Why?

Trojan and backdoor scripts are common attacks. Once on a computer they are virtually impossible to remove. It is possible to wipe the system but then all data is lost and there is a chance the backdoor is still there. To mitigate the attack, one should disconnect all types of internet to prevent further exploitation of the machine.

Steps to set up environment:

1. Step by step of how you set up the environment

Server:

1. In the Server Manager, go to the Dashboard section.

2. Select Add roles and features.

a. Select Role-based or feature-based installation.

b. Select your server in the list.

c. Select Active Directory Domain Services.

d. Click through until you start the installation and then keep the wizard open as it installs everything.

3. Click the link to Promote this server to a domain controller.

4. Go through the AD DS Installation Wizard:

a. Select Add a new forest.

b. Set the Root domain name to be: comp3550.private

c. For the Forest functional level and Domain functional level, choose Windows Server 2012 R2 or Windows Server 2016, depending on which version of Windows Server you’re using.

d. Choose a password for the Directory Services Restore Mode account.

e. Ignore the warning about DNS delegation.

f. Don't change the NetBIOS domain name.

g. Select the default locations for the various folders

h. After it runs prerequisite checks, click Install.

5. After installation is complete (takes ~5 minutes) the server will reboot.

1. Step by step of how you conducted the attack. Elaborate on all the numbers you see during the attack (network traffic, etc)

* The script pulls information from libraries and creates a connection to the network
* Once connected to the network, the attack script then obtains the client IP address and connects. Once connected, the attack begins
* Make sure python command is working
* Run the script and follow on screen instructions

Mitigation Techniques

So the first thing we need to do is identify what type of trojan horse we are dealing with. In our case it is a backdoor trojan. This type of Trojan allows hackers to remotely access and control a computer, often for the purpose of uploading, downloading, or executing files at will.

With backdoor/trojan horse virus’ there are a few pre-emptive things a user can do to avoid having their device infiltrated by one. These are some pretty standard security methods.

* Never download or install software from a source you do not completely trust.
* Never open an attachment or run a program sent to you in an email you are not expecting, especially if you do not know the sender
* Keep all software on your computer up to date with the latest version.
* Make sure a Trojan antivirus is installed and running on your computer

Now if it is already too late and the trojan horse / backdoor hack has made its way into your computer then here is what you will need to do.

1. Install antivirus software on the computer if it is not already installed.
2. Update the virus definitions of the antivirus software.
3. Disconnect the computer from the internet once the definition update is complete.
4. Reboot the computer.
5. Run a full system scan using the newly installed antivirus software and wait.
6. Run a second full system scan with your antivirus software as soon as the first one completes. This is important to make sure nothing was missed the first time around.
7. Perform a system restore
8. Click the “Start” button.
9. Select “All Programs” folder.
10. Click “Accessories” folder.
11. Click “System Tools” folder.
12. Click “System Restore”.
13. Select “Restore my computer to an earlier time.”
14. From here you will select the time that best fits your needs, ensure that this selection is a time before the device became infected.

8. Reconnect your computer to the internet.