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 rede interna sofreu um ataque DDoS e ficou comprometida por 2 horas, durante esse período a rede da organização ficou inutilizável. foi inundada com um fluxo de pacote ICMP, fazendo assim com que os usuários não conseguissem acessar nenhum recurso da rede, a equipe de gerenciamento de incidentes respondeu rapidamente e bloqueou a entrada de pacotes ICMP, interrompendo os serviços de rede não-críticos e liberando os serviços de rede críticos.
Identify	A equipe de segurança fez verificações e percebeu que a rede da organização estava sendo inundada por fluxo de pacotes ICMP, fazendo assim com que os usuários não conseguissem acessar nenhum recurso da rede.
Protect	A equipe de gerenciamento de incidentes respondeu rapidamente e bloqueou a entrada de pacotes ICMP, interrompendo os serviços de rede não-críticos e liberando os serviços de rede críticos.
Detect	Após feita uma investigação sobre o incidente a equipe descobriu que o ataque aconteceu devido a um firewall mal configurado, essa vulnerabilidade permitiu o ataque do agente mal-intencionado.
Respond	Para resolver esse evento de segurança, a equipe de segurança de rede

	implementou: ● Uma nova regra de firewall para limitar a taxa de entrada de pacotes ICMP ● Verificação do endereço IP de origem no firewall para verificar se há endereços IP falsos nos pacotes ICMP recebidos ● Software de monitoramento de rede para detectar padrões de tráfego anormais ● Um sistema IDS/IPS para filtrar algum tráfego ICMP com base em características suspeitas
Recover	Como não houve perda de dados a equipe não precisou fazer nenhum processo de recuperação de dados, somente a restauração do sistema.

Reflections/Notes: