|  |  |
| --- | --- |
| **Cyber Security Fundamentals**  Diploma in CSF/IT/DS/IM & CICTP Programme  Year 1 (2021/22) 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 bind with a file,
  + Distribute the Trojan to take over the control of victim’s (server) computer.

**Activity:**

ProRAT (Remote Administration Tool), is a Microsoft Windows based backdoor Trojans horse. ProRat uses a client and server to operate and opens a port on the computer which allows the client to perform numerous operations on the machine that is being controlled.

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

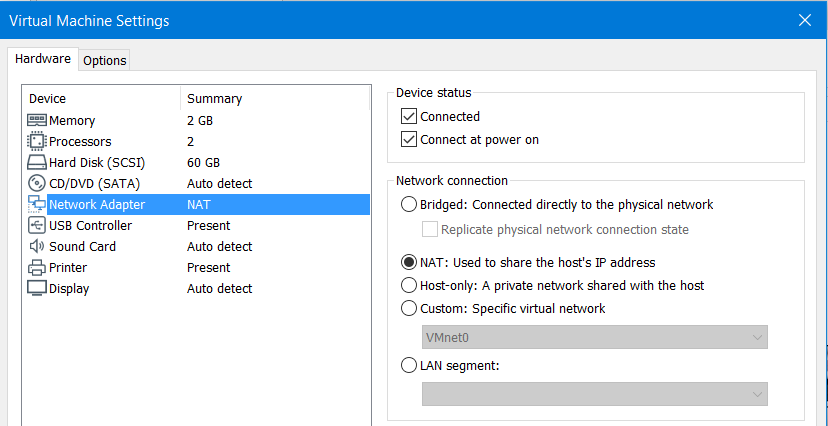
**Instructions**

* Make sure you have completed the Week 2 practical and now you have TWO Windows 10 Virtual Machines.
* ONE Windows 10 VM will be used as attacker and the other ONE used as victim.
* During the practical, you need to frequently toggle between the two VMs, remember clearly which is your attacker VM and which is your victim VM.

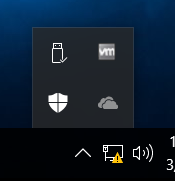
**Preparation Steps:**

**Note: The below steps need to be performed on both Windows 10 VMs.**

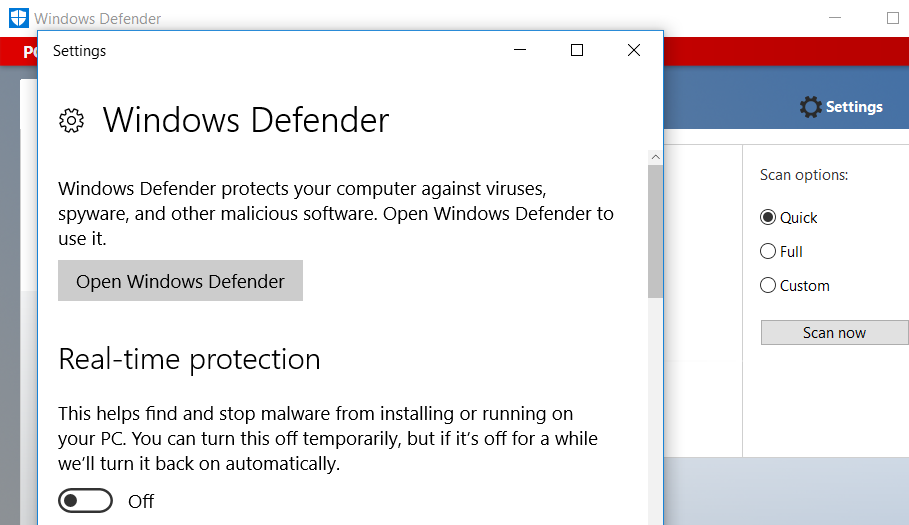
1. Before starting, you can take a snapshot for each VM and name as “Before Week 4 Practical”. So that you can always revert back to this state and re-do the practical.
2. From your VMware Workstation, right click **both** of your Windows 10 VMs and select **Settings**.
3. Select the **Network Adapter** and ensure the Network Connection is “**NAT**”.



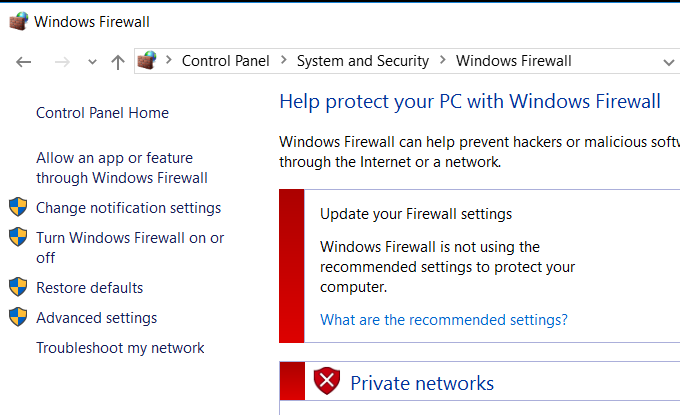
1. Login to both Windows 10 VM and open the Windows Defender.



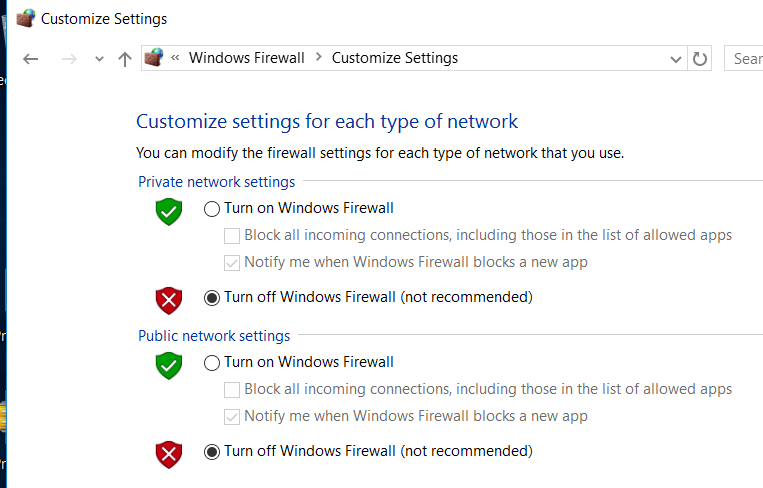
1. On the Windows Defender, click Settings. Then turn off the Real-time protection.



1. Next, go to Control Panel \ System and Security \ Windows Firewall.
2. Select **Turn Windows Firewall on or off**.



1. Ensure your Windows Firewall is turned off.



1. Download the “7z Installer.ex” from CSF Week 2 folder in MeL website into both of your virtual machines. Rename the file into “7z Installer.exe” and run it to installed on both VMs. This is for you to zip or unzip a file later.

**Note: You need to repeat the above steps on both Windows 10 VMs.**

# Task 1: Installing ProRAT Trojan (only on Attacker’s computer)

Step 1: Download proRAT.zip file from MeL\CSF Module\Week5.

Step 2: Unzip using password **2020csf** and run the “ProRat” software.

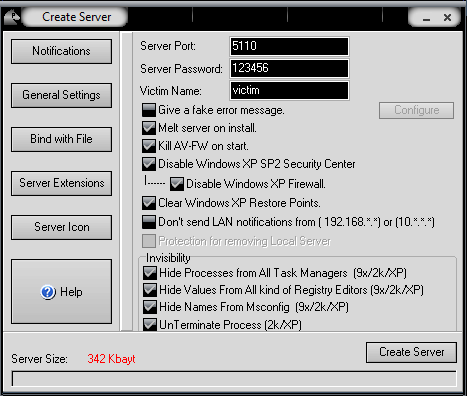
# Task 2: Create the ProRAT Server

Step 1: Click the “Create” button at the bottom. Choose “Create ProRAT Server”.

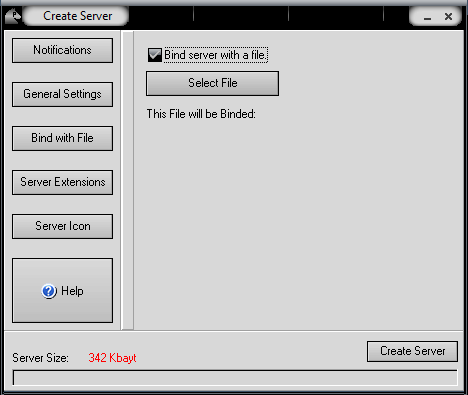




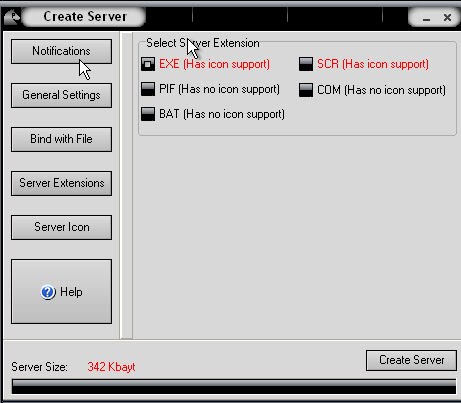
Step 2: Select “General Settings”. Leave the port number as 5110. Take note of the password, you will need it later.



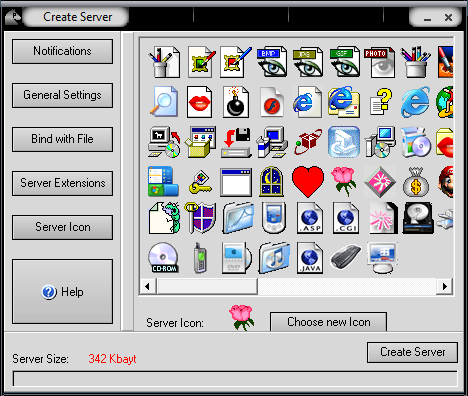
Step 3: Click on the “Bind server with a file”, then select a file to bind. You can create a new image or text file and then bind to it.

****

Step 4: Select “Server Extensions” and choose EXE which is the default.



Step 6: Click on the “Server Icon” and choose an icon image. (Choose a non-suspicious file icon, e.g. Word, PDF, etc.).



Step 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 3: Sending Trojan to Victim

Step 1: You have to password protect this “binded-server” file else it will be detected as Trojan and blocked.

Right click the file, select “7-zip” then “Add to Archive”. Enter password as “ZIP” and check “Encrypt File names”.

Step 2: Find your own ways to pass this file from the attacker’s machine to the victim’s machine.

1. You can do so by sending the file as an email attachment from the attacker’s machine, receive and download it from the victim’s machine.

Note: Some email service provider may detect trojan and delete your email.

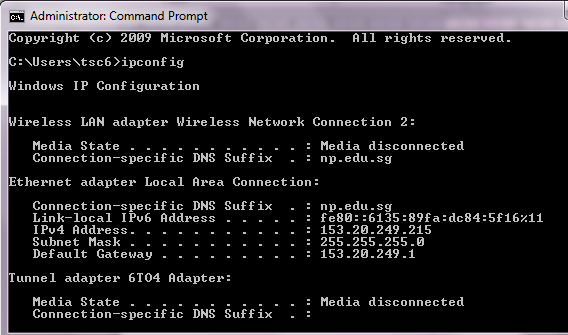
1. You can also drag this file from the attacker’s machine to the host machine, and then drag the file from host machine to the victim’s machine.
2. You may also put this file inside a thumb-drive, and from your VM, detect this thumb-drive then copy the file out.

Step 3: Once this zip file is inside the victim’s machine, unzip it using ZIP password.

Step 4: **Right click the unzipped file and select “RUN as administrator”.**

# Task 4: Connecting to Victim’s Machine

Step 1: At victim’s machine, from the Search toolbar, type **cmd** to start ***command prompt*** and type “**ipconfig**” to check the IPv4 address.



Step 2: Type in the IP address of the victim’s machine at the attacker’s ProRAT interface. Do not change the port number.

Click “Connect”.

If you cannot connect successfully, it is probably because victim’s Windows Firewall is still turned ON. Remember to turn it off.



Step 4: Attacker will be prompted the password. Enter the password you used to create the Trojan server in Task 2 Step 2, e.g. *123456*.

Step 5: Client now has full control of the infected victim’s machine. Try functions such as “Chat” and “Message” etc.

**Important: DO NOT try the “Give Damage” function, as it may damage the PC by formatting.**

- The End -