SECURING ATIBYAN NETWORK

A Practical Approach to Network Vulnerability Assessment and Mitigation

Instructor: **Mr Gbadamosi Oluwadamilola**

Academy: **Atibyan Tech Academy**

Date: **01/06/2025**

PRESENTED BY

Abdulahi

Abdulfattah

Jimoh Olabisi

Aminat

Omosanya

Olamilekan

Introduction

🔍 The Scenario

A vulnerable digital network — exposed, under silent threat.

🧠 The Challenge

Analyze. Identify. Secure.
3 analysts. 1 mission.

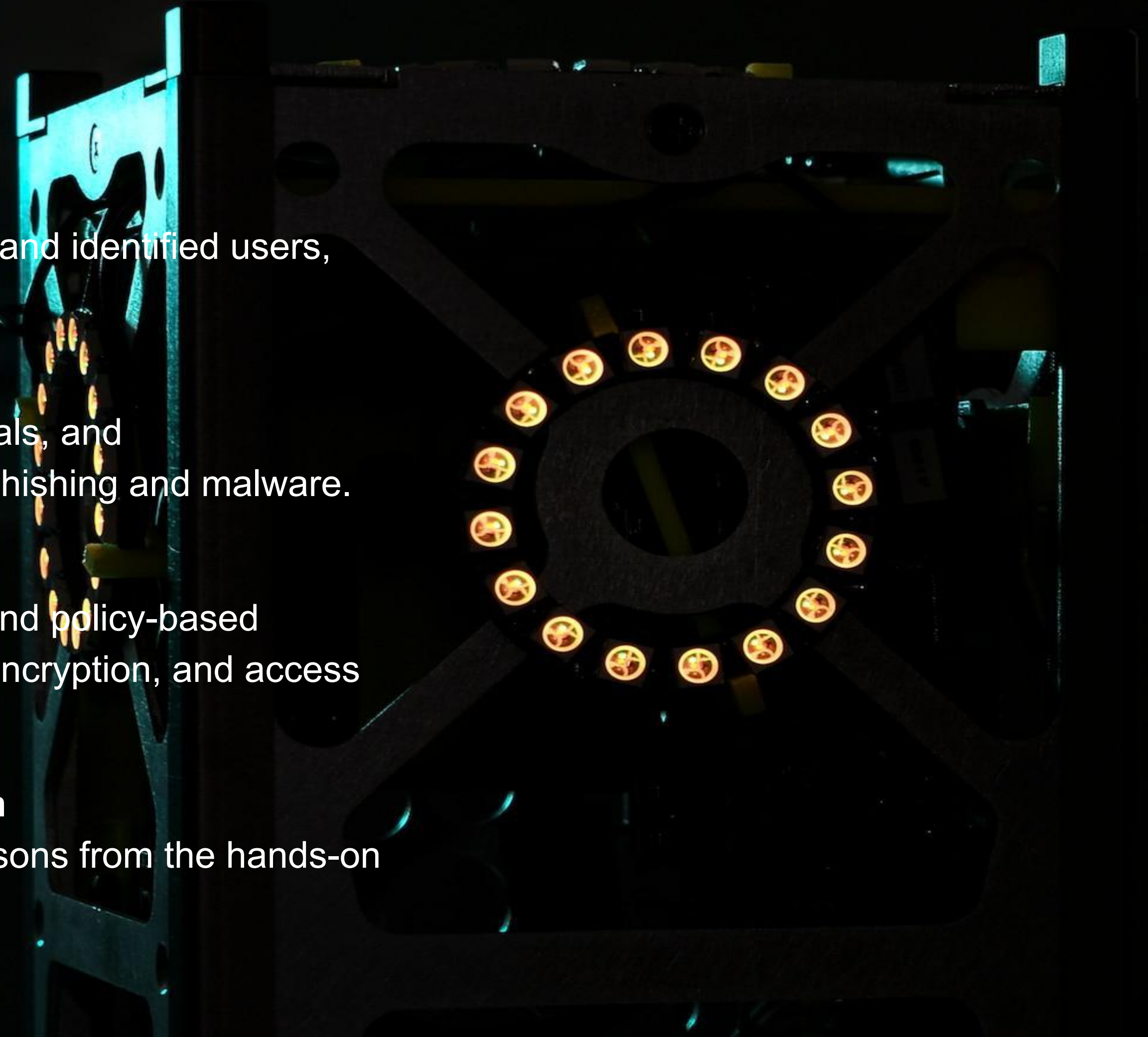
⚙️ The Objective

Harden the network by mitigating real-world cybersecurity flaws.

🕒 The Stakes

A test of skill and speed — protect the Academy’s digital backbone.

Project Overview



Phase 1: Network Analysis
Mapped the Atibyan Academy network and identified users, devices, and traffic patterns.

Phase 2: Vulnerability Assessment
Scanned for open ports, weak credentials, and misconfigurations; evaluated risks like phishing and malware.

Phase 3: Exploitation & Mitigation
Proposed and implemented technical and policy-based security measures, including firewalls, encryption, and access controls.

Phase 4: Documentation & Reflection
Compiled findings and outlined key lessons from the hands-on experience.

Environment Setup

Platform: Metasploitable 2—Atibyan Network

Tools Utilized:

- Kali Linux - Penetration testing and ethical hacking distribution
- Metasploit Framework—Penetration testing
- NVD (National Vulnerability Database)
- CVE (Common Vulnerabilities and Exposures) - Vulnerability Enumeration & Exploitation Research

Commands used and Purpose

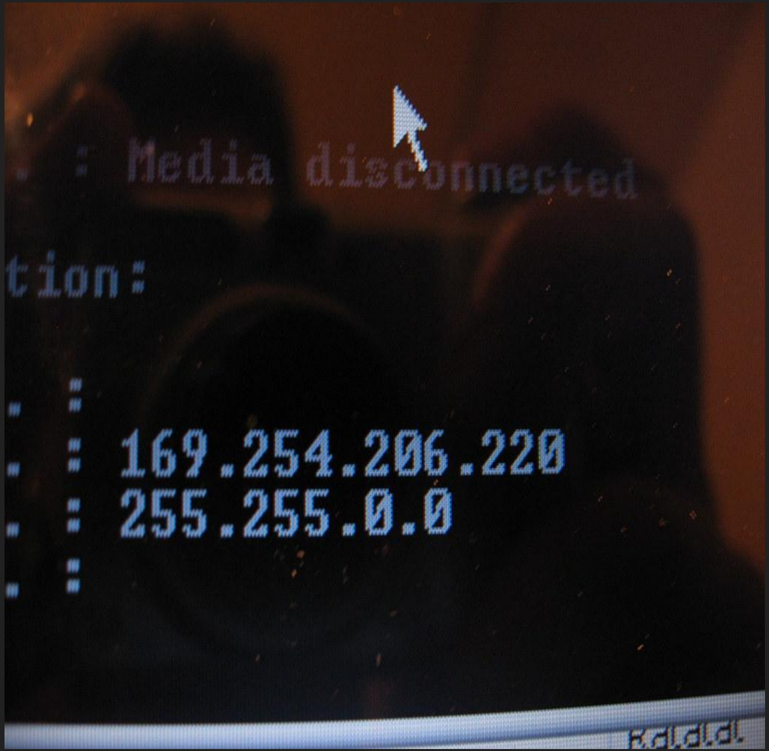
Category	Commands Used	Purpose
Reconnaissance & Enumeration	nmap,arp-scan -l, traceroute,netdiscover	Map targets and identify open services
Vulnerability Research	searchsploit,	Find known exploits or weak configurations
Exploitation	msfconsole,	Exploit vulnerabilities
Post-Exploitation	netuser,ifconfig,	Gather deeper access insights

Attack Simulation and Exploitation

What is an IP address?

An IP (Internet Protocol) address is a unique identifier assigned to each device on a network. It works like a digital address, allowing devices to find and communicate with each other across local networks and the internet.

- Example: 192.168.1.10
- Used by attackers to target specific machines
- Used in scanning, exploiting, and monitoring network activities

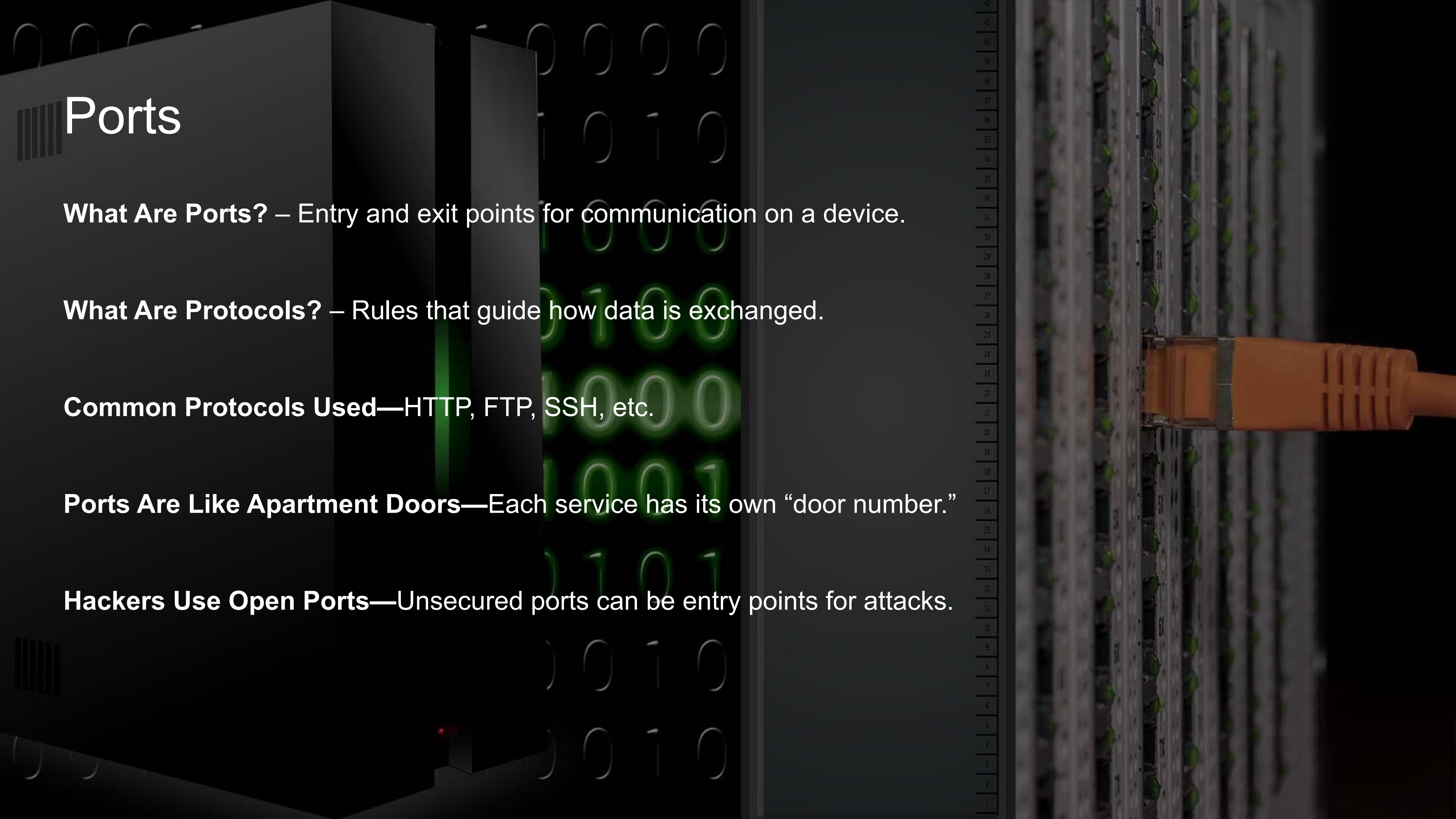


```
. : Media disconnected

tion:

. :
. : 169.254.206.220
. : 255.255.0.0
. :
```

Ports



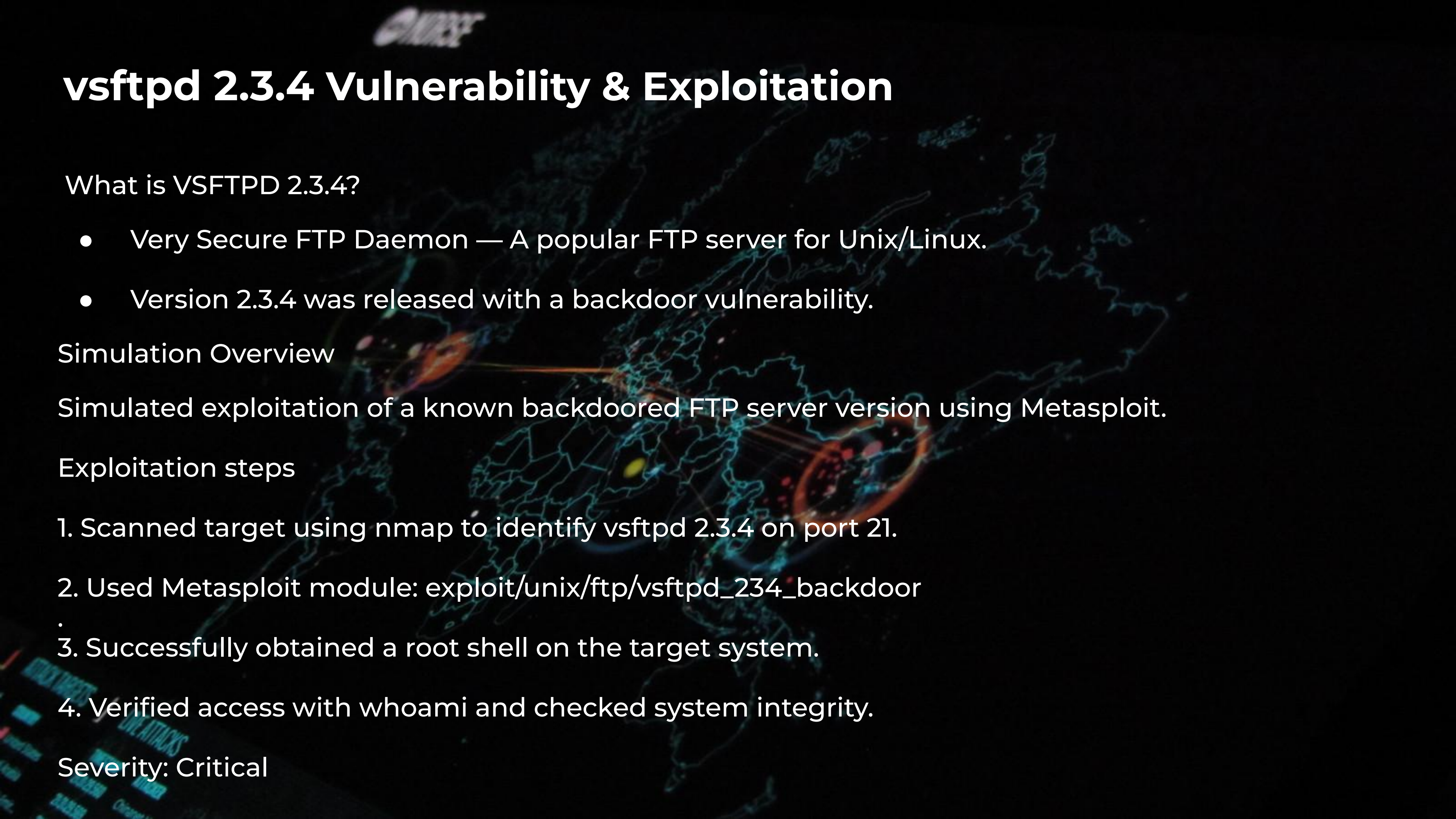
What Are Ports? – Entry and exit points for communication on a device.

What Are Protocols? – Rules that guide how data is exchanged.

Common Protocols Used—HTTP, FTP, SSH, etc.

Ports Are Like Apartment Doors—Each service has its own “door number.”

Hackers Use Open Ports—Unsecured ports can be entry points for attacks.



vsftpd 2.3.4 Vulnerability & Exploitation

What is VSFTPD 2.3.4?

- Very Secure FTP Daemon — A popular FTP server for Unix/Linux.
- Version 2.3.4 was released with a backdoor vulnerability.

Simulation Overview

Simulated exploitation of a known backdoored FTP server version using Metasploit.

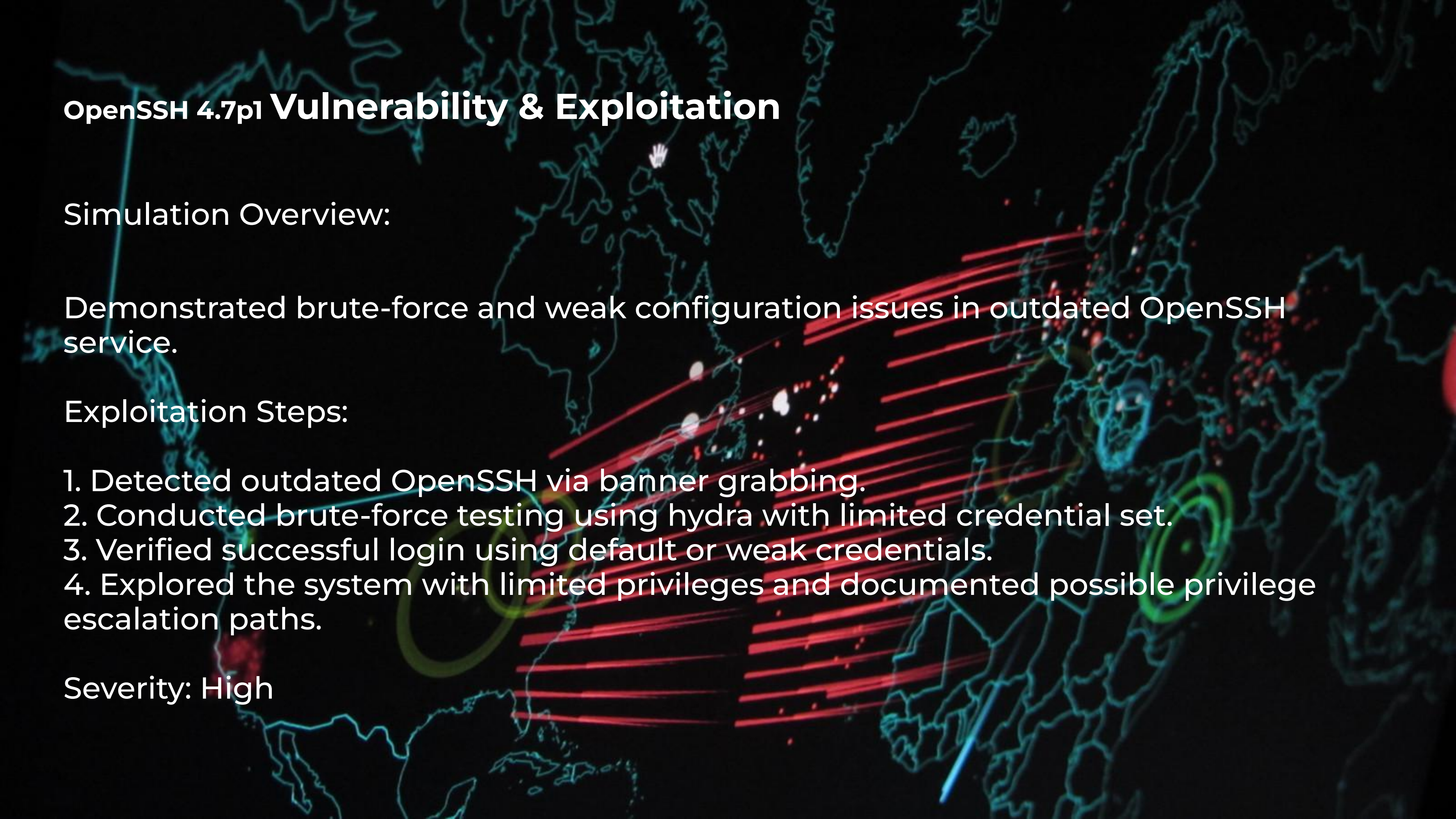
Exploitation steps

1. Scanned target using nmap to identify vsftpd 2.3.4 on port 21.

2. Used Metasploit module: exploit/unix/ftp/vsftpd_234_backdoor
.
3. Successfully obtained a root shell on the target system.

4. Verified access with whoami and checked system integrity.

Severity: Critical



OpenSSH 4.7p1 Vulnerability & Exploitation

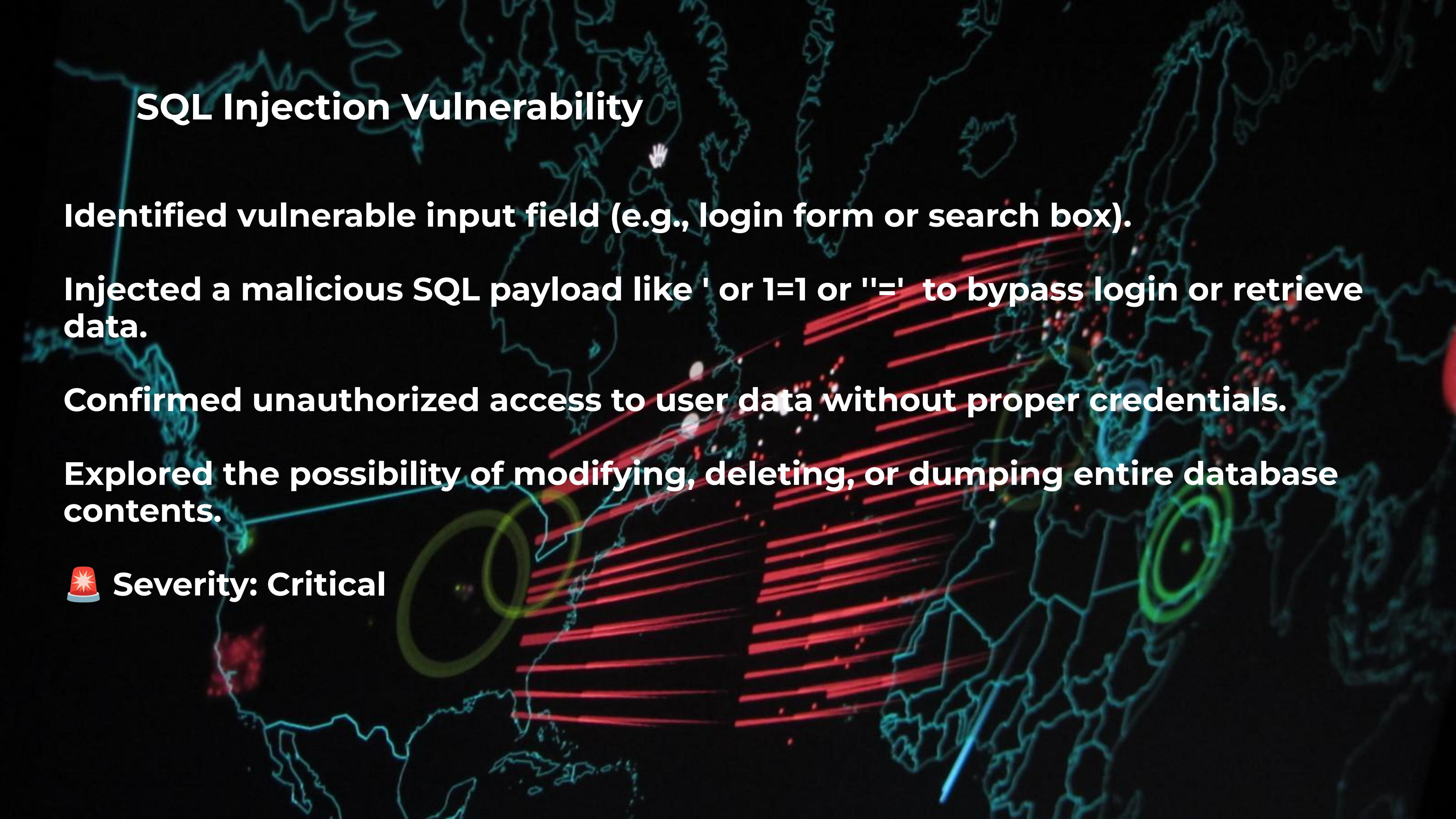
Simulation Overview:

Demonstrated brute-force and weak configuration issues in outdated OpenSSH service.

Exploitation Steps:

1. Detected outdated OpenSSH via banner grabbing.
2. Conducted brute-force testing using hydra with limited credential set.
3. Verified successful login using default or weak credentials.
4. Explored the system with limited privileges and documented possible privilege escalation paths.

Severity: High



SQL Injection Vulnerability

Identified vulnerable input field (e.g., login form or search box).

Injected a malicious SQL payload like ' or 1=1 or ''=' to bypass login or retrieve data.

Confirmed unauthorized access to user data without proper credentials.

Explored the possibility of modifying, deleting, or dumping entire database contents.

🚨 Severity: Critical

Linux telnetd

Simulation Overview:

Simulated credential interception and plaintext communication risk.

Exploitation steps:

1. Identified Telnet service on port 23 using `nmap`.
2. Connected using `telnet` client to simulate login.
3. Captured Telnet session using `tcpdump` or `Wireshark` to observe plaintext credentials.
4. Demonstrated how an attacker could steal login info and reuse it for unauthorized access.

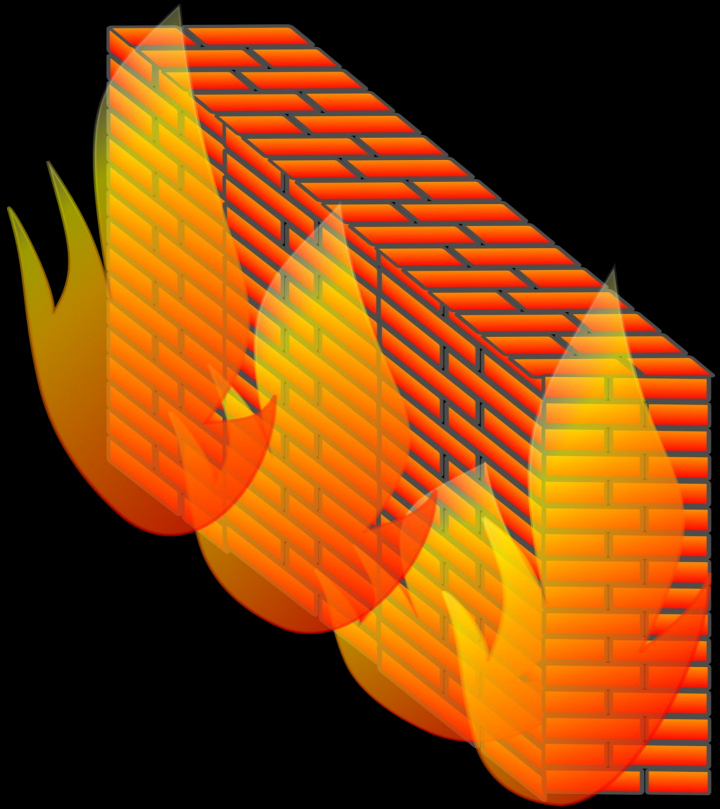
Severity: Medium

Firewall and Network Controls

Firewall & Network Controls

Configure `iptables` or `ufw` to:

- Block unused ports.
- Limit SSH (port 22) access to known IP addresses.
- Allow only specific IPs for web services.



Strong Authentication

Remove default usernames/passwords.

- Enforce password complexity policies.
    - Minimum 12 characters
    - Must include uppercase, lowercase, number, symbol
- Enable account lockout after 3 failed attempts.

Patch Management

Upgrade or remove vulnerable services like:

- vsFTPd 2.3.4
- Apache 2.2.8
- Unused services like Telnet or RSH

Web Server Hardening

Disable directory listing.

- Remove test and backup files.
- Restrict access to /admin and /phpmyadmin using .htaccess.

Intrusion Detection and Monitoring

Install tools like Fail2Ban or Snort to detect brute-force attempts.

Enable system logging and centralized log review (e.g., via syslog-ng).

User & System Hygiene

- Remove unused users and groups.
- Set file permissions properly (/etc/passwd, /var/www).
- Disable root SSH login.
-
  Use symmetric encryption for local, high-speed processing.
-
- Use asymmetric encryption for secure sharing.
- Always encrypt backups, and verify restoration integrity.
- Enforce least privilege access for sensitive files.
- Automate secure backups with tools like cron, rsync, and GPG

Conclusion

- The Atibyan Academy project provided a high-fidelity simulation of real-world network defense challenges.
- Practical engagement with vulnerabilities and mitigation reinforced technical proficiency.
- Future work: Build a layered defense model incorporating zero trust, SIEM analytics, and routine red-teaming exercises.

Notes:

- All simulations were conducted within a controlled lab environment.
- No real systems were harmed; this was purely for educational and assessment purposes.
- Ethical guidelines and institutional policy were followed at all times

THANK YOU