**Week 6 Homework Submission File: Advanced Bash - Owning the System**

Please edit this file by adding the solution commands on the line below the prompt.

Save and submit the completed file for your homework submission.

**Step 1: Shadow People**

1. Create a secret user named sysd. Make sure this user doesn't have a home folder created:
   * 
2. Give your secret user a password: Target4tt@cK
   * Enter new UNIX password: 
     Retype new UNIX password: 
     passwd: password updated successfully 
3. Give your secret user a system UID < 1000:
   * 
4. Give your secret user the same GID:
   * 
5. Give your secret user full sudo access without the need for a password:



# Al low members of group sudo to execute any command 
%sudo ALL; (ALL :ALL) ALL 
sysd ALL-(ALL) NOPASSWD:ALL 

1. Test that sudo access works without your password:

sysd@scavenger-hunt:—S touch examplel. txt 
sysd@scavenger-hunt:—S Is 
Desktop Documents Documentsl Downloads examplel . txt Pictures public Videos 
sysd@scavenger-hunt:—S chmod examplel. txt 

**Step 2: Smooth Sailing**

1. Edit the sshd\_config file:
2. CNU nano 2.9.3 
   etc ssh sshd confi 
   sopenBSD: 1.101 2017/03/14 djm EXP S 
   This ts the sshd server system-wide configuration file. 
   See 
   sshd_conftg(5) for more information. 
   This sshd was compiled with 
   The strategy used for options tn the default sshd_conftg shipped with 
   OpenSSH ts to specify options with their default value where 
   possible, but leave them commented. 
   Uncommented options override the 
   default value. 
   *Port 22 
   port 2222 
   #AddressFamtly any 

**Step 3: Testing Your Configuration Update**

1. Restart the SSH service:
   * systemctl reload sshd
2. Exit the root account:
   * Closed terminal, closed machine and signed back in.
3. SSH to the target machine using your sysd account and port 2222:
   * ssh sysd@192.168.6.105 -p 2222 
     sysd@192.168.6.105's password: 
     Welcome to Ubuntu 18.04.3 LTS (GNU/Ltnux 4.15.0-70-genertc x86 _ 64) 
     * Documentation: 
     * Management: 
     * Support: 
     https : / [help . ubuntu . com 
     https : / [landscape . canonical . com 
     https : / /ubuntu . com/advantage 
     system information as of Tue oct 20 UTC 2020 
     System load: 
     Usage of / : 
     Memory usage 
     Swap usage: 
     * Introducing 
     53.2% of 9.78GB 
     : 25% 
     0% 
     Processes : 
     Users logged in: 
     107 
     1 
     IP address for enpes3: 10.0.2.15 
     IP address for enpes8: 192.168.6.105 
     autonomous high availability clustering for MicroK8s 
     production environments! Super simple clustering, hardened Kubernetes, 
     with automatic data store operations. A zero-ops HA K8s for anywhere. 
     https : / /mtcrok8s . to/htgh- availability 
     * Canonical Ltvepatch ts available for installation. 
     Reduce system reboots and improve kernel security 
     https : / /ubuntu . com/ltvepatch 
     75 packages can be updated. 
     updates are security updates. 
     New release '20.04.1 LTS' available. 
     Run 'do-release-upgrade' to upgrade to it. 
     *** System restart required *** 
     . Activate at: 
     The programs included with the Ubuntu system are free software; 
     the exact distribution terms for each program are described tn the 
     individual files tn /usr/share/doc/*/copyrtght. 
     Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by 
     applicable law. 
4. Use sudo to switch to the root user:
   * sysd@scavenger-hunt:—S sudo su 
     You found flag _7 : SISzmr05X2tSQfOdeJVDpph5pBPpVL60ye 

**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 
     sysd@192.168.6.105's password: 
     Welcome to Ubuntu 18.04.3 LTS (GNU/Ltnux 4.15.0-70-genertc x86 64) 
     * Documentation: 
     * Management: 
     * Support: 
     https : / [help . ubuntu . com 
     https : / [landscape . canonical . com 
     https : / /ubuntu . com/advantage 
     System information as of 
     Tue oct 20 06:41 UTC 2020 
     System load: 
     Usage of / : 
     Memory usage 
     Swap usage: 
     53.2% of 9.78GB 
     : 25% 
     0% 
     Processes : 
     Users logged in: 
     IP address for enpes3: 
     IP address for enpOs8: 
     111 
     2 
     10.0.2.15 
     192.168.6.1 
     * Introducing autonomous high availability clustering for MicroK8s 
     production environments! Super simple clustering, hardened Kubern 
     etes , 
     with automatic data store operations. A zero-ops HA K8s for anywh 
     ere. 
     https : / /mtcrok8s . to/htgh- availability 
     * Canonical Ltvepatch ts available for installation. 
     Reduce system reboots and improve kernel security 
     https : //ubuntu . com/ltvepatch 
     75 packages can be updated. 
     e updates are security updates. 
     New release '20.04.1 LTS' available. 
     Run 'do-release-upgrade' to upgrade to it. 
     . Activate at: 
     SYS 
     Last loqtn• 
     restart required *** 
     . Tue oct 20 2020 from 192.168.6.104 
2. Escalate your privileges to the root user. Use John to crack the entire /etc/shadow file:
   * john . [shadow 
     Loaded 8 password hashes with 8 different salts (crypt, generic cryp 
     Press 'q' or Ctrl-C to abort, almost any other key for status 

computer 
f reedom 
trustnol 
dragon 
Lakers 
asswerd 
(stallman) 
(babbage) 
(mttntk) 
(lovelace) 
(turtng) 
(sysadmtn) 

© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.