

Security Countermeasures

1 Technology

1.1 HARDWARE

- 1.1.1 Routers
- 1.1.2 Firewalls
- 1.1.3 Smart cards
- 1.1.4 USB tokens
- 1.1.5 Computers
- 1.1.6 Switches
- 1.1.7 Wireless Access Points
- 1.1.8 STU-III

1.2 SOFTWARE

- 1.2.1 Intrusion detection systems
 - 1.2.1.1 Techniques
 - 1.2.1.1.1 Anomaly detection
 - 1.2.1.1.2 Signature detection
 - 1.2.1.1.3 Target monitoring (integrity checking)
 - 1.2.1.1.4 Stealth probes
 - 1.2.1.2 Types
 - 1.2.1.2.1 Host based
 - 1.2.1.2.2 Network based
- 1.2.2 Anti-virus
 - 1.2.2.1 Types
 - 1.2.2.1.1 Host
 - 1.2.2.1.2 Network border gateway
 - 1.2.2.2 Techniques
 - 1.2.2.2.1 Signature detection
 - 1.2.2.2.2 Behavior detection
- 1.2.3 Firewalls
 - 1.2.3.1 Packet filters
 - 1.2.3.2 Stateful packet inspection
 - 1.2.3.3 Application proxy
- 1.2.4 Computer Forensics
 - 1.2.4.1 Data acquisition
 - 1.2.4.1.1 Partition imaging
 - 1.2.4.1.2 Data recovery
 - 1.2.4.1.3 File copy
 - 1.2.4.2 Data validation
 - 1.2.4.2.1 Hashes
 - 1.2.4.2.2 Checksums

- 1.2.4.3 Data analysis
 - 1.2.4.3.1 Text search
 - 1.2.4.3.2 Hash validation
- 1.2.4.4 Disk wiping
 - 1.2.4.4.1 Secure delete
- 1.2.5 Vulnerability assessment scanners
 - 1.2.5.1 Host
 - 1.2.5.2 Network
 - 1.2.5.3 Application scanner

2 People

2.1 SYSTEM ADMINISTRATORS

2.2 SYSTEM USERS

2.3 INCIDENT RESPONDERS

- 2.3.1 Team Manager
- 2.3.2 Team Leader
- 2.3.3 Information Protection Analyst

2.4 MANAGERS

2.5 SYSTEM STAKEHOLDERS

2.6 WARFIGHTERS

2.7 NETWORK ENGINEERS

3 Policies and Practices

3.1 ADMINISTRATIVE POLICIES

- 3.1.1 Acceptable use
- 3.1.2 Account management
- 3.1.3 Configuration management
- 3.1.4 Password policy
- 3.1.5 Security education training awareness program (SETAP)

3.2 ADVISORIES SERVICES

- 3.2.1 IAVA
- 3.2.2 IAVB
- 3.2.3 IAVT
- 3.2.4 Bugtraq

3.2.5 Subscription services

3.3 SECURITY AUDITING

3.3.1 Interviews

3.3.2 Vulnerability assessment

3.3.2.1 Scanning

3.3.2.2 Penetration testing

3.3.2.3 Red teaming

3.3.3 Log review

3.4 RISK MANAGEMENT PLANNING

3.4.1 Quantitative analysis

3.4.2 Qualitative analysis

3.4.3 Asset valuation

3.4.4 Safeguard selection

3.4.5 Cost benefit analysis

3.5 PERSONNEL SECURITY

3.5.1 Biometrics

3.5.2 Smart cards & tokens

3.5.3 FORTESSA cards

3.5.4 Other authentication

3.6 PHYSICAL & ENVIRONMENTAL SECURITY

3.6.1 Marking & labeling

3.6.2 Storage media handling

3.6.3 Access control lists

3.6.4 Security testing

3.6.5 Declassification/destruction

3.7 NETWORK SEGMENTATION

3.7.1 DMZ implementation

3.8 INCIDENT REPORTING PROCEDURES

3.9 INCIDENT RESPONSE

3.9.1 Prepare

3.9.2 Identify

3.9.3 Contain

3.9.4 Eradicate

3.9.5 Recover

3.9.6 Follow up

3.10 INFOCON PROCEDURES

3.11 DOCUMENTATION

3.11.1 Security Requirements Traceability Matrix (SRTM)

3.12 PUBLIC KEY INFRASTRUCTURE