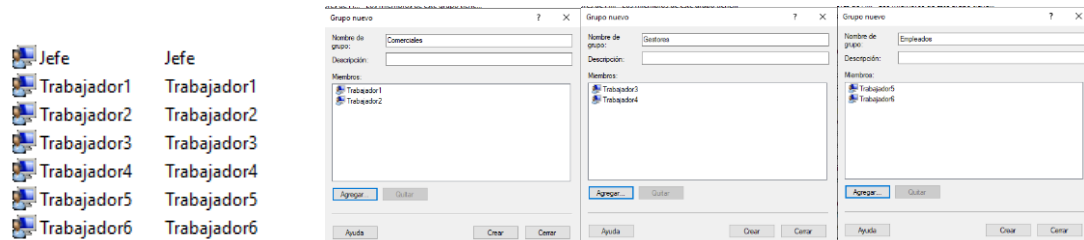


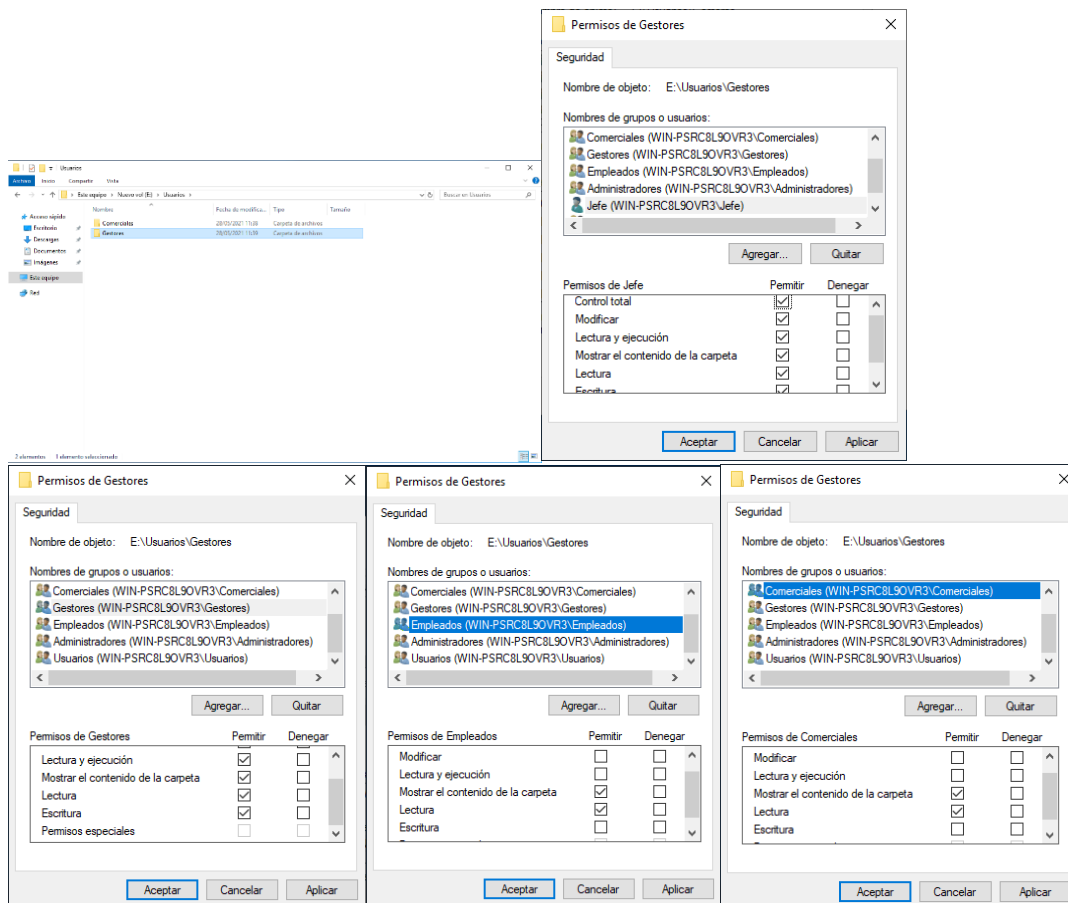
Desde una máquina virtual con Microsoft Windows y con la configuración de la tarjeta de red más oportuna entre las máquinas virtuales que intervengan:

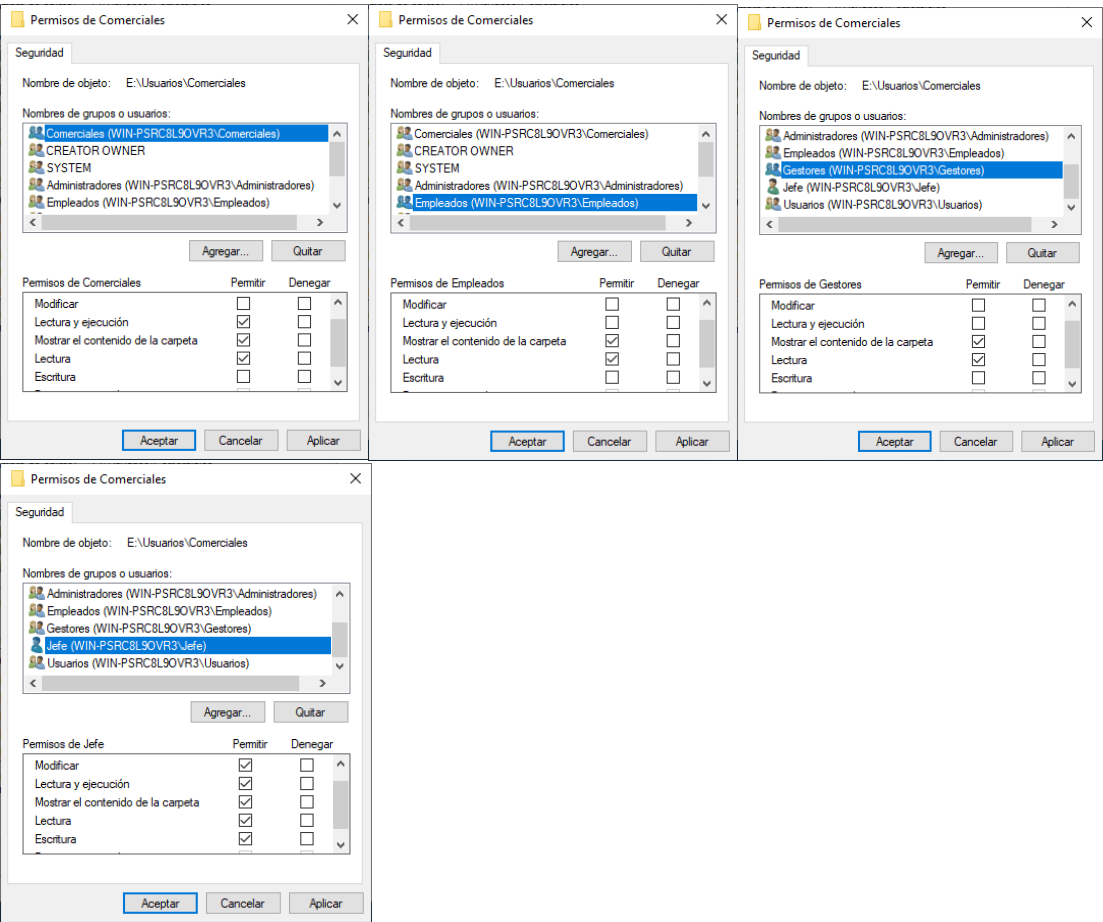
1. Permisos:

a) Crea un usuario llamado Jefe y los siguientes grupos de usuarios con al menos dos usuarios en cada uno de ellos: Comerciales, Gestores y Empleados



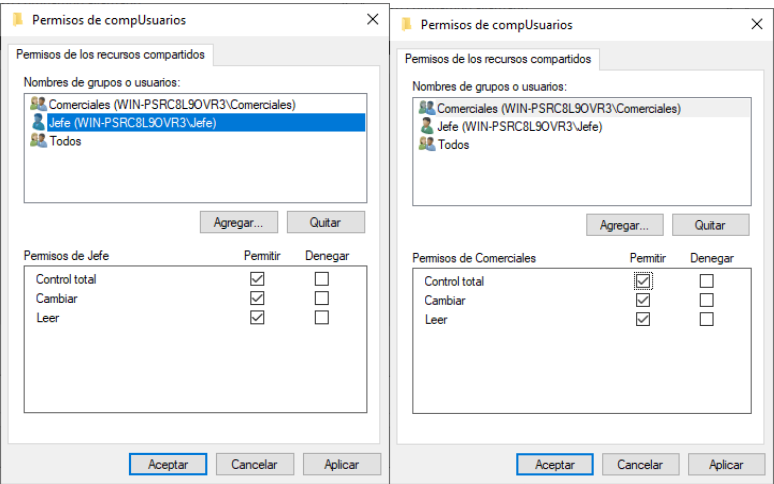
b) En una unidad de distinta a la del sistema operativo, crea una carpeta llamada Usuarios, que contenga otras dos: Comerciales y Gestores. A las carpetas Comerciales y Gestores tienen acceso todos los usuarios, pero solo los Gestores podrán modificar, leer y ejecutar sobre la carpeta Gestores. De igual forma, los usuarios del grupo Comerciales podrán modificar, leer y ejecutar sobre la carpeta Comerciales. El usuario Jefe será el único que pueda modificar los permisos de todas las carpetas



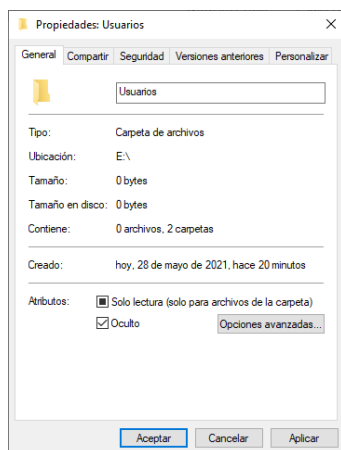


2. Permisos de red:

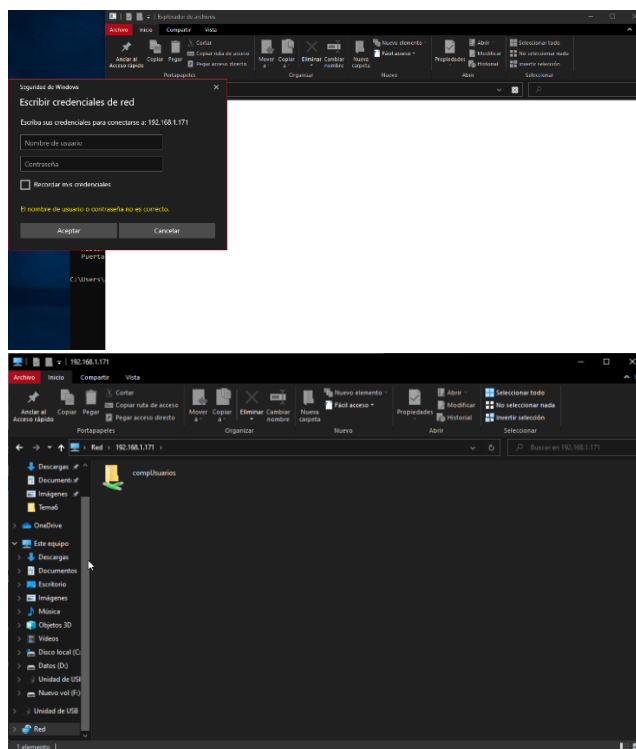
a) Comparte la carpeta Usuarios con el nombre compUsuarios para que solo los usuarios Comerciales y el usuario Jefe tengan acceso a ella desde otro equipo.



b)Modifica este último recurso compartido como oculto



c)Accede desde otro equipo al recurso compartido oculto anterior con un usuario con permisosd)Comprueba los recursos compartidos del equipo3.Derechos de usuarios. Realiza las acciones oportunas para que solo los Administradores del sistema y el usuario Jefe puedan apagar el equipo



4.Directivas de seguridad. Crea dos GPO para prohibir el acceso a 'Configuración de PC' y 'Panel de Control', así como cumplir los requisitos de complejidad de las contraseñas

Cumplir Complejidad Contraseña

Ámbito: Detalles Configuración Delegación

Vinculos

Mostrar vinculos en esta ubicación: eric.sospedra.com

Los siguientes sitios, dominios y unidades organizativas están vinculados a este GPO:

Ubicación	Exigido	Vinculo habilitado	Ruta
Domain Controllers	No	SI	eric.sospedra.com/Domain Controllers

Filtros de seguridad

La configuración en este GPO solo se puede aplicar a los grupos, usuarios y equipos siguientes:

Nombre

- Comerciales (ERIC/Comerciales)
- Empleados (ERIC/Empleados)
- Gerentes (ERIC/Gerentes)
- Jefe (ERIC/Jefe)
- Usuarios autenticados

Prohibir Configuración PC

Ámbito: Detalles Configuración Delegación

Vinculos

Mostrar vinculos en esta ubicación: eric.sospedra.com

Los siguientes sitios, dominios y unidades organizativas están vinculados a este GPO:

Ubicación	Exigido	Vinculo habilitado	Ruta
Domain Controllers	No	SI	eric.sospedra.com/Domain Controllers

Filtros de seguridad

La configuración en este GPO solo se puede aplicar a los grupos, usuarios y equipos siguientes:

Nombre

- Comerciales (ERIC/Comerciales)
- Empleados (ERIC/Empleados)
- Gerentes (ERIC/Gerentes)
- Jefe (ERIC/Jefe)

Propiedades: Apagar el sistema

Configuración de seguridad local Explicación

Apagar el sistema

Administradores

WIN-NBNIH0DG3UQ Jefe

Agregar usuario o grupo...

Quitar

Aceptar Cancelar Aplicar

Editor de administración de directivas de grupo

Panel de control

Configuración

Seleccione un elemento para ver su descripción.

Configuración

Estado

Comentario

Agregar o quitar programas	No configurada	No
Configuración regional y de idioma	No configurada	No
Impresoras	No configurada	No
Pantalla	No configurada	No
Personalización	No configurada	No
Programas	No configurada	No
Ocultar los elementos especificados del Panel de control	No configurada	No
Abrir siempre Todos los elementos del Panel de control al...	Habilitada	No
Prohibir el acceso a Configuración de PC y a Panel de control	No configurada	No
Mostrar solo los elementos especificados del Panel de control	No configurada	No
Visibilidad de la página de configuración	No configurada	No

Propiedades: La contraseña debe cumplir los requisitos de...

Configuración de directiva de seguridad Explicación

La contraseña debe cumplir los requisitos de complejidad

Definir esta configuración de directiva:

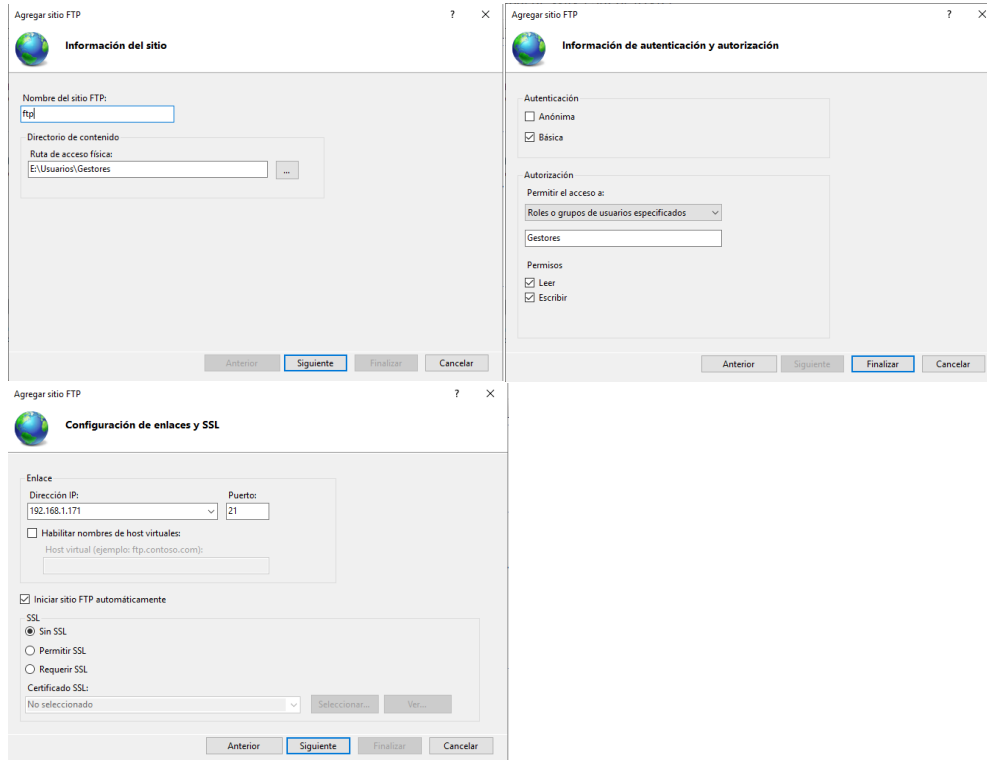
Habilitada

Deshabilitada

Aceptar Cancelar Aplicar

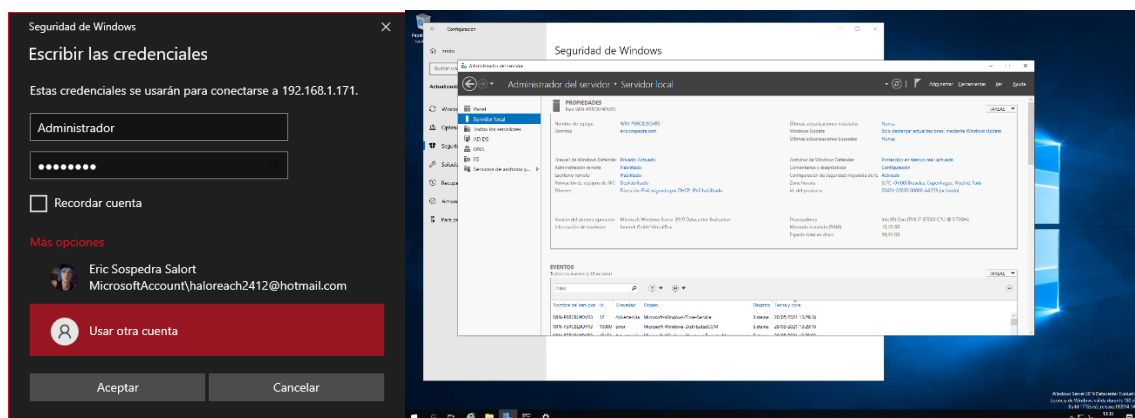
5.Servidores:

a)Instala un servidor FTP con acceso a la carpeta Gestores, de modo que solo los usuarios del grupo Gestores puedan hacer uso del servicio



b)Instala el servidor de aplicaciones de Windows en el equipo de modo que aparezca nuestro nombre y apellidos cuando accedamos a él (localhost). Para lo que debemos crear una página web muy simple y sustituirla por al predeterminada. Abre el puerto 80 mediante el Firewall de Windows para poder escuchar solicitudes de entrada HTTP.

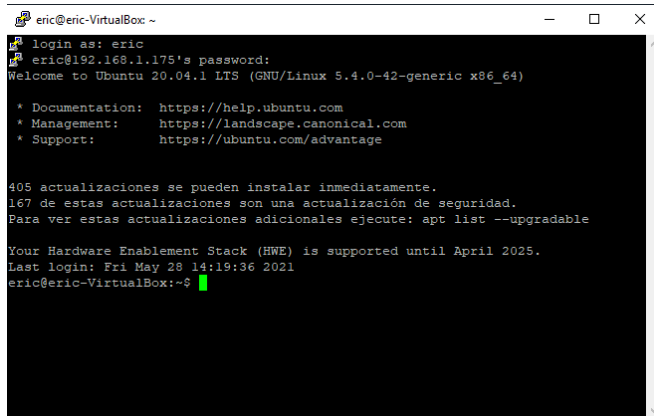
6.Conexión remota. Desde otro equipo con Microsoft Windows, accede al equipo mediante Conexión de escritorio remoto



7.Herramientas de seguridad:a)Cifra los archivos (si no existen, los creas) de la carpeta Comerciales con EFS.b)Cifra una unidad entera con BitLocker.

No me permite activar el bitlocker por culpa de que no puedo hacerlo sin una identificación TPM valida

c)Accede a otro equipo Ubuntu mediante una sesión SSH con la aplicación PuTTY (se deberá configurar previamente un servidor SSH en él).

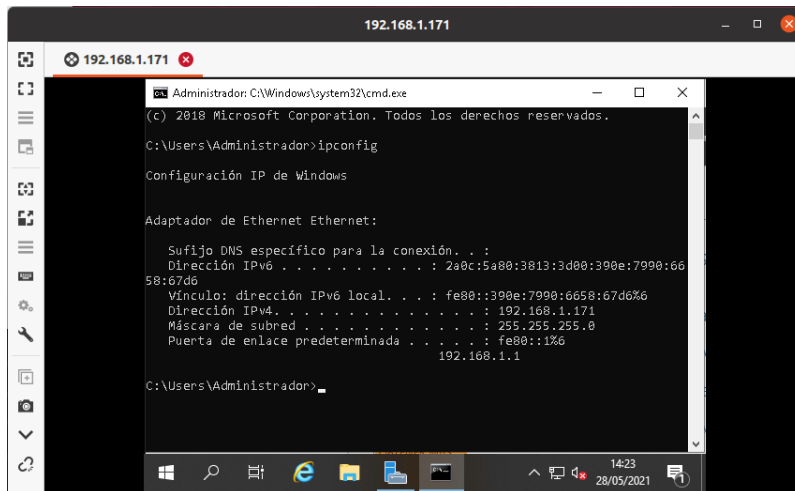


```
eric@eric-VirtualBox ~  
login as: eric  
eric@192.168.1.175's password:  
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-42-generic x86_64)  
  
 * Documentation:  https://help.ubuntu.com  
 * Management:    https://landscape.canonical.com  
 * Support:       https://ubuntu.com/advantage  
  
405 actualizaciones se pueden instalar inmediatamente.  
167 de estas actualizaciones son una actualización de seguridad.  
Para ver estas actualizaciones adicionales ejecute: apt list --upgradable  
  
Your Hardware Enablement Stack (HWE) is supported until April 2025.  
Last login: Fri May 28 14:19:36 2021  
eric@eric-VirtualBox:~$
```

Desde una máquina virtual con Ubuntu y con la configuración de la tarjeta de red más oportuna entre las máquinas virtuales que intervengan:

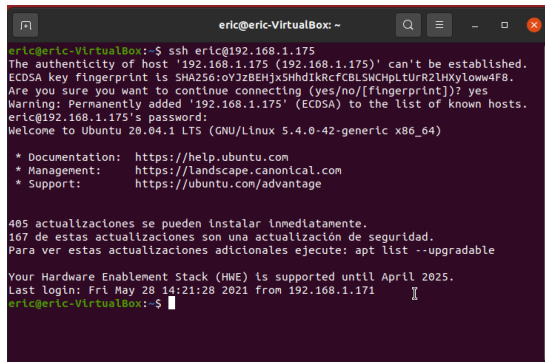
8.Conexión remota y herramientas de seguridad

a)Accede al equipo Windows anterior mediante la aplicación Remmina.



```
192.168.1.171  
Administrator: C:\Windows\system32\cmd.exe  
(C) 2018 Microsoft Corporation. Todos los derechos reservados.  
C:\Users\Administrador>ipconfig  
Configuración IP de Windows  
  
Adaptador de Ethernet Ethernet:  
Sufijo DNS específico para la conexión. . . :  
Dirección IPv6 . . . . . : 2a0c:5a00:3813:3d00:390e:7990:6658:67d6  
Vínculo: dirección IPv6 local. . . : fe80::390e:7990:6658:67d6%6  
Dirección IPv4. . . . . : 192.168.1.171  
Máscara de subred . . . . . : 255.255.255.0  
Puerta de enlace predeterminada . . . . : fe80::1%6  
192.168.1.1  
C:\Users\Administrador>
```

b)Accede a otro equipo Ubuntu mediante SSH por línea de comandos



```
eric@eric-VirtualBox: ~  
eric@eric-VirtualBox:~$ ssh eric@192.168.1.175  
The authenticity of host '192.168.1.175 (192.168.1.175)' can't be established.  
ECDSA key fingerprint is SHA256:0VJ28Ehja5MhdiKncfcalsWChpturR2lwyklow4F8.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.1.175' (ECDSA) to the list of known hosts.  
eric@192.168.1.175's password:  
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-42-generic x86_64)  
  
 * Documentation:  https://help.ubuntu.com  
 * Management:    https://landscape.canonical.com  
 * Support:        https://ubuntu.com/advantage  
  
485 actualizaciones se pueden instalar inmediatamente.  
167 de estas actualizaciones son una actualización de seguridad.  
Para ver estas actualizaciones adicionales ejecute: apt list --upgradable  
  
Your Hardware Enablement Stack (HWE) is supported until April 2025.  
Last login: Fri May 28 14:21:28 2021 from 192.168.1.171  
eric@eric-VirtualBox:~$
```

9.Descarga la versión Opensource Appliance CD basado en CentOS de Pandora FMS desde <https://sourceforge.net/projects/pandora/> e instálala en una máquina virtual siguiendo los pasos de instalación. A continuación, debemos:

- a)Detectar los dispositivos de la red
- b)Revisar los sistemas detectados
- c)Monitorizar el tráfico de red sobre una interfaz

10.Descarga e instala el sistema operativo Security Onion (<https://securityonion.net>). Después, haz uso de cualquier herramienta IDS apoyándote en la documentación técnica oficial.