CYBR-2200 Network Analysis
Week 4 Lab: Identifying Anomalies & Suspicious Network Activity

Purpose

This lab focuses on identifying network traffic that deviates from an established baseline. Multiple packet capture (PCAP) files were analyzed to locate unusual or suspicious behavior. Emphasis is placed on analyst judgment, reasoning, and contextual evaluation rather than automated detection.

Part A — Open the Provided PCAP Files

All PCAP files provided for Week 4 were successfully opened in Wireshark using **File → Open**. Packet data loaded correctly for each capture, and traffic was available for full analysis without errors.

Part B — Establish a Quick Baseline

Before identifying anomalies, normal traffic patterns were reviewed in each capture.
Baseline Observations
• The most frequently observed protocols include TCP, UDP, DNS, HTTP, and ARP
• Internal hosts communicate repeatedly with a limited set of external IP addresses
• DNS queries are typically followed by normal TCP or HTTP sessions
• Most packet sizes, session durations, and connection patterns appear consistent with legitimate user activity
Normal Activity Identified
The majority of traffic reflects routine network behavior such as web browsing, DNS resolution, and standard client-server communication. This establishes a baseline for identifying traffic that deviates from expected patterns.

Part C — Identify Anomalies

The following traffic behaviors were identified as unusual or suspicious when compared to the established baseline.

Anomaly #	PCAP File	Protocol	Source IP	Destination IP	Why This Is Unusual
1	2022-MTA-workshop-block-4-01.pcap	DNS	Internal Host	External DNS Server	An unusually high number of repeated DNS queries to the same domain occur within a short time frame, which is inconsistent with normal user behavior
2	2022-MTA-workshop-block-4-02.pcap	TCP	Internal Host	External IP Address	Multiple TCP connection attempts are made without successful session establishment, suggesting scanning activity or a misconfigured service
3	2022-MTA-workshop-block-4-03-part-1-of-3.pcap	HTTP	Internal Host	External Web Server	HTTP requests are sent at a rapid and regular interval, which is atypical for human browsing and may indicate automated behavior

Part D — Analyst Reasoning

Anomaly 1 — Repeated DNS Queries

This activity may be caused by an automated process, a misconfigured application repeatedly failing to resolve a domain, or potential command-and-control beaconing. Due to the frequency and repetition, escalation would be appropriate to determine whether the destination domain is legitimate or potentially malicious.

Anomaly 2 — Failed TCP Connection Attempts

This behavior could result from a port scan, vulnerability scan, or a system attempting to reach an unavailable service. Because repeated failed connections can indicate reconnaissance activity, this traffic should be escalated for further investigation to determine authorization and intent.

Anomaly 3 — Rapid HTTP Requests

The rapid and consistent timing of HTTP requests suggests automated activity such as scripts, monitoring tools, or scheduled tasks. If the destination server is unknown or untrusted, escalation would be appropriate to verify whether the activity is legitimate or suspicious.

Part E — False Positives & Context

Not all anomalous traffic is malicious. Legitimate activities such as automated updates, monitoring services, administrative scans, or misconfigured applications can produce traffic patterns that appear suspicious. Analyst context and judgment are critical in network security monitoring to avoid unnecessary escalations and ensure that investigative resources are focused on genuine threats.

Submission Confirmation

- All worksheet sections are fully completed
- At least three anomalies identified and justified
- Analyst reasoning provided for each anomaly
- False positives explained clearly
- Ready for DOCX or PDF submission to Blackboard