

Lab Report: Using Ethical Hacking Techniques to Exploit a Vulnerable Workstation

Make sure you submit your completed Lab Report (this document) to Canvas. There is NO Lab Assessment Worksheet required (we will use the Lab Quiz in Canvas instead).

SECTION 1

Do not complete Section 1.

SECTION 2

1. Lab Report file including screen captures of the following:
 - a. open ports on the victim system;

The screenshot shows a Nessus scan report for the IP address 172.30.0.55. The report displays a list of open ports and their associated services. A table of ports is visible, including ports 21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6687, 8009, and 8180. The table columns are Port, State, Service, Reason, Product, Version, and Extra info.

Port	State	Service	Reason	Product	Version	Extra info
21	tcp open	ftp	syn-ack	vsftpd	2.3.4	
22	tcp open	ssh	syn-ack	OpenSSH	4.7p1 Debian 3ubuntu1	protocol 2.0
23	tcp open	telnet	syn-ack	Linux telnetd		
25	tcp open	smtp	syn-ack	Postfix smtpd		
53	tcp open	domain	syn-ack	ISC BIND	9.4.2	
80	tcp open	http	syn-ack	Apache httpd	2.2.8	(Ubuntu) DAV/2
111	tcp open	rpcbind	syn-ack		2	RPC #100000
139	tcp open	netbios-ssn	syn-ack	Samba smbd	3.X - 4.X	workgroup: WORKGROUP
445	tcp open	netbios-ssn	syn-ack	Samba smbd	3.0.20-Debian	workgroup: WORKGROUP
512	tcp open	exec	syn-ack	netkit-rsh rshexec		
513	tcp open	login	syn-ack			
514	tcp open	shell	syn-ack	Netkit rshd		
1099	tcp open	java-rmi	syn-ack	Java RMI Registry		
1524	tcp open	shell	syn-ack	Metasploitable root shell		
2049	tcp open	ifs	syn-ack		2.4	RPC #100003
2121	tcp open	ftp	syn-ack	ProFTPD	1.3.1	
3306	tcp open	mysql	syn-ack	MySQL	5.0.51a-3ubuntu5	
5432	tcp open	postgresql	syn-ack	PostgreSQL DB	8.3.0 - 8.3.7	
5900	tcp open	vnc	syn-ack	VNC		protocol 3.3
6000	tcp open	X11	syn-ack			access denied
6687	tcp open	irc	syn-ack	UnrealIRCd		
8009	tcp open	ajp13	syn-ack	Apache Jserv		Protocol v1.3
8180	tcp open	http	syn-ack	Apache Tomcat/Coyote JSP engine	1.1	

- b. critical vulnerabilities identified by Nessus;

Using Ethical Hacking Techniques to Exploit a Vulnerable Workstation

LAB GUIDE

- Section 1: Hands-On Demonstration
- Section 2: Applied Learning
 - Part 1: Use Zenmap to Scan a Subnet Address
 - Part 2: Conducting a Vulnerability Scan with Nessus

Part 2: Conducting a Vulnerability Scan with Nessus

files to the desktop.

16. From the vWorkstation desktop, open the `youname_S2_VictimScan` file to review your scan results in a new browser window.

When prompted, click **Allow Blocked Content** to open the report in an Internet Explorer window.

17. Make a screen capture showing the **Critical Severity vulnerabilities** for the 172.30.0.55 scan and paste it into the Lab Report file.

18. Minimize the browser window.

19. Close the remote TargetWindows02 connection.

172.30.0.55

Severity	CVSS v3.0	Plugin	Name
CRITICAL	9.8	134862	Apache Tomcat AJP Connector Request Injection (GHOSTcat)
CRITICAL	9.8	34970	Apache Tomcat Manager Common Administrative Credentials
CRITICAL	9.8	51988	Bind Shell Backdoor Detection
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0	34460	Unsupported Web Server Detection
CRITICAL	10.0*	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	61708	VNC Server 'password' Password
CRITICAL	10.0*	10203	rexecd Service Detection
HIGH	8.8	55523	vsftpd Smiley Face Backdoor

c. details of the 55523 vulnerability;

Using Ethical Hacking Techniques to Exploit a Vulnerable Workstation

LAB GUIDE

- Section 3: Lab Challenge and Analysis

Part 3: Exploit the Victim System using Metasploit

5. At the msf prompt, execute `search vsftpd`.

Metasploit will search for all attack vectors on the victim system that work against the vsftpd service. It will return the following exploit:

```
exploit/unix/ftp/vsftpd_234_backdoor. You will also notice that Metasploit has ranked this vulnerability as excellent, indicating that the exploit is almost certain to work.
```

6. At the msf prompt, execute `use exploit/unix/ftp/vsftpd_234_backdoor` to use the exploit identified in the Metasploit search results.

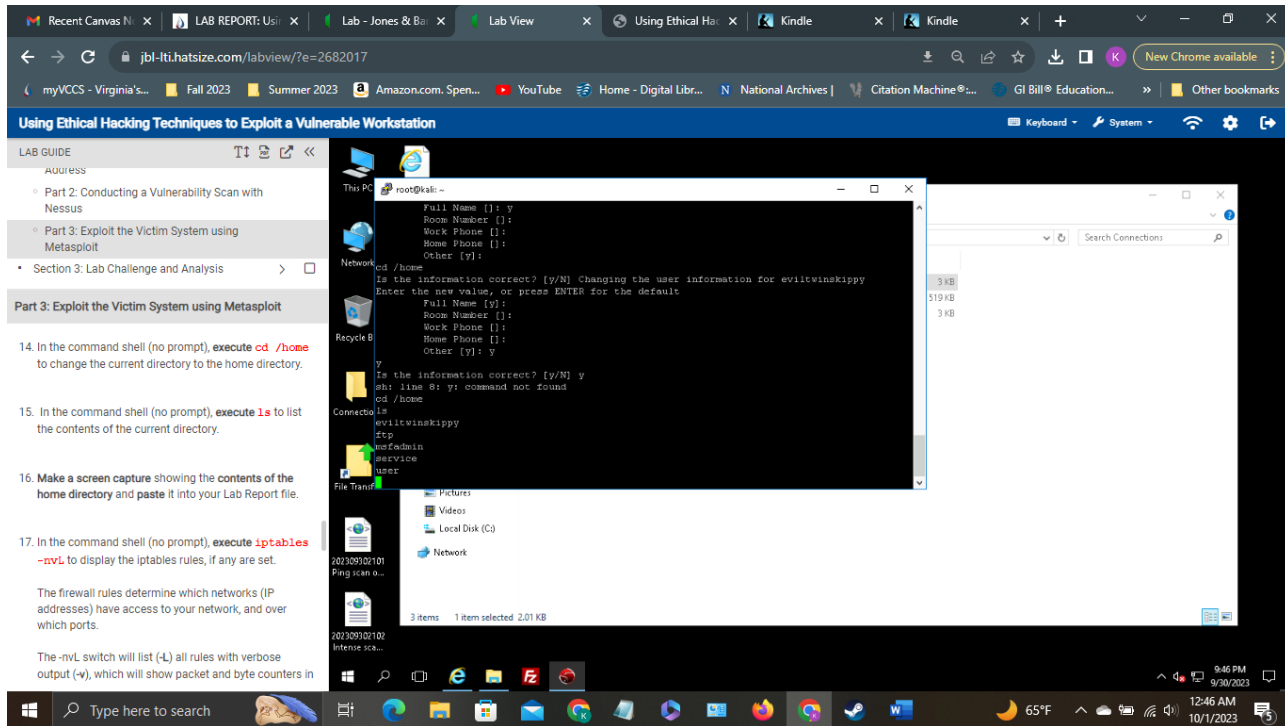
7. At the msf exploit (`vsftpd_234_backdoor`) prompt, execute `set RHOST 172.30.0.55` to identify the remote host as the victim system.

8. At the msf prompt (`vsftpd_234_backdoor`) execute

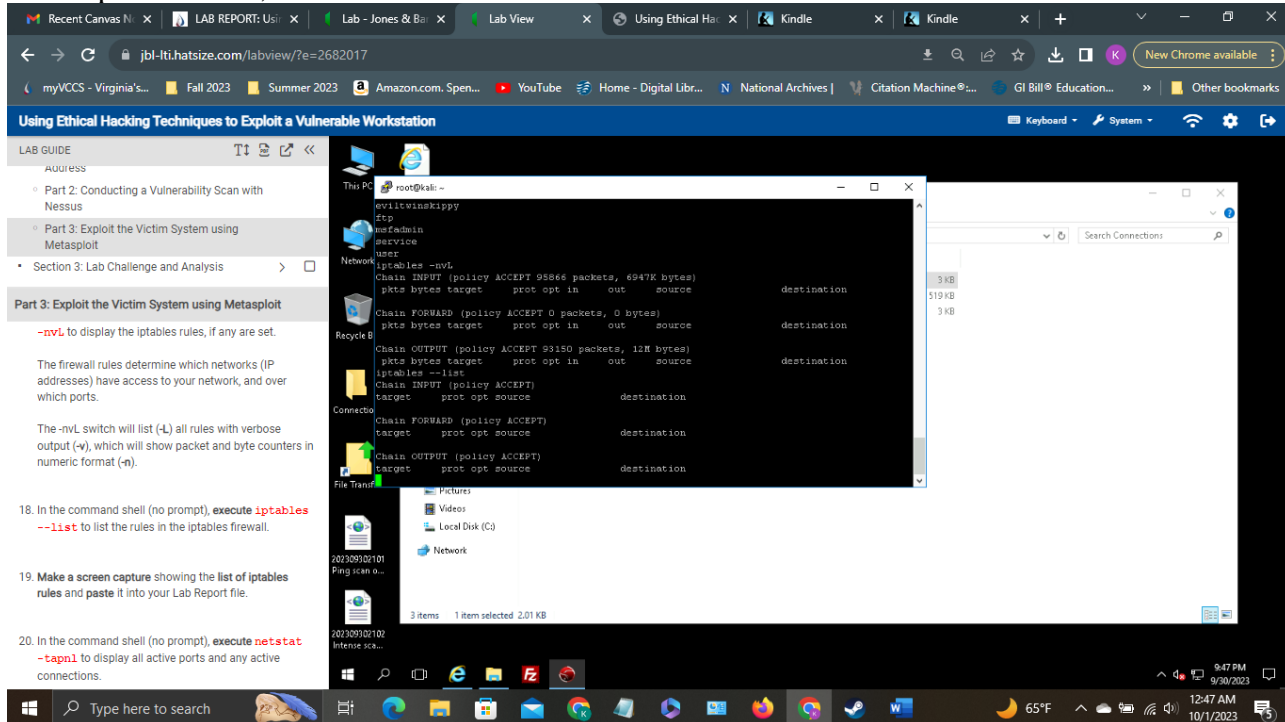
```
root@kali:~# msf5 (root) > search vsftpd
[*] Module database cache not built yet, using slow search

Matching Modules
=====
Name                               Disclosure Date  Rank  Description
-----
exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03      excellent VSFTPD v2.3
4 Backdoor Command Execution
```

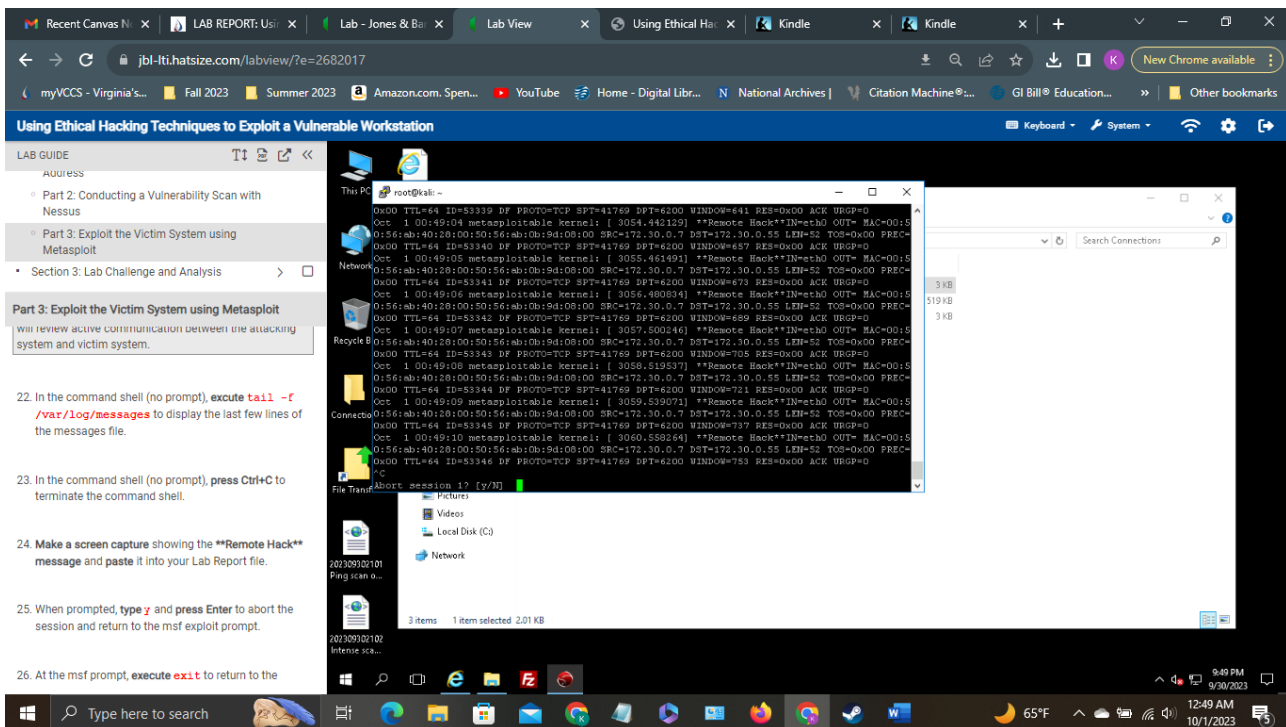
d. contents of the /home directory;



e. list of iptables rules;



f. ****Remote Hack**** message in the log;



2. Files downloaded from the virtual environment:

a. Zenmap Ping scan;



202309302101 Ping scan on 172.30.0.0_2

b. Zenmap Intense scan;



202309302102 Intense scan on 172

c. yourname_S2_VictimScan;



kurtwilliams_S2_VictimScan.html.html

3. Any additional information as directed by the lab:

a. recommended solution for the vsftpd vulnerability.

Student: Kurt Williams
Instructor: Joel Kirch
Course: TC295.ITN.261.O01C.FA23
Date: 10/1/2023

The screenshot shows a web browser window with multiple tabs. The active tab is titled "Using Ethical Hacking Techniques to Exploit a Vulnerable Workstation". The browser address bar shows the URL "https://www.tenable.com/plugins/nessus/55523". The page content is for the "vsftpd Smiley Face Backdoor" plugin, which is rated as "HIGH" severity. The page includes sections for Synopsis, Description, Solution, and Risk Information. The Synopsis states: "The remote FTP server contains a backdoor, allowing execution of arbitrary code." The Description explains that the version of vsftpd running on the remote host has been compiled with a backdoor, and attempting to login with a username containing a smiley face triggers the backdoor. The Solution section advises to "Validate and recompile a legitimate copy of the source code." The Risk Information section lists a CVSS v2 score of 8.3 and a Risk Factor of Critical. On the left side of the browser, there is a "LAB GUIDE" sidebar with a table of contents. The current section is "Part 3: Exploit the Victim System using Metasploit". The sidebar also contains a "Note" at the bottom: "Note: This completes Section 2 of this lab. In the next steps, you will use the File Transfer folder to move any files from the vWorkstation to your local system that are to be submitted as part of your lab deliverables. Refer to the instructions in the Common Lab Tasks document for more".

SECTION 3

Do not complete Section 3.