# Cybersecurity

# **Project 3.2.6 Eradicate the Vulnerabilities**

Copy and paste screenshots and/or answer questions from the activity.

**Vulnerability #1: Unreal Backdoor Detection 46882:**

Reconnaissance/Scanning:

1. Describe how you would have found this vulnerability. Zenmap
2. Based on your findings, what do you know about this vulnerability? The version and information about the vulnerability

Compromise:

1. What tool did you use for your exploit? Nessus and Powershell
2. Provide screenshots of your results

Graphical user interface, text, application, email

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

Text

Description automatically generated

1. Describe what you discovered.

Username and hot along with access to private information that if put in the wrong hands will be bad.

Remediation

1. Describe how you will get rid of this vulnerability

Use iptables commands to clear rules and add ones to only allow some FTP traffic and deny all other traffic.

**Vulnerability #2: SQL Injection:**

Reconnaissance/Scanning:

1. Describe how you would have found this vulnerability. Ip address of the machine (10.2.0.5) gets typed into chrome.
2. Based on your findings, what do you know about this vulnerability? Steal information from a database and entering other code into the website

Compromise:

1. What tool did you use for your exploit? Google chrome
2. Provide screenshots of your results

Table

Description automatically generated with low confidence

Table

Description automatically generated with low confidence

1. Describe what you discovered.

Salary of the workers and all their usernames

Remediation

1. Describe how you will get rid of this vulnerability

Make sure the code is correct for the website.

**Iptables Configuration on PumpPLC:**

In order to preserve the network requirements and remidate as many of the attacks as possible, the following iptables rules were implemented on PumpPLC.

sudo iptables -F INPUT

sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

sudo iptables -A INPUT -p tcp --dport ssh j ACCPET

sudo iptables -A INPUT -p tcp --dport ftp -s 10.2.0.6 -j ACCEPT

sudo iptables -A INPUT -p tcp --dport http -s 10.2.0.6 -j ACCEPT

sudo iptables -A INPUT -p tcp --dport https -s 10.2.0.6 -j ACCEPT

sudo iptables -A INPUT -p tcp --dport http -s 10.2.0.7 -j ACCEPT

sudo iptables -A INPUT -p tcp --dport https -s 10.2.0.7 -j ACCEPT

sudo iptables --policy INPUT DROP

\*confirm rules\*

sudo iptables-save