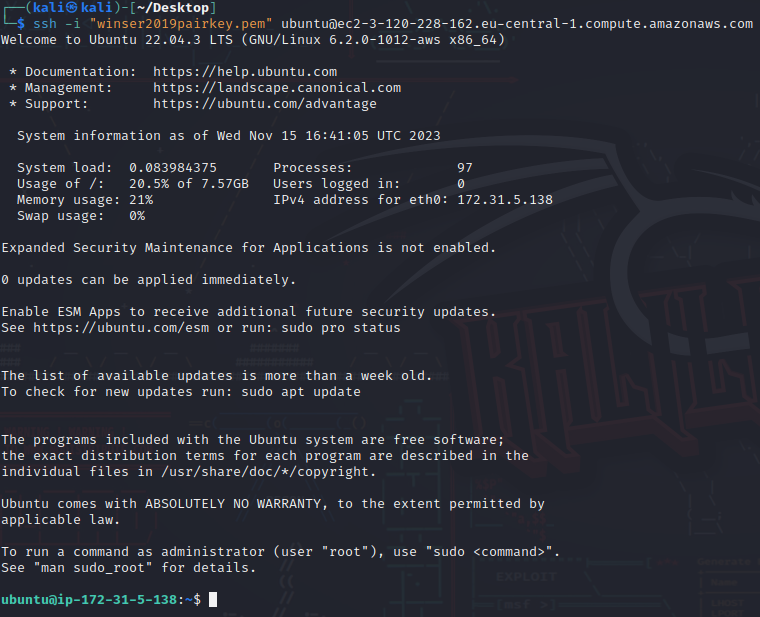
Rodrigo Brasil 11/2023

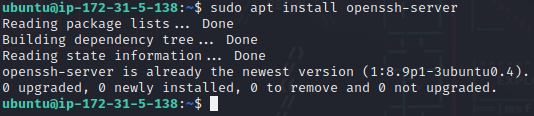
### **Part 1: Staging**

Ubuntu EC2 instance deployed 

Connected with ssh with a kali machine using the pair key given when creating the instance

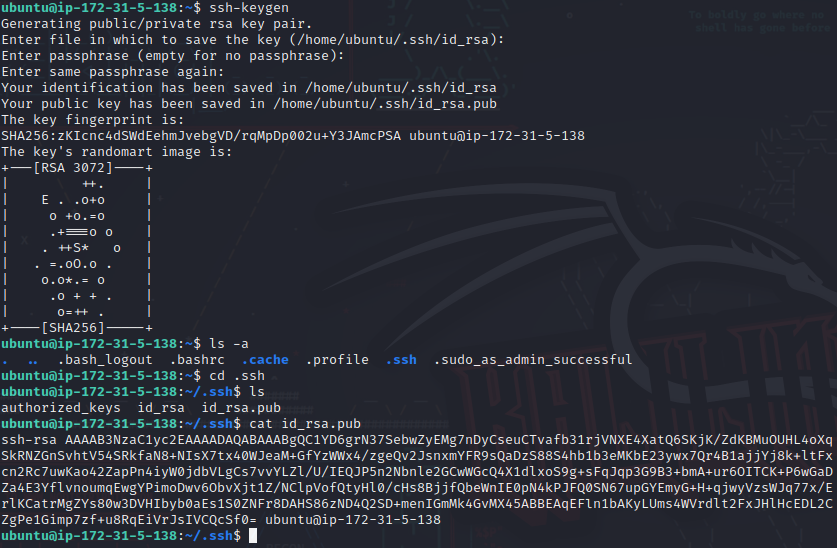
### 

### **Part 2: SSH public key authentication on Linux**



Use the command “sudo apt install openssh-server” to install ssh

ssh is already installed on the ubuntu Instance

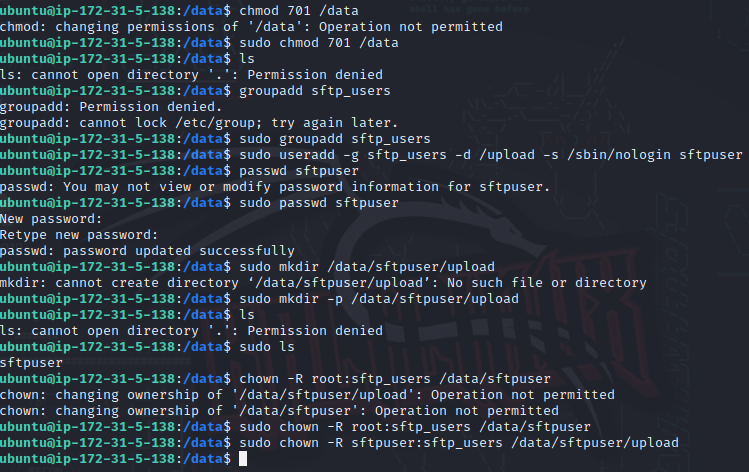


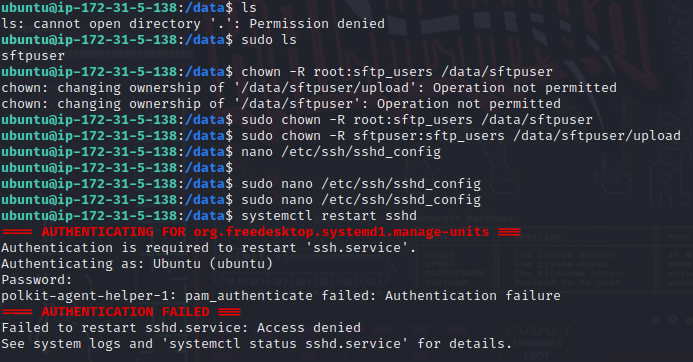
ssh keys generated using the “ssh-keygen” command

generated the private key “id\_rsa” and the public key “id\_rsa.pub”

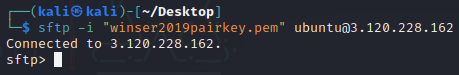
which was not necessary for other steps

### **Part 3: Secure File Transmission with SCP and SFTP on Linux**



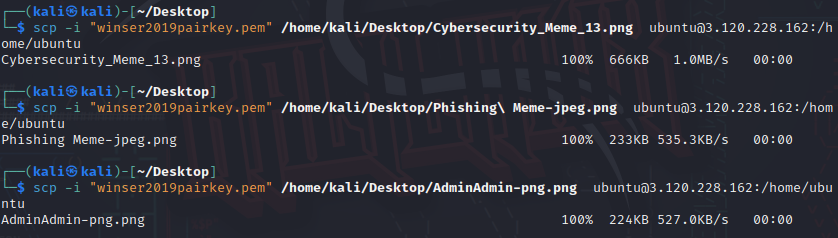


SFTP directories and user created

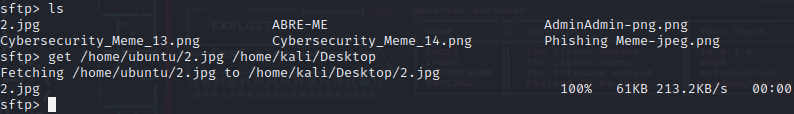


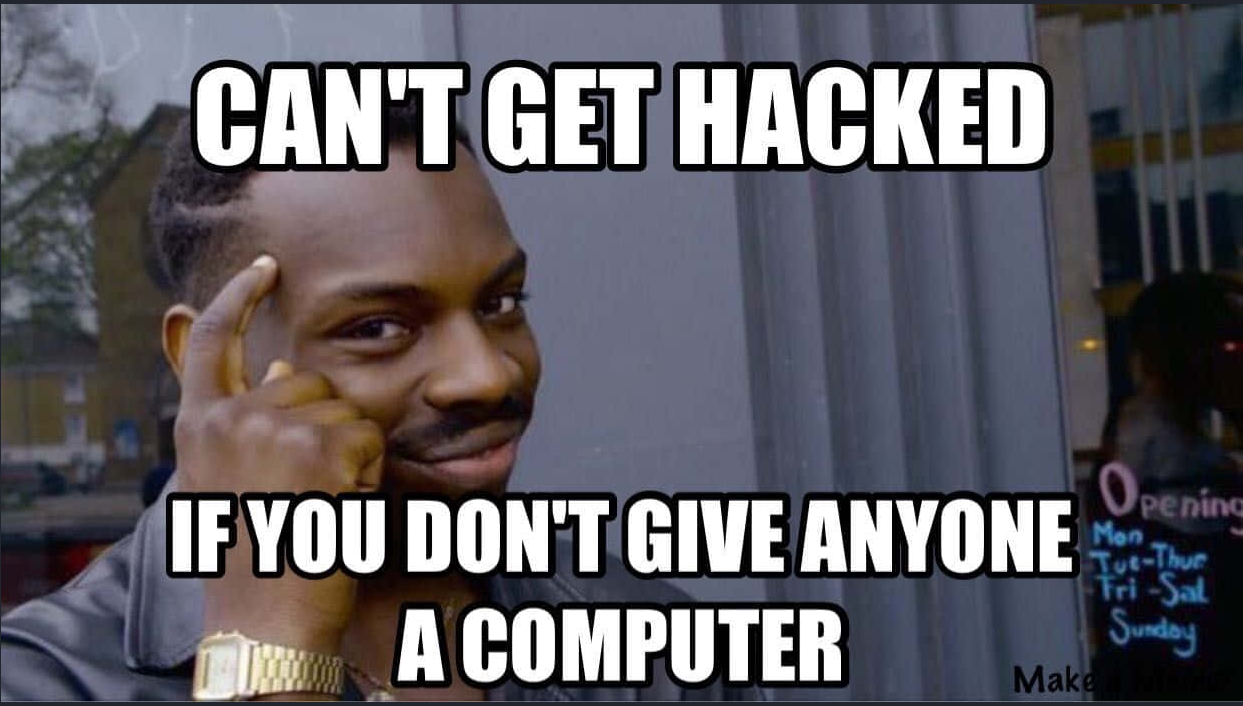
finally was able to connect to the sFTP server

had to log in with the user already created in the Instance

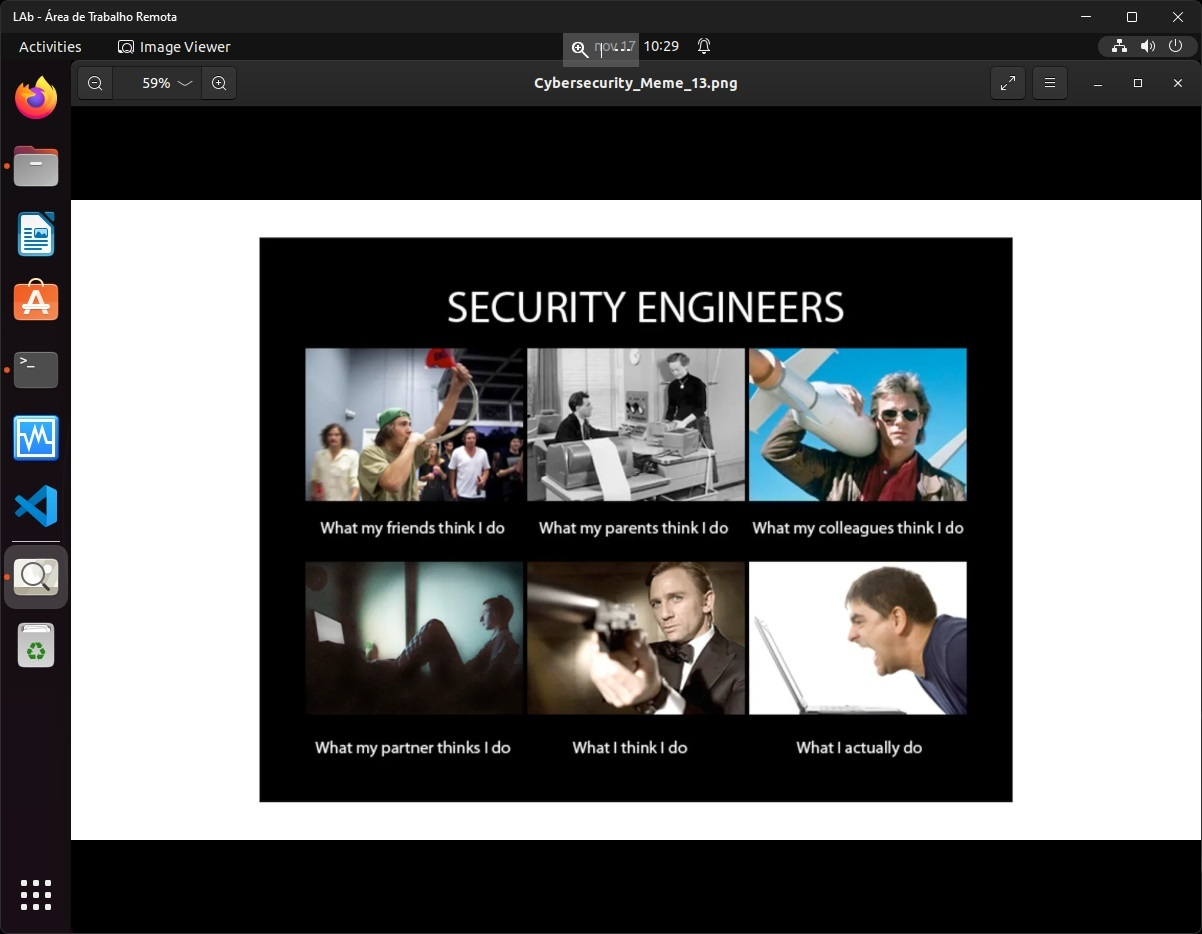


Successfully uploaded the memes to the sFTP server



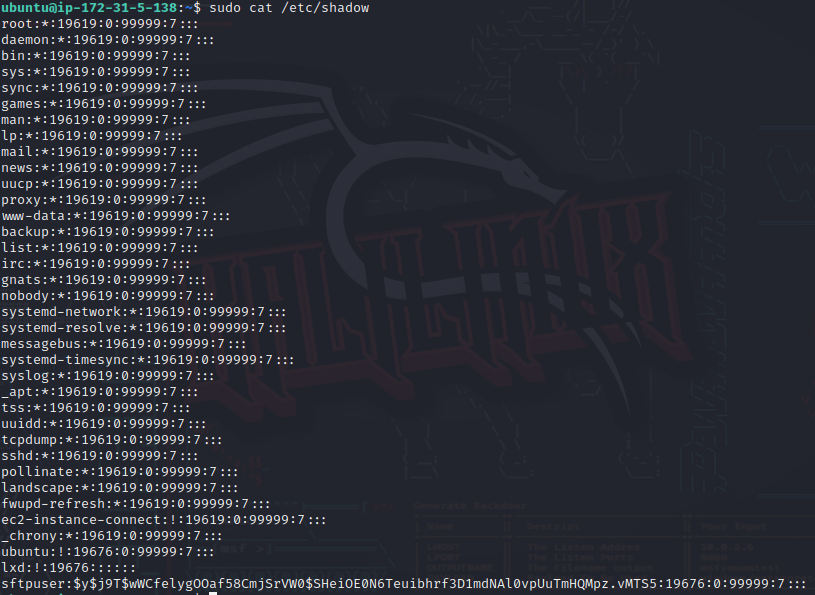


And successfully Downloaded a meme from the sFTP server



My colleague successfully was able to download a meme i uploaded to the sFTP server

### **Part 4: Encryption and Decryption on Linux**



Using the command cat /etc/shadow it gave me a dump of the passwords hashes

### **Part 5: Report Via End-User Training**

* Explain the need for secure data transmission as it relates to confidentiality.

Secure data transmission is imperative for upholding confidentiality by protecting sensitive information from unauthorized access, eavesdropping, tampering, and other potential threats. It not only addresses the technical aspects of data security but also plays a crucial role in compliance, trust-building, and maintaining a competitive edge in various sectors.

* Explain the difference between FTP and SFTP.

Data using FTP is sent in plaintext, which means that the information can be intercepted by attackers if the connection is not secured using additional measures. SFTP, on the other hand, is a secure version of file transfer that encrypts both the control and data channels. The encryption is typically achieved using SSH (Secure Shell) protocols.

* + Do they use the same ports?

No. FTP uses the port 21 while SFTP uses port 22

* + Do they use the same software?

While there may be software that supports both FTP and SFTP, the protocols themselves are not interchangeable.

* + What are some examples of software used to access FTP and SFTP servers?

For FTP FileZilla and WinSCP. For SFTP OpenSSH and PuTTY

* How does SCP protect the data being transmitted?

SCP protects the data using the SSH protocol

* How difficult was it to exfiltrate credentials from Linux system files?

I wasn't able to

* + How might a threat actor (or a pentester) utilize insecure FTP access?

There are multiple ways a threat actor can utilize FTP access some of them are: File Tampering and Injection - If the FTP server allows write access, a threat actor could tamper with existing files or inject malicious files onto the server.

Exfiltration of Sensitive Data - Once unauthorized access is gained, a threat actor could exfiltrate sensitive data stored on the FTP server.

#### 