Dom Moore
Lab Database Encryption and hashing

Part 1: Staging

Prepare the following operating systems for today's lab:

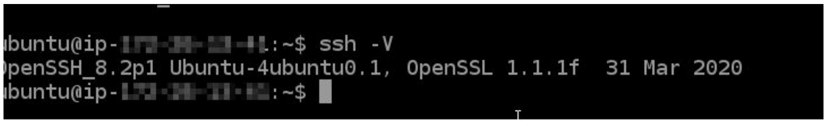
Step 1- Deploy a Linux VM on a cloud provider of your choosing. Ubuntu Linux 20.04 Focal Fossa

Step 2 -In your Linux VM install OpenSSH

Step 3 - In Microsoft Azure, deploy SQL database

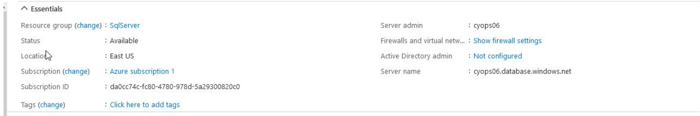
Step 4 - install Microsoft SQL Server Management Studio (SSMS) and establish

Deploy Linux VM / Install OpenSSH



```
ubuntu@ip-[redacted]:~$ ssh -V
OpenSSH_8.2p1 Ubuntu-4ubuntu0.1, OpenSSL 1.1.1f  31 Mar 2020
ubuntu@ip-[redacted]:~$ 
```

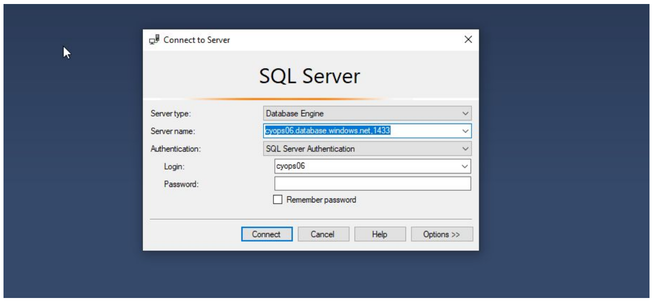
Deploy Azure SQL database



Resource group (change) : SqlServer
Status : Available
Location : East US
Subscription (change) : Azure subscription 1
Subscription ID : da0cc74c-fc80-4780-978d-5a29300820c0
Tags (change) : Click here to add tags

Server admin : cyops06
Firewalls and virtual netw... : Show firewall settings
Active Directory admin : Not configured
Server name : cyops06.database.windows.net

SQL SSMS



Server type: Database Engine
Server name: cyops06.database.windows.net,1433
Authentication: SQL Server Authentication
Login: cyops06
Password:
☐ Remember password

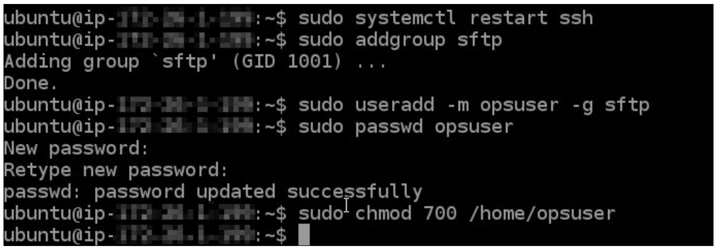
Part 2: Secure File Transmission with SFTP on Linux

Step1 - Deploy an SFTP server on your cloud Linux system.

Step 2- Ask a classmate to authenticate into it and either transmit you a file or download a file from the SFTP server.

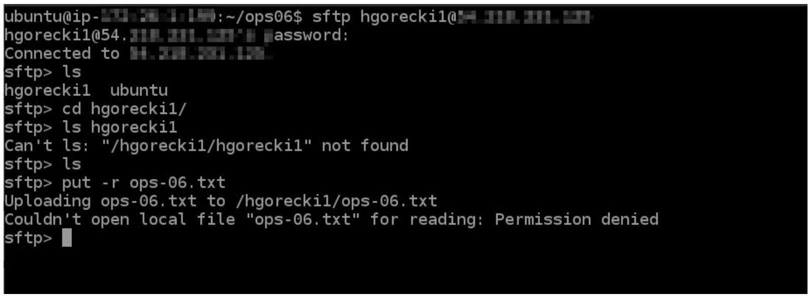
Step -3 Document your setup and file transmission process with screenshots and descriptions.

Deploy sftp server



```
ubuntu@ip-[redacted]:~$ sudo systemctl restart ssh
ubuntu@ip-[redacted]:~$ sudo addgroup sftp
Adding group `sftp' (GID 1001) ...
Done.
ubuntu@ip-[redacted]:~$ sudo useradd -m opsuser -g sftp
ubuntu@ip-[redacted]:~$ sudo passwd opsuser
New password:
Retype new password:
passwd: password updated successfully
ubuntu@ip-[redacted]:~$ sudo chmod 700 /home/opsuser
ubuntu@ip-[redacted]:~$ 
```

File Transmit



```
ubuntu@ip-[redacted]:~/ops06$ sftp hgorecki1@[redacted]
hgorecki1@54.[redacted]assword:
Connected to [redacted]
sftp> ls
hgorecki1  ubuntu
sftp> cd hgorecki1/
sftp> ls hgorecki1
Can't ls: "/hgorecki1/hgorecki1" not found
sftp> ls
sftp> put -r ops-06.txt
Uploading ops-06.txt to /hgorecki1/ops-06.txt
Couldn't open local file "ops-06.txt" for reading: Permission denied
sftp> 
```

File Transmit:

To transmit the file to another remote PC I needed the credentials of the user for the remote desktop. After receiving the credentials I was able to log in using the sftp user@ip address command. Once I was authenticated and given permission I was able to navigate within the user’s directory. In order for me to transmit a file I had to create a file within a directory on my local pc then navigate to the remote user directory and use command put -r and file name. The file was then uploaded to the remote directory but my privileges were limited.

Part 3: Secure File Transmission with SCP on Linux

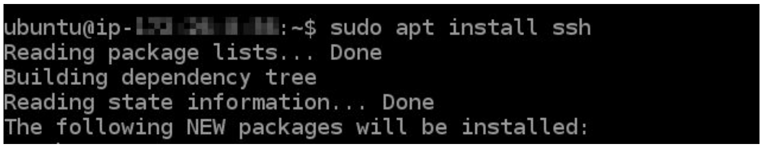
On your Linux VM in the cloud:

Step 1- Install OpenSSH.

Step 2 - Successfully perform a file transmission from your local computer to your Linux VM using the SCP command.

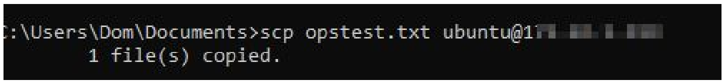
Step 3 - Document your setup and file transmission process with screenshots and descriptions.

Install SSH



```
ubuntu@ip-[redacted]:~$ sudo apt install ssh
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
```

scp Transmission



```
:\Users\Dom\Documents>scp opstest.txt ubuntu@1[redacted]
        1 file(s) copied.
```

Scp transmission:

To transfer a file from my local desktop to a remorse desktop I needed to establish an ssh connection through the terminal as well as have the user name and IP address to the remote desktop. Once I had the path that I wanted to send the file I created an ssh path using the SCP command once a connection was established I had to authenticate and was able to proceed to complete the file transfer.

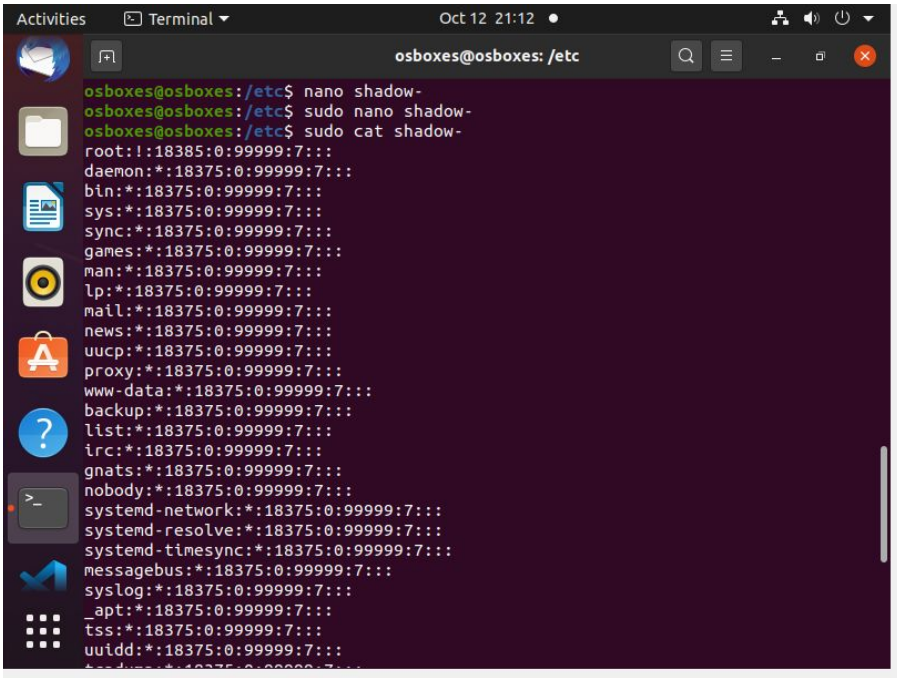
Part 4: Encryption and Decryption on Linux

Let’s take a look at where Linux stores user credentials.

Step 1 - As the administrator of the Ubuntu Linux VM, dump the password hash file or strings.

Step 2 - Document your setup and process with screenshots and descriptions.

Hash Dump



```
osboxes@osboxes:/etc$ nano shadow-
osboxes@osboxes:/etc$ sudo nano shadow-
osboxes@osboxes:/etc$ sudo cat shadow-
root:!:18385:0:99999:7:::
daemon:*:18375:0:99999:7:::
bin:*:18375:0:99999:7:::
sys:*:18375:0:99999:7:::
sync:*:18375:0:99999:7:::
games:*:18375:0:99999:7:::
man:*:18375:0:99999:7:::
lp:*:18375:0:99999:7:::
mail:*:18375:0:99999:7:::
news:*:18375:0:99999:7:::
uucp:*:18375:0:99999:7:::
proxy:*:18375:0:99999:7:::
www-data:*:18375:0:99999:7:::
backup:*:18375:0:99999:7:::
list:*:18375:0:99999:7:::
irc:*:18375:0:99999:7:::
gnats:*:18375:0:99999:7:::
nobody:*:18375:0:99999:7:::
systemd-network:*:18375:0:99999:7:::
systemd-resolve:*:18375:0:99999:7:::
systemd-timesync:*:18375:0:99999:7:::
messagebus:*:18375:0:99999:7:::
syslog:*:18375:0:99999:7:::
_apt:*:18375:0:99999:7:::
tss:*:18375:0:99999:7:::
uuidd:*:18375:0:99999:7:::
```

Obtaining Hash:

To gain access to the hash folder, you first have to establish yourself as a root user or use the Sudo command. Once you have established yourself with the correct privileges you can cd /etc/shadow- once in the correct folder you can nano/ vim into the folder or cat the contents of the file onto the terminal.

Part 5: Credential Exfiltration and Decryption on SQL Databases

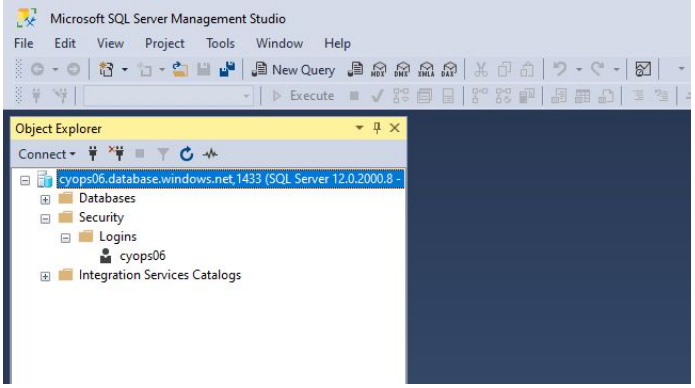
Next, we'll extract encrypted credentials from a SQL DB.

Step 1 - Deploy SQL database SSMS

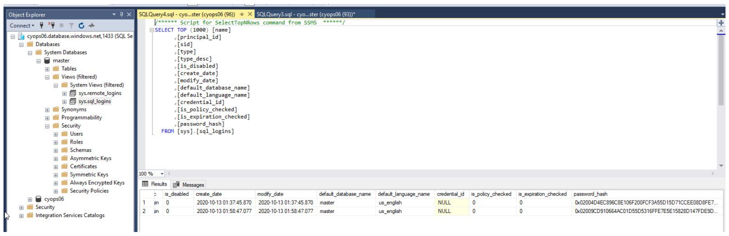
Step 2 - Dump the hashes.

Step 3 - Document your setup and process with screenshots and descriptions.

Deploy Sql


Microsoft SQL Server Management Studio
File
Edit
View
Project
Tools
Window
Help
New Query
Execute
Object Explorer
Connect
cyops06.database.windows.net,1433 (SQL Server 12.0.2000.8 -
Databases
Security
Logins
cyops06
Integration Services Catalogs

Dump Hashes



```
/****** Script for SelectTopNRows command from SSMS  ******/
SELECT TOP (1000) [name]
      ,[principal_id]
      ,[sid]
      ,[type]
      ,[type_desc]
      ,[is_disabled]
      ,[create_date]
      ,[modify_date]
      ,[default_database_name]
      ,[default_language_name]
      ,[credential_id]
      ,[is_policy_checked]
      ,[is_expiration_checked]
      ,[password_hash]
  FROM [sys].[sql_logins]
```

	:	is_disabled	create_date	modify_date	default_database_name	default_language_name	credential_id	is_policy_checked	is_expiration_checked	password_hash
1	jin	0	2020-10-13 01:37:45.870	2020-10-13 01:37:45.870	master	us_english	NULL	0	0	0x02004D4EC896C8E106F200FCF3A55D15D71CCEE08D8FE7...
2	jin	0	2020-10-13 01:58:47.077	2020-10-13 01:58:47.077	master	us_english	NULL	0	0	0x02009CD910664AC01D55D5316FFE7E5E15828D147FDE9D...

SQL Hashdump:

I began this process by creating a new user and user password, within the database folders I navigated to log in, right-click and select new user, I then ran the SQL command CREATE USER username Password "password"; to establish a new user and password. My news step was to navigate the master database and search for names with login, once the list was narrowed down I navigated to SQL.syslogin and searched for login, ran the first 200 rows, and received all users and passwords within the database.

Part 6: Reporting

Add to your submission your answers to the below discussion prompts:

- Explain the need for secure data transmission as it relates to confidentiality
    - Secure data transmission is a vital part of all elements of the CIA and confidentiality is an important aspect of that when it comes to keeping sensitive information limited to the individuals with the proper access.

- Explain the difference between FTP and SFTP.
        - The main difference is security sftp is the secure file transfer protocol and is the method that should be used when transferring any type of data.
    - Do they use the same ports?
        - SFTP uses port 22 by default but can be configured to listen on other ports if configured properly, and the FTP default port is considered to be 21
    - Do they use the same software?
        - They are similar frames of technologies but ssh has been improved to have many more features making the later FTP version non-relevant anymore.
    - What are some examples of software used to access FTP and SFTP servers?
- How does SCP protect the data being transmitted? Does it?
    - It also uses ssh secure protocol but as of 2019 it was reported as outdated and recommended that sftp is used to replace it.
- How difficult was it to exfiltrate credentials from Linux system files?
    - Did you learn any tactics/techniques you might use in the future for CTFs/ pentesting? The most difficult part was establishing a connection, every time I tried to gain access it would time out and once I got in I had some permission issues but once the connections were stable the commands to execute were straightforward.
- How do SQL databases store user passwords?
    - Compared to operating systems, how easily can databases be protected from attack? They store them within the master database in a file called system login which is not a good way and the naming conventions make that file an easy target.