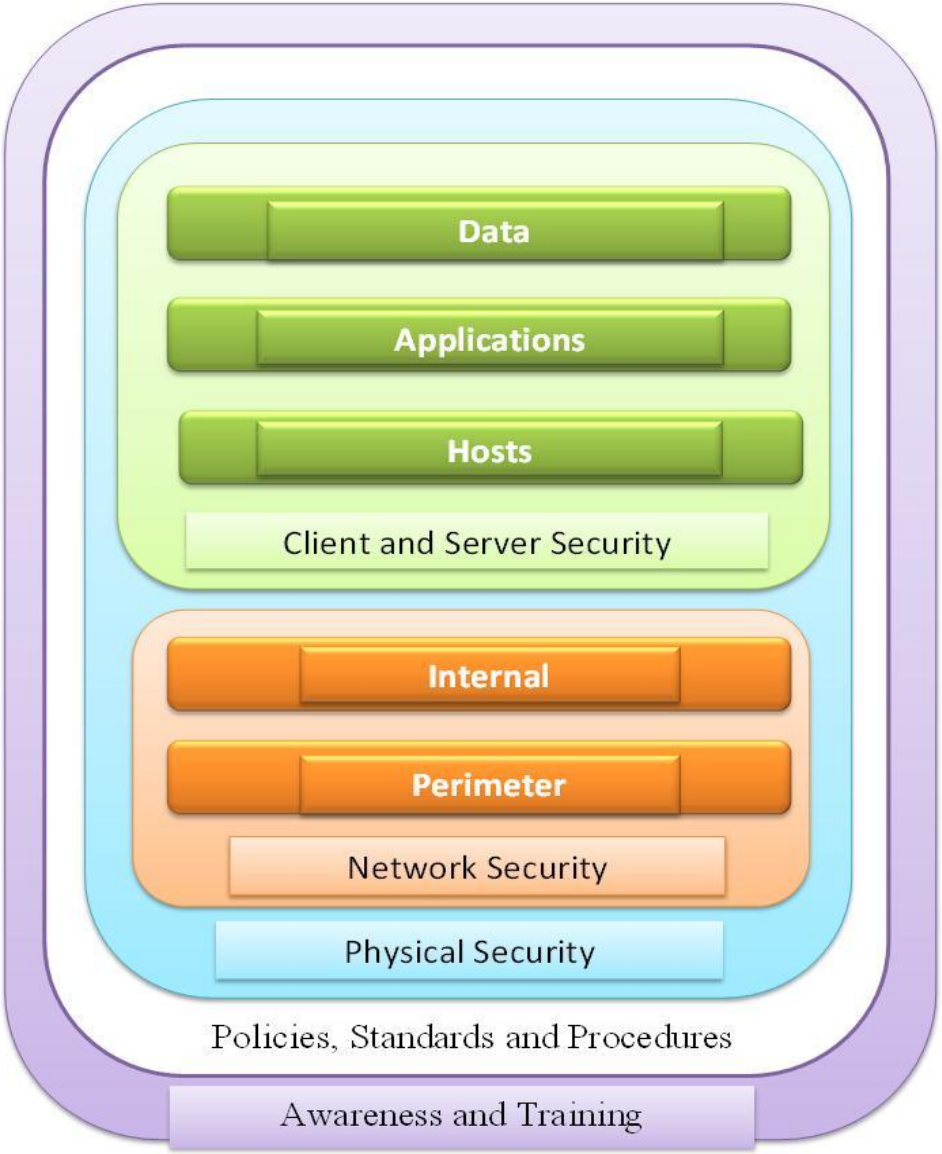
IT Performance and Security Scanning to Expand Defense-In-Depth

Kevin Savoy, MBA, CPA, CISA, CISSP
Director of Hospital and IT Audits

Courtney Oxman, MS, CIA, CISA, CRISC
Associate Director of IT Audits

IT Performance and Security Scanning

- Agenda
  1. Defense in Depth Security Model
  2. What is Scanning?
  3. Physical Security Scanning
  4. Performance Scanning
  5. Network Security Scanning
  6. Client/Server and Host-Based
  7. Industry Trends



Data

Applications

Hosts

Client and Server Security

Internal

Perimeter

Network Security

Physical Security

Policies, Standards and Procedures

Awareness and Training

Defense-in-Depth Security Model

Defense-In Depth Security Model

- Awareness and Training
- Policies, Standards and Procedures
- Physical Security
- Network Security
- Client and Server Security

Model Wrapper

- Awareness and Training

- Deliberately planned and deployed (formal) awareness and training program.

- The ‘glue’ that holds a defense-in-depth model together as it is implemented, operated and maintained.

- Creates an understanding using common terminology, concepts and knowledge.

Model Base

- Policy, Standards and Procedures (PSP)

- Foundation for governance, best practices and 'how to'.
- Affects every other layer in the model.
- **Policy** that requires a documented **IT Performance and Security Scanning Plan**.
- **Standards** provide guidance on the plan's design and contents, where to implement and what tools to use.

What Is Scanning?

- Scanning is an automated process or program that searches (monitors) for certain conditions in a continuous, periodic or ad hoc manner.
- The results of a ‘hit’ can be a log, report or alert or it can initiate/trigger another process.
- Includes robust program suites like Nessus or custom scripts or ‘triggers’ searching logs or event activities.
- IT industry does scanning in many different forms.

Physical Security Scanning

- **Badge and Biometric Access:** Afterhours, weekends and holiday access monitoring and reporting/alerting.
- **Master Key Use:** Intended to allow fire and police access, use of master key should be monitored and reported/alert.
- **Open Doors:** Propping doors open or lock not re-engaged should be reported/alert.
- **Motion Detectors:** Activated by movement to produce reporting/alert.
- **Communication of Alerts:** Where is your reporting/alert going? Properly staffed and monitored to make use?

Performance Scanning

- Often network traffic or database monitoring and analysis, can be used to identify attacks such as DoS.

- **NetQoS** is a network management software for performance management and response time analysis. QoS=Quality of Service.
- Noted by both Forrester and Deloitte
- Targets network interface or a given server or router or specific applications.
- For internet applications such as VoIP, Video-on-demand or other consumer services.

Network Security Scanning

- Referred to as ‘**Vulnerability Scanning**’ plays a critical role in enterprise vulnerability management.
- Scans and detects vulnerabilities on client PCs, servers, routers, firewalls, network appliances and system software and applications.
- Vulnerabilities detected include open ports, back doors, poorly written scripts and unpatched operation systems.

Network Security Scanning Examples

- **Nessus:** One of the most popular and capable, particularly for Unix.
- **Qualys:** Software as a service (SaaS) solution, web-based with network discovery/mapping, asset prioritization, reporting and remediation tracking.
- **MBSA:** Microsoft Baseline Security Analyzer determines security state based on Microsoft security recommendations.
- **Rapid7 Nexpose:** Designed to support entire vulnerability management lifecycle (discovery, detection, verification, risk classification, impact analysis, reporting and mitigation).

Network Security Scanning

- Can be performed from the outside looking in or from the inside looking around.

- **External:** Working from the cracker’s viewpoint.
- **Perimeter:** DMZ containing hosts most vulnerable to attack (email, web, DNS servers, etc.).
- **Internal:** Inside using elevated trust and privileges.

Client/Server and Host-Based

- **Center for Internet Security (CIS):** Now has a *Security Benchmark Division* providing best practice for security configurations.
- Benchmark configuration standards for different operating systems such as UNIX, Solaris, etc.
- Using CIS security benchmarks to configure IT systems has been shown to eliminate 80-95% of known security vulnerabilities.
- Global de facto standard for IT security configurations.
- Their benchmark scanning is host-based.

Client/Server and Host-Based

- **Web Coding Scanners:** Specific to web codes, scans program code to identify vulnerable/exploitable code.
  - Coupled with training on secure coding, effective means of reducing risk of hacks. Use in SDLC, testing.
- **Web Application Scanners:** Scanning programs which go through the web front-end to identify potential security vulnerabilities in the web application.
- **IBM AppScan:** Prominent web application vulnerability scanner with enterprise product licensing.
- **MosaicSecurity.com:** List of web application scanners.

Client/Server and Host-Based

- **Application Firewalls:** Controls input, output and access to, from or by an application or service.
- Monitors and blocks input, output or system service calls not meeting firewall's policy.
- Two types-Network and Host-Based Application Firewalls.
- Creates logs that can be scanned for reporting/alerts.

Client/Server and Host-Based

- **Database Scanners:** Programs scanning database to find vulnerabilities to bypass controls, break into the database or compromise the system.
  - IDs improper configuration settings along with known weaknesses in the database software.
- **Database Logging and Audit Trails:** Use of customized scripts or ‘triggers’ to identify high-risk activities or events and initiate reports/alerts.

Industry Trends

- **Convergence and Product Suites:**
- Scanning tools are merging multiple techniques and approaches into what is referred to as a '**convergence**'.
- Often referred to as a software or product 'suite'.
- For example, **Nessus**, traditionally a network security product, has a 'plug-in' module for scanning database compliance. Operating system related modules can also be obtained.
- **Subscriptions:** 3rd Party used to run scans and/or interpret scans or logs for reporting, alerts or to initiate mitigating actions.

Audit Considerations

Review and evaluate IT performance and security scanning strategies, plans and practices as they may apply to the following areas:

- Network
- Database
- Operating System
- (Web) Code Development
- Vulnerability Assessment
- Intrusion Detection and Prevention
- Antivirus

Audit Considerations

- Review Related Strategies and Plans
- Review Related Policies, Standards and Procedures
- Review Standards for Scanning Tools Used
- Review Tool Deployment Plans
- Review Remediation Management
- Review Metrics Maintained and Reporting

Related References:

- **The Open Web Security Project (OWASP):** https://www.owasp.org global non-profit focused on improving (web) software security.
- **Microsoft Patterns and Practices:** http://msdn.microsoft.com, Chapter 4 Design Guidelines for Secure Web Applications.
- **Gartner, Inc.:** http://www.gartner.com, leading global IT research and advisory company providing insight for strategic and operational IT decision making. Client base with corporate, government and educational sectors.

Related References

- **SECTOOLS.ORG:** http://sectools.org/tag/web-scanners/, Top 125 Network Security Tools, web scanners and vulnerability scanners.
- **NIST:** http://www.secureworks.com/research/articles/orther_articles/security-web-applications/
- **Does any one have suggestions based upon their experiences?**