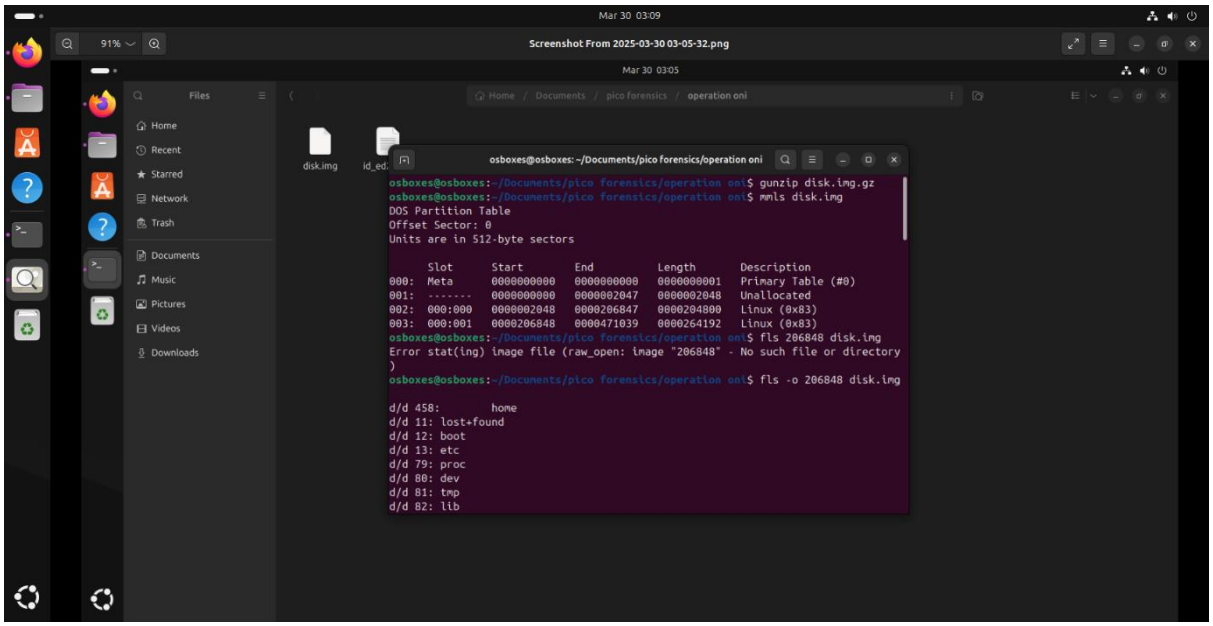
Description

Download this disk image, find the key and log into the remote machine. Note: if you are using the webshell, download and extract the disk image into /tmp not your home directory.

Download disk image

Remote machine: ssh -i key_file -p 65007 ctf-player@saturn.picoctf.net



At first unzip the document

gunzip disk.img.gz

mmls disk.img

DOS Partition Table

Offset Sector: 0

Units are in 512-byte sectors

Slot	Start	End	Length	Description
000:	Meta	0000000000	0000000000	0000000001 Primary Table (#0)
001:	-------	0000000000	0000002047	0000002048 Unallocated
002:	000:000	0000002048	0000206847	0000204800 Linux (0x83)
003:	000:001	0000206848	0000471039	0000264192 Linux (0x83)

Then use mmls to get the partitions

Then use fls to check the partitions in details

fls -o 206848 disk.img

d/d 458: home

d/d 11: lost+found

d/d 12: boot

d/d 13: etc

d/d 79: proc

d/d 80: dev

d/d 81: tmp

d/d 82: lib

d/d 85: var

d/d 94: usr

d/d 104: bin

d/d 118: sbin

d/d 464: media

d/d 468: mnt

d/d 469: opt

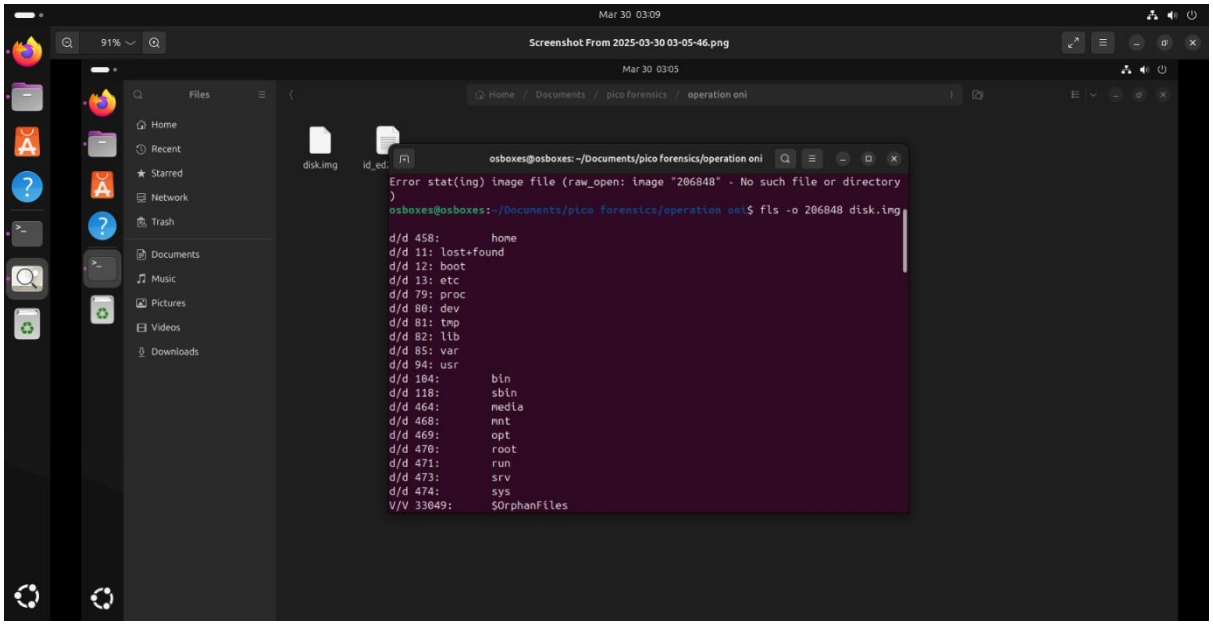
d/d 470: root

d/d 471: run

d/d 473: srv

d/d 474: sys

V/V 33049: $OrphanFiles



Check the root folder

fls -o 206848 disk.img 470

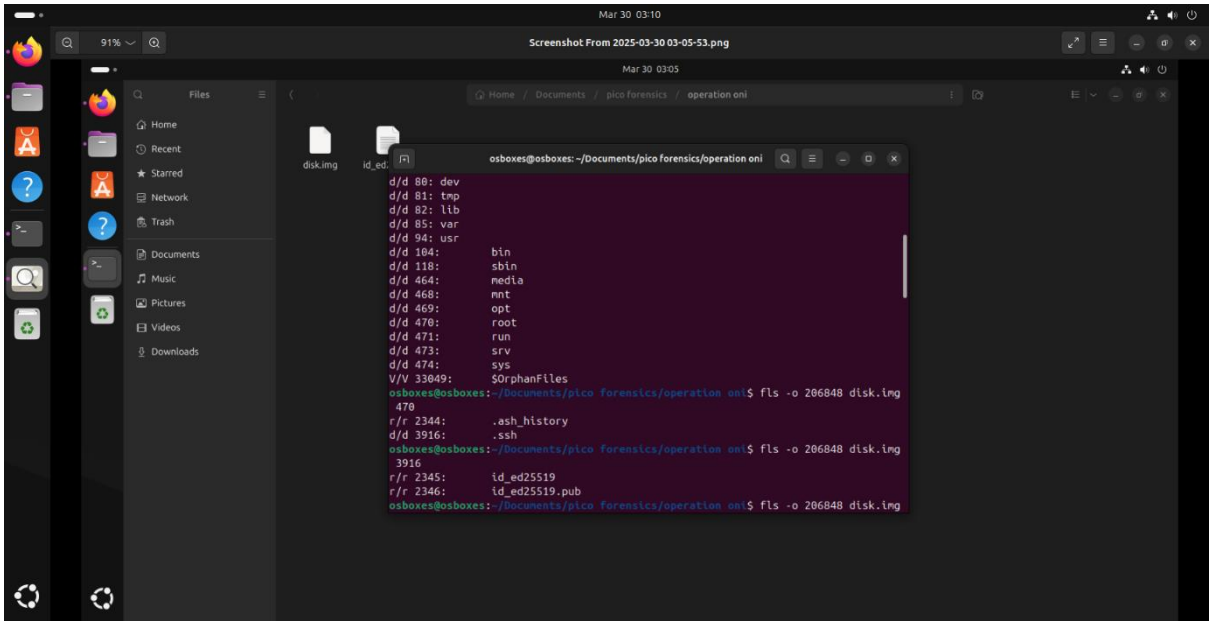
r/r 2344: .ash_history

d/d 3916: .ssh

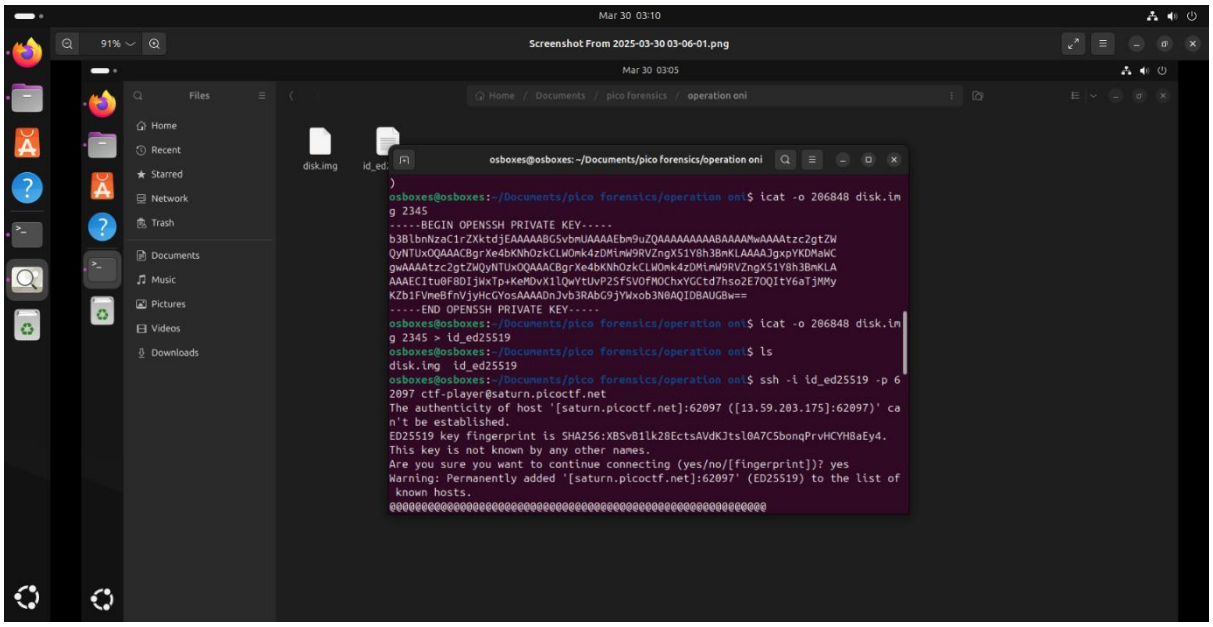
fls -o 206848 disk.img 3916

r/r 2345: id_ed25519

r/r 2346: id_ed25519.pub



We have .ssh and id _ed check them and download them with I cat



icat -o 206848 disk.img 2345

-----BEGIN OPENSSH PRIVATE KEY-----

b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW

QyNTUxOQAAACBgrXe4bKNhOzkCLWOmk4zDMimW9RVZngX51Y8h3BmKLAAAAJgxpYKDMaWC

gwAAAAtzc2gtZWQyNTUxOQAAACBgrXe4bKNhOzkCLWOmk4zDMimW9RVZngX51Y8h3BmKLA

AAAECltu0F8DIjWxTp+KeMDvX1lQwYtUvP2SfSVOfMOChxYGCtd7hso2E7OQItY6aTjMMy

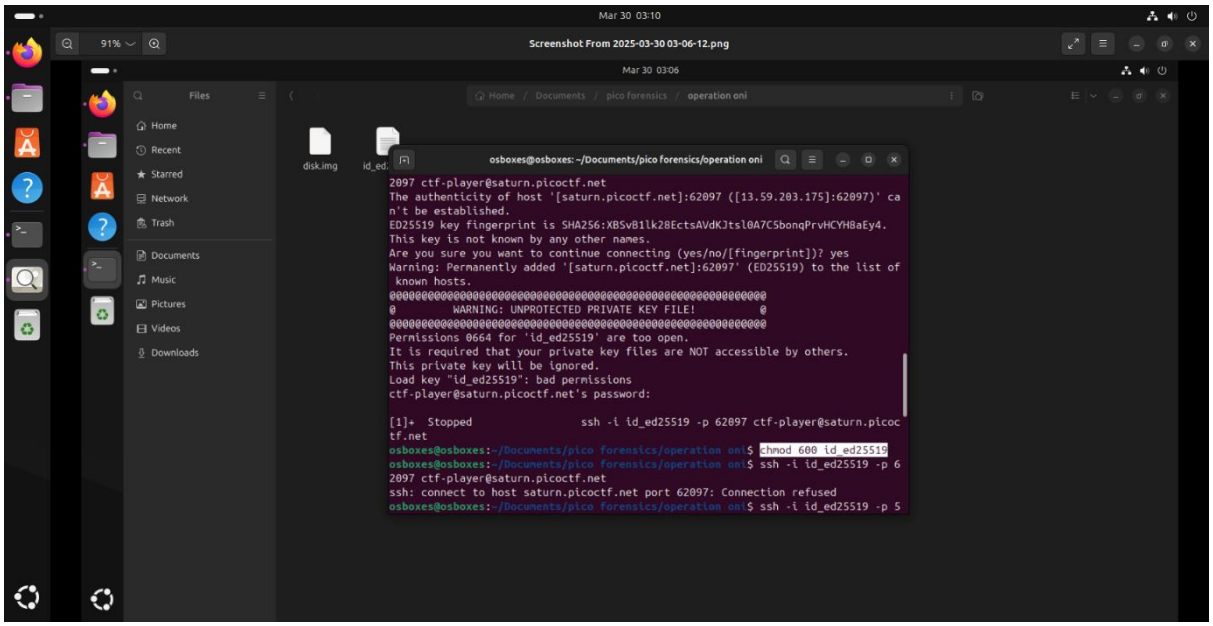
KZb1FVmeBfnVjyHcGYosAAAADnJvb3RAbG9jYWxob3N0AQIDBAUGBw==

-----END OPENSSH PRIVATE KEY-----

icat -o 206848 disk.img 2345 > id_ed25519

Lower the permissions

chmod 600 id_ed25519



And use the file and get the flag