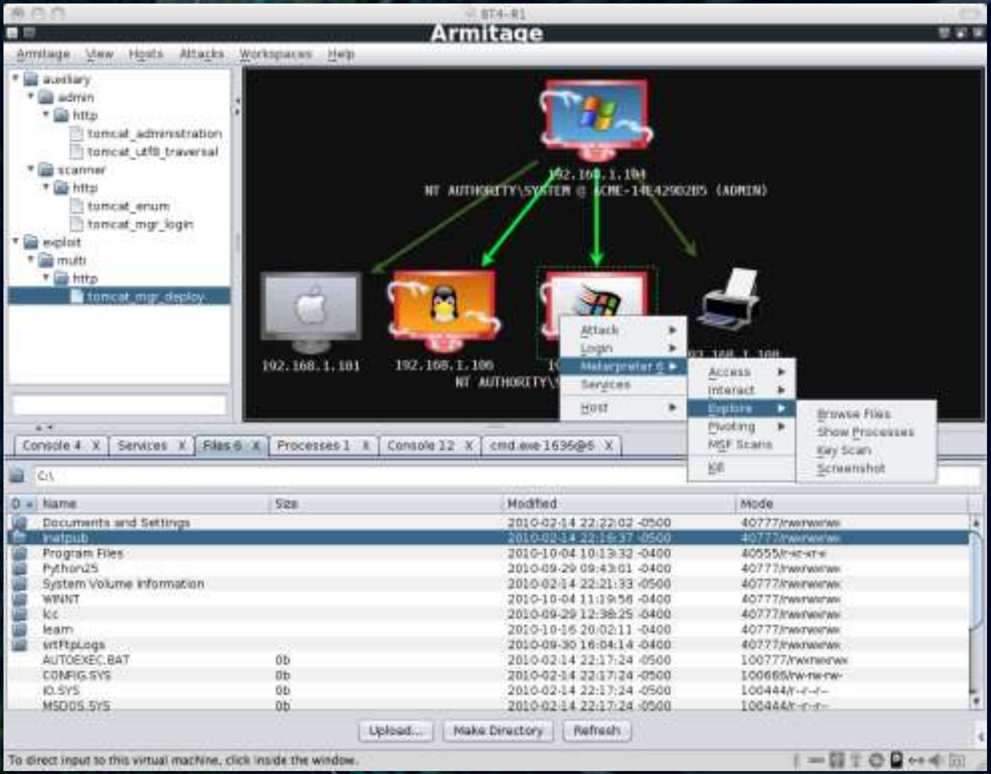
Cyber Attack for Management

The Armitage Project

ISSA DC / 18 Jan 11

Today…

- Your speaker
- On Hacking…
- What is Armitage?
- Demonstration
- Q&A



D	Name	Size	Modified	Mode
	Documents and Settings		2010-02-14 22:22:02 -0500	40777/rwxrwxrwx
	Inetpub		2010-02-14 22:16:37 -0500	40777/rwxrwxrwx
	Program Files		2010-10-04 10:13:32 -0400	40555/r-xr-xr-x
	Python25		2010-09-29 09:43:01 -0400	40777/rwxrwxrwx
	System Volume Information		2010-02-14 22:21:33 -0500	40777/rwxrwxrwx
	WINNT		2010-10-04 11:19:56 -0400	40777/rwxrwxrwx
	lcc		2010-09-29 12:38:25 -0400	40777/rwxrwxrwx
	learn		2010-10-16 20:02:11 -0400	40777/rwxrwxrwx
	srtFtpLogs		2010-09-30 16:04:14 -0400	40777/rwxrwxrwx
	AUTOEXEC.BAT	0b	2010-02-14 22:17:24 -0500	100777/rwxrwxrwx
	CONFIG.SYS	0b	2010-02-14 22:17:24 -0500	100666/rw-rw-rw-
	IO.SYS	0b	2010-02-14 22:17:24 -0500	100444/r--r--r--
	MSDOS.SYS	0b	2010-02-14 22:17:24 -0500	100444/r--r--r--

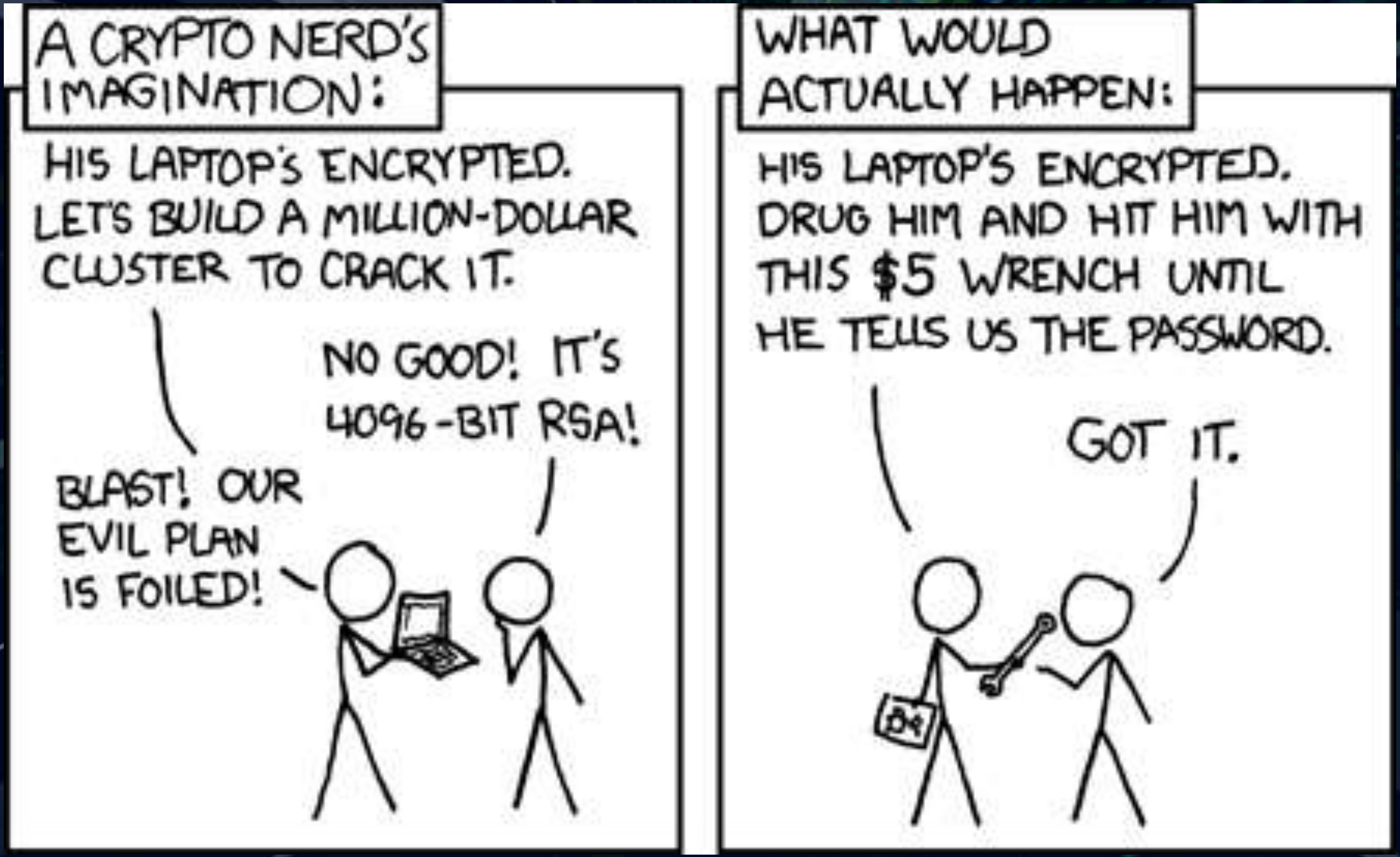
Your Speaker…

- Systems Administrator
- NOSC Crew Commander
- Cyber Ops R&D Team Lead
- Red Team Member
- Penetration Tester

Hacking is like… magic

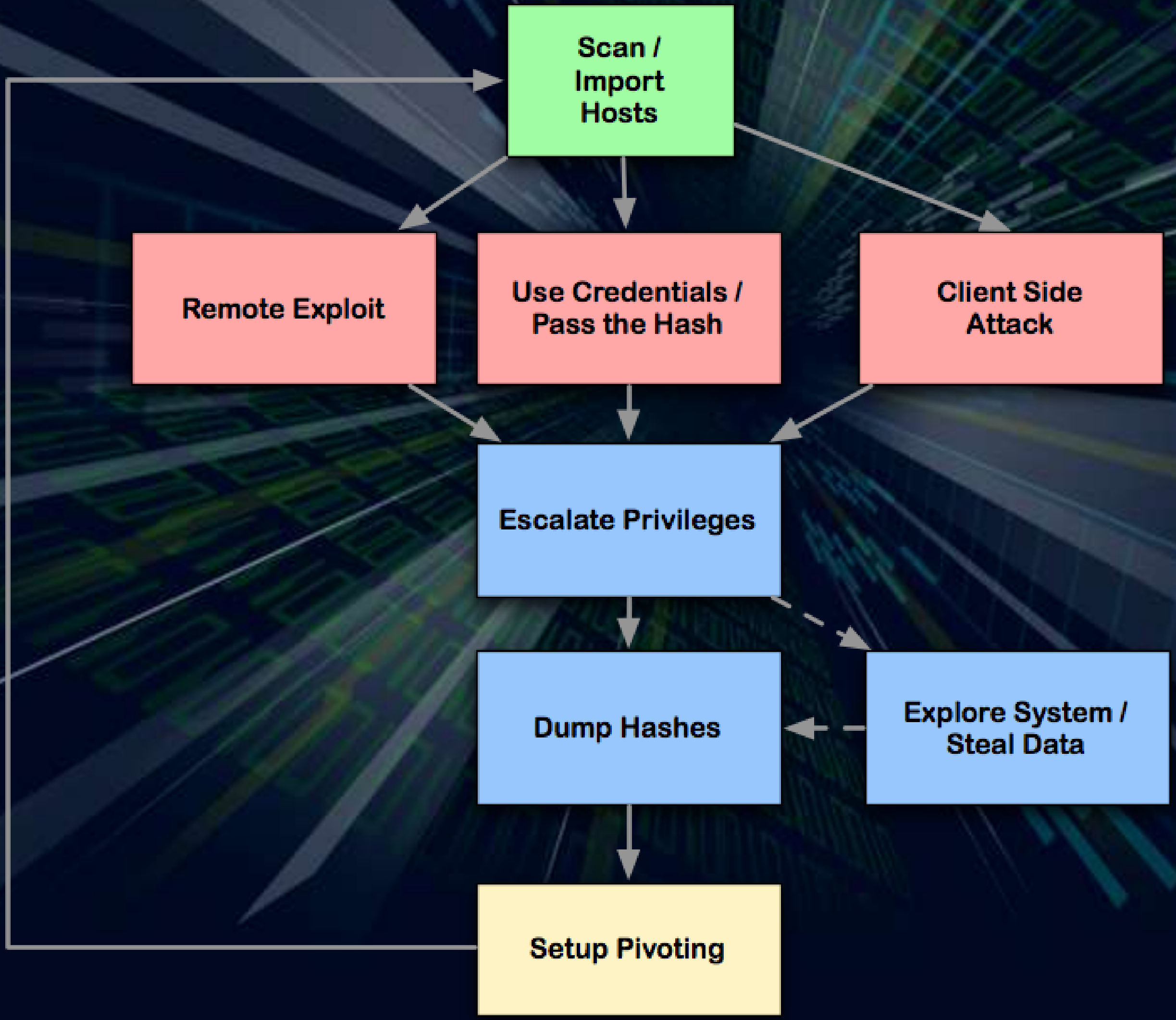
Frederick Bancroft
Prince of Magicians
Act II – The Magnificent Orient and the Wizard's Enchantments.

It’s easier than you think…


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Cartoon: XKCD by Randall Munroe: http://xkcd.com/538

Hacking is a Process



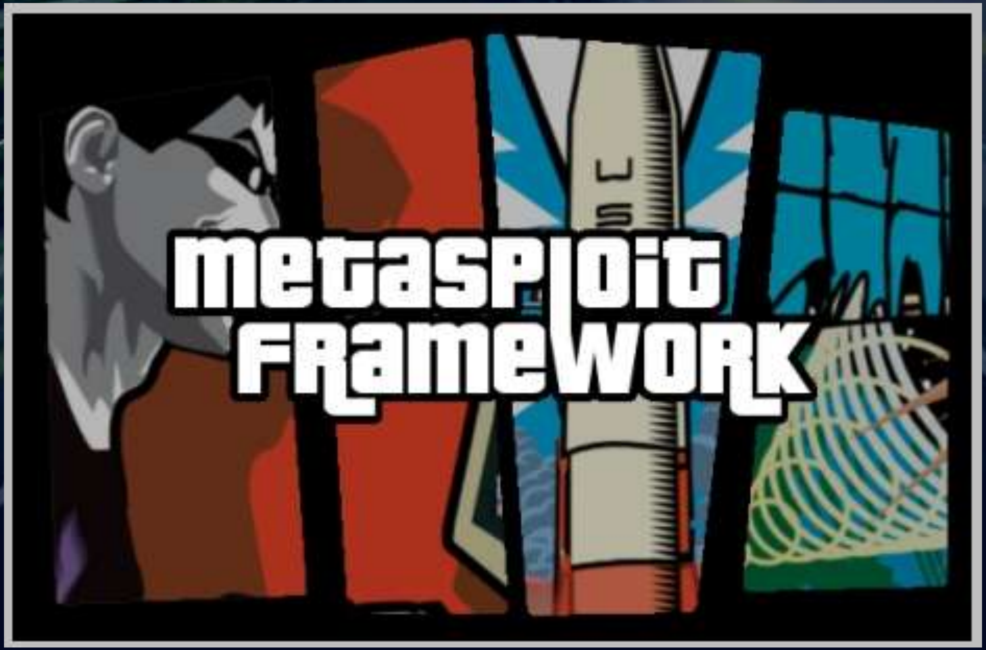
On Hacking

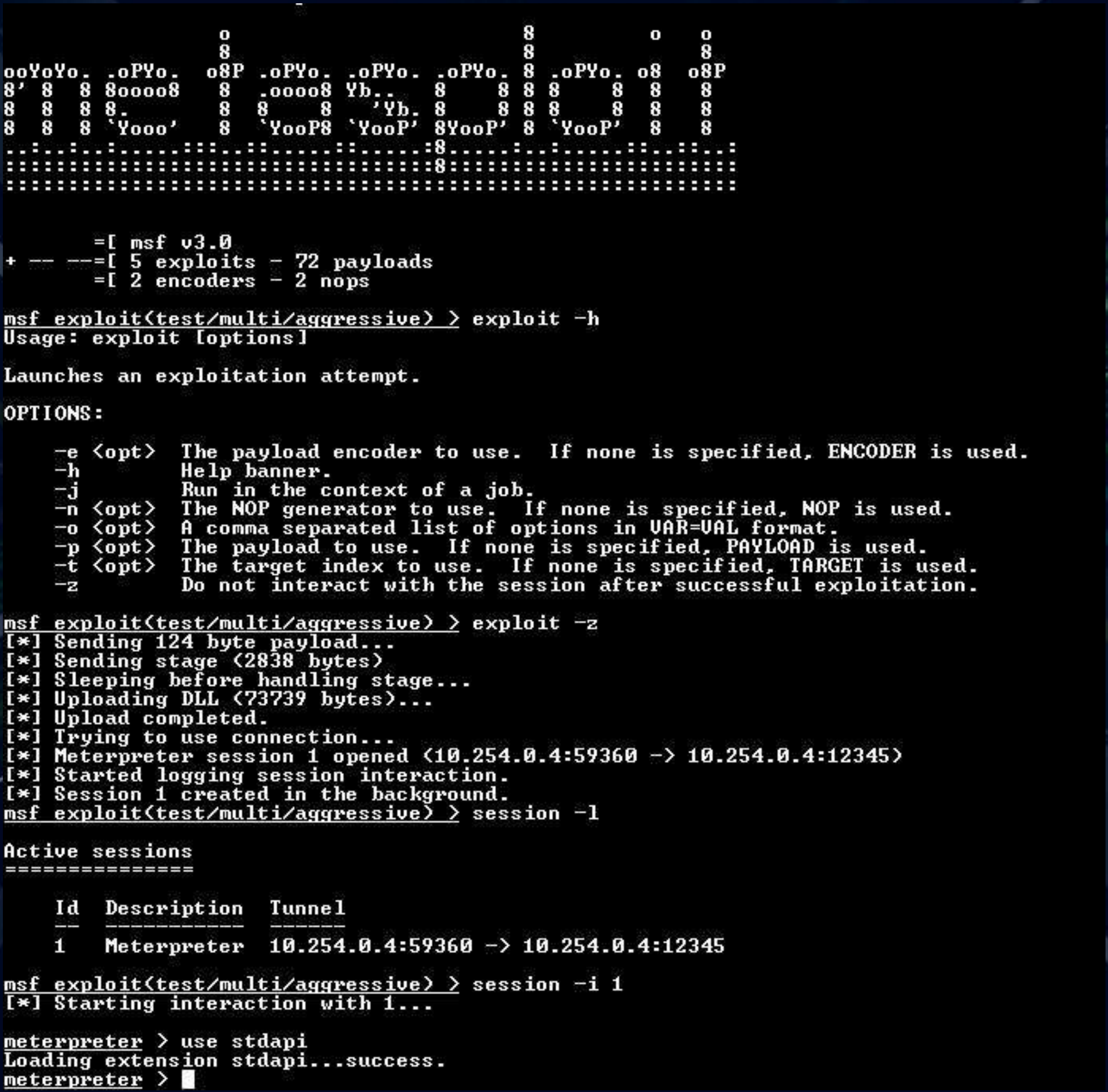
- It’s like magic…
- It’s easier than you think
- It’s a process

Metasploit

- A Penetration Testing and Exploit Development Framework

http://www.metasploit.com





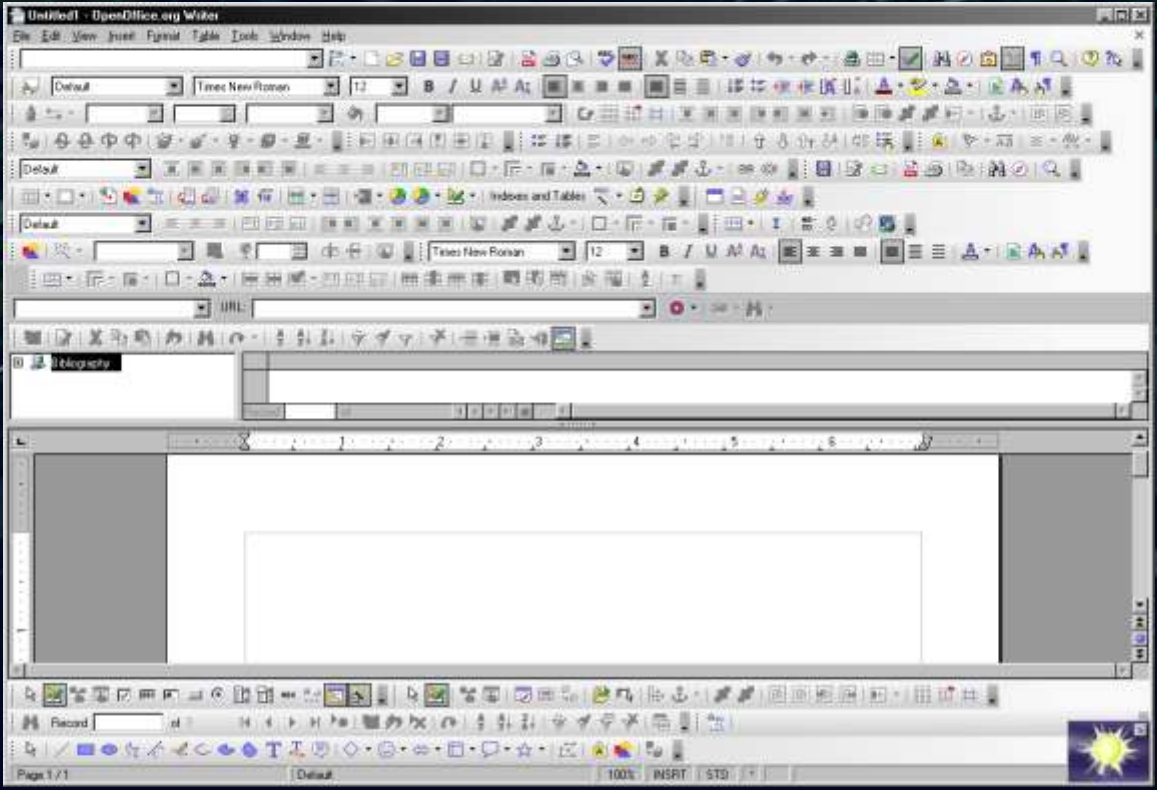
```
                 o                       8         o   o
                 8                       8             8
ooYoYo. .oPYo.  o8P .oPYo. .oPYo. .oPYo. 8 .oPYo. o8  o8P
8' 8  8 8oooo8   8  .oooo8 Yb..   8    8 8 8    8  8   8
8  8  8 8.       8  8    8   'Yb. 8    8 8 8    8  8   8
8  8  8 `Yooo'   8  `YooP8 `YooP' 8YooP' 8 `YooP'  8   8
..:..:..:......::..::.....::.....:8.....:..:.....::..::..:
::::::::::::::::::::::::::::::::::8:::::::::::::::::::::::
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::


       =[ msf v3.0
+ -- --=[ 5 exploits - 72 payloads
       =[ 2 encoders - 2 nops

msf exploit(test/multi/aggressive) > exploit -h
Usage: exploit [options]

Launches an exploitation attempt.

OPTIONS:

    -e <opt>  The payload encoder to use.  If none is specified, ENCODER is used.
    -h        Help banner.
    -j        Run in the context of a job.
    -n <opt>  The NOP generator to use.  If none is specified, NOP is used.
    -o <opt>  A comma separated list of options in VAR=VAL format.
    -p <opt>  The payload to use.  If none is specified, PAYLOAD is used.
    -t <opt>  The target index to use.  If none is specified, TARGET is used.
    -z        Do not interact with the session after successful exploitation.

msf exploit(test/multi/aggressive) > exploit -z
[*] Sending 124 byte payload...
[*] Sending stage (2838 bytes)
[*] Sleeping before handling stage...
[*] Uploading DLL (73739 bytes)...
[*] Upload completed.
[*] Trying to use connection...
[*] Meterpreter session 1 opened (10.254.0.4:59360 -> 10.254.0.4:12345)
[*] Started logging session interaction.
[*] Session 1 created in the background.
msf exploit(test/multi/aggressive) > session -l

Active sessions
===============

    Id  Description  Tunnel
    --  -----------  ------
    1   Meterpreter  10.254.0.4:59360 -> 10.254.0.4:12345

msf exploit(test/multi/aggressive) > session -i 1
[*] Starting interaction with 1...

meterpreter > use stdapi
Loading extension stdapi...success.
meterpreter > █
```

What is Armitage?

- A GUI for Metasploit
  - Recommends exploits
  - Configures modules
  - Aids Post Exploitation
  - Friendly to Command-line Users

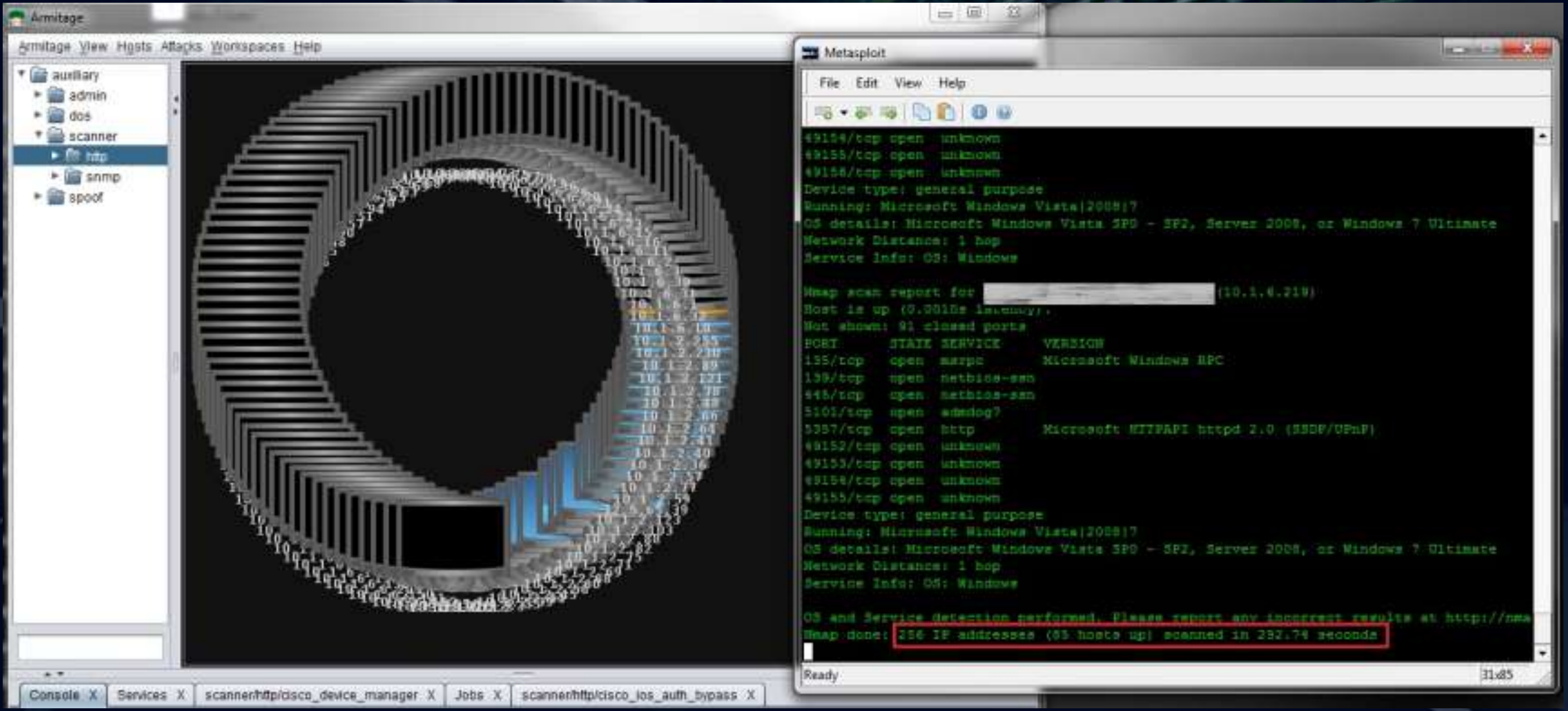
What is Armitage?

- A GUI for Metasploit
- Goal: Avoid this…



What is Armitage?

- Usable for your penetration tests?



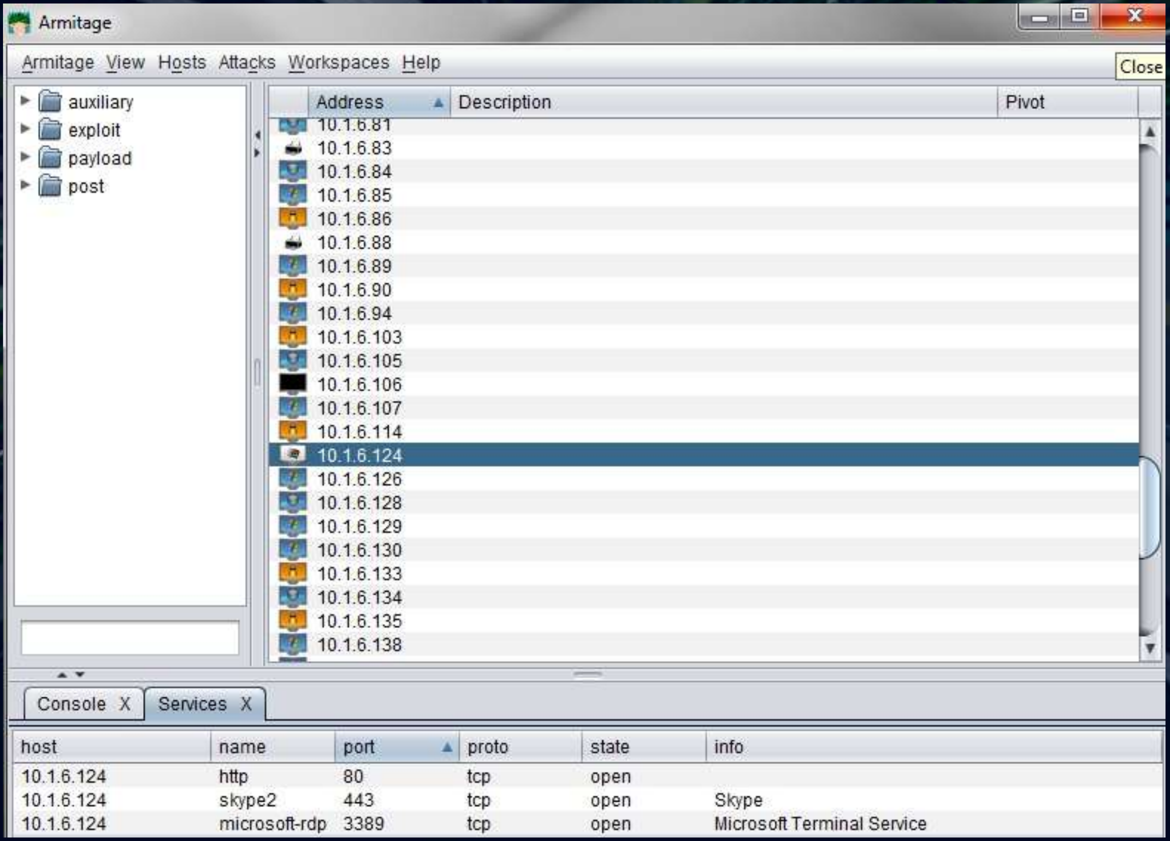
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
admin
dos
scanner
http
snmp
spoof
Metasploit
File Edit View Help
Ready
31x85
Console X
Services X
scanner/http/cisco_device_manager X
Jobs X
scanner/http/cisco_ios_auth_bypass X

```
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS details: Microsoft Windows Vista SP0 - SP2, Server 2008, or Windows 7 Ultimate
Network Distance: 1 hop
Service Info: OS: Windows

Nmap scan report for [redacted] (10.1.6.219)
Host is up (0.0015s latency).
Not shown: 91 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
5101/tcp  open  admdog?
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS details: Microsoft Windows Vista SP0 - SP2, Server 2008, or Windows 7 Ultimate
Network Distance: 1 hop
Service Info: OS: Windows

OS and Service detection performed. Please report any incorrect results at http://nma
Nmap done: 256 IP addresses (85 hosts up) scanned in 232.74 seconds
```

Image courtesy of @guerilla7 on Twitter.

What is Armitage?

- Usable for your penetration tests



Address	Description	Pivot
10.1.6.81		
10.1.6.83		
10.1.6.84		
10.1.6.85		
10.1.6.86		
10.1.6.88		
10.1.6.89		
10.1.6.90		
10.1.6.94		
10.1.6.103		
10.1.6.105		
10.1.6.106		
10.1.6.107		
10.1.6.114		
10.1.6.124		
10.1.6.126		
10.1.6.128		
10.1.6.129		
10.1.6.130		
10.1.6.133		
10.1.6.134		
10.1.6.135		
10.1.6.138		

host	name	port	proto	state	info
10.1.6.124	http	80	tcp	open	
10.1.6.124	skype2	443	tcp	open	Skype
10.1.6.124	microsoft-rdp	3389	tcp	open	Microsoft Terminal Service

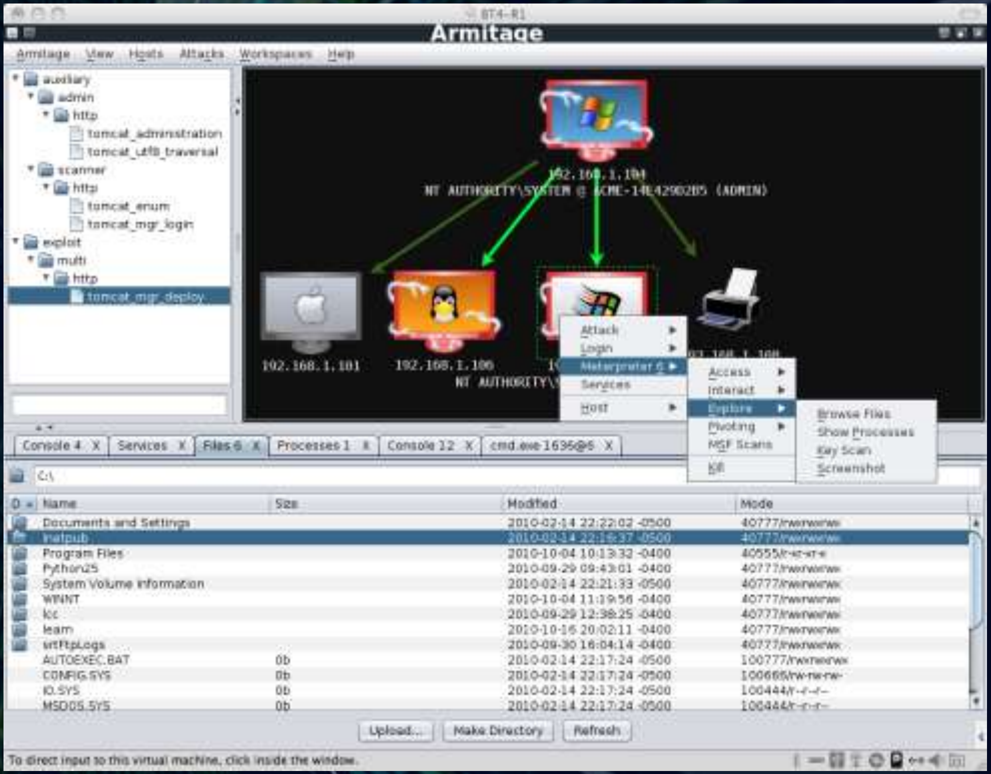
Image courtesy of @guerilla7 on Twitter.

Stop, Demo Time!

- Scanning
- Exploitation
- Post Exploitation
- Maneuver

Today…

- Your speaker
- On Hacking…
- What is Armitage?
- Demonstration
- Q&A



C:\

D	Name	Size	Modified	Mode
	Documents and Settings		2010-02-14 22:22:02 -0500	40777/rwxrwxrwx
	Inetpub		2010-02-14 22:16:37 -0500	40777/rwxrwxrwx
	Program Files		2010-10-04 10:13:32 -0400	40555/r-xr-xr-x
	Python25		2010-09-29 09:43:01 -0400	40777/rwxrwxrwx
	System Volume Information		2010-02-14 22:21:33 -0500	40777/rwxrwxrwx
	WINNT		2010-10-04 11:19:56 -0400	40777/rwxrwxrwx
	lcc		2010-09-29 12:38:25 -0400	40777/rwxrwxrwx
	learn		2010-10-16 20:02:11 -0400	40777/rwxrwxrwx
	wtFtpLogs		2010-09-30 16:04:14 -0400	40777/rwxrwxrwx
	AUTOEXEC.BAT	0b	2010-02-14 22:17:24 -0500	100777/rwxrwxrwx
	CONFIG.SYS	0b	2010-02-14 22:17:24 -0500	100666/rw-rw-rw-
	IO.SYS	0b	2010-02-14 22:17:24 -0500	100444/r--r--r--
	MSDOS.SYS	0b	2010-02-14 22:17:24 -0500	100444/r--r--r--

To direct input to this virtual machine, click inside the window.

Go get it…

- Website
  - http://www.fastandeasyhacking.com
- Twitter
  - @armitagehacker
- Email
  - contact@fastandeasyhacking.com