

In this hands-on project, you will use the Metasploitable-2 Lab Environment that you have previously installed. Reconnaissance:

1. (total 10 pts) Assume that you do not know the IP address of the Metasploitable-2 machine. Hint: you can find this tool in the 01 – Information Gathering section (see Figure 1).

a. Which tool in the Kali Linux that you can use for finding the IP address of the Metasploitable server? (3 pts).

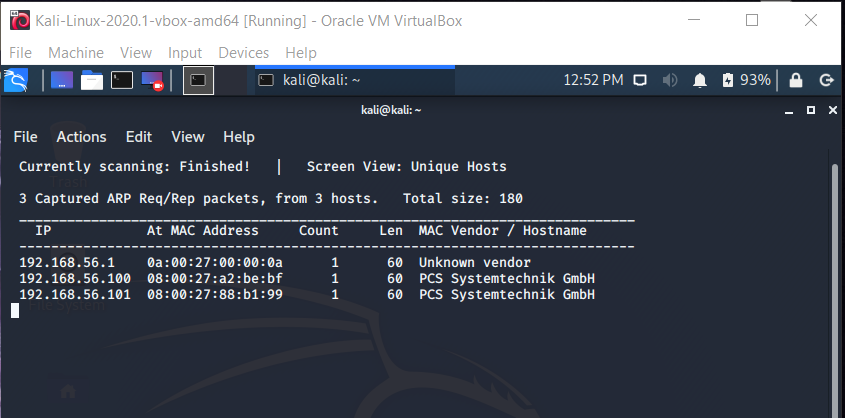
The tool in Kali Linux you would use to find the IP address of a Metasploitable server is Netdiscover.

b. Describe your chosen tool briefly (5 pts).

Netdiscover is an ARP scanner that can be used to scan for live hosts in a network. It can also scan for multiple subnets.

c. Include the screenshot that display the results when you are running this tool for finding the Metasploitable-2 server IP address (2 pts).

The Metasploitable IP address is 192.168.56.101.



2. (total 30 pts) When you have found the IP address of the target server (i.e., Metasploitable-2 server), use the nmap command to find the details information of the target server.

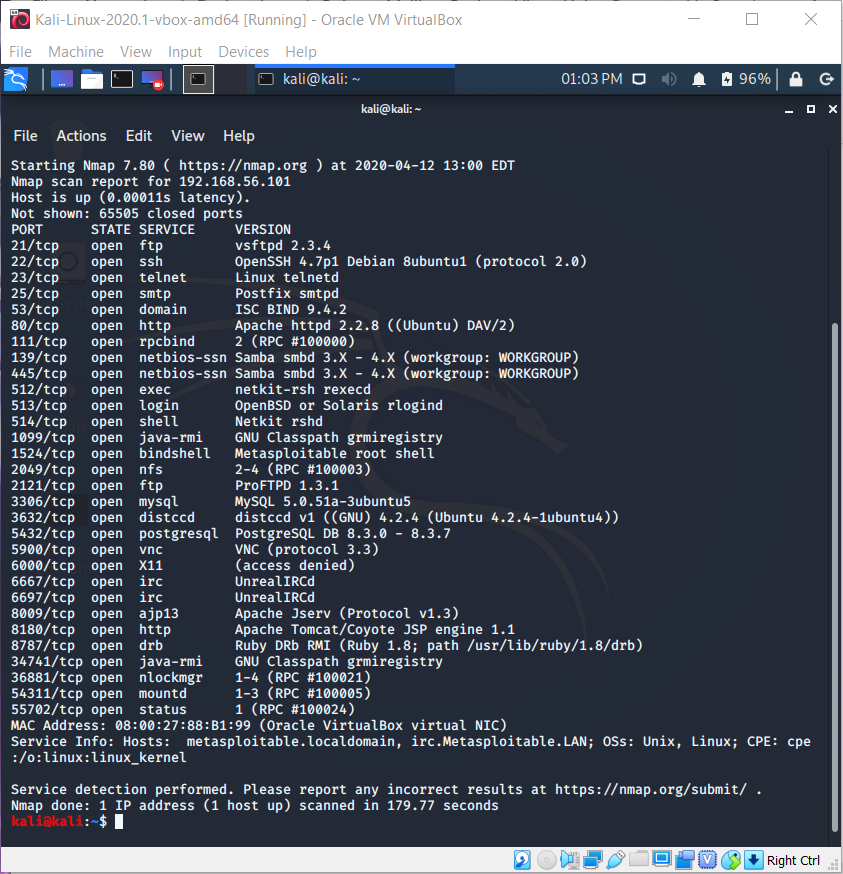
a. What is the different between the Nmap operation in the stealthy mode and nonstealthy mode? (5 pts) Give the example of the nmap command in the stealthy mode and nmap command in the non-stealthy mode. (2 pts)

SYN scan also known as stealth scan makes use of sending a SYN packet and looking at the response. It is quick, scanning multiple ports per second on a fast network not hindered by invasive firewalls. SYN scan is unobtrusive and stealthy due to never finishing TCP connections. -sS is the command used for steathly mode. TCP connect scan is the default TCP scan type when SYN scan is not an option. This is the case when a user does not have raw packet privileges. -sT is the command for steathly mode. A non-stealth port scanner will use of the TCP connect() method of connecting to the destination host.

b. What nmap command that you can use to scan all ports for finding the details information about the target server like the example screenshot in the Figure 2.? (3 pts). Show the screenshot of the complete results from the nmap command that you use in b). (2 pts)

Nmap -sV -p-65535 192.168.56.101

c. What nmap command that you can use to scan the target server and show the following results (see Figure 3)? (3 pts)



Nmap -sV -p-65535 192.168.56.101

d. Besides open or closed state, there are four other states that may appear when you use nmap for port scanning. Briefly explain these six port states (5 pts).

Open - Actively accepting TCP connections, UDP datagrams or SCTP associations to this port.

Closed - Accessible (receives and responds to Nmap packets), but no application listening on it.

Filtered - Cannot determine whether the port is open because packet filtering stops its probes from reaching the port.

Unfiltered - Port is accessible, but Nmap is incapable to tell whether it is open or closed.

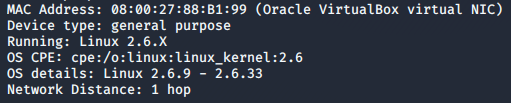
Open|filtered - Unable to determine whether a port is open or filtered. Occurs for scan types in which open ports give no response.

Closed|Filtered - Unable to determine whether a port is closed or filtered. Only used for the IP ID idle scan.

e. What is the Operating System version of the target server? (3 pts) Please include a screenshot that support your answer (2 pts)

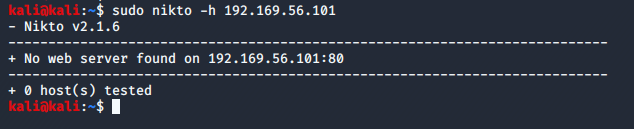
Linux 2.6.X

OS details: Linux 2.6.9 – 2.6.33



f. Explain whether the target server has a running webserver (3 pts) and include a screenshot that support your answer (2 pts)

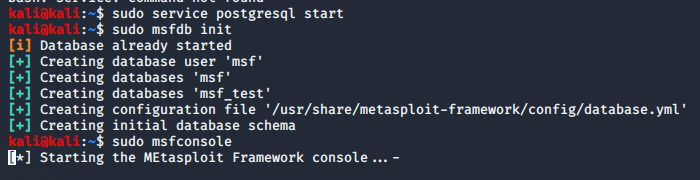
No, the target server is not running a webserver.



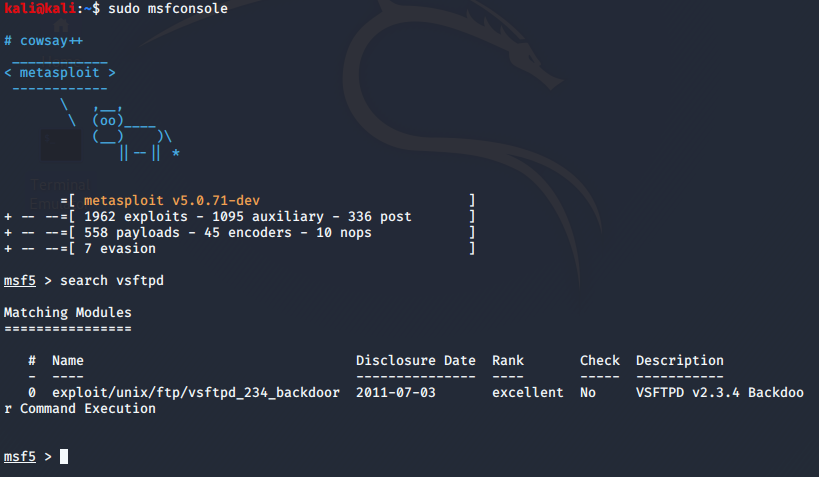
Exploit Vulnerabilities:

From the nmap results, we can see many open ports that can be the target. There are several ways to investigate whether each port has a vulnerability issue. We use the FTP service at port 21 as an example. As you can see, the ftp version is vsftpd 2.3.4. You can use the following tools:

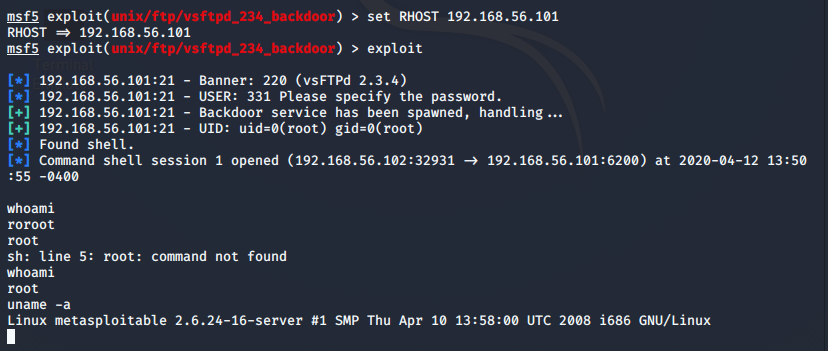
• Using Metasploit. First you need to run postgresql and msfdb init, and then run Metasploit. See figure 4.



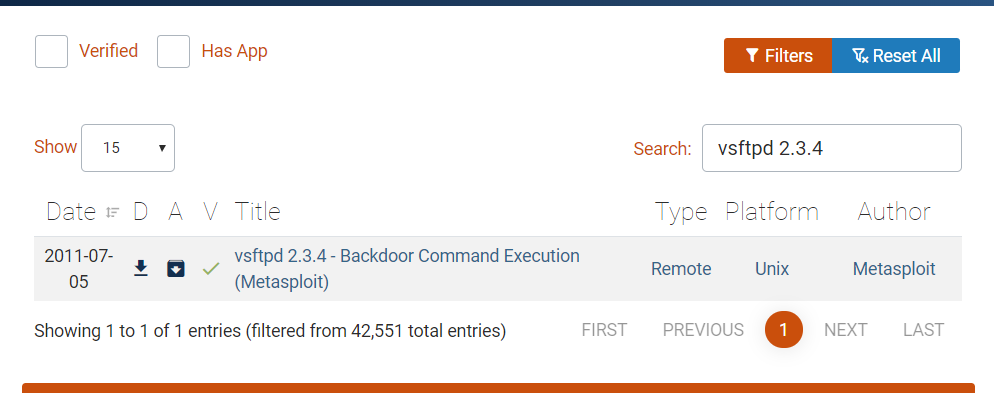
Then search if a vsftpd exploit is available (See Figure 5).



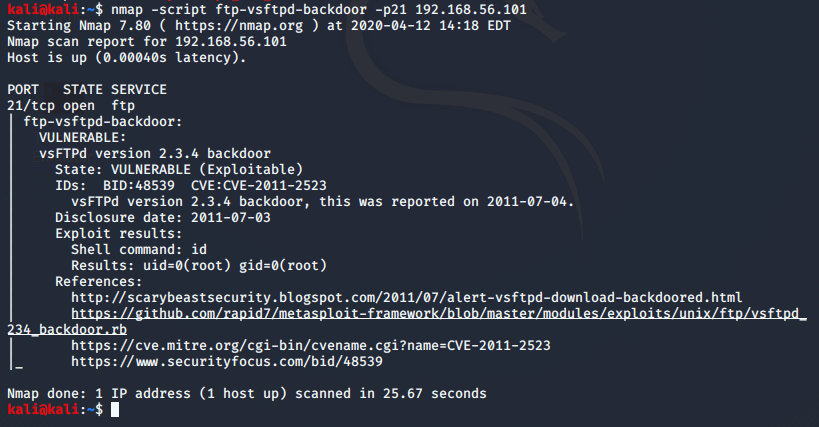
Search an exploit in the metasploit You can use this explain as shown in Figure 6.



• Search in the exploit-db.com (see Figure 7)

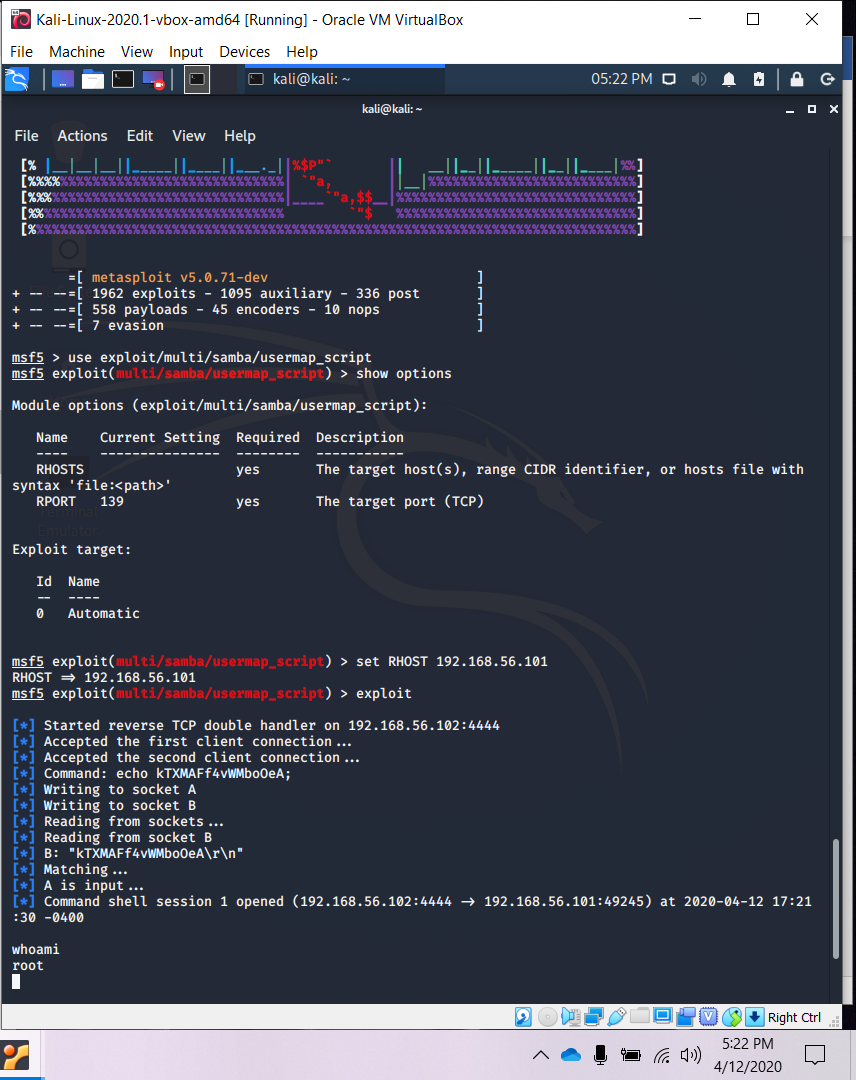


• Using the available nmap scripts to find any exploits. The list of scripts can be found in here: <https://nmap.org/nsedoc/>

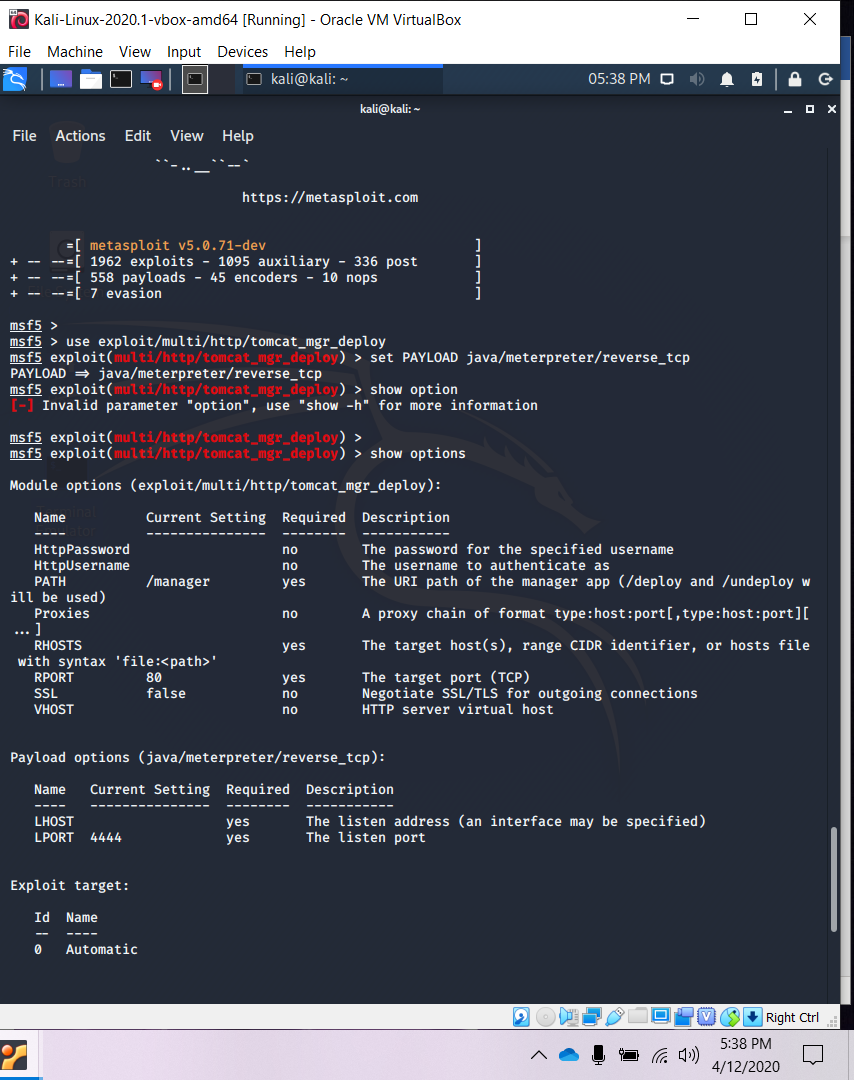


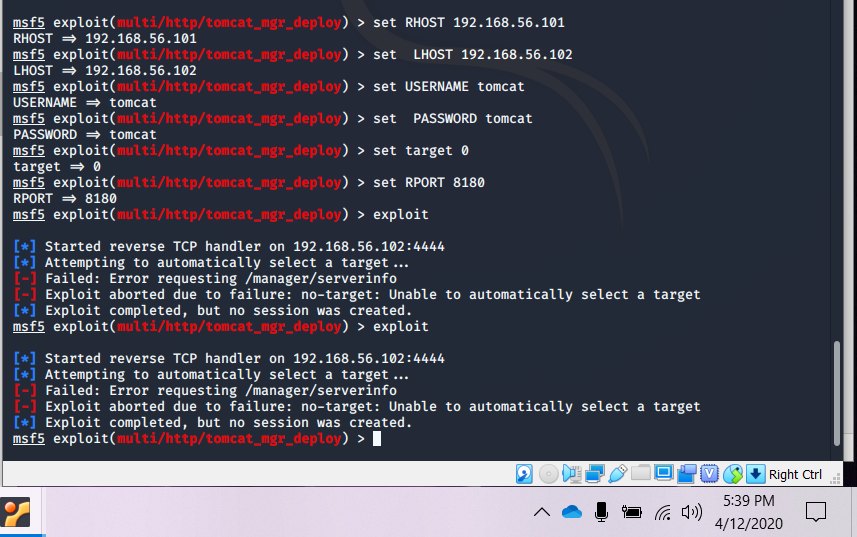
3. (40 pts) Find and show four other exploits in the Metasploitable-2. For each exploit, describes the vulnerability and the steps that you. Also include the screenshots to show that you successfully exploit the vulnerability.

a. SAMBA (Samba “username map script” Command Execution) - Samba is a freeware program that permits users to access and use files, printers, and other normally shared resources over Internet. To exploit SAMBA, we do:

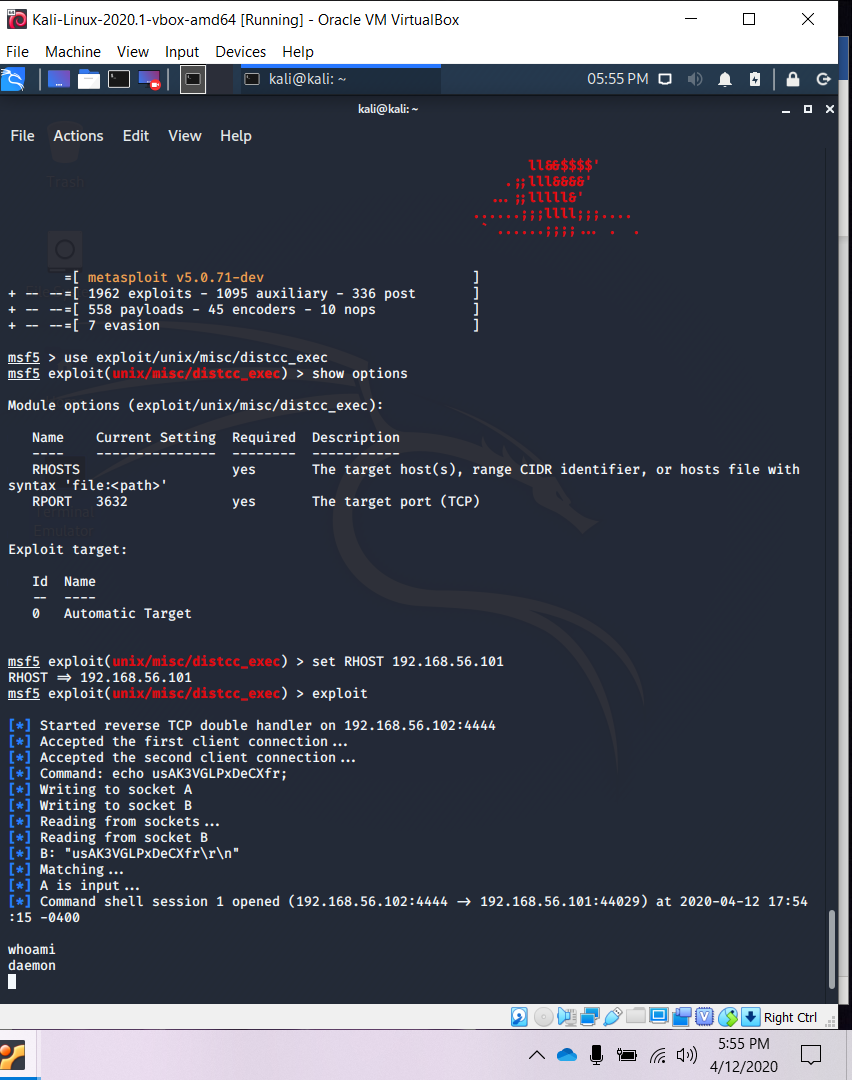


b. Tomcat (Apache Tomcat Manager Application Deployer Authenticated Code Execution) - Tomcat is an application server created to execute Java servlets and render web pages that use Java Server page coding. Tomcat’s default username as well as password are tomcat. To exploit Tomcat, we do:

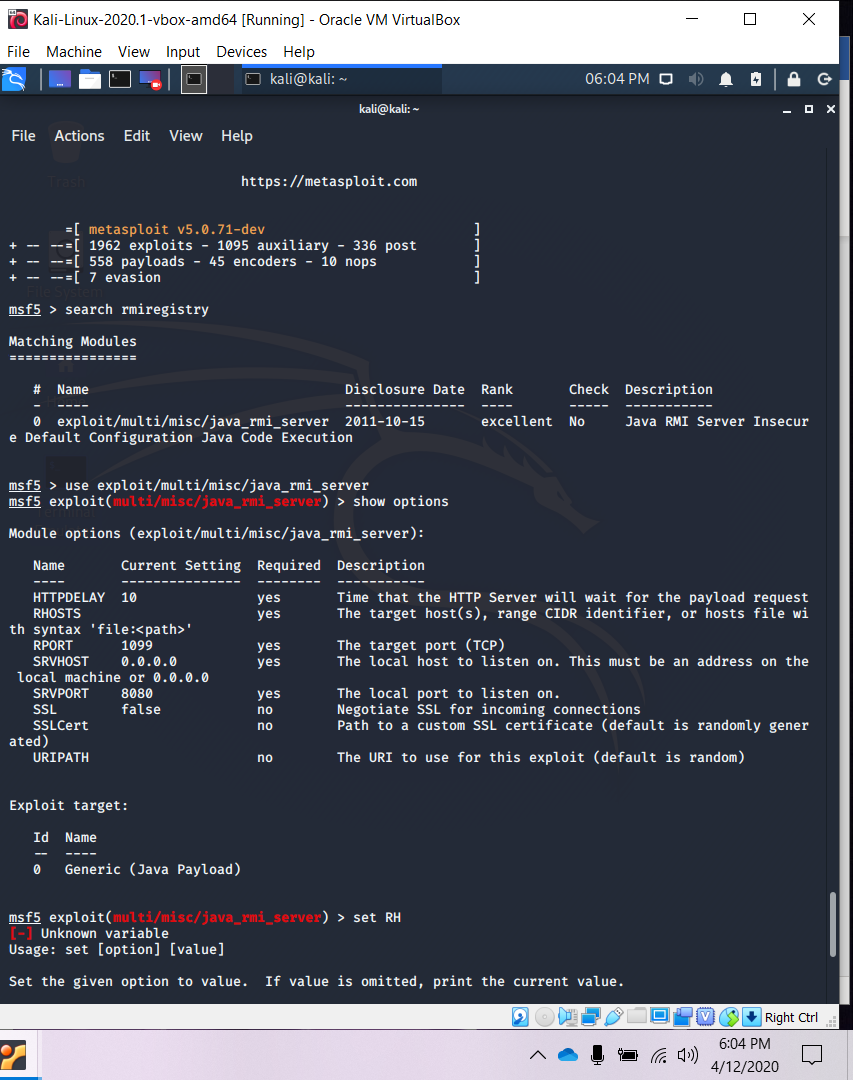


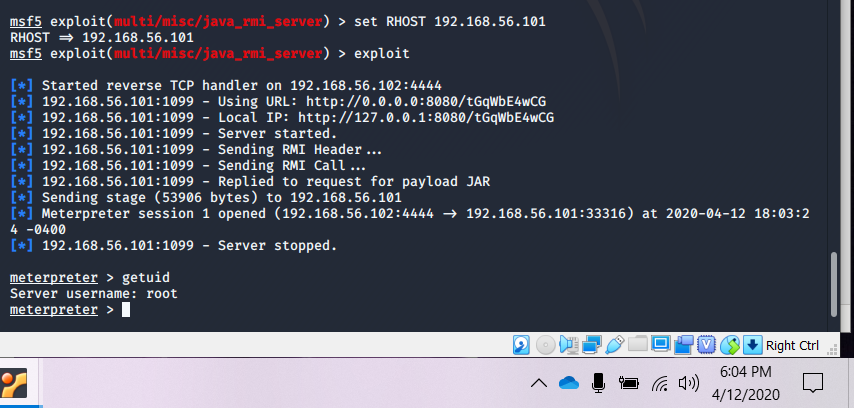


c. DISTCC (DistCC Daemon Command Execution) - DISTCC is a program to distribute builds of C, C++, Objective C or Objective C++ code transversely on several machines on the same network. To exploit DISTCC, we do:



d. GNU Classpath RMI Registry (Java RMI Server Insecure Default Configuration Java Code Execution) - GNU Classpath is a set of vital libraries for supporting the Java programming language. To exploit GNU Classpath RMI Registry, we do:

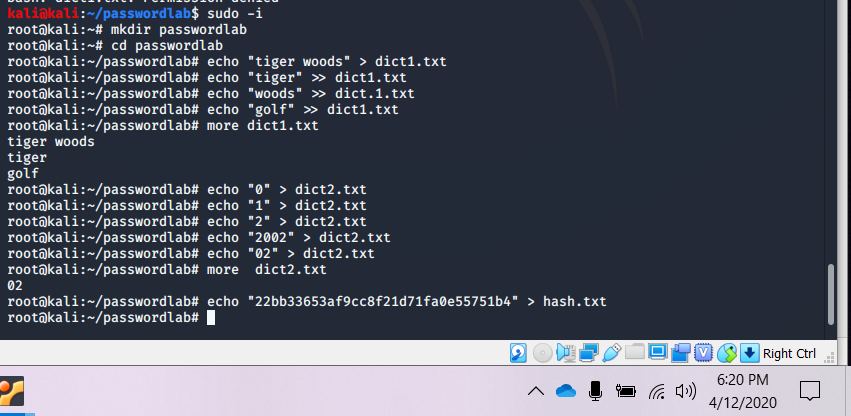




Challenge Passwords with Kali Tools (adopted from the Cisco Networking Academy Program)

A hash value has been recovered for a user, and it is your job to crack this value. Rather than using a brute force method that could take a long time, you will be using known information to crack this value much quicker. The user is a golf fan and has specifically talked about Tiger Woods. In addition, it was discovered from one of his social media public profiles that he graduated in 2002. It is very typical for users to create passwords using words from their special interests or hobbies. When their special interests are known, wordlists can be very helpful in recovering passwords or cracking hashes. The following hash value was provided to you by a known golf fan, and it is your job to crack it: 22bb33653af9cc8f21d71fa0e55751b4

4. (20 pts) Create a passwordlab folder in Kali Linux as your working directory. In this folder, create two dictionary files, and one hash file as shown in Figure 9.



1. What command in Kali Linux that can be used to determine the hash type in the hash.txt file? Describe this tool.

Hash-identifier – this is a simple to use command Line Interface (CLI) software. It helps to identify the different types of hashes used to encrypt data and passwords.

1. What command in Kali Linux that can be used to crack this hash file given these two dictionary files? Explain your steps, and show the cracked password. Include the screenshot of the Kali Linux output to justify your answer.

Go into the created directory. Input the command: John –wordlist=dict1.txt dict2.txt –format=raw-md5 hash.txt

The “–wordlist” includes those words into a library

The “–format” is the type of format the hash is in.

