

Practica 07 Ej 3

Verifica la auditoria de control de acceso “Visor de sucesos” de dicho usuario en Windows y Linux.

Practica 07 Ej 3

Windows

Accedo al Visor de evento busco por auditorias correctas y con el ID 4624

The screenshot shows the Windows Event Viewer application running on a virtual machine named 'Win10_SRI'. The left-hand pane displays the 'Visor de eventos (local)' tree, with 'Seguridad' selected under 'Registros de Windows'. The main pane shows a list of filtered events. The filter criteria are: 'Registro: Security; Origen: ; Palabra clave: win:AuditSuccess; Id. del evento: 4624'. There are 1,575 events matching these criteria. The table below shows the first six events, all of which are successful logons (ID 4624) from 'Microsoft Windows' at 18:20:58.

Palabras clave	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Auditoría correc...	06/10/2023 18:20:58	Microsoft Windo...	4624	Logon
Auditoría correc...	06/10/2023 18:20:58	Microsoft Windo...	4624	Logon
Auditoría correc...	06/10/2023 18:20:57	Microsoft Windo...	4624	Logon
Auditoría correc...	06/10/2023 18:20:49	Microsoft Windo...	4624	Logon
Auditoría correc...	06/10/2023 18:20:48	Microsoft Windo...	4624	Logon
Auditoría correc...	06/10/2023 18:20:48	Microsoft Windo...	4624	Logon

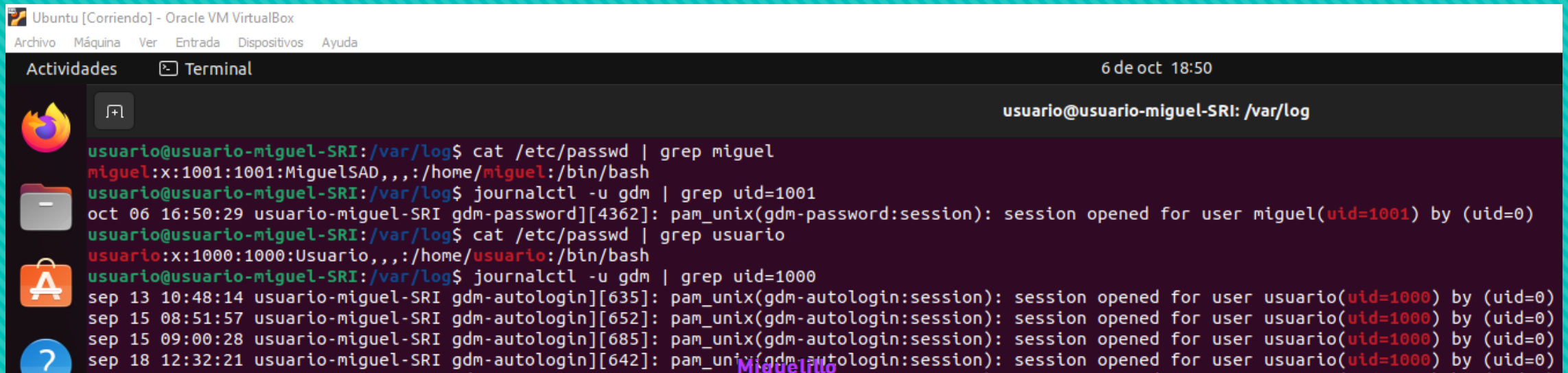
Below the table, the details for the selected event (ID 4624) are shown. The event description is 'Se inició sesión correctamente en una cuenta.' The 'Firmante' section shows the security ID as SYSTEM, the account name as DESKTOP-7PEK6DGS, and the domain as WORKGROUP. The 'Información de inicio de sesión' section shows the session type as 2, the administrator mode as restricted, and the account as virtual. The 'Nivel de suplantación' is 'Suplantación'. The 'Nuevo inicio de sesión' section shows the security ID as DESKTOP-7PEK6DG\MiguelSAD, the account name as MiguelSAD, and the domain as DESKTOP-7PEK6DG.

Miguelillo

Practica 07 Ej 3

Ubuntu

Primero miraremos el uid del usuario del que queremos ver los inicios de sesión consultando en passwd. Después con el comando journalctl -u gdm filtraremos por el uid para encontrarlo antes si no podemos ver todos los registros a mano



```
Ubuntu [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

Actividades  Terminal  6 de oct 18:50

usuario@usuario-miguel-SRI: /var/log

usuario@usuario-miguel-SRI:/var/log$ cat /etc/passwd | grep miguel
miguel:x:1001:1001:MiguelSAD,,,:/home/miguel:/bin/bash
usuario@usuario-miguel-SRI:/var/log$ journalctl -u gdm | grep uid=1001
oct 06 16:50:29 usuario-miguel-SRI gdm-password[4362]: pam_unix(gdm-password:session): session opened for user miguel(uid=1001) by (uid=0)
usuario@usuario-miguel-SRI:/var/log$ cat /etc/passwd | grep usuario
usuario:x:1000:1000:Usuario,,,:/home/usuario:/bin/bash
usuario@usuario-miguel-SRI:/var/log$ journalctl -u gdm | grep uid=1000
sep 13 10:48:14 usuario-miguel-SRI gdm-autologin[635]: pam_unix(gdm-autologin:session): session opened for user usuario(uid=1000) by (uid=0)
sep 15 08:51:57 usuario-miguel-SRI gdm-autologin[652]: pam_unix(gdm-autologin:session): session opened for user usuario(uid=1000) by (uid=0)
sep 15 09:00:28 usuario-miguel-SRI gdm-autologin[685]: pam_unix(gdm-autologin:session): session opened for user usuario(uid=1000) by (uid=0)
sep 18 12:32:21 usuario-miguel-SRI gdm-autologin[642]: pam_unix(gdm-autologin:session): session opened for user usuario(uid=1000) by (uid=0)
```