

2.5 Linux rootkits

- ▶ **root** (high privilege access) **kit** (set of utilities)
- ▶ File integrity tools
 - AIDE, Samhain and Tripwire
- ▶ Rootkit scanners
 - Rootkit Hunter and Chkrootkit

AIDE

- ▶ Advanced Intrusion Detection Environment.
- File and directory integrity checker.
- /etc/aide.conf

Demo #1



Thank You!