Lab Template

1. **Make a bash script that performs the tasks specified.** **Take a screenshot of the script and copy/paste the bash script into your lab report**
2. points)

**A screenshot of a computer program

Description automatically generated**

**#! /bin/bash**

**# Tasked to do 4 things**

**# Accept a cmd line argument (ip address)**

**ip\_address="$1"**

**echo "Ip address: $ip\_address"**

**# Runs an nmap full port scan against IP address**

**echo "Running nmap full port scan on $ip\_address"**

**nmap -p- "$ip\_address"**

**# Runs an nmap service version scan against the IP**

**echo "Running service version scan on $ip\_address"**

**nmap -sV "$ip\_address"**

**# Runs an nmap OS scan against the IP**

**echo "Running OS scan on $ip\_address"**

**nmap -O "$ip\_address"**

1. **In your own words, describe what the script status.sh is doing. You may provide screenshots to supplement your answer.**
2. points)

The script records the status of the webserver for Apache2 ever so often. This will be saved in a directory called /var/www/html/logs. At the end of the script, we have a few lines of codes to limit the amount of files in the directory to prevent it getting to large.

A computer screen shot of white text

Description automatically generated

1. **Submit a screenshot of the following command once you have obtained root**

**echo [netid] && id && cat /var/www/html/status.sh && ip addr**

1. oints)

A screenshot of a computer program

Description automatically generated

1. **Identify a PE vector that looks like this. Take a screenshot of your findings.**
2. oints)

A screen shot of a computer code

Description automatically generated

1. **Submit a screenshot of the following command once you have obtained root**

**echo [netid] && id && hostname && ip addr**

1. oints)

A computer screen shot of a computer

Description automatically generated

1. **Submit a screenshot of you logging in as Quinn via SSH**

(5 points)

A computer screen with white text

Description automatically generated

1. **Why might resetting a user's password be a poor method of persistence?**

(5 points)

Resetting a users password is a poor method of persistence because it will be detected and notify the user and administrator. If a user attempts to log in after a password reset and is unsuccessful, the user may scan their account and be alerted. The administrator will have access to reset passwords to the account and changing passwords create footprints. The footprints are logged into a document and the administrator can respond to security breach.

1. **In your own words, what is this binary doing? Be detailed (2+ sentences).**

(10 points)

The program checks to view if the user is Preston. They get the user by running the whoami command. The user you are now is stored in an array and printed if you are Preston and if matches, then you would be given access granted. If you are not Preston, it will say your name and terminate. When you are given access, a root shell will be provided.

1. **What happens when you run the command “ls”? Why does this happen?**

**Be specific (2-3 full sentences).**

(10 points)

When we run ls after modifying it, it outputs “PATH ABUSE!!”. This is occurring because the “export PATH=,:$PATH” command will cause the system to check the directory “.” first which causes “PATH ABUSE!!” to be printed since it appears inside the directory “.”. Going forward the only thing that will appear in the directory “.” when ls is executed is “PATH ABUSE!!”.

   10.) **Submit a screenshot of the following command once you have obtained root**

**echo [netid] && id && hostname && ip addr**

(10 points)

A computer screen shot of a computer

Description automatically generated

    11.) **Submit a screenshot of santana being able to run any command as sudo**

**echo “[netid]” && sudo -l**

(10 points)

A blue screen with white text

Description automatically generated