Intrusion Detection
Who am I?

• Informal Security Education
• CS - Colby College
  – Honors work in Static Analysis
• Fortify Software
  – Engineer
  – Architect
  – Product Management
• HP
• AlienVault
  – Products

• BlackHat
• RSA
What is it?
What are you looking for?

- Pattern – known sequences of behaviors that indicate malicious activity

- Statistical – deviations from normal (anomalous) behavior that could indicate malicious activity
Where are you looking for it?

- User Activity
- Application Activity
- Operating System Activity
- Network Activity

- SIEM
- SIEM / Host-based IDS
- Host-based IDS
- Network-based IDS
Where are you looking for it?

- User Activity
- Application Activity
- Operating System Activity
- Network Activity

- SIEM
- SIEM / Host-based IDS
- Host-based IDS
- Network-based IDS

Why so many products??
Different Data

- SIEM
- Host-based IDS
- Network-based IDS

- Event logs
- Operating system events
- Raw network data
Host-based IDS
Host-based IDS

• Monitors operating system activity
  – File changes
  – Registry
  – Application / Processes

• Deployment:
  – Agent
  – Remote

• Products
  – OSSEC (free)
  – McAfee EPO
  – Symantec HIDS
  – Tripwire
Host-based IDS

<var name="SYS_USERS">^apache$|^mysql$|^www$|^nobody$|^nogroup$|^portmap$|^named$|^rpc$|^mail$|^ftp$|^shutdown$|^halt$|^daemon$|^bin$|^postfix$|^shell$|^info$|^guest$|^psql$|^user$|^users$|^console$|^uucp$|^lp$|^sync$|^sshd$|^cdrom$|^ossec$</var>

<rule id="40101" level="12">
  <if_group>authentication_success</if_group>
  <user>$SYS_USERS</user>
  <description>System user successfully logged to the system.</description>
  <group>invalid_login,</group>
</rule>
Host-based IDS

Pro
• Process level inspection
• Acute behavioral detection
• User attribution

Cons
• Easy to disable
• High Administrative Costs
Network IDS
Network IDS

- Monitors network activity
  - Protocol Usage
  - Deep Packet Inspection
  - File Identification
- Deployment:
  - Inline
- Products
  - Suricata (free)
  - McAfee IntruShield
  - Cisco
  - Juniper
Network IDS


Network IDS

Pro
• Difficult to disable
• Early identification of threats
• Broad rulesets available

Cons
• Difficult to derive context
SIEM
SIEM

• Monitors anything you can feed it
  – VPN, Firewall, Application, Email server, door readers, etc

• Deployment:
  – Central

• Products
  – ArcSight (HP)
  – IBM (Q1)
  – OSSIM (Free)
Data Normalization Example

Juniper SRX – Session Denied Raw Log Event

#Sep 25 06:26:09 1.1.3.1 2010-09-25T06:26:10.420 SRX2-NY RT_FLOW - RT_FLOW_SESSION_DENY
[junos@2636.1.1.1.2.35 source-address="1.2.3.4" source-port="1234" destination-address="2.3.4.5"
destination-port="80" service-name="junos-http" protocol-id="6" icmp-type="0" policy-name="DENY"
source-zone-name="trust" destination-zone-name="untrust"]
Data Normalization Example

Juniper SRX – Session Denied Raw Log Event

#Sep 25 06:26:09 1.1.3.1 2010-09-25T06:26:10.420 SRX2-NY RT_FLOW - RT_FLOW SESSION_DENY
[junos@2636.1.1.2.35 source-address="1.2.3.4" source-port="1234" destination-address="2.3.4.5" destination-port="80" service-name="junos-http" protocol-id="6" icmp-type="0" policy-name="DENY" source-zone-name="trust" destination-zone-name="untrust"]

NORMALIZED

Event ID=SESSION_DENY
Date=September 25, 2010 6:26:09
Source IP=1.2.3.4
Source Port=1234
Source Zone=trust
Destination IP=2.3.4.5
Destination Port=80
Destination Zone=untrust
Service Name=Junos HTTP
Protocol=TCP
ICMP Type=Echo
Policy=Deny
Data Normalization Example

Juniper SRX – Session Denied Log Event

#Sep 25 06:26:09 1.1.3.1 2010-09-25T06:26:10.420 SRX2-NY RT_FLOW – RT_FLOW_SESSION_DENY
[junos@2636.1.1.2.35 source-address="1.2.3.4" source-port="1234" destination-address="2.3.4.5" destination-port="80" service-name="junos-http" protocol-id="6" icmp-type="0" policy-name="DENY" source-zone-name="trust" destination-zone-name="untrust"]

NORMALIZED

Event ID=SESSION_DENY
Date=September 25, 2010 6:26:09
Source IP=1.2.3.4
Source Port=1234
Source Zone=trust
Destination IP=2.3.4.5
Destination Port=80
Destination Zone=untrust
Service Name=Junos HTTP
Protocol=TCP
ICMP Type=Echo
Policy=Deny

• Necessary for cross-data source correlation
  – Identify similar data from different data sources (User Name, IP Address, etc.)
• Each data source requires some custom logic
  – Each log has a unique format
Correlation Example

Correlation can be thought of as a state machine
Correlation Example

Probing

Each event can ‘match’ and progress the state

**Event 1**

Event ID=SESSION_DENY
Date=September 25, 2010 6:26:09
Source IP=1.2.3.4
Source Port=1234
Source Zone=trust
Destination IP=2.3.4.5
Destination Port=80
Destination Zone=untrust
Service Name=Junos HTTP
Protocol=TCP
ICMP Type=Echo
Policy=Deny
Correlation Example

Probing

Event 1
Event ID=SESSION_DENY
Date=September 25, 2010 6:26:09
Source IP=1.2.3.4
Source Port=1234
Source Zone=trust
Destination IP=2.3.4.5
Destination Port=80
Destination Zone=untrust
Service Name=Junos HTTP
Protocol=TCP
ICMP Type=Echo
Policy=DENY

Event 2
Event ID=SESSION_DENY
Date=September 25, 2010 6:26:10
Source IP=1.2.3.4
Source Port=1234
Source Zone=trust
Destination IP=2.3.4.5
Destination Port=443
Destination Zone=untrust
Service Name=Junos HTTP
Protocol=TCP
ICMP Type=Echo
Policy=DENY

Subsequent events need to match within time window
Correlation Example

Probing

Event 3
Event ID=SESSION_CREATE
Date=September 25, 2010 6:26:11
Source IP=1.2.3.4
Source Port=1234
Source Zone=trust
Destination IP=2.3.4.5
Destination Port=22
Destination Zone=untrust
Service Name=Junos HTTP
Protocol=TCP
ICMP Type=Echo
Policy=Deny

Subsequent events need to match within time window
Correlation Example

Probing

DENY

Event ID=SESSION_DENY
Date=September 25, 2010 6:26:09
Source IP=1.2.3.4
Source Port=1234
Source Zone=trust
Destination IP=2.3.4.5
Destination Port=80
Destination Zone=untrust
Service Name=Junos HTTP
Protocol=TCP
ICMP Type=Echo
Policy=Deny

DENY

Event ID=SESSION_DENY
Date=September 25, 2010 6:26:10
Source IP=1.2.3.4
Source Port=1234
Source Zone=trust
Destination IP=2.3.4.5
Destination Port=443
Destination Zone=untrust
Service Name=Junos HTTP
Protocol=TCP
ICMP Type=Echo
Policy=Deny

ALLOW

Event ID=SESSION_CREATE
Date=September 25, 2010 6:26:11
Source IP=1.2.3.4
Source Port=1234
Source Zone=trust
Destination IP=2.3.4.5
Destination Port=22
Destination Zone=untrust
Service Name=Junos HTTP
Protocol=TCP
ICMP Type=Echo
Policy=Deny

ALARM — Probing
Source IP=1.2.3.4
Source Port=1234
Source Zone=trust
Destination IP=2.3.4.5
Destination Port=80,443,22
Protocol=TCP

Fully loaded state machine generates an alarm
SIEM

**Pro**
- Flexible and complete

**Cons**
- Expensive to deploy
Example
Example

M. Cochran disconnects from network

Infection

M. Cochran reconnects to network

Snort detect Mariposa / Paveo CnC

Host identified as infected

M. Cochran disconnects from network

Potential Detection Point:
Snort identify Malicious Binary

Potential Detection Point:
Symantec Identify Infection

Potential Detection Point:
OSSEC Reports Infection

Snort identify Malicious Binary

Potential Detection Point:
Symantec Identify Infection

Potential Detection Point:
OSSEC Reports Infection

Host identified as infected

M. Cochran disconnects from network

Snort detect Mariposa / Paveo CnC

Host identified as infected