Assignment Two

Guide to Integrating Forensic Techniques into Incident Response

In addition to the readings in your text, please read the specified sections of NIST's Guide to Integrating Forensic Techniques into Incident Response (NIST SP 800-86). [1] Based upon your readings, answer the following questions.

	Chapter Title	**Pages**
2	Establishing and Organizing a Forensics Capability	8
3	Performing the Forensic Process	7
4	Using Data from Data Files	15
5	Using Data from Operating Systems	12
6	Using Data from Network Traffic	18
7	Using Data from Applications	10
8	Using Data from Multiple Sources	5
9	Browse Appendix A	

Table One

Based on your reading (NIST 800-86), answer the following questions.

1. Name and briefly describe the four process phases for performing digital forensics.

2. Name the three organizational groups that are the primary forensic tool users.

3. What is incident (handling) response?

4. What is an incident response team?

5. When reporting an incident, what information should be provided?

6. Name and describe four categories of tools that should be available to respond to an incident.

7. What is a Denial of Service (DoS) attack?

8. Name and describe five DoS attack containment strategies.

9. Briefly define malicious code.

10. Briefly define an unauthorized access incident. Give several examples.

11. Briefly describe a multiple component incident.

Journal Article Two

For next week's Journal Article select an article that deals with an incident that has Intrusion Detection or Network Security Monitoring attributes. Better journals will explain the relationship between Intrusion Detection and Incident Response.

Outside Reading Two

For next week, read "An Extended Model of Cybercrime Investigations." [2] Based upon your reading of the paper, answer the following four questions.

1. Why is a good model of cybercrime important?

2. Typically, how is the awareness created that an investigation is needed? Give two different types of examples.

3. What is the largest single gap in the existing models that the proposed model remedies?

4. According to the author, what makes this model more comprehensive than previous models?

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

2. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.80.1289&rep=rep1&type=pdf