

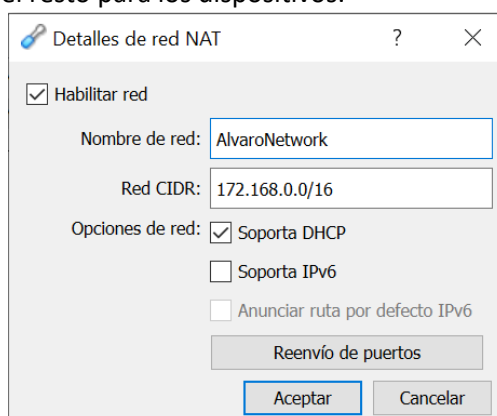
Facultad:	Ciencias Jurídicas y Empresariales
Grado:	Gestión de la Ciberseguridad
Asignatura:	Fundamentos de las TICs y la Ciberseguridad
Fecha:	17 de diciembre de 2021
Valor de examen:	60% de la nota final. Nota máxima 6 puntos.
Nombre y Apellidos.	Álvaro Luis Ruiz Alcántara
DNI.	77492313T

Instrucciones

- El examen se entregará en formato Word (extensión .doc o .docx) o formato pdf, sin cifrar en la tarea de Canvas creada al efecto de manera obligatoria.
- El alumno debe incluir pantallazos y breves justificaciones de lo realizado en el ejercicio. (Sugerencia: Utilizar el software Recortes incluido en Windows).

1. Mediante el uso del software de gestión de máquinas virtuales (Oracle Virtual Box), crea una red de NAT con VirtualBox con un direccionamiento de red de clase B simple con máscara de 16 bits. Asigna esta red a las dos máquinas virtuales (Windows 10 y Kali Linux). Muestra con pantallazos el proceso de configuración y de asignación a las máquinas virtuales. ¿Cuántas direcciones de red podríamos tener simultáneamente con esta configuración? **0,5 PUNTOS.**

Mediante VirtualBox, accedemos a preferencias y en Red, creamos una nueva red NAT, como tiene que ser clase B, los primeros 16 bits deben estar reservados para el identificador de red y el resto para los dispositivos.



Con esta configuración, se pueden llegar a tener 65533 dispositivos, una IP se reserva para la dirección de red (todos los bits de los dispositivos a 0) y otra para la dirección broadcast (todos los bits reservados para los dispositivos a 1). En caso de tener un router, también se reservaría una IP para este dispositivo, que suele ser los cuartetos de los dispositivos a 1.

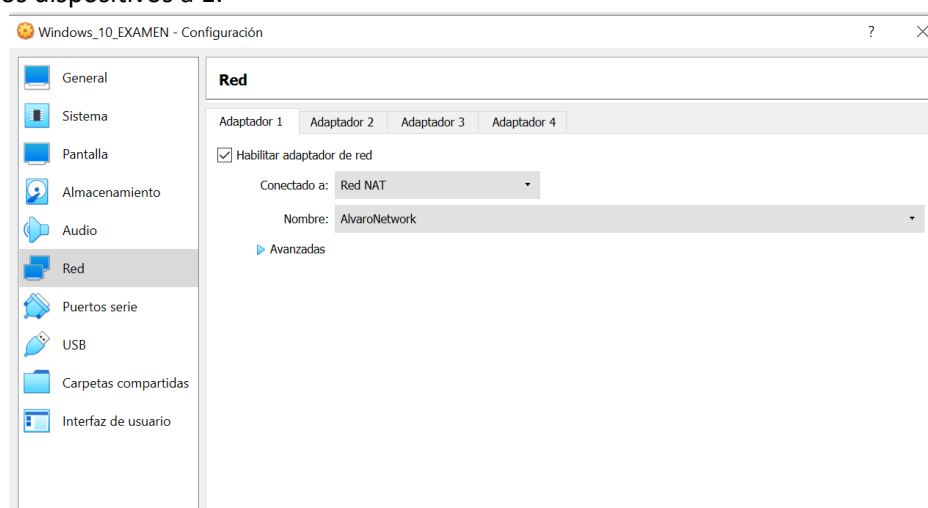


Ilustración 1 - Red NAT en la máquina de Windows

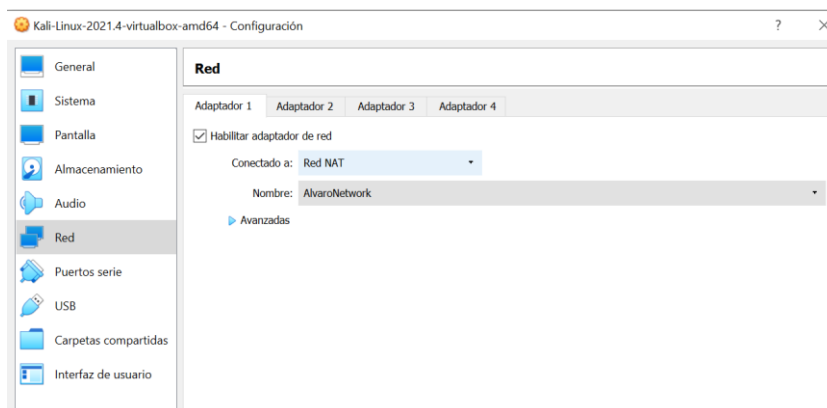


Ilustración 2 - Red NAT en la máquina de Kali

2. ¿Cómo o con que comando comprobarías que disponemos de comunicación entre las dos máquinas virtuales? ¿Disponemos de comunicación bidireccional con ese comando? Si no tuviéramos conexión en algún sentido, ¿Por qué creéis que sucede esto? ¿Cómo podríamos conseguir habilitar esta comunicación? Justifica las respuestas y muestra pantallazos de los resultados. **0,5 PUNTOS.**

Podríamos probar con ping, que comprueba mediante paquetes ICMP si las dos máquinas se ven. Aún así, en caso de que una de las máquinas rechace este tipo de paquetes, no quiere decir que no se vean.

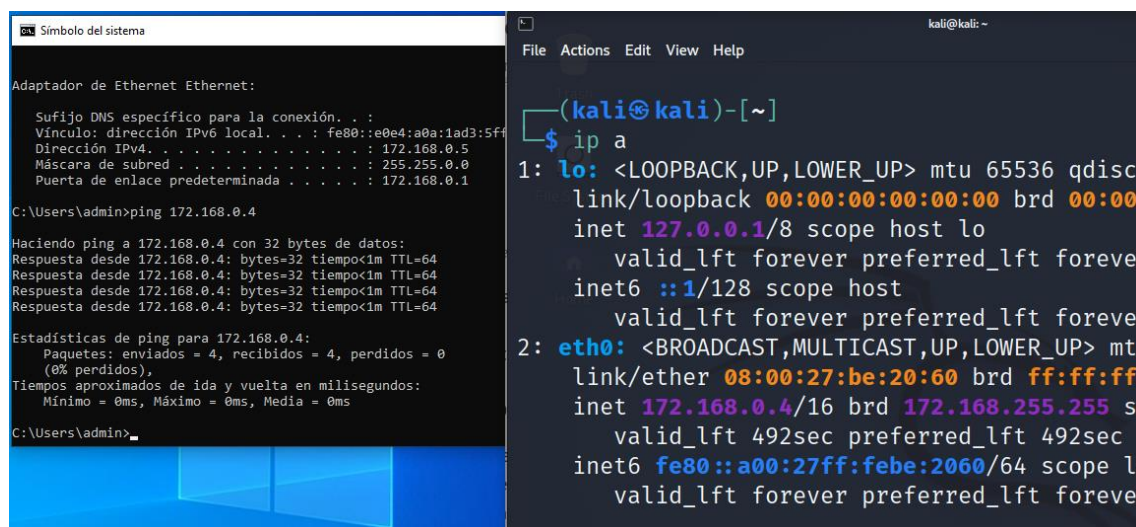


Ilustración 3 - Ping de Windows a Kali

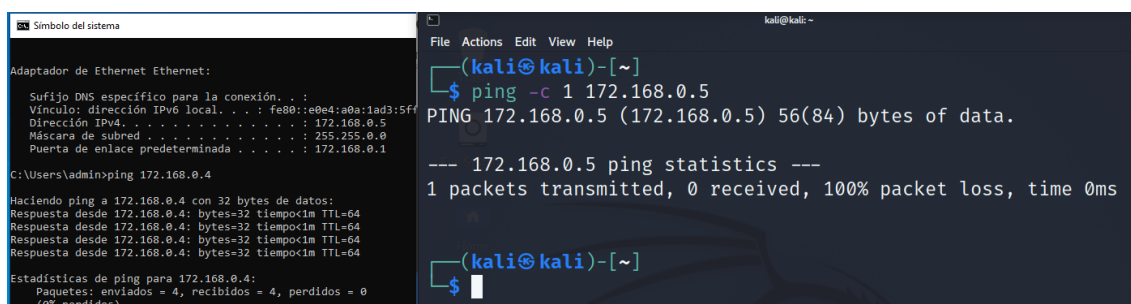


Ilustración 4 - Ping de Kali a Windows

La comunicación por ICMP no es bidireccional porque Windows tiene por defecto una regla en su firewall que rechaza este tipo de paquetes, para conseguir que los acepte, se debe desactivar el firewall, desactivar la norma que los bloquea en redes locales o crear una norma de excepción.

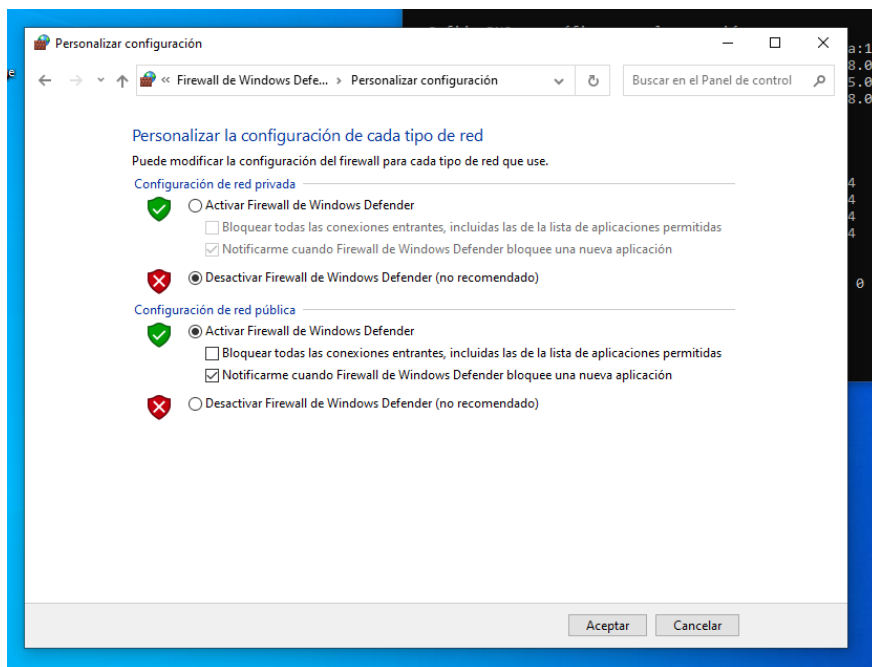


Ilustración 5 - Desactivación de Firewall en redes locales

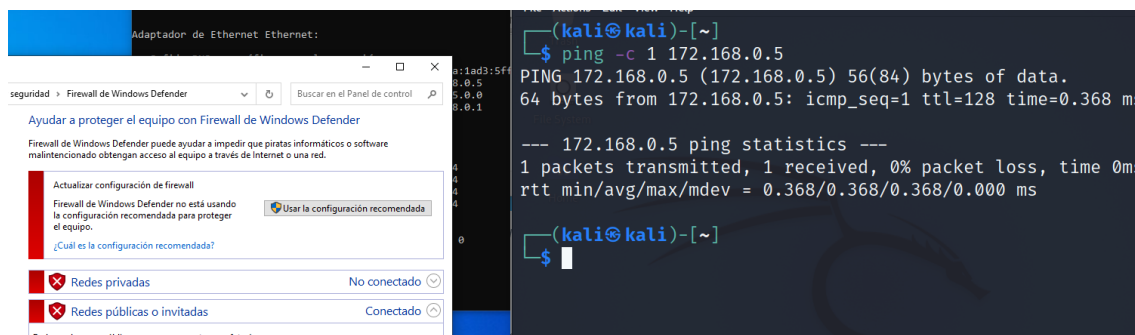


Ilustración 6 - Comunicación bidireccional con firewall desactivado

3. Crea el usuario "UFV+ Inicial nombre alumno + Primer apellido alumno" en tu máquina Windows 10 sin privilegios de administrador. Muestra pantallazos del proceso realizado. **0,5 PUNTOS.**

Para crear usuarios, se procede a ir al menú de creación de estos mediante el buscador de Windows.

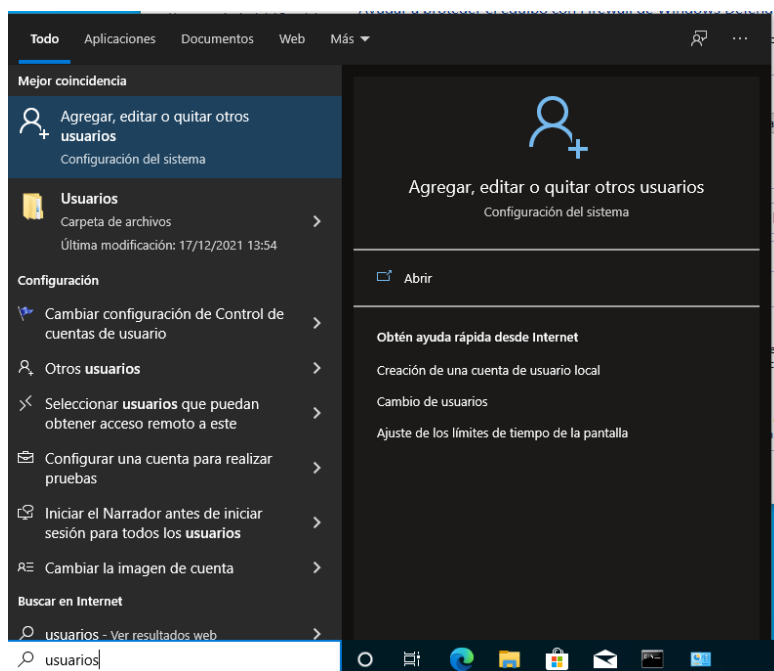


Ilustración 7 - Buscador de Windows

Se hace click en la siguiente opción:

Otros usuarios

Permite que las personas que no forman parte de tu familia inicien sesión con sus propias cuentas. Esto no las agregará a tu familia.

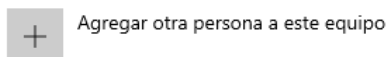


Ilustración 8 – Opción de agregar otro usuario al equipo

Para crear usuarios dentro del equipo local, se selecciona “Agregar usuario sin cuenta de Microsoft”.

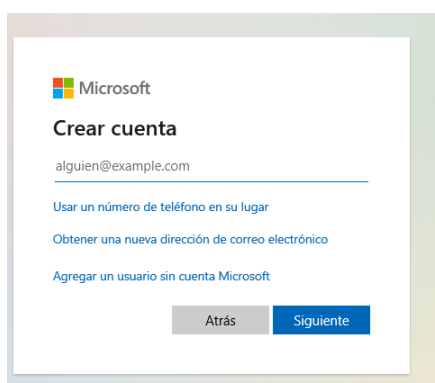


Ilustración 9 - Solicitud de credenciales de Microsoft

Se procede a rellenar los datos del usuario y las credenciales:

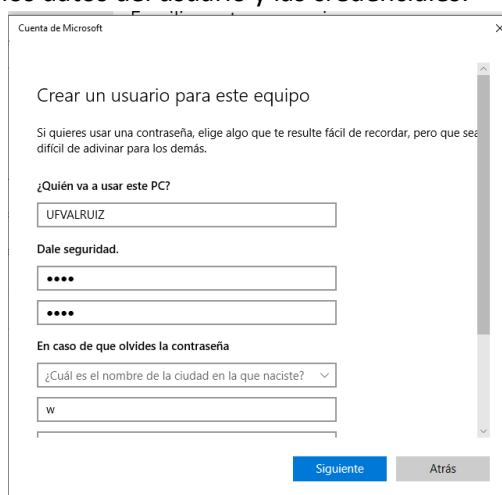


Ilustración 10 - Datos del usuario

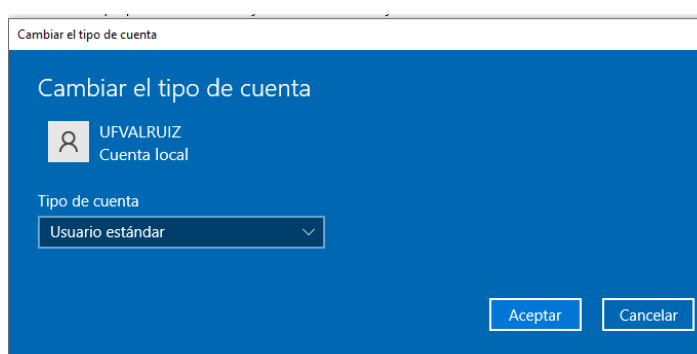


Ilustración 11 - Se crea un usuario estándar

4. Bloquea el tráfico entrante a tu máquina a los puertos 80 y 443 mediante el firewall de Windows. Muestra pantallazos del proceso realizado. **0,5 PUNTOS.**

Para ello, se procede a entrar a la configuración avanzada del firewall como se muestra en la siguiente imagen:

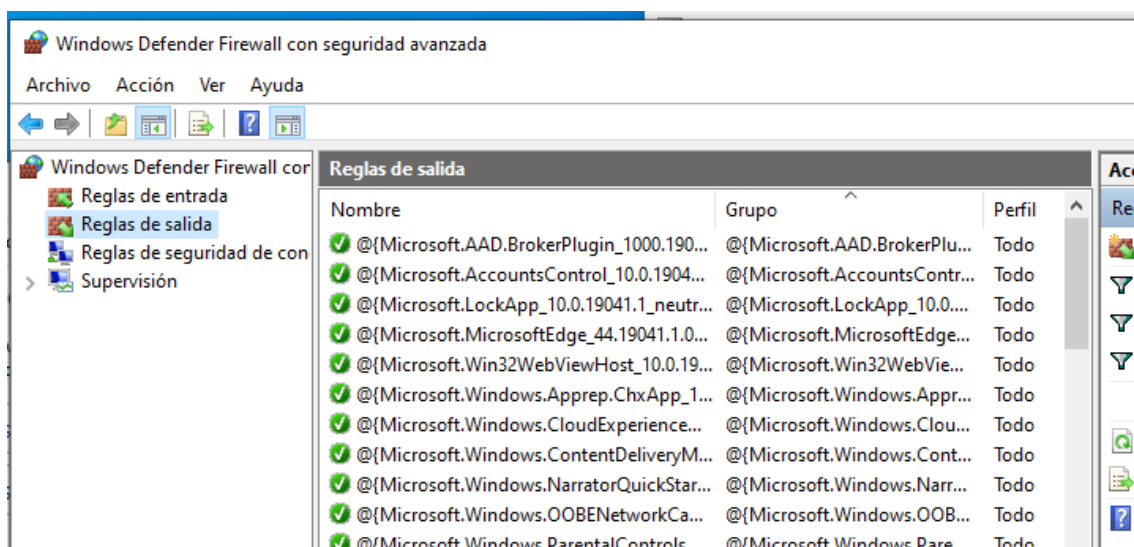


Ilustración 12 - Configuración avanzada del firewall

Una vez ahí, se crea una norma con le objetivo de bloquear todas las conexiones salientes mediante los puertos 80 (HTTP) y 443 (HTTPS).

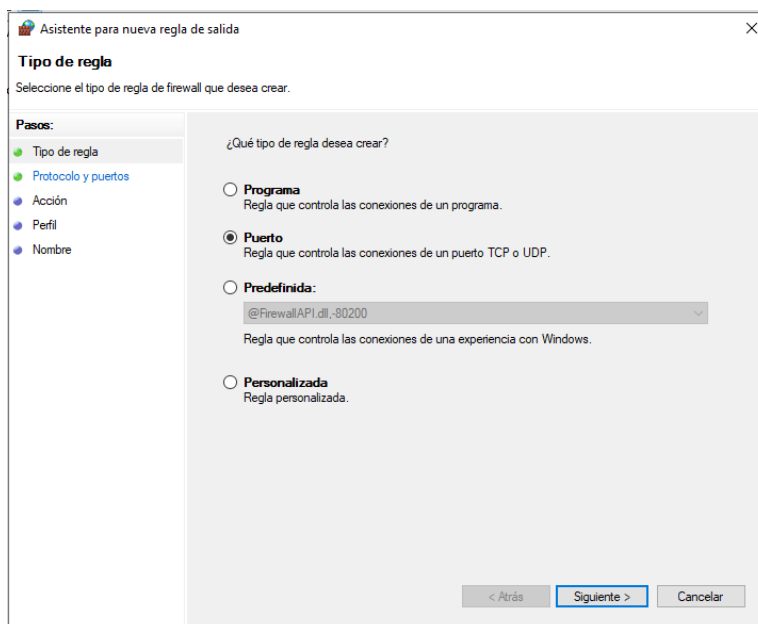
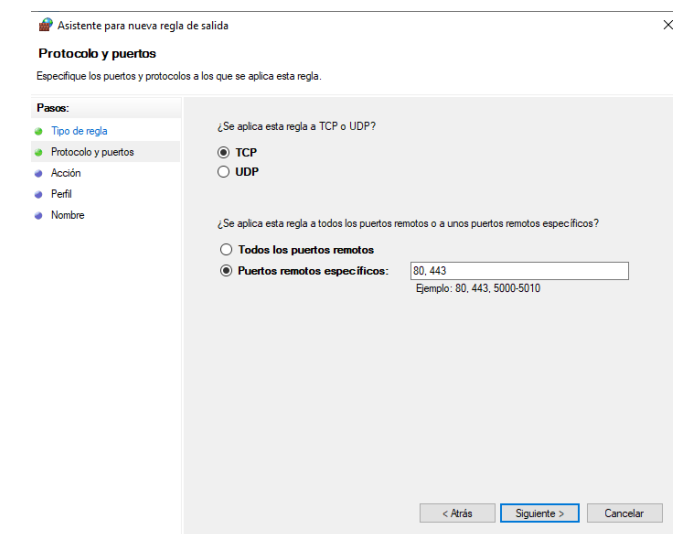
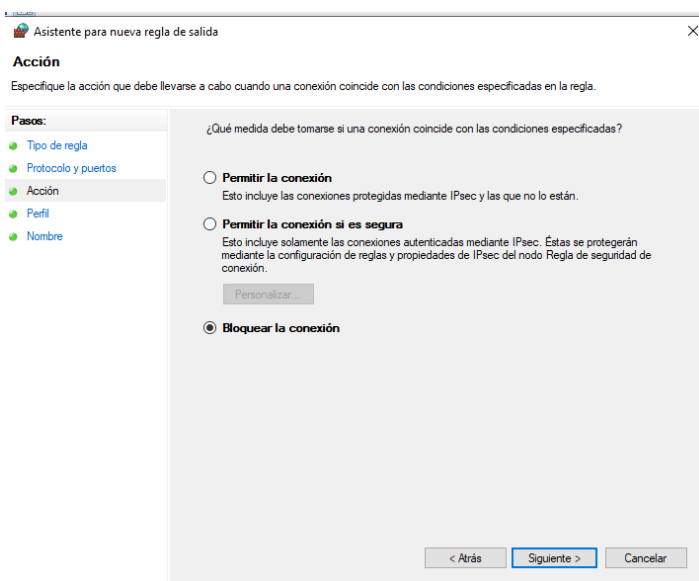


Ilustración 13 - Restricción de conexión mediante puertos

Se bloquea las conexiones a estos puertos mediante el protocolo TCP (se hará la misma norma pero con la casilla de UDP activada).

*Ilustración 14 - Puertos que se deseen bloquear*

En este apartado, se debe seleccionar “Bloquear conexión”.

*Ilustración 15 - Se selecciona "Bloquear conexión"*

La regla se aplicará en todos los dominios y redes:

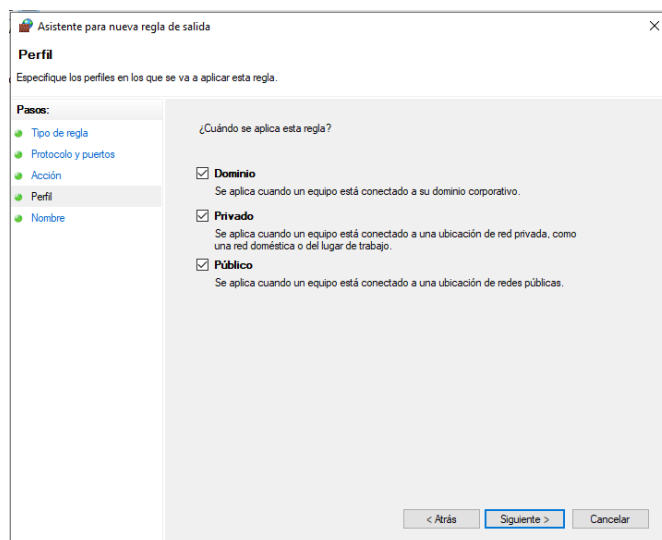


Ilustración 16 - Donde se aplica la regla

Se procede a insertar un título en la norma:

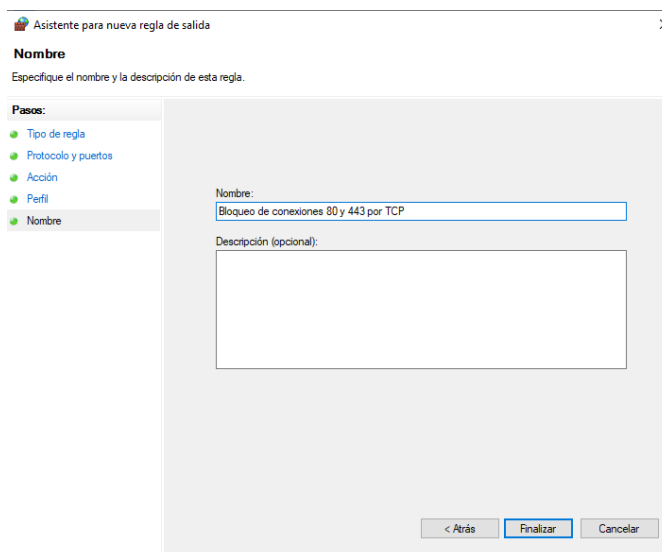


Ilustración 17 - Se inserta un título de la regla

Se comprueba que la norma funciona.

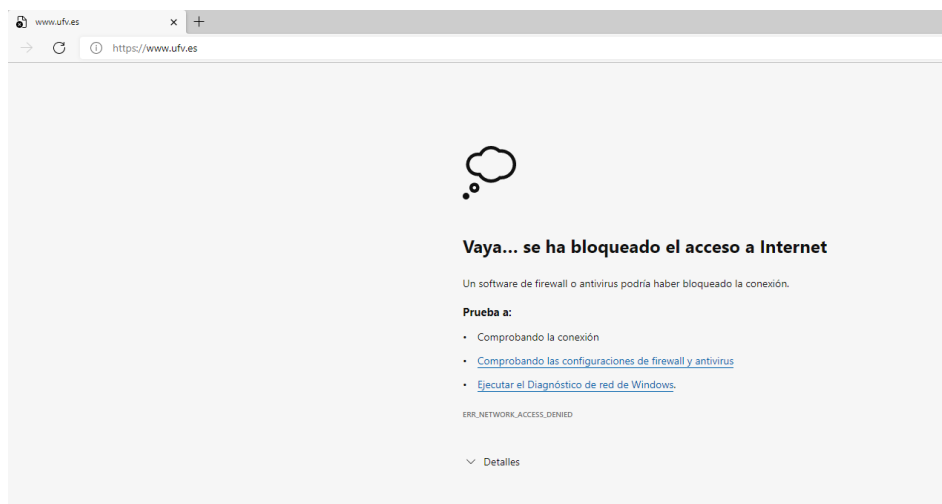


Ilustración 18 - Funcionamiento de la norma en el puerto 443

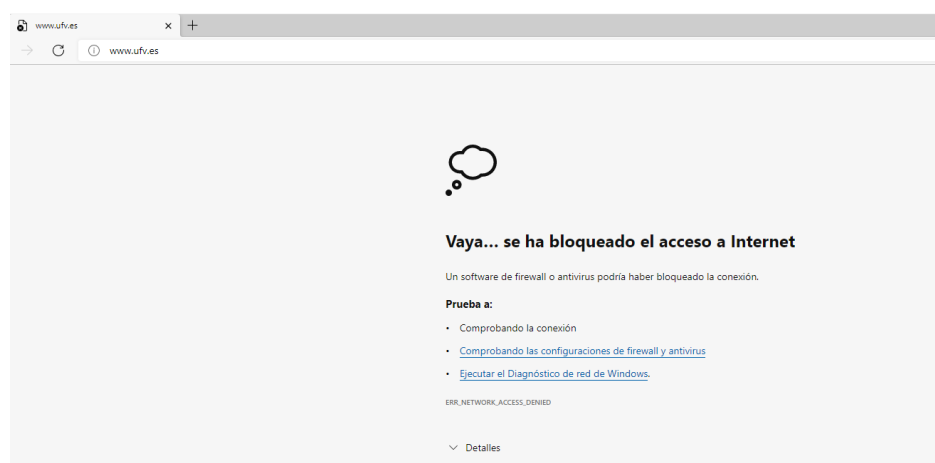


Ilustración 19 - Funcionamiento de la norma en el puerto 80

5. Crea una carpeta “CarpetadePrueba” dentro de **/home/usuario** en la máquina Kali Linux. ¿Qué tamaño tiene la carpeta? ¿Quién es el propietario de la carpeta? Crea dentro de la carpeta **/home/usuario** el fichero “ficheropruueba.txt”. Muestra que permisos tiene. Muestra pantallazos del proceso realizado. **0,5 PUNTOS.**

Para crear una carpeta dentro de “/home/usuario” se accede primero a esa ubicación y luego se usa el comando `mkdir` para crear el directorio, para comprobar los permisos y el propietario del directorio, se usa `ls -la`. Como se muestra en la siguiente imagen.

```
(kali㉿kali)-[~]
$ pwd
/home/kali

(kali㉿kali)-[~]
$ mkdir CarpetadePrueba

(kali㉿kali)-[~]
$ ls -la
total 156
drwxr-xr-x 16 kali kali 4096 Dec 17 08:19 .
drwxr-xr-x  3 root root 4096 Dec  2 01:36 ..
-rw-r--r--  1 kali kali   1 Dec  2 01:42 .bash_history
-rw-r--r--  1 kali kali  220 Dec  2 01:36 .bash_logout
-rw-r--r--  1 kali kali 5349 Dec  2 01:36 .bashrc
-rw-r--r--  1 kali kali 3526 Dec  2 01:36 .bashrc.original
drwxr-xr-x  6 kali kali 4096 Dec 16 13:33 .cache
drwxr-xr-x  2 kali kali 4096 Dec 17 08:19 CarpetadePrueba
drwxr-xr-x  9 kali kali 4096 Dec  2 01:39 .config
```

Ilustración 20 - Creación de carpeta y observación de permisos

La carpeta como se puede observar, tiene todos los permisos para el usuario que lo creó (Kali), ejecución y lectura para el grupo, y ejecución para el resto. El tamaño del directorio son 4096 bits.

Dentro del directorio /home/usuario, se procede a crear un archivo de texto mediante el comando touch y ver los permisos que tiene con ls -la.

```
(kali㉿kali)-[~]
$ touch ficheropruueba.txt

(kali㉿kali)-[~]
$ ls -la
total 156
drwxr-xr-x 16 kali kali 4096 Dec 17 08:26 .
drwxr-xr-x  3 root root 4096 Dec  2 01:36 ..
-rw-r--r--  1 kali kali   1 Dec  2 01:42 .bash_history
-rw-r--r--  1 kali kali  220 Dec  2 01:36 .bash_logout
-rw-r--r--  1 kali kali 5349 Dec  2 01:36 .bashrc
-rw-r--r--  1 kali kali 3526 Dec  2 01:36 .bashrc.original
drwxr-xr-x  6 kali kali 4096 Dec 16 13:33 .cache
drwxr-xr-x  2 kali kali 4096 Dec 17 08:26 CarpetadePrueba
drwxr-xr-x  9 kali kali 4096 Dec  2 01:39 .config
drwxr-xr-x  2 kali kali 4096 Dec  2 01:39 Desktop
-rw-r--r--  1 kali kali   55 Dec  2 01:39 .dmrc
drwxr-xr-x  2 kali kali 4096 Dec  2 01:39 Documents
drwxr-xr-x  2 kali kali 4096 Dec  2 01:39 Downloads
-rw-r--r--  1 kali kali 11759 Dec  2 01:36 .face
lrwxrwxrwx  1 kali kali   5 Dec  2 01:36 .face.icon → .face
-rw-r--r--  1 kali kali   0 Dec 17 08:26 ficheropruueba.txt
drwxr-xr-x  3 kali kali 4096 Dec  2 01:39 .gnupg
```

Ilustración 21 - Creación de fichero y observación de permisos

El fichero pertenece a Kali, y tiene permisos de escritura y lectura para el usuario propietario y lectura para el grupo y el resto.

6. **Mueve** el fichero “ficheropruueba.txt” dentro de la carpeta “Carpeta de Prueba” con comandos. Ahora **copia** el fichero a su ubicación original, manteniendo una copia en el origen por comandos. Muestra pantallazos del proceso realizado. Todo el proceso debe realizarse en la máquina Kali Linux. **0,5 PUNTOS.**

Para mover el fichero, se usa el comando mv.

```
(kali@kali)-[~]  
$ mv ficheropruueba.txt Carpeta de Prueba  
  
(kali@kali)-[~]  
$ ls Carpeta de Prueba  
ficheropruueba.txt
```

Ilustración 22 - uso de mv

Para copiar el fichero a su ubicación original, se usa el comando cp y se usa ls para mostrar que el fichero se encuentra en las dos ubicaciones.

```
(kali@kali)-[~]  
$ cp Carpeta de Prueba/ficheropruueba.txt .  
  
(kali@kali)-[~]  
$ ls Carpeta de Prueba  
ficheropruueba.txt  
  
(kali@kali)-[~]  
$ ls  
Carpeta de Prueba Desktop Documents Downloads ficheropruueba.txt Music Pictures Public Templates Videos
```

Ilustración 23 - Copia de archivo

7. Encuentra la ubicación de los siguientes ficheros: Muéstralo con pantallazos. **0,5 PUNTOS.**

- Fichero “shadow”
- Fichero “dhclient.conf”

Se usa el comando find para localizar los archivos.

```
(root@kali)-[/]  
# find / -name shadow  
find: '/run/user/1000/gvfs': Permission denied  
/etc/shadow
```

Ilustración 24 - Uso de find para localizar shadow

```
(root@kali)-[/]  
# find / -name dhclient.conf  
find: '/run/user/1000/gvfs': Permission denied  
/etc/dhcp/dhclient.conf
```

Ilustración 25 - Uso de find para localizar dhclient.conf

8. Comprime el fichero “ficheropruueba.txt” a un **tarball**. Descomprímelo después. Muestra pantallazos del proceso realizado. **0,5 PUNTOS.**

Se usa el comando tar para comprimir el archivo.

```
(root@kali)~[/home/kali/CarpetadePrueba]
# tar -cvf ficheropruueba.txt.tar.gz *
ficheropruueba.txt

(root@kali)~[/home/kali/CarpetadePrueba]
# ls
ficheropruueba.txt  ficheropruueba.txt.tar.gz
```

Ilustración 26 - Compresión de archivo

Se usa el mismo comando, pero con la flag “x” para descomprimir el archivo:

```
(root@kali)~[/home/kali/CarpetadePrueba]
# rm ficheropruueba.txt

(root@kali)~[/home/kali/CarpetadePrueba]
# ls
ficheropruueba.txt.tar.gz

(root@kali)~[/home/kali/CarpetadePrueba]
# tar -xvf ficheropruueba.txt.tar.gz
ficheropruueba.txt

(root@kali)~[/home/kali/CarpetadePrueba]
# ls
ficheropruueba.txt  ficheropruueba.txt.tar.gz

(root@kali)~[/home/kali/CarpetadePrueba]
#
```

Ilustración 27 - Descompresión del archivo

9. Establece los siguientes permisos al fichero “ficheropruueba.txt”. Muestra pantallazos del proceso realizado. **0,5 PUNTOS.**
- Lectura y ejecución para Usuario, Escritura y ejecución para Grupo, nada para el resto.
Se usa chmod con los números adecuados a los permisos para asignárselos a ficheropruueba.txt

```

(root@kali)~/CarpetadePrueba
# chmod 530 ficheropruoba.txt

(root@kali)~/CarpetadePrueba
# ls -la
total 20
drwxr-xr-x  2 kali kali  4096 Dec 17 08:39 .
drwxr-xr-x 16 kali kali  4096 Dec 17 08:38 ..
-r-x-wx---  1 kali kali    0 Dec 17 08:26 ficheropruoba.txt
-rw-r--r--  1 root root 10240 Dec 17 08:39 ficheropruoba.txt.tar.gz
  
```

Ilustración 28 - Asignación de permisos

b. 100011110

Se convierte el número binario a decimal separándolo en tres secciones y queda: 436
Se asignan los permisos correspondientes al fichero.

```

(root@kali)~/CarpetadePrueba
# chmod 436 ficheropruoba.txt

(root@kali)~/CarpetadePrueba
# ls -la
total 20
drwxr-xr-x  2 kali kali  4096 Dec 17 08:39 .
drwxr-xr-x 16 kali kali  4096 Dec 17 08:38 ..
-r---wxrw-  1 kali kali    0 Dec 17 08:26 ficheropruoba.txt
-rw-r--r--  1 root root 10240 Dec 17 08:39 ficheropruoba.txt.tar.gz
  
```

Ilustración 29 - asignación de permisos 2

c. 193

Pasamos a binario 193 y queda: 11000001. Se divide en tres secciones y queda:
601

```

(root@kali)~/CarpetadePrueba
# chmod 601 ficheropruoba.txt

(root@kali)~/CarpetadePrueba
# ls -la
total 20
drwxr-xr-x  2 kali kali  4096 Dec 17 08:39 .
drwxr-xr-x 16 kali kali  4096 Dec 17 08:38 ..
-rw-----  1 kali kali    0 Dec 17 08:26 ficheropruoba.txt
-rw-r--r--  1 root root 10240 Dec 17 08:39 ficheropruoba.txt.tar.gz
  
```

Ilustración 30 - Asignación de permisos 3

10. ¿Cómo buscarías en Shodan servidores Apache en Italia con sistema operativo Linux? Muestra pantallazos del proceso realizado. **0,5 PUNTOS.**

country:"IT" server:"apache" os:"linux VERSION"

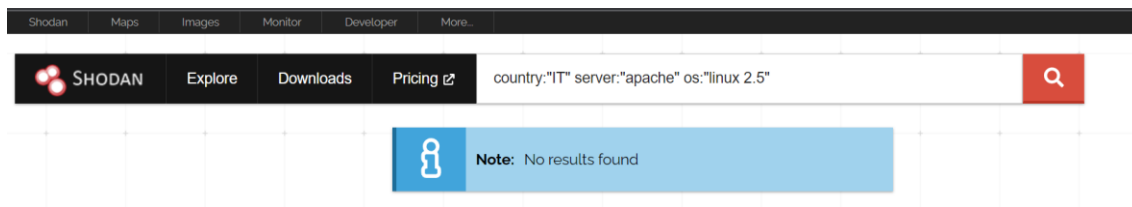


Ilustración 31 - Búsqueda en shodan

11. Utiliza algún operador o dork del buscador Bing para saber los dominios compartidos con la página web www.as.com. Muestra pantallazos del proceso realizado. **0,5 PUNTOS.**

Comparten 237 dominios (entre ellos Antena3) con la ip donde está alojada as.com. Para ver la ip de as.com se ha usado ping.

```

C:\Users\aruiz>ping as.com

Haciendo ping a as.com [199.232.198.133] con 32 bytes de datos:
Respuesta desde 199.232.198.133: bytes=32 tiempo=132ms TTL=60

Estadísticas de ping para 199.232.198.133:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 132ms, Máximo = 132ms, Media = 132ms
Control-C
^C

```

Ilustración 32 - ping para ver la ip de as.com

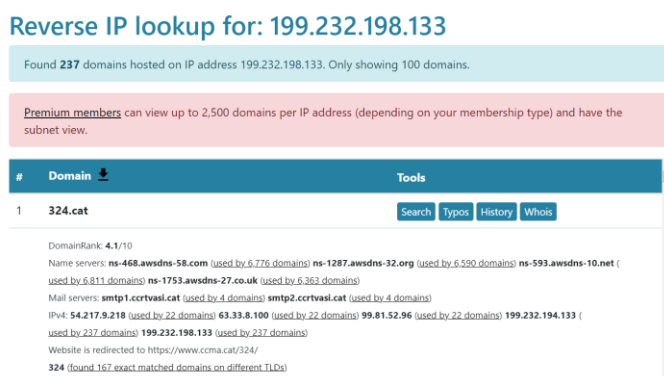


Ilustración 33 - Dominios de as.com

Examen Práctico 17 de diciembre de 2021

12. Cifrar con AES el examen y mándalo al correo electrónico del profesor con la siguiente contraseña (solamente el contenido entre las dobles comillas) “*EuLdLm17122020@”
Muestra pantallazos del proceso realizado. **0,5 PUNTOS.**