Government Polytechnic Kanpur
POST GRADUATE DIPLOMA IN CYBER SECURITY

LAB MANUAL

Networking Concepts & Security Lab Manual

Lab Title: [**Networking Concepts & Security Lab Manual**]
Subject: [Networking Concepts & Security]
Course: [POST GRADUATE DIPLOMA IN CYBER SECURITY]
Semester: [1st Semester)]
Session: [2024-2025]
Lab Instructor: [**Mr. Himanshu Singh**]

Submitted by:
Name:_____
Roll Number:_____
EnRollment Number:_____
Class: [INFORMATION TECHNOLOGY 5TH Semester]

INDEX

Networking Concepts & Security SYLLABUS:

DETAILED CONTENTS

Unit I:

Introduction to Network Security
Types of networks,
IP Address,
NAT,
IP Subnets,
DHCP Server,
Ports,
DNS,
Proxy Servers,
Virtual Private Networks,
DNS Server,
OSI and TCP/IP Model,
TCP Vs. UDP,
Routers,
Switches,
Endpoint solutions,
Access Directory,
TOR Network.
Networking Devices (Layer1,2,3) -
Different types of network layer attacks–
Firewall (ACL, Packet Filtering, DMZ, Alerts and
Audit Trails) – IDS, IPS and its types (Signature based, Anomaly based, Policy based, Honeypot based)
and setup.

Unit II:

Virtual Private Networks

VPN and its types
–Tunnelling Protocols
– Tunnel and Transport Mode
–Authentication Header
Encapsulation Security Payload (ESP)-
IPSEC Protocol Suite – IKE PHASE 1,
II – Generic Routing
Encapsulation (GRE).

Implementation of VPNs.

Unit III:

Network Attacks Part 1

Sniffing concepts,
Sniffing Techniques
MAC Attack,
DHCP attack,
ARP poisoning,
Spoofing,
DNS poisoning.
Wireshark,
packet analysis,
display and capture filters,
Ettercap,
sniffing counter
measures,
sniffing protection tools.
Denial of service (DOS)/Distributed Denial of service (DDOS):
Concepts, DOS/DDOS Technique,
Botnets,
DDOS, DOS/DDOS attacking tools,
DOS/DDOS counter Measures,
DOS/DDOS
protection tools.
Vulnerability scanning tools:
Concepts, Scanning Techniques,
Tools: Nessus,
OpenVAS,
Sparta,
Nexpose,
Nmap.
Network Scanning Report Generation,
Striping,
Router attacks,
VPN pentesting,
VOIP pentesting,
Enumeration techniques:
SMTP,
SNMP,
IPsec, VOIP,
RPC,

Telnet,
FTP,
TFTP,
SMP,
IPV6 and BGP.

Unit IV: Network Attacks Part 2

Network Exploitation OS Detection in network,
Scanning: nmap, open ports,
filtered ports,
service detection,
metasploit framework,
interface of metasploit framework,
network vulnerability
assessment, evade anti viruses and firewalls,
metasploit scripting,
exploits,
vulnerabilities,
payloads,
custom payloads
, nmap configuration,
Social Engineering toolkit,
Xero sploit Framework,
exploits
delivery, burp-suite,
End Point Security.

Unit V: Wireless Attacks

Wireless concept, wireless encryption, wireless threats, wireless hacking methodology, wireless hacking and security tools, Bluetooth hacking, countermeasures to wireless threats, Protocols, MAC
Filtering, Packet Encryption, Packet Sniffing, Types of authentications, ARP Replay attack, Fake Authentication Attack, De authentication, Attacks on WEP, WPA and WPA-2 Encryption, fake hotspots, evil twin attack, fluxion framework

List of Practical's:

1. **Brute force attack using open-source tools.**
2. **Identifying network attacks using Nmap, Metasploit.**
3. **Selecting a Capture Interface and creating the first pcap file using Wireshark.**
4. **Using Capture filters in Wireshark.**
5. **Finding a Text String in a Trace File using Wireshark.**
6. **Understanding Packet Loss and Recovery process.**
7. **Identifying DOS & DDOS Attack.**
8. **VPN & VOIP pentesting using open-source tools.**
9. **Demonstration of IDS using or any other open-source tool.**
10. **Demonstration of IPS using snort or any other open-source tool.**

List of Practical's:

1. Brute force attack using open-source tools.
2. Identifying network attacks using Nmap, Metasploit.
3. Selecting a Capture Interface and creating the first pcap file using Wireshark.
4. Using Capture filters in Wireshark.
5. Finding a Text String in a Trace File using Wireshark.
6. Understanding Packet Loss and Recovery process.
7. Identifying DOS & DDOS Attack.
8. VPN & VOIP pentesting using open-source tools.
9. Demonstration of IDS using or any other open-source tool.
10. Demonstration of IPS using snort or any other open-source tool.

Lab Manual: Finding a Text String in a Trace File Using Wireshark

Objective:

To learn how to find specific text strings in a network packet capture (trace file) using Wireshark.

Requirements:

- Wireshark (installed on your system)
- A trace file (PCAP file) with network traffic for analysis

Step-by-Step Instructions:

1. Capture or Open a Trace File

a. Opening a PCAP File:

- Launch Wireshark on your machine.
- Navigate to `File -> Open` or press `Ctrl+O`.
- Browse and select the PCAP file you want to analyze.

b. Capturing Live Traffic (Optional):

- If you don't have a pre-existing PCAP file, you can capture live network traffic:
  - Choose your network interface from the list (e.g., Ethernet, Wi-Fi).
  - Click on the blue shark fin icon (`Start Capture`) to start capturing.
  - Once enough packets are captured, click the red square (`Stop Capture`).

2. Identify Protocols Carrying Text Information

Wireshark captures packets for many protocols, but not all protocols carry human-readable text.

Common protocols that carry text data include:

- **HTTP (for web traffic)**
- **SMTP/IMAP/POP3 (for email)**
- **DNS (for domain queries)**
- **FTP (for file transfer)**

To focus your search, identify which protocols may contain the string you're looking for. You can use Wireshark's built-in filters to narrow down the traffic to relevant protocols before searching.

Example filters:

- For HTTP: `http`
- For DNS: `dns`
- For FTP: `ftp`

3. Finding a Specific Text String

Wireshark provides a tool to search for text strings within packet contents (such as URLs, payloads, or chat messages).

Steps:

- **Click on `Edit` from the menu and select `Find Packet` (or press `Ctrl+F`).**
- **In the search dialog box, select the `String` tab.**

Search by:

- **Packet List: Searches for the text in the main packet summary.**
- **Packet Details: Searches through the packet tree in the middle pane.**
- **Packet Bytes: Searches through the raw packet data in the bottom pane (this option is often used to find text embedded in payloads).**

Search options:

- **Enter the text string you want to search for.**
- **Choose how you want the search to be performed:**
  - **`ASCII` for human-readable text.**
  - **`UTF-8`, `UTF-16`, or other encodings depending on your expected data.**

Example: If you are looking for a specific website, you can type in part of the URL, such as `example.com`.

4. Filtering the Traffic for Specific Text

After locating the text, you can use Wireshark filters to narrow down the packet list to just those containing the string.

Example:

- If you found a string related to an HTTP GET request, filter by the HTTP protocol and search specifically for that request, e.g., `http contains "example.com"`.

5. Analyzing the Results

Once you have found the packet or packets containing the desired text string:

- **Inspect the packet:** Click on the packet in the list to see its details in the middle pane.
- **View payload:** If the string is within the packet payload, it will be highlighted in the hexadecimal and ASCII representation in the bottom pane.
- **Follow stream (Optional):** For protocols like HTTP or FTP, you can follow the entire conversation:
  - Right-click on the packet and choose `Follow -> TCP Stream` (or UDP Stream for UDP traffic).
  - This will show you the complete conversation between the client and server, making it easier to understand the context of the text string.

6. Exporting or Saving Packets

If the packet or stream is of particular interest, you can export it for further analysis:

- Go to `File -> Export Specified Packets`.
- Choose the packets you want to export and save them to a new PCAP file.

Example Scenario:

Objective:

Find a specific login string (e.g., "admin") in an HTTP packet capture.

1. **Open the capture file** containing HTTP traffic.
2. Use the `http` filter in the display filter bar to limit the capture to HTTP traffic.
3. Go to `Edit -> Find Packet`, select the `String` tab, and enter "admin" in the search box.
4. Choose `Packet Bytes` and `ASCII` as the search options.
5. Wireshark will highlight the first packet containing the string "admin" in its payload.
6. Once found, you can follow the TCP stream to see the entire HTTP conversation (e.g., login request).

Explanation:

Wireshark captures all network traffic, including the packet headers and payloads. Many protocols (such as HTTP, FTP, and SMTP) transport human-readable text, often revealing usernames, URLs, or other data in plaintext if not encrypted.

By searching for a text string in the captured packets, Wireshark allows analysts to pinpoint sensitive information, locate specific communication, or debug network problems. This feature is especially useful when investigating login attempts, file transfers, or web requests, as these may contain important strings like URLs, usernames, commands, or search terms.

Lab Questions:

1. What types of protocols typically carry human-readable text?
2. How would you search for a specific username in an FTP conversation?
3. How can you narrow your search if you suspect the text string is part of an HTTP POST request?
