NGEE ANN SCHOOL OF INFOCOMM TECHNOLOGY

Cyber Security Fundamentals Diploma in CSF/IT/DS/IM & CICTP Programme Year 1 (2023/24) Semester 1	Week 5 Practical
Whitespace Week Activity – Trojan Attack	

Objectives

At the end of this activity, you will be able to:

- Create a Trojan server that binds with a file.
- Distribute the Trojan to take over the control of victim's computer.

Background

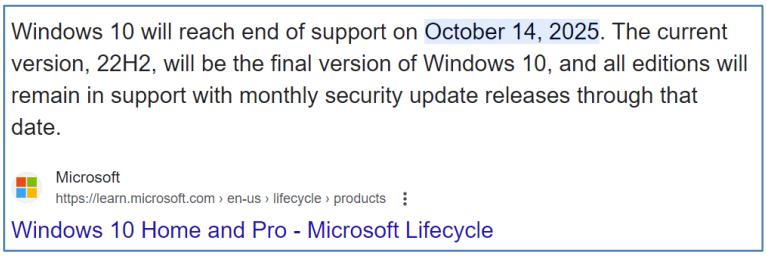
About ProRAT

ProRAT (Remote Administration Tool) is a Windows-based backdoor Trojan that is capable of allowing the victim machine (as a ProRAT client) to be remotely controlled by the attacker machine (as the ProRAT server) over a network.

In this practical, we will use the ProRat software to experience a Trojan attack.

Practical Scenario for this Trojan Attack: Unsupported Operating System at Risk

On April 27, 2023, Microsoft announced that Windows 10 will reach end of support on October 14, 2025. This means Windows 10 will no longer receive any new features, updates or patches from that day. If you want to remain supported, you will be required to upgrade to Windows 11.



If you continue to use an unsupported version of Windows after its end of life, your computer will still work, but it will become **vulnerable to security risks (e.g. malware).**

In this practical, your first task is to install a Windows 10 VM (which is not the latest version of Windows) to simulate an unsupported OS which will be vulnerable to attacks by the Win11_Attacker VM.

Complete all the tasks starting from the following pages to complete the Trojan attack.

NGEE ANN SCHOOL OF INFOCOMM TECHNOLOGY

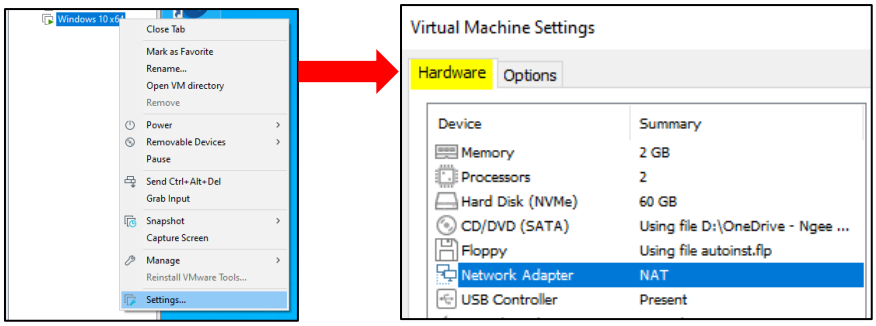
Preparation

Task 1: Install an Unpatched Windows OS (Win10_Victim VM)

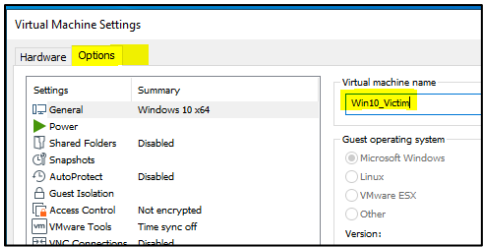
1. Download the Windows 10 image from the below link:
   Win10_21H2_English_x64.iso

2. You have learnt and experienced on how to install a Windows 11 VM during Week 2 practical. Now you may use the same approach to install a **Windows 10 Education VM.**

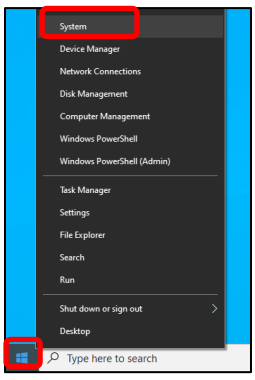
3. After you successfully installed the Windows 10 VM, edit the Virtual Machine Settings from VMware Workstaion. On Hardware tab, make sure the Network Adapter of this VM is using NAT.



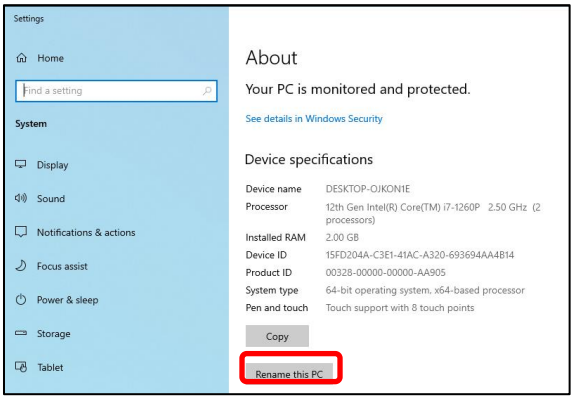
4. On Options tab, change the Virtual machine name into **Win10_Victim**.



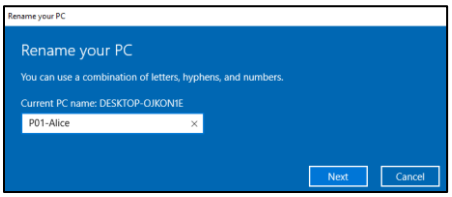
5. Power on Win10_Victim, right click the Windows icon and select System.



6. On the System Information page, select “Rename this PC”.



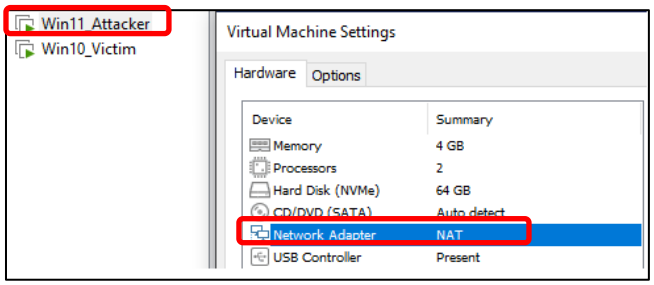
7. Rename the PC name using your CSF module group number and your name. For example, if you are from P01 and your name is Alice, name the PC as **P01-Alice**.



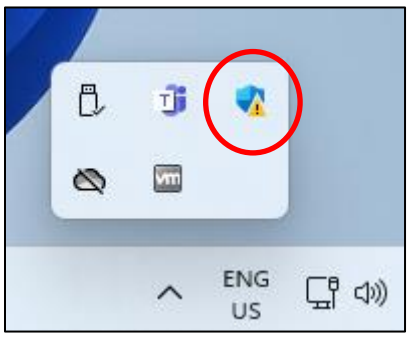
8. There will be a restart required to change to PC name.

Task 2: Prepare the Attacking Environment (Win11_Attacker VM)

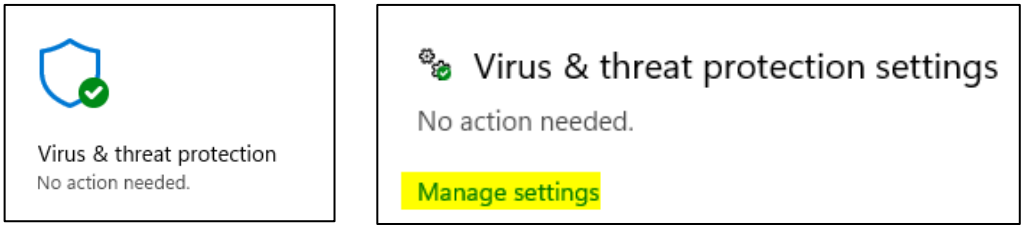
1. Make sure your Win11_Attacker created in Week 2 practical is using NAT as Network Adapter too. Power on the VM.



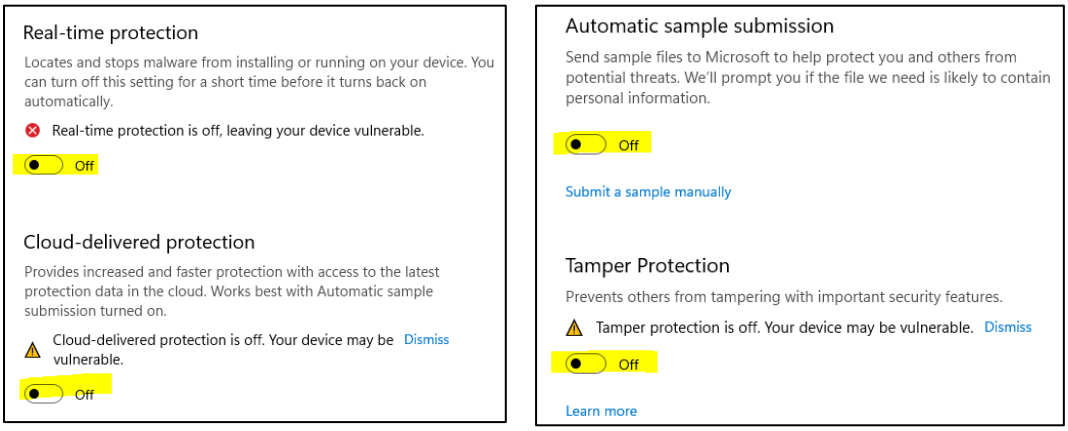
2. Login to Win11_Attacker VM and click the below icon to open the Windows Security.



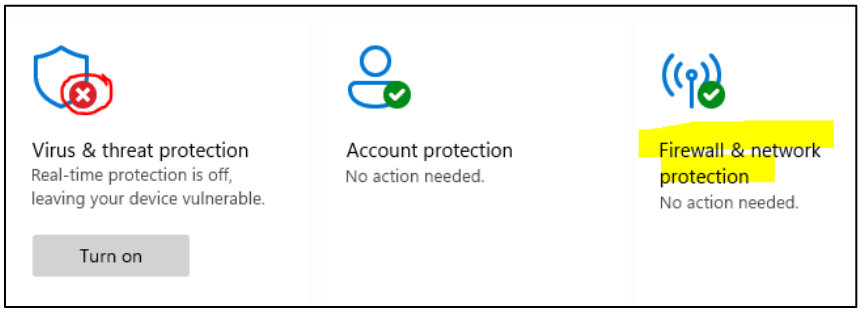
3. Click “Virus and threat protection” and select “Manage settings” under the “Virus & threat protection settings”.



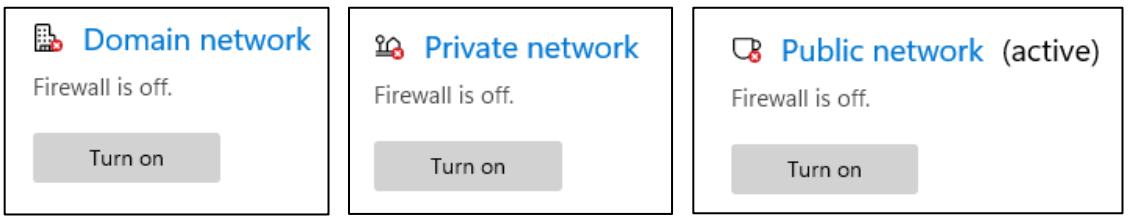
4. Turn off all the protections. **Note that the “Real-time protection” might be automatically turned on each time your re-start the VM. So remember to always check if it is OFF.**



5. Return back to the Windows Security main page, you should see the Virus & threat protection is turned off. Next, click “Firewall & network protection”.

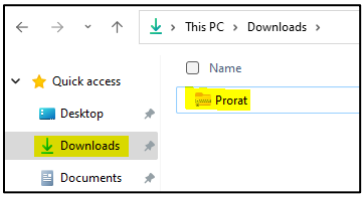


6. Click all the three networks’ firewall and turn off all. You should result in the below screen after that.

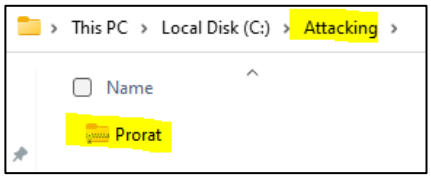


7. Using the Microsoft Edge browser from your Win11_Attacker VM to access your PoliteMall, download the Prorat.zip file.

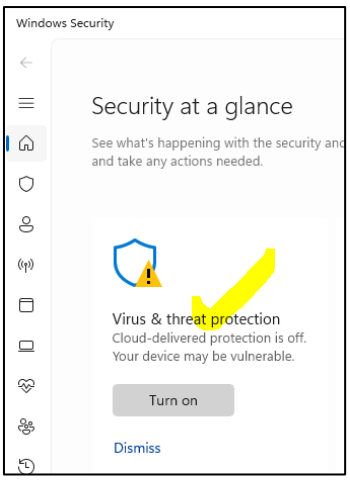
8. The Prorat.zip file should be downloaded and saved to the default “Downloads” folder as shown below.

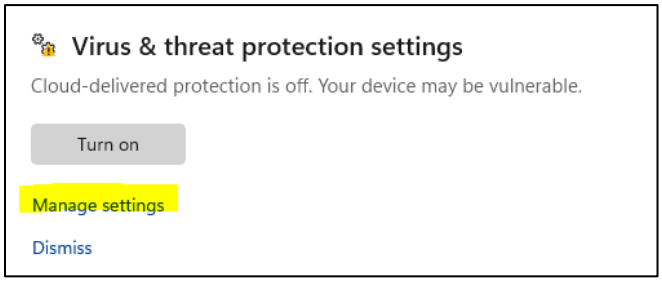


9. Create a new folder called “Attacking” in C:\ drive and move the Prorat.zip file here.

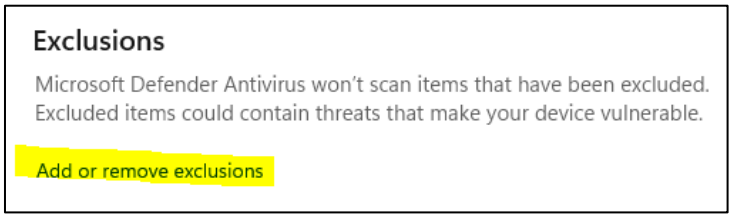


10. Click the Windows Security icon and select the Virus & threat protection. Click Manage settings.

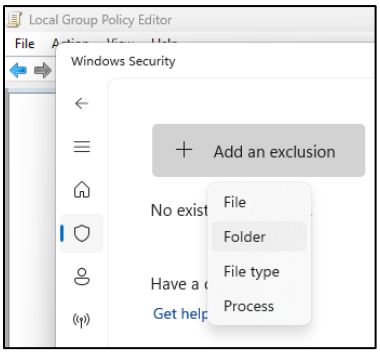




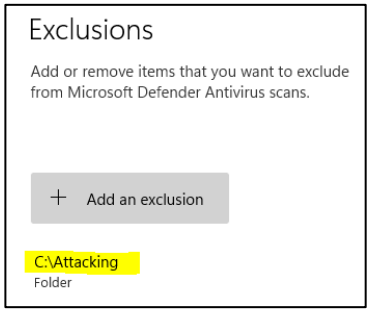
11. Scroll down to “Exclusions” and click “Add or remove exclusions”.



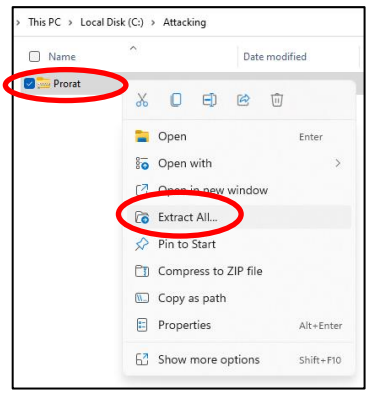
12. Click “Add an exclusion” and select “Folder”. Select the folder path C:\Attacking which you created in the previous steps.

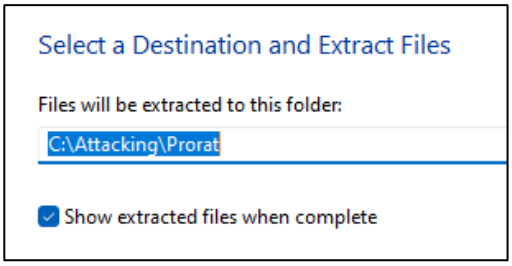


13. Make sure now you have an exclusion similar to the below.

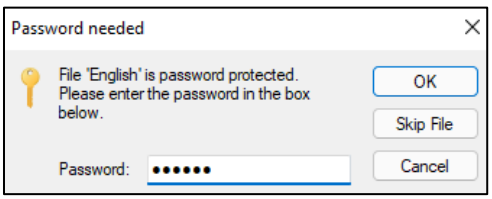


14. Right click Prorat.zip and select Extract All. You can extract to the current folder as default.

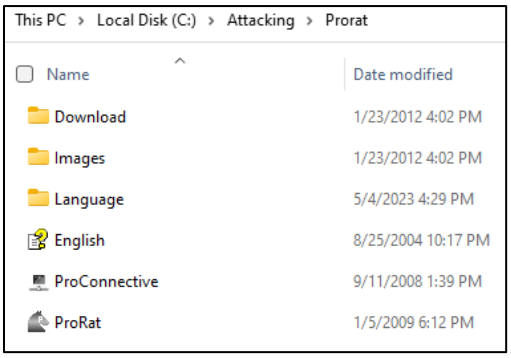




15. When promoted to enter password to extract files, type password – **csf123** then click OK.

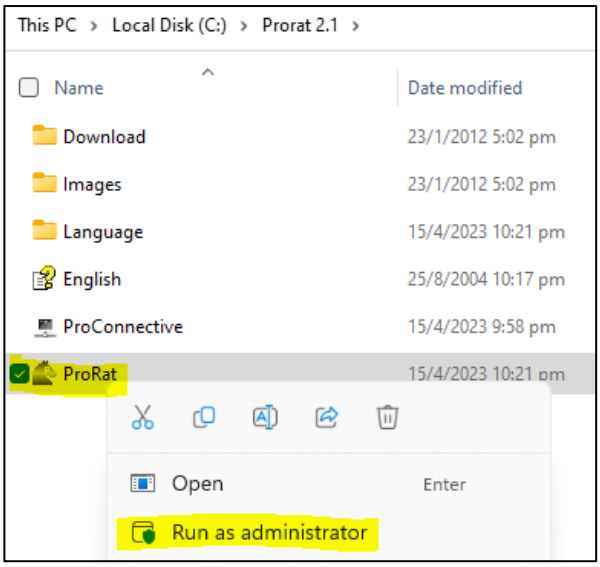


16. Make sure your extracted Prorat folder has the complete files and folders as shown below.



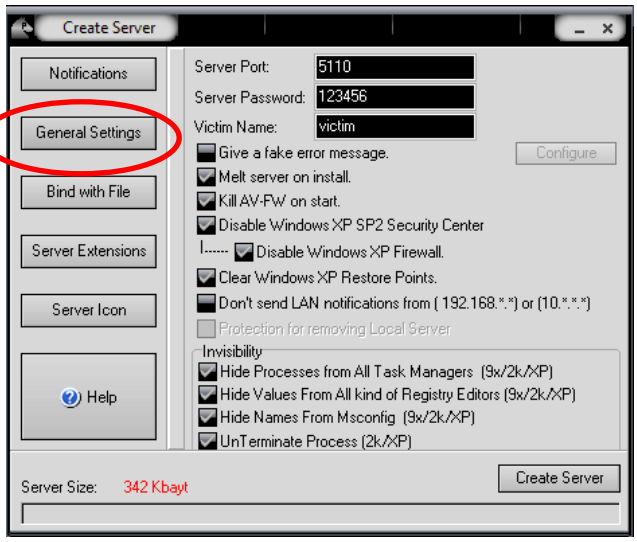
Task 3: Create the ProRAT Server

1. Right the ProRat software and select "**Run as administrator**".

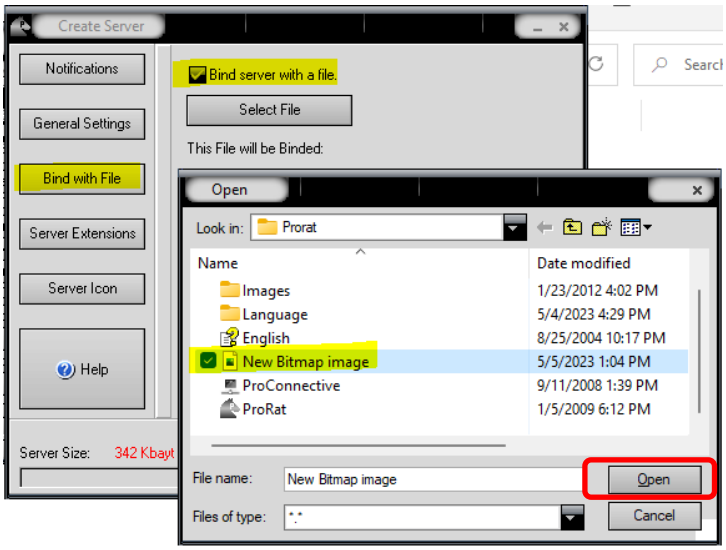


2. Click the "Create" button at the bottom. Choose "**Create ProRAT Server**".

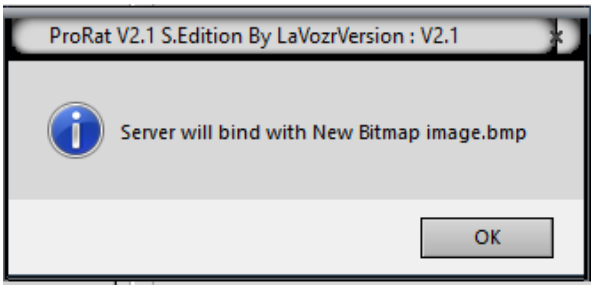
3. Select "**General Settings**". Keep default **Server Port** as **5110**. You may also use the default password 123456.



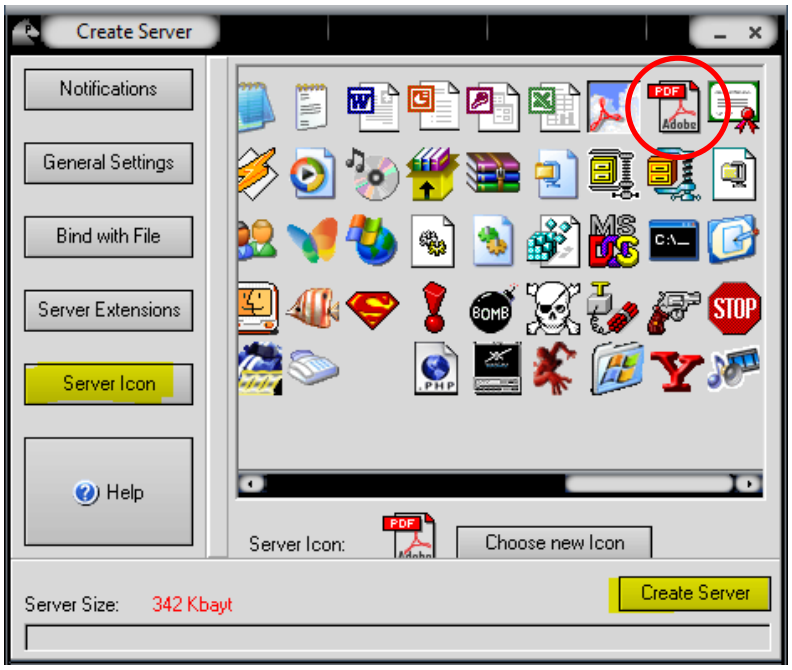
4. Click on the "**Bind with File**", prepare to select a file to bind.
   For example, you can go back to the Prorat folder and create a new file (eg. an image file), select it and click Open.



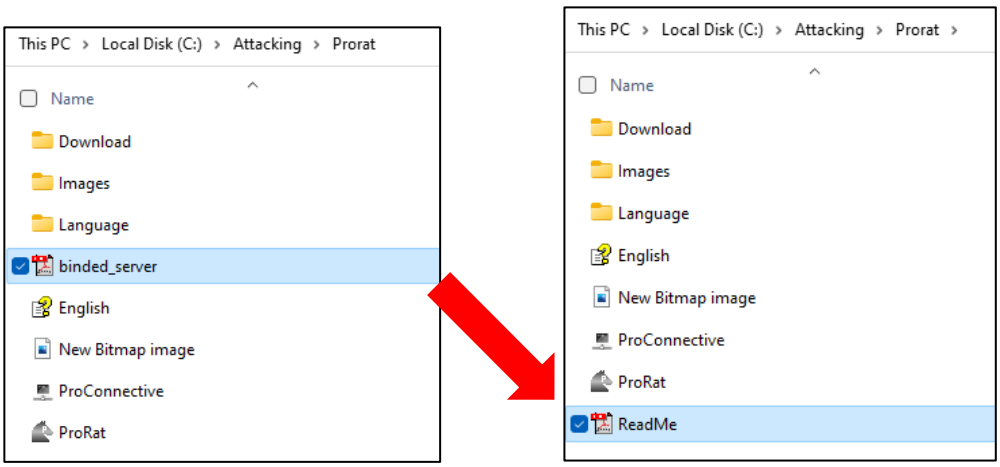
5. Click ok to complete the binding.



6. Click on the “Server Icon” and choose an icon image. (Choose a non-suspicious file icon to such as Adobe PDF to trick the victim)

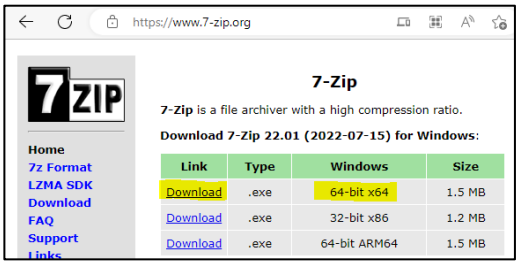


7. Click “Create Server”. The server with the name “binded-server” will be created in the same folder as ProRAT folder. Rename this file if necessary to make it less suspicious.

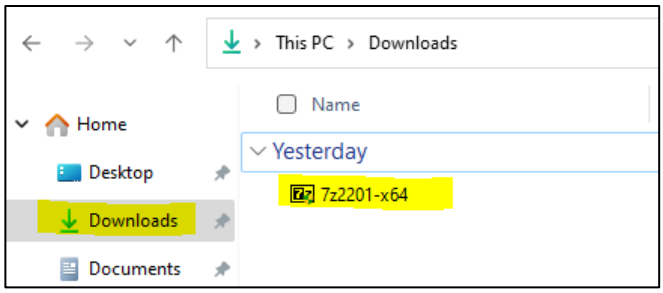


Task 4: Sending Trojan from Win11_Attacker VM to Win10_Victim VM

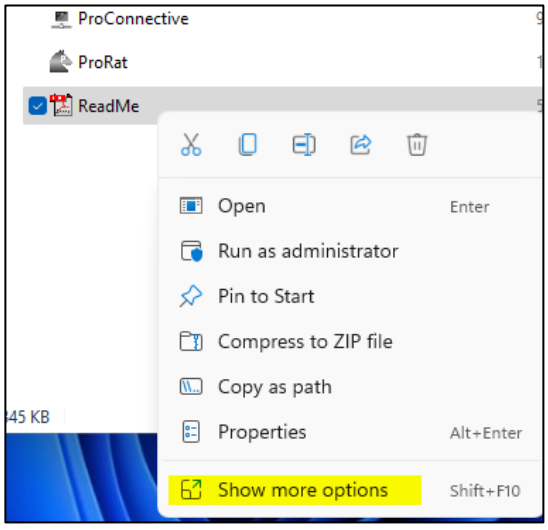
1. You have to password protect your trojan file else it will be detected quickly and removed by Victim’s OS.
2. On Win11_Attacker, open the browser and access https://www.7-zip.org/.
3. Click the first download link to download 7-Zip software installer.



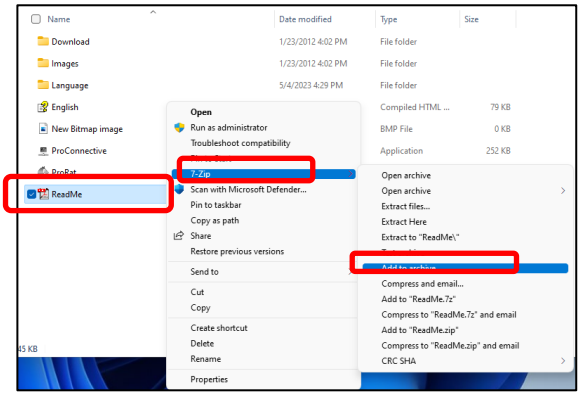
4. After download completes, find the installer from the default download folder and double click to run it. This will install the 7-Zip software to the Win11_Attacker VM.



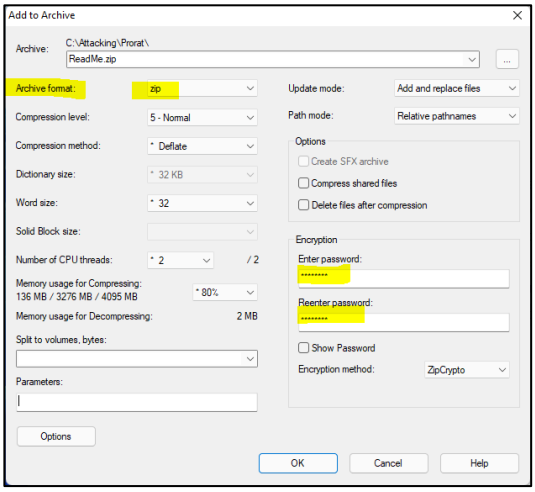
5. After installation completes, locate your trojan, right click it, and select “Show more options”.



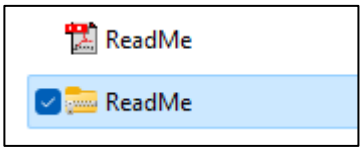
6. Select “7-zip” then “Add to Archive”.



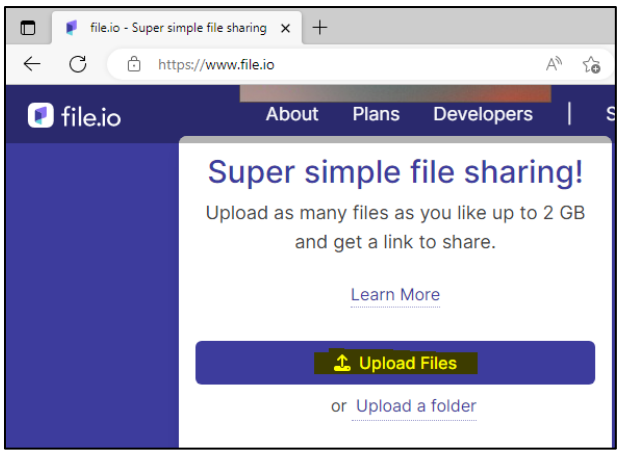
7. Select archive format as “zip” and set a strong password for encryption. Click OK.



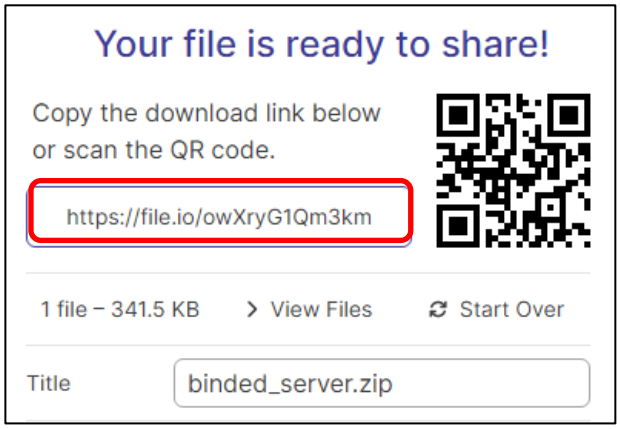
8. Your trojan is now encrypted with password, and it’s ready to be sent to the victim’s machine.



9. It’s recommended to use some online temporary file sharing services to transfer this file. For example, access https://www.file.io/ using the browser in Win11_Attacker. Select “Upload Files”.



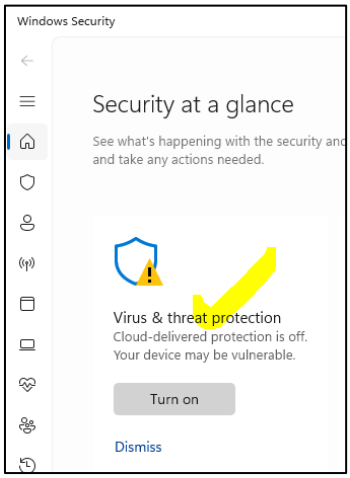
10. After uploading completes, a download link to the file is generated.

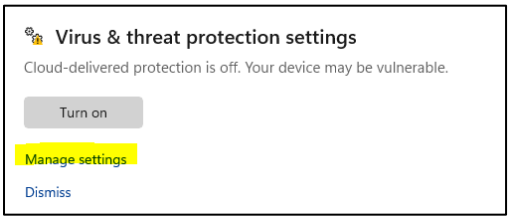


11. This link is just like any malicious link that an attacker prepared and trick the victim to download it.

Task 5: Simulate a Vulnerable Environment (Win10_Victim VM)

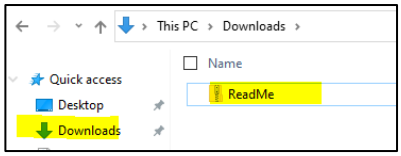
1. Switch to Win10_Victim VM which you have just installed, click the Windows Security icon and then select the Virus & threat protection. Click Manage settings.



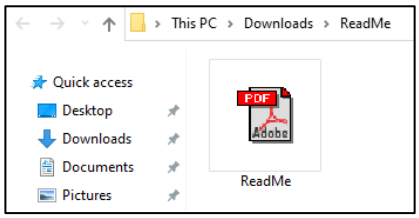


2. Make sure all the 4 protections are turned off:
   - Real-time protection
   - Cloud-delivered protection
   - Automatic sample submission
   - Tamper Protection

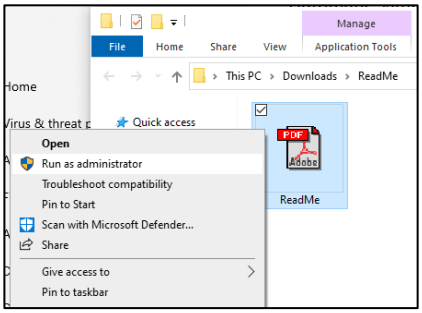
3. Open the browser, access the download link you just generated. Download the file.



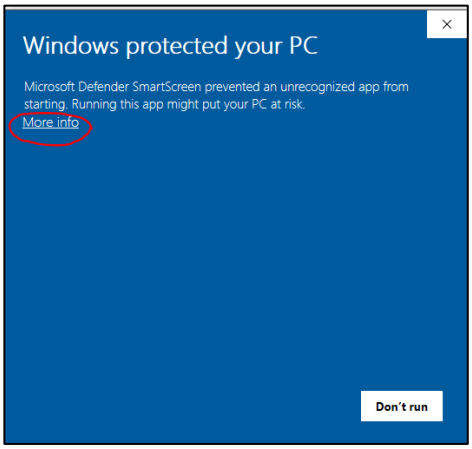
4. Right click the zip file and select “Extract All”, use the default folder path to extract, and key in the password you set previously.



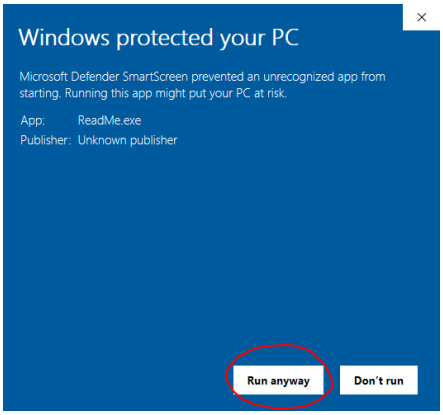
5. Right click the extracted file and select “RUN as administrator”.



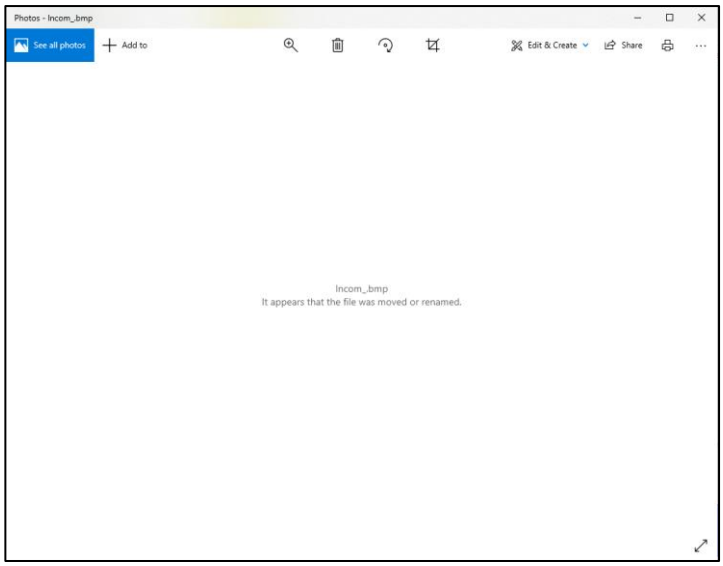
6. There will be a warning pop-up because your OS detects something malicious. Click “More info” to proceed.



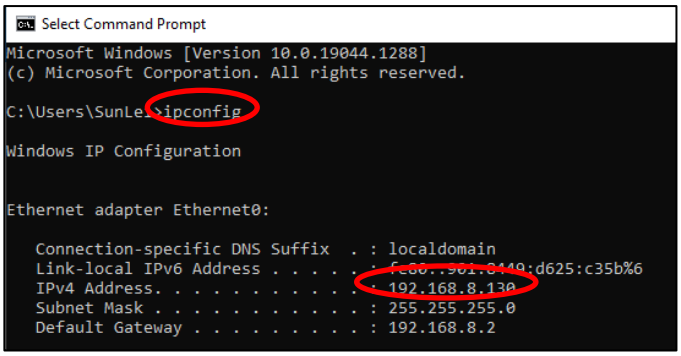
7. Now you are able to click “Run anyway”.



8. An empty image file is opened, **leave it open**. This will create a backdoor for attacker to remotely control the victim if the attacker knows the victim machine's IP address.



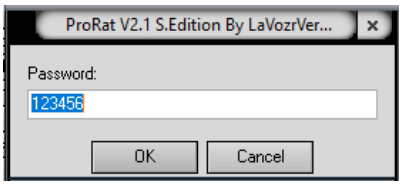
9. At victim's machine, from the Search toolbar, type **cmd** to open the command prompt and type "ipconfig" to check the IPv4 address. Do take note that everyone's VM may have a different IP address. **Take note of your own victim's IP address.**



NGEE ANN SCHOOL OF INFOCOMM TECHNOLOGY

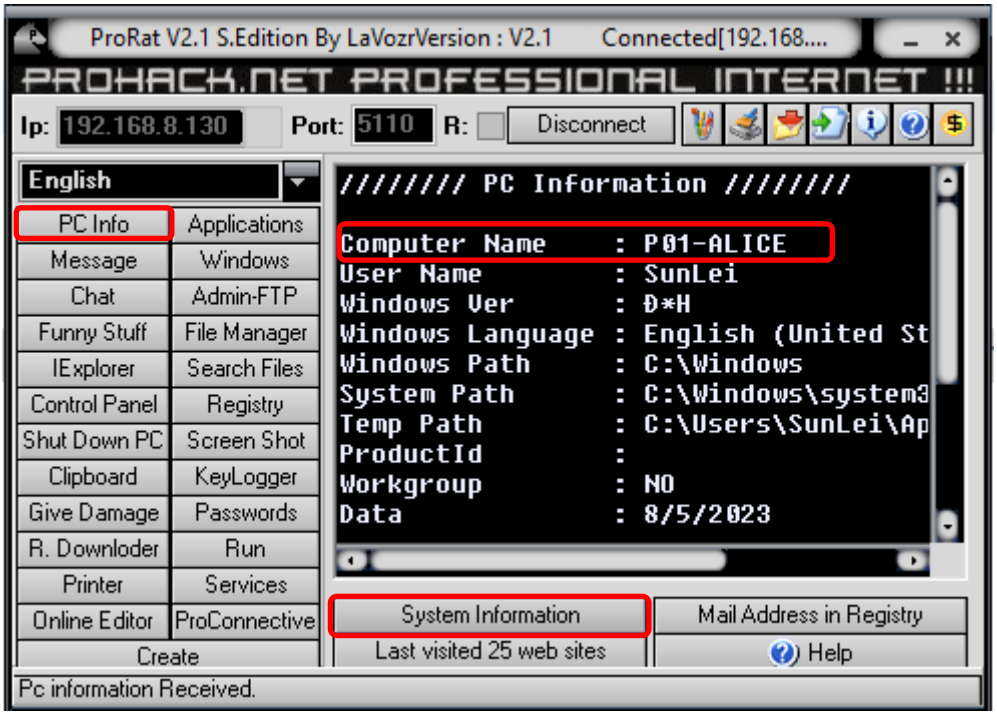
Task 6: Lauch the Trojan Attack (on Win11_Attacker VM)

1. Type in the IP address of the victim's machine at the attacker's ProRAT interface. Do not change the port number.
2. Click "Connect". The password should be the initial password 123456 if you have not changed it in Task 3 – Step 3.

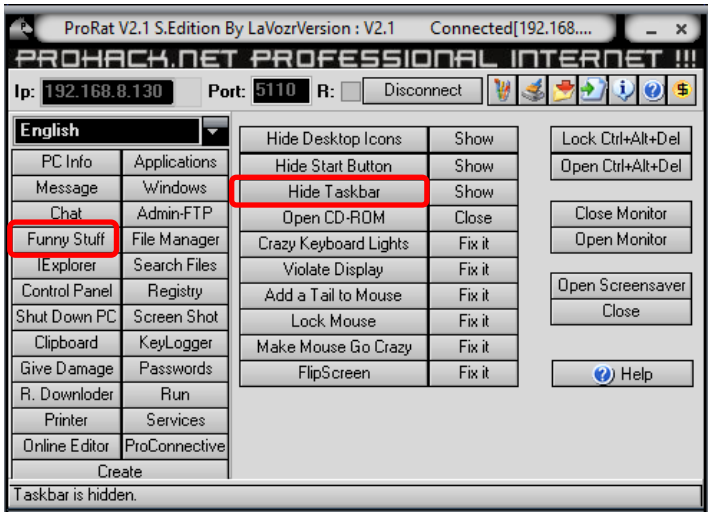


3. The status changed to "Connected" and now you have established a remote connection to the victim.

4. Click “PC Info” followed by “System Information”. The computer name of the victim VM should be displayed and you should have already changed it according to your group and name. Take a screenshot of it and submit it to PoliteMall as an evidence to complete this practical.



5. You can also explore some of the available functions to control the victim machine. Such as selecting “Funny Stuff” and then hide the victim machine’s taskbar and etc.



Important: DO NOT try the “Give Damage” function, as it may re-format the victim machine. You may not be able to use is anymore.

6. You have successfully launched a trojan attack!
7. Do complete the two reflection questions and submit the screenshot evidence on PoliteMall.

== The End ==