Assignment One

Computer Security Incident Handling Guide

Please read the sections specified in Table One from NIST's Computer Security Incident Handling Guide (NIST SP 800-61). [1] Based upon your reading, answer the questions that follow.

#	Chapter Title	Pages
2	Organizing A Computer Security Incident Response Capability	15
3	Handling an Incident	27
4	Handling Denial of Service Incidents	12
5	Handling Malicious Code Incidents	10
6	Handling Unauthorized Access Incidents	8
7	Handling Inappropriate Usage Incidents	5
8	Handling Multiple Component Incidents	3
9	Browse Appendix A	

Table One

Questions

Based on your reading of NIST 800-61, briefly answer the following questions.

1. In the context of NIST 800-61, what is an incident?

2. Provide examples of three different types of incidents.

3. What is incident response?

4. Why is incident response important?

5. Describe the importance of communications during incident response.

6. Name both external and internal entities with which communications needs to be maintained.

7. What does NISST 800-61 define as a "jump kit"?

8. For your online blog, find a current article that relates to incident response. Write a brief, one to three paragraph, article concerning why you choose that article and why it is relevant to incident response.

Prior to the next class, place the document online. Make the document accessible from our Online Class Group.

Journal Article One

For next week's Journal Article select an article that deals with a computer crime that could have had its impact lessoned by an appropriate incident response. Be sure to specifically describe how an appropriate incident response could have lessoned the impact of the crime.

Outside Reading

For next week, read "Corporate Forensics Class Design with Open Source Tools and LiveCDs." [2] While this paper is dated, it remains relevant. Come to the next class prepared to discuss the similarities and differences between Law Enforcement and Corporate Forensics. (Note that originally the first class lecture was based on this paper.)

1. http://csrc.nist.gov/publications/PubsSPs.html

2. http://www.tech.uh.edu/cae-dc/documents/CORPORATEForensicsCrowley.pdf