# Lab 1 — Advanced Exploitation Lab (Metasploitable2)

Author: Harshal Harekar

Date:14/10/2025

## Objective

This lab focuses on chaining exploits against a vulnerable machine.

## Environment

* Attacker: Kali Linux (host-only network)
* Target: Metasploitable2 VM (192.168.18.138)
* Tools: Metasploit, Python3, Nmap

## Steps

1. Setup & Reconnaissance

Run nmap scan on the target: *nmap -sV -p- 192.168.18.138*. Look for vulnerable services.

A computer screen shot of a computer

AI-generated content may be incorrect.

2. Chained Exploit Simulation (UnrealIRCd Backdoor -> Privilege Escalation)

Initial Access: Launch Metasploit (msfconsole).

A screen shot of a computer

AI-generated content may be incorrect.

Search for the UnrealIRCd exploit

A screen shot of a computer

AI-generated content may be incorrect.

Use the exploit, set payload, set RHOSTS, LHOST and LPORT



A screenshot of a computer screen

AI-generated content may be incorrect.

UnrealIRCd backdoor exploit dropped you straight in as root.

I will be still simulating the steps for privilege escalation.

A common technique on older Linux systems is to find SUID binaries that can be abused.

A screenshot of a computer program

AI-generated content may be incorrect.

See nmap in the list. Older versions of Nmap had an interactive mode that could be used to escape to a root shell.

In the shell, run: nmap --interactive and then at the nmap prompt, type !sh to get a root shell.

A screenshot of a computer

AI-generated content may be incorrect.

## Log

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Exploit ID | Description | Target IP | Status | Payload |
| 1 | UnrealIRCd Backdoor -> Privilege Escalation | 192.168.18.138 | Success | Shell |