

# 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**.

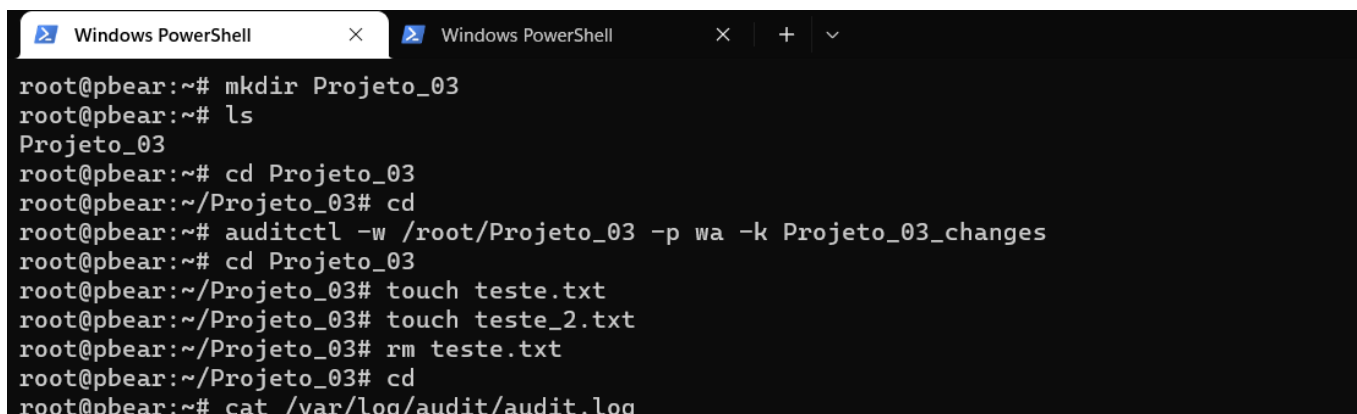
Determinei as seguintes regras de monitoramento para a pasta **Projeto\_03** :

**# auditctl -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 :



```
Windows PowerShell
root@pbear:~# mkdir Projeto_03
root@pbear:~# ls
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:~# cat /var/log/audit/audit.log
```

```
Windows PowerShell
```

```
type=BPF msg=audit(1670546819.351:509): prog-id=109 op=UNLOAD
type=BPF msg=audit(1670546819.351:510): prog-id=108 op=UNLOAD
type=BPF msg=audit(1670546819.351:511): prog-id=107 op=UNLOAD
type=CONFIG_CHANGE msg=audit(1670546918.730:512): audit=0 ses=4 subj=unconfined op=add_rule key="Projeto_03_changes" list=4 res=10AUDID="root"
type=SYSCALL msg=audit(1670546918.730:512): arch=c000003e syscall=44 success=yes exit=1092 a0=4 al=7fffcdcf16130 a2=444 a3=0 items=1 ppid=2780 pid=4175 audit=0 uid=0 gid=0 fsuid=0 euid=0 suid=0 sgid=0 fsgid=0 tty=pts0 ses=4 comm="audittctl" exe="/usr/sbin/audittctl" subj=unconfined key=(null)DARCH=x86_64 SYSCALL=sendto AUDID="root" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" FSGID="root" SGID="root" FSGID="root"
type=SOCKADDR msg=audit(1670546918.730:512): saddr=10000000000000000000000000SADDR={ saddr_fam=netlink nlnk=fam=16 nlnk-pid=0 }
type=CWD msg=audit(1670546918.730:512): cwd="/root"
type=PATH msg=audit(1670546918.730:512): item=0 name="/root/Projeto_03" inode=40495 dev=fe:01 mode=040755 uid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap-fi=0 cap-fe=0 cap_fver=0 cap_froot=000UID="root" OGID="root"
type=PROCTITLE msg=audit(1670546918.730:512): proctitle=617564697463746C0E2D770E2F726F742F50726FA65746F5F30330E2D70007761002D6B0050726FA65746F5F30335F6368616E676573
type=SYSCALL msg=audit(1670547069.016:513): arch=c000003e syscall=27 success=yes exit=3 a0=ffffffffffc al=7ffcf32f3df6 a2=941 a3=1b6 items=2 ppid=2780 pid=4179 audit=0 uid=0 gid=0 fsuid=0 euid=0 suid=0 sgid=0 fsgid=0 tty=pts0 ses=4 comm="touch" exe="/usr/bin/touch" subj=unconfined key="Projeto_03_changes"DARCH=x86_64 SYSCALL=openat AUDID="root" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=CWD msg=audit(1670547069.016:513): cwd="/root/Projeto_03"
type=PATH msg=audit(1670547069.016:513): item=0 name="/root/Projeto_03" inode=40495 dev=fe:01 mode=040755 uid=0 ogid=0 rdev=00:00 nametype=PARENT cap_fp=0 cap-fi=0 cap-fe=0 cap_fver=0 cap_froot=000UID="root" OGID="root"
type=PATH msg=audit(1670547069.016:513): item=1 name="/teste.txt" inode=36528 dev=fe:01 mode=0100644 uid=0 ogid=0 rdev=00:00 nametype=CREATE cap_fp=0 cap-fi=0 cap-fe=0 cap_fver=0 cap_froot=000UID="root" OGID="root"
type=PROCTITLE msg=audit(1670547069.016:513): proctitle=746F7563680074657374655E747874
type=SYSCALL msg=audit(1670547079.820:514): arch=c000003e syscall=257 success=yes exit=3 a0=ffffffffffc al=7ffefdc35df4 a2=941 a3=1b6 items=2 ppid=2780 pid=4181 audit=0 uid=0 gid=0 fsuid=0 euid=0 suid=0 sgid=0 fsgid=0 tty=pts0 ses=4 comm="touch" exe="/usr/bin/touch" subj=unconfined key="Projeto_03_changes"DARCH=x86_64 SYSCALL=openat AUDID="root" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=CWD msg=audit(1670547079.820:514): cwd="/root/Projeto_03"
type=PATH msg=audit(1670547079.820:514): item=0 name="/root/Projeto_03" inode=40495 dev=fe:01 mode=040755 uid=0 ogid=0 rdev=00:00 nametype=PARENT cap_fp=0 cap-fi=0 cap-fe=0 cap_fver=0 cap_froot=000UID="root" OGID="root"
type=PATH msg=audit(1670547079.820:514): item=1 name="/teste_2.txt" inode=36593 dev=fe:01 mode=0100644 uid=0 ogid=0 rdev=00:00 nametype=CREATE cap_fp=0 cap-fi=0 cap-fe=0 cap_fver=0 cap_froot=000UID="root" OGID="root"
type=PROCTITLE msg=audit(1670547079.820:514): proctitle=746F7563680074657374655F322E747874
type=SYSCALL msg=audit(1670547094.752:515): arch=c000003e syscall=263 success=yes exit=0 a0=ffffffffffc al=55eb3970640 a2=0 a3=fffffffffffffffbc items=2 ppid=2780 pid=4182 audit=0 uid=0 gid=0 fsuid=0 euid=0 suid=0 sgid=0 fsgid=0 tty=pts0 ses=4 comm="rm" exe="/usr/bin/rm" subj=unconfined key="Projeto_03_changes"DARCH=x86_64 SYSCALL=unlinkat AUDID="root" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=CWD msg=audit(1670547094.752:515): cwd="/root/Projeto_03"
type=PATH msg=audit(1670547094.752:515): item=0 name="/root/Projeto_03" inode=40495 dev=fe:01 mode=040755 uid=0 ogid=0 rdev=00:00 nametype=PARENT cap_fp=0 cap-fi=0 cap-fe=0 cap_fver=0 cap_froot=000UID="root" OGID="root"
type=PATH msg=audit(1670547094.752:515): item=1 name="/teste.txt" inode=36528 dev=fe:01 mode=0100644 uid=0 ogid=0 rdev=00:00 nametype=DELETE cap_fp=0 cap-fi=0 cap-fe=0 cap_fver=0 cap_froot=000UID="root" OGID="root"
type=PROCTITLE msg=audit(1670547094.752:515): proctitle=726D0074657374652E747874
type=USER_AUTH msg=audit(1670547103.524:516): pid=4188 uid=1000 audit=1000 ses=3 subj=unconfined msg='op:PAM:authentication grantors=pam_permit acct="root" exe="/usr/libexec/polkit-agent-helper-1" hostnames=? addr=? terminal=? res=success'UIDID="andreia" AUID="andreia"
type=USER_ACCT msg=audit(1670547103.528:517): pid=4188 uid=1000 audit=1000 ses=3 subj=unconfined msg='op:PAM:accounting grantors=pam_permit acct="root" exe="/usr/libexec/polkit-agent-helper-1" hostnames=? addr=? terminal=? res=success'UIDID="andreia" AUID="andreia"
type=USER_AUTH msg=audit(1670547110.336:518): pid=4203 uid=1000 audit=1000 ses=3 subj=unconfined msg='op:PAM:authentication grantors=pam_permit acct="root" exe="/usr/libexec/polkit-agent-helper-1" hostnames=? addr=? terminal=? res=success'UIDID="andreia" AUID="andreia"
type=USER_ACCT msg=audit(1670547110.340:519): pid=4203 uid=1000 audit=1000 ses=3 subj=unconfined msg='op:PAM:accounting grantors=pam_permit acct="root" exe="/usr/libexec/polkit-agent-helper-1" hostnames=? addr=? terminal=? res=success'UIDID="andreia" AUID="andreia"
root@pear:~#
```

## 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**

The image displays two terminal windows side-by-side. The left window is a Windows PowerShell prompt with the user 'andre' at 'PS C:\Users\andre>'. The user has executed the command 'ssh root@192.168.0.123', and the terminal shows the SSH connection process, including the password prompt and the login banner for Debian GNU/Linux. The right window is a Debian GNU/Linux terminal with the user 'andre' at 'andre@pbear:~'. The user has executed the command 'tail -f /var/log/audit/audit.log', which displays a large amount of SELinux audit logs, including messages about process creation, file access, and SELinux context changes.

