

Confined execution environment - Sandbox

A sandbox is tightly-controlled set of resources for untrusted programs to run in

- ➔ Sandboxing servers - virtual machines
- ➔ Sandboxing programs
 - Chroot and AppArmor in Linux
 - Sandbox in MacOS Lion
 - Metro App Sandboxing in Windows 8
- ➔ Sandboxing applets - Java and Flash in web browsers

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”