

Network and System Security

A Practical Guide 

Practical Network and System Security

ENGINEERED NETWORKS

Date: 03/08/05

© 2005 Engineered Networks

www.engineered-net.com

ssurdock@engineered-net.com

Rev: 1.0

Page: 1

Why Bother?

- Spyware, spam, Adware
- Viruses, Worms, Trojan Horses
- DOS attacks
- Theft of data
- Theft of resources
- Unauthorized Access by Insider

Why Bother? Because...

- System Availability
- System Performance
- Time to repair
- Lawsuits
- Reputation
- Your Job

What's InfoSec about

- Confidentiality
- Integrity
- Availability
- (Accountability)
- Manage the risk

NIST Security Guidelines (I)

- Supports the Mission of the Organization
- Is an Integral Element of Sound Management
- Should Be Cost-Effective
- Systems Owners Have Security Responsibilities Outside Their Own Organizations

NIST Security Guidelines (II)

- Responsibilities and Accountability Should Be Made Explicit
- Requires a Comprehensive and Integrated Approach
- Should Be Periodically Reassessed
- Is Constrained by Societal Factors




The Steps

- Assess
- Protect
- Detect
- Respond

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 - 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

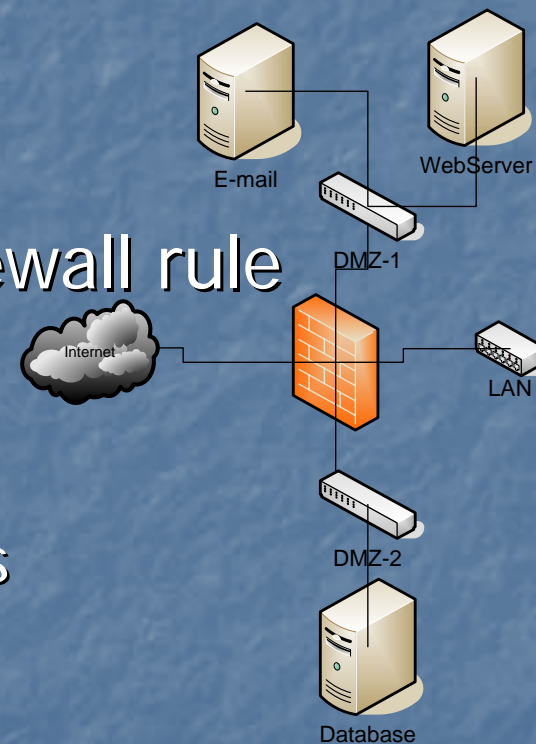
- Virus protection
- spam control
- Firewalls – control gates
- Apply security patches A.S.A.P.
- Practice sensible computing
 - Don't open it unless you know it's safe

More Protection

- Transmit sensitive data over secure channel
- Encrypt sensitive data if not physically secure
- Unique, complex passwords

And More Protection

- ...will eventually fail
- Defense in depth
- Carefully use "ANY" in a firewall rule
- Secure the host
 - Limit available services
 - Review file/folder permissions
 - Enforce permissions

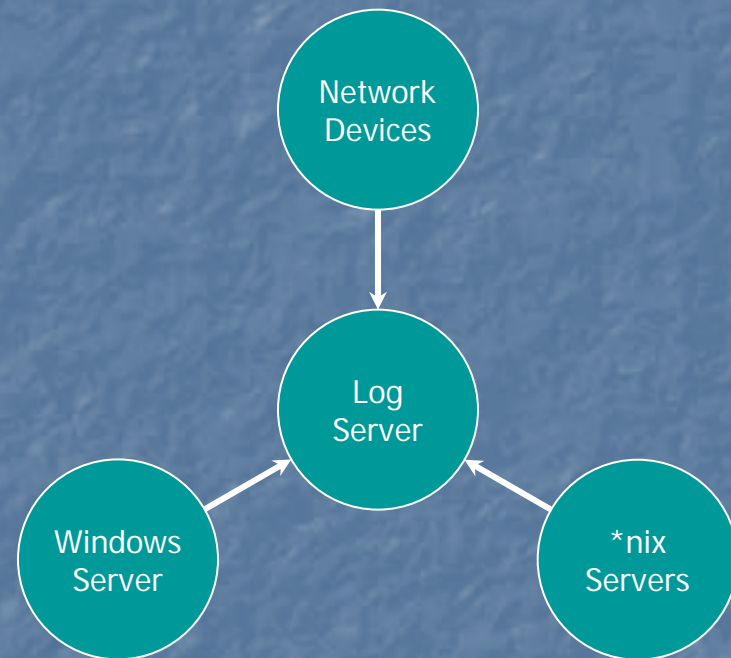


Detection

- 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
- Most newer firewalls have built-in

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 behavior 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>

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, RRDTOOL,
<http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/>
- 4) Tobi Oetiker, 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 Proise & Matt Pepe, *Incident Response & Computer Forensics, Second Edition*. (McGraw-Hill/Osborne, 2003)