\*\*Cybersecurity Incident Report\*\*

\*\*Subject:\*\* SYN Flood Attack on Travel Agency Website

\*\*Date:\*\* [Insert Date]

\*\*Reported by:\*\* [Your Name]

\*\*Company:\*\* [Your Organization]

\*\*Severity Level:\*\* High

---

## \*\*1. Incident Summary\*\*

On [insert date], an \*\*automated alert\*\* from the monitoring system indicated an issue with the \*\*company's web server\*\*. Employees attempting to access the website received a \*\*connection timeout error\*\*. Upon investigation using a \*\*packet sniffer (Wireshark/tcpdump)\*\*, an unusually \*\*high volume of TCP SYN requests\*\* was detected originating from an unfamiliar IP address. The web server was overwhelmed, indicating a \*\*SYN Flood Attack\*\*, a type of \*\*Denial-of-Service (DoS) attack\*\*.

### \*\*Key Findings:\*\*

| Observation | Details |

|------------|---------|

| \*\*Attack Type\*\* | SYN Flood Attack |

| \*\*Impact\*\* | Website downtime, employee inability to access sales data |

| \*\*Observed Pattern\*\* | High volume of half-open TCP connections |

| \*\*Source of Attack\*\* | Single unknown IP address |

| \*\*Affected Protocol\*\* | TCP |

---

## \*\*2. Technical Analysis\*\*

### \*\*2.1. Understanding the Attack\*\*

- When a user visits a website, their computer and the web server establish a \*\*three-way TCP handshake\*\*:

1. \*\*SYN\*\* – The client requests a connection.

2. \*\*SYN-ACK\*\* – The server acknowledges and sends a response.

3. \*\*ACK\*\* – The client confirms and the connection is established.

- In a \*\*SYN Flood Attack\*\*, the attacker sends \*\*multiple SYN requests\*\* but never completes the handshake, leaving the server waiting indefinitely.

- The server \*\*runs out of resources\*\* as it keeps waiting for ACK responses that never arrive.

### \*\*2.2. Packet Log Analysis\*\*

| Timestamp | Source IP | Destination IP | Protocol | Status |

|-----------|-----------|---------------|----------|--------|

| 13:45:23 | 192.51.100.45 | 203.0.113.10 | TCP SYN | Incomplete |

| 13:45:24 | 192.51.100.45 | 203.0.113.10 | TCP SYN | Incomplete |

| 13:45:25 | 192.51.100.45 | 203.0.113.10 | TCP SYN | Incomplete |

These logs indicate a large number of \*\*SYN requests without ACK responses\*\*, confirming an \*\*ongoing SYN Flood Attack\*\*.

---

## \*\*3. Impact Analysis\*\*

### \*\*3.1. How the Attack Affected the Website\*\*

| Impact Area | Description |

|------------|-------------|

| \*\*Website Downtime\*\* | Customers and employees were unable to access the travel agency's sales portal. |

| \*\*Server Resource Exhaustion\*\* | The web server struggled to handle legitimate requests due to high volumes of half-open connections. |

| \*\*Loss of Revenue\*\* | Potential loss of customers who could not book vacation packages. |

| \*\*Strain on IT Resources\*\* | Required IT team intervention to mitigate and recover the system. |

---

## \*\*4. Immediate Mitigation Actions\*\*

- \*\*Server Taken Offline Temporarily\*\*: Allowed the system to recover from resource exhaustion.

- \*\*Firewall Rules Updated\*\*: Blocked the attacker's IP address.

- \*\*Monitored Network Traffic\*\*: Used \*\*Wireshark\*\* to capture further attack patterns.

---

## \*\*5. Long-Term Security Recommendations\*\*

To \*\*prevent future SYN Flood Attacks\*\*, the following security measures should be implemented:

| Recommendation | Description |

|---------------|-------------|

| \*\*Enable SYN Cookies\*\* | Forces the client to send an extra response before a connection is established, reducing half-open connections. |

| \*\*Rate Limiting\*\* | Limits the number of simultaneous SYN requests per IP address. |

| \*\*Intrusion Prevention System (IPS)\*\* | Detects and blocks malicious SYN Flood patterns automatically. |

| \*\*Deploy a Web Application Firewall (WAF)\*\* | Helps prevent network-layer attacks against the web server. |

| \*\*Use DDoS Protection Services\*\* | If the attack scales up, a cloud-based service should be used to mitigate further disruptions. |

---

## \*\*6. Conclusion\*\*

This \*\*SYN Flood Attack\*\* resulted in a \*\*temporary outage of the company's travel sales website\*\*, impacting both \*\*customers and internal employees\*\*. The \*\*attack targeted the TCP handshake process\*\*, preventing the server from processing legitimate connections.

While \*\*blocking the attacker's IP\*\* provided short-term relief, additional security measures such as \*\*SYN Cookies, rate limiting, and IPS deployment\*\* are necessary to \*\*prevent future DoS incidents\*\*.

\*\*Next Steps:\*\*

✔ Review firewall rules to prevent recurrence.

✔ Implement \*\*SYN Flood protection mechanisms\*\*.

✔ Monitor for \*\*repeated attack attempts\*\* using security logs.

---

\*\*Prepared by:\*\* [Your Name]

\*\*Role:\*\* Cybersecurity Analyst

\*\*Date:\*\* [Insert Date]

---

### \*\*📌 How to Use This Report in Google Docs:\*\*

1. \*\*Open [Google Docs](https://docs.google.com/)\*\*.

2. \*\*Click "Blank Document"\*\*.

3. \*\*Copy and paste this entire report\*\* into the document.

4. \*\*Format it as needed (add company branding, colors, highlights, etc.)\*\*.

5. \*\*Save as `.docx` or `.pdf` for professional use\*\*.

🚀 Now your \*\*incident report is professional, structured, and ready for use in your cybersecurity portfolio!\*\* Let me know if you need any modifications!