

# Network and System Security

A Practical Guide 

Practical Network and System Security

ENGINEERED NETWORKS

[www.engineered-net.com](http://www.engineered-net.com)

ssurdock@engineered-net.com

Date: 03/18/05

© 2005 Engineered Networks

Rev: 1.0

Page: 1

# Why Bother?

- System Availability
- System Performance
- Lawsuits
- Your Job

# 10,000 Foot View<sup>1</sup>

- Assessment
- Protection
- Detection
- Response

# Assessment




- What are the assets?
  - What is their value?
- What are the threats?
- What are the vulnerabilities?
- What is the risk?
  - Risk = threat x vulnerability x asset value

# Assessment - Techniques

- Assemble a small inter-departmental team
- Identify top-level systems & sub-systems
- Identify the threats
- Identify the vulnerabilities
- Develop a plan & policies
- Methodologies
  - OCTAVE - <http://www.cert.org/octave/>



# Assessment - Tools

- You WILL need network & system diagrams
- You will need to understand threats
- Use NMAP to find devices on your network 
- Use Nessus to find vulnerabilities 
- Microsoft Baseline Security Analyzer 

# Protection

- ...will eventually fail
- Defense in depth
- NEVER use "ANY" in a firewall rule
- Secure the host
  - Limit available services
  - Review file/folder permissions
  - Enforce permissions

# Protection

- Control physical access
- Secure the network
- Secure the desktop
- Patch, patch, patch, patch, patch
  - <http://www.us-cert.gov/>

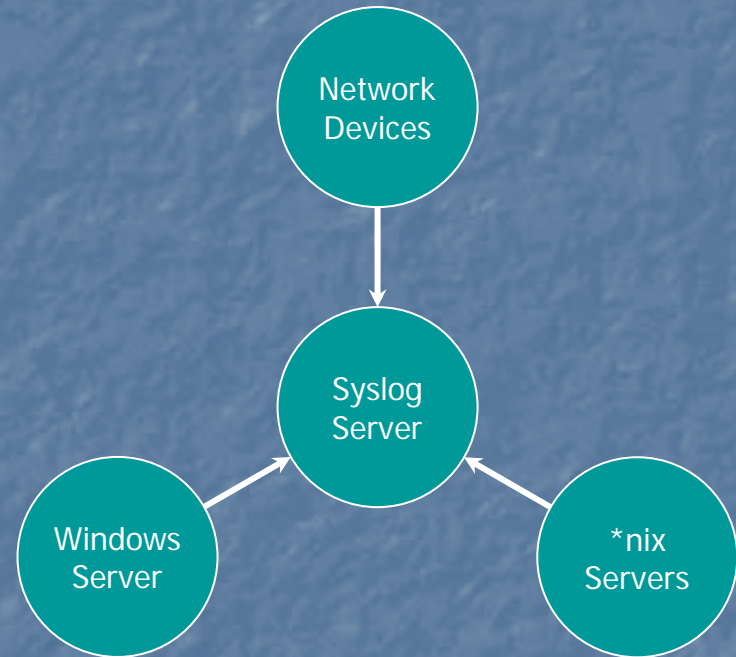


# Detection

- Looking for violations of the security policy
- Logging
- Statistical Data
- Session Data
- Packet Data

# Detection - Logging

- Time correlated events are *easy* to find
- Alert on configuration changes
- Great for troubleshooting too!





# Detection – Statistical Data

- Derived from polling devices
- Trended for a *baseline*
- Visually digestible
- RRD based - MRTG, Cricket, CACTI, RRFW

# Detection – Session Data

- Who is talking to who, with what, and how much.
- Detect Internet abusers
- Detect hacked machines
- Cisco routers include NetFlow reporting
- Commercial and free tools exist to help visualize the data

# Detection – Packet Data

- Look at individual packets for anomalies
- Network Intrusion Detection Systems
  - SNORT – King of free NIDS 
- Manual inspection
  - ETHEREAL – King of free packet analyzers 

# Response<sup>8</sup>

- Prepare the procedures and Incident Response Team before a problem occurs.
- I found a possible policy breach, now what?

# Response

- Initial investigation to collect basic details (who, what, where, when)
- Response strategy
- Investigate by reviewing collected data
- Report the findings to the proper authorities
- Fix what was broken to make sure it doesn't happen again

# Security Framework

- Assessment
  - Calculate risk & create plan
- Protection
  - Enforce the traffic you want
- Detection
  - Logging and alerting
- Response
  - Make sure it doesn't happen (again)

# The End

- Thank you for coming!
- The Presentation can be found at:  
<http://www.engineered-net.com/Library>
- The winner is...

# Bibliography

- 1) Richard Bejtlich, *The Tao of Network Security Monitoring – Beyond Intrusion Detection*. (Addison-Wesley, 2004)
- 2) Steve A. Rouiller, Virtual LAN Security: weaknesses and countermeasures,  
<http://www.sans.org/rr/whitepapers/networkdevs/1090.php>
- 3) [Tobi Oetiker](http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/), RRDTOOL,  
<http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/>
- 4) [Tobi Oetiker](http://people.ee.ethz.ch/~oetiker/webtools/mrtg/), MRTG, <http://people.ee.ethz.ch/~oetiker/webtools/mrtg/>
- 5) Cricket, <http://cricket.sourceforge.net/>
- 6) CACTI, <http://www.raxnet.net/products/cacti/>
- 7) RRFW, <http://rrfw.sourceforge.net/>
- 8) Kevin Mandia, Chris Prosise & Matt Pepe, *Incident Response & Computer Forensics, Second Edition*. (McGraw-Hill/Osborne, 2003)