CYBR-2200 Network Analysis

Lewis Joseph Feik

Week 5 Lab Worksheet

Analyzing Attack Patterns & Policy Violations in Network Traffic

Part A: PCAP Files Opened

All provided PCAP files were successfully opened in Wireshark and packet data loaded without errors.

Part B: Suspicious or Policy-Violating Traffic Identified

PCAP File	Traffic Type Observed	Protocol(s)	Source IP	Destination IP / Domain	Why This Is Concerning
block-5-01.pcap	Suspicious outbound connections	HTTPS, DNS	Internal host	Unusual external domain	Possible command-and-control beaconing behavior
block-5-02.pcap	Phishing-related traffic	HTTP, TLS	Internal workstation	Look-alike domain	User accessed a domain mimicking a legitimate service
block-5-03.pcap	Unauthorized file download	HTTP	Internal host	File-sharing site	Executable file downloaded from non-approved source
block-5-04.pcap	Encrypted traffic with key log provided	TLS 1.3	Internal system	External server	Encrypted session potentially hiding malicious

					payload delivery
block-5-05.pcap	Anonymization/Tunneling indicators	DNS, TLS	Internal device	Suspicious domain pattern	Traffic patterns consistent with anonymization services
block-5-06.pcap	Large data transfer	HTTPS	Internal workstation	Cloud storage service	Possible unauthorized data exfiltration
block-5-07.pcap	Repeated connection attempts	TCP	Internal host	Multiple external IPs	Scanning or automated activity detected
block-5-08.pcap	Unapproved remote access behavior	TLS, TCP 443	Internal workstation	Unknown remote host	Potential remote control session established

Part C: Evidence & Interpretation

For each example identified above, traffic patterns, protocol behavior, and destination characteristics were analyzed.
Evidence included repeated outbound connections, suspicious domain naming conventions, file download activity,
large encrypted transfers, and unusual connection frequency.

Some examples indicate potential confirmed malicious activity, such as phishing-related traffic and suspicious
remote access sessions. Others represent policy violations, such as downloading files from unapproved sources
or using anonymization services that violate acceptable use policies.

Additional information needed to confirm intent would include endpoint logs, user authentication records,

antivirus alerts, firewall logs, and confirmation from the user regarding activity legitimacy.
Correlating network traffic with endpoint behavior would help determine whether the activity was intentional, accidental, or malicious.

Part D: Analyst Decision-Making

When responding to confirmed malicious activity, an analyst should immediately contain the threat by isolating
affected systems, blocking malicious domains or IP addresses, preserving evidence, and escalating the incident
according to the organization's incident response plan.

For policy violations that are not necessarily malicious, the response may involve documenting the activity,
notifying management, providing user education, or applying administrative controls rather than initiating
full incident response procedures. The key difference is that confirmed attacks require containment and
eradication, while policy violations typically require corrective action and monitoring.