Lesson 1: Some MISC Challenges

The weird things you encounter.

flagbot (CTF@VIS)

August 30, 2024

Table of Contents

Goals and outlook

Goals of this Lesson

- Some basic Misc stuff (explanation)
- Approaching a Miscellaneous Challenge (quick demo)
- Example: Linux permissions and basic commands (explanation)
- Running Docker (explanation)
- A proof-of-work (challenge)

Discord Invite Link

Basic infos and tipps

Miscellaneous Challenges in General

- Look at the Dockerfile (contains lots of info)
  - Versions up-to date?
  - Sus PHP backdoor version?
- Beware of malicious challenges (might execute any stuff)
  - Docker-compose?
  - Un-containerized binaries?
- Where is the flag?
- What are the interaction points?
  - What would be ways to get the flag?
  - What do we need to do that?

Miscellaneous Challenges in General

- Bash? $\rightarrow$ Shellcheck!
- Open Source? $\rightarrow$ Check Issues

  Closed ones as well
- Documentation? $\rightarrow$ Skim it.

  Anything in the challenge looking different? Might be on purpose to make the challenge work.

  Weird command options in the man page?

  "Bugs" section of man page

Approaching a Miscellaneous Challenge

Misc by example - Hidden Sheets

- Full disclousure: Not done this challenge, might mess it up

Linux basics for Misc challenges

Linux basic commands

- Commands:
  - touch, ls, cd, rm, echo, cat, nc, whoami, vim, nano, ssh
- Permissions:
  - How to make a program executable: `chmod +x myprogram`
  - How to view permissions: `ls -la myprogram`
- What is `sudo`?

Linux basic commands (by example)

```
generic@motorbrot:~$ mkdir Downloads/example-dir
generic@motorbrot:~$ cd ~/Downloads/example-dir
generic@motorbrot:~/Downloads/example-dir$ touch asdf
generic@motorbrot:~/Downloads/example-dir$ cat "second file" > 2nd_file.txt
cat: 'second file': No such file or directory
generic@motorbrot:~/Downloads/example-dir$ echo "second file" > 2nd_file.txt
generic@motorbrot:~/Downloads/example-dir$ echo 2nd_file.txt
2nd_file.txt
generic@motorbrot:~/Downloads/example-dir$ cat 2nd_file.txt
second file
generic@motorbrot:~/Downloads/example-dir$ ls -la
total 62
drwxrwxr-x  2 generic generic   4 Feb 28 15:33 .
drwxr-xr-x 53 generic generic 245 Feb 28 15:32 ..
-rw-rw-r--  1 generic generic  12 Feb 28 15:33 2nd_file.txt
-rw-rw-r--  1 generic generic   0 Feb 28 15:33 asdf
generic@motorbrot:~/Downloads/example-dir$ chmod +x asdf
generic@motorbrot:~/Downloads/example-dir$ ./asdf
generic@motorbrot:~/Downloads/example-dir$ ls -la
total 62
drwxrwxr-x  2 generic generic   4 Feb 28 15:33 .
drwxr-xr-x 53 generic generic 245 Feb 28 15:32 ..
-rw-rw-r--  1 generic generic  12 Feb 28 15:33 2nd_file.txt
-rwxrwxr-x  1 generic generic   0 Feb 28 15:33 asdf
generic@motorbrot:~/Downloads/example-dir$ echo "echo hello" >> asdf
generic@motorbrot:~/Downloads/example-dir$ ./asdf
hello
```

Linux basics links

- Symbolic Links (short symlinks) and hardlinks (actual file)
- Useful e.g. to redirect hard-coded database location to elsewhere
- Can be used for shenanigans:
  - If you are constrained to stay within a "jail directory", maybe only checked if path starts with /jail. So /jail/mysymlink would work to get to elsewhere.
  - Devs often don't think about what happens if a symlink is input.

Changing file attributes

- Does not show up in `ls -la`
- Requires root or specific capabilities for certain flags
- `+i` to make immutable, `-i` to remove immutability
- `+a` to "make file append-only"
- More in the man page
- Rarely useful doing that in a challenge - except maybe A/D
- Good to have heard of when something is behaving weirdly
- `lsattr`

What is / Using Docker

- Building
  - `docker build -t mytag .`
- Running
  - `docker run -p8888:1337 -it mytag`
- Building and Running without tagging
  - `docker run -p8888:1337 -it $( docker build -q .  )`
- Inspecting the running container from the inside
  - `docker ps`
  - `docker exec -it 8182a21 /bin/bash`

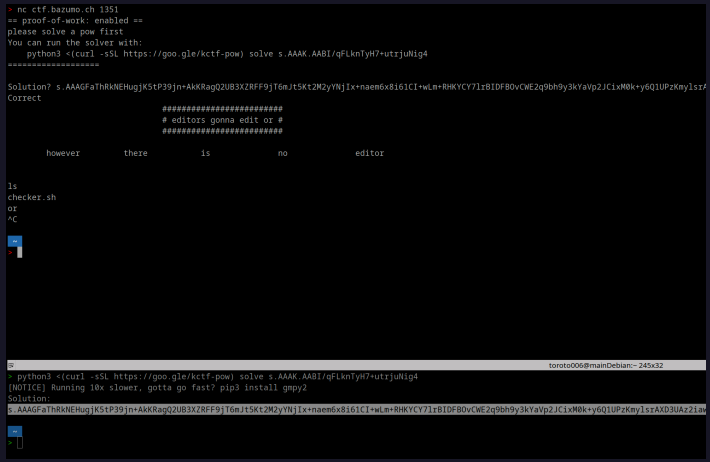
What is / Using Docker

- Overview
  - `docker image list`
  - `docker container list`
- Cleaning
  - `docker container rm 123123123`
  - `docker image rm 12318ab`
  - `docker system prune`

Challenges to play for you

Editors are everything, right? (POW)

`nc ctf.bazumo.ch 1351`



Whystudies1

http://ctf.bazumo.ch:1353
https://cdn.vis.ethz.ch/ctf/whystudies1

Whystudies2

http://ctf.bazumo.ch:1354
https://cdn.vis.ethz.ch/ctf/whystudies2