Expansion of the SURFnet Intrusion Detection System

R. Buijs
P. Siekerman
System and Network Engineering

Universiteit van Amsterdam
SURF\textcopyright

7-2-2007
Contents

1 Assignment

2 Intrusion Detection Systems

3 SURFnet IDS

4 IDS Software

5 Conclusion
Assignment

Suggest improvements to SURFnet IDS.
- Greater diversity

IDS product research
Intrusion Detection Systems

What is an IDS?

HIDS
- Host based
- Monitors attacks to host

NIDS
- Network based
- Monitors malicious traffic on network, multiple hosts
Intrusion Detection Systems

- **Low-interaction**
  - Service emulator
  - Limited to emulation
  - Easier to detect

- **High-interaction**
  - Runs real services
  - Real host, or virtual
  - Zero day attacks
Distributed sensor-based HIDS

Sensor
- Any PC
- USB stick
- Remastered Knoppix
- OpenVPN
SURFnet IDS

Expansion of SURFnet IDS

Client LAN

Internet

VPN Tunnel

Honeypot/Tunnel Server
- Nepenthes
- openVPN

Logging Server
- Postgresql
- Web interface

Server LAN

Client LAN

VPN Tunnel

VPN Tunnel

VPN Tunnel

Sensor

Sensor

Firewall
SURFnet IDS server

- **Nepenthes**
  - Simulates vulnerabilities, and collects malware
  - More than 20 simulations currently available
  - Reports to PostgreSQL database

- **Argos**
  - High interaction IDS
  - Can be used to analyse Zero day attacks
Customer can log in
Access to information of their sensor
Which attacks
Statistics
 Tripwire
Samhain
  - Client-server based
Aide
Honeyd:
- Simulates a host with vulnerable services
- Simulates complicated networks
- Well documented
- Infrequently updated
Honeytrap:

- Simple: "Poor man’s service emulator"
- Mirror mode
- Regularly updated
- Badly documented
- No community
IDS Software: Prelude (1)

Prelude:
- IDS Framework
- Sensors
- IDMEF (XML)
- Policies
- Web-interface Prewikka
Prelude test:
- Slow
- Web-interface needs to be modified
IDS Software: Snort

- Network traffic analyse tool

Operation Modes
- Sniffer / logger mode
- Inline mode
- Network intrusion detection mode
IDS Software: Snort NIDS mode

- Rules
- Alerts
- Logging

Implementation

Maintenance
Conclusion

- Let SURFnet IDS detect more malicious traffic
- Our advice: Integrate Snort
- SURFnet IDS will cover a greater diversity of malicious traffic
Questions?