Incident report analysis

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

Summary	A companhia sofreu um ataque DoS resultando em indisponibilidade dos serviços de rede com inundação de pacotes ICMP assim impedindo o acesso a recursos da rede, a equipe de combate a incidentes respondeu bloqueando a entrada de pacotes ICMP, interrompendo todos os serviços de rede não críticos off-line e restaurando serviços críticos Em seguida a equipe de segurança da empresa entendeu que se tratava de um ataque flood de pings ICMP na rede da empresa devido a firewall não configurado permitindo a invasão do agente mal-intencionado
Identify	A empresa sofreu um ataque de negação de serviço (DoS), o agente malicioso explorou a falha em um firewall não configurado, resultado na inundação do sistema com pacotes ICMP resultando em indisponibilidade do acesso interno da rede
Protect	Para se prevenir de ataque futuros recomenda-se regras de firewall (rate limiting ICMP), filtragem de tráfego, politicas de hardening e segmentação de rede, com essas práticas de segurança aplicadas ajudam a reduzir invasões futuras
Detect	Para detectar rapidamente ataques semelhantes a esse recomenda-se softwares de monitoramento de rede e alertas para tráfego ICMP anormal,

	com isso permitindo resposta rápida a um ataque. Adicionalmente recomenda-se a implementação de IDS/IPS para analisar e bloquear anomalias
Respond	Inicialmente recomenda-se bloquear o ICMP suspeito, impedindo mais flood de pings, isolar sistemas afetados e manter em operação o sistema crítico. Sequencialmente recomenda-se a coleta de logs para análise para identificar origem do incidente
Recover	Restaurar serviços não críticos para a empresa voltar em operação, revisar configurações de firewall, atualização de politicas de segurança e rede e melhorar planos de resposta

---

Reflections/Notes: