CYBR-2200 Network Analysis

Week 7 Final Network Traffic Analysis Report

Student Name: Brylan Williamson

Instructor: Gina Llanos Cramer

Date: 2/26/2026

Executive Summary

The analysis of the provided packet capture files revealed two distinct categories of network activity: normal client based communication and external reconnaissance scanning against public facing servers. In the webserver scanning captures, multiple unrelated external IP addresses attempted to initiate TCP connections to servers 188.165.143.159 and 54.191.67.23 by sending SYN packets to various destination ports. The servers responded with RST, ACK packets, indicating that the ports were closed but reachable. No successful TCP three way handshakes or application-layer sessions were observed, suggesting reconnaissance rather than exploitation. In contrast, the exercise captures demonstrated legitimate internal client activity involving DNS resolution and encrypted HTTPS communication with Microsoft infrastructure.

This activity matters because port scanning is commonly the first phase of a cyber attack. Although no compromise or malicious payload delivery was observed, the scanning confirms that the servers are publicly accessible and actively being probed. Continuous reconnaissance increases the likelihood of future attack attempts, particularly if services are misconfigured or exposed unnecessarily. It is recommended that firewall configurations be reviewed, only required services remain publicly accessible, and monitoring systems remain enabled to detect escalation beyond reconnaissance activity.

Network Environment Overview

The packet captures show a mixed environment consisting of internal client systems and publicly accessible external servers. Internal hosts were observed using private IP addressing within the 10.5.31.0/24 range, including systems 10.5.31.182 and 10.5.31.139. These hosts communicated with an internal DNS server at 10.5.31.5 to resolve domain names before initiating outbound connections. This structure indicates a typical client-server enterprise or lab network configuration.

External communication included legitimate outbound connections to Microsoft owned infrastructure such as 40.83.247.108 and 13.107.42.16 over HTTPS. Additionally, public facing servers with IP addresses 188.165.143.159 and 54.191.67.23 were observed receiving inbound connection attempts from multiple external IP addresses. Traffic patterns show normal

outbound client behavior alongside inbound internet based scanning activity targeting exposed servers.

Baseline Traffic Analysis

Normal network traffic within the captures followed expected communication patterns. Internal hosts first issued DNS queries over UDP port 53 to the internal DNS server 10.5.31.5. For example, 10.5.31.182 resolved client.wns.windows.com, and 10.5.31.139 resolved config.edge.skype.com. The DNS responses included valid CNAME records pointing to Microsoft-managed infrastructure, indicating legitimate service resolution.

Following DNS resolution, the internal hosts established TCP connections over port 443 with external servers. Proper TCP three way handshakes were observed, followed by TLSv1.2 Client Hello messages containing appropriate Server Name Indication values matching the requested domains. These sessions represent encrypted HTTPS communication consistent with Windows Notification Services and Microsoft Skype or Teams configuration traffic. No abnormal ports, malformed packets, or incomplete sessions were identified within the baseline captures, confirming legitimate and expected client behavior.

Identified Anomalies or Malicious Activity

The primary anomalous activity identified in the packet captures was external port scanning directed at public facing servers. In the file 2022-MTA-workshop-webserver-scanning-1-of-2.pcap, multiple external IP addresses sent TCP SYN packets to server 188.165.143.159 targeting ports including 23, 445, 943, 2424, 5555, 5038, and 9986. The absence of completed TCP handshakes indicates that these were connection attempts rather than established sessions.

In the file 2022-MTA-workshop-webserver-scanning-2-of-2.pcap, similar behavior was observed targeting server 54.191.67.23. External IP addresses sent SYN packets to ports such as 3136, 445, 13136, and 7191. The server responded with TCP RST, ACK packets, confirming that the ports were closed. The repeated probing of multiple ports from unrelated global IP addresses is consistent with automated reconnaissance scanning tools attempting to identify open services. Although no exploitation was observed, this behavior deviates significantly from baseline traffic patterns and represents security relevant activity.

Evidence and Indicators

Several key indicators support the identification of reconnaissance activity:

Public Servers Targeted: 188.165.143.159 and 54.191.67.23

Internal Hosts Observed: 10.5.31.182 and 10.5.31.139

Internal DNS Server: 10.5.31.5

Microsoft Infrastructure IPs: 40.83.247.108 and 13.107.42.16

Ports Targeted During Scanning: 23 (Telnet), 445 (SMB), 3136, 943, 2424, 5555, 5038, 9986, 13136, 7191

Domains Observed in Legitimate Traffic: client.wns.windows.com and config.edge.skype.com

TCP Flags Observed During Scanning: SYN and RST, ACK

The SYN only connection attempts without completed handshakes, combined with RST, ACK responses from the servers, clearly indicate port scanning behavior. In contrast, legitimate baseline traffic showed complete TCP handshakes followed by encrypted TLS sessions over port 443.

Analyst Assessment and Recommendations

Based on the observed evidence, the activity should be classified as confirmed external reconnaissance rather than a confirmed security breach. The scanning activity demonstrates that the public facing servers are exposed to internet wide probing but does not show signs of

successful compromise or exploitation. The risk level is assessed as low to moderate, as reconnaissance alone does not indicate a breach but represents the first stage of potential attack activity.

It is recommended that firewall configurations be reviewed to ensure only necessary ports and services are exposed to the internet. Intrusion detection or intrusion prevention systems should be enabled to monitor repeated scanning attempts and alert administrators to increased activity levels. Server logs and firewall logs should be reviewed for patterns of repeated access attempts from the same IP addresses. Additional data such as endpoint security logs and extended network captures would help confirm whether any further suspicious activity occurred beyond the captured timeframe.