A Project Report

ON

SCNF | Secure Campus Network Framework

BY

Student Name: SHIVAM SWARAJ **Roll No:** 23CA2591054

Program Name: BCA (CYBERSECURITY) **Semester:** 5th

Group Project: NO **Group Code:** SS

APEX UNIVERSITY, JAIPUR

(DEC. 2025)

Table of Content

Abstract

Universities today deal with serious cybersecurity threats. With everyone relying on computers and the internet, risks just keep growing. The Secure Campus Network Framework (SCNF) project tackles this challenge head-on. Its goal? Build a campus network that's not just secure, but also flexible and easy to manage.

Here's how the project works: it splits the network into logical segments using VLANs. This way, Admin, Faculty, Students, and Server rooms each get their own secure space. No more messy overlap. DHCP handles IP addresses automatically, which cuts down on mistakes and saves time. For communication between these groups, the team uses the Router-on-a-Stick method. This keeps things organized and lets departments talk to each other—but only when it's needed.

Security isn't an afterthought. Access Control Lists (ACLs) block unauthorized users from crossing into areas they don't belong. To really put the system to the test, the team runs an ethical hacking simulation. Using Kali Linux tools—Nmap, Nikto, Metasploit, and Wireshark—they dig into the network's weak spots and study possible attack routes. They don't just stop at finding problems; they map these issues back to the campus network and recommend targeted security fixes.

The big takeaway? Segmenting the network, automating tasks, and keeping a close eye on security policies matter a lot. The SCNF project gives universities a real-world blueprint for building safer, smarter networks.

Introduction

Campus networks keep everything running—classes, admin stuff, even day-to-day communication. They handle a ton of sensitive data: student records, staff info, all the critical resources. So, security isn't just important—it's non-negotiable. That's why we kicked off the Secure Campus Network Framework (SCNF) project. The main goal? Build a campus network that's not just secure, but also organized and ready to grow, using what we've learned in different tech courses.

We pulled in ideas from Ethical Hacking, Advanced CTP Cyber Security, Software Project Management (SPM), and IT Acts and Cyber Laws. With Ethical Hacking, we got inside the mind of an attacker—ran controlled hacks, found weak spots. On the cybersecurity side, we put things like VLAN segmentation, DHCP automation, inter-VLAN routing, and access control into action to lock down the network. Project management wasn't just a box to check. It helped us plan, execute, handle risks, test, and keep our documentation sharp. And the legal side? We dove into the IT Act so we'd know exactly what's legal, what's not, and how to stay compliant, especially around unauthorized access and protecting all that personal data.

In the end, the SCNF project isn't just a tech demo. It's proof that when you mix technical know-how, solid management, and a handle on the law, you can build a campus network that's actually ready for the real world.

Project

Secure Campus Network Framework (SCNF)

What is SCNF?

-> Secure Campus Network Framework
-> is a Simulated model built for an educational institution.
-> It focuses on protecting digital infrasture, student data, and communication channels from Cyber threats using ethical hacking, risk management, and cyber law.

Its includes:

-> Network design (on process)
-> Vulnerability Scanning & penetration testing
-> Data Protection policies (Under IT 2000/2008)
-> Risk analysis & incident response plan
-> Forensics simulation for Cyber incidents
-> Project management using Trello.

Why is it imp?

Because most educational institutions face:

-> Weak internal network security.
-> Unprotected student/staff data.
-> Lack of Cybersecurity polices.
-> No formal risk.

Objective:

To Design and implement a secure, efficient, and compliant network System for a college campus that integrates technical cybersecurity controls, risk management, and legal compliance in one complete framework.

Phase I

Network Design

Objective

To Design a secure & scalable campus network that connects all departments (Admins, Faculty, Students, library, lab, etc). with proper segmentation, routing and firewall protection.

1) Open Cisco Packet Tracer
2) drag & drop
   - ⊕ 3 PCs (Faculty, Admin, Students)
   - ✱) 1 Switch (Switch 2960)
   - ✱) 1 Router (Router 2811)

2960 Switch (Used to connect multiple devices in LAN.)

Router 2811 (Used to connect to internet or different network)

↓ Its Supports FastEthernet 0/0 & 0/1, Routing Protocol & basic IP configration)

It used for small/medium office. support 24 fast Ethernet, VLAN, & basic cont.

Port Type	Speed	Used	Meaning
FastEthernet (FE)	100Mbps	older Router/ Switch	Fast but older Standar.
Giga bit Ethernet	1000Mbps	modern device	Newer / Faster

Why we use this cable ?

		Use case
1) Copper straight-Through		- Connect different types of devices
2) Crossover Cable		- Connect similar devices
3) Console	(For configuration using terminal)	(used for CLI Access, not for network data)
4) Fiber	(for long-distance, High-speed links)	

#

PC → Switch → Router → Internet (or other network)

✱) Switch checks the MAC address and sends data to the right device in LAN.

✱) Router check the IP address and decides where to send data outside the LAN.

Problem / Error

Switch 2960 — fa0/24 — fa0/0 — Router 2811

Both are shut

let's Fix it

Why it Red?

1) Interface is shut down by default
2) No IP or device connected

Step1 click the Router

Step 2 Go the CLI

Step 3 N Enter

Step 4 enable Router

5 configure terminal Router#

6 interface fa 0/0 Router(config)#

7 no shutdown Router(config-if)#

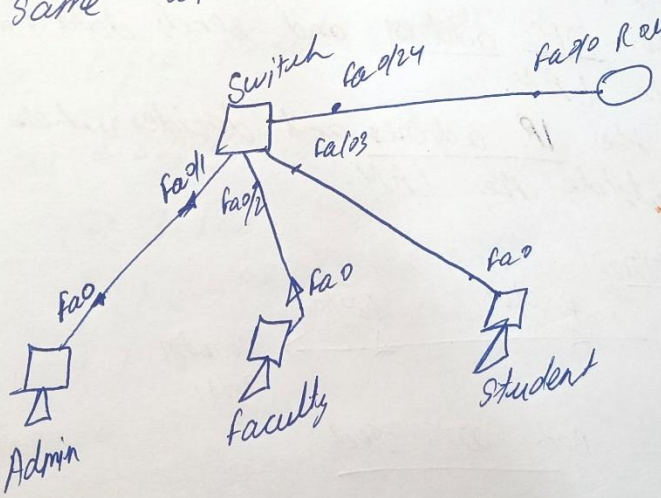
8 Exit "

9 Exit "

When you type No shutdown you should see:

%. Link-5-Changed: Interface FastEthernet 0/0, changed State to up

do the same with Switch.



Step 2 Assigning IP addresses & Basic Connectivity Test

Goal:
We will give IPs to all the devices so they can talk to EO.

Step 1
Let choose IP
192.168.10.0 /24

So we will have 192.168.10.1 to 192.168.10.254

Device	interface	IP	Default Gateway
Router	Fa 0/0	192.168.10.1	—
Admin	NIC	192.168.10.2	192.168.10.1
Faculty	NIC	192.168.10.3	"
Student	NIC	192.168.10.4	"

Step 2 configure to Router
1) Click on Router
2) CLI
3) N
4) enable
5) configure terminal
6) interface fa 0/0
7) IP address 192.168.10.1 255.255.255.0
8) No shut down
9) Exit
10) Exit

This assign the IP 192.168.10.1 to the Master' port.

Notes
1) First IP (192.168.10.0) can't assign to device
2) Last IP (192.168.10.255) for broadcast not assign to device
So we have 254 usable IPs.
2) Class A (127) is a loopback addrs is used to test itself inside the PC so it is also not useable.

Step2 configure Each PC's IP

1) Click on the PC
2) Go to Desktop
3) Click on IP configuration
4) IPv4 address (192.168.10.2
5) Click on Subnet
6) Default Gateway (192.168.10.1)

Now do same with all other.

#Step3 Test connection

1) Click on Admin PC
2) Go to Destop
3) Click on Command prompt
4) type ping 192.168.10.1
   we get reply of 4 pack

"Reply From 192.161.10.1 : bytes 32 time 1ms TTL=255
"
"
"

5) Ping 192.168.10.3

all the connection are working.

Step 3

Adding VLANs and segmenting the campus

Goal

- Segment the campus network logically into different department department or user group.
  - Admin
  - Faculty
  - Students.

-) Each group will be on its own VLAN, improving security, performance, and management.

VLAN

-) Virtual Local Area Network
-) It's creating separate networks inside the same switch.

Why to use

1) Security: Student cannot access Admin PCs directly
2) Organization: Make network management easier.

Plan VLAN

VLAN name	VLAN ID	Devices	Purpose
Admin	10	Admin PC	Administrative
Faculty	20	Faculty PC	Faculty network
Students	30	Student PC	Student network

Step 3.1 Create VLANs on the Switch

1) Click Switch → CLI
2) enable
3) configure Terminal
4) Vlan 10
5) name admin
6) exit
7) vlan 20
8) name Faculty
9) exit
10) vlan 30
11) name Students
12) exit

Now VLans are created

Step 3.2 Assign Ports to VLANs.

Port	VLAN
Fa 0/1	10 (admin)
Fa 0/2	20 (faculty)
Fa 0/3	30 (students)

Switch command

```
Switch (config)# interface fa 0/1
Switchport mode access
Switchport access vlan 10
exit.
```

Do the same for faculty and Students ports,

interface fa 0/24
Switchport mode ~~trunk~~ trunk
↑
For Router

Step 3.3 Router Configuration (Inter-VLAN Routing)

- PCs in different VLANs cannot talk unless the router "routes" between ~~if~~ VLANs.
- Create sub-interfaces on the router.

```
Router > enable
         configure terminal
         interface fa0/0.10
         encapsulation dot1Q 10
         ip address 192.168.10.1  255.255.255.0
         exit
```

" fa0/0.20

20

192.168.20.1

fa0/0.30

30

192.168.30.1

Each sub-interface represents one VLAN's gateway.

Step 3.4 → Assign IPs to PCs.

VLAN	PC IP	Subnet	Gateway
Admin	192.168.10.2	255.255.255.0	192.168.10.1
Faculty	192.168.20.2	"	192.168.20.1
Students	192.168.30.2	"	192.168.30.1

Now go to each PCs (Admin, faculty, Student) ~~for~~ and change the IP & Default Gateway with above mention.

Default Gateway = Router sub-interface IP for that VLAN.

Some imp command

① On Switch

enable
Show vlan brief

→ tells which VLAN exist & which ports are in which VLAN.

② Show interfaces status

→ Shows port status (connected/not connected) and VLAN assignment.

③ on the Router

enable
show IP interface brief

→ Shows all interfaces and their IPs and status (up/down).

④ on the Switch

Show interfaces fa 0/24 switchport

→ Show wheather that port is trunk / access and allowed VLANs.

Router & Switch Commands

1. enable — Both

Mode change:

Switch> → Switch#

* This command takes you from User EXEC mode (limited access) to Privileged EXEC mode, where you see and change configurations.

Why Use:

We can't configure or show full details in user mode.

2. Configure Terminal — Both

Mode change:

Switch# → Switch(config)#

* Opens global configuration mode, where you can make permanent configuration changes.

Why use:

This mode allows us to create VLANs, IP & enable interface, etc.

3. Interface fastEthernet 0/24 — B

* You're entering configuration mode for a specific port on the switch.

Why used

We did this to set Fa 0/24 (the port connecting to the router) as a trunk port.

4. Switchport mode trunk S

Meaning:

Changes the selected port's mode from "access" (for single VLAN) to "trunk" (for carrying multiple VLANs).

Why used:

Trunk ports carry traffic for all VLAN's b/w the switch and the router — needed for Inter-VLAN Routing (router-on-a-stick).

5. Switchport mode access

* Sets the port to work with only one VLAN (used for PCs or single devices).

Why used

We used this when connecting PCS - each port assigned to one VLAN (Admin, Faculty, Students.)

6. Switchport access vlan 10 (or 20, 30) S

* Assigns the current port to a specific VLAN

Why used:

So the PC connected to that port becomes a part of the VLAN (for segementation & security)

7) VLAN 10 S

* Create VLAN number 10 in the VLAN database

Why need:

We created VLANs for admin(10), faculty(20), student(30)

8) name Admin
used on: Switch after creating VLAN
* Gives a friendly name to the VLAN for easy identification

Why used:

So we can see "Admin" instead of just "10" in VLAN summary.

9) Show vlan brief

Display all VLAN's, their names, and which ports belong to them.

Why used:

To verify if VLANs were created and ports correctly assigned.

10) Show interfaces fastEthernet 0/24 switchport

Show the detailed configuration of a particular port - mode, VLANs allowed, trunk/native VLANs, etc.

Why Used:

To confirm that fa 0/24 (Router–Switch link) is properly set as a trunk.

11 no shutdown B

Turns the interface ON (by default, some are "administratively down").

12 inter fastEthernet 0/0

Enter configuration mode for the router's physical port (connected to the switch).

Why used: on Router

To assign IP address and enable communication with the switch.

13 ip address 192.168.10.1 255.255.255.0 B

Used on: Router interface

* Assigns an IP and subnet mask to that interface

Why used:

Every router interface needs an IP — it becomes the default gateway for that network.

14 interface fastEthernet 0/0.10

Used on: Router

⇒ Creates a subinterface on fa0/0 for VLAN 10 (Admin network)

Why used:

In Router-on-a-stick, each VLAN gets its own subinterface for routing.

15 encapsulation dot1Q 10 (R)

802.1Q is an IEEE networking standard
It is used to add small tag inside an Ethernet frame that tell which VLAN that packet belongs to.

Used on: Router (inside subinterface)

⇒ Meaning:

Defines that this subinterface will handle VLAN ID 10 using 802.1Q tagging.

Why used:

Tells the router which VLAN this subinterface belong to
Without this, it wouldn't know how to separate VLAN traffic.

16 ip address 192.168.10.1 255.255.255.0

Used on: Router subinterface

* Gives VLAN 10 its own IP gateway

Why used:

So all PCs in VLAN 10 (Admin) use 192.168.10.1 as their default gateway.

What is Interface?

An interface in networking means a "connection point through which a device (like a router, Switch, or PC) communicate with other device.

We can think of it like a door or port that allows data to go in or out of a device.

Subinterface

A subinterface is like a virtual (software-based) interface created inside a physical interface

Step 04

Add DHCP Server on Multiple Routers for Dynamic Routing

Objective:

To automatically assign IP address via (DHCP) & enable communication between VLANs or across different network segments.

 # Goal:

- Add more PCs in each VLAN
- Setup a DHCP server that gives them IPs automatically.
- Test communication b/w VLANs.

 # Steps for DHCP conf:

We had added following devices:

- 1 DHCP Server
- 2-3 new PCs for all VLANs

Connections:

- Connect DHCP server → Switch (FastEthernet port FA 0/23)
- Connect new PCs to switch ports:
  - VLAN 10: Admin
  - VLAN 20: Faculty
  - VLAN 30: Students

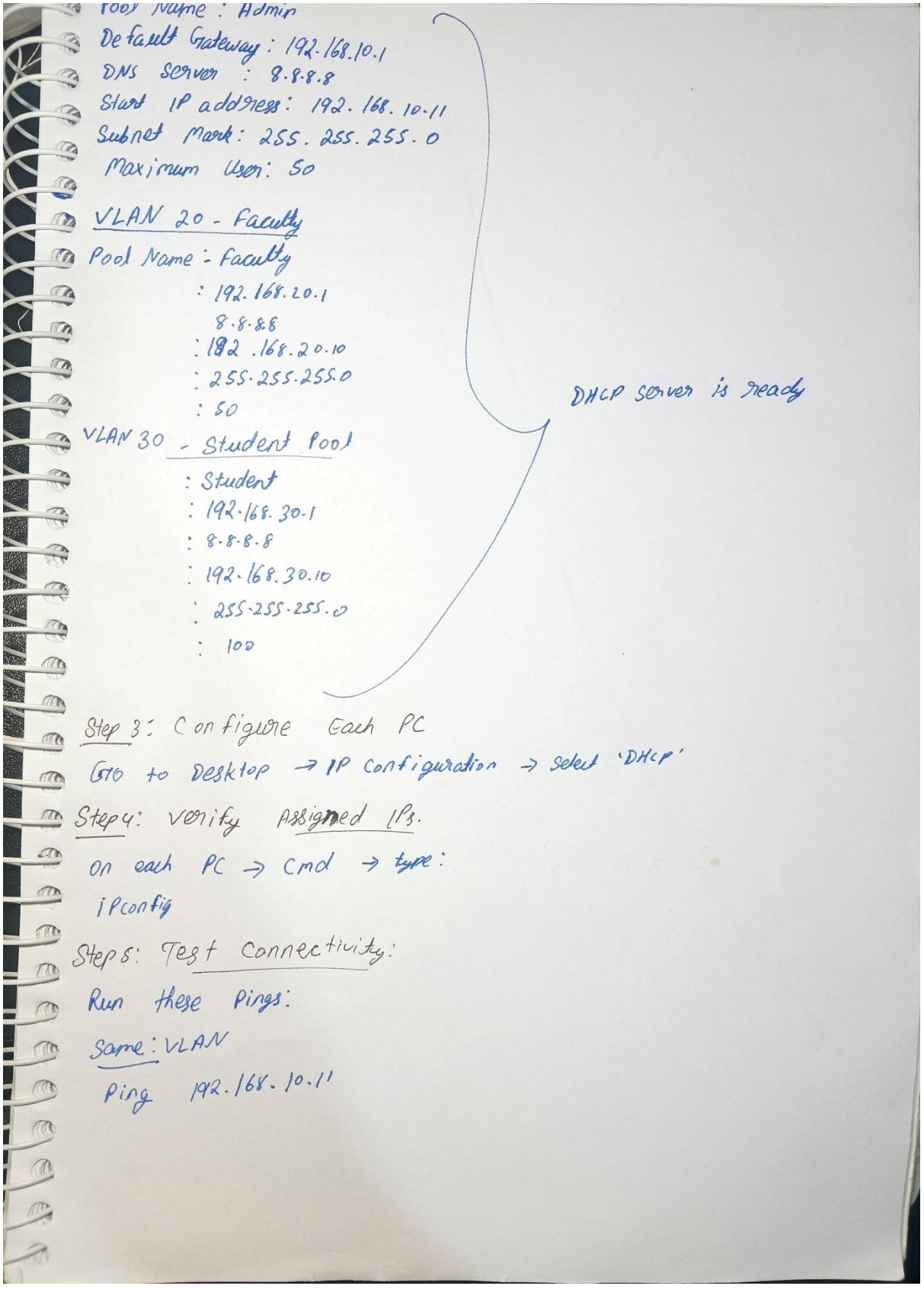
→ we will use Straight-through cables

Step 2: Configure DHCP Server

Click on the server → Go to services tab → DHCP

Turn DHCP service = on

VLAN 10 - Admin Pool



Pool Name : Admin
Default Gateway : 192.168.10.1
DNS Server : 8.8.8.8
Start IP address : 192.168.10.11
Subnet Mask : 255.255.255.0
Maximum User : 50

VLAN 20 - Faculty
Pool Name - Faculty
: 192.168.20.1
8.8.8.8
: 192.168.20.10
: 255.255.255.0
: 50

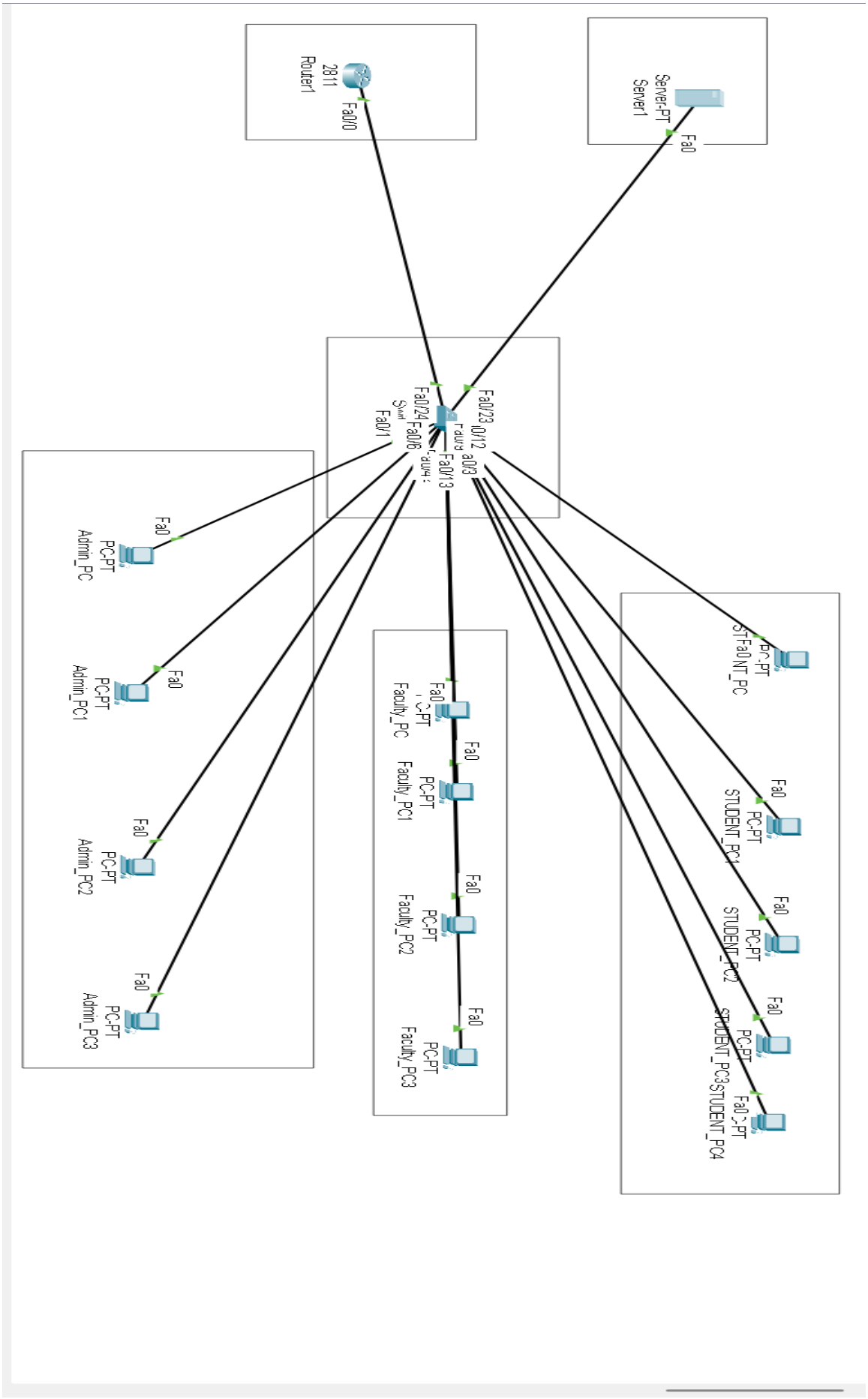
VLAN 30 - Student Pool
: Student
: 192.168.30.1
: 8.8.8.8
: 192.168.30.10
: 255.255.255.0
: 100

DHCP server is ready

Step 3: Configure Each PC
Go to Desktop → IP Configuration → Select 'DHCP'

Step 4: Verify Assigned IPs.
On each PC → Cmd → type:
IPconfig

Step 5: Test Connectivity:
Run these Pings:
Same VLAN
Ping 192.168.10.11


Router1
2811
Fa0/0
Server1
Server-PT
Fa0
Fa0/24
Fa0/1
Fa0/23
Fa0/13
Admin_PC
Admin_PC1
Admin_PC2
Admin_PC3
Faculty_PC
Faculty_PC1
Faculty_PC2
Faculty_PC3
STUDENT_PC
STUDENT_PC1
STUDENT_PC2
STUDENT_PC3
STUDENT_PC4
PC-PT

Ethical Hacking Simulation and Analysis

Introduction to Ethical Hacking

Ethical hacking is the process of identifying vulnerabilities in a system in a controlled and authorized manner. In this project, ethical hacking techniques were simulated to analyze possible security threats to the Secure Campus Network Framework (SCNF).

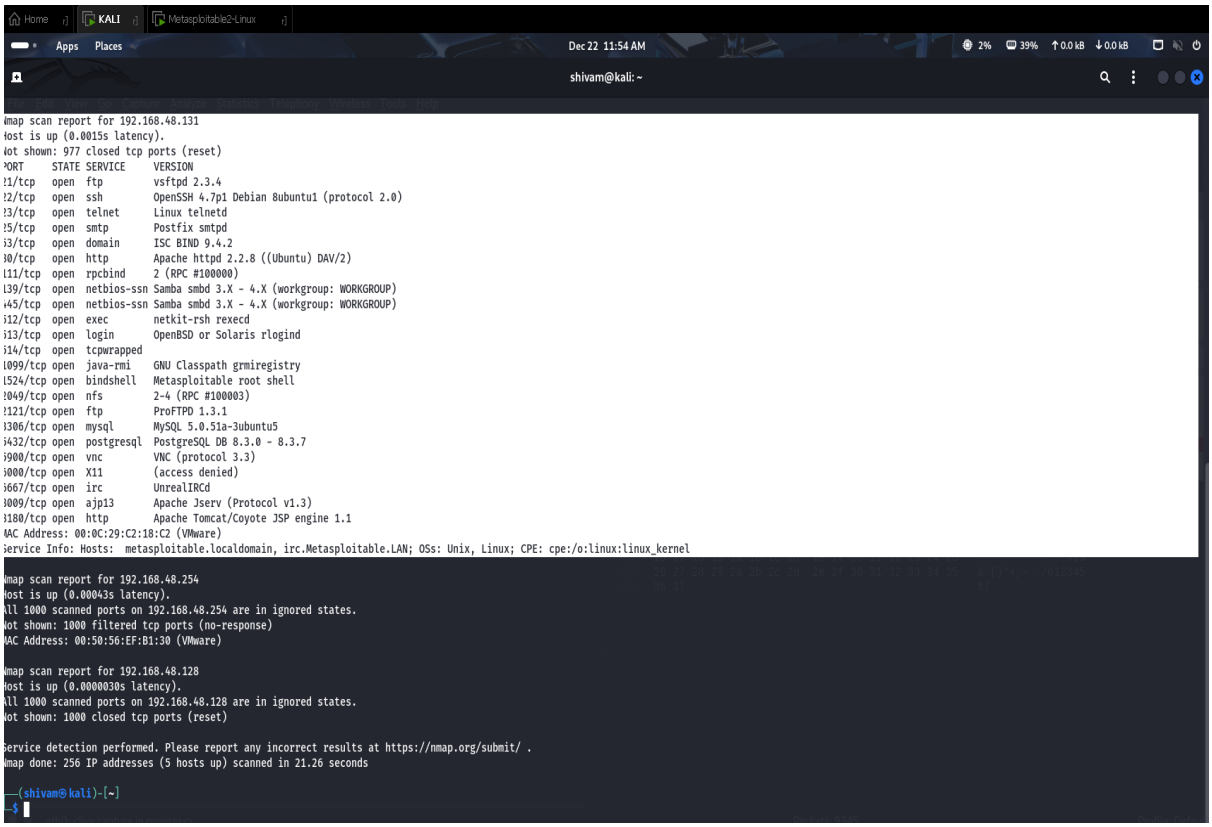
Attacker & Target Assumption

In this project, ethical hacking was performed in a controlled laboratory environment. Kali Linux was used as the attacker machine, and a vulnerable test server (Metasploitable2) was used as the target system. The results obtained from this simulation were logically mapped to the campus network designed in Cisco Packet Tracer.

Reconnaissance Phase (Nmap)

The reconnaissance phase was performed using the Nmap tool. Nmap was used to scan the target system to identify open ports and running services.

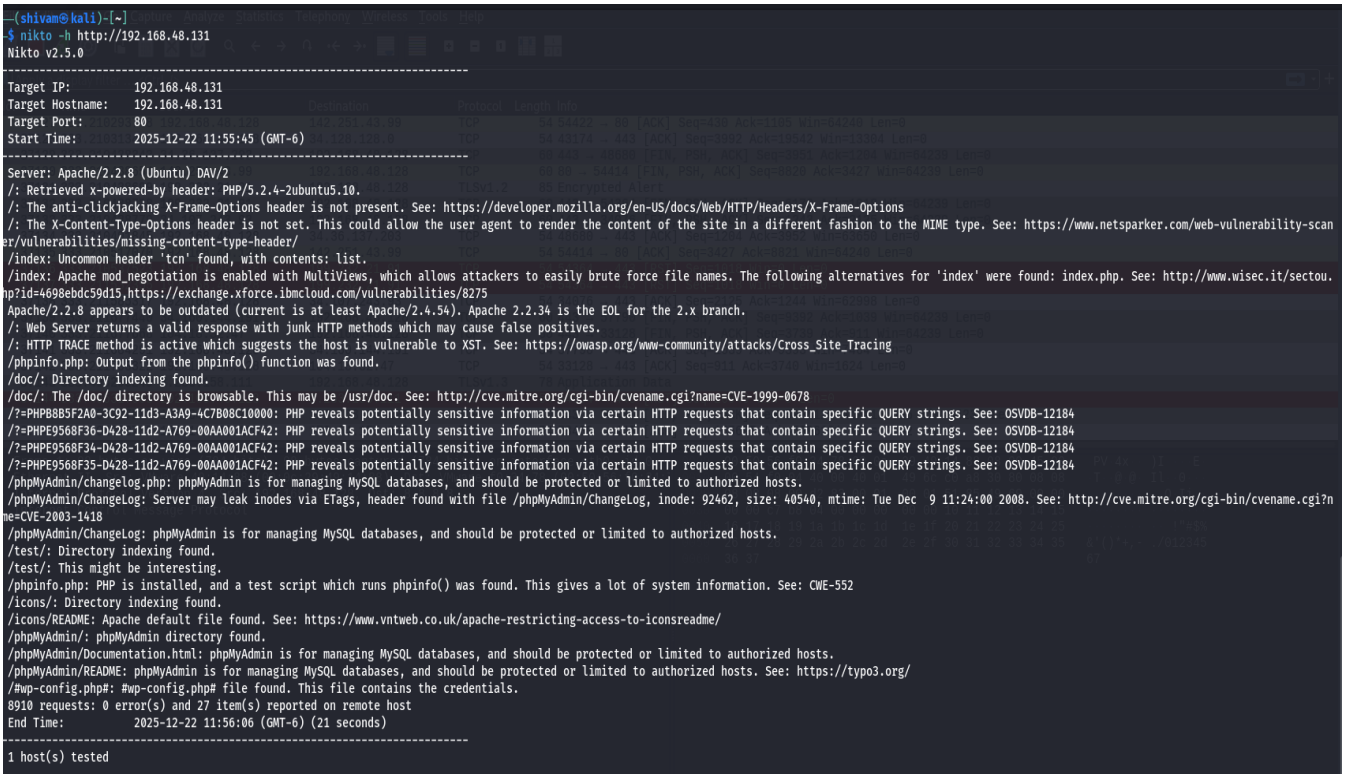
The scan revealed multiple open ports such as FTP, SSH, and HTTP, indicating potential attack surfaces.



This screenshot shows the result of an Nmap scan performed on the target system. Nmap detected multiple open ports and running services such as FTP, SSH, Telnet, HTTP, MySQL, and Samba. The presence of many open ports increases the attack surface of the system. This scan represents the reconnaissance phase of ethical hacking, where attackers gather information about the target.

Vulnerability Scanning (Nikto)

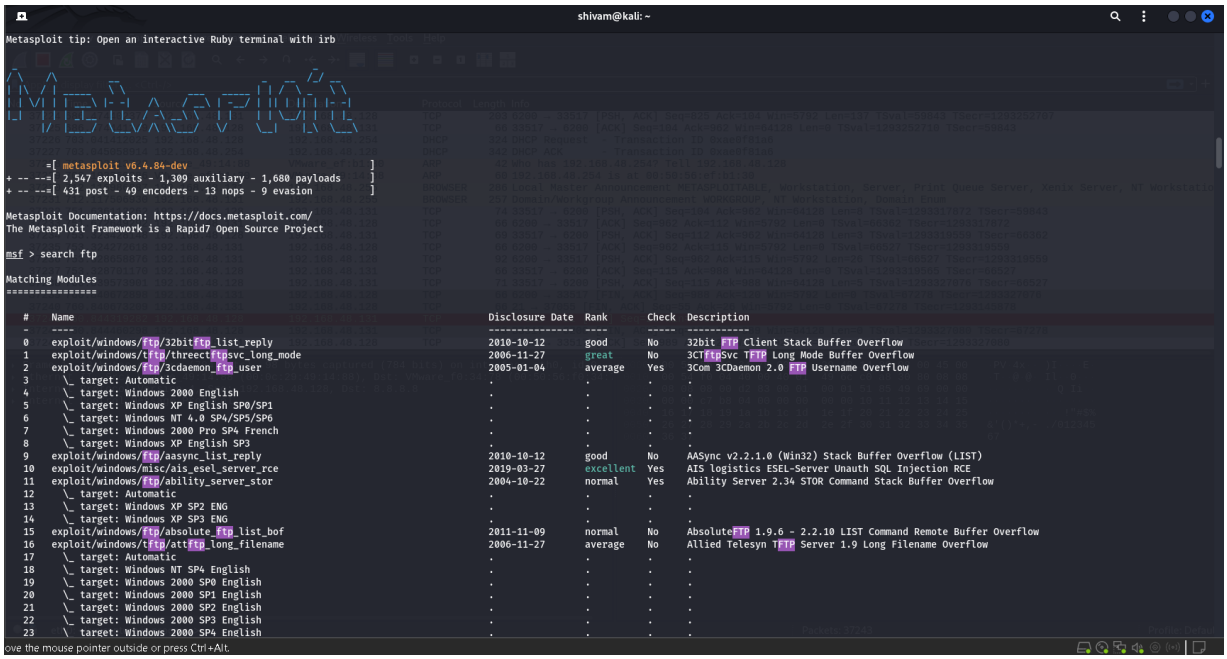
After reconnaissance, vulnerability scanning was conducted using the Nikto tool. Nikto helped in identifying web server misconfigurations, outdated software versions, and insecure settings that could be exploited by attackers.

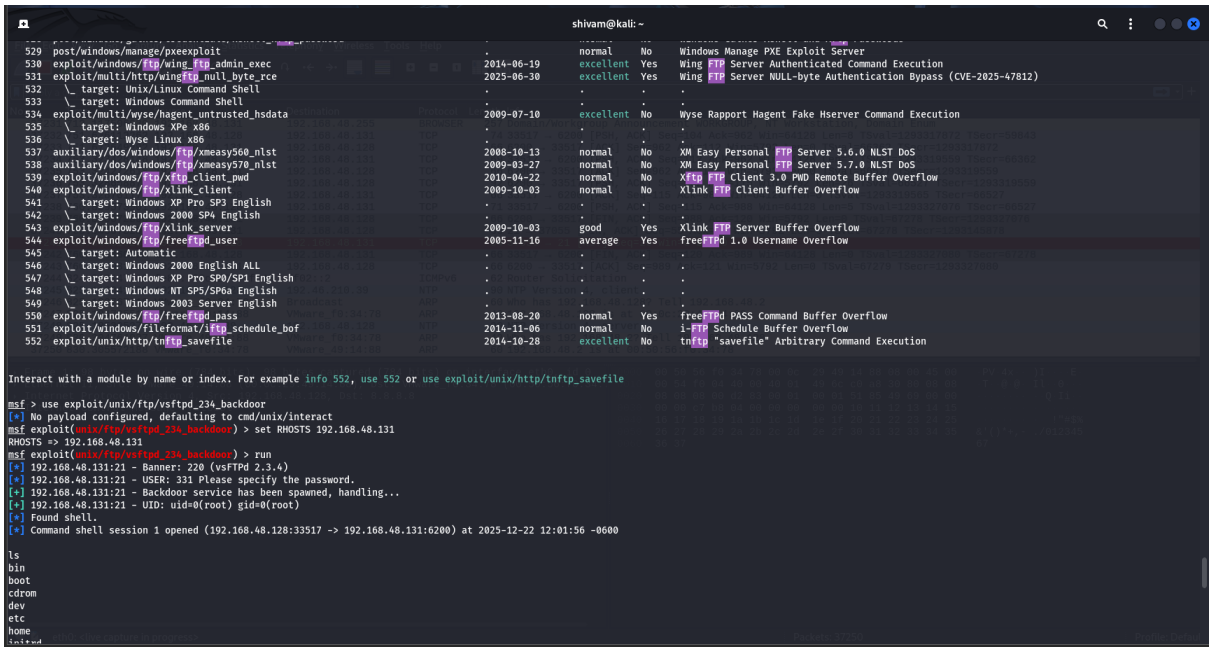


This screenshot shows the output of the Nikto web vulnerability scanner. Nikto identified several issues such as outdated Apache server version, directory indexing enabled, presence of sensitive files, and exposed PHP information. These findings indicate poor server hardening and misconfiguration, which can be exploited by attackers if not properly secured.

Exploitation Demonstration (Metasploit)

A controlled exploitation demonstration was performed using the Metasploit framework to understand how weak services can be exploited. This demonstration was conducted only for academic and learning purposes.



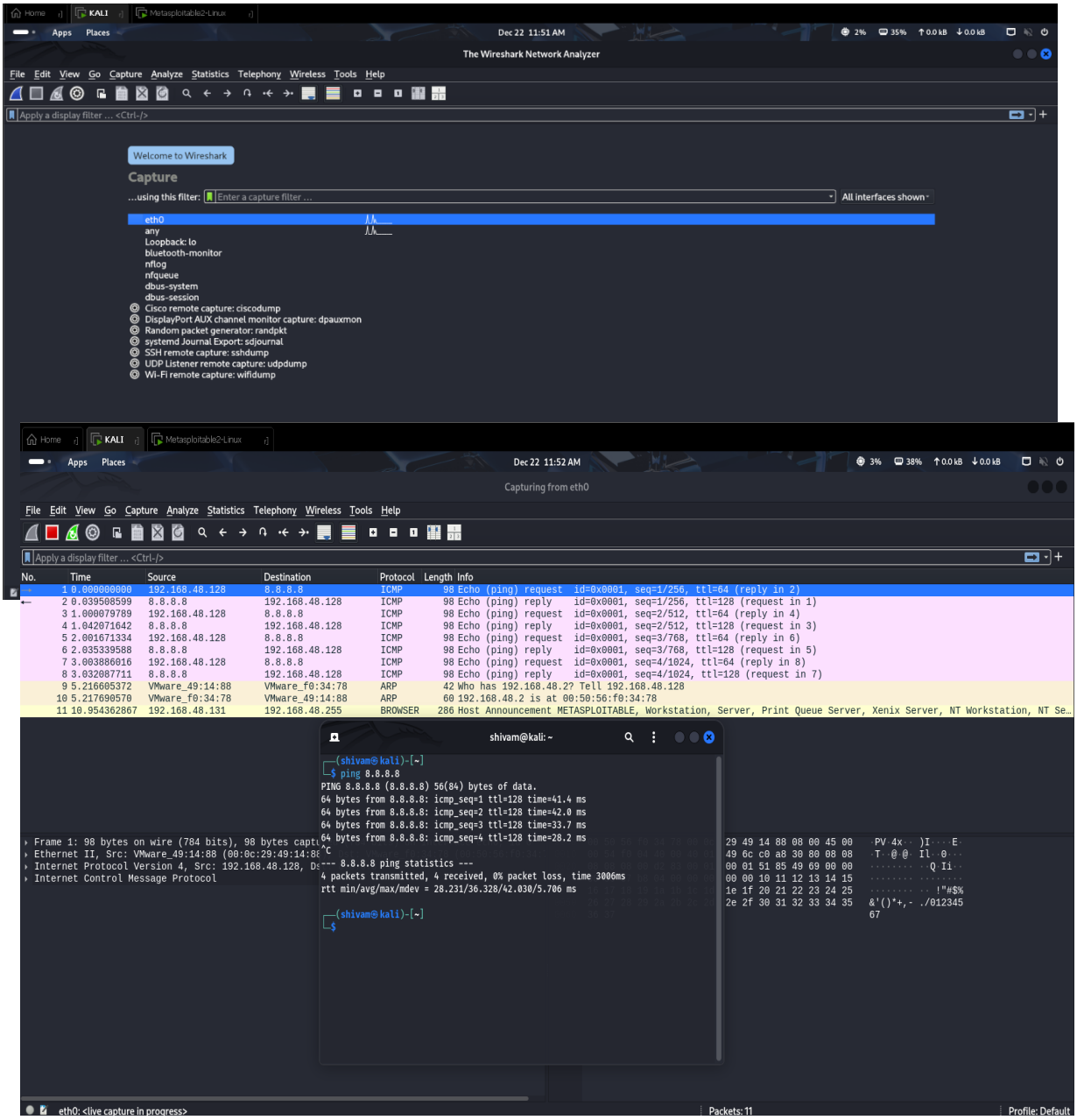


This screenshot shows the Metasploit Framework running on Kali Linux. The attacker searched for FTP-related exploit modules using Metasploit's

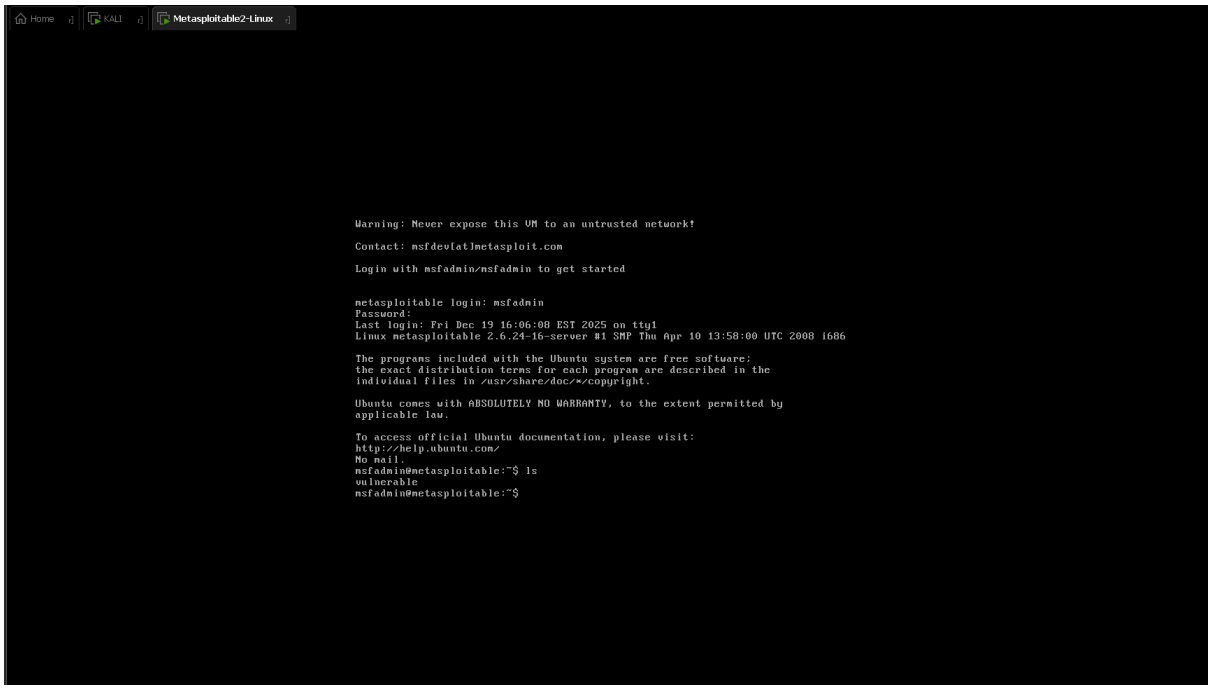
built-in search functionality. The output lists multiple exploit modules related to FTP vulnerabilities. This step represents the vulnerability identification phase, where an attacker searches for known exploits based on detected services.

Traffic Analysis (Wireshark)

Network traffic was captured and analyzed using Wireshark. This helped in understanding how unencrypted data packets can be intercepted during communication. The analysis highlights the importance of encryption and secure network design.



TARGET



This screenshot shows the Metasploitable2 Linux system, which is an intentionally vulnerable virtual machine used only for learning and ethical hacking practice. The warning message clearly states that this system should never be exposed to an untrusted network. The successful login using default credentials demonstrates weak authentication, which is a common security issue in poorly configured servers. This system is used as a target machine to safely demonstrate attacks in a controlled environment.

Application of Software Project Management (SPM) in SCNF Project

Introduction

Software Project Management (SPM) plays a crucial role in planning, executing, monitoring, and successfully completing any technical project. In the Secure Campus Network Framework (SCNF) project, SPM principles were applied to ensure proper planning, systematic execution, risk handling, and timely completion of the project.

Project Planning and Scope Definition

At the initial stage, the scope of the SCNF project was clearly defined. The project goal was to design a secure campus network using VLANs, DHCP, inter-VLAN routing, security controls, and ethical hacking simulation. Defining the scope helped avoid unnecessary features and ensured focus on syllabus-oriented objectives.

Key activities planned included:

- Campus network design
- VLAN implementation
- IP addressing and DHCP setup
- Security implementation
- Ethical hacking simulation
- Documentation and final submission

Work Breakdown Structure (WBS)

The project was divided into smaller and manageable tasks using the concept of Work Breakdown Structure (WBS). Each major activity was broken into sub-tasks such as network planning, configuration, testing, troubleshooting, and documentation. This made the project easier to manage and reduced complexity.

Scheduling and Time Management

A week-wise project roadmap was created to schedule tasks properly. The project followed a phased approach:

- Initial planning and design
- Network configuration
- Security implementation
- Ethical hacking simulation
- Documentation and review

This scheduling helped in tracking progress and completing tasks within the given academic timeline.

Use of Project Management Tools

Project management tools such as Trello were used to track tasks, monitor progress, and manage deliverables. Tasks were categorized into “To Do”, “In Progress”, and “Completed” stages. This improved visibility of project progress and helped maintain discipline throughout execution.

Risk Management

Risk management principles were applied during the project. Possible risks such as misconfiguration, IP conflicts, security loopholes, and time constraints were identified early. Preventive measures like proper testing, VLAN segmentation, ACL implementation, and backup documentation were taken to minimize project risks.

Quality Management and Testing

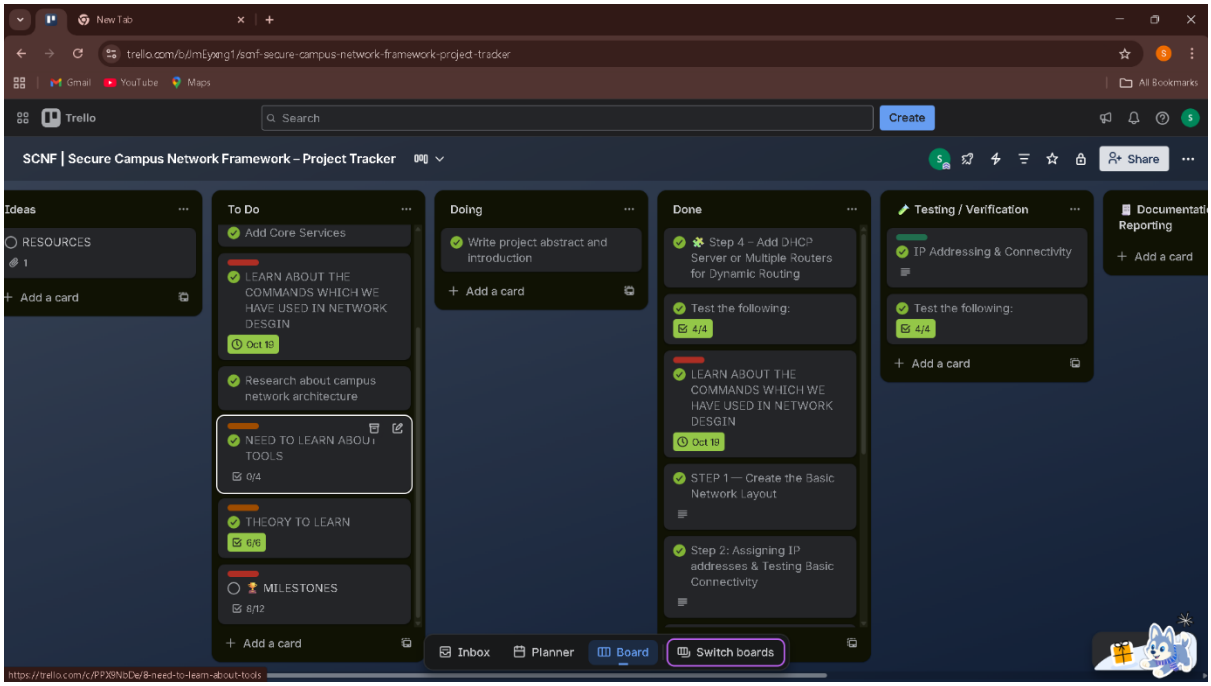
Quality assurance was ensured by continuously testing each module after implementation. Network connectivity, DHCP functionality, inter-VLAN communication, and security rules were tested using ping and traceroute commands. Ethical hacking tools were used to identify vulnerabilities and validate the effectiveness of security controls.

Monitoring and Control

Progress was monitored regularly by verifying configurations and testing outputs. Any issues encountered during implementation were resolved using a structured troubleshooting approach. This ensured the project remained aligned with objectives and met quality standards.

Documentation and Project Closure

Detailed documentation was prepared throughout the project lifecycle. Hand-written notes, screenshots, configuration outputs, and ethical hacking results were compiled into a structured project report. Final review ensured that all objectives were achieved before submission.



IT Act Sections Applicable to SCNF Project

Section 43 – Unauthorized Access and Damage

This section kicks in when someone gets into a computer system without permission or messes with it.

Simulated Violation:

Ethical hackers showed how easy it was to slip into services like FTP and HTTP on a server with weak security.

Protection Steps:

Split up departments using VLANs

Set up Access Control Lists (ACLs) to block unwanted traffic

Made sure only authorized people could get to the servers

Section 66 – Computer-Related Offenses (Hacking)

Section 66 covers hacking and any shady or dishonest stuff done with computers.

Simulated Violation:

Testers used Metasploit to exploit weak services in a safe, controlled setup.

Protection Steps:

Built a secure network from the ground up

Blocked ports that weren't needed

Stayed alert about risks from outdated software

Section 43A – Protection of Sensitive Personal Data

This part says organizations have to use reasonable security measures to guard sensitive personal data.

Risk Found:

Sensitive info was exposed because the server wasn't set up right.

Compliance Steps:

Kept the server network separated with VLANs

Used DHCP with strict IP allocation

Locked down access to admin resources

Section 72 – Breach of Confidentiality and Privacy

Section 72 deals with leaking confidential info without permission.

Risk Found:

Packet captures revealed how easy it is to grab unencrypted data.

Protection Steps:

Segmented the network

Pushed for encryption and secure protocols

Kept admin access under tight control

IT Act Rules and Responsibilities

The IT Act puts responsibility on network admins to keep systems secure. Organizations need to follow good security practices. If they slack off and something goes wrong, there are penalties.

On the SCNF project, the network admin role meant:

Setting up strong access controls

Monitoring the network

Regular risk checks and fixing weak spots

How the IT Act Protects the Campus Network

The IT Act:

Gives legal backup against cyber attacks

Sets penalties for unauthorized access and stealing data

Lays out rules for data protection and system security

Makes system owners and admins accountable

By sticking to these IT Act principles, the SCNF network stays secure and legally compliant.

Conclusion

The Secure Campus Network Framework (SCNF) project brought a secure, scalable campus network to life. We didn't just sketch out ideas — we actually built and tested a system that kept things organized and protected. VLAN segmentation, DHCP automation, and inter-VLAN routing did the heavy lifting, letting us split up departments logically while keeping communication smooth.

We locked things down further with Access Control Lists, making sure only the right people could move between network segments. Then came the real test: ethical hacking. We ran Nmap, Nikto, Metasploit, and Wireshark in a controlled setup, poking around for weak spots. Whatever we found, we mapped back to our campus network to get a clear picture of the risks and figure out how to fix them.

Throughout, we leaned on Software Project Management principles — planning, execution, risk management, testing, and documentation all got their due. We didn't stop with just the technical side, either. By weaving in compliance with the IT Act, 2000, we made sure the network stood up to both security threats and legal requirements. In the end, SCNF gave us real-world experience with secure network design and hands-on cybersecurity management — not just theory, but practice.

Future Enhancements

We can make the Secure Campus Network Framework even stronger by adding some advanced security and management features. Think about bringing in a dedicated firewall and an Intrusion Detection/Prevention System (IDS/IPS) — those tools catch threats early and help the team respond fast. For internet access, use Network Address Translation (NAT) and proxy services to keep things secure.

On top of that, it's worth setting up centralized authentication, encrypting sensitive data, and rolling out Security Information and Event Management (SIEM) tools for real-time monitoring. Expanding the VLAN architecture also helps when the campus grows. Together, these upgrades make the network tougher, more scalable, and ready for whatever comes next.

Resources, Platforms, and Tools Used

- ChatGPT (Project guidance, step-by-step help, problem solving)
- YouTube (Learning tools and concepts)
    - https://youtu.be/GH9qn_DBzCk
    - https://youtu.be/DD3LopYcOYI
    - https://youtu.be/xP0DIBkAPqQ
    - https://youtu.be/frUQMHXhnvs
    - Other related videos
- Trello (Project planning and management)
- Google Search (Concept clarification and reference)
- TryHackMe (Pre-learning of ethical hacking tools and concepts)
- Cisco Packet Tracer
- Kali Linux
- Metasploitable2
- Nmap
- Nikto
- Metasploit Framework
- Wireshark
- Microsoft Word
- Microsoft PowerPoint
- Information Technology Act Reference
    - https://www.indiacode.nic.in/