Task C.

Exploit Windows 7 with a deliverable payload (60 pt).

In this task, you need to create an executable payload with the required configurations below. Once your payload is ready, you should upload it to the web server running on Kali Linux and download the payload from Windows 7, then execute it on the target to make a reverse shell (10 pt). Of course, don't forget to configure your Metasploit on Kali Linux before the payload is triggered on the target VM.

The requirements for your payload are (10 pt, 5pt each):

- Payload Name: Use your MIDAS ID (for example, pjiang.exe)
- Listening port: XXXX (follow the lab instruction)



(In the above screenshot, port 8888 is set to the listening port)

[Post-exploitation] Once you have established the reverse shell connection to the target Windows 7, complete the following tasks in your meterpreter shell:

1. Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. (10 pt)



(In the above screenshots, the screenshot command verifies the exploit worked. The second picture is a screenshot of Windows 7 server desktop)

This is the default welcome page used to test the correct operation of the Apache2 sinstallation on Debian systems. If you can read this page, it means that the Apache installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably mean that the site is currently unavailable due to maintenance. If the problem persists, please contact the

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the

ache HTTP serve

□ 1 日 日 日 40) 5:55 PN 3/17/202

•

M

Л

Ĩ

8

0

C. Wiresharl

ø

debian

site's administrator.

VMw

ache2-doc package was installed on this server

📚 Kali - Internal Work... 👲 Windo

2. Create a text file on the attacker Kali named "IMadeIT-YourMIDAS.txt" (replace YourMIDAS with your university MIDAS ID) and put the current timestamp in the file. Upload this file to the target's desktop. Then log in to Windows 7 VM and check if the file exists. You need to show me the command that uploads the file. (10 pt)



t VMware	active can							23 Public
workstattan	6	G v Window 7 → Downloads Organize ▼ Include in library ▼ Share with ▼ New folder						P S S S S S S S S S S S S S S S S S S S
1.10								0
	Chrome	👉 Favorites	Name	Date modified	Туре	Size		TjTf.jpeg
		Desktop	192.168.10.9	3/17/2024 6:16 PM	9 File		1 KB	UTeg.jpeg
and the second		Downloads	best_calculator_ever	3/17/2024 5:00 PM	Application		73 KB	20
A N	1	🔛 Recent Places	IMadeIT-jruss020	3/17/2024 5:50 PM	Application		73 KB	ch file or director
1 1 2 1	SHUTY	1000	MadelT-jruss020	3/17/2024 5:46 PM	Text Document		73 KB	
		词 Libraries						
		Documents						
		J Music						Tecolates
100	N	Pictures						jpeg Videos
	Manager Silli	Videos						VMshare
and the		all Hamana						vPeDTjTt.jpeg
	CN_	No Homegroup						jpeg zcomoreg.jpeg
	-	Computer						
	Skepinite	Local Disk (C:)						
And the second second		😪 vmshare (\\169.254.1						

(In the above screenshots, a txt file was made in Kali and sent to the Windows 7 server machine)

[Privilege escalation] Background your current session, then gain administrator-level privileges on the remote system (10 pt). After you escalate the privilege, complete the following tasks:

3. Create a malicious account with your name and add this account to the administrator group. You need to complete this step on the Attacker Side. (5 pt)





(In the above screenshot, a malicious user was created and given administrator privilege)

4. Remote access to the malicious account created in the previous step and browse the files belonging to the user, "Windows 7", in RDP. (5 pt)



(In the above screenshot, rdesktop command was used to log into the Windows 7 server from Kali Linux)