# Rootkits

- A rootkit is a collection of malicious computer software designed to enable access to a computer that is not otherwise allowed.
- After a successful intrusion into a system, usually the intruder will install a so-called "rootkit" to secure further access.
- Rootkit detection is difficult because a rootkit may be able to subvert the software that is intended to find it (rootkit scanners, antivirus).
- **NEVER TRUST A COMPROMISED MACHINE. PERIOD**

**Rootkit Scanners:**

**1. Rootkit Hunter (rkhunter)**

```
rkhunter --check
```

**2. chkrootkit**

```
chkrootkit -q
```