CSC 4570/5570 – IT Security
Fall 2020

Lab 11 - Incident Response

Table of Contents

Lab Descriptors

Logistics

Due Date:	December 4, 2019 at 11:59pm
Submission Location:	iLearn for documents, cyber range environment for systems
Points Available:	20

Objectives

- Gain root or Administrative access to machines that have lost it.
- Remove malware from systems.
- Patch systems for vulnerabilities.
- Regain normal business function.
- Write detailed incident reports on what transpired.

Assumptions

The student has completed labs 1 - 5 and or has adequate knowledge of Windows and Linux systems.

Outcomes

The student will regain lost administrative access to the machines and regain normal business functions. The student will be able to research and write a report based on the events that transpired. The student will give suggestions for what could have been done to prevent this from happening.

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

You have been hacked! Attackers have exploited numerous vulnerabilities in our systems and have gained administrator and root access. Pompeii needs you to find a way around the malware infested machines and regain control. Pompeii is losing $10,000 per hour that they are down.

Lab Details

The new environment is located under Classes/vulnsec2020/teamx
Have fun.

WWW Server

Login: **user** Password: **toor** or **useruser**

1. The website is broken.
2. The website is being blocked by browsers.. It might have malware in it
3. Make sure ftp works
4. Someone suggested we might have a rootkit? Whatever that is.
5. Do not allow any data to be exfiltrated by attackers
6. Possible ransomware
7. Fill out incident report

Active Directory (AD)

Login: Administrator P@ssw0rd!

1. Remove malware from the machine
2. Protect FinancialLogs on Desktop
3. Possible keyloggers
4. Possible ransomware
5. Fill out an incident report for each incident found.

Windows 10 Workstation

Login: **user** Password: password

1. Remove malware from machine.
2. Possible keyloggers
3. Make sure data is secure.
4. Fill out an incident report for each incident found.

Deliverables

Fill out the provided incident reports
Business tasks will be given to complete during the next lab.

Resources

Recover Windows from Malware

https://www.itbusiness.ca/news/how-to-recover-your-pc-from-a-malware-attack/15019

SSH

https://linux.die.net/man/1/ssh

Windows Task Manager

https://www.digitalcitizen.life/7-ways-launch-task-manager-windows-8

Linux Find Hidden Files

https://askubuntu.com/questions/468901/how-to-show-only-hidden-files-in-terminal