Network Traffic Logs

Network Traffic Log 1 – Low Complexity (Initial Probing)

Timestamp: 10:01:12

Source IP: 192.168.1.25

Destination IP: 192.168.1.1

Traffic Volume (MB): 1.2

Activity: Normal Internal Access

Notes: Routine login from workstation

Timestamp: 10:03:15

Source IP: 192.168.1.50

Destination IP: 203.0.113.1

Traffic Volume (MB): 3.6

Activity: Web Browsing

Notes: Web traffic to a known site

Timestamp: 10:05:20

Source IP: 10.0.0.45

Destination IP: 192.168.1.60

Traffic Volume (MB): 0.7

Activity: Remote Connection

Notes: External server connection

Timestamp: 10:08:50

Source IP: 192.168.1.10

Destination IP: 104.16.249.1

Traffic Volume (MB): 50.0

Activity: Data Download

Notes: Large download from unknown IP

Timestamp: 10:12:25

Source IP: 192.168.1.40

Destination IP: 10.0.0.145

Traffic Volume (MB): 0.9

Activity: Network Ping

Notes: Internal ping

Network Traffic Log 2 – Medium Complexity (Data Exfiltration)

Timestamp: 11:15:10

Source IP: 192.168.1.25

Destination IP: 10.1.1.1

Traffic Volume (MB): 2.1

Activity: Internal File Transfer

Notes: File sharing between systems

Timestamp: 11:16:32

Source IP: 192.168.1.10

Destination IP: 198.51.100.3

Traffic Volume (MB): 25.0

Activity: External Data Transfer

Notes: Unknown IP—possible exfiltration

Timestamp: 11:18:50

Source IP: 10.0.0.2

Destination IP: 192.168.1.25

Traffic Volume (MB): 0.5

Activity: Remote Access

Notes: Suspicious external access

Timestamp: 11:20:15

Source IP: 192.168.1.50

Destination IP: 10.0.0.200

Traffic Volume (MB): 0.8

Activity: Internal Server Request

Notes: Normal internal activity

Timestamp: 11:21:10

Source IP: 192.168.1.45

Destination IP: 203.0.113.6

Traffic Volume (MB): 45.0

Activity: Large Data Transfer

Notes: Major outbound transfer

Network Traffic Log 3 – High Complexity (Escalation and DDoS Attempt)

Timestamp: 12:10:05

Source IP: 192.168.1.12

Destination IP: 203.0.113.45

Traffic Volume (MB): 250.0

Activity: Sudden Traffic Spike

Notes: Massive outbound transfer (DDoS)

Timestamp: 12:11:45

Source IP: 198.51.100.2

Destination IP: 192.168.1.50

Traffic Volume (MB): 0.9

Activity: Unauthorised Access

Notes: Suspicious connection attempt

Timestamp: 12:13:00

Source IP: 192.168.1.5

Destination IP: 192.168.1.12

Traffic Volume (MB): 0.3

Activity: Internal Access

Notes: Normal internal access

Timestamp: 12:15:20

Source IP: 192.168.1.100

Destination IP: 203.0.113.40

Traffic Volume (MB): 300.0

Activity: Large External Transfer

Notes: Possible data breach—critical

Timestamp: 12:16:40

Source IP: 192.168.1.80

Destination IP: 104.16.0.1

Traffic Volume (MB): 500.0

Activity: DDoS Traffic Spike

Notes: Distributed attack—system overload

Red Team Attack Instructions

These will guide the Red Team (Attackers) in launching a variety of cyberattacks to test the defences of the Blue Team.

Red Team Attack Instructions

1. Phase 1 - Initial Probing

   Attack Type: Reconnaissance

   - Insert a fake IP into the network logs.
   - Monitor responses from the Blue Team.

     Objective: Gather information and see if the Blue Team responds to unfamiliar IP addresses.
2. Phase 2 - Data Exfiltration

   Attack Type: Data Breach

   - Start a data transfer from an internal IP to an unknown external IP.
   - Slowly increase traffic volume to avoid immediate detection.

     Objective: See how the Blue Team responds to abnormal traffic volume.
3. Phase 3 - DDoS Simulation

   Attack Type: Distributed Denial-of-Service (DDoS)

   - Simulate multiple IPs sending massive data packets to overwhelm the server.

     Objective: Overwhelm the network and force the Blue Team to take drastic actions.

Blue Team Role Cards

These cards outline the roles and responsibilities for each Blue Team member, ensuring everyone knows what to do.

Blue Team Role Cards

Network Admin

- Role: Monitor real-time traffic logs, identifying potential issues.
- Task: Flag any unusual activity (e.g., spikes in traffic, unfamiliar IPs).

Incident Response Lead

- Role: Coordinate the team’s response to each attack and communicate findings.
- Task: Write reports on the incidents and make decisions on containment strategies.

Security Analyst

- Role: Investigate whether suspicious IPs or unusual traffic patterns are truly malicious.
- Task: Use all available data to confirm or deny suspicious activity, guiding the team's actions.

Resource:

- Blue Team Role Cards with a brief explanation of their duties.

Problem-Solving Prompts

These prompts help the Blue Team ask critical questions during their investigation.

Prompts:

- "Is this spike in data transfer normal for this time of day?"
- "Is the IP address attempting to connect part of our internal network?"
- "What steps should we take to contain this threat?"

Resource:

- Print or display Problem-Solving Prompts on the classroom board to guide their thought process.

Incident Response Log Template

Learning Objectives:

I can work with my team to detect and respond to multiple cyberattacks.

I can analyse network traffic to identify abnormal patterns and respond to them in real-time.

I can develop strategies to mitigate cyber threats during a network breach.

Incident Log

Incident #	Incident Description	Actions Taken	Outcome	Further Action Needed
1				
2				
3				
4				

Detailed Incident Analysis

For each incident, reflect on the following:

1. Incident Overview

Provide a brief summary of the incident (e.g., abnormal network activity, unauthorised access attempts). Why did you flag this as a potential attack?

---

2. Team Response

Describe the steps your team took to investigate and mitigate the incident. Who took charge of which actions? How was the decision-making process handled?

3. Outcome and Reflection

Was the attack fully mitigated, or did more issues arise? What could have been done better? Reflect on the strategies you employed.

4. Next Steps/Recommendations

What are your recommendations for preventing similar incidents in the future? How can network security be improved based on this event?

Date: _____

Team Lead Signature: _____