(Mock) Analyzation of Network Attacks

A logo with a shark fin

Description automatically generated

Material & instructions developed by: Google Cybersecurity Professional Certificate Course

Completed by: Alexander Herman on 01/11/24

**Table of Contents:**

Activity Overview (Provided): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**2**

Scenario (Provided): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**2**

Wireshark TCP/HTTP Log (Provided):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**3-5**

Incident Report (My Work): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**6**

**Activity Overview**

In this activity, you will consider a scenario involving a customer of the company that you work for who experiences a security issue when accessing the company’s website. You will identify the likely cause of the service interruption. Then, you will explain how the attack occurred and the negative impact it had on the website.

In this course, you have learned about several common network attacks. You have learned their names, how they are carried out, and the characteristics of each attack from the perspective of the target. Understanding how attacks impact a network will help you troubleshoot issues on your organization’s network. It will also help you take steps to mitigate damage and protect a network from future attacks.

**Scenario**

You work as a security analyst for a travel agency that advertises sales and promotions on the company’s website. The employees of the company regularly access the company’s sales webpage to search for vacation packages their customers might like.

One afternoon, you receive an automated alert from your monitoring system indicating a problem with the web server. You attempt to visit the company’s website, but you receive a connection timeout error message in your browser.

You use a packet sniffer to capture data packets in transit to and from the web server. You notice a large number of TCP SYN requests coming from an unfamiliar IP address. The web server appears to be overwhelmed by the volume of incoming traffic and is losing its ability to respond to the abnormally large number of SYN requests. You suspect the server is under attack by a malicious actor.

You take the server offline temporarily so that the machine can recover and return to a normal operating status. You also configure the company’s firewall to block the IP address that was sending the abnormal number of SYN requests. You know that your IP blocking solution won’t last long, as an attacker can spoof other IP addresses to get around this block. You need to alert your manager about this problem quickly and discuss the next steps to stop this attacker and prevent this problem from happening again. You will need to be prepared to tell your boss about the type of attack you discovered and how it was affecting the web server and employees.

**Wireshark TCP/HTTP Log**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Color  as text | No. | Time | Source  (x = redacted) | Destination  (x = redacted) | **Protocol** | **Info** |
| green | 47 | 3.144521 | 198.51.100.23 | 192.0.2.1 | TCP | 42584->443 [SYN] Seq=0 Win=5792 Len=120... |
| green | 48 | 3.195755 | 192.0.2.1 | 198.51.100.23 | TCP | 443->42584 [SYN, ACK] Seq=0 Win-5792 Len=120... |
| green | 49 | 3.246989 | 198.51.100.23 | 192.0.2.1 | TCP | 42584->443 [ACK] Seq=1 Win-5792 Len=120... |
| green | 50 | 3.298223 | 198.51.100.23 | 192.0.2.1 | HTTP | GET /sales.html HTTP/1.1 |
| green | 51 | 3.349457 | 192.0.2.1 | 198.51.100.23 | HTTP | HTTP/1.1 200 OK (text/html) |
| red | 52 | 3.390692 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 53 | 3.441926 | 192.0.2.1 | 203.0.113.0 | TCP | 443->54770 [SYN, ACK] Seq=0 Win-5792 Len=120... |
| red | 54 | 3.493160 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [ACK Seq=1 Win=5792 Len=0... |
| green | 55 | 3.544394 | 198.51.100.14 | 192.0.2.1 | TCP | 14785->443 [SYN] Seq=0 Win-5792 Len=120... |
| green | 56 | 3.599628 | 192.0.2.1 | 198.51.100.14 | TCP | 443->14785 [SYN, ACK] Seq=0 Win-5792 Len=120... |
| red | 57 | 3.664863 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| green | 58 | 3.730097 | 198.51.100.14 | 192.0.2.1 | TCP | 14785->443 [ACK] Seq=1 Win-5792 Len=120... |
| red | 59 | 3.795332 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win-5792 Len=120... |
| green | 60 | 3.860567 | 198.51.100.14 | 192.0.2.1 | HTTP | GET /sales.html HTTP/1.1 |
| red | 61 | 3.939499 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win-5792 Len=120... |
| green | 62 | 4.018431 | 192.0.2.1 | 198.51.100.14 | HTTP | HTTP/1.1 200 OK (text/html) |
| green | 63 | 4.097363 | 198.51.100.5 | 192.0.2.1 | TCP | 33638->443 [SYN] Seq=0 Win-5792 Len=120... |
| red | 64 | 4.176295 | 192.0.2.1 | 203.0.113.0 | TCP | 443->54770 [SYN, ACK] Seq=0 Win-5792 Len=120... |
| green | 65 | 4.255227 | 192.0.2.1 | 198.51.100.5 | TCP | 443->33638 [SYN, ACK] Seq=0 Win-5792 Len=120... |
| red | 66 | 4.256159 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| green | 67 | 5.235091 | 198.51.100.5 | 192.0.2.1 | TCP | 33638->443 [ACK] Seq=1 Win-5792 Len=120... |
| red | 68 | 5.236023 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| green | 69 | 5.236955 | 198.51.100.16 | 192.0.2.1 | TCP | 32641->443 [SYN] Seq=0 Win-5792 Len=120... |
| red | 70 | 5.237887 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| green | 71 | 6.228728 | 198.51.100.5 | 192.0.2.1 | HTTP | GET /sales.html HTTP/1.1 |
| red | 72 | 6.229638 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| yellow | 73 | 6.230548 | 192.0.2.1 | 198.51.100.16 | TCP | 443->32641 [RST, ACK] Seq=0 Win-5792 Len=120... |
| red | 74 | 6.330539 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| green | 75 | 6.330885 | 198.51.100.7 | 192.0.2.1 | TCP | 42584->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 76 | 6.331231 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| yellow | 77 | 7.330577 | 192.0.2.1 | 198.51.100.5 | TCP | HTTP/1.1 504 Gateway Time-out (text/html) |
| red | 78 | 7.331323 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| green | 79 | 7.340768 | 198.51.100.22 | 192.0.2.1 | TCP | 6345->443 [SYN] Seq=0 Win=5792 Len=0... |
| yellow | 80 | 7.340773 | 192.0.2.1 | 198.51.100.7 | TCP | 443->42584 [RST, ACK] Seq=1 Win-5792 Len=120... |
| red | 81 | 7.340778 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 82 | 7.340783 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 83 | 7.439658 | 192.0.2.1 | 203.0.113.0 | TCP | 443->54770 [RST, ACK] Seq=1 Win=5792 Len=0... |
| red | 119 | 19.198705 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 120 | 19.521718 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| yellow | 121 | 19.844731 | 192.0.2.1 | 198.51.100.9 | TCP | 443->4631 [RST, ACK] Seq=1 Win=5792 Len=0... |
| red | 122 | 20.167744 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 123 | 20.490757 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 124 | 20.81377 | 192.0.2.1 | 203.0.113.0 | TCP | 443->54770 [RST, ACK] Seq=1 Win=5792 Len=0... |
| red | 125 | 21.136783 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 126 | 21.459796 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 127 | 21.782809 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 128 | 22.105822 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 129 | 22.428835 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 130 | 22.751848 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 131 | 23.074861 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 132 | 23.397874 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 133 | 23.720887 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 134 | 24.0439 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 135 | 24.366913 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 136 | 24.689926 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 137 | 25.012939 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 138 | 25.335952 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 139 | 25.658965 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 140 | 25.981978 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 141 | 26.304991 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 142 | 26.628004 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 143 | 26.951017 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 144 | 27.27403 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 145 | 27.597043 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 146 | 27.920056 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 147 | 28.243069 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 148 | 28.566082 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 149 | 28.889095 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 150 | 29.212108 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 151 | 29.535121 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 152 | 29.858134 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |

**Instructions**

* Identify the type of attack causing this network interruption
* Explain how the attack is causing the website to malfunction

**Incident Report**

**Problem Summary**:

After receiving an automated alert for the web server, I attempted to visit the website in question and received a connection timeout error message. After then using my packet-sniffing tool I discovered an abnormal amount of TCP SYN requests coming from the unfamiliar IP address (203.0.113.0). This is likely a DoS SYN-Flood Attack.

**Analysis**:

The incident occurred this afternoon after I received an alert from our monitoring software that our web server was experiencing issues. I responded by conducting pack-sniffing tests using Wireshark and discovered the server was receiving an abnormal amount of TCP SYN requests coming from a single unfamiliar IP address (203.0.113.0). Because it is a single address, I believe it was a DoS SYN-Flood Attack being carried out by a threat actor and not a DDoS attack. Other authentic connections were attempted during my test with some being successful at first but then returning errors after the web server became overwhelmed. After reviewing the logs, I shut down the server and reported the incident to the security team. I recommend blocking the threat actor’s IP, but we should take additional steps as he could simply spoof another IP and reengage the attack. I suggest we configure our firewall to block connections from IP addresses that send more than a set amount of TCP SYN requests per minute and contact our web server admin to have them scan for unusual or suspicious activity.