CIS 481 – Intro to Information Security

IN-CLASS EXERCISE # 12

Names of team members: Volodymyr Bestiyanets, Nick Cunningham, Timothy Mahan, and Shawn Nasr.

Logistics

A. Get into your regular team
B. Discuss and complete the assignment together. Don't just assign different problems to each teammate! That defeats the purpose of team-based learning.
C. Choose a recorder to prepare the final copy to submit to instructor in Blackboard.

Problem 1
List and briefly describe the five domains of the security maintenance model recommended by the text. See Figure 12-4 on p. 651 of the text for an overview. (10 pts.)

The five domains of the security maintenance model that the text recommends the following: external modeling, internal modeling, planning and risk assessment, vulnerability assessment and remediation, and readiness and review. The external modeling domain is the part of the maintenance model that evaluates external threats to the organization's information assets and provides preemptive awareness of new and upcoming threats, vulnerabilities, and attacks in order to execute effective and prompt defense methods. Internal monitoring focuses primarily on the identification, assessment, and management of the configuration status of an organization's information assets. This domain's purpose is to realize an informed awareness of the state of the organization's networks, information systems, and information security defenses. Planning and risk assessment is the domain that focuses monitoring the whole information security program by identifying and planning continuing information security activities that result in decreased risk. The risk assessment group identifies and documents any risks that are introduced by IT projects or information security projects. Vulnerability assessment and remediation domain is the part of the maintenance model which specifically identifies documented vulnerabilities by performing various assessments and then correcting them promptly by removing or repairing any flaws in information assets that cause vulnerabilities, or by removing the risk related to the vulnerability. Readiness and review aims to maintain the intended functionality of the information security program and make continuous improvements to it over time by using policy reviews, program reviews, and rehearsals.

Problem 2
Is the term *ethical hacker* truly an oxymoron? What's the difference between a pen tester and a hacker? See pp. 667-669 of the text for more information. (7 pts.)

The modern interpretation of hacker makes the term ethical hacker an oxymoron. The general understanding of society is that a hacker is one who will attempt to gain unauthorized or illegal access to a computer and attempt to modify it or one of its programs. It's hard to see any sort of hacker as ethical, since hackers act in a generally destructive manner to achieve various ends. A penetration tester on the other hand, is really just a hacker working to secure a system rather than break into and modify it. A pen tester will check systems for vulnerabilities, and sometimes even see how far they can get before security measures would detect a real attack. The information gathered from such activities is then used to assess further measures an

organization could take to secure a system against further such attacks, possibly from real malicious entities.

Problem 3
Describe the basic methodology involved in most all digital forensics investigations (listed on p. 680). (8 pts.)

Digital forensic investigations done today involve a step by step process in order to accurately collect and catalog evidence. First and foremost forensics involves a crime scene and percussions have to be taken in order for an investigation to legally take place. After that evidence must be collected in a specific way in order for the evidence to keep it's integrity. Any compromised evidence collected or evidence collected in an unauthorized way may not hold up in court. All potential evidence must first be identified, then the process of collecting such evidence may begin. For evidence to be used in a court of law it must be uncompromised, this means undamaged and unaltered. Once the evidence has successfully been collected it can be analyzed for authenticity. During this step it is apparent that the evidence must not become altered in any way. After analysis, evidence can be reported to the proper authorities.