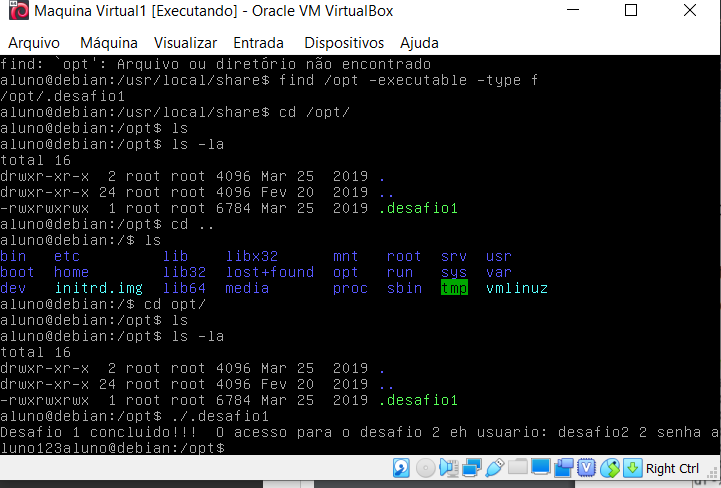
**Capturas de tela:**

**1.3.a) Encontrando o arquivo oculto:**

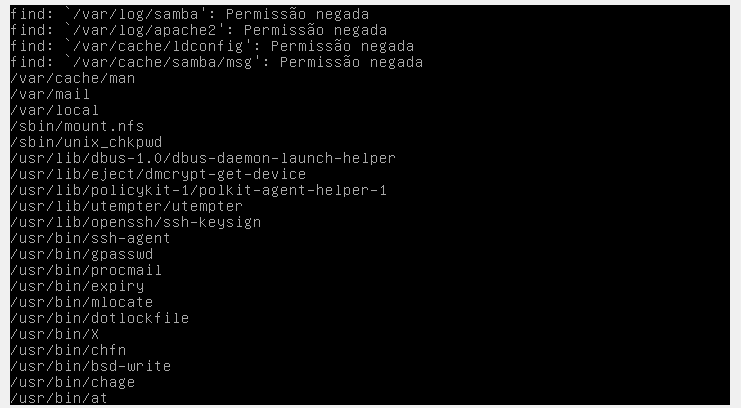


O arquivo oculto foi encontrado ao procurar em todas as pastas do sistema por arquivos ocultos através do comando acima.

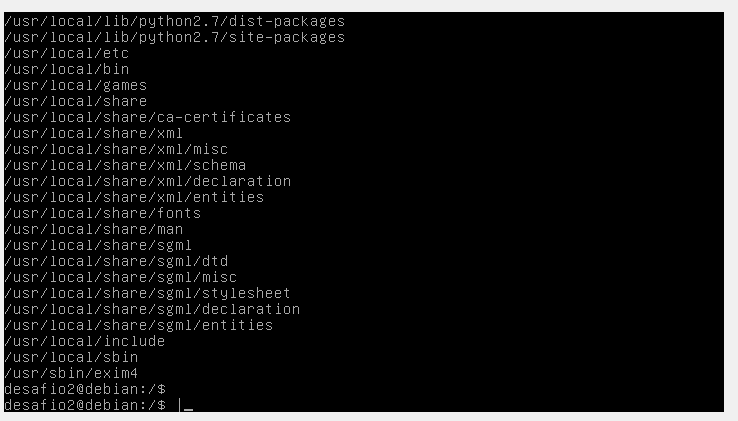
**1.3.b)** O “s”, nas permissões de arquivos significa que o arquivo sempre será executado com suas próprias permissões, não importa qual usuário o execute. O comando é: ***chmod u+s /path/to/file* .**

**Encontrando o arquivo malicioso:**

Usando o comando “find / -perm /6000”, foram encontrados os seguintes arquivos com este tipo de permissão:



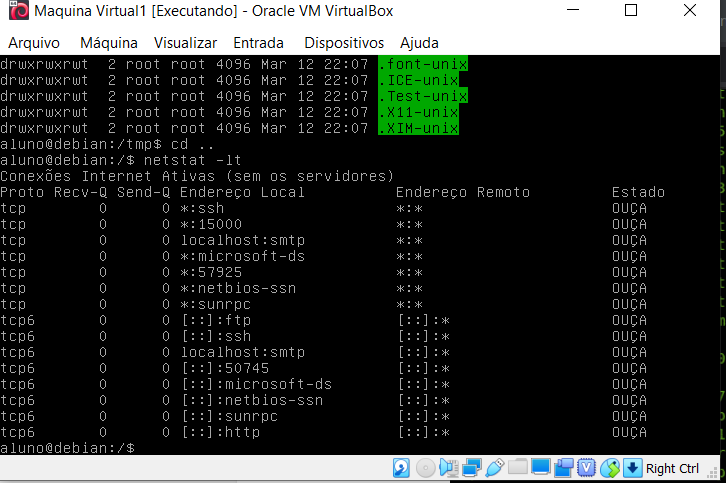




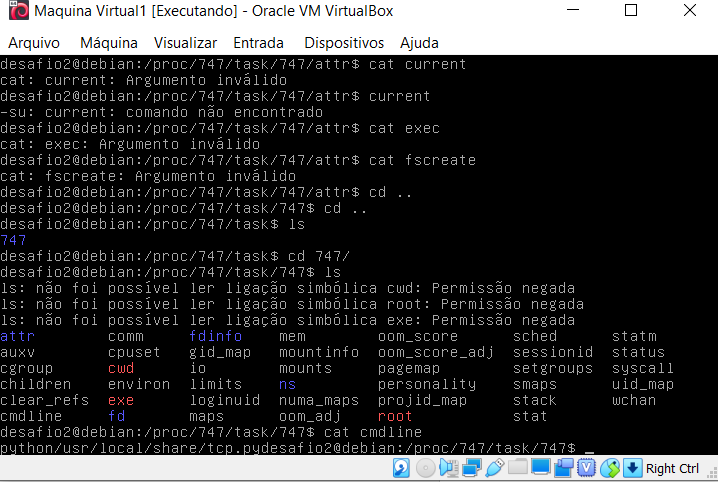
**1.3.c) Encontrando o processo malicioso:**

De maneira a encontrar o processo malicioso, foi adotada uma estratégia de procurar por portas que estão sendo usadas e que são suspeitas. Por isso, inicie procurando pelos serviços que estariam utilizando tais portas.

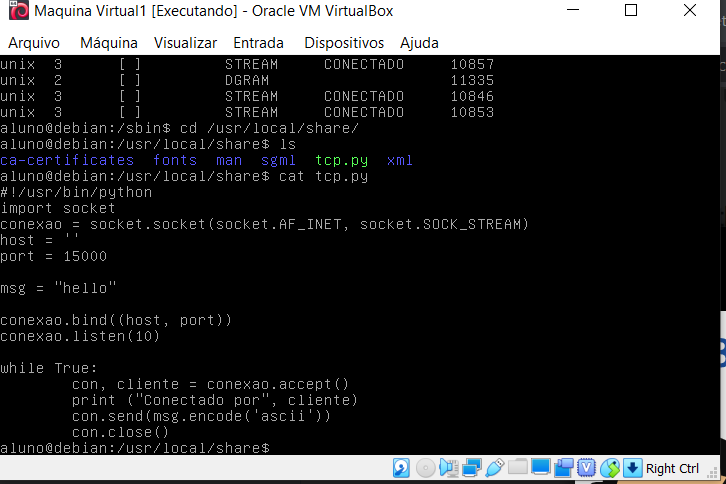
Usando netstat:



Em seguida, encontrei o PID do processo que estava utilizando esta porta e fui atrás do processo que ele estaria executando, acabei encontrando na seguinte pasta (através da linha de comando executada que deu origem a este processo):



Por fim, fui até o arquivo e encontrei o seguinte:



**Como ele é executado e onde se encontra:** python /usr/local/share/tcp.py

**Qual seu objetivo:** é um script que cria um socket que abre a comunicação através da porta 15000 para qualquer cliente.