Contents

Introduction to Networking

What is Networking? (LAN, WAN, Internet)

Networking is the practice of transporting and exchanging data between nodes over a shared medium.

- LAN (Local Area Network): A network connecting devices within a limited area (home, office).
- WAN (Wide Area Network): Connects multiple LANs over large distances (ISP networks).
- The Internet: The global system of interconnected computer networks.

Packet Tracer 8.2:

1. Open Packet Tracer. Look at the bottom-left corner for device categories.
2. Create a LAN: Click Network Devices > Switches. Drag a 2960 Switch to the canvas.
3. Click End Devices > PC. Drag two PCs onto the canvas.
4. Click the Connections (Lightning Bolt) icon. Select Copper Straight-Through (solid black line). Connect PC0 (FastEthernet0) to Switch (FastEthernet0/1). Repeat for PC1.
5. Create a WAN Link: Add a 4331 Router. Connect the Switch to the Router (GigabitEthernet). This Router acts as the gateway to the "outside" world (WAN).

OSI & TCP/IP Models

These models describe how data moves across a network.

- OSI (Open Systems Interconnection): 7 Layers (Physical, Data Link, Network, Transport, Session, Presentation, Application).
- TCP/IP: 4 Layers (Network Access, Internet, Transport, Application).

Packet Tracer (Visualizing the Layers):

1. Set up the simple LAN from the previous step.
2. Assign IP addresses to the PCs (Click PC > Desktop > IP Configuration). Set PC0 to 192.168.1.1 and PC1 to 192.168.1.2.
3. Switch to Simulation Mode (Bottom right corner, or Shift+S).
4. Click the Add Simple PDU (closed envelope icon) on the top toolbar. Click PC0 then PC1.
5. Press Play. You will see the packet travel. Click the colored square (the packet) in the Simulation Panel to open the PDU Information.
6. Inspect Layers: You will see the "OSI Model" tab showing Layer 1 (Port), Layer 2 (MAC), and Layer 3 (IP) details.

5 Examples of Layers/Protocols:

1. Layer 1 (Physical): Ethernet Cables, Fiber Optics.
2. Layer 2 (Data Link): MAC Addresses, VLANs.
3. Layer 3 (Network): IP Addresses, Routers.
4. Layer 4 (Transport): TCP (reliability), UDP (speed).
5. Layer 7 (Application): HTTP (Web), SMTP (Email).

IPv4 & IPv6 Addressing

Notes:

- IPv4: 32-bit address (e.g., 192.168.1.1). Running out of addresses.
- IPv6: 128-bit hexadecimal address (e.g., 2001:db8::1). Virtually infinite space.
- Subnetting: Dividing a large network into smaller, manageable networks.

IPv4 Addressing (The Old Standard)

Structure & Classes

An IPv4 address is a 32-bit number, typically displayed as four decimal numbers (0-255) separated by dots (e.g., 192.168.1.1).

- Total Addresses: ~4.3 Billion (We ran out of these years ago).
- Structure: Network Portion (Street name) + Host Portion (House number). The Subnet Mask tells computers where the Network part ends and the Host part begins.

The "Classful" System:

- Class A: 1.0.0.0 to 126.0.0.0 (Huge networks, supports 16M hosts).
- Class B: 128.0.0.0 to 191.255.0.0 (Medium networks, supports 65k hosts).
- Class C: 192.0.0.0 to 223.255.255.0 (Small networks, supports 254 hosts).
- *Note: 127.0.0.0/8 is reserved for Loopback (Localhost).*

Private Addresses (RFC 1918):

These are free to use in your LAN but cannot route over the internet.

1. 10.0.0.0 - 10.255.255.255 (Enterprise)
2. 172.16.0.0 - 172.31.255.255 (Labs/Docker)
3. 192.168.0.0 - 192.168.255.255 (Home)

Subnetting (CIDR)

Subnetting is borrowing bits from the Host portion to create more Networks. We use CIDR (Classless Inter-Domain Routing) notation, like /24.

- /24 means the first 24 bits are the Network.
  - Mask: 255.255.255.0
  - Available IPs: 254
- /25 means the first 25 bits are the Network (we split the /24 in half).
  - Mask: 255.255.255.128
  - Available IPs: 126

Note: Activities on IPv4 Subnetting will be dependent on the trainer.

IPv6 Addressing (The New Standard)

Structure & Hexadecimal

An IPv6 address is 128-bit, written in Hexadecimal (0-9, A-F), separated by colons.

- Example: 2001:0DB8:85A3:0000:0000:8A2E:0370:7334
- Total Addresses: 3.4×10^{38} (Undecillion). Every grain of sand on Earth could have its own IP.

Shortening Rules (Important):

1. Leading Zeros: You can remove zeros at the start of a block.
   - 0DB8 -> DB8
2. Double Colon (::): You can replace *one* contiguous string of zero blocks with ::.
   - 2001:0DB8:0000:0000:0000:0000:0000:0001 becomes 2001:DB8::1

IPv6 Address Types

Unlike IPv4, a single interface often has multiple IPv6 addresses.

1. Global Unicast (GUA): Begins with 2000::/3. Same as a Public IPv4. Routable on the internet.
2. Link-Local (LLA): Begins with FE80::/10. Mandatory. Only works on the local wire (like a shout in a room). Routers do *not* forward this.
3. Unique Local (ULA): Begins with FC00::/7. Same as Private IPv4.
4. Loopback: ::1 (Same as 127.0.0.1).

Step-by-Step in Packet Tracer (IPv6)

Enable IPv6 and configure addresses.

1. Router Config:
   - *Note: IPv6 routing is usually disabled by default on older Cisco IOS versions.*

```
enable
conf t
ipv6 unicast-routing   <-- CRITICAL STEP
interface g0/0/0
ipv6 address 2001:DB8:ACAD:1::1/64
ipv6 address fe80::1 link-local
no shutdown
```

2. PC Config:
   - Click PC > Desktop > IP Configuration.
   - IPv6 Address: 2001:DB8:ACAD:1::10
   - Prefix Length: 64
   - IPv6 Gateway: fe80::1 (Best practice is to use the Router's Link-Local address as the gateway).

3. Test:
   - PC Command Prompt: ping 2001:DB8:ACAD:1::1

Network Devices & Protocols

Devices (Switch, Router, AP, Firewall)

- Switch: Connects devices in a LAN; uses MAC addresses.
- Router: Connects different networks (LAN to WAN); uses IP addresses.
- Access Point (AP): Connects wireless devices to the wired network.
- Firewall: Filters traffic based on security rules.

Step-by-Step in Packet Tracer:

1. Switch & Router: You likely added these in Section 1.
2. Add Wireless: Go to Network Devices > Wireless Devices. Drag a Home Router or Access Point.
3. Add Firewall: Go to Network Devices > Security. Drag an ASA 5505.
4. Connect a PC to the Wireless Router (the PC requires a wireless module: Turn off PC, remove Ethernet module, insert WMP300N, turn on PC).

Examples

1. Cisco Catalyst 2960: Common Layer 2 Switch.
2. Cisco ISR 4331: Integrated Services Router.
3. Cisco Meraki MR: Wireless Access Point.
4. Cisco ASA 5506-X: Next-Generation Firewall.
5. Layer 3 Switch (3560): Can switch and route simultaneously.

Protocols (TCP/UDP, DHCP, DNS, HTTPS, ICMP)

Notes

- TCP/UDP: Transport protocols. TCP is reliable (handshake); UDP is fast (streaming).
- DHCP: Automatically assigns IPs.
- DNS: Translates names (https://www.google.com/search?q=google.com) to IPs.
- ICMP: Used for diagnostics (Ping).

Packet Tracer (DHCP Setup):

1. Place a Router and a Switch. Connect them.
2. Click Router > CLI tab. Type no if asked for initial config.
3. Enter commands:

```
enable
conf t
interface g0/0/0
ip address 192.168.1.1 255.255.255.0
no shutdown
exit
ip dhcp pool MYPOOL
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
```

4. Go to a connected PC > Desktop > IP Configuration. Switch from Static to DHCP. It should request and receive an IP.

Examples of Protocol Use:

1. HTTPS (Port 443): Secure banking website.
2. DNS (Port 53): Typing www.facebook.com instead of an IP.
3. DHCP (Port 67/68): Connecting your phone to Wi-Fi and instantly getting online.
4. ICMP: Using the ping command to check if a server is up.
5. UDP: Voice over IP (VoIP) calls where slight data loss is acceptable for speed.

Routing & Switching Essentials

Static vs Dynamic Routing

Notes

- Static: Admin manually types every route. Secure but hard to scale.
- Dynamic (OSPF, EIGRP): Routers talk to each other to find the best path automatically.

Packet Tracer (Static Route):

1. Setup 2 Routers (R1 and R2) connected via a serial or fiber cable. Connect a LAN to each.
2. On R1 CLI:

```
enable
conf t
ip route [Destination_Network] [Mask] [Next_Hop_IP]
```

   Example: ip route 192.168.2.0 255.255.255.0 10.0.0.2

3. Verify: Use the command do show ip route. Static routes are marked with S.

Routing Concepts:

1. Static Route: Good for small "stub" networks with only one exit.
2. Default Route: ip route 0.0.0.0 0.0.0.0 [Next-Hop]. "If you don't know where to send it, send it here."
3. RIP (Routing Information Protocol): Old, simple, uses hop count.
4. OSPF (Open Shortest Path First): Industry standard for large internal networks.
5. BGP (Border Gateway Protocol): The routing protocol of the Internet.

VLANs (Virtual LANs)

VLANs logically separate a physical switch into different networks. This improves security and reduces traffic congestion (broadcast domains).

Packet Tracer:

1. Click a Switch > CLI.
2. Create VLAN:

```
enable
conf t
vlan 10
name STAFF
exit
```

3. Assign Port to VLAN:

```
interface fa0/1
switchport mode access
switchport access vlan 10
```

4. Hover over the switch port in the workspace; you will see it is now in VLAN 10 (not default VLAN 1).

Examples of VLANs:

1. Data VLAN: Normal employee computers.
2. Voice VLAN: Dedicated for VoIP phones (ensures call quality).
3. Management VLAN: For admins to configure network devices.
4. Guest VLAN: Isolated Wi-Fi for visitors (cannot access Data VLAN).
5. Native VLAN: Used for trunk links between switches.

NAT (Network Address Translation)

NAT translates Private IPs (internal) to Public IPs (internet). This saves public IP addresses and hides internal network structure.

Packet Tracer (NAT Overload / PAT):

1. On a Router connecting LAN (inside) and Internet (outside).
2. Define Interfaces:

```
int g0/0 (LAN) -> ip nat inside
int g0/1 (WAN) -> ip nat outside
```

3. Create Access List (Who is allowed?):

```
access-list 1 permit 192.168.1.0 0.0.0.255
```

4. Enable NAT:

```
ip nat inside source list 1 interface g0/1 overload
```

Examples of NAT Types:

1. Static NAT: One-to-one mapping (Used for Web Servers).
2. Dynamic NAT: Mapping internal IPs to a pool of public IPs.
3. PAT (Port Address Translation): Many internal devices sharing ONE public IP (Home routers do this).
4. Port Forwarding: Allowing external users to access a specific game server or camera inside your home.
5. CGNAT (Carrier Grade NAT): ISPs doing NAT on a massive scale for mobile phones.

Network Services

DHCP and DNS Fundamentals

- DHCP (Dynamic Host Configuration Protocol): Automates the assignment of IP addresses, Subnet Masks, Gateways, and DNS servers to clients. Without it, every device needs manual configuration.
- DNS (Domain Name System): Acts as the phonebook of the internet, resolving human-readable names (e.g., google.com) into machine-readable IP addresses (e.g., 142.250.1.1).

Packet Tracer (Server Setup):

1. Place a Server-PT and a Switch. Connect them. Connect a PC to the Switch.
2. Configure Server IP: Click Server > Desktop > IP Configuration. Set Static IP: 192.168.1.10, DNS Server: 127.0.0.1.
3. Enable DHCP:
   - Go to Services tab > DHCP.
   - Service: On.
   - Default Gateway: 192.168.1.1.
   - DNS Server: 192.168.1.10.
   - Start IP: 192.168.1.100.
   - Click Save.
4. Enable DNS:
   - Go to Services tab > DNS.
   - Service: On.
   - Name: mywebsite.local.
   - Address: 192.168.1.10 (The server itself).
   - Click Add.
5. Test:
   - On the PC, set IP to DHCP. It should get 192.168.1.100.
   - Open PC Web Browser, type mywebsite.local. It should load the default server page.

Windows vs. Ubuntu Commands:

- Refresh DHCP:
  - Windows: ipconfig /release then ipconfig /renew
  - Ubuntu: sudo dhclient -r (release) then sudo dhclient (renew)
- Query DNS:
  - Windows: nslookup google.com
  - Ubuntu: dig google.com or nslookup google.com

Notes:

1. DHCP Lease: An IP is "loaned" to a coffee shop customer for 1 hour.
2. A Record: Standard DNS mapping (Host -> IPv4).
3. AAAA Record: DNS mapping for IPv6.
4. CNAME: Alias (e.g., www.site.com points to site.com).
5. DHCP Reservation: Using a MAC address to ensure a printer always gets the same "dynamic" IP.

VPN Basics (Virtual Private Network)

VPNs create a secure, encrypted "tunnel" over a public network (Internet). It preserves privacy and allows remote users to access the internal LAN as if they were physically there.

Packet Tracer Limit: PT supports Site-to-Site VPNs (connecting two routers) but has limited support for Client-to-Site (PC software) VPNs compared to real life.

Packet Tracer (Simple Concept):

- *Note: Full IPsec configuration is complex for beginners. We will simulate the "connectivity".*

1. In PT, use the VPN tab on a PC (Desktop > VPN) if a specific VPN server is configured, but usually, this is taught via Router-to-Router IPsec.
2. Concept: Two routers (HQ and Branch) configured with "Crypto Maps". When traffic matches the map (e.g., Branch trying to talk to HQ Server), the router encrypts it before sending it to the cloud.

VPN Scenarios:

1. Remote Access VPN: Employee working from home.
2. Site-to-Site VPN: Connecting New York office to London office.
3. SSL VPN: VPN accessed via a web browser (Clientless).
4. IPsec: Layer 3 encryption suite, very secure, harder to set up.
5. Split Tunneling: Routing only corporate traffic through VPN, while Spotify goes via normal internet.

Security Fundamentals

CIA Triad & Common Threats

- Confidentiality: Only authorized people can see data (Encryption).
- Integrity: Data has not been altered (Hashing).
- Availability: Data is accessible when needed (Redundancy).

Common Threats:

1. Phishing: Deceptive emails stealing credentials.
2. DDoS (Distributed Denial of Service): Flooding a server to crash it.
3. Malware: Ransomware, Viruses, Trojans.
4. Insider Threats: Disgruntled employees leaking data.
5. Man-in-the-Middle: Intercepting traffic between two parties.

Firewall Configuration & ACLs

Firewalls block or allow traffic based on rules. In Cisco routers, these rules are called Access Control Lists (ACLs).

Packet Tracer (Standard ACL):
Task: Block PC1 (192.168.1.2) from accessing the Server, allow everyone else.

1. Router CLI:

```
enable
conf t
access-list 10 deny host 192.168.1.2
access-list 10 permit any
interface g0/0  (The interface facing the LAN)
ip access-group 10 in
```

2. Test: PC1 pinging the server should fail (Destination host unreachable). PC2 should succeed.

Windows vs. Ubuntu Firewalls:

- Windows: Search for Windows Defender Firewall with Advanced Security. Create "Inbound Rule" > Block Port 80.
- Ubuntu: Use UFW (Uncomplicated Firewall).
  - sudo ufw enable
  - sudo ufw deny 22 (Block SSH)

Examples of ACL Rules:

1. Deny Specific IP: Block a known hacker IP.
2. Permit HTTP: Allow traffic on Port 80.
3. Deny ICMP: Stop people from pinging your router.
4. Time-Based ACL: Allow Facebook only during lunch break (Advanced).
5. Established: Allow traffic only if it is a reply to a request initiated from inside.

Encryption: SSH vs Telnet

- Telnet: Sends data (including passwords) in plain text. Anyone with a sniffer (like Wireshark) can read it.
- SSH (Secure Shell): Encrypts the entire session.

Packet Tracer (Secure the Router):

1. Enable Hostname & Domain (Required for crypto keys):

```
hostname R1
ip domain-name mylab.com
```

2. Generate Keys:

```
crypto key generate rsa
(Enter 1024)
```

3. Enable SSH on VTY Lines:

```
username admin secret cisco
line vty 0 4
transport input ssh
login local
```

4. Test: From a PC Command Prompt: ssh -l admin 192.168.1.1. You will be prompted for the password.

Monitoring & Incident Response

Using Logs for Detection (Syslog)

Network devices generate logs (warnings, errors, status changes). Centralizing these is crucial.

Packet Tracer (Syslog):

1. Setup: Add a Server-PT. Enable Syslog service (Service > Syslog > On).
2. Configure Router to send logs:

```
logging host 192.168.1.10  (IP of your Syslog server)
logging trap debugging
```

3. Trigger Log: Go to Router CLI, enter/exit configuration mode, or unplug a cable.
4. Check Server: Go to Server > Services > Syslog. You will see the log entries appear there remotely.

Windows vs. Ubuntu Logs:

- Windows: Event Viewer (eventvwr). Look under "Windows Logs" > "Security".
- Ubuntu: Check /var/log/syslog or /var/log/auth.log.
    - Command: tail -f /var/log/auth.log (Monitor login attempts in real-time).

SIEM Overview (Wazuh)

A SIEM (Security Information and Event Management) system, like Wazuh, collects logs from Windows, Ubuntu, and Routers, analyzes them for patterns, and alerts you.

- *Note: Packet Tracer cannot run Wazuh. This is a theoretical component or requires Virtual Machines.*

Ubuntu Implementation (Concept):

1. You install the Wazuh Manager on an Ubuntu Server.
2. You install Wazuh Agents on Windows/Ubuntu clients.
3. The agent reads the logs and sends them to the Manager.
4. The Manager has a dashboard (web UI) showing "Brute Force Attack Detected" if someone fails SSH login 10 times.

Setting up a Wazuh SIEM (Security Information and Event Management) environment.

Setup:

- Server (Manager): Ubuntu (Where logs are analyzed).
- Client (Agent): Windows (Where logs are collected).

1. Install Wazuh Manager on Ubuntu

We will use the Quickstart installation script. This installs all components (Indexer, Server, Dashboard) in one go.

Prerequisites:

- Ubuntu 20.04 or 22.04 LTS.
- Minimum 4GB RAM (Wazuh is heavy; 2GB might crash).
- Root privileges (sudo).

Step 1: Update System

Open your terminal and ensure your system is clean.

```
sudo apt update && sudo apt upgrade -y
sudo apt install curl -y
```

Step 2: Run the Installation Script

Run the official Wazuh installation script. This automates about 50 manual steps.

```
curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

(Note: The installation takes 5-10 minutes depending on internet speed.)

Step 3: Save Your Credentials

Once finished, the terminal will display a summary like this:

```
User: admin
Password: [A_Random_Generated_String]
```

COPY THIS PASSWORD IMMEDIATELY. You cannot retrieve it easily later.

Step 4: Configure UFW (Firewall)

We must open the ports so the Windows Agent can talk to Ubuntu.

```
# Dashboard access
sudo ufw allow 443/tcp
# Agent connection
sudo ufw allow 1514/tcp
# Agent enrollment
sudo ufw allow 1515/tcp
# API
sudo ufw allow 55000/tcp
# Reload firewall
sudo ufw reload
```

2. **Access the Dashboard**
    a. On your computer (or the Windows machine), open a web browser.
    b. Type: https://<UBUNTU_IP_ADDRESS>
        a. *Example: https://192.168.1.10*
    c. Security Warning: You will see a warning "Your connection is not private".
        a. This is normal (self-signed certificate).
        b. Click Advanced > Proceed to... (unsafe).
    d. Login with admin and the password you saved in Phase 1.

3. **Install Wazuh Agent on Windows**

Install the agent is using the Dashboard's built-in wizard.

Step 1: Generate the Command

a. In the Wazuh Dashboard, click the "Add agent" button (usually on the main screen or under the "Agents" tab).
b. Operating System: Select Windows MSI (64-bit).
c. Wazuh Server address: Enter the IP Address of your Ubuntu Server (e.g., 192.168.1.10).
d. Group: Leave as default.
e. Run Command: The dashboard will generate a PowerShell command at the bottom. Copy this command.

Step 2: Run on Windows

a. On your Windows machine, open PowerShell as Administrator (Right-click Start > Terminal (Admin) or PowerShell (Admin)).
b. Paste the command you copied. It will look something like this:

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.x.msi -OutFile wazuh-agent.msi; ...
```

c. Press Enter. It will download the installer, install it, and configure the IP automatically.

Step 3: Start the Agent

Once the installation finishes, start the service:

```
NET START Wazuh
```

4. **Verification and Testing**
    a. Check Connection
    - Go back to your Wazuh Dashboard.
    - Click on the Wazuh logo (top left) to refresh.
    - You should see Total Agents: 1 and Active Agents: 1.

    b. Test with a Fake "Attack"
    Let's simulate a simple event to see if Wazuh catches it.
    - On Windows: Attempt to log in with a fake user 5 times via RDP or "Run as different user".
    - On Dashboard:
        1. Click on the Agent (Windows).
        2. Go to Security Events.
    - Look for alert ID 5710 ("Attempt to login using a non-existent user").

Troubleshooting Common Issues

Issue	Solution
Agent never appears in Dashboard	1. Check if Ubuntu UFW allows port 1514/1515. 2. Can Windows ping Ubuntu? 3. Check Windows logs: C:\Program Files (x86)\ossec-agent\ossec.log.
"Connection Refused" in Browser	Ensure the Wazuh services are running on Ubuntu: sudo systemctl status wazuh-dashboard.
Forgot Password	You can reset it using the wazuh-indexer tool, but it's complex. It's often faster to reinstall for labs.

Incident Response Steps

Discussion: When a breach happens, follow the PICERL framework (SANS Institute model).
Incident Response Lifecycle:

1. Preparation: Setting up the Firewalls and SIEM *before* the attack.
2. Identification: Noticing the CPU usage is 100% and weird logs appear (DDoS).
3. Containment: Unplugging the infected cable or isolating the VLAN to stop the spread.
4. Eradication: Re-imaging the machine or removing the malware.
5. Recovery: Restoring data from backups and watching closely.
6. Lessons Learned: Updating the policy so it doesn't happen again.

Additional Activities

Lab 1: Configure Firewall Rules (UFW & iptables)

We will look at two ways to control traffic on Ubuntu: UFW (easy mode) and iptables (legacy/advanced mode).

UFW (Uncomplicated Firewall)

Goal: Allow SSH but block everything else.

1. Install & Check Status:

```
sudo apt update
sudo apt install ufw
sudo ufw status
```

2. Set Defaults (Security Best Practice): Deny all incoming traffic by default, allow all outgoing.

```
sudo ufw default deny incoming
sudo ufw default allow outgoing
```

3. Allow SSH (Prevent Lockout):

```
sudo ufw allow ssh
# OR specific port: sudo ufw allow 2222/tcp
```

4. Enable:

```
sudo ufw enable
(Press y to confirm).
```

Goal	Command
Open Port	sudo ufw allow 80
Open Port Range	sudo ufw allow 6000:6007/tcp
Allow Specific IP	sudo ufw allow from 10.0.0.5
Allow Subnet	sudo ufw allow from 10.0.0.0/24
Restrict Port to IP	sudo ufw allow from 10.0.0.5 to any port 22
Block IP	sudo ufw deny from 1.2.3.4

iptables (The Raw Tool)

Manually block ICMP (Ping) requests using raw iptables. Note: UFW actually configures iptables in the background. For this lab, we will add a direct rule.

1. View Current Rules:

```
sudo iptables -L -v
```

2. Block Pings (ICMP) from a specific IP (e.g., your Windows PC): Replace 192.168.1.5 with your Windows IP.

   ```
   sudo iptables -A INPUT -s 192.168.1.5 -p icmp -j DROP
   ```

   - -A INPUT: Append to Input chain.
   - -s: Source IP.
   - -p: Protocol.
   - -j DROP: Jump to "Drop" action (no reply sent).

3. Test: Try pinging Ubuntu from Windows. It should "Request Timed Out".
4. Delete the Rule: First, find the line number:

   ```
   sudo iptables -L --line-numbers
   ```

   Then delete (e.g., rule #1):

   ```
   sudo iptables -D INPUT 1
   ```

Lab 2: Set Up a Basic VPN Connection (WireGuard)

We will use WireGuard, a modern, faster, and simpler alternative to OpenVPN. We will set up the Ubuntu machine as a VPN Server and Windows as the Client.

Step 1: Install WireGuard on Ubuntu

```
sudo apt install wireguard -y
```

Step 2: Generate Keys

1. Generate Server Keys:

```
wg genkey | tee server_private.key | wg pubkey > server_public.key
```

2. View Keys:

```
cat server_private.key
cat server_public.key
```

(Copy these values to a notepad).

Step 3: Configure the Server Interface
Create the config file:

```
sudo nano /etc/wireguard/wg0.conf
```

Paste this content (Replace <SERVER_PRIVATE_KEY> with the key you generated):

```
[Interface]
PrivateKey = <SERVER_PRIVATE_KEY>
Address = 10.0.0.1/24
ListenPort = 51820
SaveConfig = true
```

Start the Server:

```
sudo wg-quick up wg0
sudo ufw allow 51820/udp
```

Step 4: Connect from Windows

1. Download and install the WireGuard Client for Windows.
2. Open it, click "Add Tunnel" > "Add empty tunnel".
3. Name it UbuntuVPN.
4. Paste this config:

```
[Interface]
PrivateKey = <Click 'Generate' in the windows client to get this>
Address = 10.0.0.2/24

[Peer]
PublicKey = <PASTE_UBUNTU_SERVER_PUBLIC_KEY_HERE>
Endpoint = <UBUNTU_IP_ADDRESS>:51820
AllowedIPs = 10.0.0.1/32
```

5. Click Save and Activate. You should now be able to ping 10.0.0.1 from Windows.

Lab 3: Capture and Analyze Traffic (Wireshark)

See your passwords flying in plain text.

Step 1: Install Wireshark on Ubuntu

```
sudo apt install wireshark -y
# When asked "Should non-superusers be able to capture packets?", select YES.
sudo usermod -aG wireshark $USER
```

(Log out and log back in for permissions to take effect).

Step 2: Start Capturing

1. Open Wireshark (wireshark in terminal).
2. Double-click your network interface (usually eth0 or ens33). You will see scrolling lines (packets).

Step 3: The "Plain Text" Test

1. Filter: In the top bar, type http and press Enter. (The screen will go blank as it waits for HTTP traffic).
2. Generate Traffic: Open a browser on Ubuntu (or use curl) and visit a non-secure site.
    - *Example:* http://checkip.dyndns.org or any testing HTTP site.
    - Better yet, use curl to simulate a login:

```
curl -X POST -d "user=admin&password=supersecret" http://httpbin.org/post
```

3. Analyze:
    - Look for the POST packet in Wireshark.
    - Right-click it > Follow > HTTP Stream.
    - You will see the raw text: user=admin&password=supersecret.
    - *This is why we enforce HTTPS (TLS).*

Lab 4: Detect and Block Suspicious IPs

Identify a "Ping Flood" attack and block the attacker.

Step 1: Simulate the Attack (From Windows)

1. On Windows Command Prompt, run a continuous ping:

```
ping -t <UBUNTU_IP>
```

Step 2: Detect it on Ubuntu

1. Open Wireshark on Ubuntu.
2. Filter by icmp.
3. You will see a rapid stream of "Echo (ping) request" packets.
4. Identify the Source: Look at the Source column. It will be your Windows IP (e.g., 192.168.1.5).

Step 3: Block the Attacker
Now that we have the IP from Wireshark, let's kill the connection.

a. Using UFW (The easy way)

```
sudo ufw deny from 192.168.1.5
```

b. Using iptables (The immediate way)

```
sudo iptables -I INPUT -s 192.168.1.5 -j DROP
```

Step 4: Verify
Look at your Windows Command Prompt. The pings should change from "Reply from..." to "Request timed out".
You have successfully detected an intruder (Wireshark) and neutralized the threat (Firewall).