

OSSEC-HIDS

***(Open Source – Host-based
Intrusion Detection System)***

Daniel B. Cid (daniel.cid@gmail.com)
Ahmet Ozturk (oahmet@metu.edu.tr)

May 12th, 2006
5th Linux and Free Software Festival
Ankara / Turkey

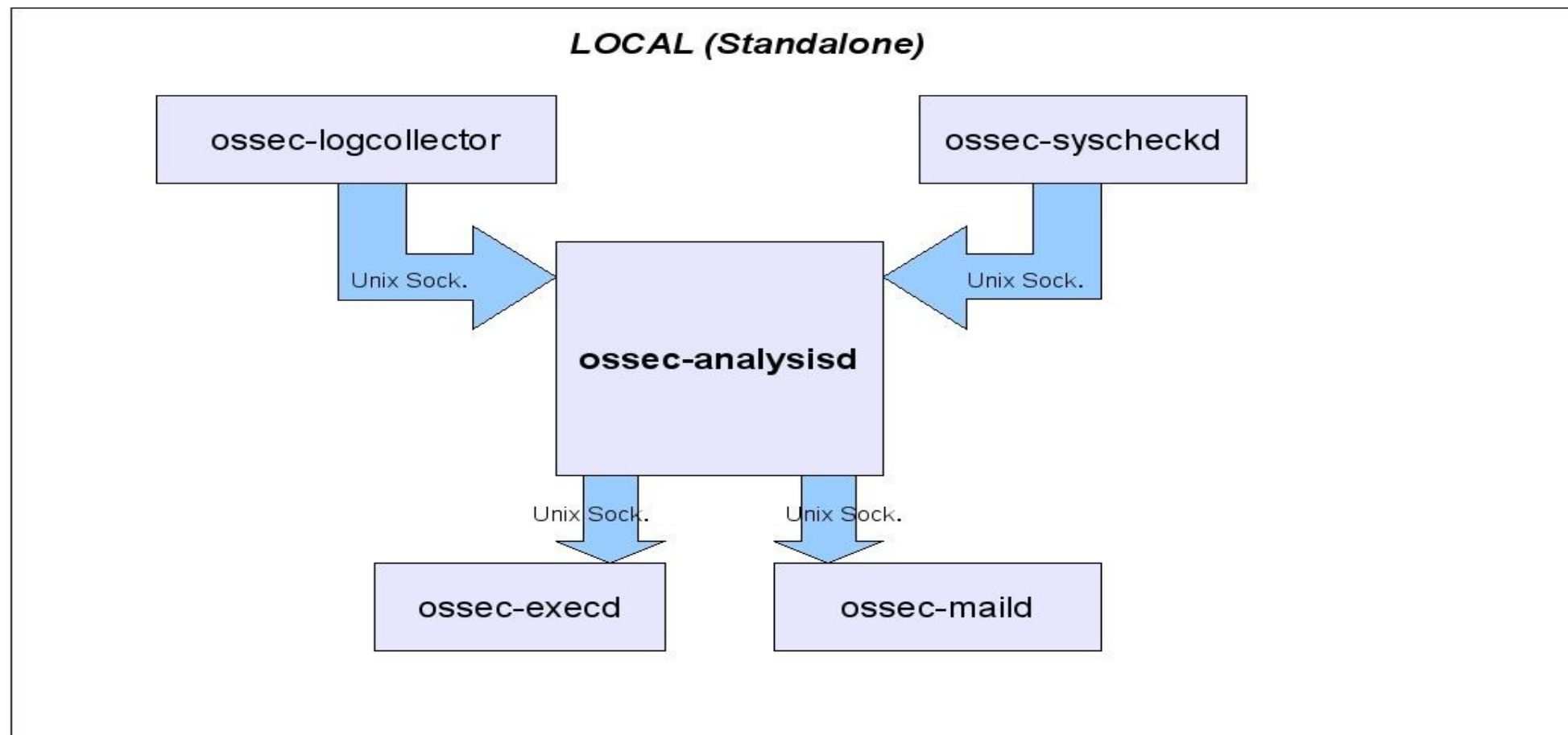
Agenda

- Capabilities
- OSSEC-HIDS Architecture
- Demo Installation
- Future Plans
- Questions

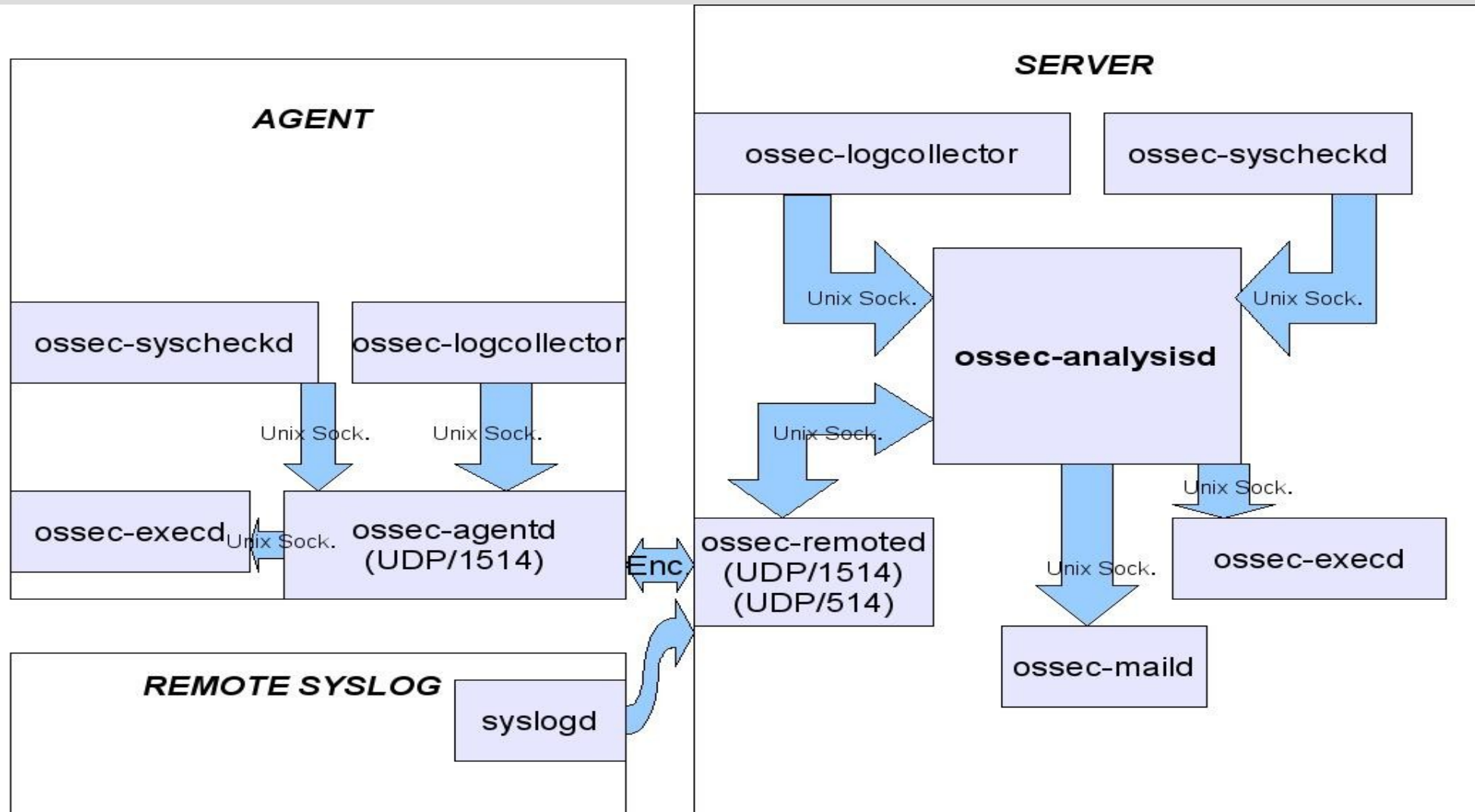
Capabilities

- Rootkit Detection
- System Integrity Checks
- Log Analysis and Alert Generation (Apache, Sendmail, Postfix, Squid, Proftpd, Bind, OpenSSH, Cisco-pix etc.)
- Active-responses (IP and user based)
- Local (standalone) and Server-Agent working models

OSSEC-HIDS Architecture - I



OSSEC-HIDS Architecture - II



Daemons - I

ossec-syscheckd

- **syscheck**
 - Monitor file changes
 - md5sum
 - date
 - file ownership
 - file permissions
- **rootcheck**
 - Rootkit / Trojan detections (signature and anomaly based)
 - Process controls
 - Port controls

Daemons - II

ossec-logcollector

- Supported Log Formats:
 - Syslog
 - Apache
 - Squid
 - Snort-full / Snort-fast
 - Windows Eventlog / IIS Log

Daemons - III

ossec-agentd

- Event forwarding
- Periodical notification to server
- Encrypted traffic between Server-Agent (symmetric keys)

Daemons - IV

ossec-remoted

- Active-response forwarding
- Encrypted traffic between Server-Agent (symmetric keys)
- Receive remote syslog messages

Daemons - V

ossec-analysisd

- Configuration / Rules & Decoders
- Monitoring Logs
- Deciding active-responses
- Generation alerts / Logging
- Decide to send e-mail the generated alerts

Daemons - VI

ossec-execd

- Applying and checking of generated active-responses
 - firewall-drop
 - iptables
 - ipfilter
 - ipfw
 - aix-ipsec
 - host-deny
 - disable-account

Daemons - VII

ossec-maild

- Reporting generated alerts via e-mail

Demo Installation

- Installation
- Configuration and rule files
- Generating sample alerts

Future Plans

- Prepare an user interface
- More documentation
- Generate more rules and support more applications
- Generate an active-response for e-mail systems

Thanks ...
Questions ?

(<http://www.ossec.net>)