Cybersecurity Incident Report

Stephen Langford
2/17/25

Section 1: Identifying the Attack

Potential Cause of the Website Disruption

The website experienced a **connection timeout error** due to a suspected **Denial-of-Service (DoS) attack**.

Key Evidence from Network Logs

A network analysis using **Wireshark** revealed a pattern of excessive **SYN packets** targeting **port 443 (HTTPS)**.

- The attack began at **packet 52**, where an **IP address (203.0.113.0)** initiated multiple **SYN requests** to the web server.
- Each **SYN packet** had a **zero-length payload**, characteristic of a **SYN Flood attack**.
- The server responded with **SYN-ACK packets**, but the attacker **never completed the handshake**, leading to resource exhaustion.

Possible Causes:

- A **SYN Flood attack**, where a malicious actor overwhelms the server with half-open TCP connections.
- A **misconfigured firewall or security policy** failing to mitigate SYN Flood attempts.
- **Botnet activity**, where multiple compromised devices execute a coordinated attack.

Section 2: How the Attack Caused Website Malfunction

Understanding the TCP Three-Way Handshake

When legitimate users attempt to connect to the website, the following **TCP handshake** occurs:

1. **SYN (Synchronize)** – The client sends a **SYN packet** to the web server on port **443** (HTTPS).
2. **SYN-ACK (Synchronize-Acknowledge)** – The server responds with a **SYN-ACK packet** to confirm communication.
3. **ACK (Acknowledge)** – The client sends an **ACK packet**, completing the connection.

What Happens During a SYN Flood Attack?

- The attacker **sends thousands of SYN packets** but **never replies with ACK packets**.
- The server **keeps waiting for responses**, causing its **connection table to fill up**.
- Once the table is full, the server **cannot accept new connections**, leading to **legitimate users being unable to access the website**.
- The server eventually **sends RST (Reset) packets** as a defensive measure, but the attack **continues to flood SYN packets**.

Key Findings from the Network Logs

- The logs show **multiple SYN packets** from **203.0.113.0**, all targeting **port 443** with **no corresponding ACKs**.
- At **packet 73**, the server starts responding with **RST, ACK** packets, indicating it **is overwhelmed**.
- At **packet 77**, the server returns a **504 Gateway Timeout**, confirming that it **cannot process new connections**.
- The flood of SYN packets continues, preventing the website from serving legitimate traffic.

Section 3: Mitigation & Recommendations

Immediate Actions Taken

- **Blocking Malicious IPs**: Firewall rules were updated to block **203.0.113.0** and similar sources.
- **Rate Limiting**: SYN flood protection mechanisms were enabled to **limit excessive connection attempts**.
- **Traffic Filtering**: Intrusion Detection System (IDS) rules were updated to drop abnormal SYN requests.

Long-Term Solutions

- **Enable SYN Cookies**: This will help prevent half-open connections from consuming resources.
- **Deploy Web Application Firewall (WAF)**: Protects against **layer 7 DoS attacks** targeting HTTPS.
- **Monitor Network Traffic**: Using **tcpdump/Wireshark** to detect unusual SYN activity before disruption occurs.
- **Consider Cloud-Based DDoS Mitigation**: Services like **Cloudflare** or **AWS Shield** can absorb large-scale attacks.

Section 4: Conclusion

- The website downtime was caused by a **SYN Flood DoS attack** that overwhelmed the web server's ability to process legitimate connections.
- Logs confirmed **thousands of SYN packets with no follow-up ACKs**, leading to resource exhaustion.
- **Mitigation steps** were taken to block the attack, including **IP blocking, SYN cookies, and firewall rule updates**.

Example Screenshot of Logs:

No.	Time	Source	Destination	Protocol	Info
47	3.144521	198.51.100.23	192.0.2.1	TCP	42584->443 [SYN] Seq=0 Win-5792 Len=120...
48	3.195755	192.0.2.1	198.51.100.23	TCP	443->42584 [SYN, ACK] Seq=0 Win-5792 Len=120...
49	3.246989	198.51.100.23	192.0.2.1	TCP	42584->443 [ACK] Seq=1 Win-5792 Len=120...
50	3.298223	198.51.100.23	192.0.2.1	HTTP	GET /sales.html HTTP/1.1
51	3.349457	192.0.2.1	198.51.100.23	HTTP	HTTP/1.1 200 OK (text/html)
52	3.390692	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
53	3.441926	192.0.2.1	203.0.113.0	TCP	443->54770 [SYN, ACK] Seq=0 Win-5792 Len=120...
54	3.49316	203.0.113.0	192.0.2.1	TCP	54770->443 [ACK Seq=1 Win=5792 Len=0...
55	3.544394	198.51.100.14	192.0.2.1	TCP	14785->443 [SYN] Seq=0 Win-5792 Len=120...
56	3.599628	192.0.2.1	198.51.100.14	TCP	443->14785 [SYN, ACK] Seq=0 Win-5792 Len=120...
57	3.664863	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
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...
67	5.235091	198.51.100.5	192.0.2.1	TCP	33638->443 [ACK] Seq=1 Win-5792 Len=120...
68	5.236023	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...