Homework 8: Linux Rootkits

Learn how to find Linux rootkits on the Internet and use a rootkit-checking program.

1. Going to PacketStormSecurity.org

First, I opened my browser, went to the Packet Storm Security website, and searched for LRK5 in the search bar. After hitting enter, I found some results, and among them was Linux Rootkit 5 as mentioned in iA screenshot of a computer

Description automatically generated

2. Listing Five Trojaned Linux Commands

When I checked out the description for Linux Rootkit 5, I saw that some common Linux commands get infected (Trojaned) when this rootkit is used. Five of the Trojaned commands are:

* ls – which lists files and directories
* ps – shows running processes
* netstat – displays network connections
* ifconfig – shows network interface settings
* login – for user login

A screenshot of a computer

Description automatically generated

These are commands that hackers alter to hide what they’re doing on the system.

3. Running the Terminal Commands

Next, I opened the Terminal in Kali Linux and typed these commands:

sudo apt update

sudo apt-get install chkrootkit

sudo chkrootkitA screenshot of a computer

Description automatically generated

A computer screen shot of a dragon

Description automatically generatedA computer screen shot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

This installed and ran a tool called chkrootkit, which checks for rootkits (like LRK5) on the system.

4. Comparing the Commands

After the chkrootkit scan finished, I checked the results to see if any of the commands I listed earlier (ls, ps, ifconfig, login and netstat) were flagged. Thankfully, none of them were listed as infected, which is a good sign that the system is clean.

5. What chkrootkit Does

The chkrootkit tool scans your system for rootkits by checking if any system files have been replaced with fake ones. It looks for rootkits, worms, or suspicious files. If it finds something bad, it will list it. In my case, it didn't find any rootkits, but there were a few warnings about suspicious files, and they should be checked out to make sure the system is safe.

This tool helps figure out if hackers have infected your system by hiding dangerous software, and the scan results show if there's anything to worry about.

A screenshot of a computer

Description automatically generated

The warning about a packet sniffer in chkrootkit might be related to Wireshark if you're using it for network analysis, as in mycase. Wireshark often puts the network interface into promiscuous mode to capture all network traffic. This mode allows Wireshark to see packets intended for other devices on the network.

The wted warning is part of the chkrootkit tool, and while it doesn't automatically mean there's an issue, it’s still a good idea to check further. It might indicate hidden processes or tampered logs, so verifying system integrity is important.

The chkwtmp warning flagged two deletions in the log between October 6, 06:55:50 and 06:57:12, but in this case, I know it was me. This shows that the tool is doing its job by detecting any changes.