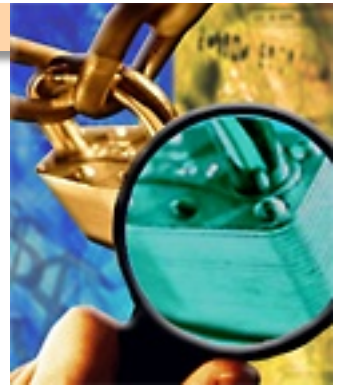
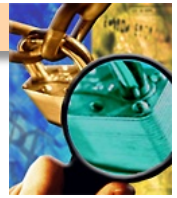


Security Best Practices

Vulnerability Assessment Course

All materials are licensed under a Creative Commons “Share Alike” license.



- **http://creativecommons.org/licenses/by-sa/3.0/**

You are free:

to Share — to copy, distribute and transmit the work

to Remix — to adapt the work

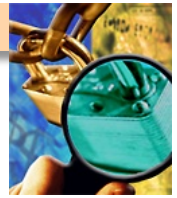
Under the following conditions:

Attribution — You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

Share Alike — If you alter, transform, or build upon this work, you may distribute the resulting work only under the same, similar or a compatible license.

Agenda

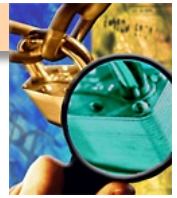
- Security Best Practices
- Assessment Lessons Learned



Best Practices

- Build security in from the beginning
- Establish an approach that protects high value systems from a sophisticated adversary
- Embrace the principles of Defense-in-Depth
- Establish a fault tolerant security model

Security in Design

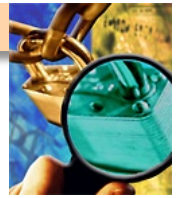


- Up-front design criteria for hosts, networks, applications and systems
- Difficult to retrofit information protection into an environment where none previously existed
- Protection designed into a system should be consistent with the threat to which it is likely to be exposed
- Major consideration should be given to the class of vulnerabilities that are likely to be present in a specific environment

Security in Design (cont.)

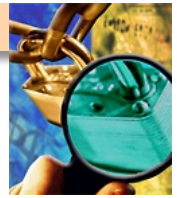
- **Common techniques:**
  - **Provide mechanisms for unique identification and authentication, auditing and discretionary access**
  - **Develop applications that do not require additional software that is not or cannot be secured**
  - **Ensure applications can function on an operating system that has been securely configured, consistent with best commercial and DOD guidelines**

Security Approach



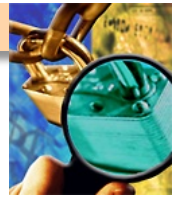
- Identify assets
- Identify potential threats
- Segment networks based on sensitivity and community of interest
- Implement Defense-in-Depth
- Continually re-assess security posture

Common Assets



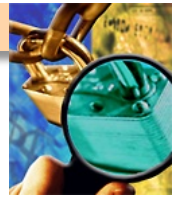
- Office information systems
- Public affairs web server
- Command and control information
- Logistics information
- Personnel information
- Financial information
- Communications infrastructure

Potential Threats



- Accidental loss of data
- Malicious users
- Hackers
- Terrorists
- Directed foreign intelligence collection
- Targeted information warfare attack
- Virus attacks
- Malicious code
- Denial of service

Defense-in-Depth

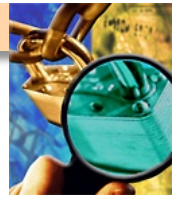


- Security configuration management
- Boundary protection
- Intrusion detection
- Incident response
- Vulnerability assessments
- Anti-virus
- Auditing

Security Configuration Management

- Underlying principle: Ensures individual systems can withstand an attack if perimeter defenses are breached
- Implementation: Individual systems configured such that they are relatively resistant to common attacks
- Common techniques
  - Utilize security configuration guidance (e.g., NSA, DISA, vendor, etc.)
  - Deactivate all network services that are not required for the function a particular system
  - Implement mechanisms for identification and authentication, auditing, and discretionary access
  - Require the use of secure protocols with strong I&A even on internal segments

Boundary Protection

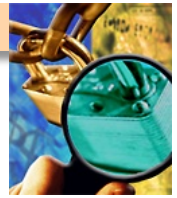


- **Underlying principle: Establishes a perimeter defense for the security domain**
  - **Should be defined based on organization's assets and potential threats to those assets.**
  - **Should be defined to providing a high degree of security while still maintaining the connectivity necessary to meet mission requirements**
  - **Should be defined to maintain the separation of systems based on the function of the system and the community of interest for the data residing on the system**

Boundary Protection (cont.)

- Implementation: Firewalls to provide real-time filtering and routing of authorized connections, unauthorized connections blocked
- Common techniques
  - Filtering/Routing (host by host, network service and protocol level)
  - Deny all policy – rule that denies any traffic that has not been explicitly allowed in or out of the network
  - DMZ for publicly accessible servers
  - Segment systems based on community of interest - e.g. critical C2 from OIS
  - Real-time alerting of malicious connection attempts

Boundary Protection (cont.)



- Implementation: Proxy servers to provide protection for internal web clients from malicious web sites
- Common techniques
  - Strip potentially malicious executable mobile content
  - Shield client IP address – prevents web sites from tracking individual clients
  - Block unauthorized sites – e.g. hacking sites

Anti-Virus

- Underlying principle: Defends individual hosts from infection from malicious code
- Implementation: Memory resident and on-demand scanners for workstations and servers
- Common techniques
  - Multi-level protection scheme: workstations, servers and email scanning
  - Filter capability – ability to filter emails based on subject name, attachments, etc.
  - In-bound and out-bound at gateway

Intrusion Detection

- Underlying principle: Provides the indications and warning that an attack is in progress
- Implementation: Sensors placed on the network and on individual hosts
- Common techniques
  - Multiple methods – one method may not identify all malicious traffic
  - Signature based, policy based, anomaly based
  - Real-time alerting of malicious connection attempts

Incident Response

- Underlying principle: Provides the plan of action for reacting to a successful attack
- Implementation: Procedures to isolate, contain and recover from unauthorized activity
- Common techniques
  - Have detailed plan
    - Evaluation - Determine validity, scope, and other relevant facts
    - Containment - Isolate system so trusted hosts can not be compromised
    - Notification
      - Preserve data required for criminal investigation
    - Eradication
      - Change passwords or re-install OS depending on the scope
    - Recovery - Fix the problem that caused the compromise
  - Exercise tactics and procedures

Vulnerability Assessments

- Underlying principle: Provides the opportunity to address weaknesses before an enemy can exploit them
- Implementation: Scanning tools that identify vulnerabilities in computer hardware, software, networks and operating systems
- Common techniques
  - Multiple packages – one package may not identify all vulnerabilities
  - Ability to identify backdoors behind the security perimeter, e.g. modems, VPNs, etc. – all potential vulnerabilities need to be assessed
  - Correction verification mechanism – ability to check if vulnerability has been eliminated

Auditing

- Underlying principle: Provides a record of actions taken within a system or network environment
- Implementation: Network and host level auditing programs
- Common techniques
  - Enable auditing/accounting
  - Review (system/application, web, firewall, etc.)
  - Centralized logging/analysis

Observations in Network Security

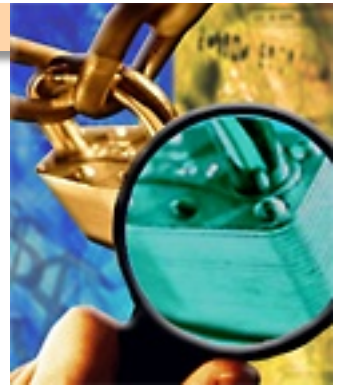
- Firewalls work well
  - The entire network security is dependent on the weakest link
  - Not all assets are behind the firewall
- Operational requirements always dictate some “holes” in the firewall security policy
- Intrusion detection must be used to monitor “holes”
  - If a VPN is used IDS cannot be done at the network perimeter
- Firewalls must be supplemented with host level scanning

Observations in Host Security

- Host security is highly dependent on specific operating system version and individual configuration
  - A constant “patch and wait” problem
  - Security patches often break other things or operational necessity can make applying patches impractical
  - Often patches are not released until after vulnerabilities are being widely exploited
  - Patches for some applications (i.e. IIS, MS SQL server, IE, etc.) are released at a rate which is unmanageable
- It is easier and more effective to block traffic to most hosts, then secure all internal hosts as time permits

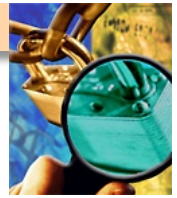
Challenges

- Multiple layers of security can make networks operations and troubleshooting very complex
- Too much dependence on vendors' products developed with rush to market as the goal
  - Security is often overlooked
- Applications developed with a goal of using latest technology instead of meeting the requirement
- Risk mitigations action increase complexity and cost
- Many security recommendations are dismissed because majority do not understand the threat

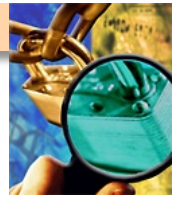


Assessment Lessons Learned

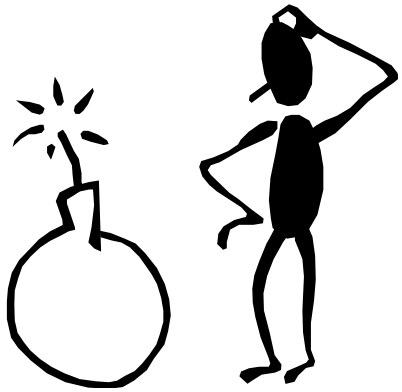
Assessment Process



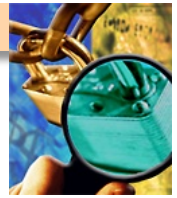
- Preparation Issues
  - Required notification process to organization
  - Organization approval for the assessment
  - Reporting templates useful to all concerned
  - Assessment objects available
  - Staff available to participate
  - Backing
- Preparation of the assessment plan
  - Use any organization specific assessment templates or guidance
  - Organization specific assessment plan
  - Organization approval of the assessment plan
  - Use organization approved tools or formats



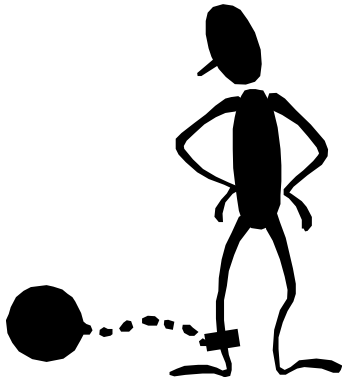
Obstacles



- The “Waiting Game”
- “I don’t understand”
- Scope is inaccurate
- Network diagram is inaccurate
- More systems than previously reported
- Unanticipated technology
- Documentation not availability
- Script outputs not provided
- Appropriate connectivity not provided
- Systems administrators lying, changing script outputs, or making corrections and re-running scripts
- Argumentative systems owners and administrators
- Asked to change finding
- Others...

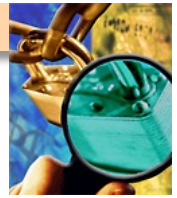


Pitfalls



- Poorly defined scope
- Coming in blind
- Not anticipating common delays
- Relying too heavily on tools
- Relying on a checklist
- Relying on a script
- Reporting false positives
- Not providing the impact of a finding
- Inaccurately characterizing the risk
- No network cable, power cord, other equipment
- Temptation to change a finding
- Arguing with a systems administrator
- *Others...*

Baseline Configuration

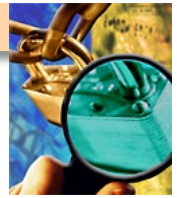


- Organization has not established its own baseline configurations
- Although NSA/DISA established a gold standard, may be too much for some installations and breaks applications
- Baseline configurations are a mandatory control under CM-2 of NIST SP 800-53

Configuration Management

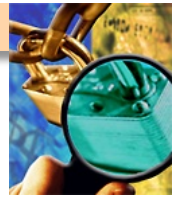
- Systems are inconsistently and improperly implemented- even within the same operational environment
- Many default configurations are still set (CM-6)
- ‘Least Privilege Principle’ is not appropriately implemented (AC-6)
- Unsecure protocols like (ftp, telnet)

Risk Management



- Security Risk Management (RM) needs to be considered right along with other project RM
- Most RM that takes place was for compliance rather than as a tool to help secure the system
- The Risk Assessments done now are of low quality and value – needs to correspond to impact level
- RM must be part of the overall project plan for the application/architecture
- Risk Assessment should be based on organization security policy

Application Security



- Applications remain vulnerable to many different types of attacks
  - Input is not validated
  - Improper session control (AC-11, AC-12)
  - Account Management is (AC-2) often weak and improper
  - Improper error handling messages
- Database application vulnerable to internal threat

Certification and Accreditation

- Many systems operating under an Interim Authority to Operate (IATO) for extended period (CA-6)
- Some systems did not have System Security Plans (PL-2) nor Risk Assessment (CA-2)
- Documents developed by organization to meet requirements, and not to solve issues (Contingency Plans)

Database Security

- Database Baselines are usually not implemented consistently
- Default accounts remain active (AC-2)
- Access management of database account is not secure
- Auditing logs are seldom enabled
- Accountability – confusion on where application DB programmer job ends and the maintainers begins has lead to implementation problems.

Access Control

- The ‘Principle of Least Privilege is seldom implemented correctly (AC-6)
- Systems have excessive ports and protocols enabled providing unnecessary access (CM-6)
- Excessive access were being granted into sensitive databases (AC-2)
- Administrator interfaces open directly to the Internet (AC-17)
- Developers often have full privileges into the production environment (AC-6/SA-8,10)
- Files often had world read, write and execute permissions (UNIX) (AC-4)

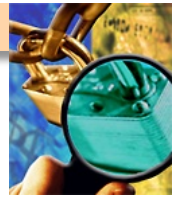
Operating Systems

- **Elements of Assessments**
  - Look at system partitioning
  - Centralized audit log important
  - Look for social engineering opportunities
  - Examine for defense in depth (or lack of)
  - Assessments confirm organization policies
- **Active Assessments**
  - Scan (ping sweep, port scans, OS Detection)
  - Enumerate (users, list file shares, identify applications)
  - Access (password "sniff", file share brute force, SAM DB, buffer overflows)
  - Escalate privileges (crack passwords, known exploits)
  - Pilfer (evaluate trusts)

Services

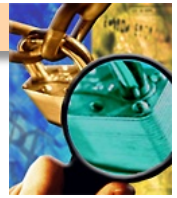
- There are critical security implications of improper DNS configuration
- Thorough evaluation of DNS must be completed
  - Automated tools provide a network view of the service (nessus, nmap, dig, dnswalk)
  - Automated tools will not tell you additional information such as improper ACL's, logging config, transfer hosts and other details
  - Manual review of named.conf or equivalent
- Assessor should have DNS references on hand during review if not familiar with DNS configuration settings

Common Findings



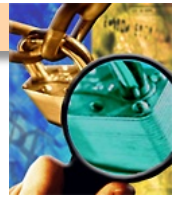
- **Windows Best Practices**
  - Patches and additional software
  - Minimize Network Services (e.g., IIS, AD)
  - Minimize Boot Services
  - Enhance Logging
  - File/Directory Permissions/Access
  - System Access, Authentication, and Authorization
  - User Accounts and Environment
  - System Partitioning
- **Follow best practice and configuration guides**
- **Always set complex passwords and change them often**
- **Perform periodic assessments**

Common Findings



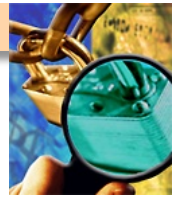
- **UNIX Best Practices**
  - Patches and additional software (e.g., OpenSSH, TCP Wrappers)
  - Minimize Network Services (e.g., inetd, sendmail)
  - Minimize Boot Services
  - Kernel Tuning
  - Enhance Logging
  - File/Directory Permissions/Access
  - System Access, Authentication, and Authorization
  - User Accounts and Environment

Common Findings



- Network Observations
  - Disable unneeded services and protocols
  - Encrypt routing updates with strongest algorithm available
- Poor ACL's
- Lack of Auditing
- Poor Configuration
- Operational requirements always dictate some "holes" in the firewall security policy
- Intrusion detection must be used to monitor "holes"
- Firewalls must be supplemented with host level scanning
- External recursion allowed

Conclusions



- **What have we learned from assessments?**
- The system owners have many controls which are not being addressed
- Need SLA in procurement phase
- The information systems security office has areas that can be improved upon, especially C&A, RA and CP.
- Embedding security into the SDLC is the best methodology NIST 800-64R2
- Accountability is important from the system owner, to OIS, to the vendor implementing the controls
- Standard reporting template would be useful
- Application security tools are not generally available (code analyzer)
- Databases behind firewalls are protected from external threats but still vulnerable to internal threats – focus on securing database application.
- Information security not part of technical architecture

Questions