

Operation oni

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 60951 ctf-player@saturn.picoctf.net`

1- Unzip the file to extract the disk image.

2- Run `binwalk -e nameoffile`. This will create a new directory containing other directories, `ext-root-0` and `ext-root`. When we opened `ext-root-0`, we found some directories, including the root directory.

3- We entered the root directory and found it empty, so let's search for hidden files.

4- Enter `ls -al`, and we found two hidden files: `.ssh/.ssh-history`.

5- Open the `.ssh` directory, and we found the key file `id_ed25519`.

```
[root@kali:~]# cat /dev/urandom | tr -dc 'a-z0-9' | fold -w 64 | xargs sha256sum | grep -o '[a-z0-9]*' | xargs echo | xargs cat > id_ed25519
[root@kali:~]# mv id_ed25519 /home/.../_disk.img.extracted/ext-root-0/root/.ssh/
[root@kali:~]# ssh -i id_ed25519 -p 49832 ctf-player@saturn.picoctf.net
The authenticity of host '[saturn.picoctf.net]:49832 ([13.59.203.175]:49832)' can't be established.
ED25519 key fingerprint is SHA256:XBSvB1lk28EctsAVdKJtsl0A7C5bonqPrvHCYH8aEy4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? XBSvB1lk28EctsAVdKJtsl0A7C5bonqPrvHCYH8aEy4
Please type 'yes', 'no' or the fingerprint: SHA256:XBSvB1lk28EctsAVdKJtsl0A7C5bonqPrvHCYH8aEy4
Warning: Permanently added '[saturn.picoctf.net]:49832' (ED25519) to the list of known hosts.
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 6.5.0-1016-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

ctf-player@challenge:~$ pwd
/home/ctf-player
ctf-player@challenge:~$ ls
flag.txt
ctf-player@challenge:~$ cat flag.txt
picoCTF{k3y_5l3u7h_339601ed}ctf-player@challenge:~$ Connection to saturn.picoctf.net closed by remote host.
Connection to saturn.picoctf.net closed.
```