Tea-Suprem Exploit Help Document

Welcome to the TeaSuprem Exploit. This software allows you the user to “exploit” with TeamViewer to upload a payload of your choice to a scammers’ computer to do anything you can create or program. In this document I will be teaching you how to use the software and some requirements and notes.

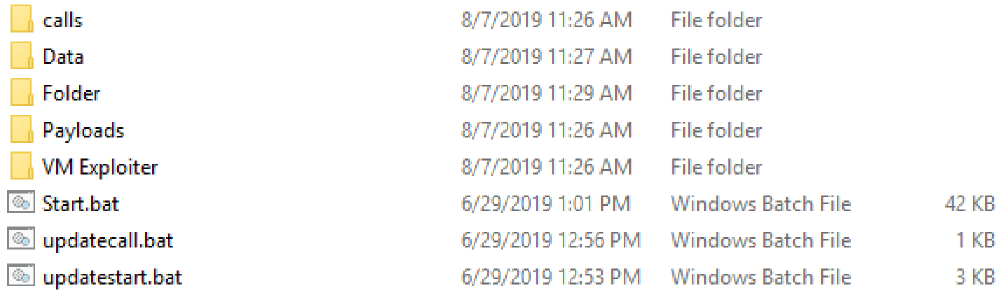
How do I get started?

Well first you need to download the Exploit from the GitHub page.

https://github.com/IWickGames/TeaSuprem-Exploit

Use the ‘Clone or download’ button and ‘Download Zip’ this will download the project onto your computer. Extract the Zip archive and navigate to the directory with the exploit.

You should end up in a folder looking something like this;



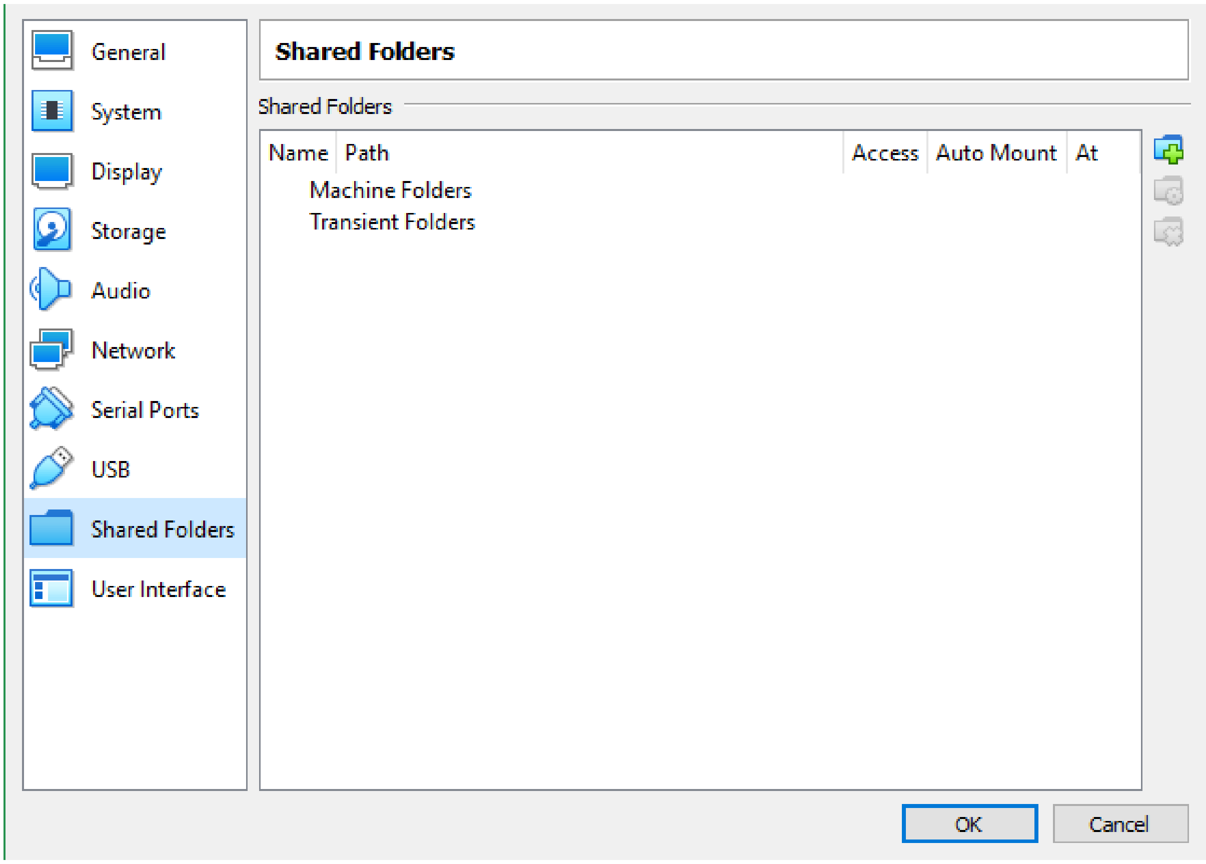
calls	8/7/2019 11:26 AM	File folder	
Data	8/7/2019 11:27 AM	File folder	
Folder	8/7/2019 11:29 AM	File folder	
Payloads	8/7/2019 11:26 AM	File folder	
VM Exploiter	8/7/2019 11:26 AM	File folder	
Start.bat	6/29/2019 1:01 PM	Windows Batch File	42 KB
updatecall.bat	6/29/2019 12:56 PM	Windows Batch File	1 KB
updatestart.bat	6/29/2019 12:53 PM	Windows Batch File	3 KB

Run the Start.bat file in that folder. Because you are running this for the first time you should see a setup prompt appear. Fill out the information, first fill in your local IP address and then the VM Shared folder name. That folder will appear in the same directory. Your setup is now complete!

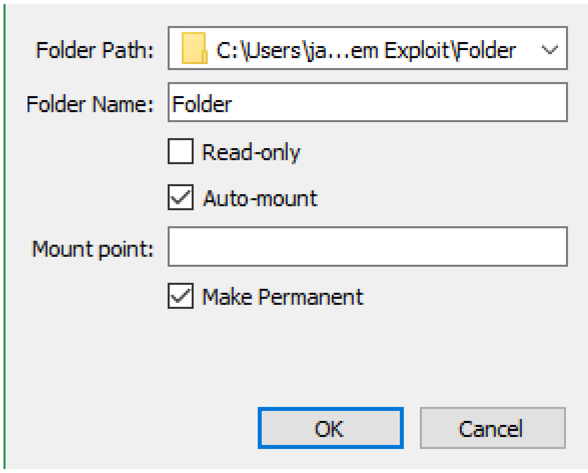
Now open your VM application or choice, I’m using Virtual Box. If you use VMware here is there help page for Shared folders.

https://www.vmware.com/support/ws5/doc/ws_running_shared_folders.html

If you use Virtual Box here is how to set it up. While running the VM make sure you have Guest Editions installed. Then on the Tabs with File, Machine, etc. Click ‘Devices’, Shared Folders, Shared Folders Settings. You should now be here;



Click the Folder with a Green Plus icon. In the Folder Path Section click the Dropdown and then click 'Other…'. Select that shared folder you have created in your Setup. This will select that folder to be shared.



Folder Path: C:\Users\ja…em Exploit\Folder

Folder Name: Folder

□ Read-only

☑ Auto-mount

Mount point:

☑ Make Permanent

Make sure Read-only is **not selected**! Same for on the Vmware. If read only is selected the TeaSuprem Exploit will not be able to talk to the Host wile in the VM. This will stop the log from working and it will be stuck on waiting for connections. Well guess what? You done! You have now setup the TeaSuprem Exploit.

Create Payloads

Now you know you can upload you own files to a scammers PC using this exploit. Open the Framework using the Start.bat and wait for the Menu to load. You will see an option called “Create Payload” on option 6. Select it by typing 6 and then pressing enter. You will then be shows all the existing payloads and also be prompted to name a new one. Type in your name and click enter, a folder will open prompting you to drag in your payload.exe file. It must be named payload.exe or the exploit will not work.

Remove Payloads

This is easy to do. Just like create payloads select 7 by typing 7 and pressing enter. You will be shows all the payloads that exist, type in the payload name and press enter and the payload will be removed.

Integrity Checks

Integrity Check make sure that your exploit package is not missing any files. Its easy to run just select 5 by typing 5 and pressing enter on your keyboard. If you see any files between the lines those are files that are missing. If this shows, download the package off the GitHub page and drag the file into its directory.

Setup

Setup allows you to change your settings after you have ran the exploit just select it by typing 2 and pressing enter. Then fill in your local IP and your VM Shared Folder name.

Reset Systems

This will reset the VM folder. This is used after you have run the exploit and attacked a scammer using it. Activate it by typing 3 and pressing enter. Then let it run.

Update

You can update the exploit by typing 9 and pressing enter. Then let the update run.

Using the Exploit

Now that you know what all of the options do I will talk about how to run and exploit a scammer. First run the VM and the Exploit with Start.bat and the VM software of your choice.

Upload the VM Exploiter folder to your VM and hide it. Make sure the scammer will never see this folder or it will giveaway what you are trying to do!

After you have uploaded the folder and hid it run the Exploit RUN.exe file and wait for the setup menu to show up this is for VM compatibility. Type in your VM folder name.

It will look like \\VBoxSvr\<YourFolderName>

/\

This is what you want

Type that into the Setup window and press enter, the program will then Hide the windows and start running in the background. The exploit is now waiting for a scammer or you to open TeamViewer and login to a computer. When they do the macro will very quickly upload your payload to their computer and run it using the Run box.

Thank you for Using the Tea-Suprem Exploit

Created by: @IWickGames#7827

Coded by: @IWickGames#7827

Discord Channel Invite Code: `w2Afaur`

Thank you and all the people in my discord channel for supporting this project and brining the Idea to life and adding your ideas to the project!

This was created just to see if it could happen and then to fight the scammer army!

Note;

I IWickGames do not take any responsibility for anything you do with this program as it allows you to select the payload you are responsible for any action you do.

Thank you!