incidente de Segurança Cibernética (DNS_ICMP_yummyrecipesforme)

Visão Geral do Cenário

Este documento detalha a investigação de um incidente de rede, focando na análise do tráfego **DNS** e **ICMP** para identificar o protocolo de rede impactado. A capacidade de analisar dados de ferramentas de monitoramento de rede é fundamental para diagnosticar e responder a eventos de segurança.

No **modelo TCP/IP**, a camada de Internet, onde o **IP** (Internet Protocol) estrutura pacotes de dados em datagramas, oferece informações cruciais. A inspeção desses datagramas permite a identificação de padrões e anomalias que podem indicar atividades suspeitas ou maliciosas.

Dominar a identificação de tráfego anômalo em uma rede é uma competência essencial para profissionais de segurança cibernética. Essa habilidade não só aprimora a **avaliação de riscos**, mas também fortalece as defesas da **segurança da rede**.

Detalhes do Incidente

Como analista de segurança cibernética em uma empresa especializada em serviços de TI, fui acionado devido a **relatos de múltiplos clientes** que enfrentavam dificuldades para acessar o site `www.yummyrecipesforme.com` . O sintoma comum era a exibição da mensagem de erro: "porta de destino inalcançável".

Minha responsabilidade imediata foi **analisar a situação** e determinar o protocolo de rede afetado. Ao tentar acessar o site, repliquei o erro. Para iniciar a investigação, utilizei o **tcpdump**, uma ferramenta de análise de tráfego de rede.

Durante a tentativa de acesso ao site, o navegador envia uma consulta **UDP** a um servidor **DNS** para resolver o nome de domínio em um endereço IP. A análise do tráfego revelou que, ao enviar pacotes UDP para o servidor DNS, eram recebidos

pacotes **ICMP** contendo a mensagem de erro: "porta udp 53 inacessível".

Análise Técnica do Registro Tcpdump

O registro do tcpdump forneceu as seguintes informações críticas:

```
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
```

Fluxo de Solicitação (UDP): As primeiras linhas do registro indicam uma solicitação originada do meu sistema (IP: `192.51.100.15`) para o servidor DNS (IP: `203.0.113.2.domain`), buscando a resolução de `yummyrecipesforme.com`. Esta solicitação foi encapsulada em um pacote **UDP**.

Resposta de Erro (ICMP): As linhas subsequentes mostram a resposta ao pacote UDP. A entrada `ICMP 203.0.113.2` sinaliza o início de uma mensagem de erro, indicando que o pacote UDP não pôde ser entregue na **porta 53** do servidor DNS.

Carimbos de Data/Hora: Cada evento no registro é acompanhado por um carimbo de data/hora preciso, como `13:24:32.192571`, registrando o momento da ocorrência.

Endereços IP Envolvidos:

Origem da Solicitação: `192.51.100.15` (sistema do analista).

Destino da Solicitação: `203.0.113.2.domain` (servidor DNS).

Na resposta de erro ICMP, o endereço de origem é `203.0.113.2` e o destino é `192.51.100.15`.

Detalhes Adicionais do Pacote:

ID da Consulta: `35084` (observado na primeira linha de erro).

Sinalizadores: O caractere `+` após o ID da consulta denota a presença de sinalizadores associados à mensagem UDP. O `A?` especifica uma consulta DNS para um registro A, que associa um nome de domínio a um endereço IP.

Protocolo de Resposta: ICMP, seguido pela mensagem de erro específica.

Mensagem de Erro Central: A mensagem "udp port 53 unreachable" é o ponto focal da investigação. A **porta 53** é a porta padrão para o serviço **DNS**. A indicação de "unreachable" (inacessível) sugere que a solicitação UDP para `www.yummyrecipesforme.com` não alcançou o serviço DNS no servidor, possivelmente devido à **ausência de um serviço escutando na porta DNS designada**.

Padrão de Repetição: O registro demonstra que as tentativas subsequentes de resolução DNS resultaram em respostas ICMP idênticas, confirmando a persistência do problema.

Conclusão e Próximos Passos

Com base nesta análise, a investigação foca na identificação precisa do **protocolo de rede** e do **serviço** afetados por este incidente. Um **relatório de incidente** detalhado foi elaborado para documentar as descobertas e as ações recomendadas.

Segue o relatório: Relatório de Incidente de Rede: DNS_ICMP