# Incident report analysis

Ataque Flood de ICMP sobrecarregando a rede por meio de um DDoS.

| **Summary** | |
|---|---|
| Identify | Como se tratava de um Flood por meio de ICMP, que gerou um ataque DDoS, foram afetadas toda a rede interna da empresa. No caso, existia um firewall não configurado fazendo o ataque flood ICMP por ping. Dispositivos que foram afetados com esse ataque e processos(diretamente):<br>- Parte estrutural da rede: Servidores, firewalls, modens, roteadores.<br>- Sistema desligado por duas horas afetando os processos casuais dos funcionários.<br>Nesse caso, como foi a rede que foi atacada, todas as pessoas da organização precisam dessa liberação o quanto antes, para não ser afetada.<br>No caso também pode se notar que com o firewall não configurado ele burlou o firewall de borda. Podendo criar uma ponte direta com as máquinas que estão na rede. |
| Protect | Para esse caso, como foi um flood ICMP, que parou a rede, a única coisa era bloquear todo o tráfego ICMP, interrompendo os serviços não críticos offline.<br>Proteções criada, para assegurar a rede contra esse tipo de ataque:<br>- Inclusão de uma camada de defesa IDS/IPS para filtrar algum tráfego ICMP com base em características suspeitas.<br>- Regra no firewall para limitar a entrada de pacotes ICMP.<br>- Adicionar um software de monitoramento de rede para detectar padrões incomuns. |
| Detect | Depois do ataque foi feita uma reunião de implementações, abordando diferentes ferramentas que trariam uma segurança a mais para a rede. |

| | |
|---|---|
| | - Software de análise rede(WireShark): Além de ter a parte de análise de rede, daria para configurar aviso sobre padrões incomuns, como pacotes contínuos com a mesma carga de tráfego, etc.<br>- Siem Tool(Splunk ou Chronicle): A ferramenta SIEM analise logs e analise as vulnerabilidades e ameaças que o servidor tem, para diminuição de riscos.<br>- IDS/IPS: Uma camada de proteção que ajudaria a filtrar melhor a entrada de tráfego dentro da rede, o IDS ajudaria a detectar os padrões incomuns na rede, e alertava sobre eles. E o IPS seria a segunda camada, que alertava e dependendo da regra que configurarmos nele, bloqueia o tal tráfego incomum.<br>- Auditorias de segurança: 1 vez ao mês, fazerem relatórios com eles trazerem melhorias tanto em questão de regras quanto em questão de ferramentas.<br>- Treinamentos curtos para funcionários ajudam no combate contra as vulnerabilidades. |
| Respond | Pára esse caso, o que aconteceu, no momento do ataque bloquearam todo o tráfego ICMP, interrompendo todos os serviços de rede não críticos offline e restaurando os críticos. Uma resposta rápida e ágil, que resultou em uma melhora rápida.<br>Agora com as proteções que colocamos é algo mais diferente, diante de uma ataque como esse tem muitos avisos e bloqueios automáticos e o mais certo a se fazer é:<br>- Está acontecendo o ataque e o firewall e o IDPS está bloqueando o tráfego ICMP, logo isso já é uma salva, e um tempo para que consigamos fazer algo.<br>- Avisar os superiores pois ainda tem muito tempo até acontecer algo. Assim, bolando um plano de defesa.<br>- Podendo achar que o problema é a raiz dele, às vezes é um ataque |

| | |
|---|---|
| | ICMP direto de dentro da rede e não só por um firewall não configura implantado, talvez em uma máquina que sofreu de um ataque botnet.<br>O que mudou?<br>Nada, se sofrer o ataque vai ser igual, mas terá mais tempo para bolar um plano e fazer uma defesa mais eficaz, sem ter que parar a rede ou sistemas, enquanto o IDPS e o firewall está bloqueando a rede está funcionando perfeitamente, e você e sua equipe está fazendo um plano de defesa conclusivo. |
| Recover | Após o ataque, é feito a contenção dos servidores, isolados e fazendo uma analise minunciosa para tirar malwares e resquícios dos agente malicioso logo após, é avisado aos superiores que será rodado o backup(caso tenha danificado, se não danificou, só checar para ver se nao teve sobras do agente malicioso) a restauração dos firewall e rede acontece por meio de um backup feito anteriormente pela equipe de TI, no caso é feito a cada 1 semana 1 backup de firewalls, servidores, redes, tudo. Será feito um email sendo enviado a cada funcionário explicando o que aconteceu e informando como eles podem se preparar defensivamente contra ataques, e também informando como eles podem defender a organização contra ataques, notando padrões nocivos ou até mesmo engenharia social, por meio de phishing e outros métodos. |

---

| |
|---|
| Reflections/Notes: |