Host-based intrusion detection with OSSEC

Bastian Neuburger, b.neuburger@gsi.de

02 May 2011

Agenda

Agenda

- Short overview about intrusion detection

Agenda

- Short overview about intrusion detection
- Introduction to OSSEC

Agenda

- Short overview about intrusion detection
- Introduction to OSSEC
- Examples

Intrusion Detection Systems (IDS)

There are three main types:

[1] In addition to those there are also protocol/application-based IDS

Intrusion Detection Systems (IDS)

There are three main types:

- Network-based IDS (e.g. Snort)

[1] In addition to those there are also protocol/application-based IDS

Intrusion Detection Systems (IDS)

There are three main types:

- Network-based IDS (e.g. Snort)
  - Those monitor the network for e.g. ARP spoofing, botnet traffic, malware on the wire

[1] In addition to those there are also protocol/application-based IDS

Intrusion Detection Systems (IDS)

There are three main types:

- Network-based IDS (e.g. Snort)
  - Those monitor the network for e.g. ARP spoofing, botnet traffic, malware on the wire
  - Problematic to handle encrypted traffic

[1] In addition to those there are also protocol/application-based IDS

Intrusion Detection Systems (IDS)

There are three main types:

- Network-based IDS (e.g. Snort)
  - Those monitor the network for e.g. ARP spoofing, botnet traffic, malware on the wire
  - Problematic to handle encrypted traffic
- Host-based IDS

[1] In addition to those there are also protocol/application-based IDS

Intrusion Detection Systems (IDS)

There are three main types:

- Network-based IDS (e.g. Snort)
  - Those monitor the network for e.g. ARP spoofing, botnet traffic, malware on the wire
  - Problematic to handle encrypted traffic
- Host-based IDS
  - As the name already says, those run on the hosts

[1] In addition to those there are also protocol/application-based IDS

Intrusion Detection Systems (IDS)

There are three main types:

- Network-based IDS (e.g. Snort)
  - Those monitor the network for e.g. ARP spoofing, botnet traffic, malware on the wire
  - Problematic to handle encrypted traffic
- Host-based IDS
  - As the name already says, those run on the hosts
- Hybrid IDS [1]

[1] In addition to those there are also protocol/application-based IDS

Problems with IDS

Problems with IDS

- False positives/negatives

Problems with IDS

- False positives/negatives
- Getting information from all that data

Problems with IDS

- False positives/negatives
- Getting information from all that data
- Not being aware of the limitations of an IDS

OSSEC

OSSEC

- Is a GPL licensed HIDS

OSSEC

- Is a GPL licensed HIDS
- Sensors:

OSSEC

- Is a GPL licensed HIDS
- Sensors:
  - file integrity

OSSEC

- Is a GPL licensed HIDS
- Sensors:
  - file integrity
  - process output

OSSEC

- Is a GPL licensed HIDS
- Sensors:
  - file integrity
  - process output
  - log files

OSSEC

- Is a GPL licensed HIDS
- Sensors:
  - file integrity
  - process output
  - log files
  - (+ some kernel level anomaly detection stuff)

OSSEC

- Is a GPL licensed HIDS
- Sensors:
  - file integrity
  - process output
  - log files
  - (+ some kernel level anomaly detection stuff)
- Provides intrusion prevention mechanisms

OSSEC

- Is a GPL licensed HIDS
- Sensors:
  - file integrity
  - process output
  - log files
  - (+ some kernel level anomaly detection stuff)
- Provides intrusion prevention mechanisms
- Sports an extensive rule set by default

OSSEC

- Is a GPL licensed HIDS
- Sensors:
  - file integrity
  - process output
  - log files
  - (+ some kernel level anomaly detection stuff)
- Provides intrusion prevention mechanisms
- Sports an extensive rule set by default
- Available for MS Windows (agent only), *nix (full support)

OSSEC

- Is a GPL licensed HIDS
- Sensors:
  - file integrity
  - process output
  - log files
  - (+ some kernel level anomaly detection stuff)
- Provides intrusion prevention mechanisms
- Sports an extensive rule set by default
- Available for MS Windows (agent only), *nix (full support)
- Can also analyse e.g. Cisco PIX, FWSM logs

Architecture

Architecture

- Local or distributed (server/agent)

Architecture

- Local or distributed (server/agent)
- Agents collect data and send it to the server

Architecture

- Local or distributed (server/agent)
- Agents collect data and send it to the server
- Servers analyse/correlate the data and take care of

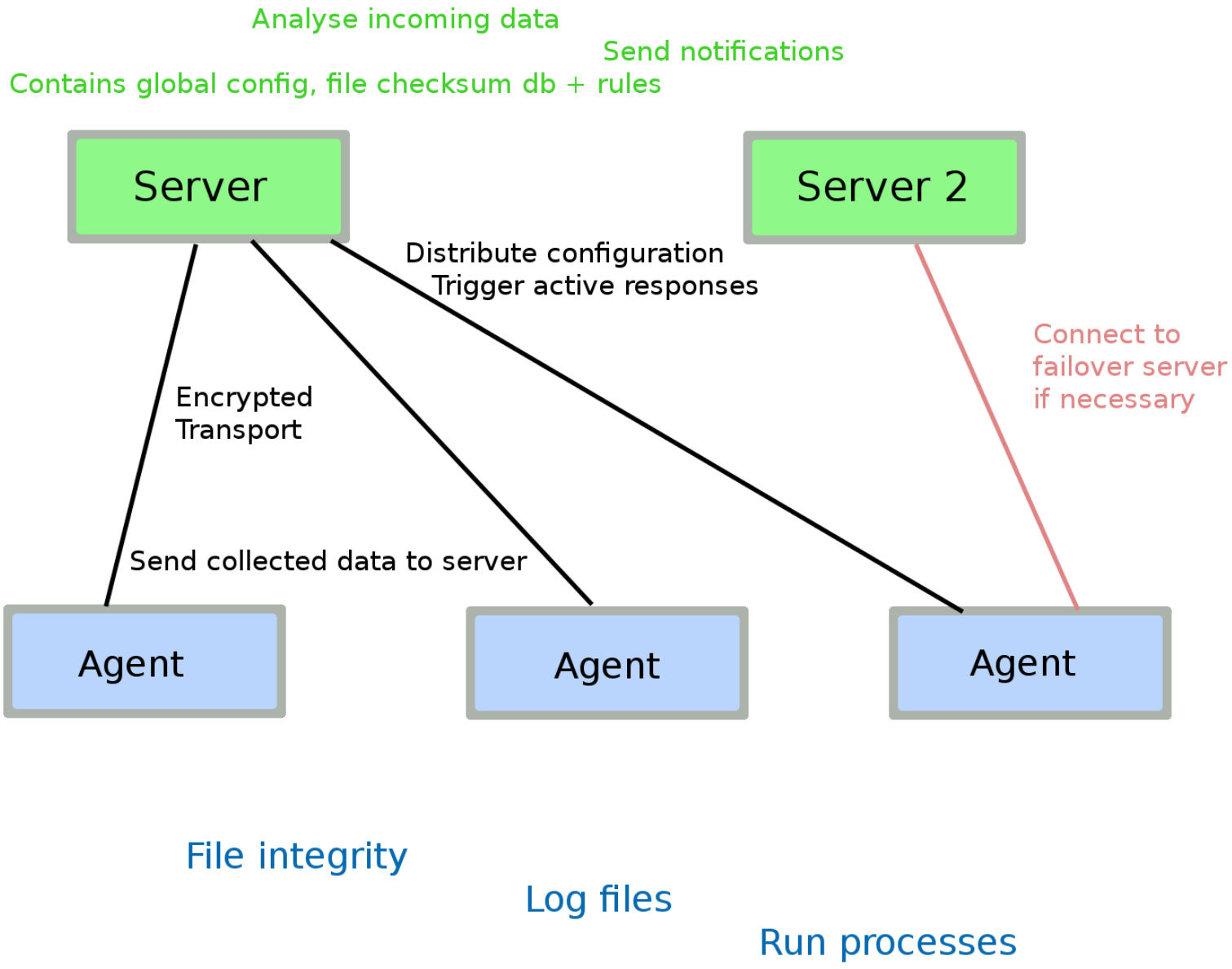
Architecture

- Local or distributed (server/agent)
- Agents collect data and send it to the server
- Servers analyse/correlate the data and take care of
  - sending notifications

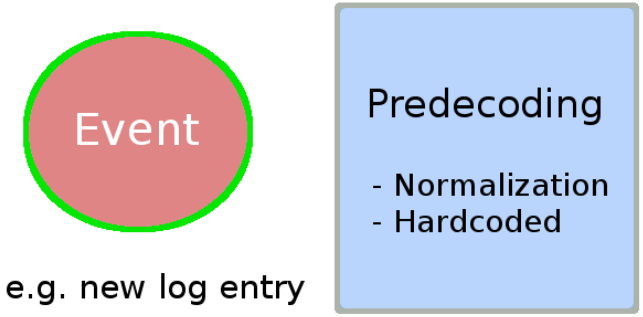
Architecture

- Local or distributed (server/agent)
- Agents collect data and send it to the server
- Servers analyse/correlate the data and take care of
  - sending notifications
  - triggering **active responses**

Architecture (2)



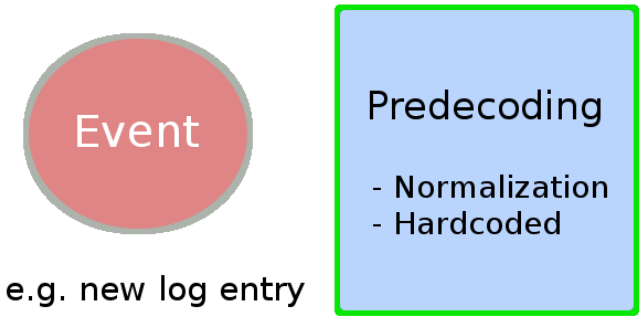
Analysis



[Time 2010.01.01 10:58:38 UTC] [Facility auth] [Sender sshd] [PID 400] [Message error: PAM: Authentication failure for illegal user root from 192.168.1.6] [Level 3] [UID -2] [GID -2] [Host ossec-agent1]

Jan 01 11:33:22 ossec-agent2 sshd[10718]: Accepted password for root from 192.168.1.6 port 48272 ssh2

Analysis

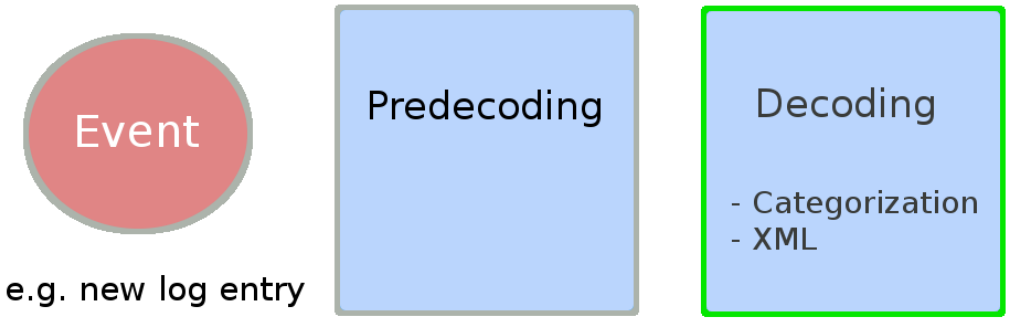


[Time 2010.01.01 10:58:38 UTC] [Facility auth] [Sender sshd] [PID 400] [Message error: PAM: Authentication failure for illegal user root from 192.168.1.6] [Level 3] [UID -2] [GID -2] [Host ossec-agent1]

Jan 01 11:33:22 ossec-agent2 sshd[10718]: Accepted password for root from 192.168.1.6 port 48272 ssh2

Time/Date:	2010 Jan 01 10:58:38	2010 Jan 01 11:33:22
Hostname:	ossec-agent1	ossec-agent2
Program name:	sshd	sshd
Log:	error: PAM: Authentication failure for illegal user root from 192.168.1.6	Accepted password for root from 192.168.1.6 port 48272 ssh2

Analysis



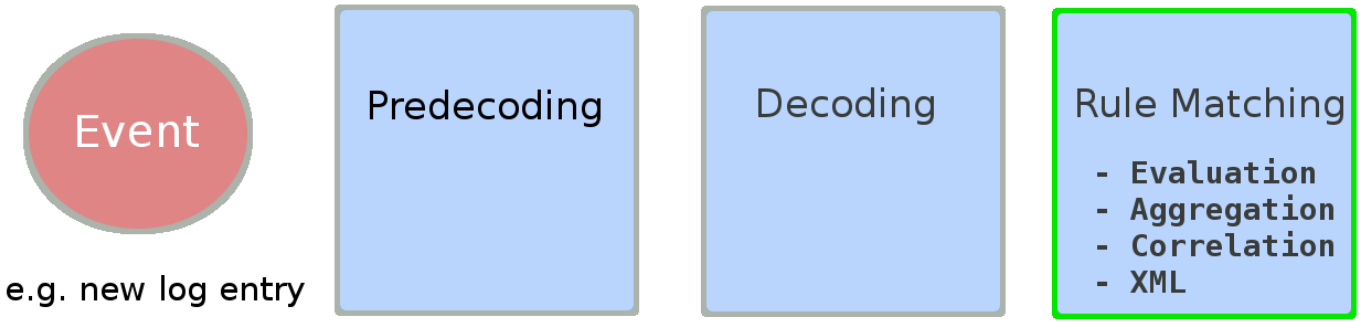

```
<decoder name ="sshd">
  <program_name>^sshd</program_name>
</decoder>

<decoder name="ssh-invfailed">
  <parent>sshd</parent>
  <prematch>^Failed \S+ for invalid user|^Failed \S+ for illegal user</prematch>
  <regex offset="after_prematch">from (\S+) port \d+ \w+$</regex>
  <order>srcip</order>
</decoder>
```

New key value pairs!

decoded_as: sshd
srcip: 192.168.1.6

Analysis

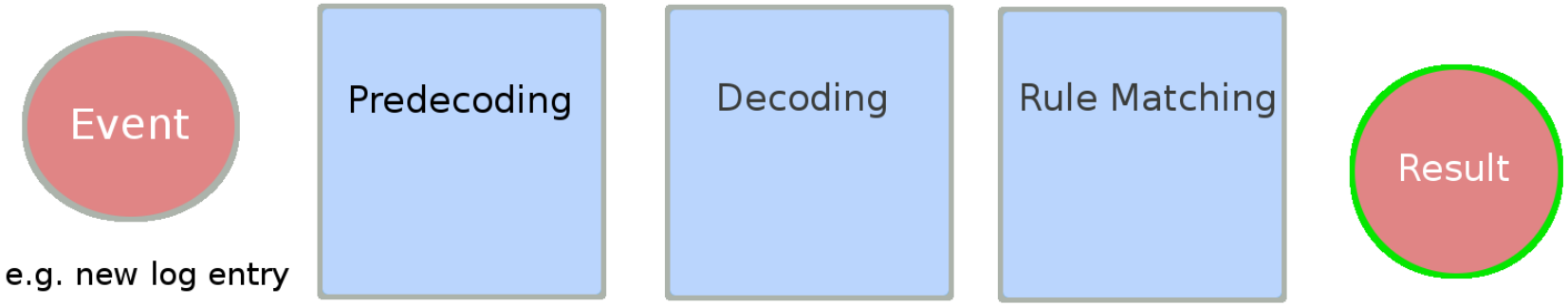



```
<rule_id="123456" level="7">
  <decoded_as>sshd</sshd>
  <srcip>192.168.1.6</srcip>
  <match>root</match>
  <group>localnet,sshd,</group>
  <description>My cat is trying to login as root again!</description>
</rule>

<rule_id="123457" level="10" frequency="5" timeframe="60">
  <if_matched_sid>123456</if_matched_sid>
  <description>5 times within a minute, that's to many </description>
  <group>localnet,repeatedproblems,</group>
</description>
```

Even more key/value pairs:
- rule id,
- group,
- alert level

Analysis



Take action depending on **alert level**, **group**, **rule id**:

- Write event to DB or logfile
- Send me an e-mail
- Send an e-mail to another person
- Ban offenders by autocreating iptables rule

Usage

Usage

- Detect intrusions (obviously)

Usage

- Detect intrusions (obviously)
- Auto ban repeated offenders

Usage

- Detect intrusions (obviously)
- Auto ban repeated offenders
- Monitor non-intrusion related aspects

Usage

- Detect intrusions (obviously)
- Auto ban repeated offenders
- Monitor non-intrusion related aspects
  - E.g. malfunctioning RAID controllers

Usage

- Detect intrusions (obviously)
- Auto ban repeated offenders
- Monitor non-intrusion related aspects
  - E.g. malfunctioning RAID controllers
  - Use granular e-mail notifications to inform respective co-workers

Usage

- Detect intrusions (obviously)
- Auto ban repeated offenders
- Monitor non-intrusion related aspects
  - E.g. malfunctioning RAID controllers
  - Use granular e-mail notifications to inform respective co-workers
  - Or even trigger infrastructure wide unmounts of affected fs exports

Usage

- Detect intrusions (obviously)
- Auto ban repeated offenders
- Monitor non-intrusion related aspects
  - E.g. malfunctioning RAID controllers
  - Use granular e-mail notifications to inform respective co-workers
  - Or even trigger infrastructure wide unmounts of affected fs exports
- Use reporting functionality for statistics or forensic purposes

Usage

- Detect intrusions (obviously)
- Auto ban repeated offenders
- Monitor non-intrusion related aspects
  - E.g. malfunctioning RAID controllers
  - Use granular e-mail notifications to inform respective co-workers
  - Or even trigger infrastructure wide unmounts of affected fs exports
- Use reporting functionality for statistics or forensic purposes
  - E.g. which ports currently open in my firewall are actually used?

Usage

- Detect intrusions (obviously)
- Auto ban repeated offenders
- Monitor non-intrusion related aspects
  - E.g. malfunctioning RAID controllers
  - Use granular e-mail notifications to inform respective co-workers
  - Or even trigger infrastructure wide unmounts of affected fs exports
- Use reporting functionality for statistics or forensic purposes
  - E.g. which ports currently open in my firewall are actually used?
  - E.g. take logfiles from a post-mortem image and hand it to the analysis and reporting engine

Usage

- Detect intrusions (obviously)
- Auto ban repeated offenders
- Monitor non-intrusion related aspects
  - E.g. malfunctioning RAID controllers
  - Use granular e-mail notifications to inform respective co-workers
  - Or even trigger infrastructure wide unmounts of affected fs exports
- Use reporting functionality for statistics or forensic purposes
  - E.g. which ports currently open in my firewall are actually used?
  - E.g. take logfiles from a post-mortem image and hand it to the analysis and reporting engine
- Policy enforcement

Community & Questions

- `http://www.ossec.net`
- Mailing list/Google group: `http://groups.google.com/group/ossec-list`
- Active development: `https://bitbucket.org/dcid/ossec-hids`
- IRC channel: `#ossec` at `irc.freenode.org`
- The community helps improving documentation/rule set, join them!

Community & Questions

- `http://www.ossec.net`
- Mailing list/Google group: `http://groups.google.com/group/ossec-list`
- Active development: `https://bitbucket.org/dcid/ossec-hids`
- IRC channel: `#ossec` at `irc.freenode.org`
- The community helps improving documentation/rule set, join them!

- Are there any questions?