Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption

Podemos identificar varias situações incomuns no log:

58	3.730097	198.51.100.14	192.0.2.1	TCP	14785->443 [ACK] Seq=1 Win-5792 Len=120...
59	3.795332	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win-5792 Len=120...
60	3.860567	198.51.100.14	192.0.2.1	HTTP	GET /sales.html HTTP/1.1
61	3.939499	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win-5792 Len=120...
62	4.018431	192.0.2.1	198.51.100.14	HTTP	HTTP/1.1 200 OK (text/html)
63	4.097363	198.51.100.5	192.0.2.1	TCP	33638->443 [SYN] Seq=0 Win-5792 Len=120...
64	4.176295	192.0.2.1	203.0.113.0	TCP	443->54770 [SYN, ACK] Seq=0 Win-5792 Len=120...
65	4.255227	192.0.2.1	198.51.100.5	TCP	443->33638 [SYN, ACK] Seq=0 Win-5792 Len=120...
66	4.256159	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win-5792 Len=0

1. A partir do No.61 começa a ficar mais devagar a troca de pacotes, e mais para baixo vai ficando demorado. Também podendo ser notado que até o 61, a requisições de entrada no sistema de IP normais, e também, requisições desses mesmo IP de HTTP, sendo assim trazendo uma certa legitimidade.

2.O ip 203.0.133.0 se repete muitas vezes, podendo notar que ele só manda protocolos SYN, sempre mitigando pouco a pouco, para não dar as caras logo. Podendo ser visto como um ataque de inundação SYN.

3.Depois do NO.132, podemos notar que so existe chamada do servido do IP 203.0.113.0 para o ip de destino 192.0.2.1, pensando em ser um DDoS, por conta da inundação, mas ficando claro, ao olhar o protocolo que está sendo mandando, que seria o SYN, trazendo então a tona o ataque de inundação SYN, que é um tipo de ataque que simula uma conexão TCP e inunda um servidor com pacotes SYN. E também podendo notar que ao mandar pacotes SYN, o tempo de resposta do servidor vai ficando mais lento. Passando para o último a 50 milésimos, podendo notar que o normal é 3.

Section 2: Explain how the attack is causing the website to malfunction

Quando um pacote é enviado usando TCP, é iniciado o processo conhecido como 3-way handshake para garantir que a comunicação ocorra de forma confiável e íntegra. As etapas são:

1. O cliente envia um pacote SYN ao servidor solicitando uma conexão;
2. O servidor responde com um pacote SYN/ACK confirmando o recebimento;
3. O cliente então envia um ACK final, estabelecendo a conexão TCP.

No ataque de inundação SYN (SYN Flood), um agente malicioso envia uma grande quantidade de pacotes SYN, mas nunca completa o handshake. Isso faz com que o servidor mantenha diversas conexões “semiabertas” (half-open), consumindo recursos até que ele não consiga mais aceitar novas conexões — podendo levar à lentidão ou indisponibilidade do serviço.

Nos logs abaixo, é possível identificar múltiplos pacotes SYN do IP 203.0.113.0 para o IP do servidor 192.0.2.1, sem resposta ACK. Isso evidencia um ataque gradual, iniciado de forma lenta para evitar detecção por ferramentas de análise (ex: Wireshark).

Como resposta ao incidente, deve-se bloquear o IP ofensivo, aplicar regras de proteção no firewall (como rate limiting para SYN ou uso de SYN cookies), além de configurar alertas automáticos para padrões anômalos semelhantes no futuro.

122	20.167744	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
123	20.490757	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
124	20.81377	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
125	21.136783	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
126	21.459796	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
127	21.782809	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
128	22.105822	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
129	22.428835	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
130	22.751848	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
131	23.074861	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
132	23.397874	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
133	23.720887	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
134	24.0439	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
135	24.366913	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
136	24.689926	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
137	25.012939	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
138	25.335952	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
139	25.658965	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
140	25.981978	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
141	26.304991	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0