What is a rootkit?

A rootkit is malware whose purpose is to hide the attacker's presence, files, processes, network connections, and other malware, by tampering with the operating system's own view of itself. It can live in user space (hooking libraries, for example via `LD_PRELOAD`) or in kernel space (a malicious driver or kernel module that intercepts system calls), with the deepest in firmware or a bootkit. Because it subverts the tools you would use to detect it, a kernel rootkit often requires offline or out-of-band detection. It maps to MITRE T1014.

HOW IT WORKS

01 How rootkits work

A rootkit intercepts the calls used to enumerate the system and filters out the attacker's artifacts:

- User-mode: a malicious library loaded via `/etc/ld.so.preload` or `LD_PRELOAD` hooks functions like `readdir` so the attacker's files and processes are omitted.
- Kernel-mode: a loadable kernel module (or Windows driver) hooks syscalls/`ps`/`netstat` paths to hide PIDs, files, and connections, and to give the attacker covert control.
- Bootkit/firmware: loads before the OS, surviving reinstalls.

Installing one needs root/SYSTEM. Documented for defensive context.

> IT HIDES FROM YOUR TOOLS
>
> *A rootkit's danger is that it subverts the very tools you would use to find it,* `ps`, `ls`, `netstat`, *even EDR. Kernel rootkits often need out-of-band detection: a clean boot, memory forensics, or comparison from outside the running OS.*

HOW TO DEFEND

- Prevent the root/SYSTEM compromise a rootkit needs to install, this is the real defense.
- Use Secure Boot, signed drivers/modules, and kernel integrity protections so unsigned kernel code cannot load.
- Detect out-of-band: memory forensics, offline disk analysis, and comparing system state from outside the running OS.
- File integrity monitoring and baselining to spot tampering.
- Rebuild from known-good media when a kernel/firmware rootkit is suspected, cleaning in place is unreliable.

SOURCES

[1] MITRE ATT&CK: Rootkit (T1014)

[2] NIST SP 800-83 Malware Incident Prevention and Handling

[3] MITRE ATT&CK: Persistence (TA0003)

Find the backdoors an attacker would leave behind.
securelayer7.net/learn/persistence/what-is-a-rootkit

Open online