Análise de relatório de incidente

Instruções

À medida que você continua neste curso, pode usar este modelo para registrar seus achados após concluir uma atividade ou para fazer anotações sobre o que aprendeu a respeito de uma ferramenta ou conceito específico. Você também pode usar esta tabela como uma forma de praticar a aplicação do framework NIST a diferentes situações que encontrar.

Sumário	A organização sofreu um ataque DDoS que interrompeu todos os serviços da rede por duas horas. O ataque foi executado por meio de um fluxo massivo de pacotes ICMP (ping flood) que explorou uma vulnerabilidade em um firewall não configurado corretamente. A equipe de resposta a incidentes conteve o ataque, bloqueando os pacotes ICMP e desativando serviços não essenciais. Posteriormente, a equipe de segurança implementou novas regras de firewall, verificação de endereço IP de origem, monitoramento de tráfego de rede e um sistema de IDS/IPS para prevenir futuros incidentes.
Identificar	A equipe de segurança cibernética investigou o evento de segurança e descobriram que um agente mal-intencionado explorou um firewall mal configurado para inundar a rede com pacotes ICMP. A equipe de resposta a incidentes agiu de acordo com a função.
Proteger	Para proteger a organização contra ataques semelhantes, a equipe de segurança implementou primeiramente uma nova regra de firewall para limitar a taxa de entrada de pacotes ICMP, mitigando o risco de sobrecarga. Em segundo lugar, foi habilitada a verificação do endereço IP de origem no firewall para verificar se há endereços IP falsos nos pacotes ICMP recebidos. Adicionalmente, foi implementado um sistema IDS/IPS para filtrar tráfego

	malicioso de forma proativa com base em características suspeitas.
Detectar	Para melhorar a detecção de futuras ameaças, a empresa implementou um software de monitoramento de rede para analisar padrões de tráfego anormais. Além de terem adicionado um sistema IDS/IPS para filtrar tráfego ICMP com base em características suspeitas e alertar a equipe de segurança sobre essas atividades suspeitas, aumentando a velocidade e eficiência da detecção.
Responder	Durante o incidente, a equipe de resposta agiu prontamente para conter o ataque. A primeira ação foi bloquear a entrada de todo tráfego ICMP no firewall, o que interrompeu o ataque. Simultaneamente, todos os serviços de rede não críticos foram desativados para reduzir a superfície de ataque e preservar recursos para os serviços essenciais. Após a contenção, a equipe comunicou o status do incidente à equipe de segurança cibernética que investigou o evento de segurança.
Recuperar	A equipe restaurou os serviços de rede críticos para retomar as operações essenciais da empresa e em seguida, os serviços não críticos foram reativados gradualmente, enquanto o novo sistema de monitoramento de rede observava o tráfego para garantir que o ambiente estava estável e seguro.

Reflexões e Notas: A causa raiz foi uma falha de processo. Um firewall não configurado indica a ausência de uma política de auditoria regular e de gestão de configurações para dispositivos de rede. A segurança não foi comprometida por uma falha no equipamento, mas pela falta de revisão humana e de procedimentos operacionais padrão.