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

<u>-w <path></path></u>	Insert watch at <path></path>
<u>-p [r w x a]</u>	Set permissions filter on watch
[r = read; w = write; x=execute; a=attribute]	
-k <key></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 :

```
Windows PowerShell × | Windows PowerShell | X | + | V

root@pbear:~# mkdir Projeto_03

root@pbear:~# cd Projeto_03

root@pbear:~/Projeto_03# cd

root@pbear:~# auditctl -w /root/Projeto_03 -p wa -k Projeto_03_changes

root@pbear:~# cd Projeto_03

root@pbear:~/Projeto_03# touch teste.txt

root@pbear:~/Projeto_03# touch teste_2.txt

root@pbear:~/Projeto_03# rm teste.txt

root@pbear:~/Projeto_03# cd

root@pbear:~/Projeto_03# cd

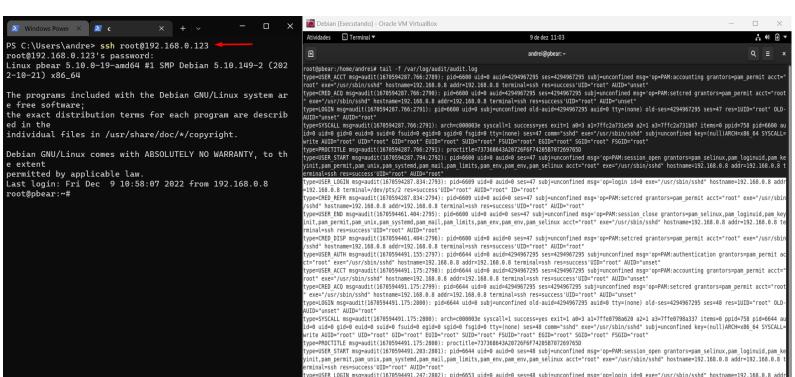
root@pbear:~# cat /var/log/audit/audit.log
```



Monitoramento de Syscall

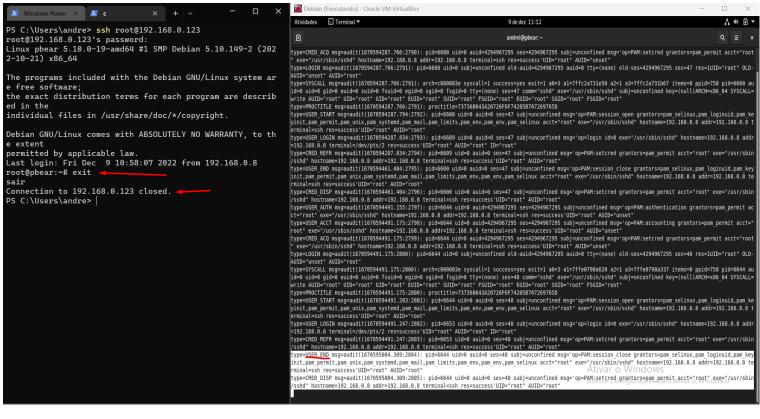
Monitorei a entrada e saída de um usuário na máquina virtual remotamente, via <u>WIndows PowerShell</u>. Usando <u>ssh</u>, a fim de monitorar o processo <u>sshd</u>.

Monitoramento da Syscall do sshd, afim de detectar o login



ype-user_tooim msg-audit[10703941:247:260; piu-uoo3 uud-audu-0 ses-40 subj-untoniinen msg- op-togin lu-0 eke- /usi/sbi 192.168.0.8 terminal=/dev/pts/2 res-success'UID="root" AUID="root" iD="root" iD="root" ype-CRED REFR msg-audit[1670594491.247:2803): pid-6653 uid=0 auid=0 ses-48 subj-unconfined msg-'op-PAM:setcred grantors-pam // sshd" hostname=192.168.0.8 addr=192.168.0.8 terminal=ssh res=success'UID="root" AUID="root"

Ativar o Window



Monitoramento da Syscall do sshd, afim de detectar o logoff