Lab 11 - Business Injections

Table of Contents

Lab Descriptors

Logistics

Due Date:	December 4, 2020 at 11:59pm
Submission Location:	iLearn for documents, cyber range environment for systems
Points Available:	20

Objectives

To accurately document incidents.

Assumptions

The student has completed labs 1-10 and has started lab 11.

Outcomes

The student will be able to report incidents correctly. The incident reports will tell the instructor everything that has happened with a system and allow the instructor to offer guidance without ever seeing the system.

Topics Addressed

- CSF - 4 Basic Risk Assessment
- CSF - 10 CIAAA-NP
- CSF - 13 Security Mechanisms
- CSF - 14 Malicious Activity Detection
- CSP - 1A - 1N Core Cyber Principles
- ISC - 1A Non-Storage Devices
- ISC - 2 Storage Devices
- ISC - 3A-3B Virtualization / Cloud
- ISC - 5 Networks
- ISC - 12A OS and Application Updates
- ISC - 13A Vulnerability Windows
- BNW - 4 Common Network Devices
- BNW - 6 Network Services
- BNW - 6 Network Applications
- BNW - 8 Use of basic network administration tools
- LSA - 2 User Accounts Management
- LSA - 3 Command Line Interfaces
- LSA - 4 Configuration Management
- LSA - 5 Updates and Patches
- LSA - 7 Managing System Services
- LSA - 8 Virtualization
- OSA - 2 User Accounts Management
- OSA - 3 Command Line Interfaces
- OSA - 4 Configuration Management
- OSA - 5 Updates and Patches
- OSA - 7 Managing System Services

- OSA - 8 Virtualization
- WSA - 2 User Accounts Management
- WSA - 3 Command Line Interfaces
- WSA - 4 Configuration Management
- WSA - 5 Updates and Patches
- WSA - 7 Managing System Services
- WSA - 8 Virtualization

NICE Framework Categories

- Securely Provision (SP)
- Operate and Maintain (OM)
- Analyze (AN)

Introduction

Knowing how to properly document an incident is one of the most important skills in cybersecurity. Businesses often face attacks, and documentation is a key component after these occur. These documents will help form remediation plans or help determine the cause of the breach.

Lab Details

Select a single incident that you found on any of the machines and fill out the following forms from the link below:

- Incident Identification
- Incident Survey
- Incident Containment
- Incident Eradication

https://www.sans.org/score/incident-forms .

Additional Information

Do not use the **contact form** or the **communication log**.

Deliverables

1. The incident response report with a block for each of the incidents found. This report is from last class and is less paperwork, but is still important. (Include screenshots if you took any)

2. The full incident report for the single incident you selected. This full report will be exactly what will be required for all incidents for a real business.

3. Come up with a remediation plan for the incident. Keep it short.

Resources

Sans Forms

https://www.sans.org/score/incident-forms

How to document a security incident

https://resources.infosecinstitute.com/how-to-document-security-incidents-for-compliance-in-10-steps/#gref