Security Auditing & Risk Analysis

A day into the minds of the eccentrics:

Wietse Venema & Dan Farmer

April 30th, 1996

Overview du jour

- Introduction
- Definitions & philosophies
- A simple firewall audit
- How to audit a host

Overview du jour (cont.)

- The fish.com audit
- Auditing networks
- Reporting
- The AT&T audit

The book

- Practical
- Comprehensive
- Audacious
- Addison-Wesley
- Late

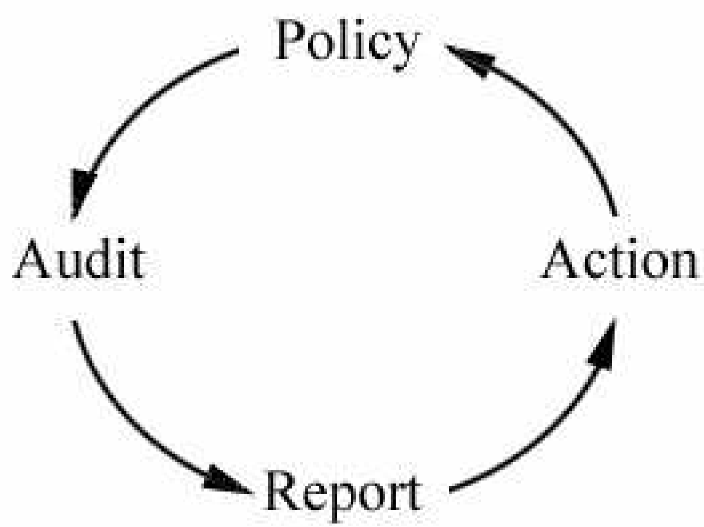
Security Auditing & Risk Analysis

- What is security?
- What **is** a Security Audit?
- Risk Analysis
- Security policies

Security Auditing & Risk Analysis (cont.)

- Why do a security audit?
- Who can audit?
- When to audit?
- Tools of the trade
- How to do an audit...

What is a security audit?



What is a security audit? (cont.)

- Policy based
- Assessment of risk
- Examines site methodologies and practices
- Dynamic
- Communication

What is a security audit? (cont.)

Component	% of time
Preparation	10
Reviewing Policy/Docs	10
Talking/Interviewing	10
Technical Investigation	15
Reviewing Data	20
Writing Report	20
Presenting Report	5
Post-audit Actions	10

What kinds of Security Audits are there?

- Host
- Firewall
- Networks
- Large networks

Security Policies & Documentation

- What is a security policy?
- Components
- Who should write it?
- How long should it be?
- Dissemination
- It walks, it talks, it is alive...
- RFC 1244
- What if a written policy doesn’t exist?
- Other documentation

Components of a Security Policy

- Who can use resources
- Proper use of the resources
- Granting access & use
- System Administrator privileges
- User rights & responsibilities
- What to do with sensitive information
- Desired security configurations of systems

RFC 1244 -
"Site Security Handbook"

- Defines security policies & procedures
- Policy violations
- Interpretation
- Publicizing
- Identifying problems
- Incident response
- Updating

Other Documentation

- Hardware/software inventory
- Network topology
- Key personnel
- Emergency numbers
- Incident logs

Why do a Security Audit?

- Information is power
- Expectations
- Measure policy compliance
- Assessing risk & security level
- Assessing potential damage
- Change management
- Security incident response

Who can Audit?

- Those who have **permission!!!**
- Employee or hired gun
- Technical expertise
- Understanding of organization
- Ability to communicate

Randal Schwartz

- Perl
- Crack
- Intel vs. Schwartz
- Judgment day

When to audit?

- Emergency!
- Before prime time
- Scheduled/maintenance

Audit Schedules

Type of System	**Frequency of Audit**
Individual Host	12-24 months
Large Networks	12-24 months
Network	12 months
Firewall	6 months