

Forum:[Hack Forums](#)

Thread: [SOCIAL ENGINEERING TOOLKIT \(SET\): AN EASY POWERSHELL BASED ATTACK](#)

Mr.Zzz - August 25, 2017, 10:47 pm

In this brief tutorial we will take a look at some of the tools included with Social Engineering Toolkit (SET), mainly we will focus on an easy PowerShell based attack. We will create a PowerShell shellcode file and sending it to a target. If we can trick the target into running the shellcode we will get a remote connection to the victim's PC.

To start SET from Kali Linux main menu:

Applications>Exploitation Tools > Social Engineering Toolkit

Or just type "setoolkit" in a terminal prompt.

1. Once SET is up select "Social-Engineering Attacks"

2. Select "Powershell Attack Vectors"

3. Next choose "Powershell Alphanumeric Shellcode Injector"

4. Now just enter the IP address of the Kali system and what port you want to use for the Windows machine to connect in on. Usually the default port is 443.

5. Finally SET asks if you want to start the listener now. Type "yes" at the prompt.

It will start Metasploit framework console and SET now creates the exploit code. Then we just need to get the exploit code to the victim system. SET will place the exploit code into the "/root/.set/reports/powershell/" directory. Leave the SET window open and navigate to the powershell directory since you will see the powershell injection code in a text file, called "x86_powershell_injection.txt". Rename and change the extension from ".txt" to ".bat". When and whether a Windows PC runs the code, a remote session will open up to your Kali terminal. Then you hit enter, type "sessions -i" and the 'number Id' of the open session and you will start the interaction with the victim's machine. Once a "meterpreter" session is open we can use any Meterpreter command, or just type "shell" to get a remote command prompt.

05317832892 - August 27, 2017, 1:20 am

So this is just a .bat script that launches a powershell script which injects some meterpreter shellcode?

My preferred way is a powershell stager for empire. A lot more powerful and easier bc no av mess.

Mr.Zzz - August 27, 2017, 2:16 am

[quote='ROOTED' pid='55719763' dateline='1503822033']

So this is just a .bat script that launches a powershell script which injects some meterpreter shellcode?

Yes, it is!

Mr. Rooted,

Can you please show to all of us your preferred way.....you are talking about in my article? I'd be always very grateful to you.

We are newbies here and we want to learn, thank in advance for your reply

oscp harder - August 27, 2017, 4:26 am

Yes it will work on both [Outside the LAN and inside the LAN] Depend on target ip.

But the only problem is here is that nowadays AV becomes smart so attack like this might be fail

As hacker also smart then use smarter way as the above user stated already and try to find that techniques which AV can't detect and nowadays metasploit have those things too

Mr.Zzz - August 27, 2017, 5:31 am

oscpharder

thank you very much for your usefull answers.

You're very right about av mess.

I see, you too you are "peasant" even though willing to help people to improve their knowledge.

About av mess there should not be problem since Rooted will teach us his preferred way.....

(Aug 27, 2017 01:20 AM)ROOTED Wrote: [\[CITE\]](#) My preferred way is a powershell stager for empire. A lot more powerful and easier bc no av mess.

.....no AV message.

Faith Connors - August 27, 2017, 7:20 am

(Aug 27, 2017 05:31 AM)Mr.Zzz Wrote: [\[CITE\]](#) oscpharder

thank you very much for your usefull answers.

You're very right about av mess.

I see, you too you are "peasant" even though willing to help people to improve their knowledge.

About av mess there should not be problem since Rooted will teach us his preferred way.....

.....no AV message.

just a reminder, peasant just means you have under 50 posts, nothing more.

i've seen some pretty dumb people hit really high "ranks" in a sense who don't contribute shit, and i've seen people with under 50 completely rewrite older scripts for optimization.

as for whatever concerns you mentioned earlier, i don't see anything that is blatantly wrong by any chance. i would like you to go a little more in-depth on things, though. there's no point in making a tutorial if you don't actually explain how things work. think about things like:

>why is 443 the "preferred" or default port?

>why do we change txt to bat?

>show some code snippets from the bat/txt to show what the script is doing

>using external vs internal/private IPs

>how could you now send the file to someone?

>why is the file named "_x86" at the end?

if you don't want to type out super long answers for these questions, it's always okay to reference other tutorials, just throw in a link and say "if you're curious, read here for more."

Mr.Zzz - August 27, 2017, 11:15 am

(Aug 27, 2017 07:20 AM)Faith Connors Wrote: [\[CITE\]](#) >how could you now send the file to someone?

Faith, my dear,

thank you very much for your time.

Questions you are asking me are good. And when I say that questions are good usually I do not the answers.

But the one I quote it is the very good one. I was thinking too..... and I come out to send it through

email. And I want to say more to you.....mail's attachement.....and.....hidden behind an image.

What do you think???

Please, let me know your idea.
Many thanks in advance!

Faith Connors - August 27, 2017, 11:47 am

(Aug 27, 2017 11:15 AM)Mr.Zzz Wrote: [\[CITE\]](#) Faith, my dear,
thank you very much for your time.

Questions you are asking me are good. And when I say that questions are good usually I do not the answers.

But the one I quote it is the very good one. I was thinking too..... and I come out to send it through email. And I want to say more to you.....mail's attachement.....and.....hidden behind an image.

What do you think???

Please, let me know your idea.
Many thanks in advance!

i think that an image does not run as an executable, so you can't hide code behind an image, er, well technically you can, but it won't do anything.

there are of course exceptions to this rule like if you find a vulnerability in the codec, like the old jpg vulnerability that causes a segfault by trying to read/write memory outside of its allocated buffer caused by incomplete headers, but not only do you need to know some extremely low-level code and build your exploit on a case-by-case system, it's incredibly hard to find vulnerabilities like this as well, especially in closed-source software like the jpg2000 codec was (became open sourced shortly after)

Mr.Zzz - August 27, 2017, 12:21 pm

(Aug 27, 2017 11:47 AM)Faith Connors Wrote: [\[CITE\]](#) i think that an image does not run as an executable, so you can't hide code behind an image, er, well technically you can, but it won't do anything.

there are of course exceptions to this rule like if you find a vulnerability in the codec, like the old jpg vulnerability that causes a segfault by trying to read/write memory outside of its allocated buffer caused by incomplete headers, but not only do you need to know some extremely low-level code and build your exploit on a case-by-case system, it's incredibly hard to find vulnerabilities like this as well, especially in closed-source software like the jpg2000 codec was (became open sourced shortly after)

And what about to compress it in a RAR archive?

Faith Connors - August 27, 2017, 12:35 pm

(Aug 27, 2017 12:21 PM)Mr.Zzz Wrote: [\[CITE\]](#) And what about to compress it in a RAR archive?
you need to make it a sfx archive (self extracting) which still makes it an exe, thus not being able to send/receive by most major email providers.

Mr.Zzz - August 27, 2017, 12:54 pm

(Aug 27, 2017 12:35 PM)Faith Connors Wrote: [\[CITE\]](#) you need to make it a sfx archive (self extracting) which still makes it an exe, thus not being able to send/receive by most major email providers.

If you embedded it in a new folder then you compress, change extension in .a instead of .rar (it is still able to be opened) and finally you compress all for the last time.....Bhe....sometimes it is not

detected by ISP.

You are very right because it is not self-extracting. How can I manage it?

cheers!!!

Faith Connors - August 27, 2017, 12:57 pm

(Aug 27, 2017 12:54 PM)Mr.Zzz Wrote: [\[CITE\]](#) If you embedded it in a new folder then you compress, change extension in .a instead of .rar (it is still able to be opened) and finally you compress all for the last time.....Bhe....sometimes it is not detected by ISP.

You are very right because it is not self-extracting. How can I manage it?

cheers!!!

by isp? i think you mean by av because your isp won't give a fuck if you get hacked lol

and yeah, but the point of doing anything like that is to have a one-click way of infecting someone, just by them opening a file, not opening a file in a file in a file which in turn they have to execute. looks too fishy on its own. that's why pdf/xls/doc exploit builders exist, so you have one file which can infect a computer after opening once.

Mr.Zzz - August 27, 2017, 1:24 pm

Ciao Faith

I mean gmail, yahoo etc...etc

I can always say that it's a compromising video, very long and heavy ???

Faith Connors - August 27, 2017, 1:28 pm

(Aug 27, 2017 01:24 PM)Mr.Zzz Wrote: [\[CITE\]](#) Ciao Faith

I mean gmail, yahoo etc...etc

I can always say that it's a compromising video, very long and heavy ???

people won't look at an exe file and say "wowo cool video"

at least if they're not over the age of 80 or under 6.

also should be mentioned .rar files won't open natively on windows.

Mr.Zzz - August 27, 2017, 1:33 pm

(Aug 27, 2017 01:28 PM)Faith Connors Wrote: [\[CITE\]](#) people won't look at an exe file and say "wowo cool video"

at least if they're not over the age of 80 or under 6.

also should be mentioned .rar files won't open natively on windows.

YOU'RE GOOD!, YOU'RE VERY GOOD!!, YOU'RE VERY VERY GOOD!!!

Thank you ???

zer0dev - August 28, 2017, 3:23 am

These type of files are very easily detected by almost all anti-virus programs under [backdoor/trojan]

categories.

It's not possible to send it through email as a file, however, we have few options.

For sending the file host it on your web server or host the file on a free file hosting domains and link them through.

As for bypassing anti-virus programs, we need good FUD crypter or encoders, MSF does have good encoders, did try few of them, but they fail to bypass antivirus, may be we may get good crypter at the dark web.

-zer0dev

terry.sahil - August 28, 2017, 8:56 am

Hello ,

Anyone knows other method to send the file instead of email .

Thanks

SysAdmin - August 28, 2017, 9:20 am

(Aug 28, 2017 03:23 AM)zer0dev Wrote: [\[CITE\]](#) These type of files are very easily detected by almost all anti-virus programs under [backdoor/trojan] categories.

It's not possible to send it through email as a file, however, we have few options.

For sending the file host it on your web server or host the file on a free file hosting domains and link them through.

As for bypassing anti-virus programs, we need good FUD crypter or encoders, MSF does have good encoders, did try few of them, but they fail to bypass antivirus, may be we may get good crypter at the dark web.

-zer0dev

Or you know, don't, as there's plenty of free crypters around the internet, for example Shellter.

Stop using that cancer font.

Mr.Zzz - August 28, 2017, 9:59 am

(Aug 28, 2017 08:56 AM)terry.sahil Wrote: [\[CITE\]](#) Hello ,

Anyone knows other method to send the file instead of email .

Thanks

If you can gain physical access to the device then you can inject the file using also an USB flash drive.

zer0dev - August 28, 2017, 12:37 pm

(Aug 28, 2017 09:20 AM)SysAdmin Wrote: [\[CITE\]](#) Or you know, don't, as there's plenty of free crypters around the internet, for example, Shellter.

Stop using that cancer font.

I did use free crypters and binders, but they didn't work, at least not with, "McAfee and kaspersky".

SysAdmin - August 28, 2017, 1:57 pm

(Aug 28, 2017 12:37 PM)zer0dev Wrote: [\[CITE\]](#) I did use free crypters and binders, but they didn't work, at least not with, "McAfee and kaspersky".

Obviously, most of the ones are either heavily outdated or backdoored.

Make your own.

zer0dev - August 29, 2017, 3:49 am

(Aug 28, 2017 01:57 PM)SysAdmin Wrote: [\[CITE\]](#) Obviously, most of the ones are either heavily outdated or backdoored. Yes, that's what I told in my post.

Quote: Make your own.

Yes, I got your point,

KDE isn't working well on my desktop, that means, I go create my own DE. :/

Faith Connors - August 29, 2017, 5:25 am

(Aug 29, 2017 03:49 AM)zer0dev Wrote: [\[CITE\]](#) Yes, that's what I told in my post.

Yes, I got your point,

KDE isn't working well on my desktop, that means, I go create my own DE. :/

there's a difference between something not working and something being unstable for you.

kde is completely irrelevant, even for the point you're trying to prove.

zer0dev - August 29, 2017, 6:36 am

Obviosuly, if something is not stable, it not necessarily the end user need to create his own tool, rather I go look for alternative if any.

Faith Connors - August 29, 2017, 6:38 am

(Aug 29, 2017 06:36 AM)zer0dev Wrote: [\[CITE\]](#) Obviosuly, if something is not stable, it not necessarily the end user need to create his own tool, rather I go look for alternative if any.

we aren't talking about something being unstable for one user, we are talking about something that doesn't work, ever.

kde does work for 99% of people.

free crypters never work for anyone.

i dont see why you aren't seeing this