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

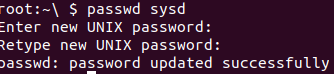
Please edit this file by adding the solution commands on the line below the prompt.

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:  
   * Your solution command here 

Our command to add the user is “useradd” with the flags “r” for creating a system user, “M” to not create a home directory for this user, “o” to allow duplicate UID in case one already exists in the system, “u” for UID which we’ll specify as “666” the devil’s number as we are doing malicious deeds on the system, and finally the username “sysd”

1. Give your secret user a password:
   * Your solution command here 

“Passwd” followed by the user allows password adding. For “sysd” we will give the password “123”

1. Give your secret user a system UID < 1000:  
   * Your solution command here

We already gave a UID, but here’s the command in case we didn’t. Usermod to modify the user and “u” flag to specify UID followed by a UID that’s under 1000.

1. Give your secret user the same GID:  
   * Your solution command here 

groupmod allows us to modify the group, “g” for the GID, same as our UID followed by the user “sysd”



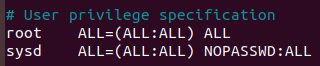
A quick piped command will show out UID and GID have successfully been implemented.

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

So now we need to get into visudo which modifies our sudoers. So we’re going to:

* + Your solution command here 

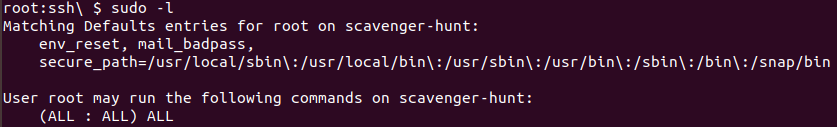
Once in visudo, we’re going to add password permissions that enable no need for a password:



1. Test that sudo access works without your password:



We run a quick piped command. NOPASSWD:ALL is indeed working. Let’s run another test just to be sure.



It worked, Moving on...

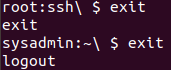
**Step 2: Smooth Sailing**

1. Edit the sshd\_config file:

Your bash commands here: 

We added the additional port of “2222” as directed.

**Step 3: Testing Your Configuration Update**

1. Restart the SSH service:  
   * Your solution command here: 
2. Exit the root account:  
   * Your solution command here 
3. SSH to the target machine using your sysd account and port 2222:  
   * Your solution command here 
4. Use sudo to switch to the root user:  
   * Your solution command here
5. 

**Step 4: Crack All the Passwords**

1. SSH back to the system using your sysd account and port 2222:  
   * Your solution command here
   * 
2. Escalate your privileges to the root user. Use John to crack the entire /etc/shadow file:  
   * Your solution command here 



We’re going to run unshadow here and combine the passwd list with everything in shadow for a single passwords.txt file. This makes it easier to run in one place. Now we use John to crack these passwords while using the list of passwords we already have.

