Intrusion Detection/Prevention Systems

- Host-based Intrusion Detection Systems (IDS)
- Host-based Intrusion Prevention systems (IPS)

✓ Based on signatures (well known programs)

✓ Based on behaviors (unknown programs)

➡ Example : Syslog and Systrace on Linux

◉ Vulnerable to malicious programs residing in the kernel called "rootkits"

Os security features

- **Ubuntu Linux**
  https://wiki.ubuntu.com/Security/Features

- **Windows 7**
  http://resources.infosecinstitute.com/windows-7-security-features/

- **OS X**
  https://www.apple.com/osx/what-is/security.html