



Specialer

Specialer 

  | 400 points

Tags: picoCTF 2023 General Skills bash ssh

AUTHOR: LT 'SYREAL' JONES, ET AL.

Description

Reception of Special has been cool to say the least. That's why we made an exclusive version of Special, called Secure Comprehensive Interface for Affecting Linux Empirically Rad, or just 'Specialer'. With Specialer, we really tried to remove the distractions from using a shell. Yes, we took out spell checker because of everybody's complaining. But we think you will be excited about our new, reduced feature set for keeping you focused on what needs it the most. Please start an instance to test your very own copy of Specialer.

`ssh -p 51212 ctf-player@saturn.picoctf.net`. The password is `fd7746b4`

This challenge launches an instance on demand.

Its current status is: **RUNNING**

Instance Time Remaining: **11:32**

[Restart Instance](#)

Hints

1

6,490 users solved

 89% Liked 

Specialer challenge

Here we got a shell that uses only certain commands

```

[Specialer$ ls
-bash: ls: command not found
[Specialer$
!      caller      do      fc      kill      return      true
./     case        done     fg      let       select     type
:      cd          echo     fi      local     set        typeset
[      command     elif     for     logout    shift      ulimit
[[     compgen      else     function mapfile    shopt      umask
]]     complete     enable   getopts popd       source     unalias
alias  compopt       esac     hash     printf    suspend    unset
bash   continue     eval     help     pushd     test       until
bg     coproc        exec     history  pwd       then       wait
bind   declare      exit     if        read      time       while
break  dirs         export   in        readarray times      {
builtin disown       false    jobs     readonly trap       }
Specialer$

```

Another thing we can see here is that to get a flag inside this shell we can rely on a few things:

- echo - there is a format to print the contents of a file
- cd - move to each directory
- (tabs) - by pressing tabs to complete commands like cd we can see all the existing list of directories

```
nutan — ssh -p 51212 ctf-player@saturn.picoctf.net — 80x24
~/Downloads/nutan — ssh -p 51212 ctf-player@saturn.picoctf.net
Specialer$ echo "$(<cadabra.txt)"
Nothing up my sleeve!
Specialer$ echo cada
cadabra.txt  cadaniel.txt
Specialer$ echo cada
cadabra.txt  cadaniel.txt
Specialer$ echo "$(<cadaniel.txt)"
Yes, I did it! I really did it! I'm a true wizard!
Specialer$ cd ..
Specialer$ cd
.hushlogin  .profile      abra/          ala/          sim/
Specialer$ cd ala
Specialer$ ls
bash: ls: command not found
Specialer$ echo
kazam.txt  mode.txt
Specialer$ echo
kazam.txt  mode.txt
Specialer$ echo "$(<kazim.txt)"
bash: kazim.txt: No such file or directory
Specialer$ echo "$(<kazam.txt)"
return 0 picoCTF{y0u_d0n7_4ppr3c1473_wh47_w3r3_d01ng_h3r3_38f5cc78}
Specialer$
```