

PROYECTO DE TECNOLOGÍAS DE SEGURIDAD

TEMA: Ataque de Man-in-the-Middle

Integrantes: Becerra Ricardo, Suntasig Ariel, Sánchez Sebastián, Terán José y Guingla Joel.

Carrera: Ingeniería de Software

Grupo: GR1SW

Fecha: 05-01-2024

Índice de Contenidos

1.	OBJETIVOS	3
2.	INFORME	3
2.1	Topología.....	3
2.2	ClearOs	3
2.3	Windows para configuración de Clear Os	5
2.4	Kali	22
3.	CONCLUSIONES Y RECOMENDACIONES	34
4.	BIBLIOGRAFÍA	34

Índice de Figuras

Figura 1.	Topología de la simulación MitM.....	3
Figura 2	Configuración adaptador 1 puente en ClearOS.....	4
Figura 3	Configuración adaptador 2 red interna.....	4
Figura 4	Configuración adaptador 3 sólo anfitrión.	4
Figura 5	Configuración modo de red.	4
Figura 6	Creación interfaz con direccionamiento estático.	5
Figura 7	Configuración de interfaz con direccionamiento dinámico.....	5
Figura 8	Configuración de la red Windows	5
Figura 9	Configuración IP Windows	6
Figura 10	Ping de Windows al ClearOS	6
Figura 11	Conexión con ClearOS desde Windows.	7
Figura 12	Configuración de modo de puerta de enlace.....	8
Figura 13	Configuración DNS de la red.	8
Figura 14	Selección de edición del ClearOS.	9
Figura 15	Sistema de registro.	10
Figura 16	Actualizaciones de software.	11
Figura 17	Elección del dominio de internet.	12
Figura 18	Configuración del nombre de host.....	12
Figura 19	Configuración zona horaria.	13
Figura 20	Selección grupo de aplicaciones a instalar.	13

Figura 21 Salir del Marketplace.	14
Figura 22 Configuración de widgets.	14
Figura 23 Instalación de widgets.	15
Figura 24 Entorno luego del reinicio.	15
Figura 25 Configuración de los widgets del Dashboard.	16
Figura 26 Configuración de IP.	17
Figura 27 Configuración servidor DHCP.	17
Figura 28 Comprobación estado de las subredes.	18
Figura 29 Direccionamiento DHCP que utilizaremos para seguir en la máquina Windows.	18
Figura 30 Configuración de la IP Windows con DHCP	19
Figura 31 Consulta de la dirección IP	19
Figura 32 Ping desde Windows a Linux.....	20
Figura 33 Firewall Windows	20
Figura 34 ipconfig /release en Windows	20
Figura 35 Cambio del Gateway en Windows	21
Figura 36 Inicio de sesión en WinSCP	21
Figura 37 Creación de una carpeta en WinSCP.....	21
Figura 38 Adaptador de red "Red interna" en máquina Linux	22
Figura 39 Asignación dirección IP a kali linux.	23
Figura 40 Conexión entre kali y windows.	23
Figura 41 Conexión desde windows a kali.	23
Figura 42. Actualización de repositorio de paquetes de descargar en kali.	24
Figura 43. Instalación de servidor FTP en kali.....	24
Figura 44. Versión del servidor FTP instalado en kali.....	24
Figura 45 Modificación de archivos.	25
Figura 46 Consulta dirección IP en Kali.	25
Figura 47 Comprobación status servidor FTP en kali.	26
Figura 48 Comando de ejecución de Ettercap en modo gráfico.	26
Figura 49 Ejecución Ettercap.	26
Figura 50 Selección de DHCP spoofing dentro de Ettercap.....	27
Figura 51 Pantalla de configuración DHCP spoofing	27
Figura 52 Configuración de IP y mascarará DHCP spoofing	28
Figura 53 Ejecución de DHCP spoofing.....	28
Figura 54 IP y gateway Windows antes del ataque.....	29
Figura 55 IP y Gateway Windows después del ataque.....	29
Figura 56 Registro de petición y asignación de IP en Ettercap	30
Figura 57 Ingreso a servidor FTP en Windows.....	31
Figura 58 Conexión a servidor FTP en windows	31
Figura 59 Creación carpeta desde Windows hacia Kali.....	31
Figura 60 Comprobaciónn creación de carpeta en Kali	32
Figura 61 Captura de tráfico de red en Wireshark en Kali	32
Figura 62 Pasos para ver contenido completo del tráfico específico	33
Figura 63 Información detallada del tráfico.....	33
Figura 64 Usuario y contraseña capturadas en Kali	33

1. OBJETIVOS

- Configurar una máquina virtual con ClearOS para actuar como servidor DHCP y puerta de enlace de la red interna.
- Configurar una máquina virtual con Windows para actuar como cliente de la red interna y conectarse al servidor ClearOS.
- Configurar una máquina virtual con Kali Linux para actuar como atacante y realizar un ataque de hombre en el medio (MitM) mediante el envenenamiento de las respuestas DHCP.
- Instalar y configurar un servidor FTP en Kali Linux para capturar la información que se envía desde el cliente Windows.
- Utilizar la herramienta Ettercap para realizar el ataque de MitM y observar el tráfico de red entre el cliente y el servidor.
- Utilizar la herramienta Wireshark para analizar los paquetes capturados y extraer información sensible como el usuario y la contraseña del servidor FTP.

2. INFORME

En el desarrollo del informe se abarcará las configuraciones necesarias para poder realizar una simulación del **Ataque de hombre en el medio**.

2.1 Topología

La topología que se utilizará será la siguiente:

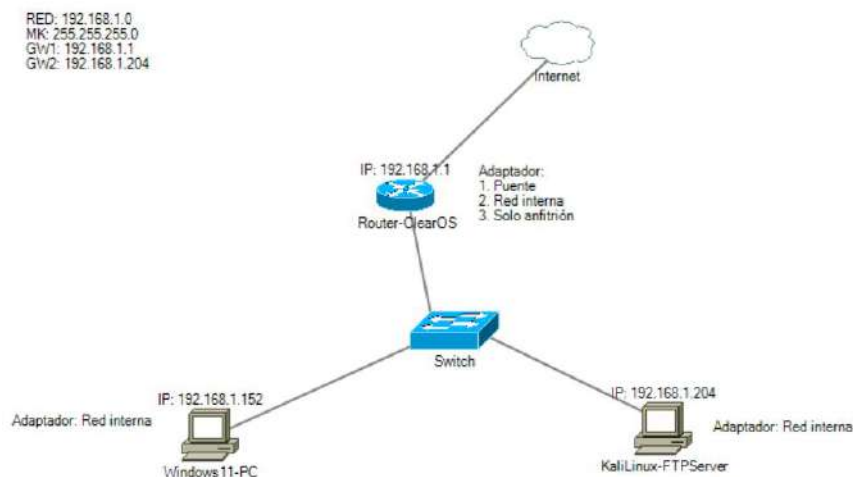


Figura 1. Topología de la simulación MitM

2.2 ClearOs

Como primer paso nos aseguramos de que nuestra máquina virtual con ClearOS tenga los 3 adaptadores de red correctamente configurados, tal y como se ve en las siguientes figuras.



Figura 2 Configuración adaptador 1 puente en ClearOS.

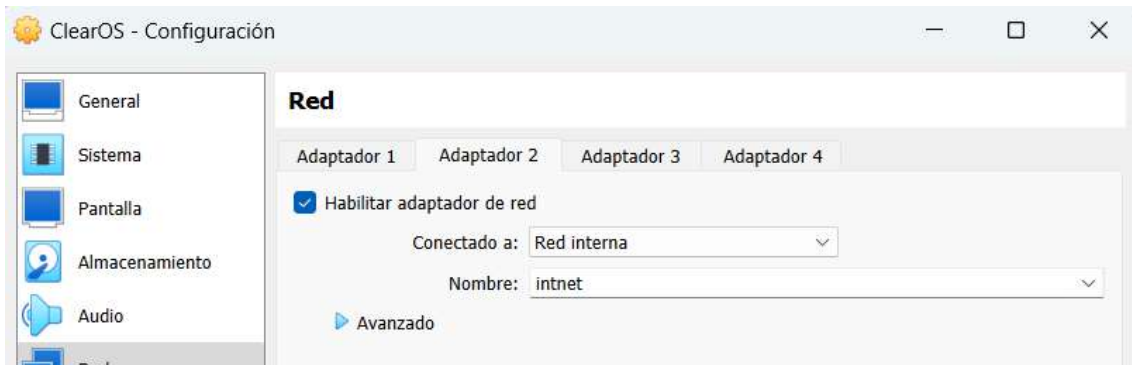


Figura 3 Configuración adaptador 2 red interna.



Figura 4 Configuración adaptador 3 sólo anfitrión.

Una vez dentro de la máquina con ClearOS nos dirigiremos a la configuración de red, donde verificaremos que el modo de red se encuentre en modo Gateway.

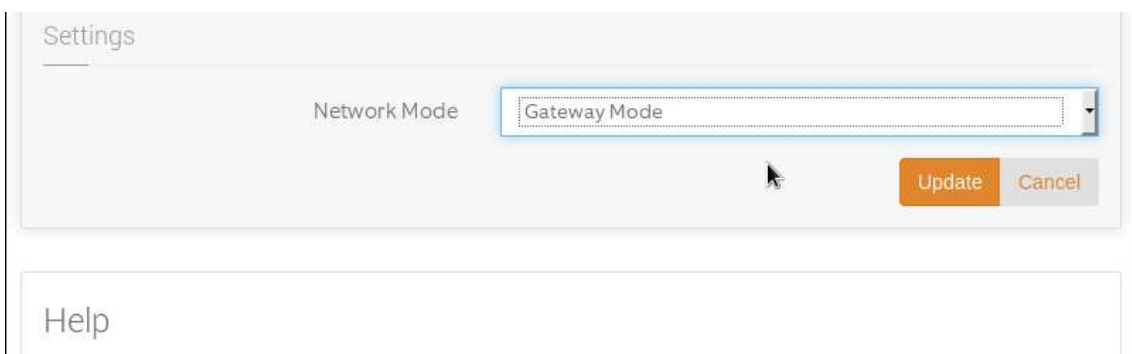
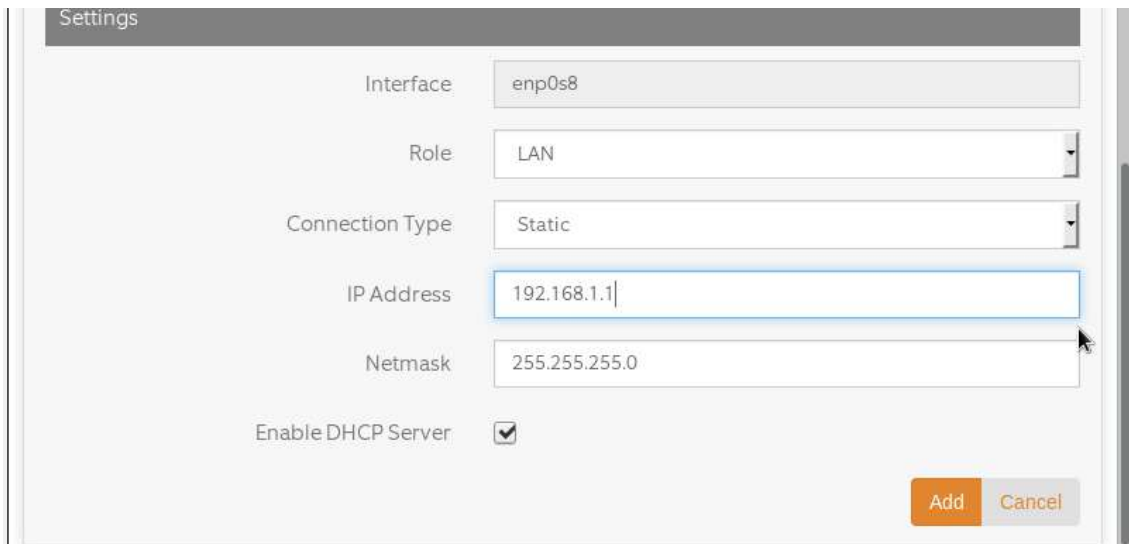


Figura 5 Configuración modo de red.

En la sección inferior añadiremos dos interfaces virtuales con el botón “Add Virtual” en los adaptadores que abrimos anteriormente, el primero funcionará de manera estática para el Gateway y tenemos que asegurarnos de marcar la casilla “Enable DHCP Server”, y el segundo será dinámico.

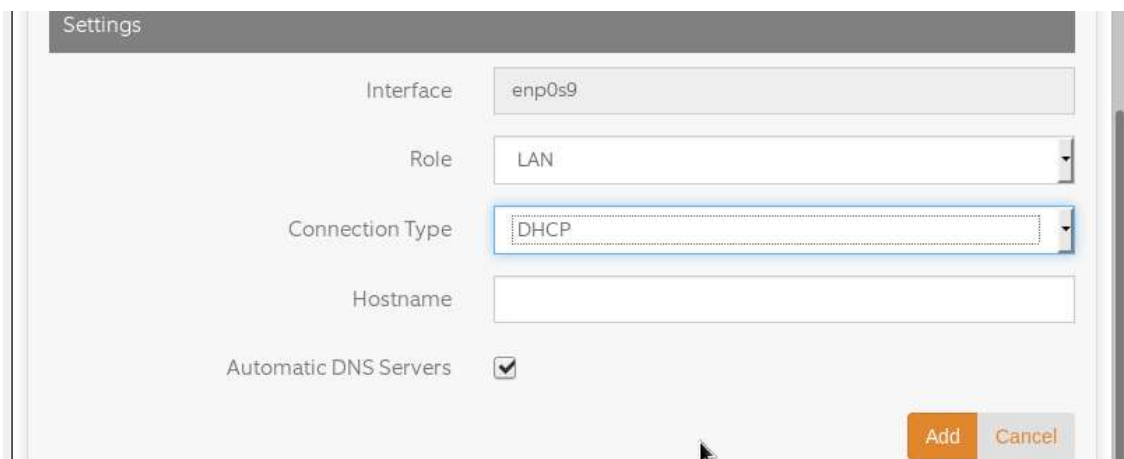


The screenshot shows a 'Settings' window for a virtual interface. The fields are as follows:

Field	Value
Interface	enp0s8
Role	LAN
Connection Type	Static
IP Address	192.168.1.1
Netmask	255.255.255.0
Enable DHCP Server	<input checked="" type="checkbox"/>

At the bottom right, there are two buttons: 'Add' (orange) and 'Cancel' (grey).

Figura 6 Creación interfaz con direccionamiento estático.



The screenshot shows a 'Settings' window for a virtual interface. The fields are as follows:

Field	Value
Interface	enp0s9
Role	LAN
Connection Type	DHCP
Hostname	
Automatic DNS Servers	<input checked="" type="checkbox"/>

At the bottom right, there are two buttons: 'Add' (orange) and 'Cancel' (grey).

Figura 7 Configuración de interfaz con direccionamiento dinámico.

2.3 Windows para configuración de Clear Os

Para la configuración de la máquina Windows es necesario que el adaptador esté configurado en una red interna como se muestra a continuación en la figura

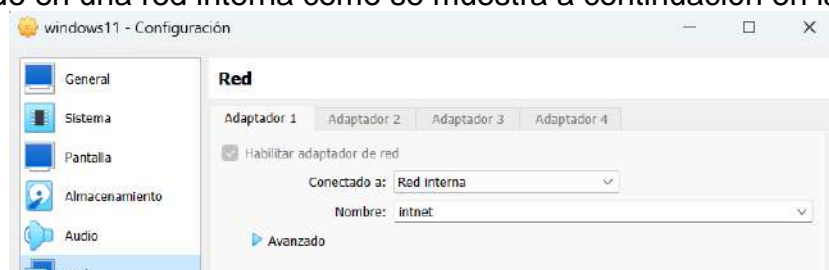


Figura 8 Configuración de la red Windows

Ahora dentro de Windows se busca Red e Internet y se configura las IPs de acuerdo a la topología.

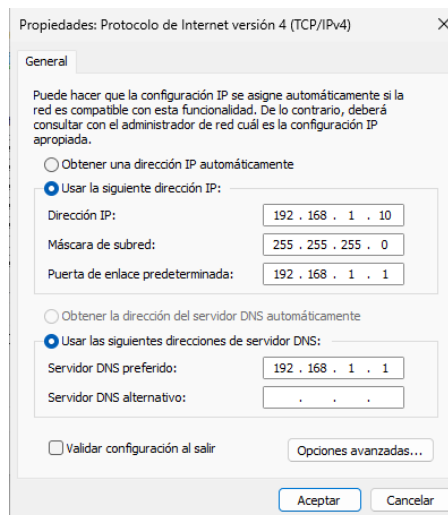


Figura 9 Configuración IP Windows

Para comprobar la conexión con la máquina del ClearOS se realiza una verificación de conectividad.

```
C:\Users\vboxuser>ping 192.168.1.1

Haciendo ping a 192.168.1.1 con 32 bytes de datos:
Respuesta desde 192.168.1.1: bytes=32 tiempo=4ms TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo=2ms TTL=64

Estadísticas de ping para 192.168.1.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 4ms, Media = 1ms
```

Figura 10 Ping de Windows al ClearOS

Entonces nos colocamos en el navegador dentro de windows e ingresamos el direccionamiento de la puerta hacia ClearOS en el puerto 81, así quedaría lo que tenemos que ingresar: <https://192.168.1.1:81>.

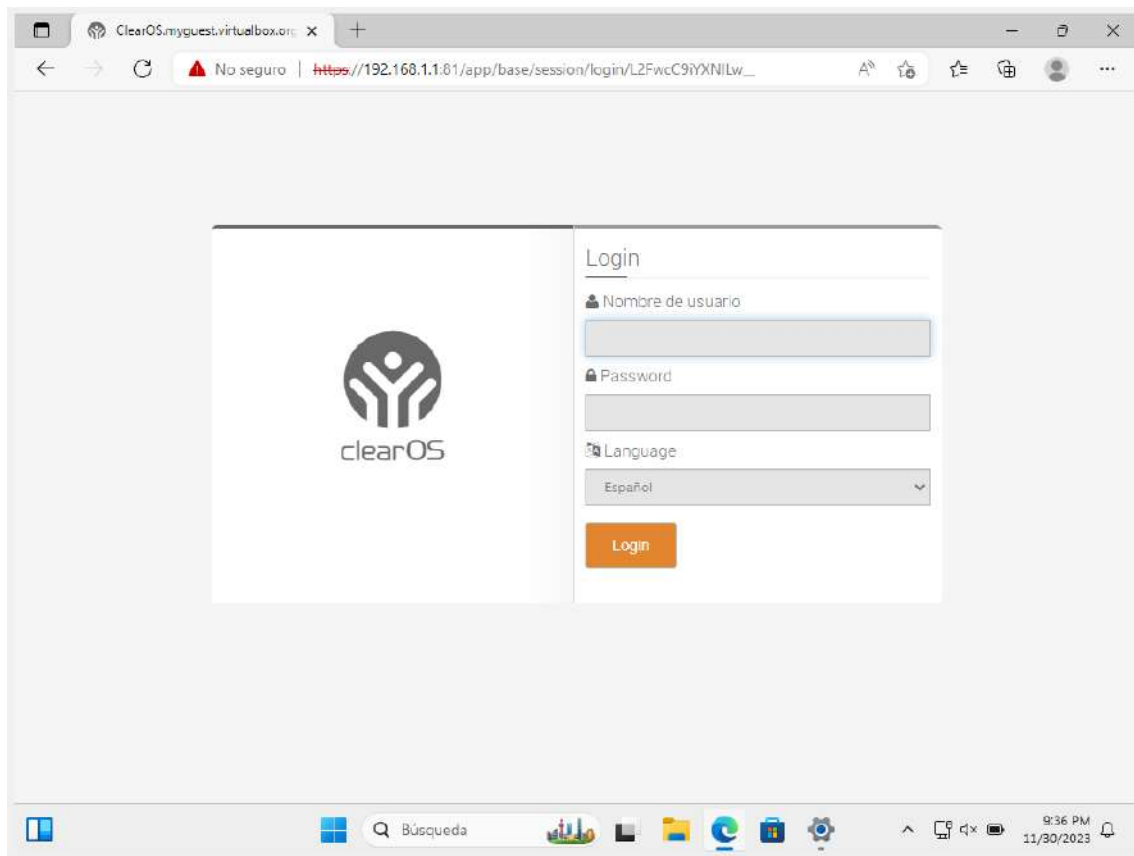


Figura 11 Conexión con ClearOS desde Windows.

Una vez dentro con las credenciales predefinidas, procedemos a deslizarnos hasta la sección de configuración y elegiremos nuevamente el modo de puerta de enlace.

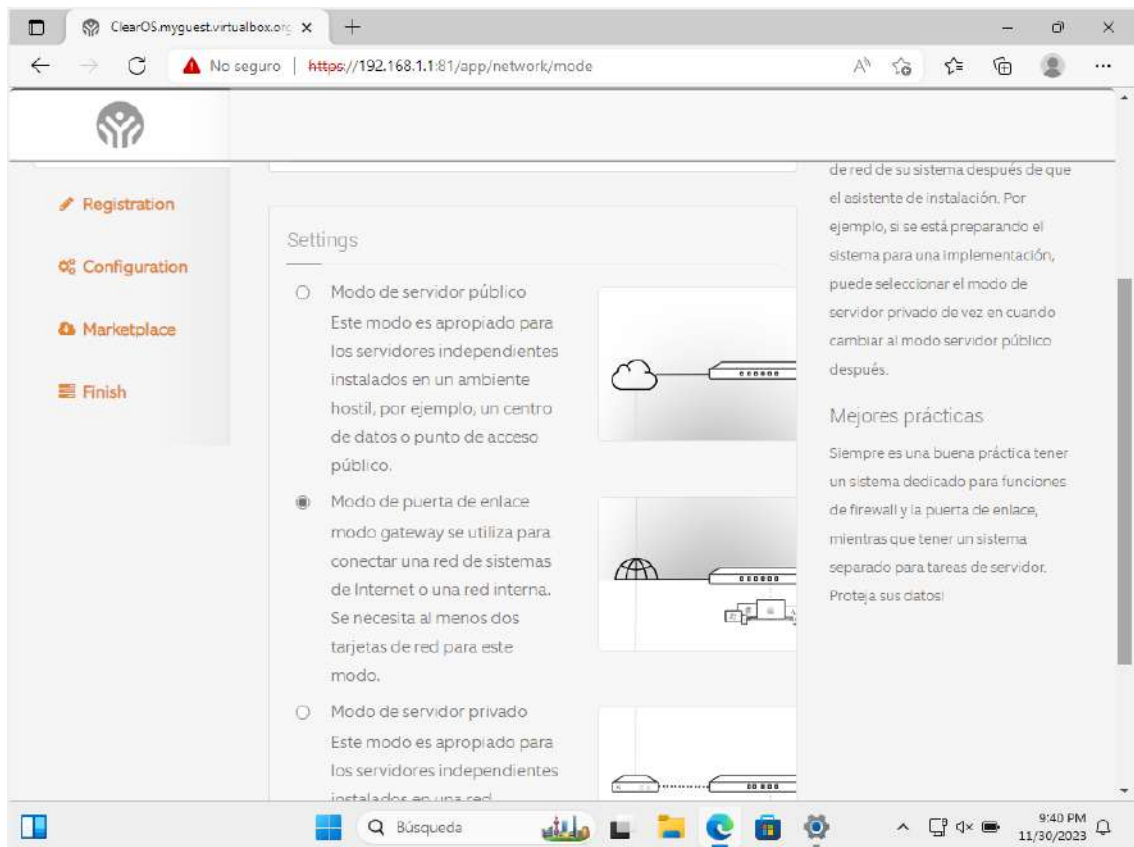


Figura 12 Configuración de modo de puerta de enlace.

En la sección de network DNS verificamos que se realice correctamente el Lookup, como se ve a continuación.

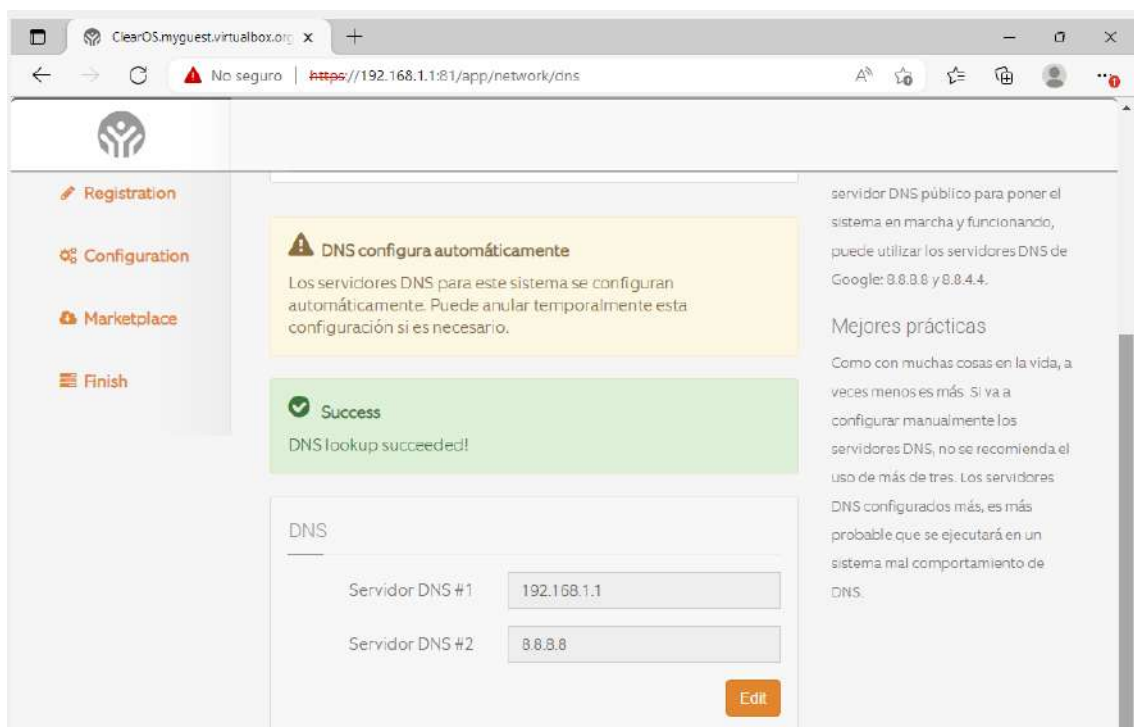


Figura 13 Configuración DNS de la red.

Ya podemos continuar con la parte de registro, en donde elegiremos la versión Community.

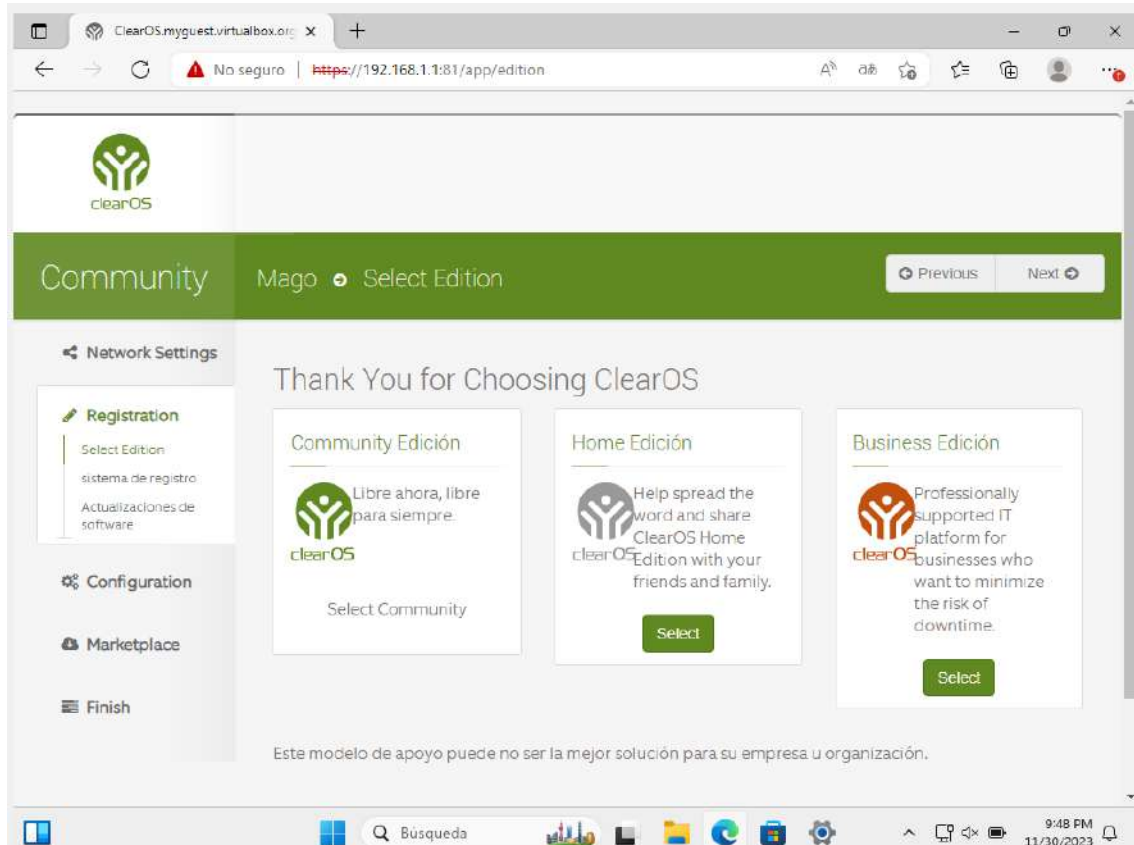


Figura 14 Selección de edición del ClearOS.

Llenaremos los campos solicitados a continuación de acuerdo con nuestros criterios. En el campo Tipo seleccionaremos la opción “instalar nueva”.

The screenshot shows a web browser window with the URL <https://192.168.1.1:81/app/registration/register/ArielSuntasig>. The page has a sidebar with navigation links: Registration, Configuration, Marketplace, and Finish. The main content area is titled "sistema de registro" and contains a form with the following fields:

- Account (ClearCenter): ArielSuntasig
- Password: [masked]
- Tipo: Instalar nueva
- Nombre del sistema: Clearos
- Ambiente: Educación
- Términos de servicio: Al hacer clic en Sistema de Registro, usted está de acuerdo con el Términos de servicio.

At the bottom of the form are two buttons: "Register System" and "Formulario de actualización". A blue banner at the top of the main content area says "Cuenta creada con éxito." On the right side, there is a section titled "registrarse" with text explaining the registration process and a "Creando una cuenta" section.

Figura 15 Sistema de registro.

Si todo fue llenado correctamente nos dará una ventana de resumen indicando que el producto ya está registrado, ahora debemos actualizar todo lo que nos marca en la siguiente sección.

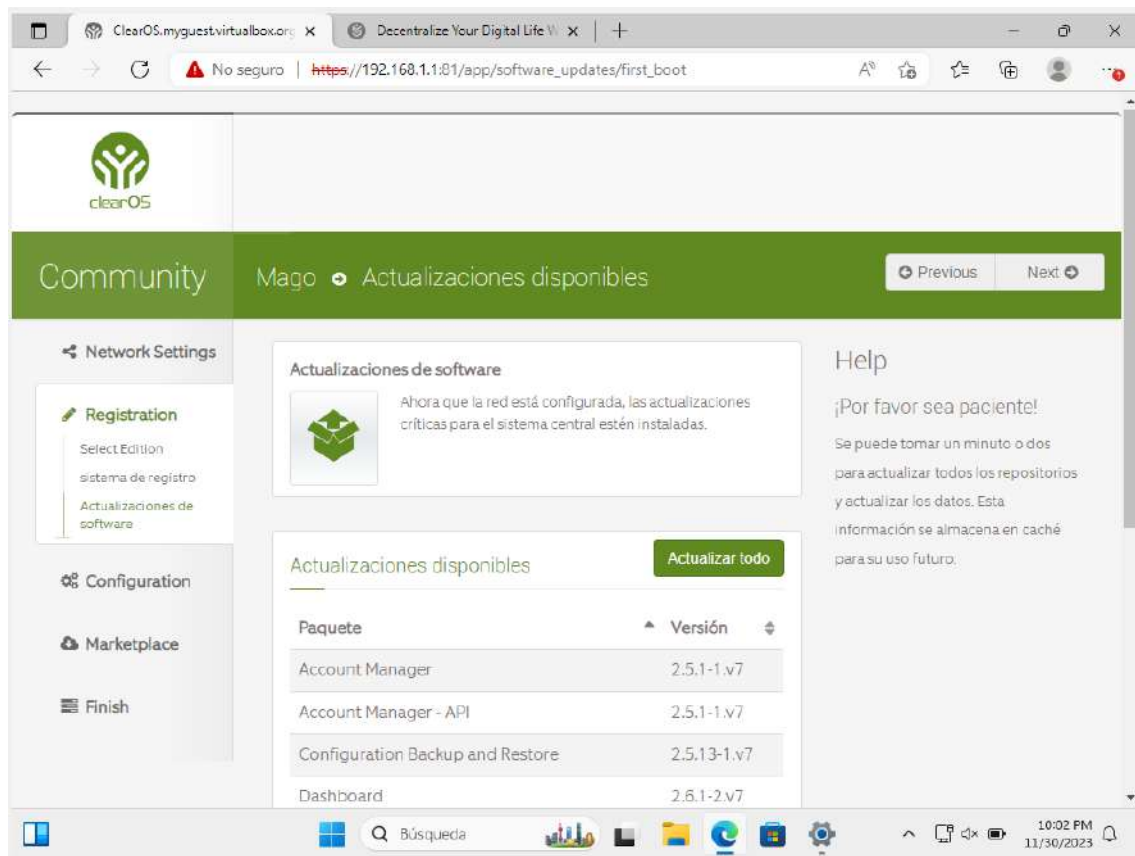


Figura 16 Actualizaciones de software.

Seguimos con la configuración del firewall, eligiendo el nombre del dominio, host y fecha.

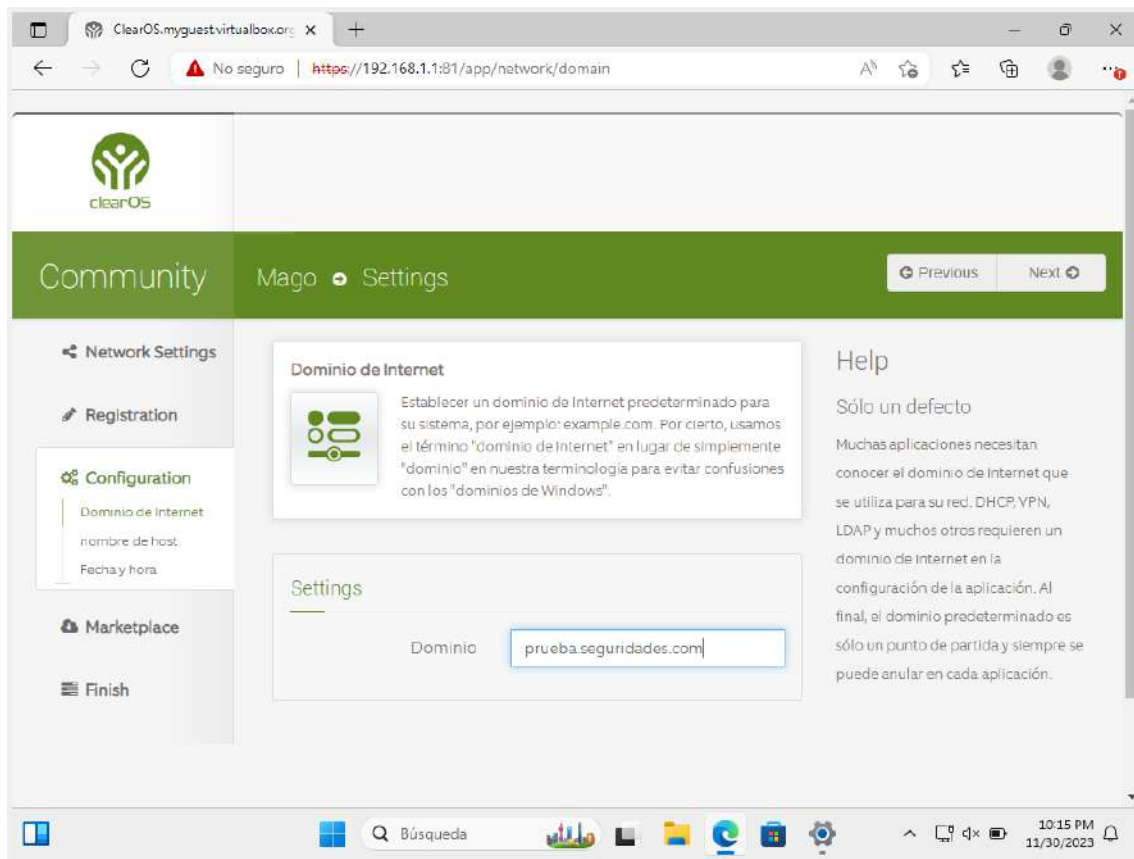


Figura 17 Elección del dominio de internet.

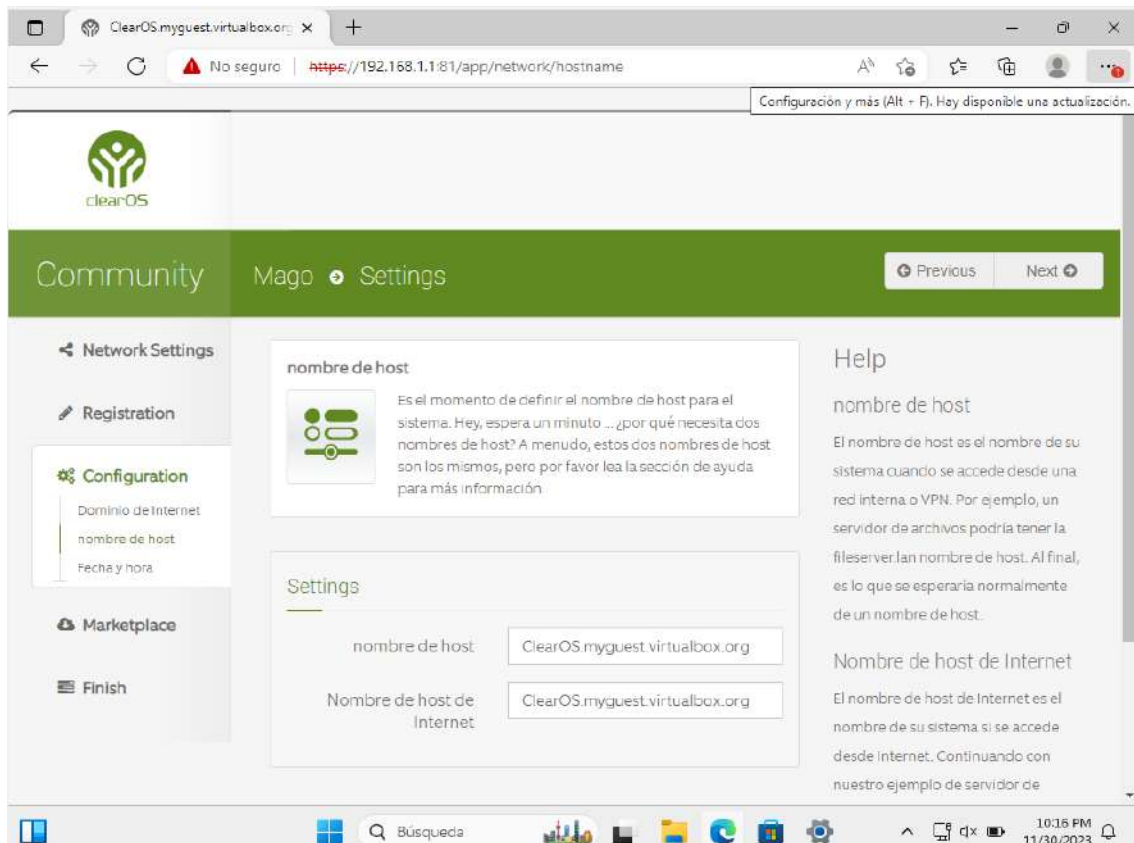


Figura 18 Configuración del nombre de host.

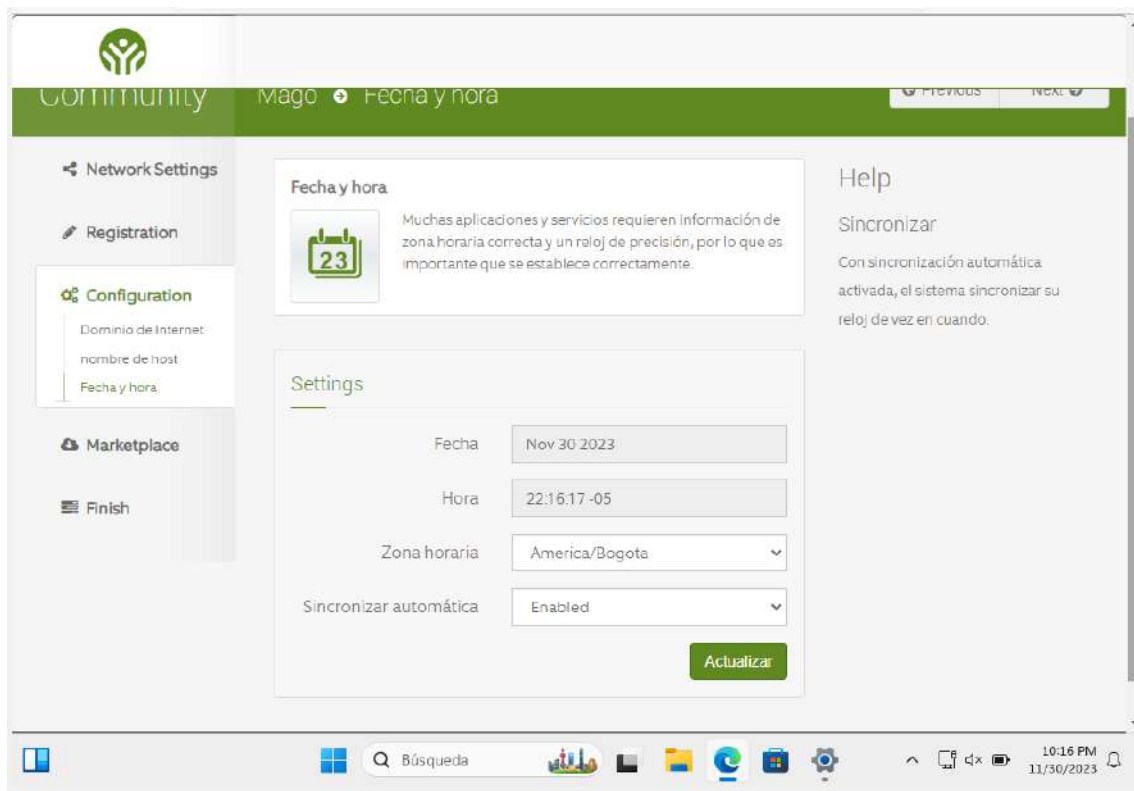


Figura 19 Configuración zona horaria.

Seguimos a la pestaña de Marketplace, donde elegiremos la opción “Por categoría”.

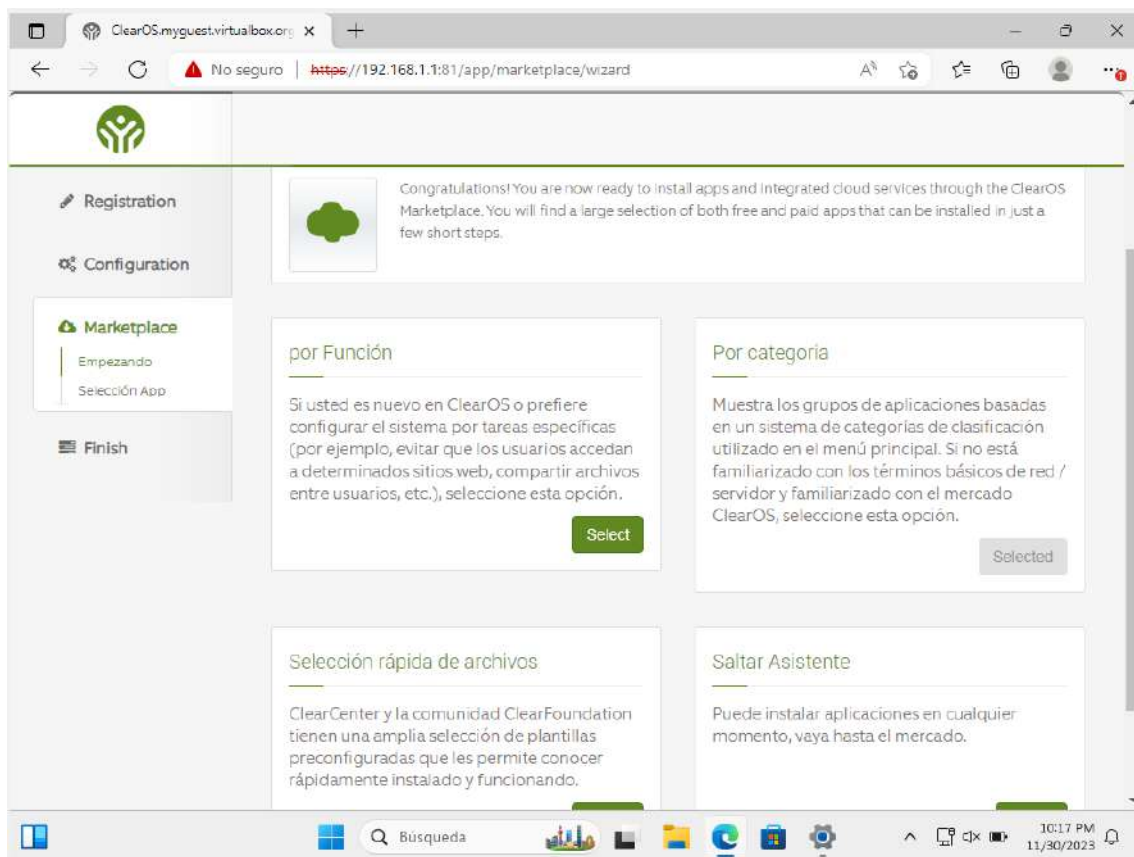


Figura 20 Selección grupo de aplicaciones a instalar.

Ahora saldremos sin instalar nada con el botón “Instalar Aplicaciones tarde”, nos pedirá confirmar.

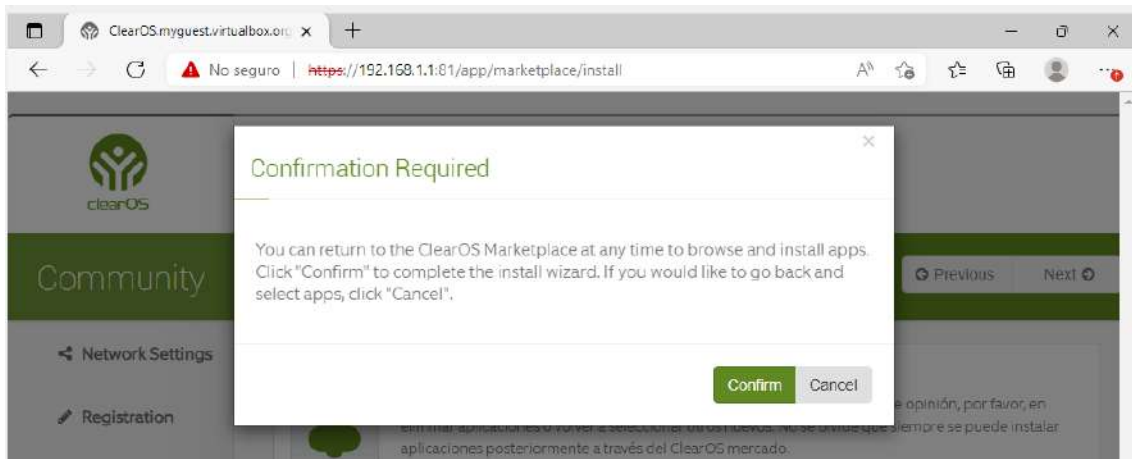


Figura 21 Salir del Marketplace.

Ahora una vez nos encontremos en el dashboard, nos dirigimos a la sección de widgets y vemos que está vacío, por lo que iremos nuevamente al Marketplace.

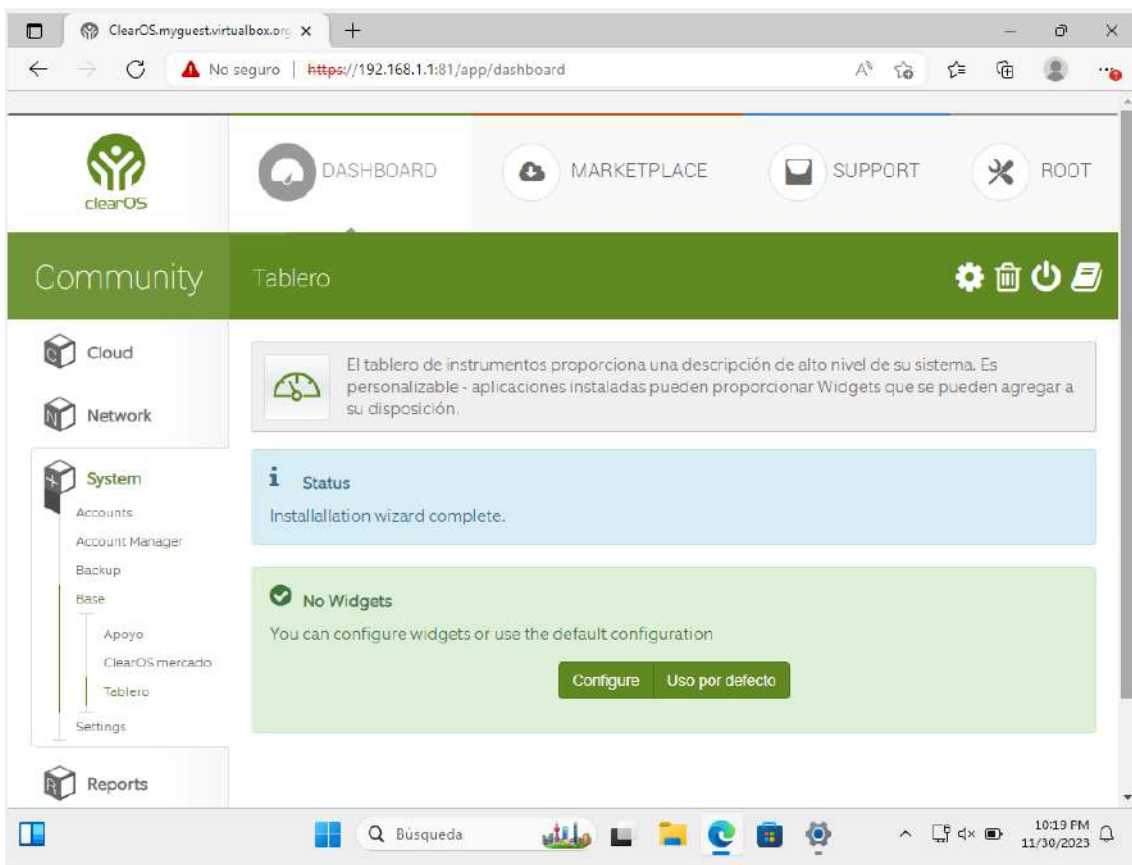


Figura 22 Configuración de widgets.

Una vez dentro del Marketplace elegiremos dos, “Custom Firewall” y “Port Forwarding”, seguimos con el proceso dando click en “Descargar e Instalar”.

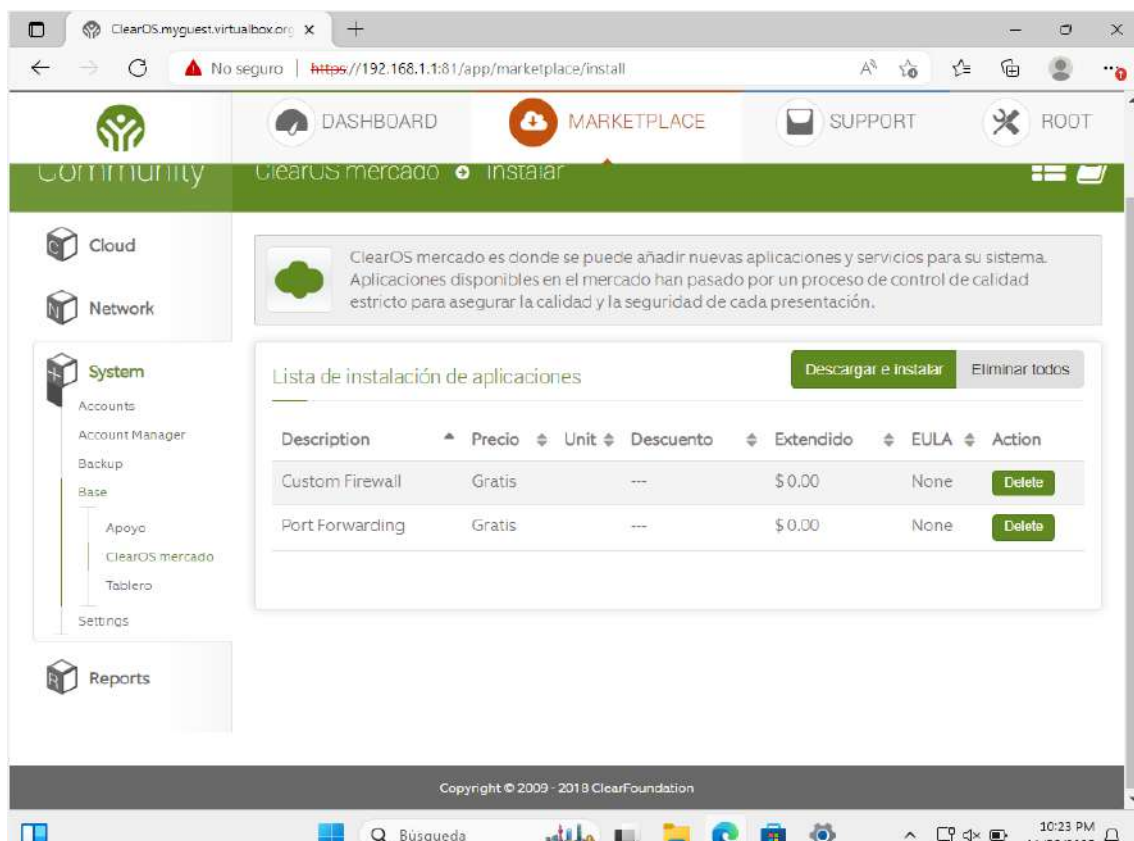


Figura 23 Instalación de widgets.

Una vez terminada la instalación de las aplicaciones procedemos a reiniciar el sistema, esto dirigiéndonos a la sección de Settings - General Settings, scrolleamos hasta el fondo y le damos en Restart, confirmando las siguientes ventanas emergentes. Cuando haya acabado de reiniciarse presionaremos el botón para retornar a la interfaz.

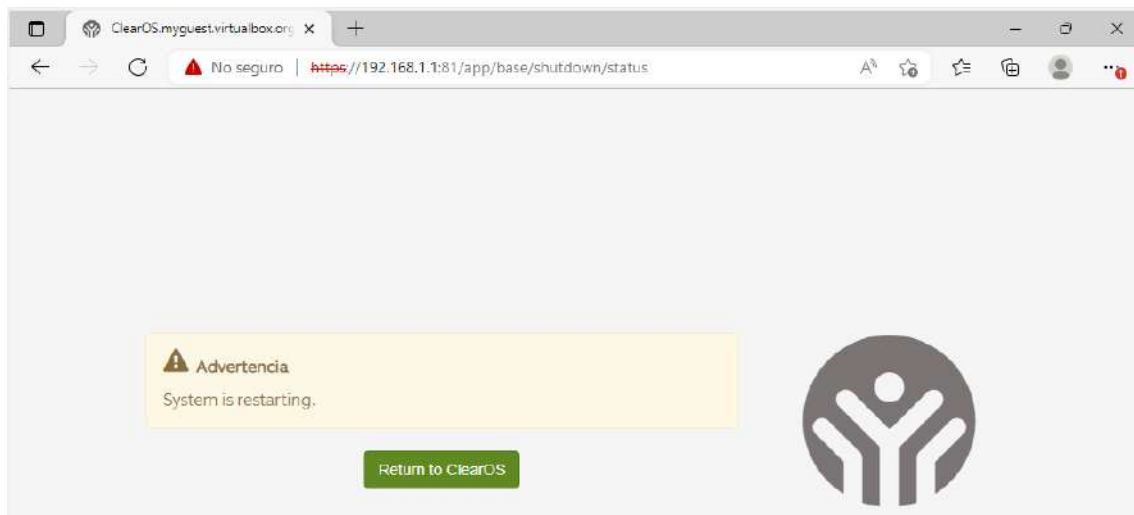


Figura 24 Entorno luego del reinicio.

Ya que estamos adentro nuevamente, podemos movernos otra vez al dashboard y configurar los widgets, seleccionaremos los dos últimos instalados.

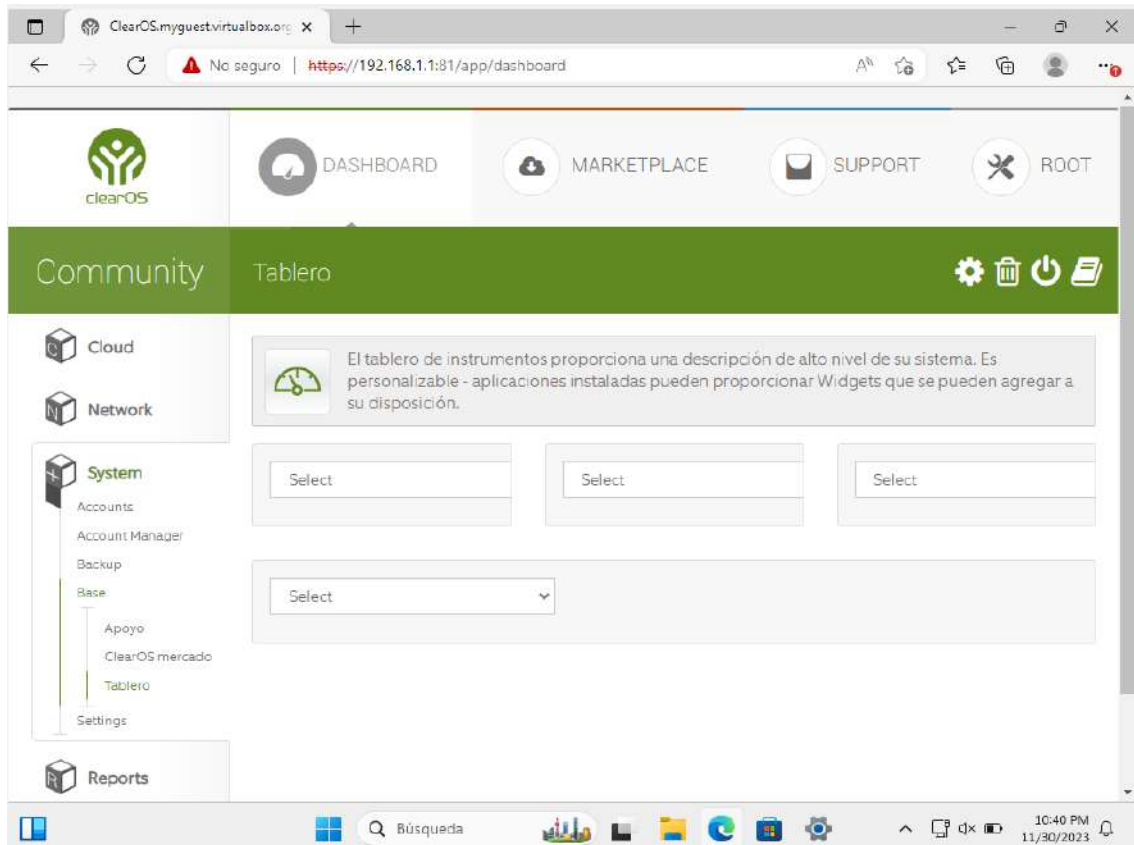


Figura 25 Configuración de los widgets del Dashboard.

Si ahora nos dirigimos nuevamente a network, podremos configurar el dominio y host que definimos hace unos pasos, para cada una de las interfaces que tenemos. Además, configuraremos la interfaz dinámica para obtener el direccionamiento de manera automática con el servidor DHCP.

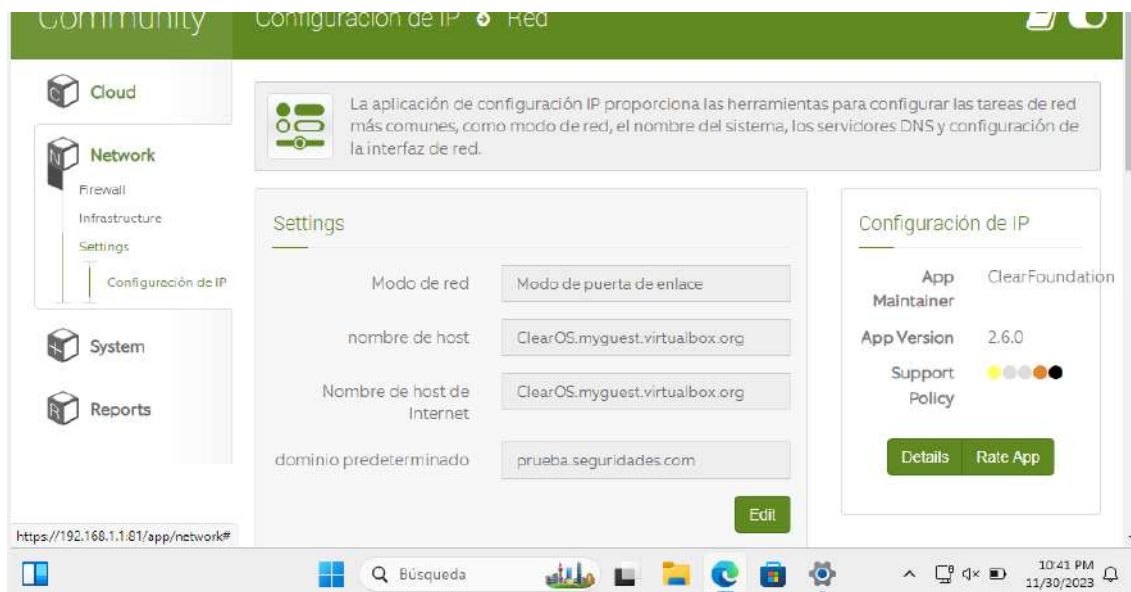


Figura 26 Configuración de IP.

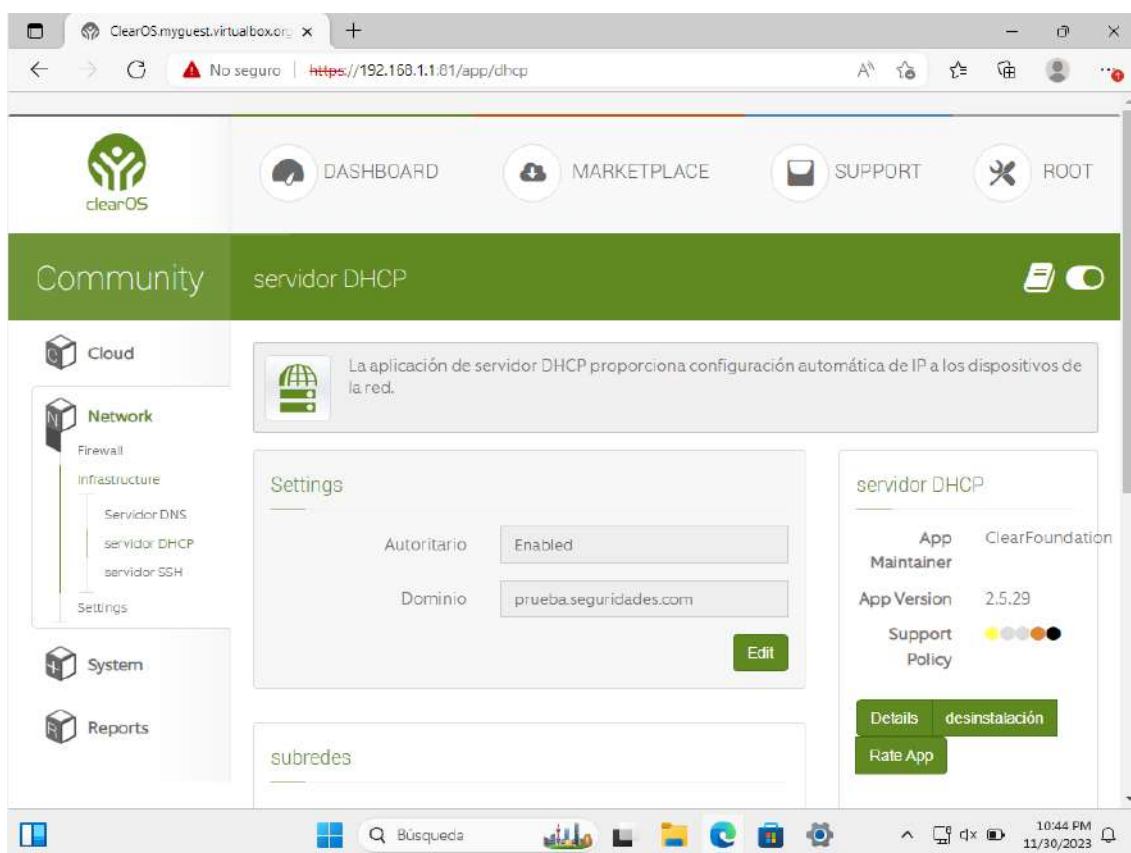


Figura 27 Configuración servidor DHCP.

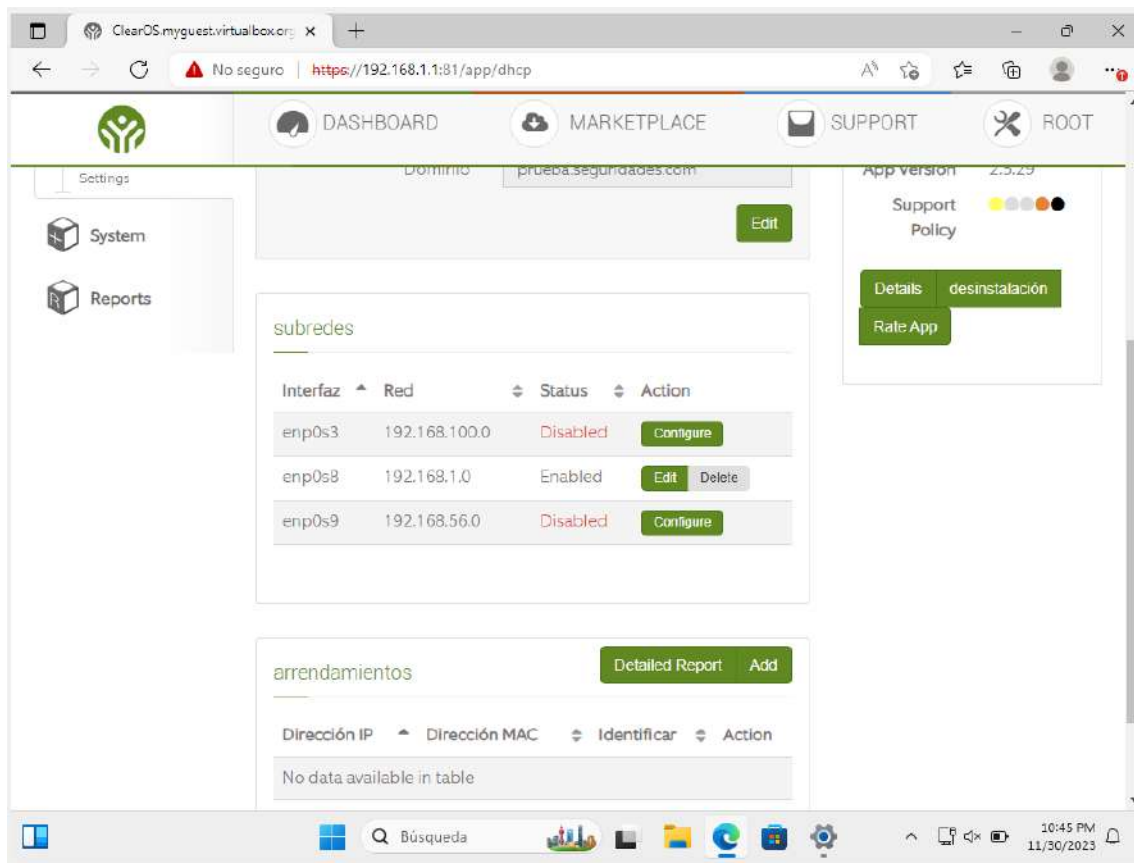


Figura 28 Comprobación estado de las subredes.

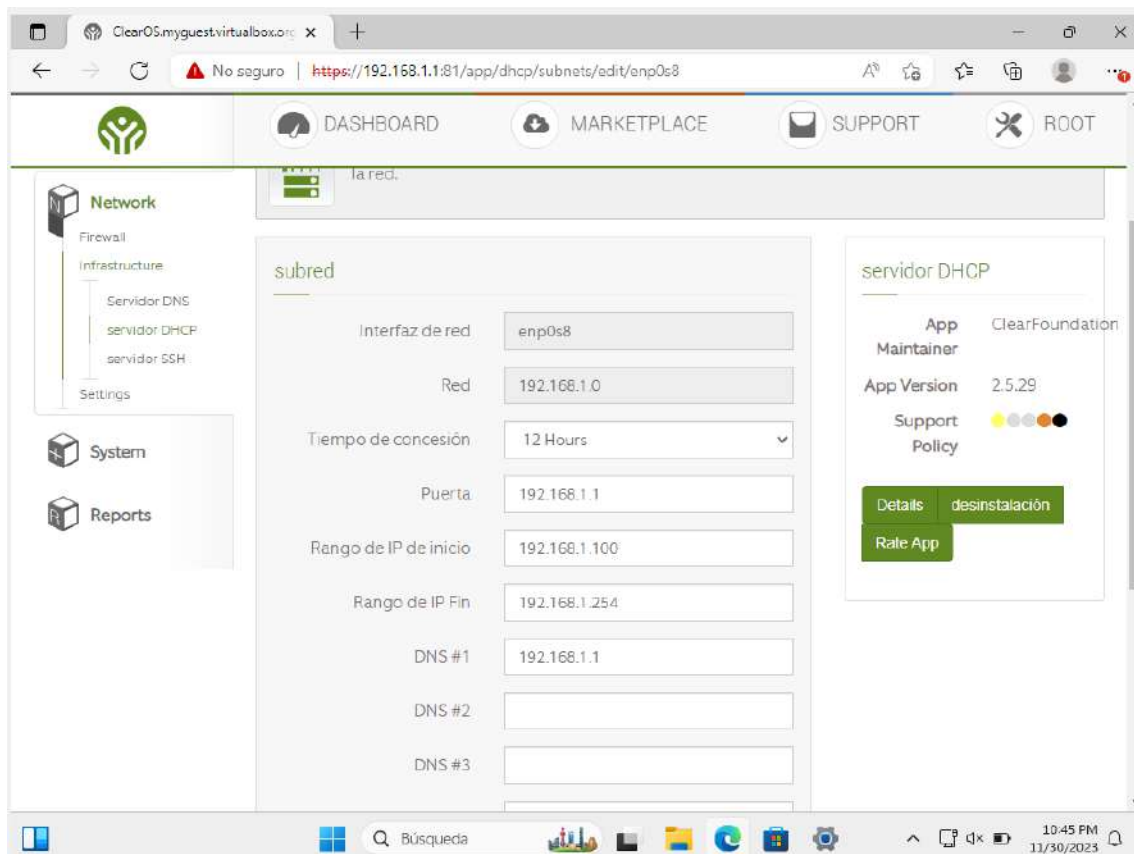


Figura 29 Direccionamiento DHCP que utilizaremos para seguir en la máquina Windows.

Ahora configurado el servidor DHCP en ClearOs se configura la IPv4 del Windows para que esta sea obtenida de manera automática (la cual es proporcionada por el servidor que se acabó de configurar).



Figura 30 Configuración de la IP Windows con DHCP

Luego se abre el símbolo de sistema para consultar la IP que ha sido proporcionada a la máquina, se usa el comando ipconfig. Importante recordar el DNS y el Gateway antes de que se realice el ataque.

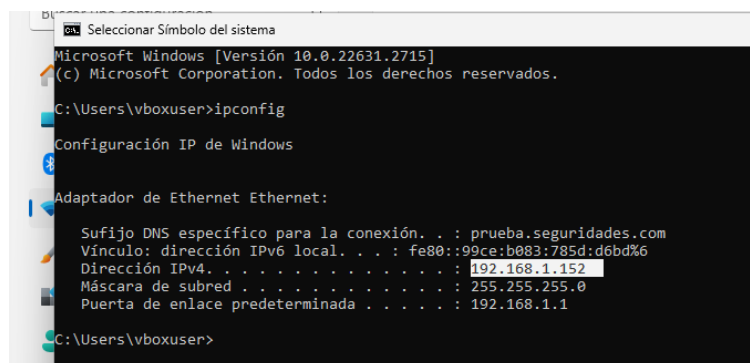


Figura 31 Consulta de la dirección IP

Se comprueba la conexión de Windows a Kali:

```

C:\Users\vboxuser>ping 192.168.1.204

Haciendo ping a 192.168.1.204 con 32 bytes de datos:
Respuesta desde 192.168.1.204: bytes=32 tiempo=13ms TTL=64
Respuesta desde 192.168.1.204: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.1.204: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.204: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.1.204:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 13ms, Media = 3ms

```

Figura 32 Ping desde Windows a Linux

Ahora se desactiva el firewall en la máquina Windows.

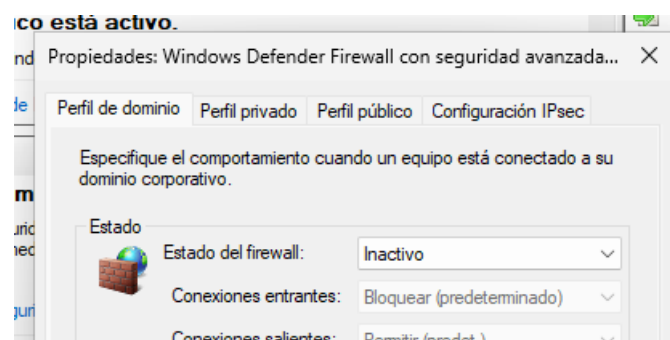


Figura 33 Firewall Windows

Luego que el ataque haya sido realizado, se realiza una configuración de red usando el comando ipconfig /release para verificar los cambios, se nota que no hay direcciones.

```

C:\Users\vboxuser>ipconfig /release

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::99ce:b083:785d:d6bd%6
    Puerta de enlace predeterminada . . . . . :

C:\Users\vboxuser>

```

Figura 34 ipconfig /release en Windows

Obtenemos la IP nuevamente y obtenemos que el Gateway es la dirección IP de la máquina Windows.

```
C:\Users\vboxuser>ipconfig /renew

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

Sufijo DNS específico para la conexión. . . :
Vínculo: dirección IPv6 local. . . : fe80::99ce:b083:785d:d6bd%6
Dirección IPv4. . . . . : 192.168.1.152
Máscara de subred. . . . . : 255.255.255.0
Puerta de enlace predeterminada. . . . . : 192.168.1.204

C:\Users\vboxuser>
```

Figura 35 Cambio del Gateway en Windows

Para probar el ataque del hombre en el medio se ingresa al servidor FTP desde Windows utilizando WinSCP

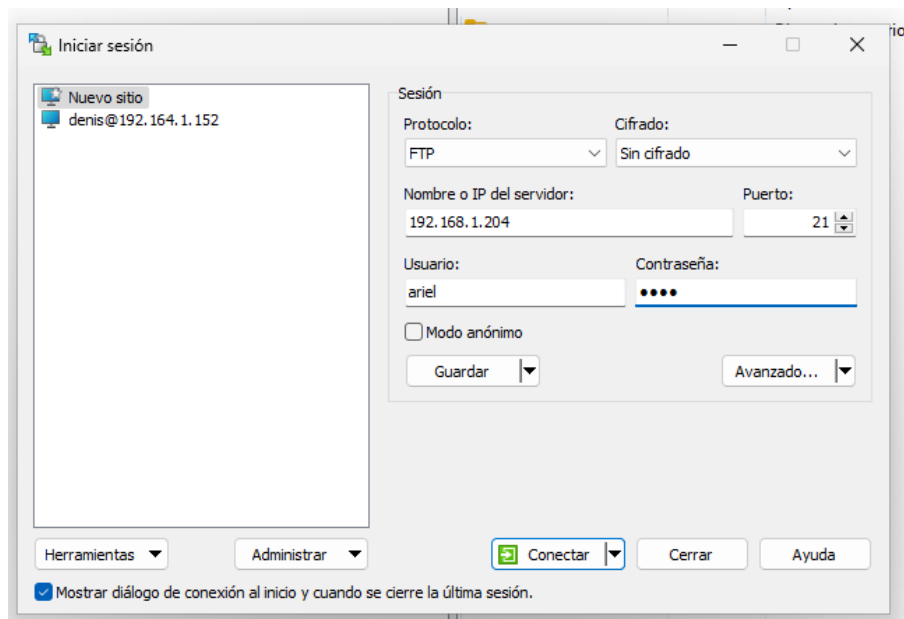


Figura 36 Inicio de sesión en WinSCP

Se conecta al servidor FTP obteniendo todo lo necesario. En WinSCP se crea una nueva carpeta.

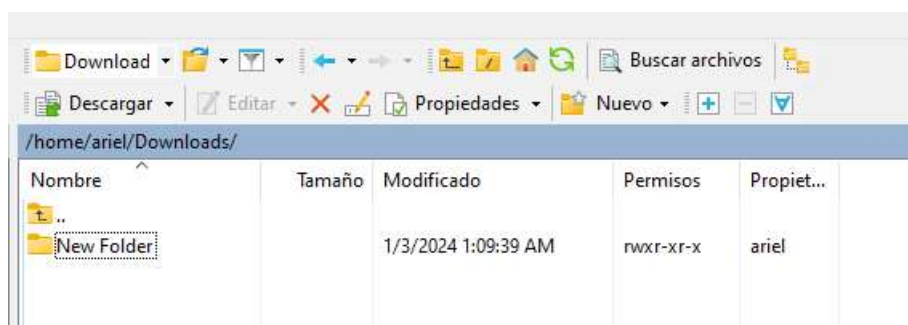


Figura 37 Creación de una carpeta en WinSCP

2.4 Kali

Para simular el ataque del hombre en el medio se utilizará una máquina virtual con el sistema operativo **Kali linux** que será la máquina entre el servidor DHCP (clearOs) y la máquina cliente (máquina Windows), que capture el tráfico de información.

Para empezar la configuración de la máquina virtual, se cambiará el adaptador de red a “red interna” para permitir que se conecte con el servidor DHCP con el fin de que pueda ser asignada una ip.

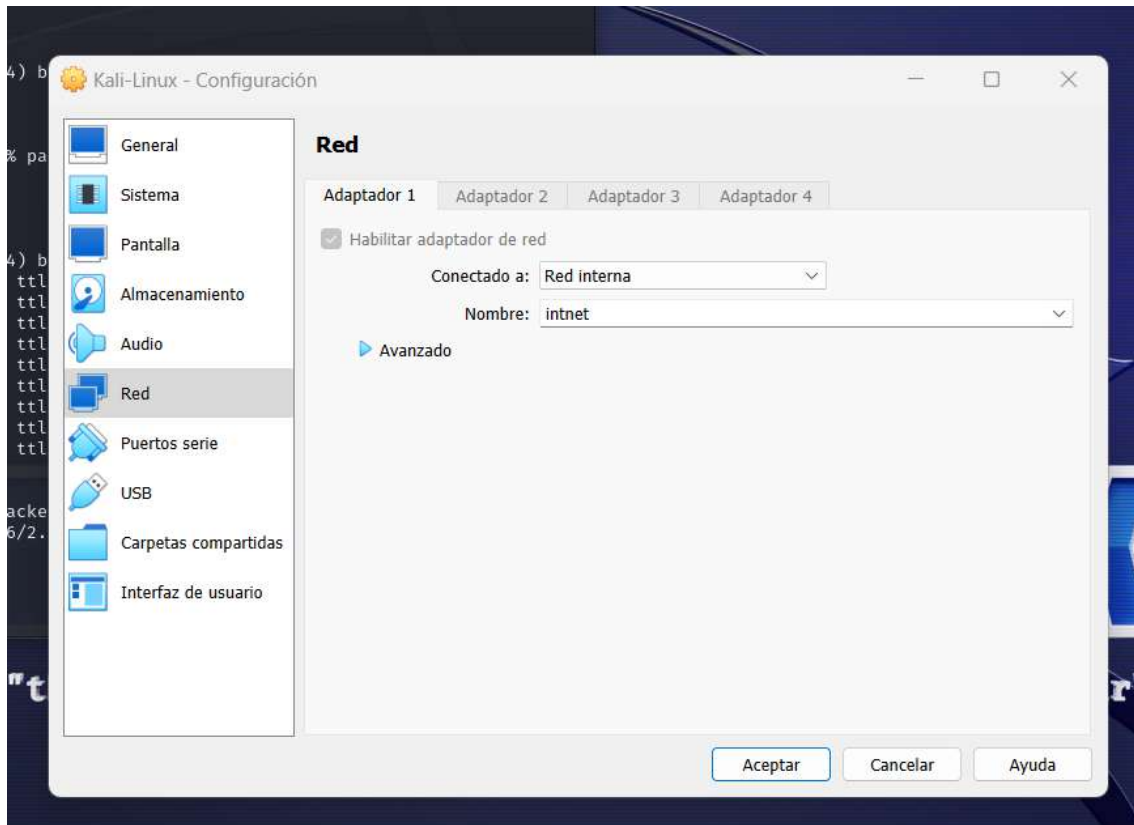


Figura 38 Adaptador de red "Red interna" en máquina Linux

Una vez encendida la máquina de Kali, se ingresa el comando **ip a** que permitirá ver la configuración y los detalles de la dirección ip que se le ha sido asignada. Así se comprueba que el servidor DHCP de la red interna funciona correctamente para Kali.


```
(ariel@kali2023)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:72:5d:42 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.204/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
        valid_lft 43140sec preferred_lft 43140sec
    inet6 fe80::a00:27ff:fe72:5d42/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Figura 39 Asignación dirección IP a kali linux.

Una vez asignada la dirección ip (192.168.1.204), se comprueba conexión hacia Windows mediante el comando **ping**.

```
(ariel@kali2023)-[~]
$ ping 192.168.1.152
PING 192.168.1.152 (192.168.1.152) 56(84) bytes of data.
64 bytes from 192.168.1.152: icmp_seq=1 ttl=128 time=1.34 ms
64 bytes from 192.168.1.152: icmp_seq=2 ttl=128 time=7.74 ms
64 bytes from 192.168.1.152: icmp_seq=3 ttl=128 time=3.65 ms
64 bytes from 192.168.1.152: icmp_seq=4 ttl=128 time=1.19 ms
64 bytes from 192.168.1.152: icmp_seq=5 ttl=128 time=1.04 ms
64 bytes from 192.168.1.152: icmp_seq=6 ttl=128 time=3.06 ms
64 bytes from 192.168.1.152: icmp_seq=7 ttl=128 time=0.956 ms
64 bytes from 192.168.1.152: icmp_seq=8 ttl=128 time=1.44 ms
64 bytes from 192.168.1.152: icmp_seq=9 ttl=128 time=0.973 ms
^C
— 192.168.1.152 ping statistics —
9 packets transmitted, 9 received, 0% packet loss, time 8024ms
rtt min/avg/max/mdev = 0.956/2.374/7.736/2.107 ms
```

Figura 40 Conexión entre kali y windows.

Para asegurar la conexión se realiza la comprobación desde la máquina Windows hacia la máquina Kali.

```
C:\Users\vboxuser>ping 192.168.1.204

Haciendo ping a 192.168.1.204 con 32 bytes de datos:
Respuesta desde 192.168.1.204: bytes=32 tiempo=13ms TTL=64
Respuesta desde 192.168.1.204: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.1.204: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.204: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.1.204:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 13ms, Media = 3ms
```

Figura 41 Conexión desde windows a kali.

A continuación, se crea un servidor ftp en la máquina Kali con un fin de poder capturar la información que se envíe a través de la máquina. Se ingresa como super administrador con el comando **sudo -i** y de actualiza.

```

(ariel@kali2023)-[~]
$ sudo -i

(root@kali2023)-[~]
#

(root@kali2023)-[~]
# apt-get update
Get:1 https://mirror.cedia.org.ec/kali kali-rolling InRelease [41.2 kB]
Get:2 https://mirror.cedia.org.ec/kali kali-rolling/main amd64 Packages [19.5 MB]
Get:3 https://mirror.cedia.org.ec/kali kali-rolling/main i386 Packages [19.1 MB]
Get:4 https://mirror.cedia.org.ec/kali kali-rolling/main amd64 Contents (deb) [45.9 MB]
Get:5 https://mirror.cedia.org.ec/kali kali-rolling/main i386 Contents (deb) [43.7 MB]
Get:6 https://mirror.cedia.org.ec/kali kali-rolling/contrib amd64 Packages [123 kB]
Get:7 https://mirror.cedia.org.ec/kali kali-rolling/contrib i386 Packages [102 kB]
Get:8 https://mirror.cedia.org.ec/kali kali-rolling/contrib amd64 Contents (deb) [296 kB]
Get:9 https://mirror.cedia.org.ec/kali kali-rolling/contrib i386 Contents (deb) [158 kB]
Get:10 https://mirror.cedia.org.ec/kali kali-rolling/non-free i386 Packages [182 kB]
Get:11 https://mirror.cedia.org.ec/kali kali-rolling/non-free amd64 Packages [227 kB]
Get:12 https://mirror.cedia.org.ec/kali kali-rolling/non-free i386 Contents (deb) [881 kB]
Fetched 130 MB in 35s (3701 kB/s)
Reading package lists... Done

```

Figura 42. Actualización de repositorio de paquetes de descargar en kali.

Se instala el servidor FTP con el comando apt-get install proftpd.

```

(root@kali2023)-[~]
# apt-get install proftpd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'proftpd-core' instead of 'proftpd'
The following packages were automatically installed and are no longer required:
  librtlsdr0 libzxing2
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  libmemcachedutil2 libpcres2-posix3 proftpd-doc
Suggested packages:
  openbsd-inetd | inet-superserver proftpd-mod-ldap proftpd-mod-mysql proftpd-mod-odbc proftpd-mod-pgsql
  proftpd-mod-sqlite proftpd-mod-geoip proftpd-mod-snp proftpd-mod-crypto proftpd-mod-wrap
The following NEW packages will be installed:
  libmemcachedutil2 libpcres2-posix3 proftpd-core proftpd-doc
0 upgraded, 4 newly installed, 0 to remove and 29 not upgraded.
Need to get 3558 kB of archives.
After this operation, 7746 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 https://mirror.cedia.org.ec/kali kali-rolling/main amd64 libmemcachedutil2 amd64 1.1.4-1 [14.6 kB]
Get:2 https://mirror.cedia.org.ec/kali kali-rolling/main amd64 libpcres2-posix3 amd64 10.42-4 [55.5 kB]
Get:3 http://http.kali.org/kali kali-rolling/main amd64 proftpd-core amd64 1.3.8.a+dfsg-1 [2552 kB]

```

Figura 43. Instalación de servidor FTP en kali.

Si la instalación se realizó de manera correcta entonces se podrá consultar la versión del servidor FTP que se ha instalado.

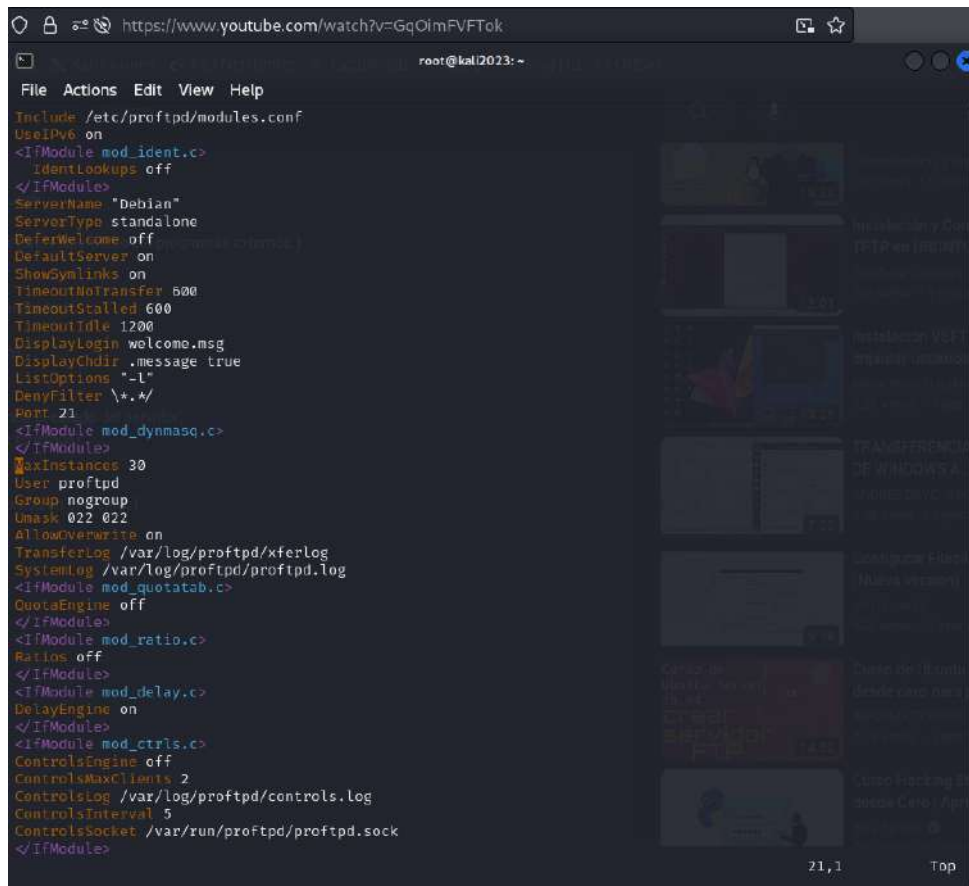
```

(root@kali2023)-[~]
# proftpd -v
ProFTPD Version 1.3.8a

```

Figura 44. Versión del servidor FTP instalado en kali.

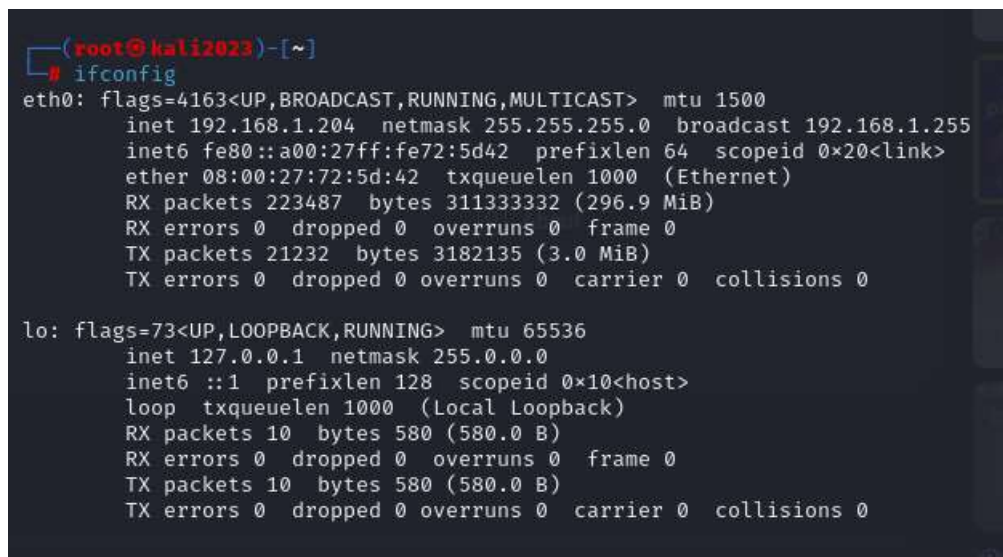
Se realizan modificaciones en los archivos necesarios.



```
https://www.youtube.com/watch?v=GqOimFVFTok
root@kali2023: ~
File Actions Edit View Help
Include /etc/proftpd/modules.conf
UseIPv6 on
<IfModule mod_ident.c>
  IdentLookups off
</IfModule>
ServerName "Debian"
ServerType standalone
DeferWelcome off
DefaultServer on
ShowSymLinks on
TimeoutNoTransfer 600
TimeoutStalled 600
TimeoutIdle 1200
DisplayLogin welcome.msg
DisplayChdir .message true
ListOptions "-l"
DenyFilter \.*/
Port 21
<IfModule mod_dynmasq.c>
</IfModule>
MaxInstances 30
User proftpd
Group nogroup
Umask 022 022
allowOverwrite on
TransferLog /var/log/proftpd/xferlog
SystemLog /var/log/proftpd/proftpd.log
<IfModule mod_quotatab.c>
  QuotaEngine off
</IfModule>
<IfModule mod_ratio.c>
  Ratios off
</IfModule>
<IfModule mod_delay.c>
  DelayEngine on
</IfModule>
<IfModule mod_ctrls.c>
  ControlEngine off
  ControlsMaxClients 2
  ControlLog /var/log/proftpd/controls.log
  ControlInterval 5
  ControlSocket /var/run/proftpd/proftpd.sock
</IfModule>
```

Figura 45 Modificación de archivos.

Se realiza una consulta de la dirección ip en Kali para verificar que se encuentra el servidor FTP.



```
(root@kali2023)-[~]
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.204 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe72:5d42 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:72:5d:42 txqueuelen 1000 (Ethernet)
    RX packets 223487 bytes 31133332 (296.9 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 21232 bytes 3182135 (3.0 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 10 bytes 580 (580.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 10 bytes 580 (580.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figura 46 Consulta dirección IP en Kali.

Con el comando **service proftpd status** se comprueba que el servidor FTP se encuentre activo y corriendo para terminar con la configuración necesaria.

```
(root@kali2023)~[~]
$ service proftpd status
● proftpd.service - ProFTPD FTP Server
   Loaded: loaded (/lib/systemd/system/proftpd.service; disabled; preset: disabled)
   Active: active (running) since Wed 2024-01-03 01:19:15 -05; 28min ago
     Docs: man:proftpd(8)
   Process: 22284 ExecStartPre=/usr/sbin/proftpd --configtest -c $CONFIG_FILE $OPTIONS (code=exited, status=0/SUCCESS)
   Process: 22285 ExecStart=/usr/sbin/proftpd -c $CONFIG_FILE $OPTIONS (code=exited, status=0/SUCCESS)
  Main PID: 22287 (proftpd)
    Tasks: 1 (limit: 2260)
   Memory: 3.4M
      CPU: 357ms
   CGroup: /system.slice/proftpd.service
           └─22287 "proftpd: (accepting connections)"

Jan 03 01:19:15 kali2023 systemd[1]: Starting proftpd.service - ProFTPD FTP Server ...
Jan 03 01:19:15 kali2023 proftpd[22284]: Checking syntax of configuration file
Jan 03 01:19:15 kali2023 systemd[1]: Started proftpd.service - ProFTPD FTP Server.
lines 1-16/16 (END)
```

Figura 47 Comprobación status servidor FTP en kali.

Una vez terminada la configuración de la máquina Kali/Linux se procederá a realizar el ataque de hombre en el medio. Para ello se usará ettercap en la máquina atacante Kali con el fin de cambiar el gateway de la máquina Windows y así poder hacer que toda la información, que viaje desde la máquina Windows hacia el servidor DNS, pase primero por la máquina Kali y así poder capturar la información.

Dentro de la máquina Kali se ejecuta el comando **sudo ettercap -G** para abrir la aplicación ettercap en modo gráfico.

```
(ariel@kali2023)~[~]
$ sudo ettercap -G

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

□
```

Figura 48 Comando de ejecución de Ettercap en modo gráfico.

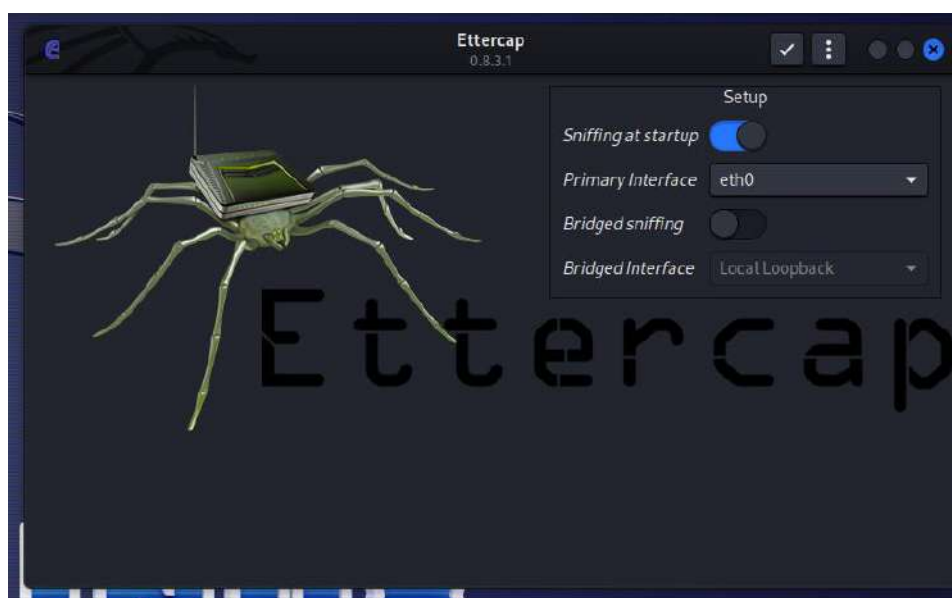


Figura 49 Ejecución Ettercap.

Ettercap es una aplicación que permite el análisis de red y pruebas de seguridad. En la parte superior derecha se encuentran tres puntos, se da click y se desplegarán opciones para el ataque hombre en el medio o MITM (Man-In-The-Middle). Se seleccionará la opción de DHCP spoofing que permitirá envenenar las respuestas del servidor DHCP.

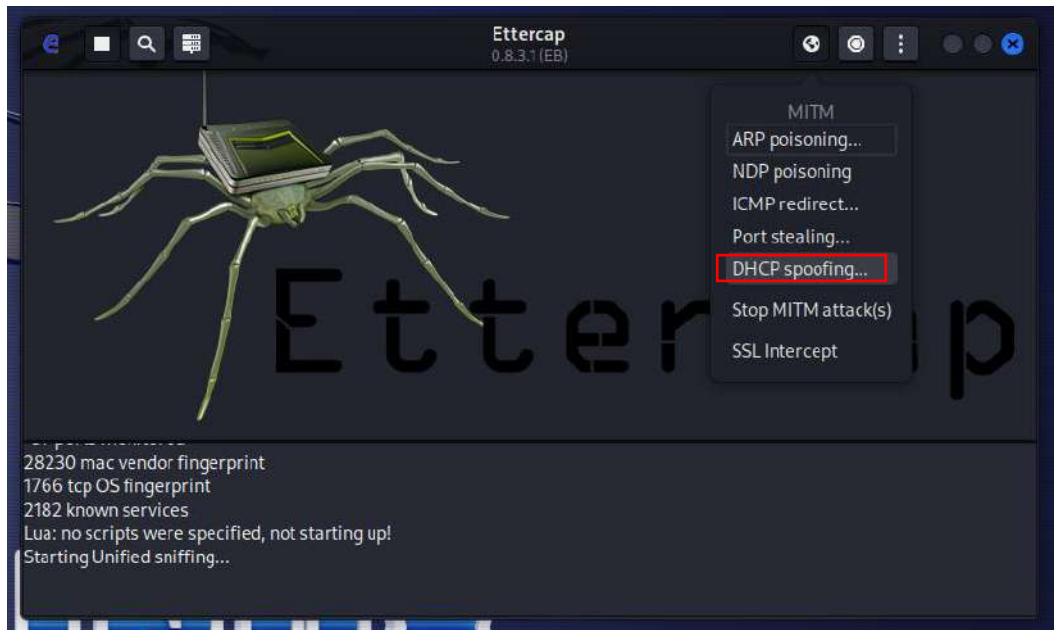


Figura 50 Selección de DHCP spoofing dentro de Ettercap.

Una vez que se selecciona la opción de DHCP spoofing para técnica para el ataque de hombre en el medio, se desplegará una pantalla como la que se muestra en la figura 51, donde se pide la máscara de la red en la que se está trabajando y el DNS Server IP donde se ingresa la dirección IP a la cual se quiera mandar la información simulando el hombre en el medio.

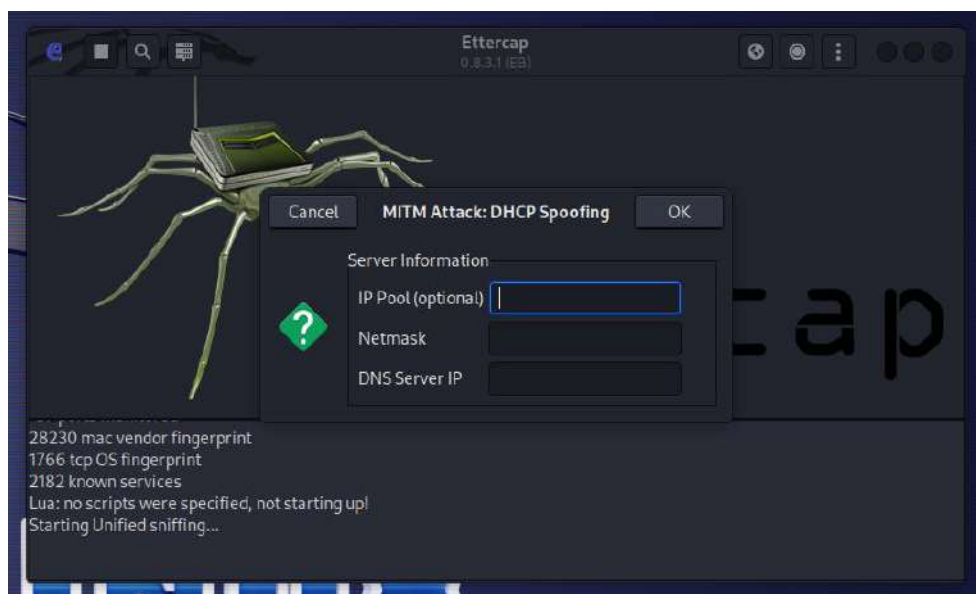


Figura 51 Pantalla de configuración DHCP spoofing


```

Adaptador de Ethernet Ethernet:

Sufijo DNS específico para la conexión. . : prueba.seguridades.com
Vínculo: dirección IPv6 local. . . : fe80::99ce:b083:785d:d6bd%6
Dirección IPv4. . . . . : 192.168.1.152
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . : 192.168.1.1

C:\Users\vboxuser>

```

Figura 54 IP y Gateway Windows antes del ataque

Con el comando **ip release** Windows dejará de tener una dirección ip, y seguido se vuelve a pedir una nueva dirección IP.

```

C:\Users\vboxuser>ipconfig /renew

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

Sufijo DNS específico para la conexión. . :
Vínculo: dirección IPv6 local. . . : fe80::99ce:b083:785d:d6bd%6
Dirección IPv4. . . . . : 192.168.1.152
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . : 192.168.1.204

C:\Users\vboxuser>

```

Figura 55 IP y Gateway Windows después del ataque

Se puede observar que la puerta de enlace predeterminada o gateway ha cambiado, y es la dirección IP de la máquina Kali, así entonces Kali está atacando con la técnica de hombre en el medio.

Si se verifica en Kali en la aplicación de Ettercap se podrá observar que

Si se verifica en Kali en la aplicación de Ettercap se podrá observar que hay un registro que desde la máquina Windows se hizo una petición de una dirección IP y como se configuró un DHCP spoofing entonces la máquina Kali fue quien actuó como servidor DHCP.

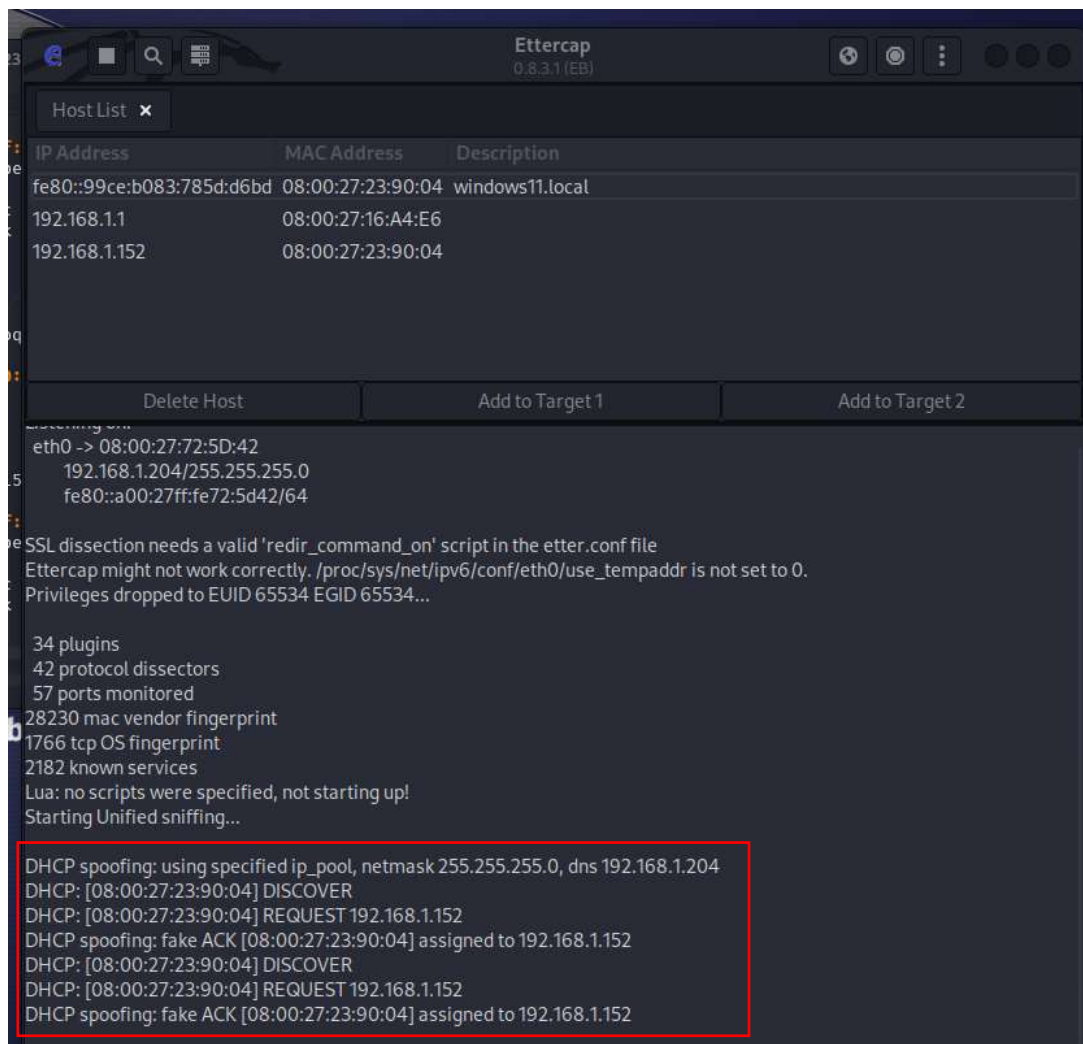


Figura 56 Registro de petición y asignación de IP en Ettercap

Para probar el hombre en el medio se ingresa al servidor ftp desde Windows utilizando WINSCP

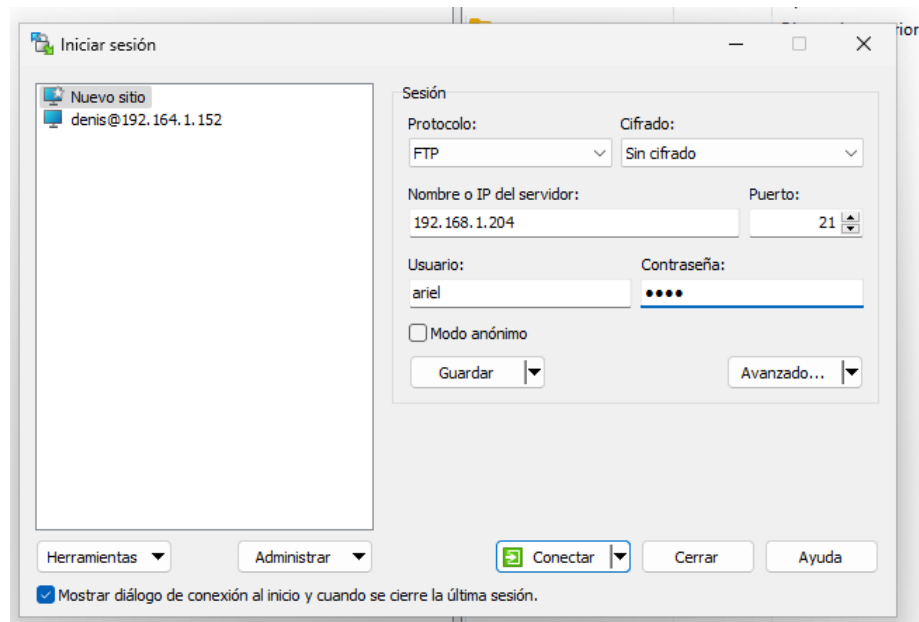


Figura 57 Ingreso a servidor FTP en Windows

Se conecta al servidor ftp obteniendo todo lo necesario.

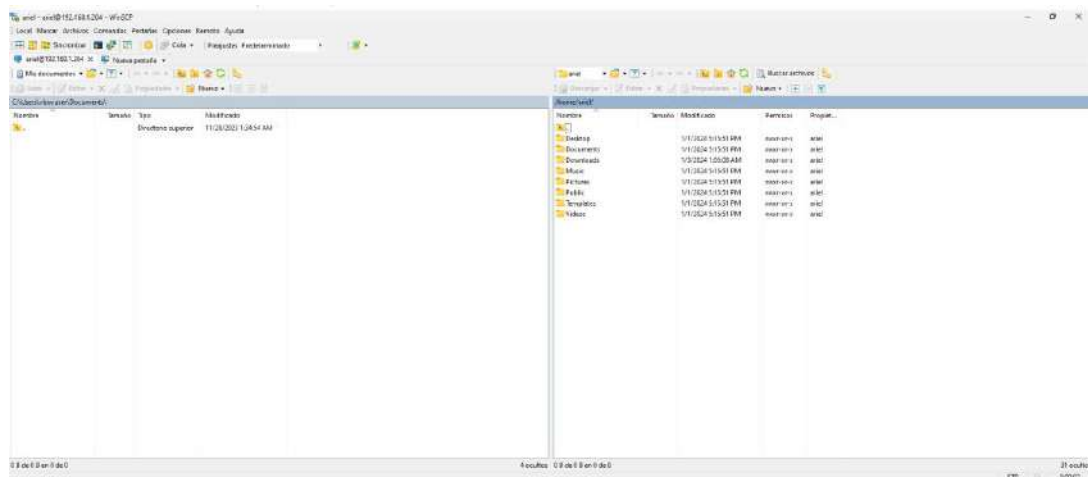


Figura 58 Conexión a servidor FTP en windows

Para comprobar que se haya hecho la conexión exitosa se creará una carpeta desde Windows, y esto se deberá reflejar en la máquina Kali.

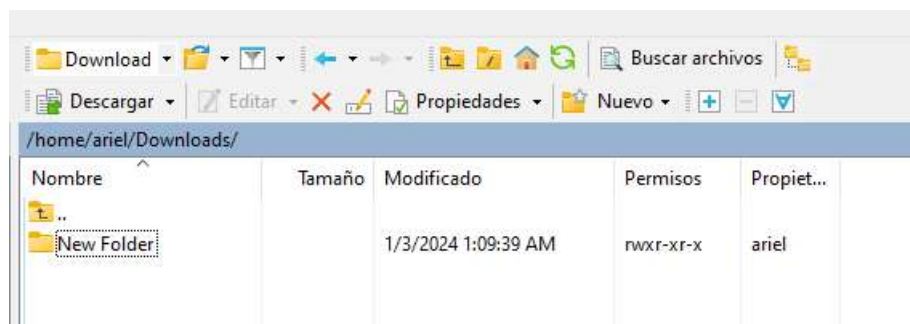


Figura 59 Creación carpeta desde Windows hacia Kali

Se verifica en Kali Linux la creación de la carpeta:

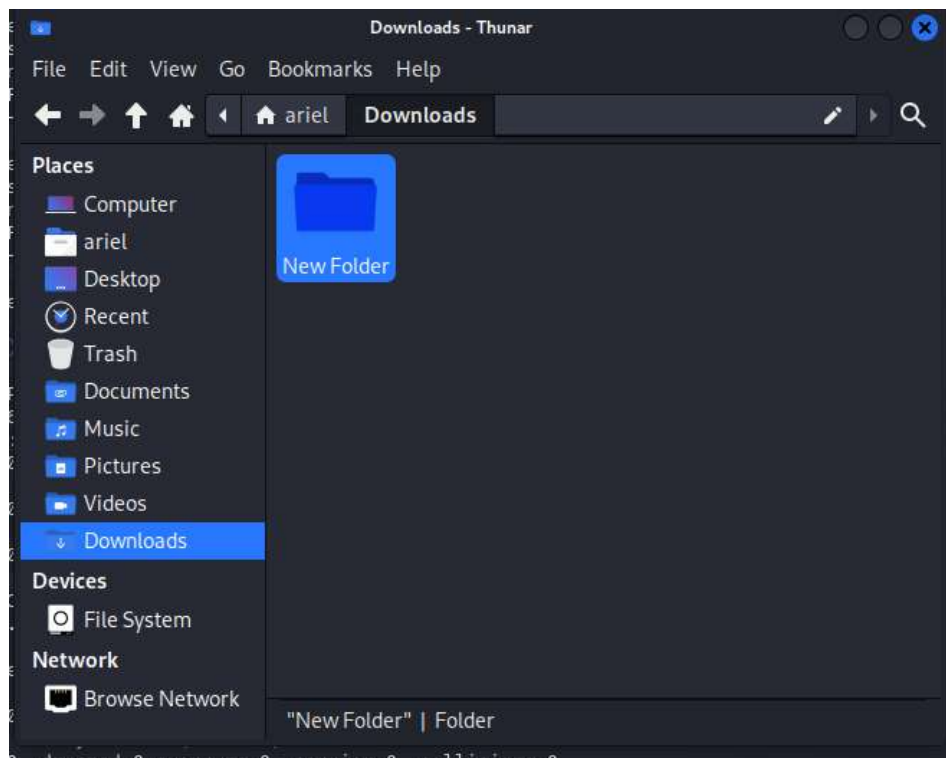


Figura 60 Comprobación creación de carpeta en Kali

En Wireshark en Kali se puede ver la captura de datos cuando se intenta ingresar a un sitio comprobando que existe una comunicación y Kali Linux está observando y capturando todo el tráfico de red.

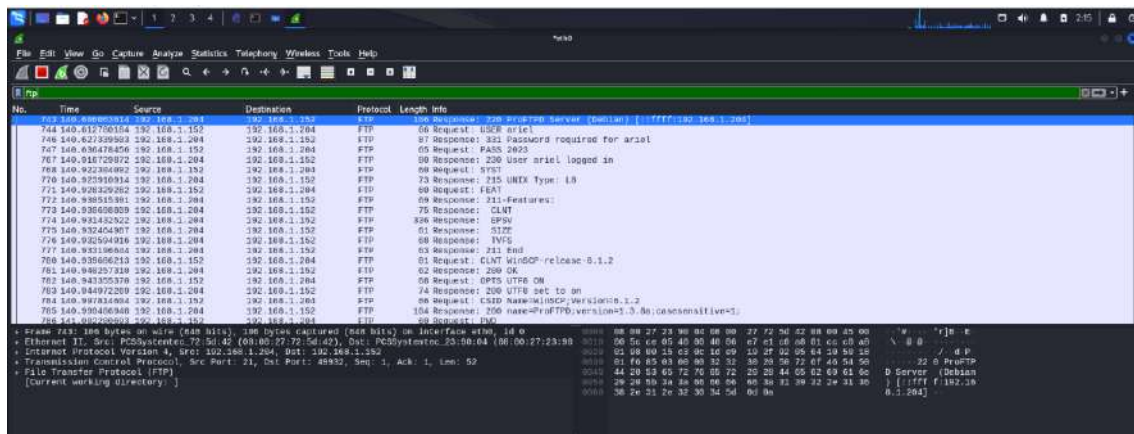


Figura 61 Captura de tráfico de red en Wireshark en Kali

Para ver el contenido completo se da clic derecho sobre el trafico que se desea analizar, seguido se da clic a Follow, posteriormente a tcp stream.

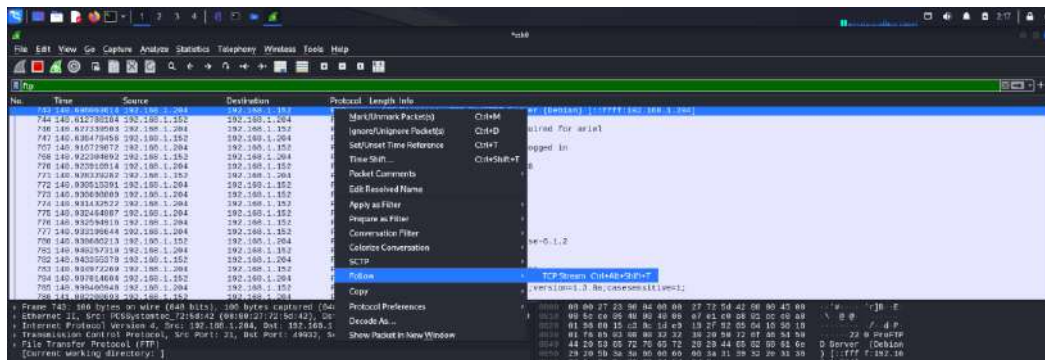


Figura 62 Pasos para ver contenido completo del tráfico específico

Obteniendo la solicitud reestructurada y con todos los datos del cliente.

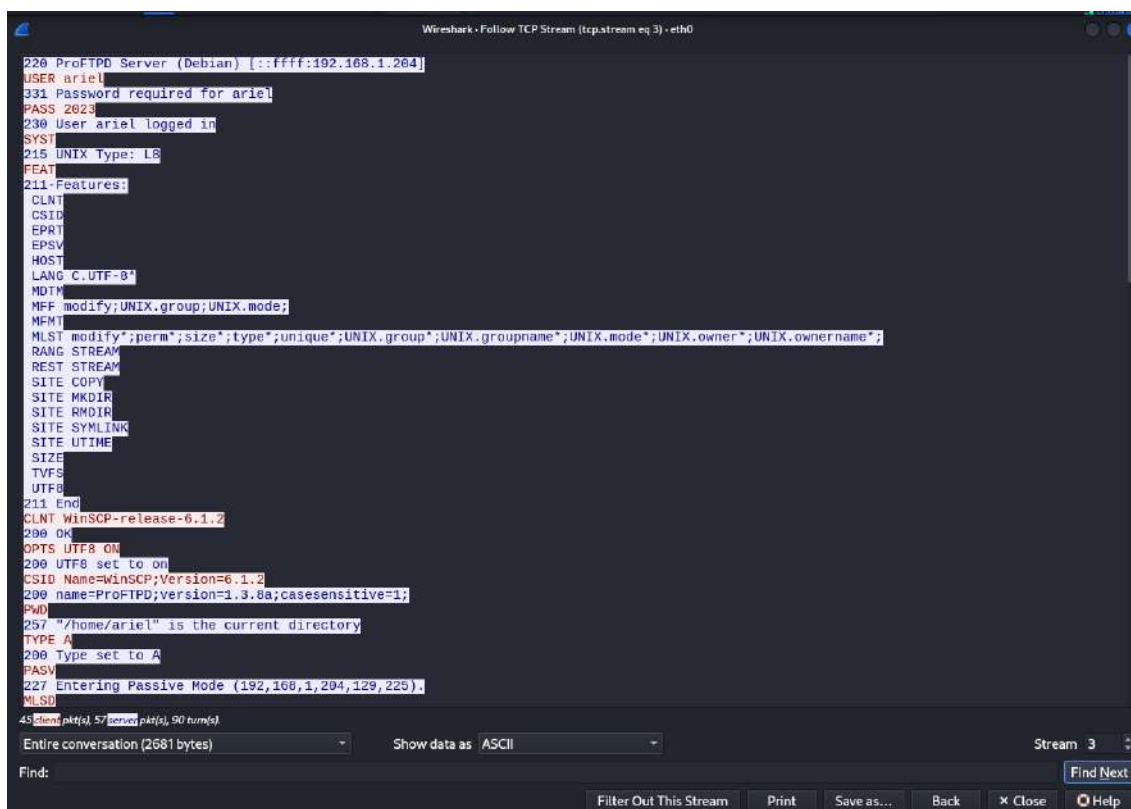


Figura 63 Información detallada del tráfico

Donde se encuentra el usuario y contraseña.

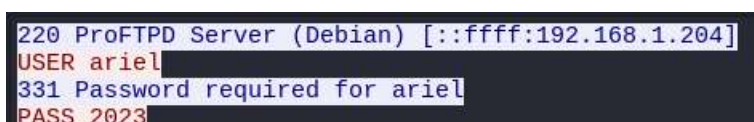


Figura 64 Usuario y contraseña capturadas en Kali

De esta forma se ha realizado la simulación del ataque de hombre en el medio capturando usuario y contraseña de un usuario.

3. CONCLUSIONES Y RECOMENDACIONES

- Se logró configurar las tres máquinas virtuales con los adaptadores de red adecuados y los parámetros de red necesarios para establecer la comunicación entre ellas.
- Se logró instalar y configurar el servidor FTP en Kali Linux y acceder al mismo desde el cliente Windows mediante el programa WinSCP1.
- Se logró realizar el ataque de MitM mediante el uso de Ettercap, cambiando el gateway del cliente Windows por la dirección IP de Kali Linux y capturando todo el tráfico de red que pasaba por esta máquina.
- Se logró analizar los paquetes capturados mediante el uso de Wireshark, identificando los protocolos involucrados, los datos enviados y recibidos, y la información sensible como el usuario y la contraseña del servidor FTP.
- Se debe verificar la configuración de red de las máquinas virtuales antes de iniciar el ataque, asegurándose de que tengan la dirección IP, la máscara de red, el gateway y el DNS correctos.
- Se recomienda desactivar el firewall de Windows para evitar que bloquee el tráfico de red entrante y saliente y dificulte el ataque.

4. BIBLIOGRAFÍA

[1] P. Zambrano, "Simulación con máquinas virtuales de un ataque de Man-in-the-middle," Clase de Tecnologías de Seguridad, EPN, 2023-B.