# Project : Cybersecurity Footprinting and Scanning Lab

By: Daksh (2023A7R003)

Cse-CyberSecuirty

# Objective

1

Perform footprinting & scanning of a target network

2

Identify open ports & services

3

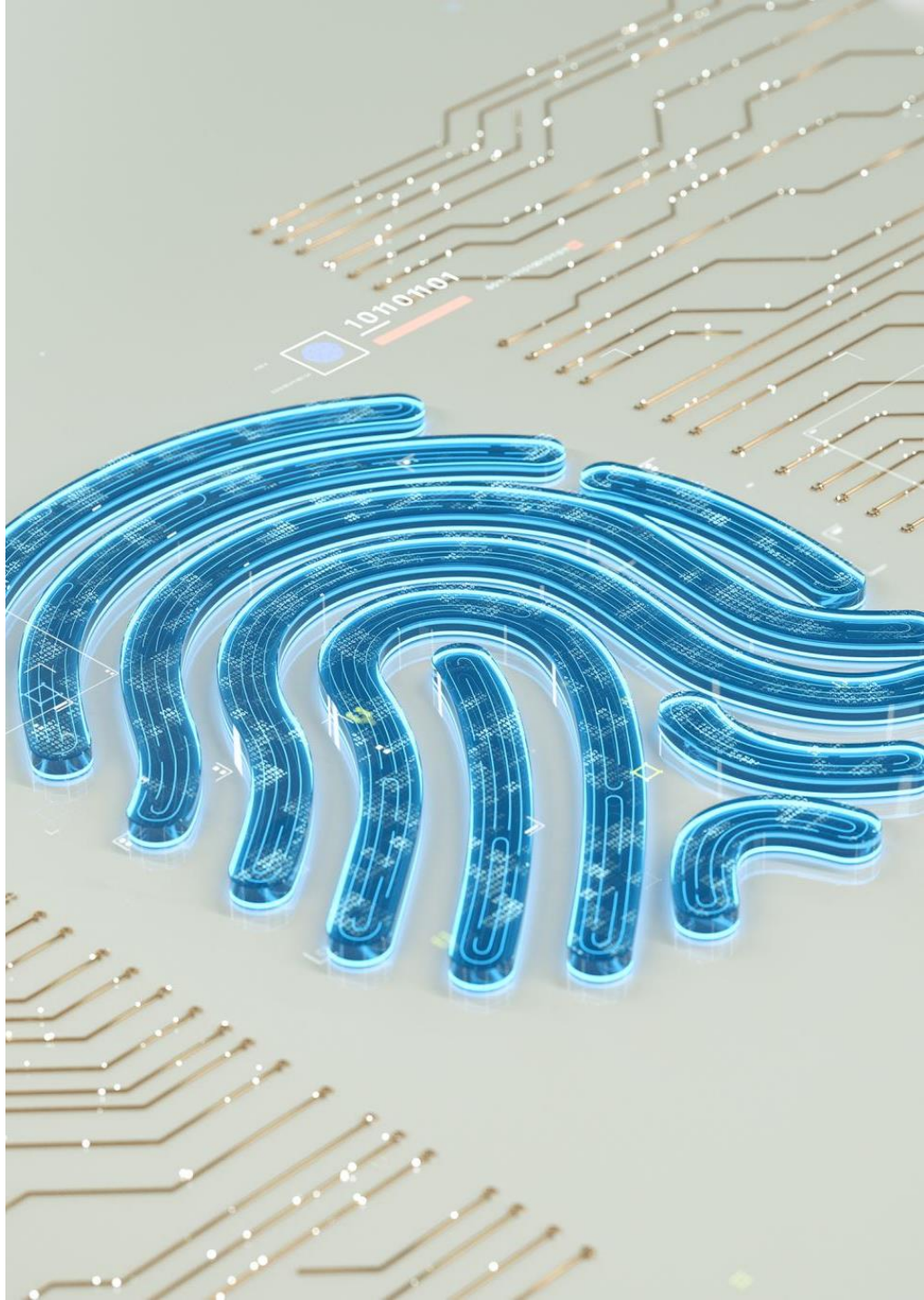
Assess risks and recommend countermeasures

# Tools Used

- **Nmap** → Port & service scanning, OS detection
- **Netdiscover** → Live host discovery in local network
- **Recon-ng** → OSINT framework for passive information gathering

# Footprinting & Scanning Activities

- Domain & IP lookup
- Host discovery (Netdiscover)
- Port scanning & service version detection (Nmap)
- OS fingerprinting
- Passive reconnaissance using Recon-ng

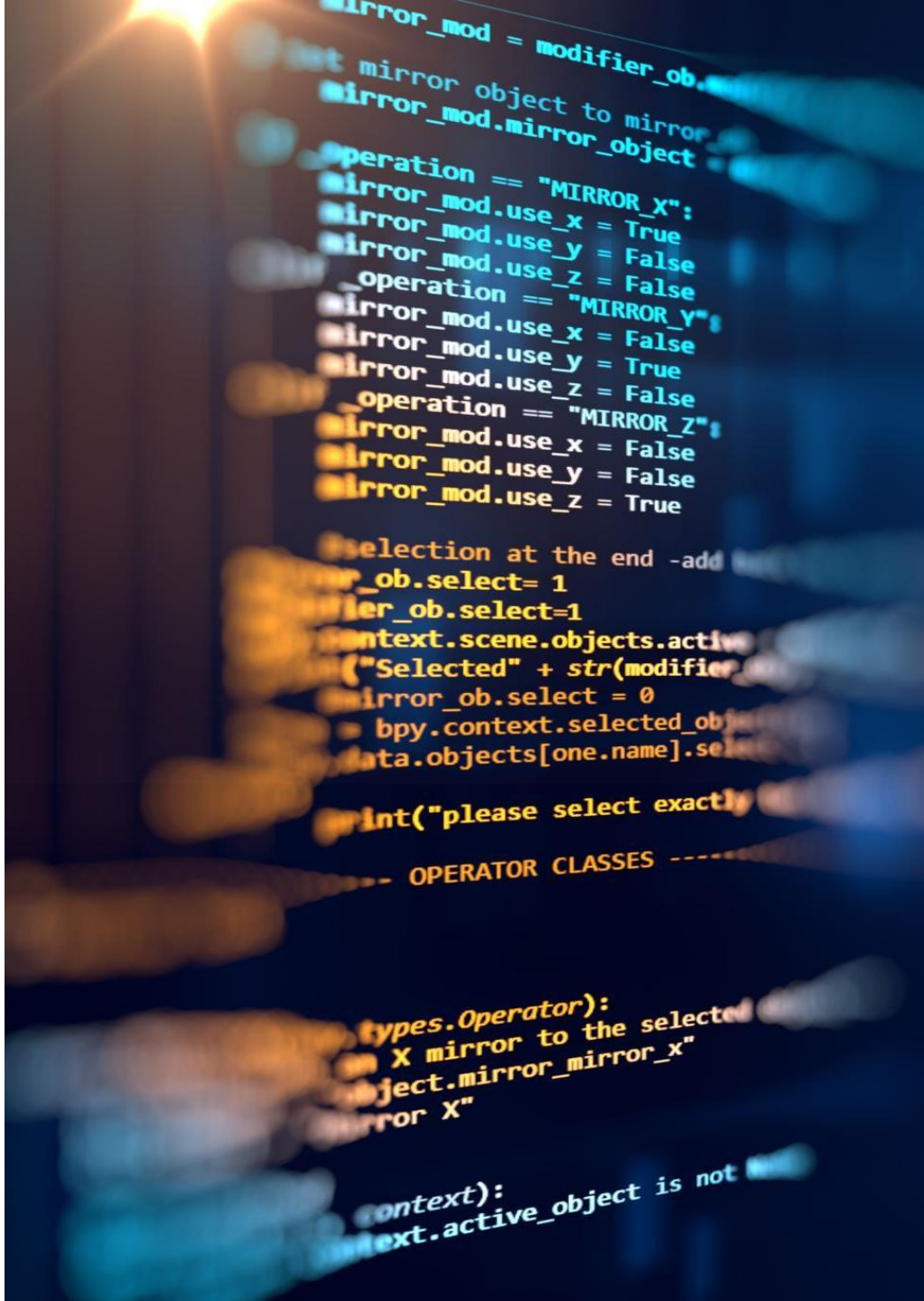


# Results

| HOST/IP | OPEN PORT | SERVICE/VERSION | RISK |
|---|---|---|---|
| 192.168.1.10 | 22 | SSH (OpenSSH 7.2) | Medium |
| 192.168.1.10 | 80 | HTTP (Apache 2.4.41) | High |
| 192.168.1.12 | 445 | SMB | High |

# Risks & Mitigation

- Risks:
  - Outdated software versions
  - Exposed services (HTTP, SMB, SSH)
  - Weak credentials possible
- Mitigation:
  - Patch & update services regularly
  - Close unnecessary ports
  - Enforce strong authentication
  - Use firewalls & IDS/IPS



# Conclusion

- Learned use of Nmap, Netdiscover, Recon-ng
- Identified open ports & possible vulnerabilities
- Proposed defense strategies to harden security posture