COMPUTER SUBJECT:	NETWORK SECURITY
TYPE:	GROUP WORK
IDENTIFICATION:	Metasploit Investigation/MICL
COPYRIGHT:	*Michael Claudius*
LEVEL:	INTERMEDIATE
DURATION:	1-2 hours - 1 month – 1 year
SIZE:	200 lines!!
OBJECTIVE:	Various techniques for utilizing exploits
REQUIREMENTS:	
COMMANDS:	

IDENTIFICATION: Metasploit Investigation/MICL

Prolog

You have successfully finalized the IT-Security course. You will like to investigate more!.

The Mission

You are to investigate and discuss different exploits to break network security.

Purpose

The purpose is understand the Metasploit achitecure, to find, investigate and apply various tools in Metasploit.

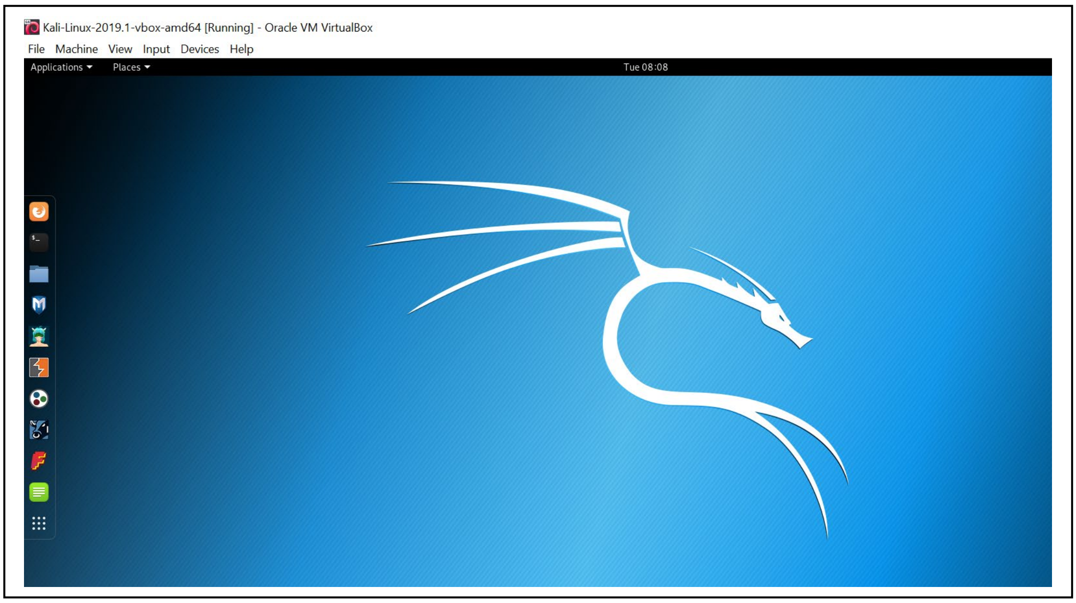
Useful links

http://tools.kali.org/

https://tools.kali.org/exploitation-tools/metasploit-framework

https://www.offensive-security.com/metasploit-unleashed/

Assignment1: Start Kali


Kali-Linux-2019.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications ▾
Places ▾
Tue 08:08

Remember Kali is using US-keyboards, which is a little annoying so here is a translation table for special signs:

Name	DK key	Name	US sign
question mark	?	under score	_
minus	-	slash	/
half	½	tilde	~
plus	+	minus	-

Assignment 2: Overview of exploits

First, you should try to get insight in Metasploit by visiting the useful links above and answer:

a. How is the architecture of Metasploit
b. Look at some important commands like msfconsole, etc
c. What is a payload?
d. What is singles, stagters, stages?
e. How are exploits utilized in Metasploit?

Assignment 3: Investigation of directories

Notice the terminal window, black square in the vertical icons-bar.
Start the *Terminal*
Use the following steps. (The text in red are the commands you will be typing)

```
service postgresql start
msfconsole
```

And see if you can get started.
Then exit msf:

```
exit
```

Modules
Metasploit modules are in : /usr/share/metasploit-framework/modules

Exploits
Exploits is a module that will take advantage of a system vulnerability
It will install a payload on the system, a payload will be a reverse shell or a metapreter, which will give you access to the computer.
The payload is what the exploit will plant on the victim

Let us surf a little around using the *cd* and *ls* commands
Type the following in sequence:

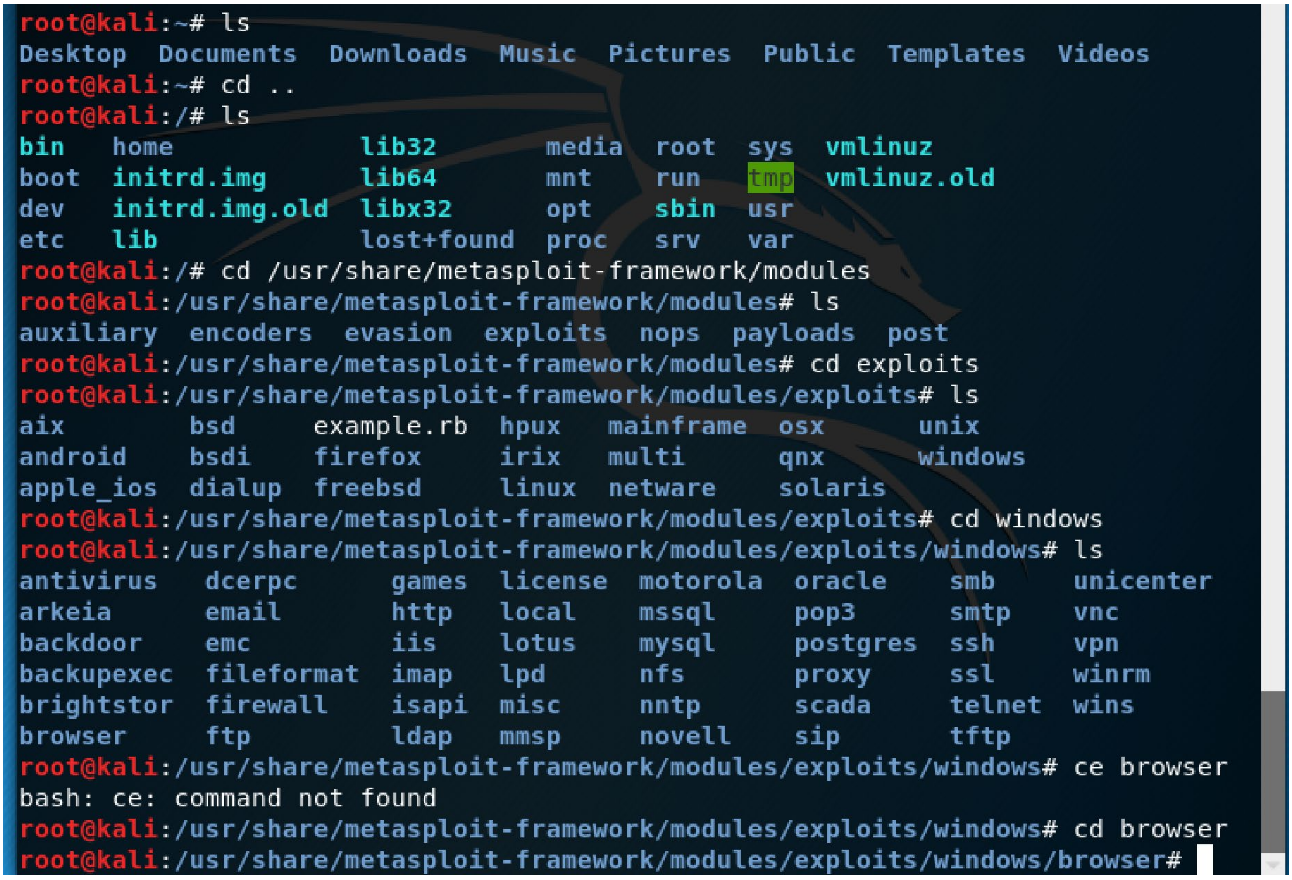
```
cd ..
ls
```

Notice the root and usr directories.
You are normally started in root-directory when Kali runs.

Now utilize *ls* or *cd* commands to explore further

```
cd /usr/share/metasploit-framework/modules
ls
cd exploits
ls
cd windows
ls
cd browser
```

and you should see something like this



```
root@kali:~# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
root@kali:~# cd ..
root@kali:/# ls
bin   home            lib32       media  root  sys  vmlinuz
boot  initrd.img      lib64       mnt    run   tmp  vmlinuz.old
dev   initrd.img.old  libx32      opt    sbin  usr
etc   lib             lost+found  proc   srv   var
root@kali:/# cd /usr/share/metasploit-framework/modules
root@kali:/usr/share/metasploit-framework/modules# ls
auxiliary  encoders  evasion  exploits  nops  payloads  post
root@kali:/usr/share/metasploit-framework/modules# cd exploits
root@kali:/usr/share/metasploit-framework/modules/exploits# ls
aix        bsd     example.rb  hpux   mainframe  osx      unix
android    bsdi    firefox     irix   multi      qnx      windows
apple_ios  dialup  freebsd     linux  netware    solaris
root@kali:/usr/share/metasploit-framework/modules/exploits# cd windows
root@kali:/usr/share/metasploit-framework/modules/exploits/windows# ls
antivirus   dcerpc      games  license  motorola  oracle    smb     unicenter
arkeia      email       http   local    mssql     pop3      smtp    vnc
backdoor    emc         iis    lotus    mysql     postgres  ssh     vpn
backupexec  fileformat  imap   lpd      nfs       proxy     ssl     winrm
brightstor  firewall    isapi  misc     nntp      scada     telnet  wins
browser     ftp         ldap   mmsp     novell    sip       tftp
root@kali:/usr/share/metasploit-framework/modules/exploits/windows# ce browser
bash: ce: command not found
root@kali:/usr/share/metasploit-framework/modules/exploits/windows# cd browser
root@kali:/usr/share/metasploit-framework/modules/exploits/windows/browser# 
```

Finally

```
ls
```

gives a lot of exploits just for the browser. Notice the adobe….exploits.
Then step back to root-directory

```
cd ~/
```

Assignment 3: Investigation of commands

help
Use help command to find more about a command or two.

msfsearch
Use msfsearch to search for the right command to use.

use
The use command: will allow you to load a module
e.g: **use** exploit/windows/browser/adobe_flash_avm2

show
After using **use** command we can apply other commands on the exploit
e.g the **show** command which will show information about this exploit

show options: will show options you can use with this exploit
show info: will give you full information about the exploit
show targets: will list the target machines if any and then we know who to attack
show payloads: list possible payloadsA target is set by the RHOSTS command.

Which you will soon use in the following sections.

But first let us use the **use** and **show** commands

```
msf5> use exploit/windows/browser/adobe_flash_avm2
msf5 exploit(windows/browser/adobe_flash_avm2) >
msf5 exploit(windows/browser/adobe_flash_avm2) > show
msf5 exploit(windows/browser/adobe_flash_avm2) > show options
msf exploit(windows/browser/adobe_flash_avm2) > show payloads
msf exploit(windows/browser/adobe_flash_avm2) > show targets
msf exploit(windows/browser/adobe_flash_avm2) > show info
```

The full information is pretty good !

If you are tired, try exit to exit the msfconsole.

```
exit
```

You canm always start again start again by using msfconsole:

```
msfconsole
```

The following search command will give you a long list of exploits

```
msf > search type:exploit platform:windows flash
```

Now you can either type the exploit name after the **use** command or you can simply highlight the exploit name from the list you got in the terminal and copy the exploit and paste it after the **use** keyword. This will be done in the next exercise.

Assignment 4: Explore the Metasploit modules

Metasploit has 6 different types of modules:

Exploits, auxiliary, post, payloads, encoders and nops

Research and explain some more Metasploit Modules
Also, explore some other exploits in Metasploit.

Form a group af 2-4 members. Choose 2-3 modules and 2-3 exploits.
Investigate 40 minutes, prepare a 5-10 minutes' presentation nicely and then be ready to present the outcome for rest of the class.

It can still take hour to become a beginner, weeks to become experienced and months/years to become an expert ☺ But anyway

Congratulation, you are now at beginners level and ready to install Metasploitable and initiate attacks.