English:

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	The company that offers graphic web design services had a security breach on its servers, where suddenly the servers went down and for about 2 hours they were unavailable due to a DDoS (Distributed Denial of Service) attack, in order to avoid further problems and to be able to restore the server later, they interrupted the non-critical services on the server.
Identify	A malicious agent recognized a failure in the server's packet input, causing the firewall to allow a greater amount of data packet input than the server could handle. The name of this DDoS attack is “ICMP Flood attack” working as if several devices, usually bots, send several messages repeatedly until the server is unable to send back the request requested by the user or bot in this case.
Protect	The main point of the recommendations for improvements in the company's security will be in the flow of traffic in the network, Stricter rules in the company's firewall, in the control of ICMP packets, to filter traffic based on suspicious characteristics. Rules that limit the number of packets sent. Installation of intrusion detection systems (IDS)

Detect	The security team needs to apply monitoring measures to the incoming flow by IP on the server. An interesting implementation would be, as previously mentioned, the implementation of IDS on the server and also security policies with stricter rules on the firewall.
Respond	For possible future events, a recommendation would be to isolate the non-critical system so as not to affect important information, try to recover any critical systems and services that were affected. And then the team will do an analysis of the attack, analyzing the IPs and LOGs used during the attack and documenting them to prevent future attacks.
Recover	To recover from a DDoS attack by ICMP flooding, access to network services need to be restored to a normal functioning state. In the future, external ICMP flood attacks can be blocked at the firewall. Then, all non-critical network services should be stopped to reduce internal network traffic. Next, critical network services should be restored first. Finally, once the flood of ICMP packets have timed out, all non-critical network systems and services can be brought back online.

Reflections/Notes:

Português:

Análise de relatório de incidente;

Instruções

Ao continuar neste curso, você poderá usar este modelo para registrar suas descobertas após concluir uma atividade ou para fazer anotações sobre o que aprendeu sobre uma ferramenta ou conceito específico. Você também pode usar este gráfico como uma forma de praticar a aplicação da estrutura NIST a diferentes situações que encontrar.

Resumo	A empresa que oferta serviços para Web design gráfico teve uma violação de segurança em seus servidores, onde de repente o servidores caíram e por cerca de 2 horas estiveram indisponíveis por conta de um ataque DDoS (Negação de Serviço Distribuído), para não ter mais problemas e pudessem ser restaurado o server posteriormente, interromperam os serviços não críticos do servidor.
Identificar	Um agente malicioso reconheceu uma falha na entrada de pacotes do servidor,fazendo com que o firewall permitisse uma quantidade de entradas de pacotes de dados maior do que o servidor suportasse. O nome desse ataque DDoS é “ICMP Flood attack” funcionando como se vários dispositivos geralmente bots, enviar várias mensagens repetidamente até que o servidor não consiga enviar de volta a solicitação pedida pelo usuário ou bot nesse caso.
Proteger	O ponto principal das recomendações de melhorias na segurança da empresa

	vai ser no fluxo de tráfego na rede, • Regras mais rígidas no firewall da empresa, no controle de pacotes ICMP, para filtrar o tráfego com base em características suspeitas. • Regras que limitam a quantidade de pacotes enviados. • Instalação de sistemas de detecção de intrusão (IDS)
Detectar	A equipe de segurança precisa aplicar medidas de monitoramento no fluxo de entrada por IP no servidor, uma implementação interessante seria como falado anteriormente, a implementação de IDS no servidor e também as políticas de segurança com regras mais rígidas no firewall.
Respond	Para possíveis futuros eventos, uma recomendação seria isolar o sistema não crítico para não afetar informações importantes, tentar recuperar quaisquer sistemas e serviços críticos que foram afetados. E em seguida a equipe fará uma análise sobre o ataque, analisando os IP's e LOG's usados durante o ataque e documentar para evitar futuros ataques.
Recover	Para se recuperar de um ataque DDoS por inundação ICMP, o acesso aos serviços de rede precisa ser restaurado para um estado de funcionamento normal. No futuro, ataques de inundação ICMP externos podem ser bloqueados no firewall. Então, todos os serviços de rede não críticos devem ser interrompidos para reduzir o tráfego de rede interno. Em seguida, os serviços de rede críticos devem ser restaurados primeiro. Finalmente, uma vez que a inundação de pacotes ICMP tenha expirado, todos os sistemas e serviços de rede não críticos podem ser trazidos de volta online.

Reflections/Notes: