Proactive Security Monitoring in a Policy Managed Network

Till Dörges
Klaus-Peter Kossakowski
Outline / ToC

- Outline / ToC
- Motivation
- POSITIF: Overview
- POSITIF: Description Languages
- PSM: Black Box
- PSM: Detailed View
- Outlook
POSITIF – Motivation

- complexity of networks ever increasing
- individual administration of components impossible
- potential solution: Policy Based Management

POSITIF
- Policy based Security Tools and Framework
- EC funded project
- provides tools and framework
- aims at high level policies
Outline / ToC

- Outline / ToC
- Motivation
- POSITIF: Overview
- POSITIF: Description Languages
- PSM: Black Box
- PSM: Detailed View
- Outlook
POSITIF – Framework (1)

- schematic overview
key elements
- tools for administrators

description
- System Description Language (SDL)
- Security Policy Language (SPL)

automatic deployment of
- policies
- (configurations)

specifying a policy pointless without monitoring
Outline / ToC

- Outline / ToC
- Motivation
- POSITIF: Overview
- POSITIF: Description Languages
- PSM: Black Box
- PSM: Detailed View
- Outlook
Description Languages

- XML based
- High level versions for administrators describing the network
- Low level versions for actual reasoning and automatic processing
  - Basically contain more details
  - Set as defaults
SDL example

- (partial) description of a firewall

```xml
<firewall id="Firewall">
  <interface id="eth0" number="1" connector="RJ45"
    technology="Ethernet" protocol="10-100BaseT">
    <addr type="ipv4"
      netmask="255.255.255.128">1.2.3.4</addr>
  </interface>
  <interface id="eth1" number="2" technology="Ethernet"
    connector="RJ45" protocol="10-100BaseT">
    <addr type="ipv4"
      netmask="255.255.255.240">1.2.3.5</addr>
  </interface>
</firewall>
```
SPL example

(partial) description of filtering rule

```xml
<xCIM_FilterEntry>
  <CIM_FilterEntryBase.Name>access1</CIM_FilterEntryBase.Name>
  <IsNegated>false</IsNegated>
  <TrafficType>IPv4</TrafficType>
  <MatchConditionType>Source Address and Mask</MatchConditionType>
  <MatchConditionValue>1.2.3.4/255.255.255.255</MatchConditionValue>
  <Action>Permit</Action>
  <DefaultFilter>false</DefaultFilter>
</xCIM_FilterEntry>
```
Outline / ToC

- Outline / ToC
- Motivation
- POSITIF: Overview
- POSITIF: Description Languages
- PSM: Black Box
- PSM: Detailed View
- Outlook
Proactive Security Monitor – Overview

- monitors administrative domain for
  - policy violations
  - attacks (slightly different from policy violations)
- highly distributed component itself
- analyzes events, takes appropriate actions
- reactions can be (semi-) automatic
PSM as a black box
Proactive Security Monitor – Blackbox

- **SDL**: description of the systems to be checked
- **SPL**: description of the policies
- **events**: all information processed by the PSM
- **configurations**: to verify their integrity

**outputs**

- Alerts
- Policy Change Requests
- Reconfiguration Requests
- Retrieve Configurations
Proactive Security Monitor – Msg Formats

- use existing standards
- IDMEF
  - report events
- IODEF
  - report incidents
  - aggregated information
Outline / ToC

- Outline / ToC
- Motivation
- POSITIF: Overview
- POSITIF: Description Languages
- PSM: Black Box
- PSM: Detailed View
- Outlook
internal components
Proactive Security Monitor – Detailed View

■ sensing components
  ■ IDS/SEM Intrusion Detection Systems
  ■ Proactive Security Scanner
  ■ Policy Violation Sensor
  ■ Proactive Configuration Checker

■ correlation and assessment
  ■ IDS and SEM Correlation
  ■ PSC Correlation
  ■ PSM Assessment
### Sensing Components

#### Comparison of IDS/SEM, PSC, PVS, PCC

<table>
<thead>
<tr>
<th>Behavior</th>
<th>Recognizes</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDS/SEM</td>
<td>Reactive Attacks / Policy Violations</td>
</tr>
<tr>
<td>PVS</td>
<td>Reactive Attacks / Policy Violations</td>
</tr>
<tr>
<td>PCC</td>
<td>Proactive Misconfigurations, Potential Attacks</td>
</tr>
<tr>
<td></td>
<td>and Potential Policy Violations</td>
</tr>
<tr>
<td>PSC</td>
<td>Proactive Vulnerabilities, Potential Attacks</td>
</tr>
<tr>
<td></td>
<td>and Potential Policy Violations</td>
</tr>
</tbody>
</table>
Sensing Components – Examples

## Detection by Component

<table>
<thead>
<tr>
<th>Incident</th>
<th>IDS/SEM</th>
<th>PVS</th>
<th>PCC</th>
<th>PSC</th>
</tr>
</thead>
<tbody>
<tr>
<td>portscan</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>cmd32.exe exploit</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>reach. of forbidden service</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>denial of allowed service</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>faulty configuration</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>write to forbidden dirs</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>forbidden attachments</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>succ. auth, wrong method</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>SSL conn., wrong certs</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>WWW down, no alert</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>
Outline / ToC

- Outline / ToC
- Motivation
- POSITIF: Overview
- POSITIF: Description Languages
- PSM: Black Box
- PSM: Detailed View
- Outlook
Outlook

- project is not finished yet
- first results look promising
- pretty complex task
  - real benefit only if everything is integrated
  - hindered by large abundance of proprietary protocols
Contact Information

- http://www.positif.org/

- Till Dörges
  PRE-CERT
  PRESECURE Consulting GmbH

  td@pre-secure-de