Relatório

Alunos: Andrei Carvalho Torres Portugal e Marina Gabriela Alves Capelo

Professor: Rafael Lopes Gomes

Disciplina: Sistemas Operacionais

09 de Dezembro de 2022

- Utilizei uma VM rodando Debian 11.5
- Configurei um servidor de SSH remoto usando o OPEN-SSH dentro do Debian, o qual acessei via Windows Powershell.

Monitorando criação e remoção de arquivos em uma pasta

Criei e monitorei a pasta **Projeto _03** no diretório **/root .** Dentro dessa pasta **criei** os arquivos : **teste.txt** ; **teste_02.txt**. Em seguida, **removi** o arquivo **teste.txt.**

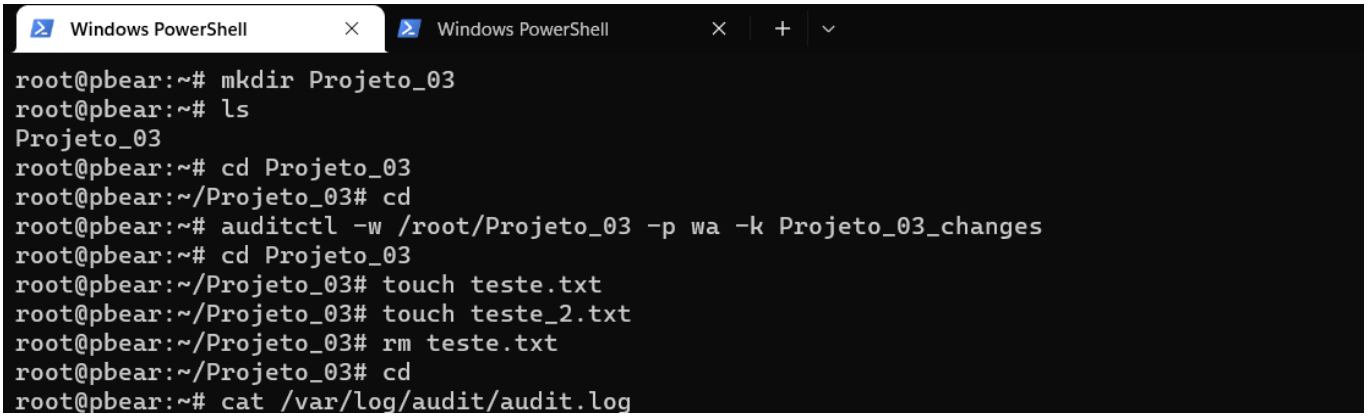
Determinei as seguintes regras de monitoramento para a pasta **Projeto_03** :

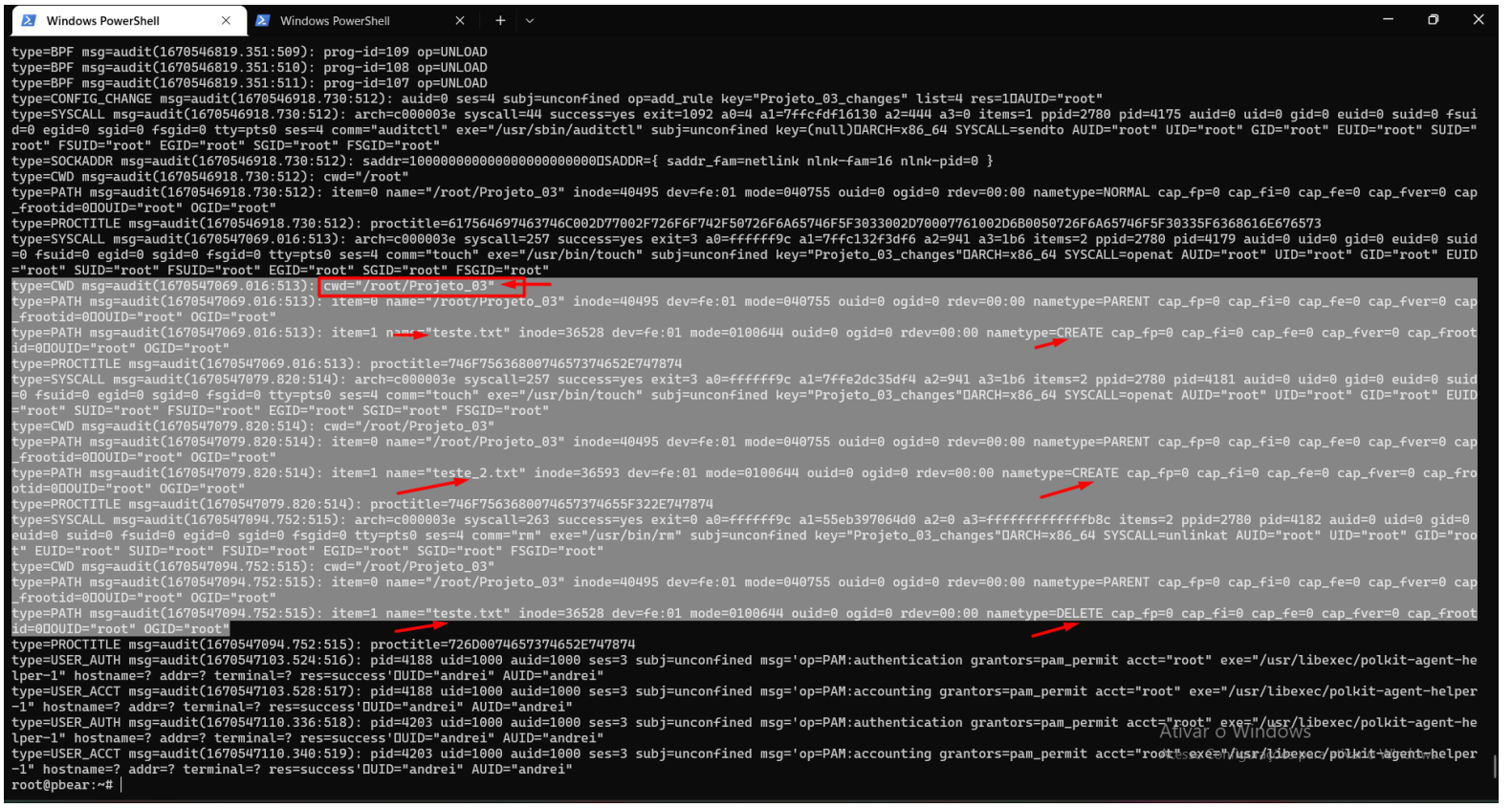
 # audittcl -w /root/Projeto_03/ -p wa -k Projeto_03_changes

-w <path> Insert watch at <path>
-p [r|w|x|a] Set permissions filter on watch
[r = read; w = write; x=execute; a=attribute]
-k <key> Set filter key on audit rule
[_changes]

Depois de tudo eu dou um **cat /var/log/audit/audit.log** para printar o log do audit. Onde ele vai me mostrar os eventos que ocorreram.

- Tudo isso é possível observar nas imagens abaixo :

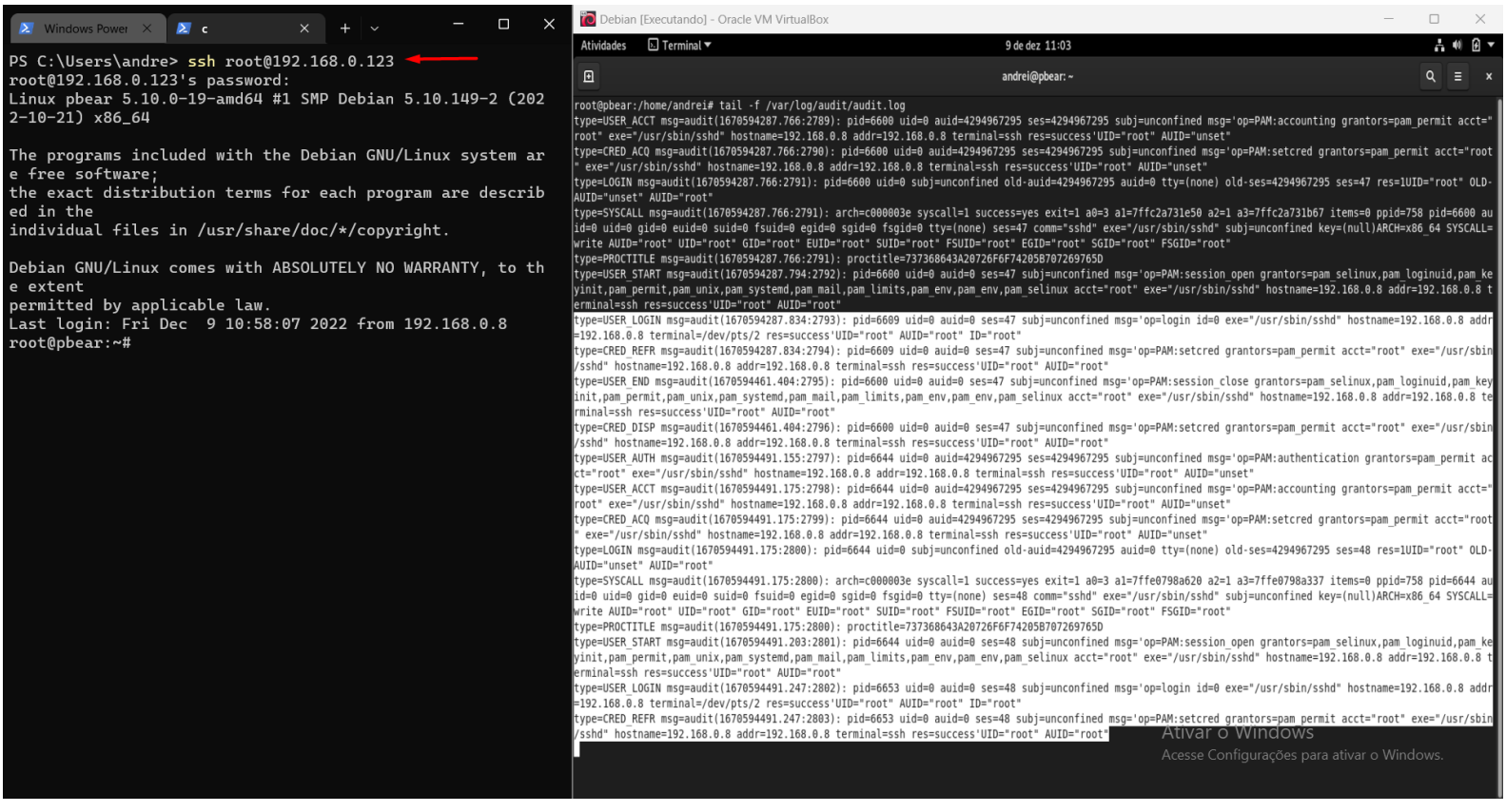


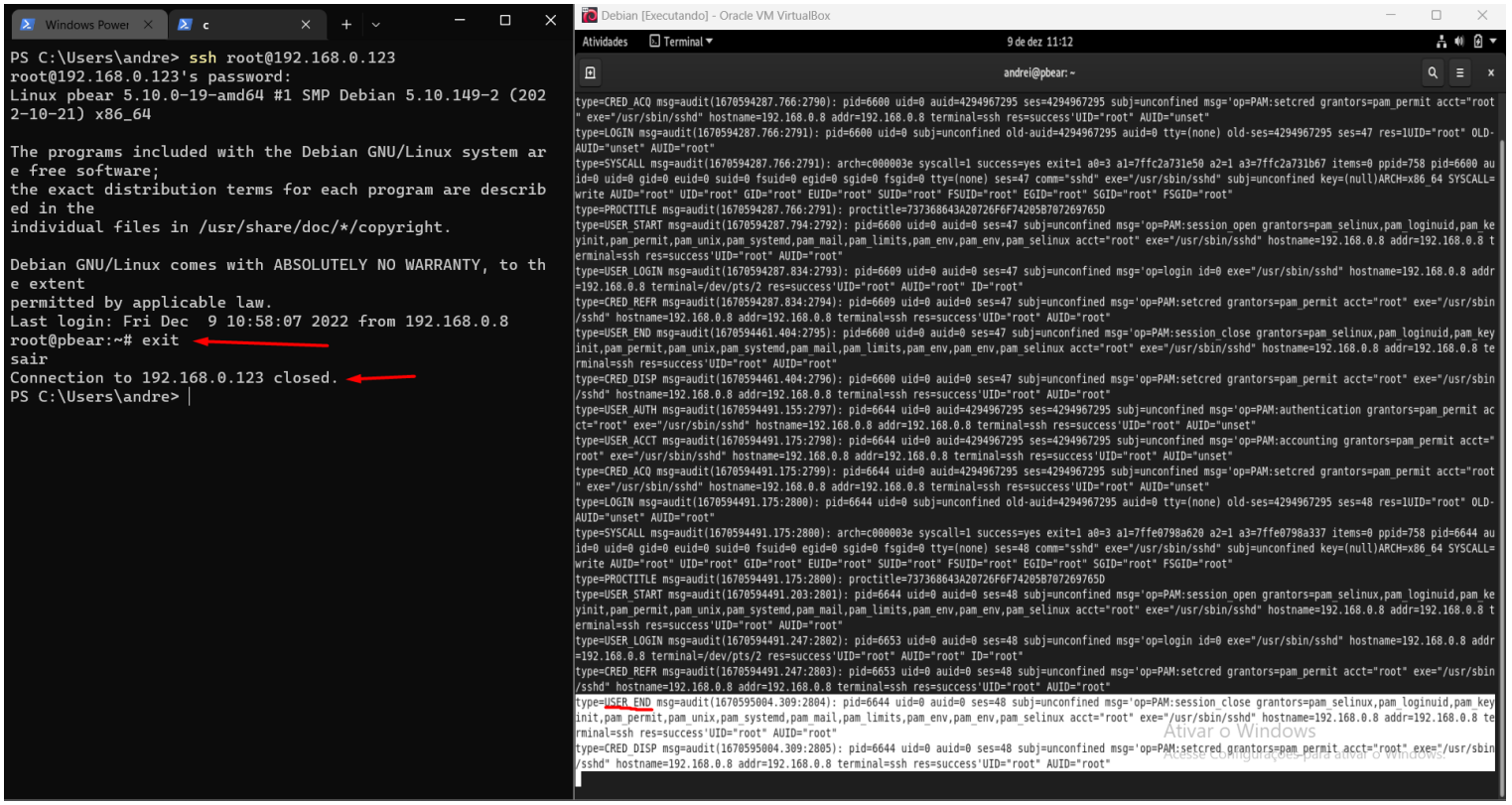


Monitoramento de Syscall

Monitorei a entrada e saída de um usuário na máquina virtual remotamente, via WIndows PowerShell. Usando ssh, a fim de monitorar o processo sshd.

- Monitoramento da Syscall do sshd, afim de detectar o **login**





- Monitoramento da Syscall do sshd, afim de detectar o **logoff**