SAST 2022 Summer Training
CTF | A Warmup for Linux

By c7w

1 Introduction

本次作业的目标是熟悉 Linux 系统中的一些基本操作。为保证趣味性，我们沿用以往的传统，采用 CTF（Capture the Flag） 的形式进行。我们会为每位同学配置一个虚拟的 Linux 服务器环境，你需要登入这个环境中，并在其中寻找类似于 `SAST2022{*******}` 的字符串，如 `SAST2022{DocReader}`，我们将这种字符串称为 “Flag”。每当你找到一个 “Flag”，你就可以通过主目录下的提交程序进行提交。

1.1 服务器连接

我们会按照报名问卷的填写情况为大家分配服务器账号，在获取到你的服务器用户名、IP 地址与账号后，请使用以下命令连接到服务器：

```
ssh <Username>@<Server IP> -p <Server Port>
```

1.2 提交方式

使用你的家目录下的 `./submit` 程序进行提交，提交格式为：

```
./submit <你的学号> SAST2022{************}
```

在提交之后，程序会输出你的提交结果。可能的情况包括：

- Wrong Answer：提交的 Flag 错误
- Accepted：提交了正确的 Flag

访问 http://121.5.165.232:12000/ 查看当前 “Flag” 的获取情况。排行榜先按获得的 “Flag” 的总“分数”降序排列，在“分数”相同的情况下按“最后一次提交时间”升序排列。

1.3 提示与注意事项

- 藏匿的 Flag 可能有多种存在形式，它可能在某个文本文件中，可能是文件的名字，也可能是程序的输出内容。
- 我们会给出所有基础与进阶 “Flag” 的提示与所有基础 “Flag” 的解答，但我们不会给出任何有关彩蛋 “Flag” 的信息。
- 欢迎与其他人交流思路，但请不要直接将 “Flag” 告诉别人，这样会影响其他人的游戏体验。
- 提交 “Flag” 的服务用了个人服务器搭建，在安全性与效率方面未做考量，请不要尝试攻击。
- 如果你忘记了 Linux 的基础教程或之前从未接触过 Linux，请先浏览一遍 Linux 教程入门。当然，下面的任务并不会都在教程中出现，因此结合任务提示，**善用 `man` 命令与搜索引擎是我们想教会你的技能** :)

2 Knowledge Base

1. 我为什么要学 Linux

从学习的角度来说，Linux 系统更加贴近于我们未来几年将要学习的系统结构、组成原理、网络原理等等课程，更加有利于我们理解“计算机”是一个怎样的工具，理解其背后的运作原理。

从应用的角度来说，不管是今后要做科研方面的学习，还是要做开发方面的学习，还是要做系统运维方面的学习，你所接触的绝大部分服务器乃至服务器集群都是依托于 Linux 系统的。如果你未来想从事计算机领域有关的工作，那么掌握 Linux 系统的使用技巧是避不开的学习环节 :(

2. 我该怎么学 Linux

鉴于我们假设同学们之前或多或少地接触过了一些命令的使用技巧（不管是计算机系的一字班新生基础技能培训，还是 OOP 课程中对有关命令的介绍），我们对 Linux 不设一节专门的课程讲解，仅提供本次作业供大家练手。当然，从头学起也没有关系，网络上的 Linux Tutorial 数不胜数，养成会用 Google 的好习惯是非常有必要的。

在本次作业中，你**可能**会用到如下命令，请首先了解它们的作用：`man`，`ssh`，`cd`，`ls`，`cat`，`chmod`，`tmux`，`vim`，`nano`，`unzip`，`scp`，`find`，`grep`，`git`，`su`... 除此之外，你还应该了解**输入输出重定向**等实用技能。

> 我该怎么查找一个命令的使用方法？这里以 `scp` 命令为例进行说明。
>
> ① 查看命令提示。输入 `scp --help` 或者 `man scp` 查看提示。比如，利用后者我们可以清楚地看到这个命令的功能，它允许的必选参数、可选参数都有哪些。
>
> ② 使用搜索引擎。你永远可以相信 Google 的能力。我们输入 `scp linux command` 等搜索关键字，便可以看到一个命令的教程与例子。

3. 关于镜像分配

鉴于我们的计算资源有限，我们会为班号为 `{计**，计**-经**，经**-计**，计科**，智**，量信**}` 的同学们优先分配服务器账号。如果你没有被分配到服务器账号也没有关系，你可以通过安装 WSL / 安装 Linux 虚拟机 / 使用 Docker 安装 Linux 镜像等方式接触到 Linux 系统。当然，对于本次作业来说，最便捷的方式便是直接拉取下述的 Docker 镜像并映射 22, 80, 3306, 10001, 10002 端口到宿主机。

3 Special Thanks

本次作业参考了 2021 年计算机系暑培 Linux 讲义与作业，感谢 @JuneTheRiver 的指导与帮助。本次作业镜像使用计算机系科协提供的 @Zeus 服务器进行分发，感谢它在 2#-308B 日日夜夜勤勤恳恳地工作。本次作业的镜像上传到了 Docker Hub，所编写代码将会在作业结束后全部开源，供后续培训设计时作为参考。

4 Basic Tasks

这些任务出现于 `/home/train/Puzzles` 文件夹下。（14 p.t.s × 6 = 84 p.t.s）

4.1 Storyteller

- The recorder seems to be broken... Why it cannot make any sound?
- *Hint*: Why cannot I execute the program? Maybe I need some additional file permission?
- Finally you can speak... But you wanna me wait u for 30 minutes?
- *Hint*: We could leave him alone talking his stories and head for other Flags first. Maybe after 30 minutes he'll shut up and give me the Flag.

4.2 Enigma

- We intercepted a signal related to The Flag.
- *Hint*: How can we replace and search for strings?

4.3 Memories

- A zipfile! How can I open it?
- A picture named `memories` inside... Again, how can I open it?
- *Hint*: Maybe we can download it from the server and view it locally?

4.4 Maze

- It is impossible I can walk out of the maze manually...
- *Hint*: We need ways to traverse the maze and filter useful infomation.

4.5 SCP-443

- The data was ERASED... I believe that there must be a backup somewhere.
- *Hint*: Are there any tools of version control able to remember the record for me?

4.6 .

- Is there still a task here?
- *Hint*: Maybe some files are hidden in the directory...

（Answers to these tasks are attached in the appendix）

5 Extra Tasks

这些任务分布在系统各处...你需要好好地探索整个系统。（4 p.t.s × 4 = 16 p.t.s）

5.1 Sudoer

- I wonder what mails my neighbor received.
- *Hint*: I cannot enter the home of my neighbor. Maybe I should check my mailbox.

5.2 TUNA

- The `apt-get` is too slow... How did we speed it up?
- *Hint*: https://mirrors.tuna.tsinghua.edu.cn/help/ubuntu/

5.3 Secret

- Every time I log in, a strange voice forces me to search for a "secret"...
- *Hint*: Every time I enter a shell, surely its configuration file of setting up environment variables would be loaded. Where is that file?
- *Hint*: We are not in `bash` shell, but `zsh` shell...
- *Hint*: What are the functions of these hidden files under my home directory?

5.4 Homeless

- Believe it or not, it is said that there is a homeless man on this server.
- *Hint*: Is there a file recording all users in the system?

6 Bonus Tasks

这些任务没有分布在服务器中，开心地寻找彩蛋吧 :)（1 p.t.s × 5 = 5 p.t.s）

- M * * *
- N * S *
- D * R *
- D * A *
- K * N *

其中 * 代表任意多个字符。

7 Appendix: Answers to Basic Tasks

- Storyteller
  - （文件权限）我们缺少文件运行权限
    - `chmod u+x storyteller`
  - （后台运行）我们需要让程序能够在后台运行
    - `tmux new -t storyteller` to create a tmux session
    - `./storyteller`
    - Press `Ctrl+B`, then `D` to detach from a tmux session
    - (After 30 minutes)
    - `tmux attach -t storyteller` to attach in a tmux session
    - Press `Ctrl+D` to end a tmux session
- Enigma
  - （文件编辑）我们需要掌握在 Linux 内使用文件编辑器的方式
    - 将 `[` 与 `]` 两个字符 **替换** 成空字符
    - 全文搜索 `SAST2022`
    - `vim` 和 `nano` 是两种常用的文件编辑器，这里我们讲解 `nano`
    - `vim Ciphered.txt` 或者 `nano Ciphered.txt`
    - Press `Ctrl + \`，搜索内容为 `[`，替换为空字串，按 `A` 全部替换
    - Press `Ctrl + \`，搜索内容为 `]`，替换为空字串，按 `A` 全部替换
    - Press `Ctrl + W`，搜索内容为 `SAST2022`
- Memories
  - （文件解压）解压缩包
    - `unzip -q Memories.zip`
  - （文件传输）我们需要掌握在服务器和本地之前传输文件的方式
    - `scp` 命令
      - （在**本地**）`scp -P <port> train@<server>:~/Puzzles/Memories/Memories.jpg .`
    - 使用 `FileZilla` 等客户端
- Maze
  - （遍历路径、命令间结果传递、过滤信息）
    - 首先阅读 `maze_builder.sh`，了解迷宫的生成方式
    - `find . | grep SAST`
      - `find .` 会输出什么？
      - `grep SAST` 进入交互模式后，对于输入的字符串会做什么操作？
- SCP-443
  - （Git）我们需要将文件恢复到以前的版本

    - `git log` 查看 commit 记录
    - 还原文件到某一版本（这两种方式有什么区别？）
        - `git checkout 0bb3 ./SCP-443`
        - `git reset --hard 0bb3`
    - `cat SCP-443 | grep SAST2022`

- .
    - （隐藏文件）我们需要查看目录中有哪些隐藏文件
        - `ls -a` 可以看到所有以 `.` 打头的隐藏文件