**Lab 2: Network Packet Analysis**

Kismat Kunwar, Tyler Joseph

Tagliatela College of Engineering

CSCI-4449-01/CSCI-6658-01: **Network Defense**

Dr. Tirthankar Ghosh

September 16, 2025

# Objective

The main objective of this lab is to analyze captured network packets using Wireshark to detect malicious activities and map them to MITRE ATT&CK techniques.

# Systems Needed

Any system with **Wireshark** installed

# Implementation Steps

## Part 1: Analyzing `pcap.pcapng`

***Unwanted activities***

The capture shows ICMP Echo Requests used as ping sweeps. The attacker sent repeated echo requests to test if the target was alive. This is the first step of reconnaissance.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 1: screenshot of ICMP Echo Request

A screenshot of a computer

AI-generated content may be incorrect.

Figure 2:screenshot of ICMP Echo Reply

Next is UDP scanning. About 1000 destination ports were probed. This confirmed that the attacker was testing services over UDP SHOWN IN figure 3.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 3; Wireshark Endpoints Statistics – UDP traffic

TCP SYN scanning followed. Roughly 1000 SYN probes were sent to different ports. SYN and SYN/ACK pairs in the capture confirm the attacker was checking for open TCP services confirmed by figure 4 and figure 5.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 4: Wireshark Endpoints Statistics: TCP traffic

A screenshot of a computer

AI-generated content may be incorrect.

Figure 5: Snippet of Count of TCP SYN probes and SYN/ACK replies

The last stage is TCP connect attempts. Fifteen ports completed the three-way handshake. Each was then reset. This shows the attacker tried to confirm open services shown in figure 6.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 6:TCP handshake completed

Altogether, these activities represent a staged reconnaissance effort that aligns with an Nmap-style port scan. The sequential use of ICMP sweeps, UDP scans, TCP SYN scans, and TCP connect probes shows a methodical process of mapping the target host’s services and network exposure.

* **Attacker IP:** 10.1.1.34
* **Target IP:** 10.1.1.36

Altogether, these activities represent a staged reconnaissance effort that aligns with an Nmap-style port scan. The sequential use of ICMP sweeps, UDP scans, TCP SYN scans, and TCP connect probes shows a process of mapping the target host’s services and network exposure. The attacker at 10.1.1.34 scanned the target 10.1.1.36 using multiple methods.

## MITRE ATT&CK Mapping

* **Tactics:** Reconnaissance, Discovery
* **Techniques:**
  + T1595 – Active Scanning
  + T1046 – Network Service Scanning

# Part 2: Analyzing `exploit.pcapng`

## Unwanted activities

TFTP Read Request for Malicious Script  
The traffic in pcap shows post-exploitation activity between attacker 10.1.1.34 and victim 10.1.1.36. The first step shown in figure 7 is a TFTP **Read Request (RRQ)** where the victim pulls post\_exploit.ps1 from the attacker machine

A screenshot of a computer

AI-generated content may be incorrect.

Figure 7:Wireshark capture showing TFTP Read Request for post\_exploit.ps1

After the script is retrieved, the victim executes its functions. The packet capture confirms the script’s contents: commands for user account creation, registry modification, exfiltration, and cleanup. This step shows how the attacker establishes persistence, elevates privileges, and prepares for data theft shown in figure 8.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 8 : Reconstructed content of post\_exploit.ps1 from Wireshark “Follow UDP Stream

### TFTP Write Request (WRQ)

The confirmation of script execution is shown by creation and transfer of exfiltrate.txt. The victim sends a TFTP **Write Request (WRQ)** to upload the file back to the attacker machine at 10.1.1.34 shown in figure 9. This marks the data exfiltration phase, where sensitive information is sent over an unencrypted and insecure protocol.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 9: TFTP WRQ showing exfiltrate.txt

## Protocol

For malicious activities as discussed above in unwanted activities section Trivial File Transfer Protocol is used shown in figure 10.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 10: TFTP used for post exploitation and exfiltration

## MITRE ATT&CK Mapping

#### Tactics

* **Execution (TA0002):** The attacker downloads and executes the malicious script post\_exploit.ps1.
* **Persistence (TA0003):** The script creates a registry run key to ensure execution on startup.
* **Privilege Escalation (TA0004):** The script adds a new administrator account called User\_Admin.
* **Exfiltration (TA0010):** The script transfers exfiltrate.txt back to the attacker system.
* **Command and Control (TA0011):** TFTP is used as a lightweight channel for attacker–victim communication.

**Techniques**

* **T1105 – Ingress Tool Transfer:** post\_exploit.ps1 is pulled onto the victim machine.
* **T1547.001 – Registry Run Keys / Startup Folder:** Persistence mechanism implemented inside post\_exploit.ps1.
* **T1136 – Create Account:** New admin account creation via the script.
* **T1048.003 – Exfiltration Over Unencrypted/Obsolete Protocol:** Data exfiltration over TFTP (exfiltrate.txt).
* **T1071.004 – Application Layer Protocol: TFTP:** Misuse of TFTP as the communication protocol.

# Observation

The packet captures show two stages of attacker activity. In Part 1, the attacker at 10.1.1.34 performed reconnaissance against the target 10.1.1.36. The capture confirmed ICMP sweeps, UDP port scanning, TCP SYN scans, and TCP connect attempts. This sequence matches an Nmap-style port scan used to map live hosts and available services.

In Part 2, the focus shifted to post-exploitation. The attacker 10.1.1.34 used TFTP to transfer files with the victim 10.1.1.36. First, the victim retrieved the malicious script post\_exploit.ps1 from the attacker. The script contained functions for account creation, registry persistence, exfiltration, and cleanup. After execution, the victim uploaded exfiltrate.txt to the attacker. This confirmed data exfiltration over TFTP.

Both stages demonstrate a complete attack chain: reconnaissance, exploitation, persistence, privilege escalation, and exfiltration.

# Conclusion

The lab showed how Wireshark can be used to trace the full lifecycle of an attack. In Part 1, packet analysis identified reconnaissance through ICMP, UDP, and TCP scanning. In Part 2, Wireshark confirmed post-exploitation behaviour including malicious script transfer, registry changes, new account creation, and exfiltration over TFTP. Mapping these actions to MITRE ATT&CK tactics and techniques highlights how packet-level evidence ties directly to known adversary behaviours. This reinforces the value of packet analysis for incident detection and response.

**Acknowledgments**. For this lab ChatGPT was used to assist with proofreading, gram-

mar correction, and stylistic improvements; all AI-generated suggestions were carefully reviewed and revised to ensure alignment with the lab’s objectives.