13.2 Laboratory Exercise

In this laboratory exercise, the student will be introduced to the stages of incident response and apply incident response concepts to mock incidents.

Introduction to Incident Management and Response

13.2.1 Specifications

This laboratory exercise will not require any technology. Rather, perform the exercises on your own, or with a partner(s).

13.2.2 Learning Objectives

- Identifying Types of Incidents
- Familiarity with Stages of Incident Response
- Assessing Incident Response Plans
- Applying Incident Response Plans
- Documenting Cyber Incidents
- Qualities of an Effective Briefing

13.2.3 Mapping to NIST Nice Framework

This laboratory exercise is intended to increase the student's skills in the area of incident response. At cyber defense competitions, students can expect to suffer from a range of cyber incidents. Skills including documenting, responding to, and briefing on cyber incidents are necessary to perform well at competitions. This laboratory exercise maps to the following KSAs from the NIST NICE Framework:

- Cybersecurity and Privacy Principles (K0004)
- Cyber Threats and Vulnerabilities (K0005)
- Hacking Methodologies (K0310)
- Documenting Reported Incidents, Problems, and Events (K0317)
- Recognize Types of Vulnerabilities (S0078)
- Accurately Define Incidents, Problems, and Events (A0025)

13.2.4 Necessary Background

This laboratory exercise does not have any necessary background. Familiarity with cyber incidents and the incident response process may be helpful but is not required. Because the exercises are open ended, expected completion time will be omitted. If being conducted in a course or other time-constrained environment, adjust the amount of time allocated for each challenge.

13.2.5 Challenges

1. *Types of Incidents* There are many different types of cyber incidents. Each with specific capabilities and purposes.

   For this task, you will be matching types of cyber incidents, seen in table 13.1, with their descriptions, seen in table 13.2.

2. *The Stages of Incident Response*

   The incident response process is well documented with many suggested procedures to go

Malware
Phishing
Denial of Service
Ransomware

Table 13.1: *Types of Incidents*

This type of incident typically uses email as its medium of attack. The malicious user sends an email pretending to be a legitimate sender and aims for the target to either click a malicious link or download a malicious file.
This type of incident typically involves locking the targets assets by encrypting their hard drive. The malicious user promises to unlock the targets assets upon receiving a sum of money.
This type of incident typically involves flooding a targets asset with so much traffic that it is unable to operate properly. The malicious user sends a mass of network traffic to the target system until it crashes or is otherwise unable to perform its intended task.
This type of incident is categorized by malicious code or software. The malicious user crafts special code to compromise the security of the target system in hope to steal data or damage the target system.

Table 13.2: *Incident Type Descriptions*

from preparing for the incident to post incident analysis.

For this task, read the mock incident response seen in table 13.3. It will have the incident response steps in it using specific terminology. Using the scenarios, try to identify the stages of incident response. The stages in the plan being referenced map to the NIST and SANS incident response frameworks. Compare your list with the list in the solutions.

3. *Assess an Existing Incident Response Plan*

   Organizations do not always have the best incident response plan in place. Sometimes this can lead to certain actions not being performed and specific evidence not being collected. In addition to letting certain aspects of the incident go unattended to, this can lead to the organization not having enough evidence or information to take the incident to court if the suspected perpetrators are determined.

   For this task, read the stages of the poorly designed incident response plan with vague terminology below. Using these stages, explain the steps you would take to respond to the incidents described below. Then assess the strengths and weaknesses of the poorly

Response	At MeCorp Energy, we recently had a cyber incident. Our team had prepared for a potential incident by contracting with a cyber assessment team who performed an assessment of our infrastructure to determine where our weak points were. Our organization identified that the attack was a standard Denial of Service attack. Further analysis revealed that the attackers used a SYN flood attack which affected our NA-West web servers. In an effort to contain the incident, upon detection, we took our NA-West server offline to prevent the incident from spreading. Once we were able to figure out how the attackers were accomplishing the SYN flood, we were able to use additional firewall rules to eradicate the attackers from our systems. We have since began working to improve our firewall rules to recover from the incident. Our team is currently performing a post incident analysis to identify the attackers and implement any findings into our incident response plan.

Table 13.3: *Sample Incident Response*

designed incident response plan.

Poorly Designed Incident Response Plan

(a) Detect the Incident

(b) Get Rid of the Threat

(c) Involve Law Enforcement

Mock Incident #1

XYZ Technologies is reporting on a recent cyber incident. On the 19th of September, 2019, at 7:43PM, our operations center detected an incident. A staff member of our administrative team received an email from their internet service provider on a personal laptop. The email was part of a phishing scheme which included a downloadable billing statement. Upon downloading the billing statement, a malicious file began running on the personal laptop. Unfortunately, the laptop was connected to the XYZ Technologies internal network, causing the malware to spread to other machines on the network.

Mock Incident #2

Delicate Deserts and Drinks has received confirmation that a recent global ransomware campaign has affected our systems. At approximately 4:27AM on April 13th, 2018, one

of our employees documented an inability to open our inventory spreadsheet for the day. Upon inspection, the file system on the affected machine is encrypted and requires a payment of $500 equivalent in Bitcoin. At present, no other machines appear to be infected, though customers commonly bring personal laptops and connect to the same network our systems are connected to. Our doors open at 7:00AM.

Mock Incident #3

The public relations manager at Ponderosa Regional Medical Center reported a loss in power in certain parts of the hospital at 5:34PM on February 11th, 2003. At present, the exact cause is unknown, though there is suspicion that the outage is the result of a cyber attack. An intern at the hospital reports that they found a thumb drive outside the hospital earlier that morning and plugged it into their workstation on the cardiac floor. Shortly thereafter, the cardiac floor lost power. Backup generators have been activated to avoid loss of life.

From here, using the poorly designed incident response plan, discuss how you would respond to the incident.

4. *Develop a New Incident Response Plan and Document*

   Incident response is not static. It is constantly improving, with new takeaways being implemented after each incident encountered.

   For this task, given the same mock incident from task 3, design a new incident response plan. Use this new plan and explain what steps your organization would take to respond to the same incidents in task 3. Explain why your plan is improved from the poorly designed plan. Additionally, document any details from the incidents that you feel are necessary.

5. *Brief Audiences on Incidents*

   After an incident, briefing an appropriate audience may be necessary. Briefings need to include enough detail to satisfy the audience but not so much that they may interfere with any ongoing incident response processes.

   For this task, practice briefing an audience based on the outcome of your discussion for

carrying out the new incident response plan. See the solutions for some key points to note.