LABORATORIO DE ACTIVE DIRECTORY

Post Exploitation Attacks

Resumen

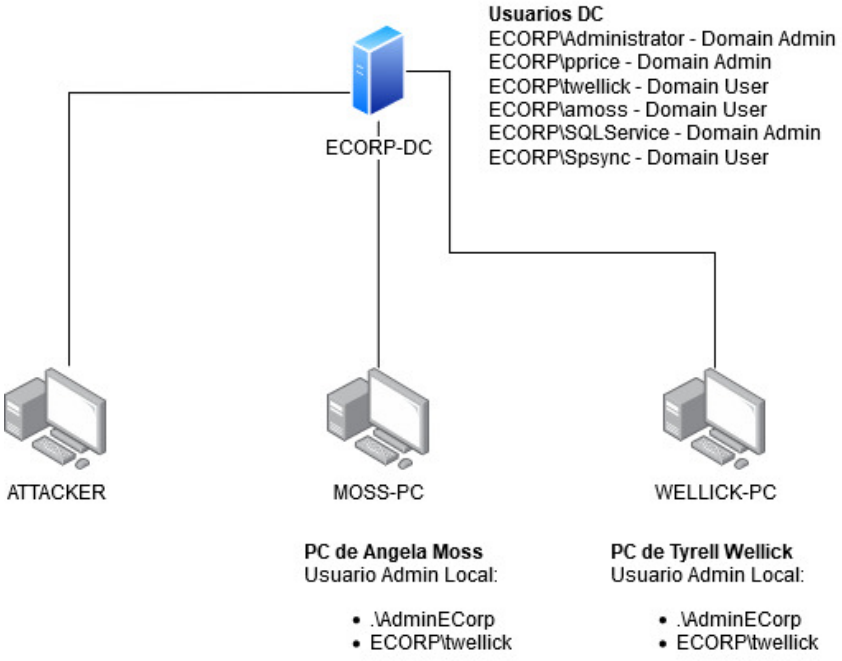
En este documento, se explicarán los procedimientos para poder montar un laboratorio de Active Directory, el cual será utilizado para realizar pruebas de penetración.

Francisco Canteli

@franc_205

ARMADO DE LABORATORIO DE ACTIVE DIRECTORY

Diagrama de Laboratorio



Requisitos

Laboratorios (Requisitos Mínimos)

- 1 VM con Windows Server 2019 (2GB de RAM)
- 1 VM con Windows 10 Enterprise (2GB de RAM)
- 1 VM con Kali Linux (2GB de RAM)

Requerimientos de Hardware (Requisitos Mínimos)

- Espacio de disco: 50Gb
- Memoria RAM: 8Gb

Laboratorios (Requisitos Recomendados)

- 1 VM con Windows Server 2019 (2GB de RAM)
- 2 VMs con Windows 10 Enterprise (4GB de RAM)
- 1 VM con Kali Linux (2GB de RAM)

Requerimientos de Hardware (Requisitos Recomendados)

- Espacio de disco: 80Gb
- Memoria RAM: 16Gb

Software de virtualización

Para poder montar nuestras máquinas virtuales, será necesario instalar algunos de los siguientes softwares de virtualización:

- VMWare Workstation: https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html
- Oracle VirtualBox: https://www.virtualbox.org/wiki/Downloads

En el workshop, estaremos utilizando Oracle VirtualBox. Al crear las VMs deberemos crear una red interna que tenga salida a internet, para esto se debe ejecutar el siguiente comando:

VBoxManage natnetwork add --netname ADLab --network "192.168.15.0/24" --enable --dhcp on

Y luego, se debe seleccionar como adaptador de red de cada una de las VMs "Red NAT", eligiendo la que tiene como nombre ADLab.

Configurar el servidor de Active Directory

1. Descargar la ISO de Windows Server 2019 desde https://www.microsoft.com/es-es/evalcenter/
2. Seleccionar la ISO Enterprise.
3. Crear la VM con nombre "*Windows Server – ECORP*" y luego configurar el adaptador de red como Red NAT seleccionando la red previamente creada.
4. A la hora de instalar la máquina virtual, seleccionar la opción "*Windows Server 2019 (Desktop Experience)*".
5. Una vez terminada la instalación, se pedirá que se establezca una contraseña para el usuario Administrator, la misma debe ser "*MyS3cretPass!*"
6. En caso de utilizar VirtualBox, se recomienda instalar las Guest Additions.
7. Renombrar el server a ECORP-DC. Para esto ir a Server Manager -> Local Server -> Computer Name -> Change -> Escribir "*ECORP-DC*" en el campo "*Computer name*"
8. Instalar Active Directory Domain Services y luego de instalarlo promover server a Domain Controller.
    - Configurar como nombre de Dominio: ECORP.local
    - Configurar como nombre de Netbios: ECORP
    - Configurar clave de DSRM (Directory Services Restore Mode) como "*Password1*"
9. Al instalar y configurar todo el AD DS, se reiniciará la máquina
10. Deshabilitar Windows Defender.

Configurar máquinas de usuario

1. Descargar la ISO de Windows 10 desde https://www.microsoft.com/es-es/evalcenter/
2. Seleccionar la ISO Enterprise.
3. Crear la VM con nombre "*Windows 10 - Tyrell Wellick*" y luego configurar el adaptador de red como Red NAT seleccionando la red previamente creada.
4. Una vez terminada la instalación, se pedirá que se cree un usuario, el mismo será:
    - *Usuario: AdminECorp*
    - *Clave: t5w9ea7gmgsdqs5v*

5. En caso de utilizar VirtualBox, se recomienda instalar las Guest Additions.
6. Renombrar el server a Wellick-PC. Para esto ir a Settings -> System -> About -> Rename This PC.
7. Deshabilitar Windows Defender.
8. En caso de querer armar el laboratorio recomendado, clonar la VM creada y luego renombrarla a "*Moss-PC*".

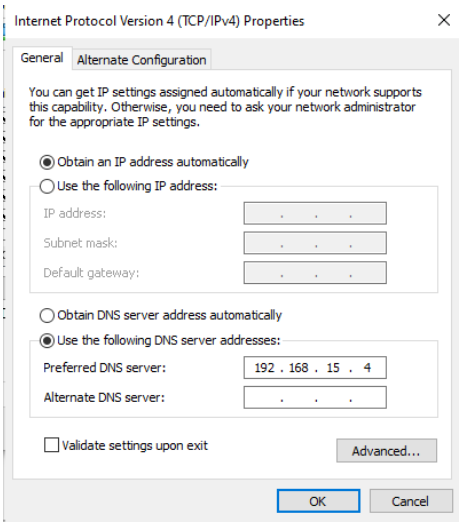
Configurar de Usuarios y Shares

1. En el servidor ECORP-DC, ir al Server Manager -> Tools -> AD users and groups.
2. Crear una OU llamada "*Users Ecorp*".
3. Crear los usuarios de dominio con sus respectivos permisos.
4. Crear una carpeta llamada "Scripts" y compartir esa carpeta. Para esto, crear la carpeta y hacer click derecho sobre ella -> Properties -> Sharing Tab -> Share -> Escribir "*everyone*" y darle Share.
5. Crear un archivo .ps1 en la carpeta Scripts que contenga el siguiente texto:

$Password=ConvertTo-SecureString "tyr3ll.2020!" -asplaintext -force //Contiene passwords locales

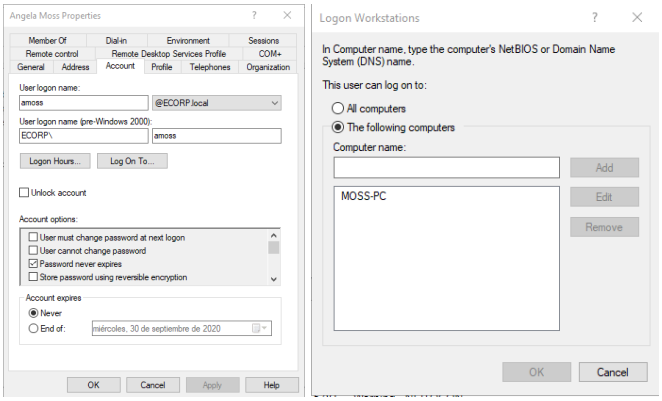
Unir máquinas a dominio y últimos ajustes

1. Configurar los DNS
   - Ir al Server ECORP-DC y obtener su IP, es importante asegurarnos de que esta IP no sea asignada por el DHCP y este asignada estáticamente.
   - En las máquinas con Windows 10, ir a Control Panel -> Network and Internet -> Network and Sharing Center -> Change Adapter Settings -> Seleccionar el adaptador de red haciendo click derecho -> Properties -> IPv4 -> Seleccionar "Use the following DNS Server Addresses" y en Preferred DNS Server escribir la IP del servidor ECORP-DC.



2. Unir a dominio
   - Luego de configurar los DNS en ambas PC, lo siguiente será unirlas a nuestro dominio ECORP.local.
   - Para esto deberemos ir a Control Panel -> System and Security -> System -> Advanced System Settings -> Computer Name Tab -> Change -> Seleccionar "Domain", escribir ECORP.local y darle aceptar.
   - Aparecerá una ventana pidiendo credenciales para poder unirnos al dominio, allí colocaremos las siguientes credenciales:

        - Usuario: Administrator
        - Clave: MyS3cretPass!
    - Luego de esto, deberemos reiniciar la máquina.
3. Agregar el permiso de Local Admin al usuario Tyrell Wellick en las máquinas de Windows 10.
    - Abrir el CMD y escribir "*control userpasswords2*", al darle enter se abrirá una nueva ventana.
    - Hacer click en Add y completar con los siguientes datos y darle Next:
        - User Name: twellick
        - Domain: ECORP
    - Luego seleccionar el permiso Administrator y darle Next.
    - Por último, darle Finish y ya el usuario ECORP\twellick será administrador local de la máquina.
4. Restringir acceso de Angela Moss solo a su PC
    - En el Server ECORP-DC, ir a Server Manager -> Tools -> Active Directory Users and Groups -> Click derecho sobre el usuario de Angela Moss -> Properties -> Account Tab -> Logon To -> Seleccionar "The following computers" y agregar "Moss-PC".



5. Configurar la cuenta de SQLService como Service Principal Name (SPN).
    - Ir al Server ECORP-DC, abrir Powershell y ejecutar el siguiente comando: *setspn -a ECORP-DC/SQLService.ECORP.local:58001 ECORP\SQLService*
6. Habilitar la detección de redes.

Usuarios

Domain Users – ECORP-DC

- Domain Admin
    - Usuario: Administrator
    - Clave: MyS3cretPass!
- Phillip Price - Permiso de **Domain Admin**
    - Usuario: pprice
    - Clave: Password2020!
- Tyrell Wellick - Permiso de **Domain User**
    - Usuario: twellick
    - Clave: tyr3ll.2020!
- Angela Moss - Permiso de **Domain User**
    - Usuario: amoss
    - Clave: P4ssw0rd1
- Cuenta de Servicio SQL - Permiso de **Domain Admin**, poner como comentario la clave
    - Usuario: SQLService

    - Usuario: #Mypassw0rd1
- Cuenta de Servicio Sharepoint UPS – **Domain User** con Permiso de Replicación
    - Usuario: Spsync
    - Clave: Mysecretpass1

Wellick-PC

- AdminECorp - Permisos de Admin local
    - User: AdminECorp
    - Clave: t5w9ea7gmgsdqs5v
- ECORP\twellick - Permisos de Admin Local

MOSS-PC

- AdminEcorp - Permisos de Admin Local
    - User: AdminECorp
    - Clave: t5w9ea7gmgsdqs5v
- ECORP\twellick - Permisos de Admin Local
- ECORP\amoss - Permisos de Domain User

Referencias

- Instalar Guest Additions: https://www.howtogeek.com/howto/2845/install-guest-additions-to-windows-and-linux-vms-in-virtualbox/
- Instalar y realizar configuración básica Active Directory: https://www.jmsolanes.net/es/instalacion-active-directory/
- Instalar y realizar configuración básica Active Directory: https://clouding.io/hc/es/articles/360010510460-C%C3%B3mo-configurar-Active-Directory-Domain-Controler
- Detección de redes: https://www.thewindowsclub.com/enable-disable-network-discovery-windows
- Azure DevTestLabs: https://azure.microsoft.com/es-es/pricing/details/lab-services/
- TCM Active Directory Lab: https://www.youtube.com/watch?v=xftEuVQ7kY0
- Instructivo de laboratorio similar Azure: https://medium.com/@kamran.bilgrami/ethical-hacking-lessons-building-free-active-directory-lab-in-azure-6c67a7eddd7f