Rootkit Scans

A rootkit is a collection of software tools that enable an attacker to gain root or administrative-level access to a computer or network and maintain this access covertly.

==========

chkrootkit

`chkrootkit` (Check Rootkit) is an open-source security tool used to detect rootkits and other malicious software on Linux systems.

To use chkrootkit, you'll need to install the `chkrootkit` package.

Running `chkrootkit`

To perform a basic scan, you simply run:

```
chkrootkit
```

Additional Options

-v	verbose output
-r /path/to/scan	Specify a specific path to scan
-q	suppress warnings
> /path/to/log	Specify log file for output

==========

RKHunter

`rkhunter` (Rootkit Hunter) is another popular open-source security tool designed to detect rootkits, backdoors, and other possible signs of compromise on Linux systems.

To use rkhunter, you'll need to install the `rkhunter` package.

Running rkhunter

A basic rootkit scan can be run using the below:

```
rkhunter --check
```

Additional Options

--update	Update rkhunter's database of known rootkits
--verbose	Verbose output
--logfile /path/to/log	Specify a log file for rkunter output

Understanding the Output

The output of `rkhunter` includes various sections and categories:

- **[OK]**: Indicates that the item being checked is within expected parameters.
- **[Warning]**: Highlights potential security issues or suspicious findings that should be investigated further.
- **[Suspicious]**: Flags items that may require attention due to unusual or unexpected behavior.
- **[Not Found]**: Indicates that an expected file or configuration item was not found.

---

rkhunter baseline

rkhunter includes the ability to create a 'baseline'. This essentially means that a scan of the system is run, and then future scans will compare against the existing baseline for any changes.

> If you suspect your system is compromised or infected with malware (including rootkits), refrain from using `rkhunter --propupd`. Running this command in such cases can potentially embed the infection into the baseline, compromising `rkhunter`'s ability to accurately detect the malware.

Create a baseline

```
rkhunter --propupd
```

```
================================================================================
```

Revision #2
Created 2024-06-30 12:49:16 UTC by Daniel
Updated 2024-06-30 13:47:01 UTC by Daniel