Paul Collado

CSC-116-71

Homework 9

1. Physical Security is an aspect of information security that addresses the design, implementation, and maintenance of countermeasures that protect the physical resources of an organization

2. The four categories are:

1) Manual locks: are installed into doors, and they can only by changed by highly trained locksmiths

2) Programmable locks: can be changed after they are put in service, allowing for combination or key changes without a locksmith and even allowing the owner to change to another access method

3) Electronic locks: can be integrated with sensors to create various combinations of locking behaviors and lend themselves to uses where they can be activated or deactivated by a switch controlled by an agent

4) Biometric locks: this includes finger, palm, and hand reader, iris and retina scanners, and voice and signature readers fall into this category

3. The most common form of alarm is the burglar alarm

4. The most serious threats within the realm of physical security are:

a) Act of human error of failure, potential deviations in quality of service by service providers and power irregularities

b) Deliberate acts of espionage or trespass, acts of information extortion, acts of sabotage or vandalism, acts of theft, software attacks, and comprises to intellectual property; acts of God

c) Forces of nature, technical failures, technical hardware failures or errors and technical software failures or errors, and management failures

d) Technical obsolescence

Homework 10

1. The three major steps in executing the project plan are:

1) Planning the project: It usually assigned to a project manager o champion, the individual manages the project and delegates parts of it to other decision makers

2) Supervising tasks and action steps: a suitable person from the information security community of interest is designated to supervise

3) Wrapping up: It’s usually handled as a procedural task and assigned to a mid-level IT or information security manager, they collect documentation, finalize status reports and deliver a final report and a presentation at a wrap-up meeting

2. Projectitis is the phenomenon of becoming so engrossed in project administration that the project itself suffers

3. The four basic conversion strategies are:

a) Direct changeover: involves stopping the old method and beginning the new

b) Phased implementation: It’s the most common conversion strategy and involves a measured rollout of the planned system, with a part of the whole being brought out and disseminated across an organization before the next piece is implemented

c) Pilot implementation: The entire security system is put in place in a single office, department, or division, and issues that arise are dealt with before expanding to the rest of the organization

d) Parallel operations: Involves running the new methods alongside the old methods

4. Technology governance is a complex process that an organization uses to manage impacts and cost caused by technology implementation, innovation, and obsolescence; and change control is a process to assure an organization that changes to systems are managed and all parties that need to be informed of the planned changes

Assignment #2

**Full name**: Directory traversal vulnerability

**Description**: In the web-based management feature on the TP-LINK TL-WR841N router with firmware 3.13.9 build 120201 Rel.54965 and earlier allows remote attackers to view the router configuration and password

**CVE Tracking number**: CVE-2012-5687

**Date of publication**: 2012-11-01

**URL Link**: <http://www.cvedetails.com/cve/CVE-2012-5687/>

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Full name**: Groupon Redemptions Vulnerability

**Description**: The groupon redemptions app for android does not verify that the server hostname matches a domain name in the subject’s Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate

**CVE** **Tracking** **number**: CVE-2012-5809

**Date of publication**: 2012-11-04

**URL Link**: <http://www.cvedetails.com/cve/CVE-2012-5809/>