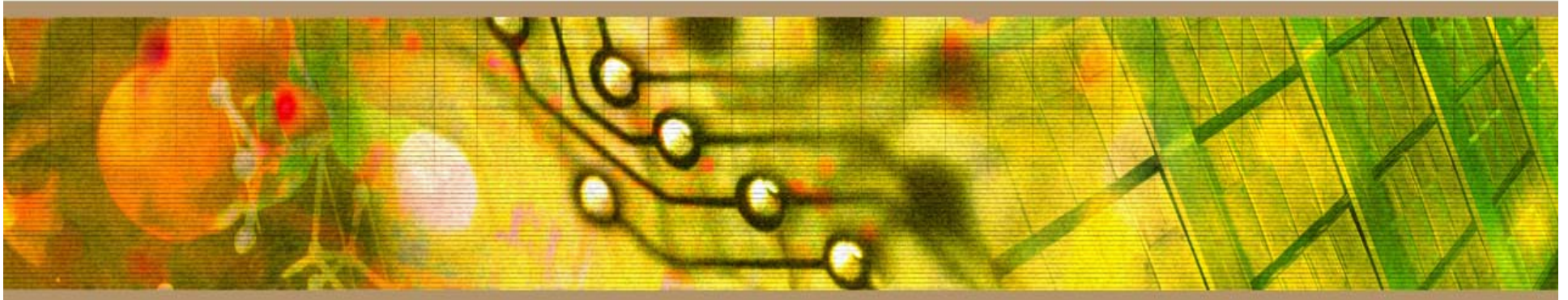




ITNS and CERIAs CISSP Luncheon Series: Operations Security



Presented by Greg Hedrick, CISSP



- From (ISC)2 Candidate Information Bulletin:
 - Operations security is used to identify the controls over hardware, media, and the operators with access privileges to any of these resources. Audit and monitoring are the mechanisms, tools and facilities that permit the identification of security events and subsequent actions to identify the key elements and report the pertinent information to the appropriate individual, group, or process.

- From (ISC)2 Candidate Information Bulletin:
 - The candidate will be expected to know the resources that must be protected, the privileges that must be restricted, the control mechanisms available, the potential for abuse of access, and the principles of good practice.

- Due care and Due Diligence efforts:
Continual effort to make sure that the correct policies, procedures, standards, and guidelines are in place and are being performed.
- This includes safeguards and countermeasures to protect resources, information, infrastructure.

- Administrative Management Controls
 - Separation of Duties
 - Job Rotation
 - Least Privilege
 - Mandatory Vacations

- **Accountability**
 - Auditing must take place as a routine matter
 - » Limited and controlled access
 - » Capturing and monitoring audit logs
 - » Helps to identify an environment that is moving away from the baseline (e.g., “Clipping Level”)

- Security Operations and Product Evaluation
 - “Operational Assurance:” Focuses on the product’s architecture, embedded features, and functionality.
 - » Examples include access control mechanisms, separation of privileged and user program code, and audit capabilities.

- Security Operations and Product Evaluation
 - “Life Cycle Assurance:” Pertains to how the product was developed and maintained.
 - » Each stage of a product’s life cycle has standards and expectations it must fulfill before it can be deemed a highly trusted product.

- Transparency is important
 - The security mechanisms and controls put in place must have a degree of transparency to allow users to be able to perform duties without extra steps to satisfy security.
 - BUT, transparency also does not disclose unnecessary information about the controls (so that they cannot be attacked or circumvented).

- Configuration Management
 - Every organization should have in place a policy for dealing with change.
 - “Change Control:” The management of security features and the implementation of levels of assurance through the diligent control of all changes made to a system’s hardware, software, and firmware configurations throughout the development and operational life cycle.

- Configuration Management
 - Example change policy steps:
 1. Request for change
 2. Approval of change
 3. Documentation of change
 4. Tested and presented
 5. Implementation
 6. Report change to management

- Media Controls
 - Preservation
 - Integrity, confidentiality, availability
 - Disposal
 - » Know the methods to sanitize
 - » Know “data remnance:” residual physical data (information that was saved and then erased).

- Trusted Recovery
 - This is how systems recover from a failure. The emphasis is on secure recovery (no exposure of information while in recover mode)
 - » System reboot
 - » Emergency system restart
 - » System cold start

- Network and Resource Availability
 - “Single point of failure:” Using one device or communications line to perform a function (or multiple functions). In order to ensure continuous operation, two or more devices or lines should be used for redundancy.
 - Examples of SPOF devices: Firewalls, routers, network access servers, T1 lines, bridges, hubs, etc.
 - Best defenses: Proper maintenance, regular backups, redundancy, UPS.

- Redundant Array of Inexpensive Disks (RAID)
 - Technology used for redundancy and performance improvement.
 - Combines several physical disks and aggregates them into logical arrays.
 - Appears as a single drive to applications/devices.
 - » Know RAID levels
 - 1 (Mirroring)
 - 3 (Byte level parity)
 - 5 (Interleave parity)
 - 15 (combination of levels 1 & 5)

■ Clustering

- Is a fault tolerant server technology that is similar to redundant servers, except each server takes part in sharing services.
- “Server cluster:” A group of servers that are viewed logically as one server to users and can be managed as a single logical system.

- Email Security
 - Know how Email works:
 - » Simple Mail Transfer Protocol (SMTP)
 - » Transmission Control Protocol (TCP)
 - » Post Office Protocol (POP)
 - » Internet Message Access Protocol (IMAP)

- “Spoof Email:” To alter the name in the “from” field.
- “Phishing Email:” Act of sending spoofed email messages that pretend to originate from a source that the user trusts and has a previous relationship with.

- Fax Security
 - Information scanned and transmitted may be sensitive, and may be able to be viewed upon receipt by an unintended viewer.
 - Fax servers
 - Fax encrypter: A bulk data-link encryption mechanism that encrypts all data that hits the network cable/telephone wire.

- Who are the hackers anyway?
 - » Black hats (the “bad” hackers)
 - » White hats (security professionals)
 - » Script Kiddies (moderately skilled)

- Network mapping and port scanning
 - Network mapping tools send out seemingly benign packets to different systems on the network, and use the response to find out information about the infrastructure.
 - Operating System Fingerprinting: Tools to map operating system, applications, and versions to the type of response and message fields they use. (e.g., response to a standard ping.)

- Network mapping and port scanning
 - Port scanning: Identifies open ports on the computer.
 - TCP wrappers: Software components that monitor incoming network traffic and control what can and cannot access services mapped to specific ports.
 - » Know common port numbers.

- Browsing: General information gathering technique (looking through files, garbage, saved storage media, shoulder surfing, etc.)
- Network sniffers: Tools that monitor traffic as it traverses a network.
 - » Can be used as a hacking or diagnostic tool.

- Session Hijacking: Attacker hijacking sessions between two users without being noticed.
 - » Know countermeasures
- Loki Attack: Uses the ICMP protocol for communications purposes. Data is written right behind the ICMP header (creates covert channel).
- Password Cracking

- Attacks and Concepts to be familiar with:
 - Backdoor
 - Denial of Service (DoS)
 - Man in the Middle
 - Mail Bombing
 - Wardialing

- Attacks and Concepts to be familiar with (pt. 2):
 - Ping of Death
 - Fake Login Screens
 - Teardrop
 - Traffic Analysis
 - Slamming and Cramming
 - Shoulder Surfing

- Penetration Testing
 - Is the process of simulating attacks on a network and its systems.
 - Is conducted at the request of the owner.
 - The goal is to test and possibly bypass security controls of a system and report the vulnerabilities to the owner of the system.

- 5 Step Process for Pen Testing
 1. Discovery
 2. Enumeration
 3. Vulnerability Mapping
 4. Exploitation
 5. Report to Management

- Degrees of Knowledge for Pen Testing
 1. Zero Knowledge
 2. Partial Knowledge
 3. Full Knowledge

Questions?