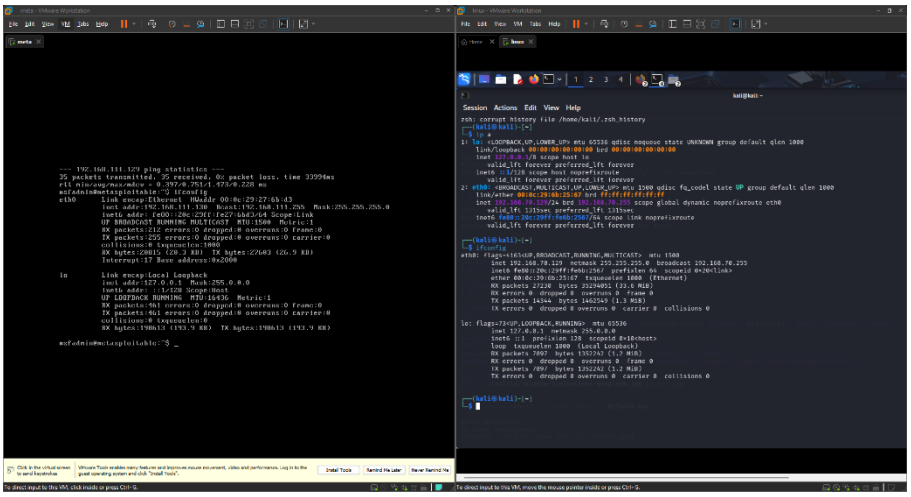
Table of Contents

1. Environment Setup

a) Kali Linux and Metasploitable Linux Machine should be installed in VBox.

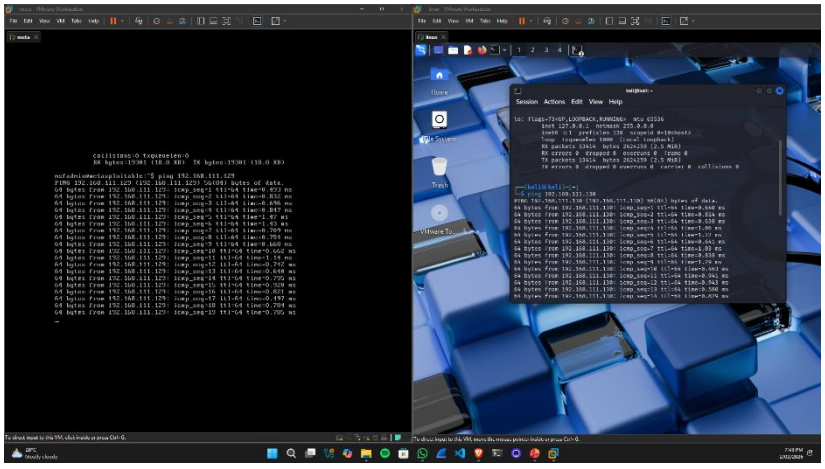
b) Demonstrate the connectivity between Kali Linux and Metasploitable Linux Machine.

Note: First, the Kali terminal is opened and the command ip a is executed to obtain the IP address of the Kali machine (right side). Next, the Metasploitable system is accessed and the command ipconfig is executed to obtain the Metasploitable IP address (left side).



1.a IP addresses of both machines

Note: Next, the Kali machine is connected to the Metasploitable machine by executing the command ping <Kali_machine_IP> (left side). Similarly, the Metasploitable machine is connected to the Kali machine by executing the command ping <Metasploitable_IP> (right side).



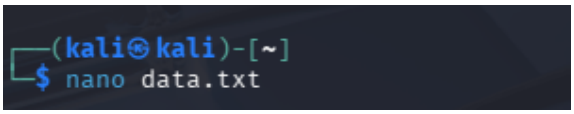
1.a Connectivity in both machines

2. Creating the target file

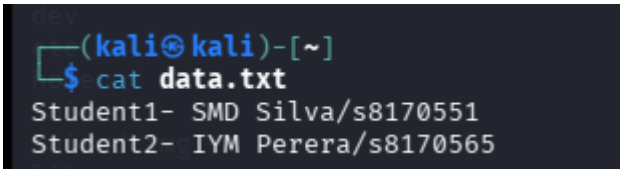
a) Encrypt the symmetric cryptography and store the cypher text a file named personalData.txt

I. Stud1 Name + Stud1 ID and Stud2Name + Stud2ID are working as a team

Note: A file is created using the Nano text editor, and the student names and IDs are saved within the file.

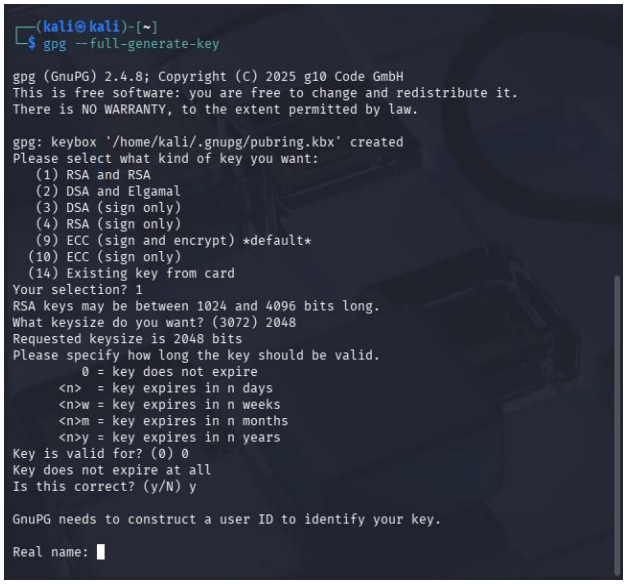


2.a open nano text editor



2.a Open data.txt

Note: A key is generated using the data.txt file, and the left-side image confirms successful key creation.



2.a Generate key

2.a created successfully

Note: Next, the data.txt file is encrypted by executing the command "gpg -e data.txt". After encryption, the file is converted to the data.txt.gpg format. The image below shows that the encryption process was completed successfully.

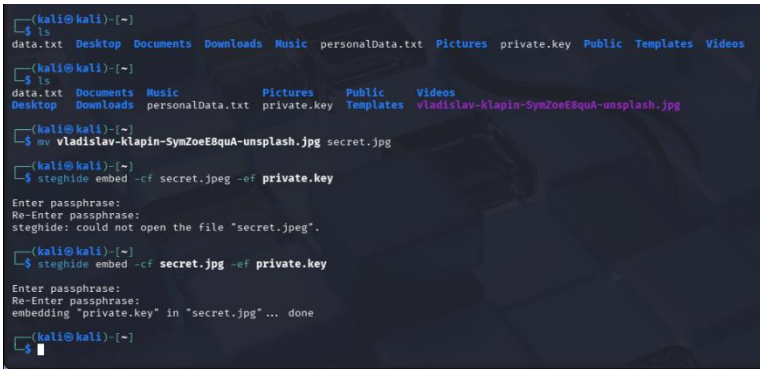
2.a encrypted

Note: Afterwards, the encrypted file is renamed to personalData.txt using the command "mv data.txt.gpg personalData.txt", and the file name is verified to confirm that the renaming was completed correctly.

2.a rename data.txt and verify

b) Hide the private key inside image using the necessary stegano tool. Name the image as secret.jpg

Note: The private key is hidden inside the image using the command "steghide embed -cf secret.jpg -ef private.key".



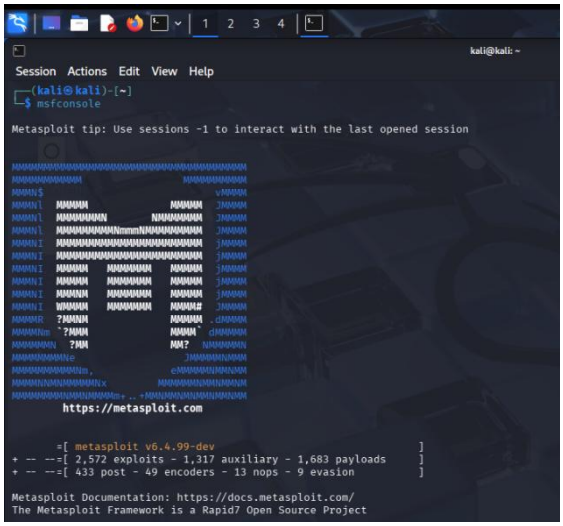
3. Remote session setup

a) Using the MSF framework from Kali Linux find all the open ports of Metasploitable.

b) Use one of the open ports to create a session from Kali Linux to Metasploitable

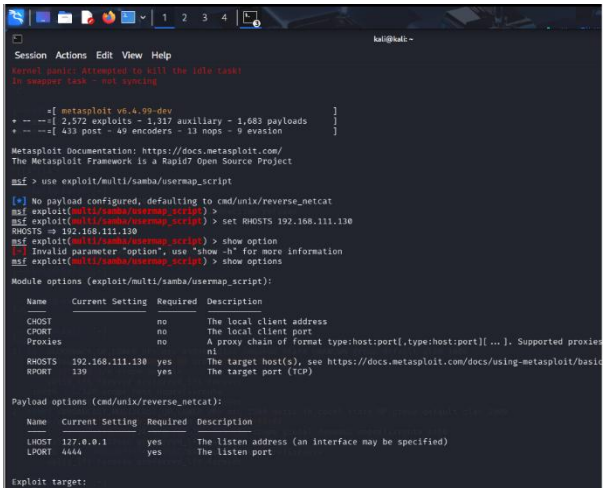
Note: Metasploit is started on the Kali machine. And an Nmap scan is performed. The result are shown in the liwer right side image. The scan is executed using command "nmap -sV 192.168.111.130"

3.a Open Metasploit

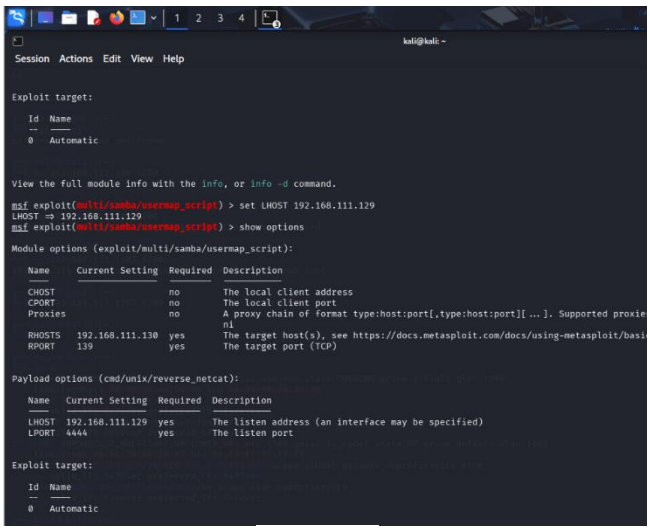


3.a Nmap scan

Note: The vulnerability exploit/multi/samba/usermap_script is selected, and the RHOST and LHOST parameters are configured. The module is loaded using the command "use exploit/multi/samba/usermap_script."



3.b use samba exploit and set RHOST



3.b set LHOST

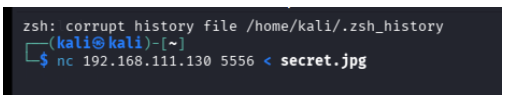
c) Copy personalData.txt and secret.jpg to Metasploitable

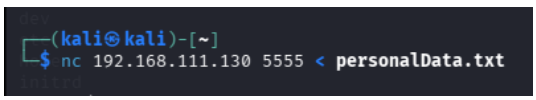
Note: The user and hostname of the system are checked, confirming that the user is root and the hostname is Metasploitable. This verifies that access has been obtained on the correct target machine, as the intended target hostname is Metasploitable.

3.c check user, hostname and upload file and image

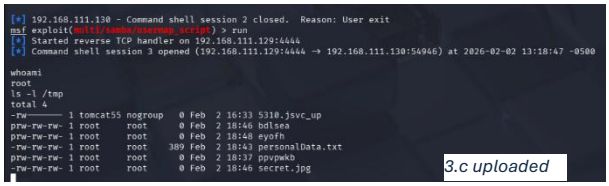
Note: After attempting to upload the personalData.txt file and the secret.jpg image to the Metasploitable system using the command upload personalData.txt and upload secret.jpg, the upload process is unsuccessful. As an alternative approach, a new terminal session is opened and the command nc 192.168.111.130 5556 is executed to establish a connection to the remote shell on the Metasploitable machine.

****This command uses Netcat (nc) to connect to a shell that is already running on the target machine.****





Note: Finally, the file and the image are uploaded to the target machine.



3.c uploaded