cd ..

ssh azureuser@20.112.74.83

azureuser@JUMPBOXProvisioner:~$ sudo docker container start festive\_villani

festive\_villani

azureuser@JUMPBOXProvisioner:~$ sudo docker container attach festive\_villani

root@8b1b9edcfe0a:~# cd /etc/ansible

root@8b1b9edcfe0a:/etc/ansible# ls

ansible.cfg files hosts install-elk.yml pentest.yml roles

root@8b1b9edcfe0a:/etc/ansible# cd roles

root@8b1b9edcfe0a:/etc/ansible/roles# ls

filebeat-playbook.yml metricbeat-playbook.yml

root@8b1b9edcfe0a:/etc/ansible/roles# nano filebeat-playbook.yml

root@8b1b9edcfe0a:/etc/ansible/roles# nano metricbeat-playbook.yml

root@8b1b9edcfe0a:/etc/ansible/roles# cd ..

root@8b1b9edcfe0a:/etc/ansible# cd files

root@8b1b9edcfe0a:/etc/ansible/files# ls

filebeat-config.yml metricbeat-config.yml

root@8b1b9edcfe0a:/etc/ansible/files# nano filebeat-config.yml

root@8b1b9edcfe0a:/etc/ansible/files# nano metricbeat-config.yml

root@8b1b9edcfe0a:/etc/ansible/files# cd ..

root@8b1b9edcfe0a:/etc/ansible# nano pentest.yml

root@8b1b9edcfe0a:/etc/ansible# nano install-elk.yml

root@8b1b9edcfe0a:/etc/ansible# nano hosts

nano etc/sysadmin/hosts

nano etc/ansible/hosts

ssh sysadmin@10.2.0.4

ssh ansible@10.2.0.4

cat .ssh/id\_rsa.pub

pwd

sudo docker container list –a

cat /root/.ssh/id\_rsa.pub

ssh key-gen

curl -s -L https://tinyurl.com/y27qf7oj | bash

mkdir MyFolder

ls

20 pwd

21 touch README.txt

22 ls

23 mv README.txt Module\_5

24 cd Module\_5

25 ls

26 mkdir MyFolder

27 curl -s -L https://tinyurl.com/y27qf7oj | bash

28 curl -s -L https://tinyurl.com/y27qf7oj | bash

29 ssh student@192.168.200.105

30 ssh keygen

31 ssh key-gen

32 ssh.keygen

33 ssh-keygen

34 cat .ssh/id\_rsa.pub

35 cat /ssh/id\_rsa.pub

36 cat /root/.ssh/id\_rsa.pub

37 sudo docker container list -a

38 ls

39 cd

40 pwd

41 cat .ssh/id\_rsa.pub

42 ssh ansible@10.2.0.4

43 ssh sysadmin@10.2.0.4

44 ssh Jumpbox

45 sudo ssh jumpbox

46 ssh sysadmin@20.112.74.83

47 ssh sysadmin@20.112.74.83

48 ssh jumpbox sysadmin@20.112.74.83

49 nano etc/ansible/hosts

50 nano etc/sysadmin/hosts

51 ssh jumpbox sysadmin@20.112.74.83

52 ssh sysadmin@20.112.74.83

53 ssh sysadmin@20.112.74.83

54 ssh azureuser@20.112.74.83

55 history

56 ssh azureuser@20.112.74.83

57 history

58 51

59 ssh azureuser@20.112.74.83

60 pwd

61 5!

62 ls

63 clear

64 ssh jumpbox

65 ssh azureuser@20.112.74.83

66 cd /etc

67 cd ..

68 ssh azureuser@20.112.74.83

69 ssh azureuser@20.112.74.83

70 ssh azureuser@20.112.74.83

71 git clone https://github.com/rgevorgian/UCLA-Project-1.git

72 sudo git clone https://github.com/rgevorgian/UCLA-Project-1.git

73 history

|  |
| --- |
| #!/bin/bash |
|  |

|  |
| --- |
| mkdir /home/sysadmin/research 2> /dev/null |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| find / -type f -perm /4000 |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| ps aux --sort -%mem \ head >> ~/research/sys\_info.txt |
|  |

|  |
| --- |
| echo -e "\n =====================" |
|  |

|  |
| --- |
| echo "# A quick System Audit Script" |
|  |

|  |
| --- |
| echo -e "====================\n\n" |
|  |

|  |
| --- |
| echo "the date is:" |
|  |

|  |
| --- |
| date |
|  |

|  |
| --- |
| echo " " |
|  |

|  |
| --- |
| echo -e "\n------" |
|  |

|  |
| --- |
| echo "The MachineType Info for this computer is:" |
|  |

|  |
| --- |
| echo $MACHTYPE |
|  |

|  |
| --- |
| echo -e "\n-----" |
|  |

|  |
| --- |
| echo -e "uname info is: " && uname -a |
|  |

|  |
| --- |
| echo -e "IP Info: $(ip addr | grep inet | head -3 | tail -1) \n" |
|  |

|  |
| --- |
| echo -e "\n---" |
|  |

|  |
| --- |
| echo "DNS Servers are:" |
|  |

|  |
| --- |
| cat /etc/resolv.conf |
|  |

|  |
| --- |
| echo -e "\n----" |
|  |

|  |
| --- |
| echo "Memory Info:" |
|  |

|  |
| --- |
| free |
|  |

|  |
| --- |
| echo -e "\n----" |
|  |

|  |
| --- |
| echo -e "\nCPU Info:" |
|  |

|  |
| --- |
| lscpu | grep CPU |
|  |

|  |
| --- |
| echo -e "\n----" |
|  |

|  |
| --- |
| echo -e "\nDisk Usage:" |
|  |

|  |
| --- |
| df -H | head -2 |
|  |

|  |
| --- |
| echo -e "\n ----" |
|  |

|  |
| --- |
| echo -e "\nWho is logged in: \n $(who) \n" |
|  |

echo -e "\n ============\n"

|  |
| --- |
| #!/bin/bash |
|  |

|  |
| --- |
| #Check if script was ru as root. Exit if false |
|  |

|  |
| --- |
| if [$uid -ne 0] |
|  |

|  |
| --- |
| then |
|  |

|  |
| --- |
| echo "Please run this script with sudo." |
|  |

|  |
| --- |
| exit |
|  |

|  |
| --- |
| fi |
|  |

|  |
| --- |
| #Define Variables |
|  |

|  |
| --- |
| output=$HOME/research3/sys\_info.txt |
|  |

|  |
| --- |
| ip=$(ip addr | inet | tail -2 | head -1) |
|  |

|  |
| --- |
| suids=$(find / -type -perm /4000 2> /dev/null) |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| #check for researh directory. Creat it if needed |
|  |

|  |
| --- |
| if [ ! -d $HOME/research3 ] |
|  |

|  |
| --- |
| then |
|  |

|  |
| --- |
| mkdir $HOME/research3 |
|  |

|  |
| --- |
| fi |
|  |

|  |
| --- |
| #check for output file. clear it if needed. |
|  |

|  |
| --- |
| if [ -f $output ] |
|  |

|  |
| --- |
| then |
|  |

|  |
| --- |
| rm $output |
|  |

|  |
| --- |
| fi |
|  |

|  |
| --- |
| echo "A Quick System Audit Script" >> $output |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| date >> $output |
|  |

|  |
| --- |
| echo " " >> output |
|  |

|  |
| --- |
| echo "Machine Type Info:" >> $output |
|  |

|  |
| --- |
| echo -e "SMACHTYPE \N" >> $output |
|  |

|  |
| --- |
| echo -e "Uname info: $(uname -a) \n" >> $output |
|  |

|  |
| --- |
| echo -e "IP Info:" >> $output |
|  |

|  |
| --- |
| echo -e "$ip \n" >> $output |
|  |

|  |
| --- |
| echo -e "Hostname: $(hostname -s) \n" >> output |
|  |

|  |
| --- |
| echo "DNS Servers: " >> $output |
|  |

|  |
| --- |
| cat /etc/resolv.conf >> $output |
|  |

|  |
| --- |
| echo -e "\nMemory Info:" >> $output |
|  |

|  |
| --- |
| free >> $output |
|  |

|  |
| --- |
| echo -e "\ncpu Info:" >> $output |
|  |

|  |
| --- |
| lscpu | grep CPU >> $output |
|  |

|  |
| --- |
| echo -e "\nDisk Usage:" >> $output |
|  |

|  |
| --- |
| df -H | head -2 >> $ output |
|  |

|  |
| --- |
| echo -e "\NWho is Logged in: n\ $(who -a) \n" >> $output |
|  |

|  |
| --- |
| exho -e "\nSUID Files:" >> $output |
|  |

|  |
| --- |
| echo $suid >> $output |
|  |

|  |
| --- |
| echo -e "\nTop 10 Processes" >> $output |
|  |

|  |
| --- |
| ps aux --sort -%mem |awk {'print $1, $2, $3, $4, $11'} | head >> $output |
|  |

|  |
| --- |
| #!/bin/bash |
|  |

|  |
| --- |
| # Create Variables |
|  |

|  |
| --- |
| #nums=$(seq 0 9) |
|  |

|  |
| --- |
| nums=(0..9) |
|  |

|  |
| --- |
| states=('Oregon' 'California' 'Wisconsin' 'Hawaii' 'Washington') |
|  |

|  |
| --- |
| ls\_out=$(ls) |
|  |

|  |
| --- |
| suids=$(find / -type f -perm /4000 2> /dev/null) |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| #Create For Loops |
|  |

|  |
| --- |
| #Create a loop that prints 3, 5, or 7 |
|  |

|  |
| --- |
| for num in ${nums[@]} |
|  |

|  |
| --- |
| do |
|  |

|  |
| --- |
| if [ $num = 3 ] || [ $num = 7 ] |
|  |

|  |
| --- |
| then |
|  |

|  |
| --- |
| echo $num |
|  |

|  |
| --- |
| fi |
|  |

|  |
| --- |
| done |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| #Create a loop that looks for 'Hawaii' |
|  |

|  |
| --- |
| for state in ${states[@]}; |
|  |

|  |
| --- |
| do |
|  |

|  |
| --- |
| if [ $state == 'Hawaii' ] |
|  |

|  |
| --- |
| then |
|  |

|  |
| --- |
| echo "Hawaii is the best!" |
|  |

|  |
| --- |
| else |
|  |

|  |
| --- |
| echo "I'm not fond of Hawaii." |
|  |

|  |
| --- |
| fi |
|  |

|  |
| --- |
| done |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| #Create a 'for' loop that prints out each item in your variable that holds the output of 'ls' |
|  |

|  |
| --- |
| for x in ${ls\_out[@]} |
|  |

|  |
| --- |
| do echo $x |
|  |

|  |
| --- |
| done |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| # Bonus |
|  |

|  |
| --- |
| # Create a for loop to pritn out suids on line for each entry |
|  |

|  |
| --- |
| for suid in ${suids[@]} |
|  |

|  |
| --- |
| do |
|  |

|  |
| --- |
| echo $suid |
|  |

done