Práctica de Evaluación 6 – Seguridad Activa 1
Fecha: 16 de octubre de 2023
Resultados de aprendizaje y Criterios de evaluación que se evalúan: RA2: a, b, c

---

DIEGO ACOSTA CABRERA,2ºASIR

Práctica de Evaluación 6 – Seguridad Activa 1 (Amenazas, Ataques, SUMO, Ataque DHCP)

Descripción de la actividad

Actividad 1 – Amenazas (10p)

1.1 Amenazas **5p**

- Enumera cuales son en el año actual los principales tipos de amenazas lógicas contra un sistema informático.

Algunos de los principales tipos de amenazas lógicas que más se frecuentan a utilizar actualmente son:

1. **Malware: Esto incluye virus, gusanos y troyanos, que pueden infectar sistemas y causar daños, robo de datos o extorsión.**
2. **Phishing: Los ataques de phishing se basan en engañar a los usuarios para que revelen información confidencial, como contraseñas o información financiera, a menudo a través de correos electrónicos fraudulentos.**
3. **Ataques de fuerza bruta: Los atacantes intentan adivinar contraseñas al probar muchas combinaciones diferentes.**
4. **Inyección de código: Esto incluye ataques como la inyección SQL, donde los atacantes introducen código malicioso en aplicaciones web para robar o manipular datos.**
5. **Ataques de denegación de servicio (DDoS): Los atacantes abruman un sistema con tráfico malicioso, lo que hace que el sistema sea inaccesible para usuarios legítimos.**
6. **Vulnerabilidades de software y sistemas operativos: Los sistemas a menudo tienen vulnerabilidades que los atacantes pueden explotar para obtener acceso no autorizado.**
7. **Ransomware: Los atacantes cifran los datos de un sistema y exigen un rescate para desbloquearlos.**
8. **Ataques a aplicaciones web: Los atacantes pueden aprovechar vulnerabilidades en aplicaciones web para robar datos o tomar el control de la aplicación.**
9. **Ataques a la nube: Con el aumento de la adopción de servicios en la nube, los ataques a la infraestructura en la nube son una amenaza creciente.**

1.2 Estudio de Ataque **5p**

- Explica el funcionamiento de un ataque DDoS.

El ataque DDoS es un ataque que se trata principalmente de parar el trafico en un servidor sobrecargando el servidor o su infraestructura con solicitudes de múltiples usuarios para crear una avalancha de tráfico en la red.

Para realizar este ataque se utilizan diferentes dispositivos denominados bots o zombies que son varios ordenadores conectados a internet que han sido infectados por algún tipo de malware y que permite al atacante utilizar ese dispositivo de forma remota sin que se de cuenta el usuario del dispositivo para realizar el ataque

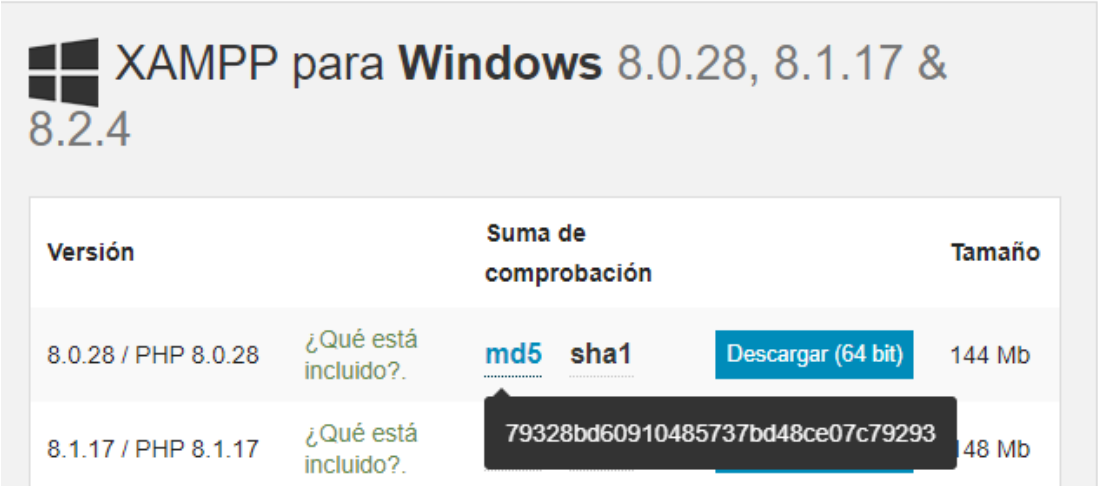
Cuando el servidor es el blanco de este ataque, cada bot envía solicitudes a la dirección IP del destino, lo que puede llegar a sobrecargar el servidor o la red y, por consiguiente, provocar una denegación de servicio al tráfico normal.

Actividad 2 – Autenticidad y Actualización de las aplicaciones informáticas **(10p)**

2.1 Origen y Autenticidad **5p**

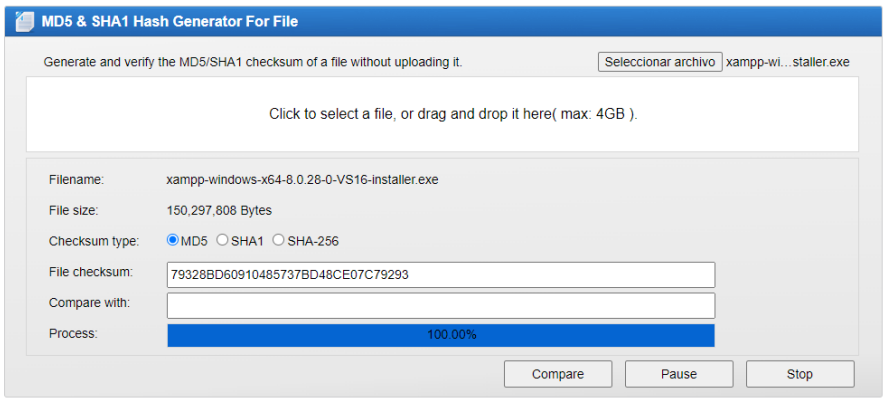
- Comprueba la autenticidad de la aplicación XAMP para Windows (Checksum). Comprueba que su huella con el md5 y sha1 coinciden con el de la página oficial para saber que el software no se ha modificado y por lo tanto es auténtico. De esta manera comprobamos que no se viola el principio de integridad, uno de los objetivos de la seguridad informática.

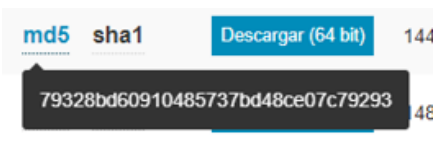
En primera instancia vamos a revisar el md5 de la pagina oficial para luego comprobar si la del archivo descargado es igual.



Ahora para comprobar que el siguiente archivo es correcto vamos a ponerlo en la siguiente página, http://onlinemd5.com/, para comprobar si el código md5 es igual

Y como podemos ver el md5 que nos da es idéntico así que no se incumpliría el principio de integridad





2.2 – Actualizaciones **5p**

- Instala la aplicación SUMO o Patch My PC, la que prefieras y describe para que se usan y que nos aporta a nivel de seguridad a nuestros equipos.

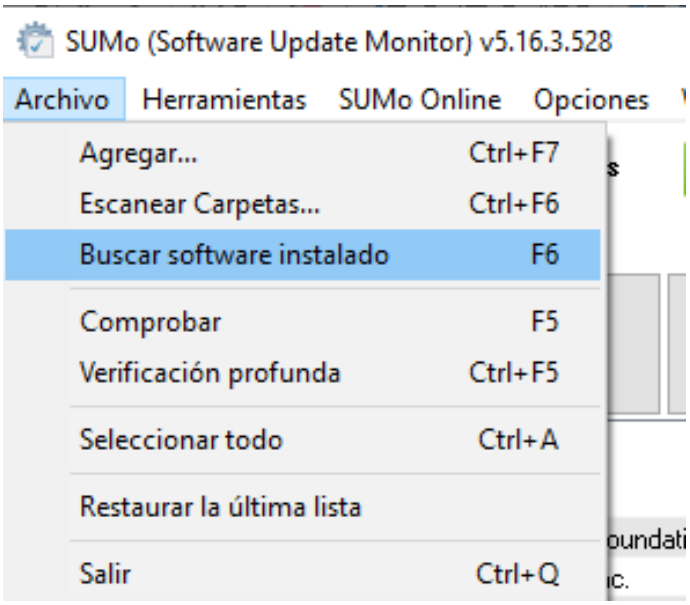
En nuestro caso hemos decidido instalar la herramienta SUMO.

Principalmente esta herramienta nos aporta conocimiento de toda aplicación de nuestro equipo que este desactualizada y con que importancia deberíamos actualizarlas, lo que en seguridad nos puede ser muy útil porque mantener actualizados los programas nos protege de que alguien que ya tenga un sploit para las versiones antiguas nos puede atacar por no tener actualizaciones que arreglen dichas brechas de seguridad.

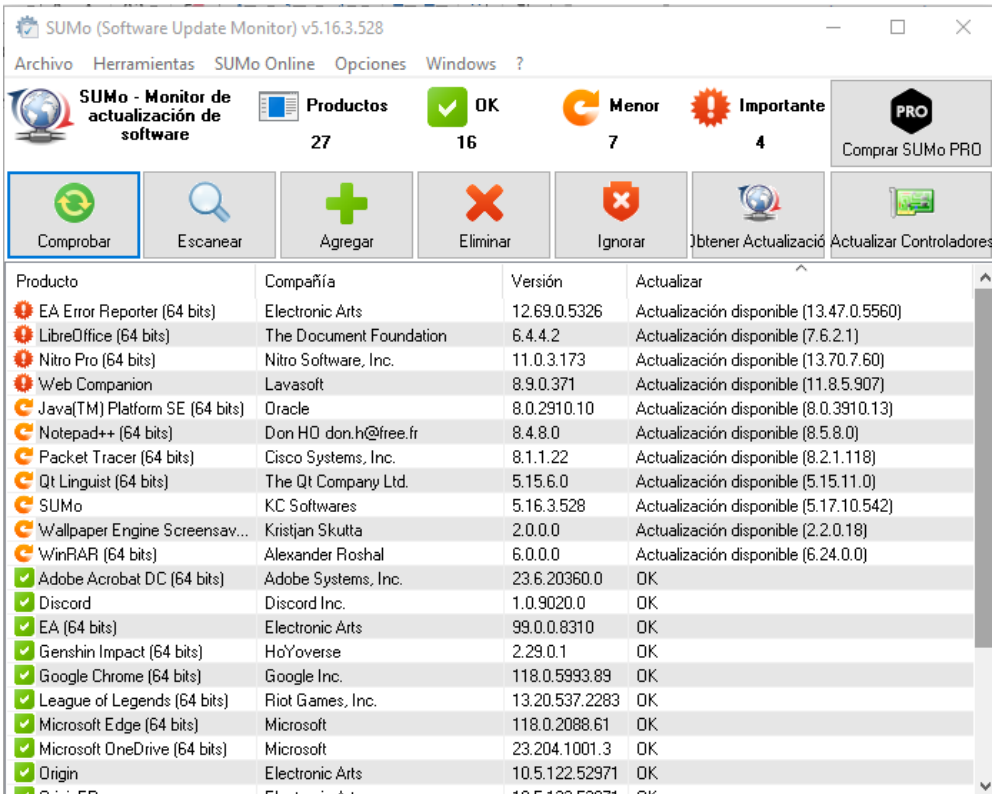
A continuación, explicare el funcionamiento básico de esta herramienta:

Ya teniendo instalado SUMO podremos escanear nuestro sofware en dos simples pasos.

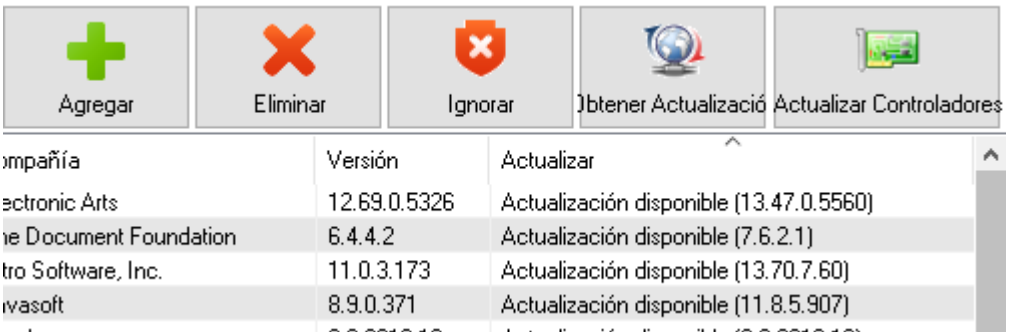
Abrimos el SUMO y nada más entrar vamos a la opción de **Archivo>>>buscar software instalado**, lo que nos hará un escaneo completo de todo el software del equipo para luego informarnos en pantalla de los resultados.



Después SUMO pasara a mostrar un resultado como el siguiente donde te saldrán todos sus programas con tres tipos de símbolos distintos dependiendo si están actualizados, hay actualizaciones menores o necesitas urgentemente una actualización.



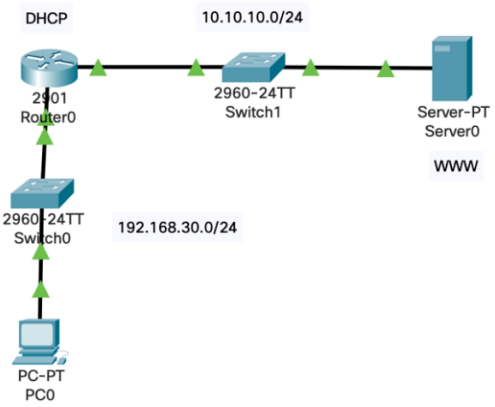
También la propia aplicación te ofrece opciones para actualizar dichas aplicaciones lo que puede ser muy útil para automatizar el proceso en caso de tener que realizarlo en muchas aplicaciones o en distintos ordenadores.



Actividad 3 – Ataque por agotamiento DHCP Packet Tracer **(10p)**

3.1 Montaje **2p**

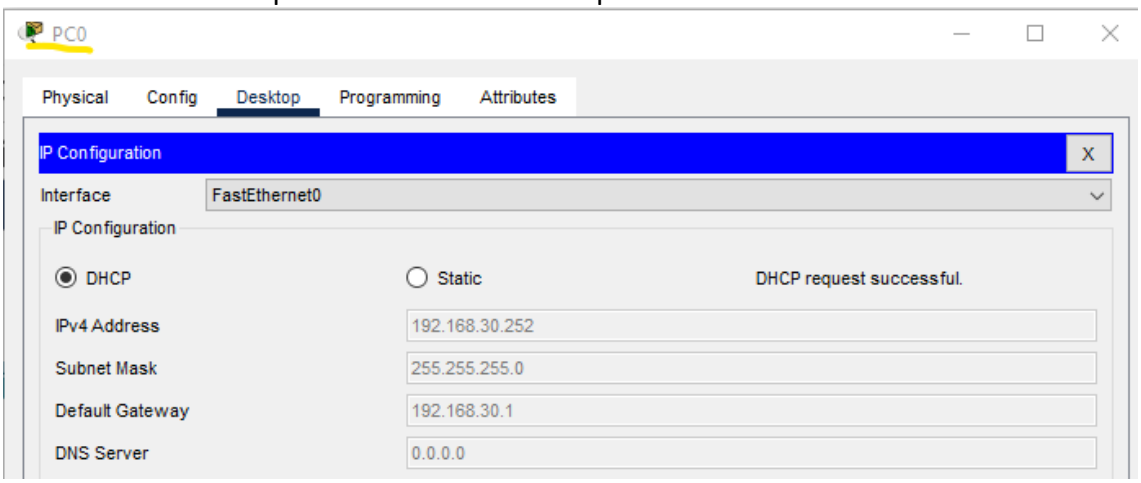
- Router realizando el servicio de DHCP + Gateway.
- En los router solo sirve ip a la red 192.168.30.0/24
- Excluimos de dar el rango de direcciones 192.168.30.1 – 192.168.30.251
- Comprobamos que el equipo recibe una ip correctamente de manera dinámica.
- Comprueba que hace ping al server, el cual tiene la ip 10.10.10.2 y puerta de enlace 10.10.10.1
- No se hace un pool en el router para que reparta en la red 10.10.10.0/24. El router solo reparte para la red 192.168.30.0/24



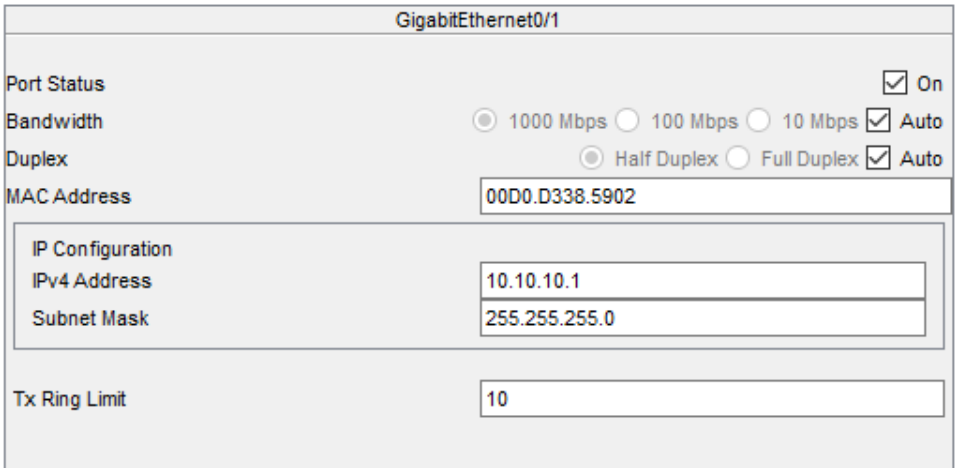
Primero realizamos un pool dhcp en la interfaz por donde este la red que necesitemos que reciba el servicio dhcp, le indicamos cual es su red y puerta de enlace y por último le decimos que no recoja IPs exclusivamente de la 1 a la 251 con el comando: "ip dhcp excluded-addres IPinicio IPfinal"

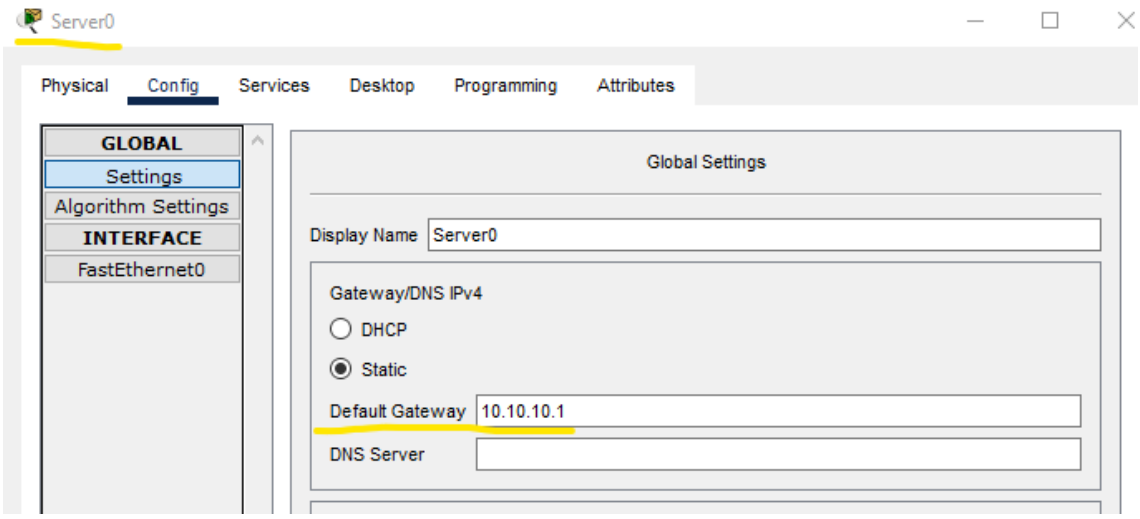
```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface Gig0/0
Router(config-if)#ip dhcp pool dhcp1
Router(dhcp-config)#network 192.168.30.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.30.1
Router(dhcp-config)#exit
Router(config)#interface Gig0/0
Router(config-if)#ip dhcp excluded-addres 192.168.30.1 192.168.30.251
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

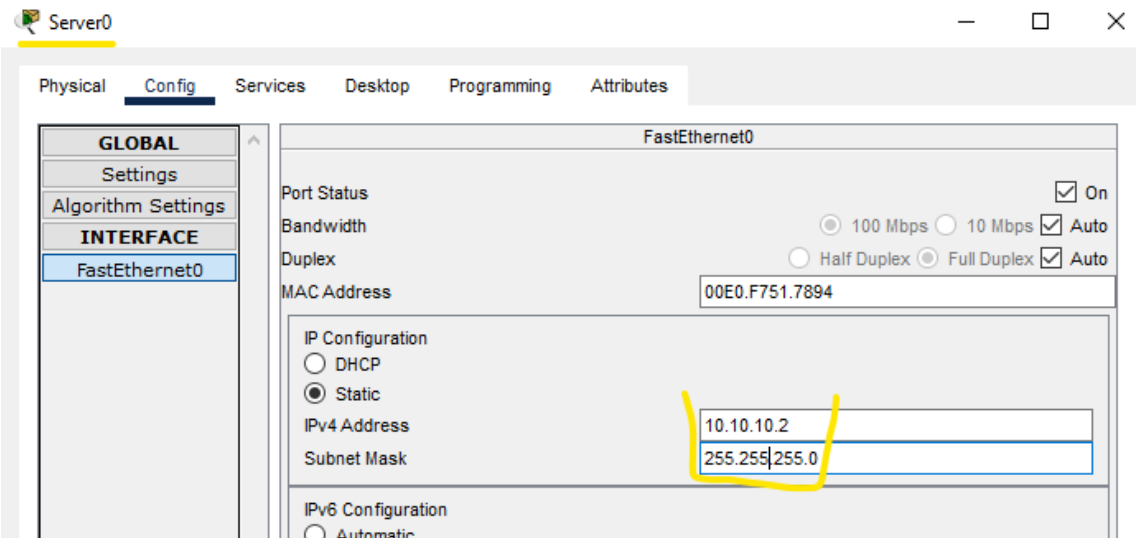
Ahora le indicamos a nuestro PC que recoja dhcp nos dará una Ip fuera del rango que nosotros indicamos que no nos debería dará ips dándonos así la 192.168.30.252.



A continuación vamos a configurar el servidor en la otra red de forma estática para comprobar si igualmente hay conexión entre ambas redes aunque una tenga o no DHCP





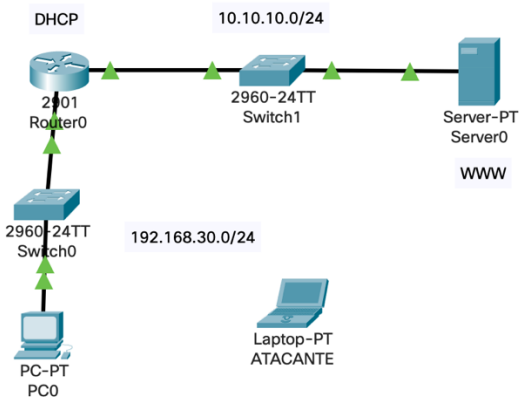


Ahora podemos ver que si hacemos un ping desde el PC nos detecta correctamente el servidor de la red sin DHCP

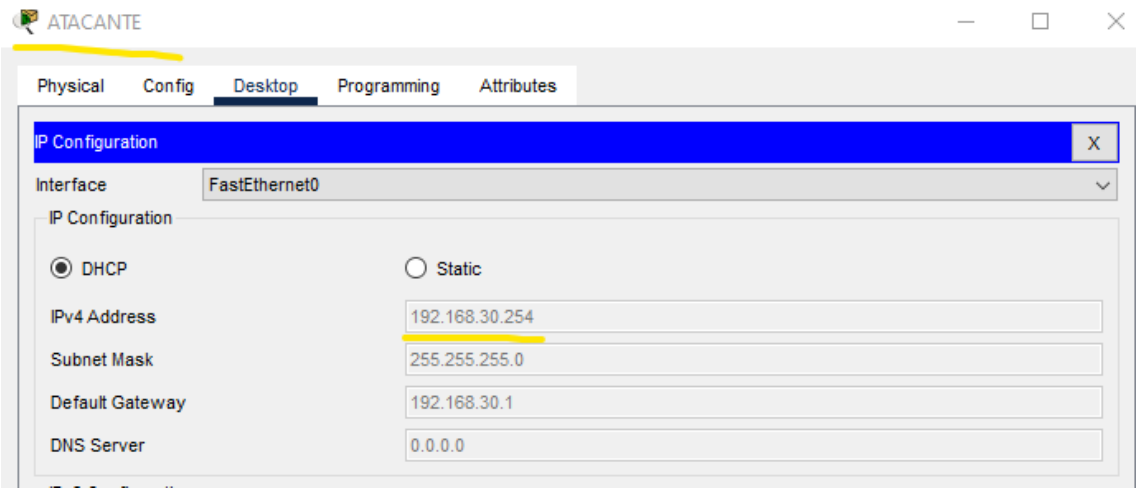
```
C:\>ping 10.10.10.2

Pinging 10.10.10.2 with 32 bytes of data:

Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127

Ping statistics for 10.10.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

3.2 Ataque por agotamiento **2p**

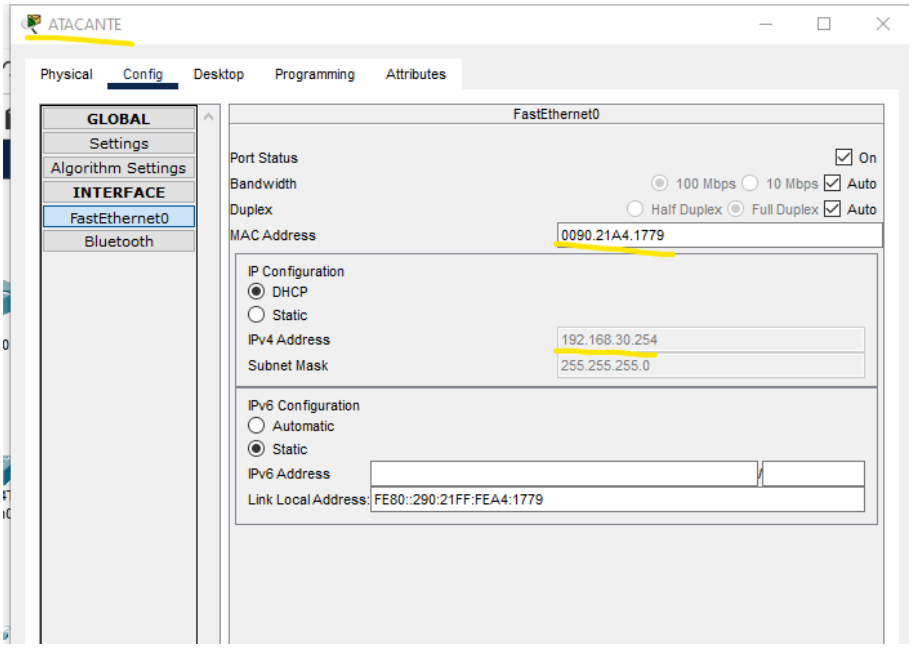
- Añadimos un portátil (El atacante) y lo conectamos a la red 192.168.30.0. Si modificamos la dirección MAC del ordenador haciendo creer que son varios equipos, agotaremos las direcciones ip que sirve el router DHCP creando una denegación de servicio en el router, dándonos este una ip fuera de nuestra red. Se realiza cambiando la mac del ordenador en la interfaz gráfica de packet tracer y renovando la ip pasando de estático a dinámico, veremos que nos da otra ip….

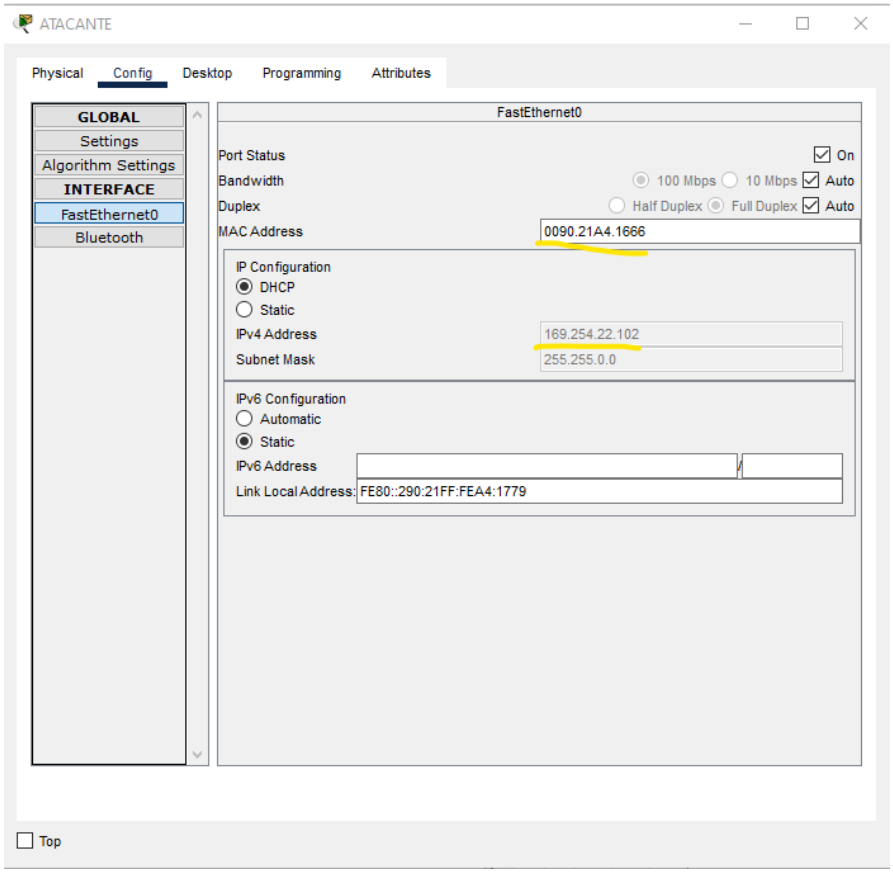


Conectamos el portátil atacante y entra en el DHCP

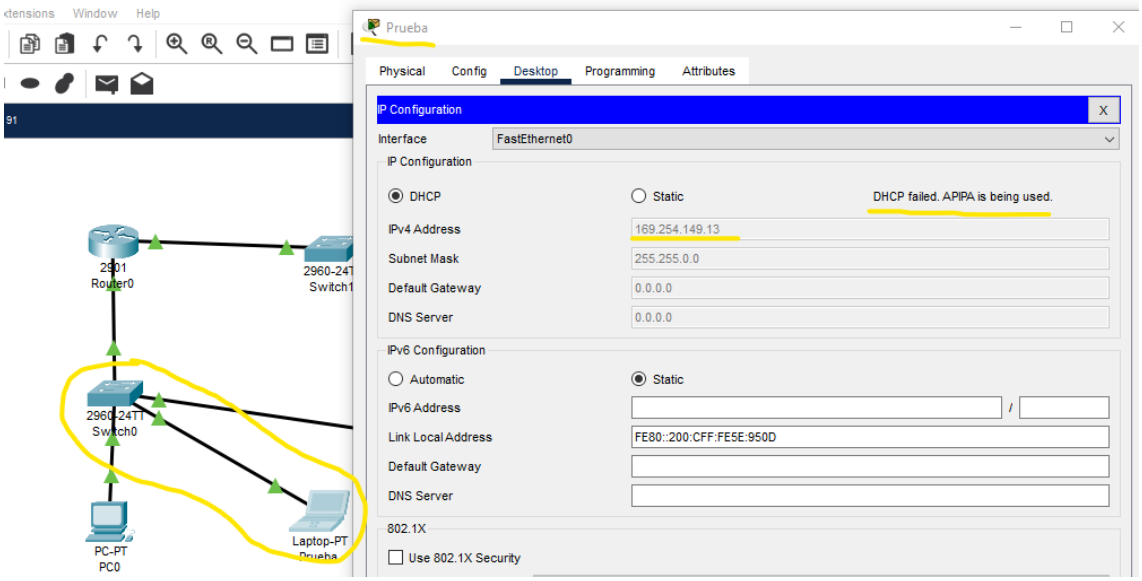


Ahora para sobrecargar la red cambiaremos nuestra MAC y veremos que nos empieza a dar IPs fuera del rango estipulado.



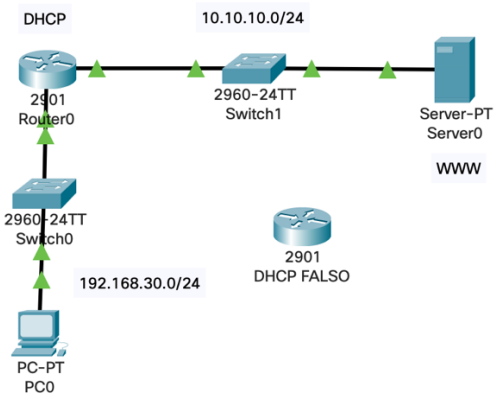


Para comprobar que si esta caída la red conectamos otro equipo cliente donde efectivamente se puede ver que da error el DHCP y nos da IPs fuera del rango estipulado.

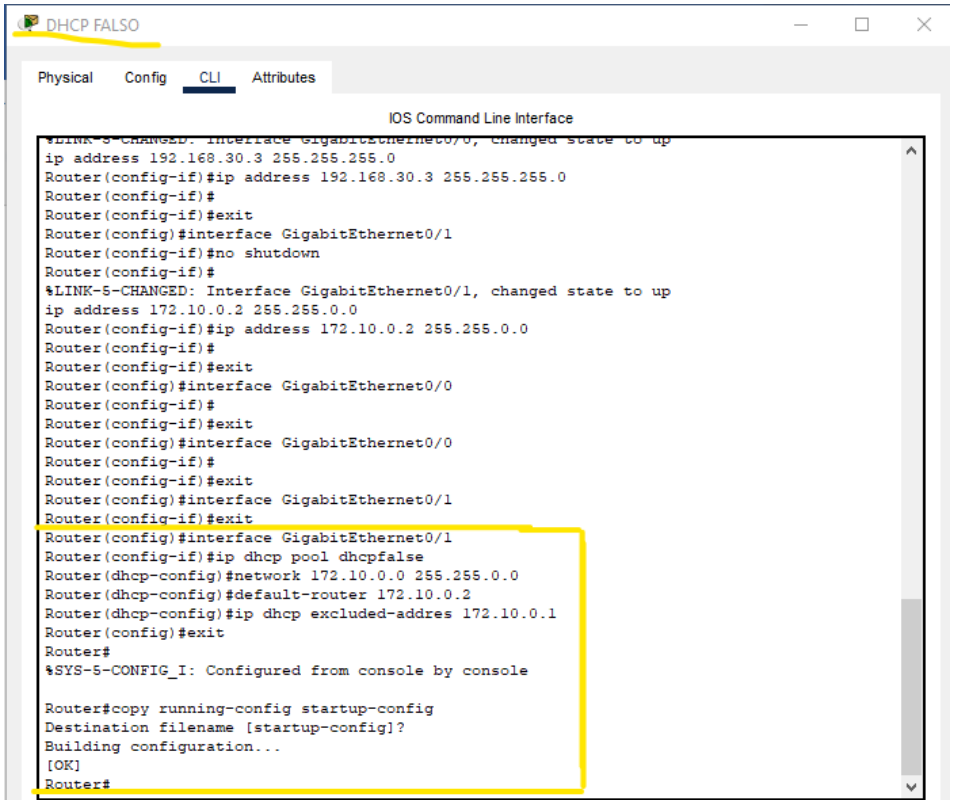


3.3 DHCP falso y damos una ip a la víctima **2p**

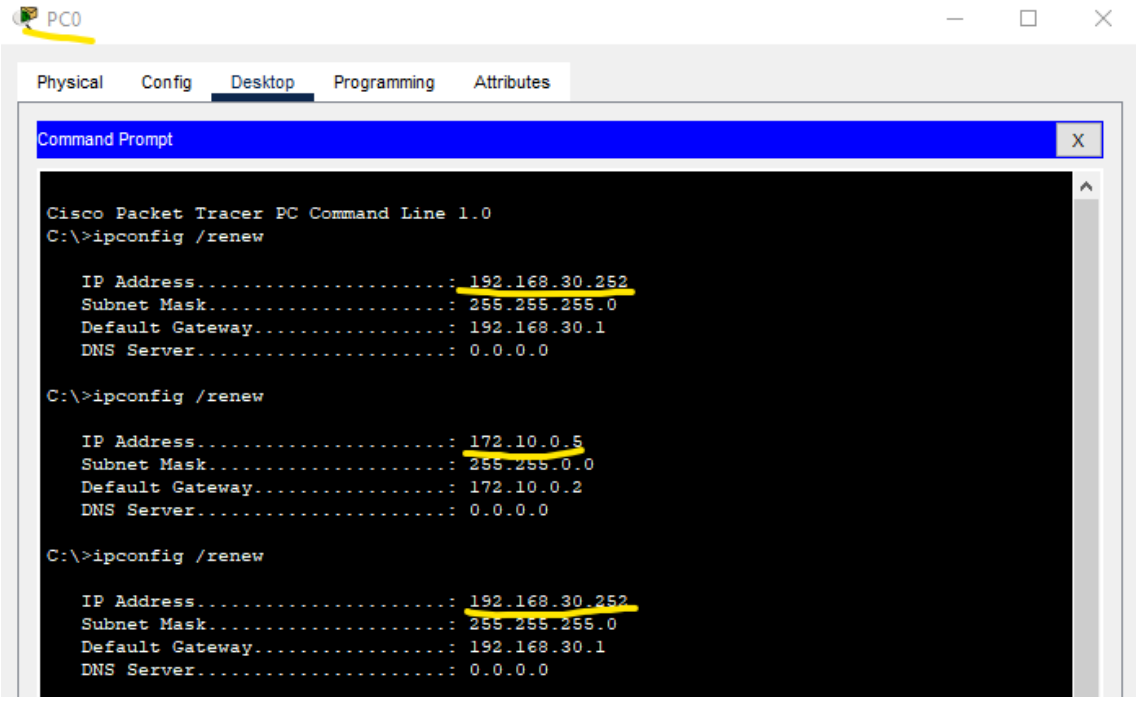
- Creo un router FALSO que va a repartir direcciones ip en nuestra red 192.168.30.0/24. En una de sus interfaces tendrá una ip LIBRE perteneciente a nuestra red, y en la otra una dirección de red de clase B, 172.10.0.0/16. Esta interfaz con la red del farsante, es la que conectaremos al switch de nuestra red. Configuramos en el router el servicio de DHCP para que excluya la dirección 172.10.0.1 y que reparta el ips de esta red 172.10.0.0/16. Recuerda que esta interfaz es la que conecto al switch de mi red. Probamos con el equipo de mi red a hacer ipconfig /renew para comprobar como en ocasiones nos da una ip del router legal y en otras un ip del router ilegal.



Con el router DHCP falso ya creado configuraremos para que la interfaz Gig0/1 tenga la Ip de clase B y excluya la 172.10.0.1.



Al conectar este router con el DHCP configurado al switch podremos ver que si renovamos la Ip del equipo cliente este ira variando entre las IPs de un DHCP u otro



3.4 DHCP Snooping **2p**

Usando la topología que queda del ejercicio 3, investiga que es el DHCP Snooping y añádelo a la arquitectura de red. Documenta todo el proceso y explica su funcionamiento.

Para esto dentro del switch activamos el DHCP SNOOPING con el comando: "ip dhcp snooping"

```
Switch#sh ip dhcp snooping
Switch DHCP snooping is disabled
DHCP snooping is configured on following VLANs:
none
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
------------------------   -------    ----------------
Switch#
```

```
Switch(config)#ip dhcp snooping
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
none
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
------------------------   -------    ----------------
Switch#
```

Para que este haga efecto deberemos indicarle que puertos son confiables para dar las IPs al servidor lo que hará que solo nos llegue IP desde estos puertos especificado en vez de darnos desde ambos DHCP

```
Switch(config)#interface Fa0/1
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
GigabitEthernet0/1         yes        unlimited
FastEthernet0/1            yes        unlimited
Switch#
```

Ahora si vamos al equipo cliente vemos que ya no nos da IP del Router DHCP falso sino que solo llegan de la red original

```
C:\>ipconfig /renew

   IP Address......................: 192.168.30.252
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 192.168.30.1
   DNS Server......................: 0.0.0.0

C:\>ipconfig /renew

   IP Address......................: 192.168.30.252
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 192.168.30.1
   DNS Server......................: 0.0.0.0

C:\>ipconfig /renew

   IP Address......................: 192.168.30.252
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 192.168.30.1
   DNS Server......................: 0.0.0.0

C:\>ipconfig /renew

   IP Address......................: 192.168.30.252
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 192.168.30.1
   DNS Server......................: 0.0.0.0

C:\>ipconfig /renew

   IP Address......................: 192.168.30.252
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 192.168.30.1
   DNS Server......................: 0.0.0.0

C:\>
```

3.5 ¿En qué nos ayuda el DHCP Snooping a evitar ataques MITM? **2p**

El DHCP Snooping ayuda a evitar ataques MITM de las siguientes maneras:

1. **Filtra tráfico DHCP malicioso**: Controla y permite solo mensajes DHCP legítimos, evitando paquetes falsos que asignen direcciones IP incorrectas o comprometan la red.
2. **Rastrea asociaciones IP-MAC**: DHCP Snooping mantiene una tabla de asociaciones IP y MAC de los dispositivos en la red. Esto ayuda a asegurarse de que un dispositivo en particular reciba la dirección IP correcta y evita que un atacante pueda asignar una dirección IP falsa a un dispositivo.
3. **Previene ARP Spoofing**: Integra medidas de seguridad, como Dynamic ARP Inspection, para verificar y controlar las respuestas ARP como mitigar los ataques de envenenamiento, evitando ataques comunes en MITM.

NOTA: Explica que se hace en cada una de estas actividades. Cada fallo descuenta **0,5p** en la actividad. Se penaliza por una mala realización del informe.