ACTIVIDAD 4 – DOMINIOS

INTEGRACIÓN DE UNA MÁQUINA VIRTUAL LINUX EN UN DOMINIO WINDOWS SERVER

Diego Mucci

Seguridad Informática

18/04/2024

Actividad 4- Dominios

Integración de una Máquina Virtual Linux en un Dominio Windows Server

Justificación:

La integración de una máquina virtual con un sistema operativo Linux a un dominio previamente creado en Windows Server es una habilidad crucial en entornos de red empresariales heterogéneos. Esta tarea permite comprender y practicar cómo integrar diferentes sistemas operativos en un entorno de red unificado, lo que es fundamental para la administración eficiente y segura de redes empresariales.

Instrucciones:

Preparación del Entorno:

Asegúrate de tener acceso a una máquina virtual con un sistema operativo Linux instalado (p. ej., Ubuntu, CentOS, Debian, Kali, etc.).

Confirma que tienes acceso a un servidor Windows con Windows Server instalado y configurado como controlador de dominio.

Configuración de la Máquina Virtual Linux:

Inicia sesión en la máquina virtual Linux con privilegios de administrador o superusuario.

Actualiza el sistema operativo Linux para asegurarte de que esté al día.

Instala los paquetes necesarios para la integración con el dominio Windows Server. Dependiendo de la distribución de Linux que estés utilizando, puedes necesitar instalar paquetes como Samba, Winbind, Kerberos, etc.

Configuración de la Integración con el Dominio Windows:

Configura el archivo de configuración de Samba (/etc/samba/smb.conf) para que la máquina Linux pueda comunicarse con el dominio Windows.

Utiliza herramientas como net join o realm join para unir la máquina Linux al dominio Windows Server. Asegúrate de proporcionar las credenciales de administrador del dominio cuando se te soliciten.

Verifica que la máquina Linux se haya unido correctamente al dominio ejecutando comandos como net ads testjoin o realm list.

Pruebas y Verificación:

Realiza pruebas para asegurarte de que la integración se haya realizado correctamente. Esto puede incluir iniciar sesión con cuentas de usuario del dominio en la máquina Linux, acceder a recursos compartidos en el dominio, etc.

Verifica que los servicios de autenticación, como Kerberos, estén funcionando correctamente en la máquina Linux.

Documentación e Informe:

Documenta detalladamente los pasos que has seguido para integrar la máquina virtual Linux al dominio Windows Server.

Prepara un informe que incluya capturas de pantalla de los pasos realizados, descripciones de cualquier problema encontrado y cómo se resolvieron, así como cualquier otra observación relevante.

Recuerda que esta tarea no solo te permitirá practicar habilidades técnicas importantes, sino que también te ayudará a comprender la importancia de la interoperabilidad entre sistemas operativos en entornos empresariales.

A un dominio no unes un usuario Kali. El usuario lo defines en el dominio y luego utilizas un equipo, en el que te identificas como usuario de un dominio para unirlo al domino.

el cambio de hostname y la modificación de los ficheros de configuración dNS no era necesario realizarlos, si bien si que lo era establecer la IP del DNS en la propia tarjeta de red. Tampoco en condicions normales es necesario establecer el servidor NTP.

Perfecto, buen trabajo!!!!

10/10

1. Lo primero de todo seria tener algunos datos en cuenta:

   Nombre del servidor de dominio: **bosquempresa.local**

   IP del servidor de dominio: **192.168.10.100**
   Esta dirección IP es la IP de nuestro servidor o controlador de dominio, el cual cumplirá también el rol de DNS, por lo tanto, utilizaremos la misma IP al configurar el DNS.

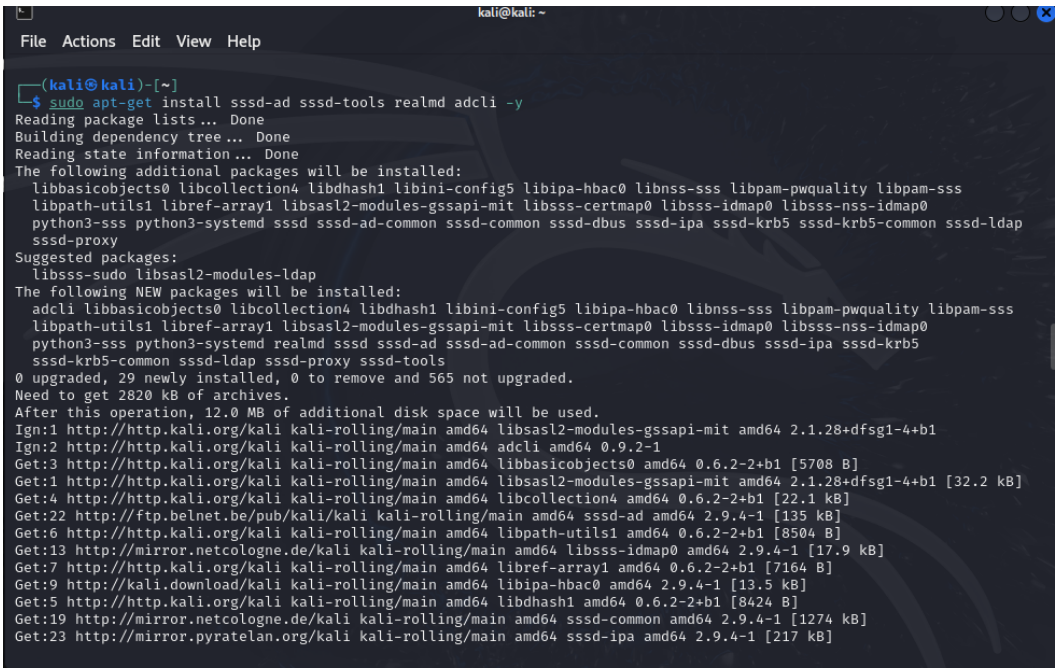
   Usuario Kali que vamos a unir al dominio**: kali**

2. Con la configuración de red de Kali Linux en NAT o Adaptador Puente, que es mediante la cual tendremos conexión a internet, vamos a actualizar la lista de paquetes disponibles ejecutando "sudo apt update". El gestor de paquetes *apt* busca en los repositorios configurados las últimas versiones de los paquetes disponibles, pero no instala ni actualiza ningún paquete en sí. Por lo tanto, después de ello, vamos ejecutar el comando "sudo apt upgrade" para instalar las nuevas versiones de estos paquetes en nuestro sistema.

   No se ha podido realizar captura de pantalla debido a que este paso se realizó más tarde porque fue uno de los errores que se dieron a la hora de unir la máquina virtual Kali Linux al dominio.

3. Cambiamos nuevamente la configuración de red de Kali Linux a Red Interna y una de las tarjetas de red de Windows Server debe estar también en Red Interna.

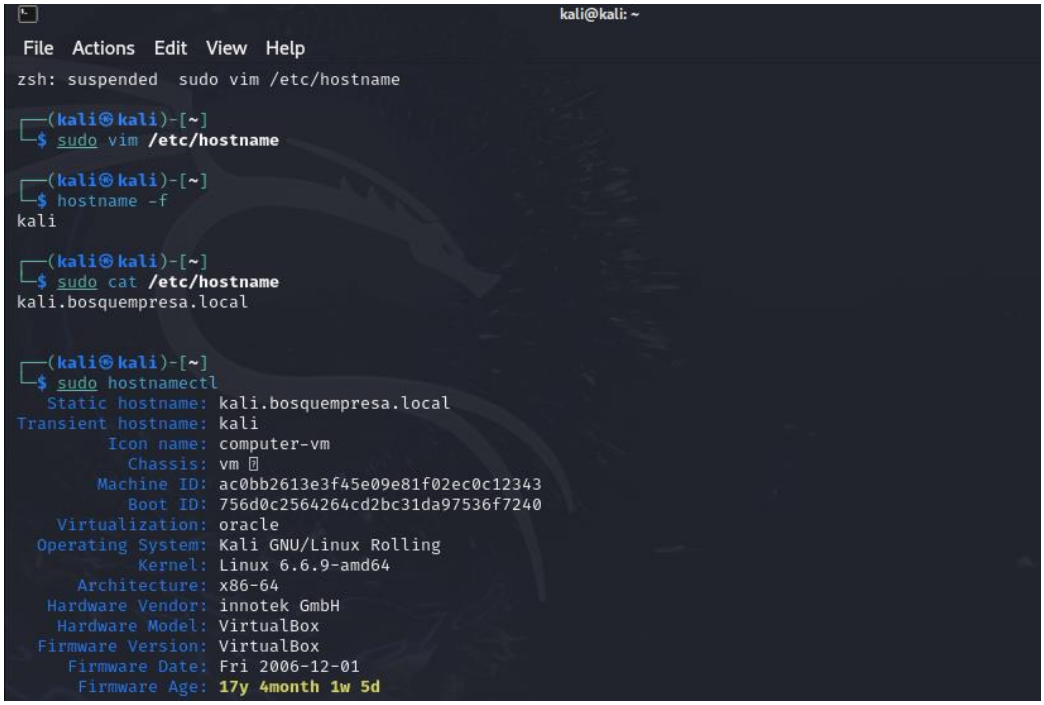
4. Instalar una serie de paquetes, llamada System Security Services Daemon (sssd), la cual va a manejar los accesos y traer la información de directorios remotos.



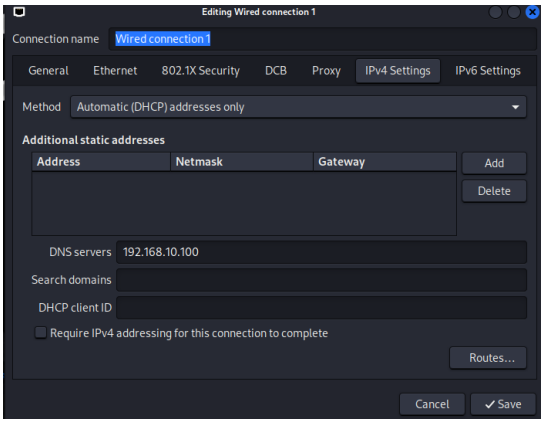
Otros paquetes fueron añadidos más tarde debido a errores que se ocasionaron. Ejecutamos el comando “sudo apt -get install libnss-sss libpam-sss samba-common-bin packagekit” para su instalación.

5. Editamos el *hostname* para que lo pueda reconocer el servidor de dominio. Para ello introducimos el comando “sudo vim /etc/hostname” y escribimos el nuevo nombre de la máquina Linux. El nombre resultante seria lo que se llama el *Fully Qualified Domain Name* (FQDN).

6. Para comprobar si el cambio de nombre se ha realizado correctamente escribimos el comando “hostname -f”. Vemos que sigue siendo kali. Para que se realice correctamente el cambio escribimos “sudo hostnamectl” y ahí podemos observar el cambio del *hostname* anterior (kali) al actual (kali.bosquempresa.local).

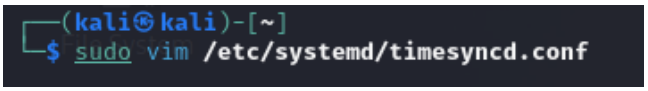


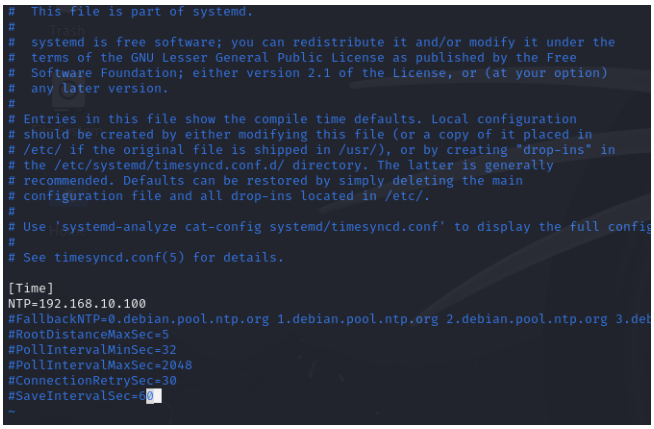
7. Cambiamos las DNS. Desde la configuración de red establecemos la dirección IP del servidor de controlador de dominio como servidor DNS principal y asignamos el método automático de DHCP.



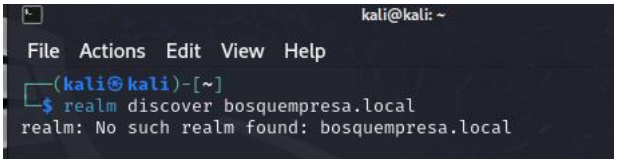
También introducimos la IP y el nombre del servidor escribiendo el siguiente comando:

8. Debemos establecer también, el servidor de hora. Para ello introducimos la IP del servidor que dará ese servicio mediante el siguiente comando:

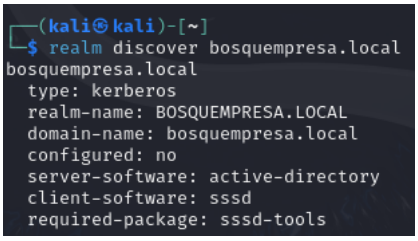




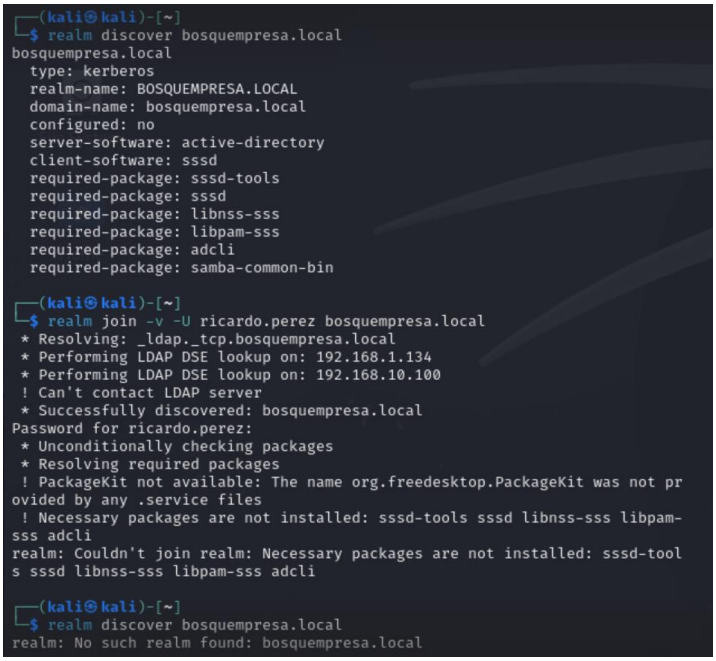
9. Aplicamos el comando “realm”, que es uno de los paquetes que hemos instalado al principio, para ver si existe ese dominio.



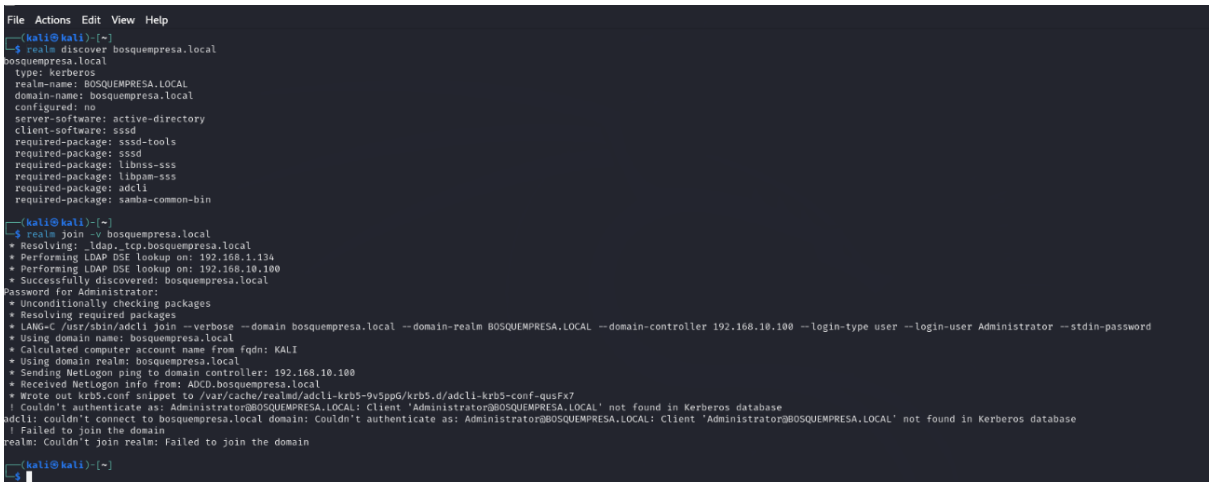
Da error, pero si ejecutamos el comando “sudo reboot” para reiniciar la máquina, vemos como los cambios se aplicaron correctamente tal y como podemos comprobar en la siguiente captura:



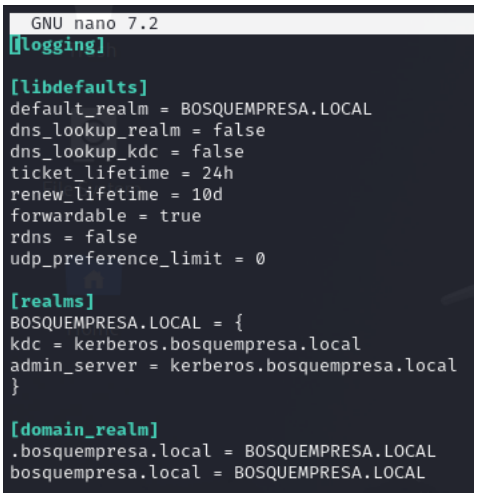
10. Al intentar unir la máquina virutal Kali Linux se produjeron diversos errores. Primero la intentamos unir para un usuario que habíamos creado en el Active Directory de Windows Server y los errores que se producían decían que faltaban algunos paquetes por instalar.



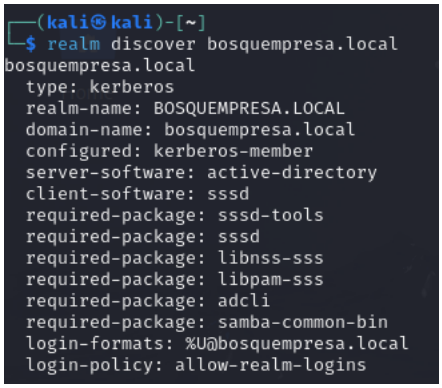
Pero como aún persistía este problema estando realmente instalados, decidimos hacer el *join* con el Administrador:



12. De esta manera dejaron de existir los errores de falta de paquetes, pero se ocasionaron otros errores (se pueden apreciar en la captura anterior), los cuales demoraron bastante en su resolución. Se tuvo que configurar el archivo Kerberos, el cual es un protocolo de autenticación de redes, mediante la ejecución del siguiente comando:



13. Anteriormente, al aplicar el comando “realm discover…” el dominio aparecía como no configurado. Pero después del paso anterior, podemos comprobar como en su configuración aparece “kerberos-member”. Esto se puede ver aplicando tanto el comando “realm discover bosquempresa.local” como el comando “realm list bosquempresa.local”.



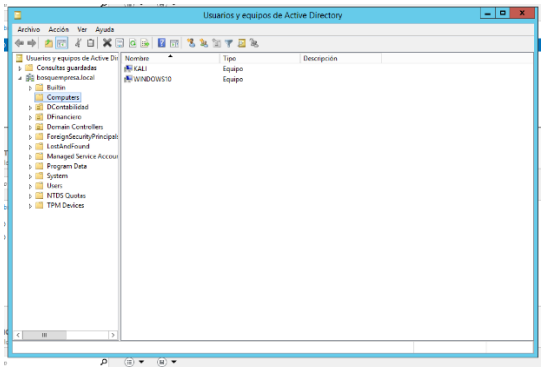
14. Volvemos a ejecutar el comando “realm join” de la siguiente manera:

“realm join -v -U Administrador bosquempresa.local” y nos da:

* Resolving: _ldap._tcp.bosquempresa.local
* Performing LDAP DSE lookup on: 192.168.1.134
* Performing LDAP DSE lookup on: 192.168.10.100
* Successfully discovered: bosquempresa.local
Password for Administrador:
* Unconditionally checking packages
* Resolving required packages
* LANG=C /usr/sbin/adcli join --verbose --domain bosquempresa.local --domain-realm BOSQUEMPRESA.LOCAL --domain-controller 192.168.10.100 --login-type user --login-user Administrador --stdin-password
* Using domain name: bosquempresa.local
* Calculated computer account name from fqdn: KALI
* Using domain realm: bosquempresa.local
* Sending NetLogon ping to domain controller: 192.168.10.100
* Received NetLogon info from: ADCD.bosquempresa.local
* Wrote out krb5.conf snippet to /var/cache/realmd/adcli-krb5-K8FpPX/krb5.d/adcli-krb5-conf-WnLu69
* Authenticated as user: Administrador@BOSQUEMPRESA.LOCAL
* Using GSS-SPNEGO for SASL bind
* Looked up short domain name: BOSQUEMPRESA
* Looked up domain SID: S-1-5-21-37191041-3392261095-2859797680
* Received NetLogon info from: ADCD.bosquempresa.local
* Using fully qualified name: kali.bosquempresa.local
* Using domain name: bosquempresa.local
* Using computer account name: KALI
* Using domain realm: bosquempresa.local
* Calculated computer account name from fqdn: KALI
* Generated 120 character computer password
* Using keytab: FILE:/etc/krb5.keytab
* A computer account for KALI$ does not exist
* Found well known computer container at: CN=Computers,DC=bosquempresa,DC=local
* Calculated computer account: CN=KALI,CN=Computers,DC=bosquempresa,DC=local
* Encryption type [3] not permitted.
* Encryption type [1] not permitted.
* Created computer account: CN=KALI,CN=Computers,DC=bosquempresa,DC=local
* Trying to set computer password with Kerberos
* Set computer password
* Retrieved kvno '2' for computer account in directory: CN=KALI,CN=Computers,DC=bosquempresa,DC=local
* Checking RestrictedKrbHost/kali.bosquempresa.local

```
*    Added RestrictedKrbHost/kali.bosquempresa.local
* Checking RestrictedKrbHost/KALI
*    Added RestrictedKrbHost/KALI
* Checking host/kali.bosquempresa.local
*    Added host/kali.bosquempresa.local
* Checking host/KALI
*    Added host/KALI
* Discovered which keytab salt to use
* Added the entries to the keytab: KALI$@BOSQUEMPRESA.LOCAL: FILE:/etc/krb5.keytab
* Added the entries to the keytab: host/KALI@BOSQUEMPRESA.LOCAL: FILE:/etc/krb5.keytab
* Added the entries to the keytab: host/kali.bosquempresa.local@BOSQUEMPRESA.LOCAL: FILE:/etc/krb5.keytab
* Added the entries to the keytab: RestrictedKrbHost/KALI@BOSQUEMPRESA.LOCAL: FILE:/etc/krb5.keytab
* Added the entries to the keytab: RestrictedKrbHost/kali.bosquempresa.local@BOSQUEMPRESA.LOCAL: FILE:/etc/krb5.keytab
* /usr/sbin/update-rc.d sssd enable
* /usr/sbin/service sssd restart
* Successfully enrolled machine in real
```

15. Comprobamos en el Active Directory de Windows Server como finalmente se ha unido exitosamente la máquina virtual Kali Linux a nuestro servidor de dominio.



CONCLUSIÓN

Para la integración de la máquina virtual Kali Linux se han visto algunos videos de Youtube, así como también leído algunas páginas web, preguntas a chat gpt y también a los compañeros para poder solventar algunos de los problemas que se ocasionaron. Pero aún así, ha sido realmente interesante para poder integrar de una mejor manera los conceptos vistos en clase y tener un registro de los errores o problemas que se puedan dar al realizar esta tipo de ejercicio.

Para poder acceder a las sesión del usuario que habíamos creado inicialmente, se le deberían dar los permisos necesarios a este usuario que se había creado en el directorio activo de Windows Server y después volver a realizar un “real join” con el nombre de ese usuario.