

Nombre del alumno:

Ignacio Ivan Sanchez Pantoja

Número de matrícula:

18108365

Nombre del profesor:

Israel Alejandro Herrera Araiza

Nombre del curso:

Controles Criptográficos De Seguridad

Actividad:

Practica 3 Configuración del modo de túneles VPN.

Fecha:

02/10/2024



Introducción:

La seguridad de la información es un aspecto crucial en el ámbito de las redes y la comunicación de datos. En esta práctica de laboratorio, se enfoca en la implementación de mecanismos de seguridad que protejan la integridad y confidencialidad de la información, con énfasis en el uso de túneles VPN a través del protocolo IPSEC (Internet Protocol Security) y la configuración de políticas de cifrado en dispositivos de red. IPSEC es ampliamente utilizado para garantizar que los datos transmitidos a través de redes inseguras, como Internet, lleguen a su destino sin ser alterados o interceptados por agentes malintencionados.

El laboratorio también profundiza en la captura de datos no cifrados transmitidos mediante el protocolo FTP (File Transfer Protocol), demostrando las vulnerabilidades que existen cuando los datos viajan en texto plano, lo que los hace susceptibles a ataques de "sniffing". A partir de esta problemática, se muestra cómo el cifrado con IPSEC, en modo ESP (Encapsulating Security Payload), protege el tráfico de red encapsulando los paquetes y evitando su captura por herramientas de monitoreo como sniffers.

Además, se exploran herramientas de cifrado de datos como GnuPG (GNU Privacy Guard), las cuales son clave para garantizar la privacidad en la transmisión de información sensible. GnuPG utiliza criptografía de clave pública para encriptar y firmar digitalmente archivos y mensajes, asegurando que solo los destinatarios previstos puedan acceder a ellos y garantizando la autenticidad e integridad del contenido.

En conjunto, la práctica busca proporcionar un enfoque integral sobre las mejores prácticas de seguridad en redes, abarcando tanto la protección del tráfico de red mediante IPSEC como la seguridad en la transmisión de archivos y mensajes mediante GnuPG. Esto pone de relieve la importancia de adoptar medidas de seguridad avanzadas en el manejo de la información, especialmente en un entorno donde las amenazas cibernéticas son cada vez más sofisticadas.

PT Activity: 00:00:19

Packet Tracer: configuración del modo de transporte de VPN

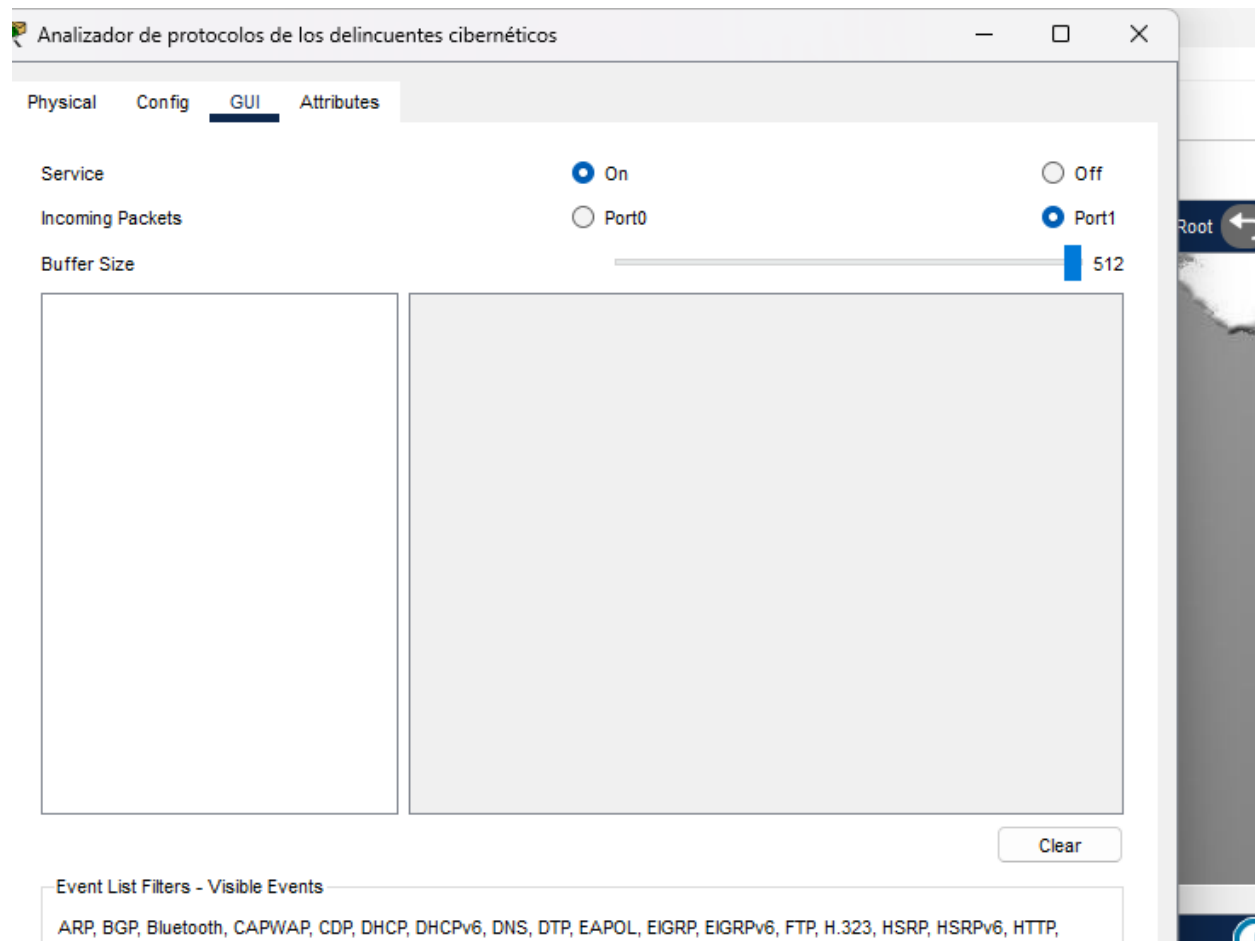
Tabla de direccionamiento

Dispositivo	Dirección IP privada	Dirección IP pública	Máscara de subred	Sitio
Servidor Private_FTP	10.44.2.254	N/D	255.255.255.0	Gotham Healthcare Branch
Servidor Public_FTP	10.44.2.253	209.165.201.20	255.255.255.0	Gotham Healthcare Branch
Branch_Router	N/D	209.165.201.19	255.255.255.248	Gotham Healthcare Branch
Computadora de Phil	10.44.0.2	N/D	255.255.255.0	Metropolis Bank HQ

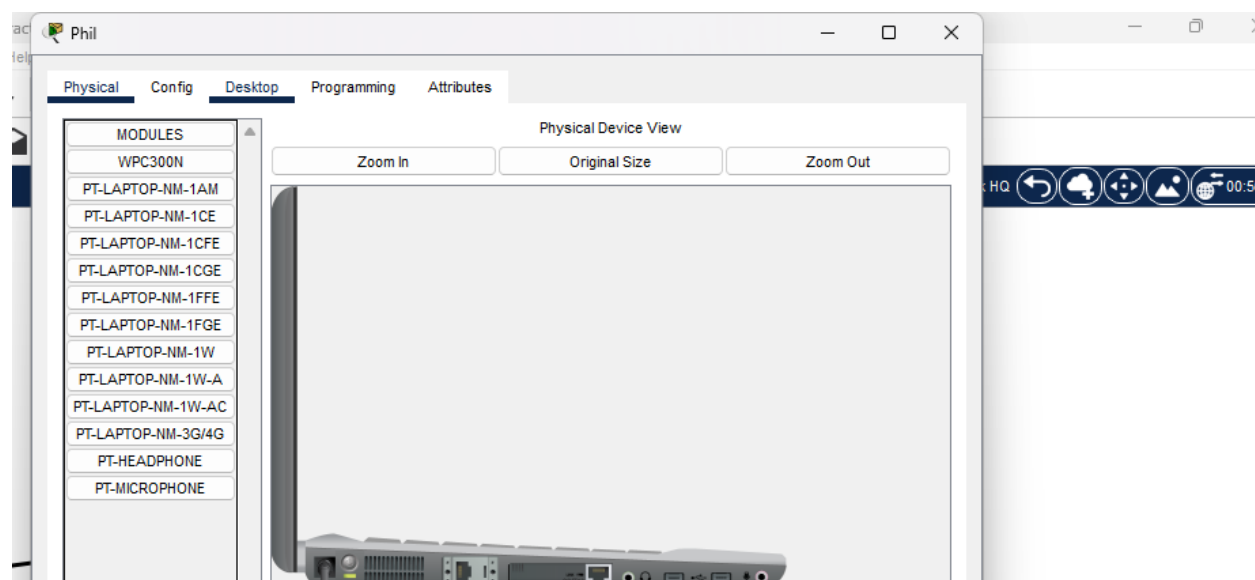
Objetivos

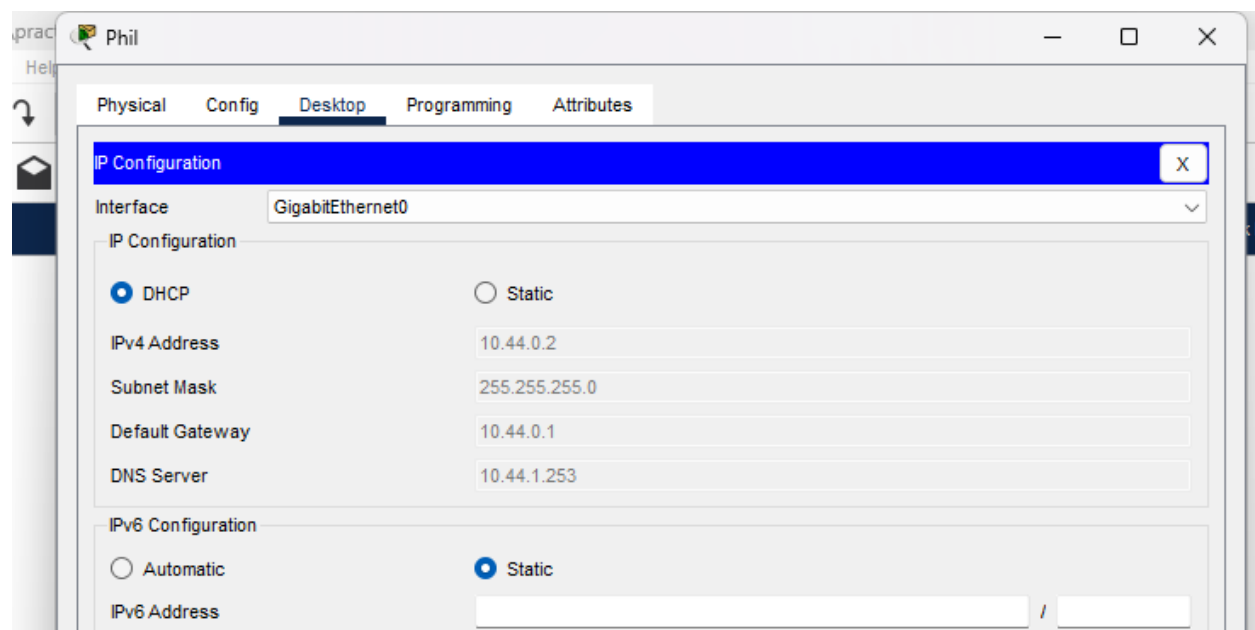
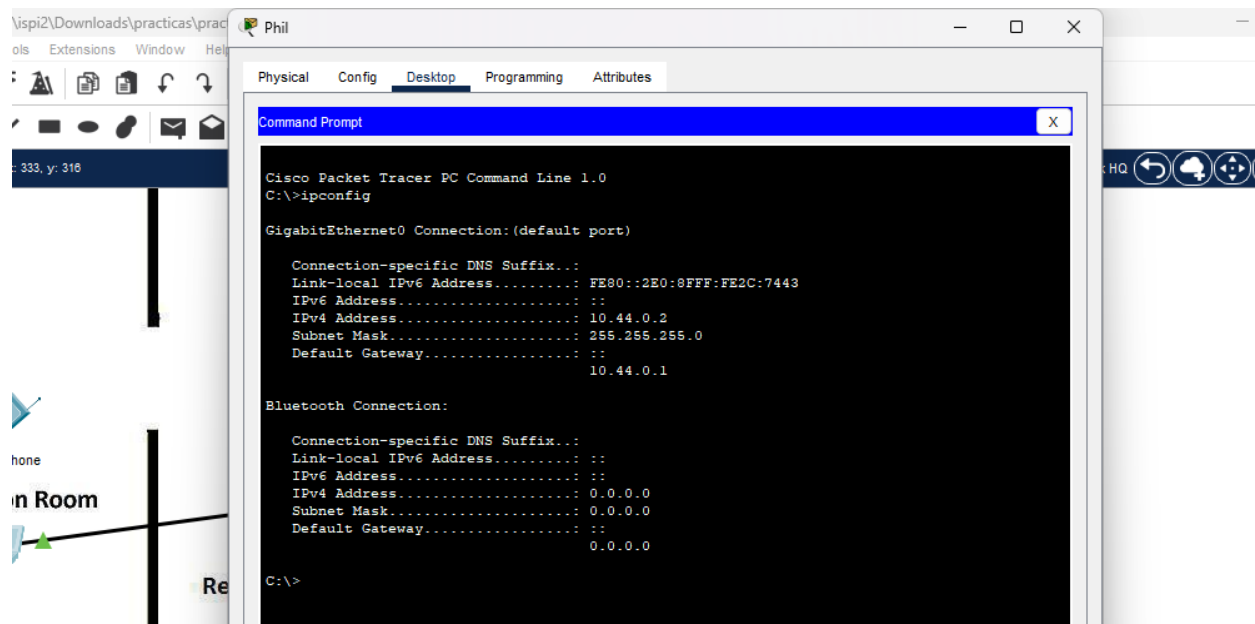
- Parte 1: enviar tráfico de FTP no cifrado
- Parte 2: configurar el cliente de VPN en Metropolis
- Parte 3: enviar tráfico de FTP cifrado

Lo primero que haremos como ya es recurrente es acudir al sniffer de red de los actores de amenaza y limpiar las entradas previas en este si es que hay alguna, como podemos observar en este caso no es así



Ahora como se nos demanda vamos a la computadora de phill configuraremos la dirección ip de la computadora por medio del servidor DHCP:





Ahora con la dirección IP accederemos al servidor FTP de Gotham:

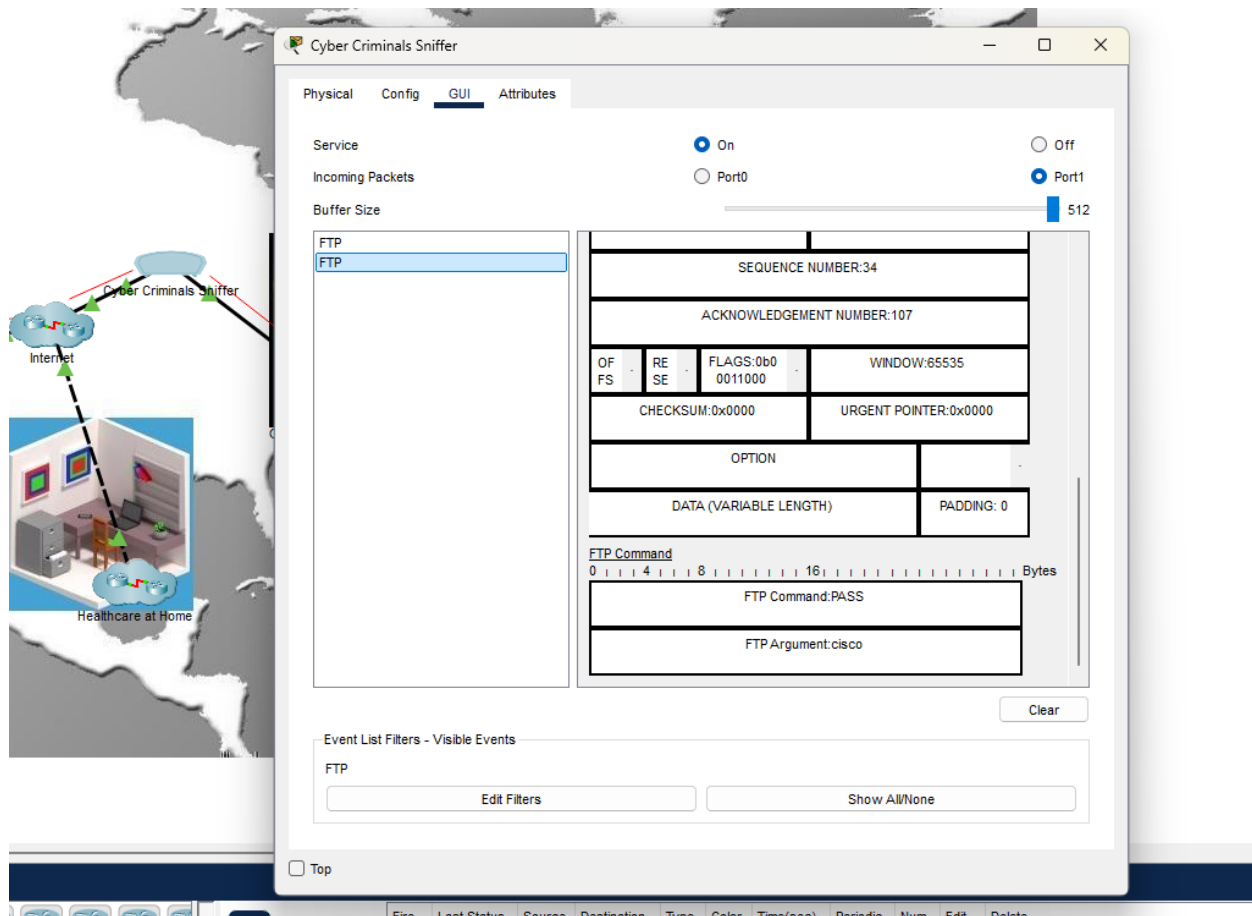
```
C:\>ftp 209.165.201.20
Trying to connect...209.165.201.20
Connected to 209.165.201.20
220- Welcome to PT Ftp server
Username:sco

%Error ftp://209.165.201.20/ (No such Account)
332- Need account for login

C:\>ftp 209.165.201.20
Trying to connect...209.165.201.20
Connected to 209.165.201.20
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

☐ Top

Las credenciales son cisco y cisco, teóricamente al los datos no viajar en ningún vpn o estar cifrados podremos ver las credenciales en texto plano, para comprobarlo iremos al sniffer de red:



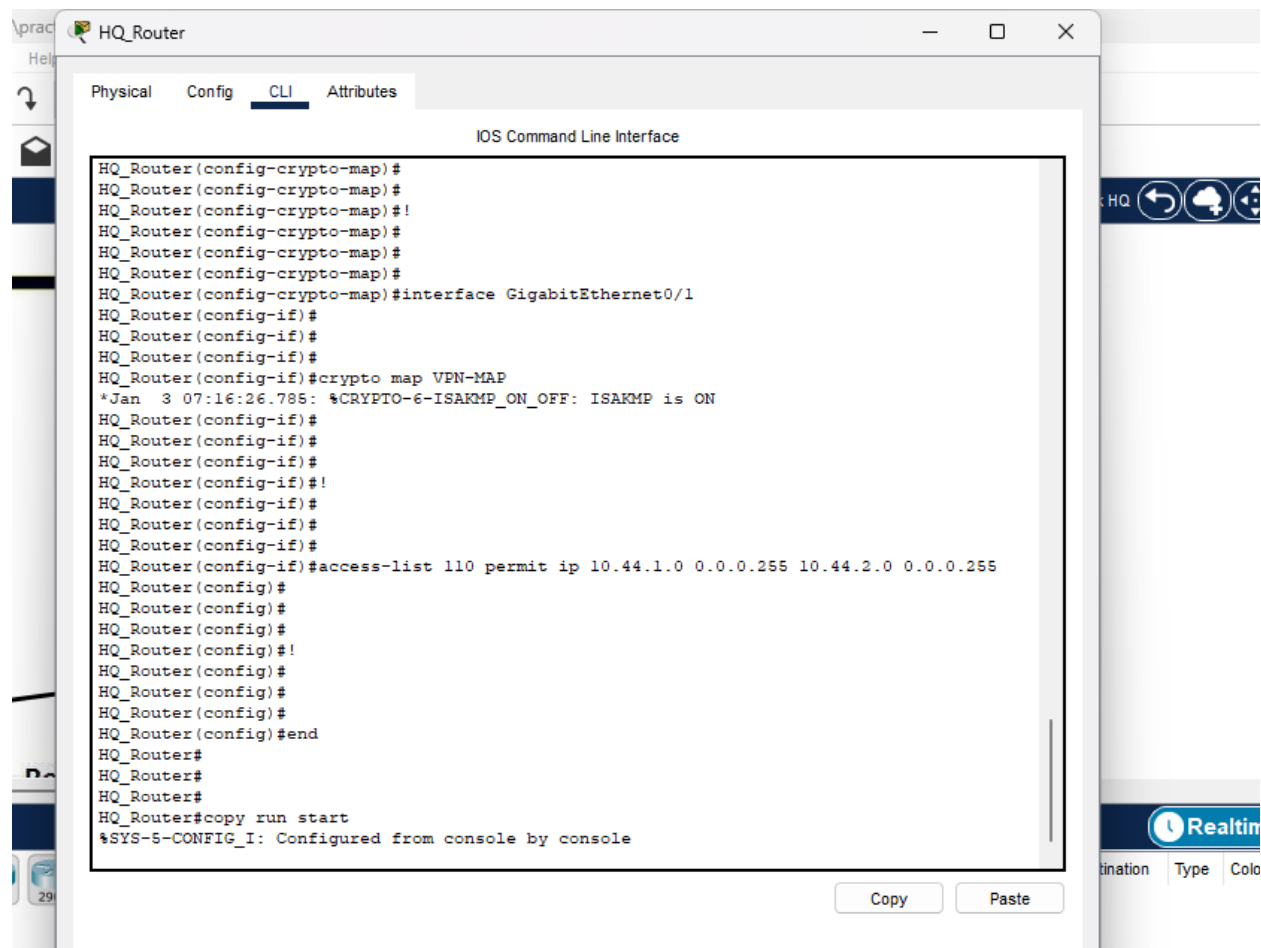
como podemos ver los credenciales ftp se capturaron ya que están en texto plano, esto es una grave amenaza para la confidencialidad de los datos, ahora bien, debemos crear un túnel VPN usando IPSEC punto a punto como se había discutido en las anteriores prácticas, IPSEC admite una serie de configuraciones para su funcionamiento, en este caso y explorando las configuraciones proporcionadas en el script se opta por utilizar el modo ESP.

IPSEC sin hacer uso de GRE puede ser configurado o generalmente es configurado para realizar conexiones punto a punto al generar una conexión punto a punto, sin embargo, una complicación del uso de IPSEC sin GRE es que no se transmitirán paquetes pertenecientes a protocolos de enrutamiento como pueden ser OSPF y EIGRP, a continuación desglosemos el script que se nos blinda por parte de la practica:

1. **enable:** Entra en el modo privilegiado del dispositivo Cisco.
2. **configure terminal:** Entra en el modo de configuración global para realizar cambios en la configuración del dispositivo.
3. **crypto isakmp policy 10:** Crea o selecciona una política ISAKMP (Internet Security Association and Key Management Protocol) con el número de prioridad 10.
4. **encr aes 256:** Especifica el algoritmo de cifrado AES con una clave de 256 bits para la política ISAKMP.

5. **authentication pre-share**: Define el método de autenticación como precompartido (pre-shared key).
6. **group 5**: Selecciona el grupo de Diffie-Hellman 5 para el intercambio de claves, que proporciona un nivel de seguridad específico.
7. **!**: Indica el final de una sección de configuración.
8. **crypto isakmp key vpnpass address 209.165.201.19**: Define la clave precompartida (vpnpass) para el peer con la dirección IP 209.165.201.19 (es decir estamos utilizando el modo IKE de IPSEC).
9. **!**: Indica el final de una sección de configuración.
10. **crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac**: Crea un conjunto de transformación IPsec llamado VPN-SET que usa ESP (Encapsulating Security Payload) con cifrado AES y autenticación HMAC-SHA una mejor implementación en comparación con la anterior practica al hacer uso de HMAC-MD5-96.
11. **!**: Indica el final de una sección de configuración.
12. **crypto map VPN-MAP 10 ipsec-isakmp**: Crea una entrada en el mapa criptográfico VPN-MAP con el número de secuencia 10, utilizando IPsec con ISAKMP.
13. **description VPN connection to Branch_Router**: Añade una descripción a esta entrada del mapa criptográfico.
14. **set peer 209.165.201.19**: Especifica el peer VPN con la dirección IP 209.165.201.19.
15. **set transform-set VPN-SET**: Asigna el conjunto de transformación VPN-SET a esta entrada del mapa criptográfico.
16. **match address 110**: Asocia esta entrada del mapa criptográfico con la lista de acceso 110.
17. **!**: Indica el final de una sección de configuración.
18. **interface GigabitEthernet0/1**: Entra en el modo de configuración para la interfaz GigabitEthernet0/1.
19. **crypto map VPN-MAP**: Aplica el mapa criptográfico VPN-MAP a la interfaz GigabitEthernet0/1.
20. **!**: Indica el final de una sección de configuración.
21. **access-list 110 permit ip 10.44.1.0 0.0.0.255 10.44.2.0 0.0.0.255**: Crea una lista de acceso (ACL) 110 que permite el tráfico IP entre las subredes 10.44.1.0/24 y 10.44.2.0/24.
22. **!**: Indica el final de una sección de configuración.
23. **end**: Sale del modo de configuración global.
24. **copy run start**: Guarda la configuración actual en la configuración de inicio para que persista después de un reinicio.

Una vez entendido el funcionamiento de este script iremos a ejecutarlo en el router HQ_Router como se indica en la practica:

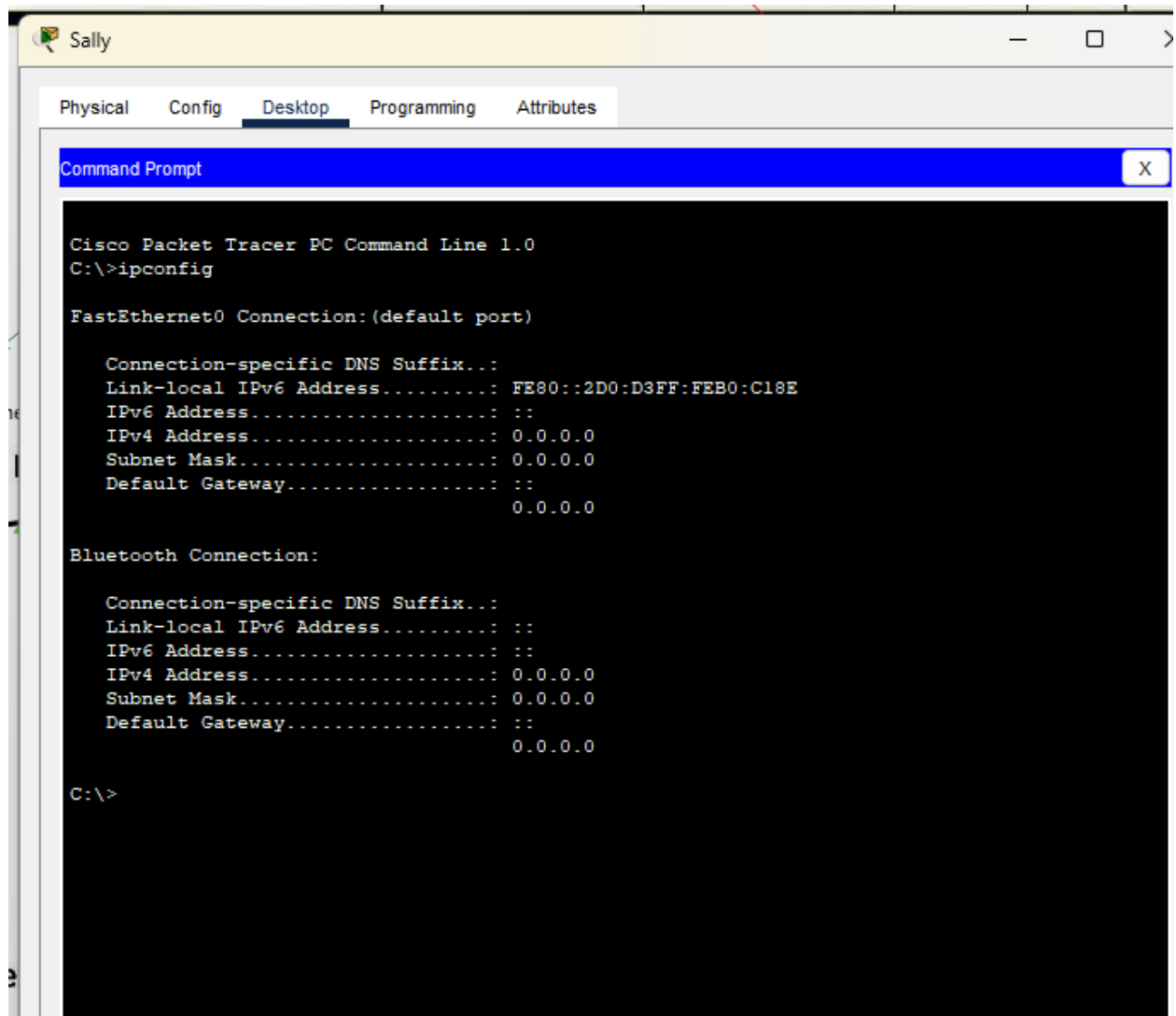


The screenshot shows a window titled 'HQ_Router' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The interface shows a series of commands being pasted into the CLI, followed by a confirmation message and a 'Copy' button.

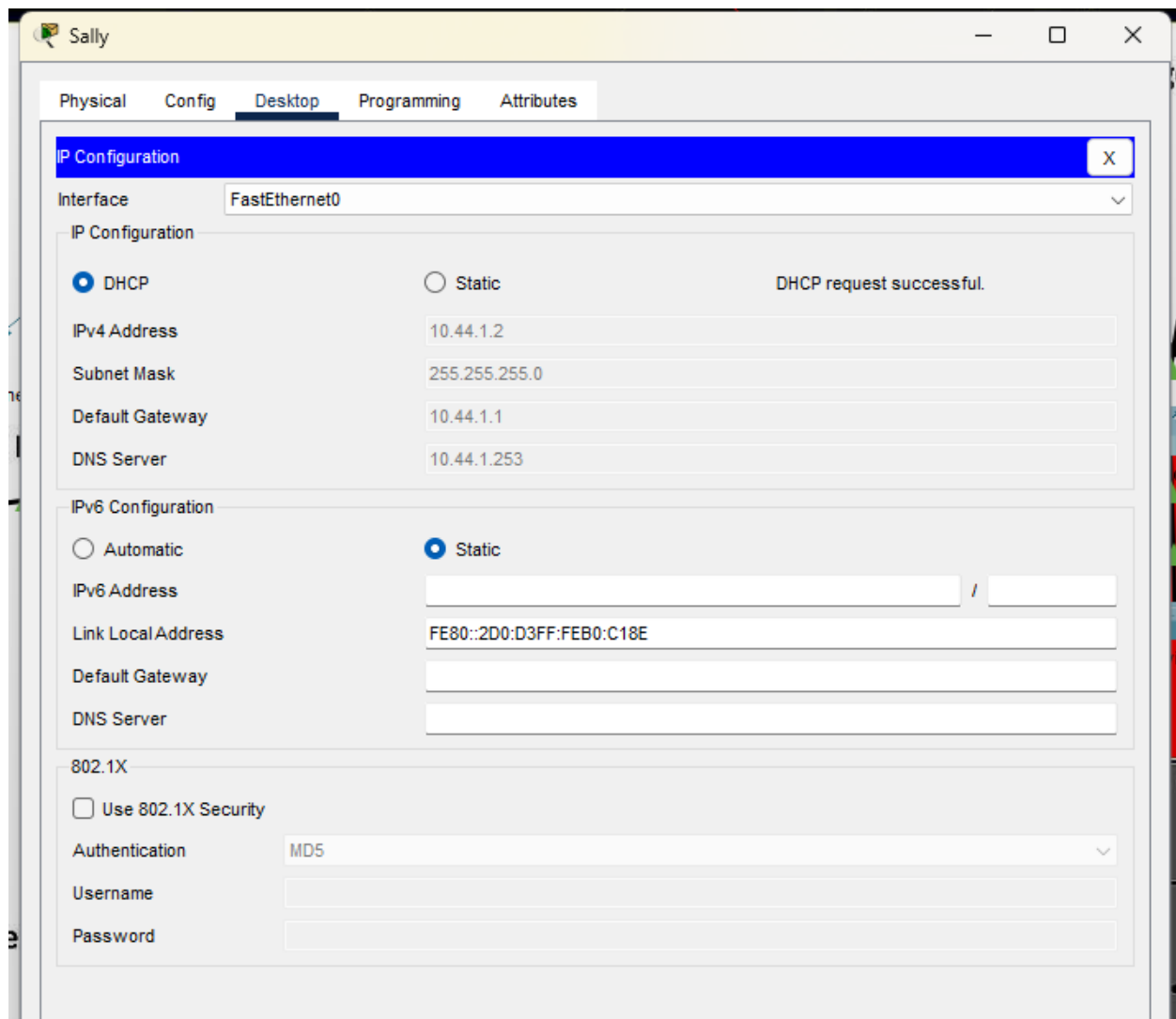
```
HQ_Router(config-crypto-map)#
HQ_Router(config-crypto-map)#
HQ_Router(config-crypto-map)#!
HQ_Router(config-crypto-map)#
HQ_Router(config-crypto-map)#
HQ_Router(config-crypto-map)#
HQ_Router(config-crypto-map)#interface GigabitEthernet0/1
HQ_Router(config-if)#
HQ_Router(config-if)#
HQ_Router(config-if)#
HQ_Router(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
HQ_Router(config-if)#
HQ_Router(config-if)#
HQ_Router(config-if)#
HQ_Router(config-if)#!
HQ_Router(config-if)#
HQ_Router(config-if)#
HQ_Router(config-if)#access-list 110 permit ip 10.44.1.0 0.0.0.255 10.44.2.0 0.0.0.255
HQ_Router(config)#
HQ_Router(config)#
HQ_Router(config)#
HQ_Router(config)#!
HQ_Router(config)#
HQ_Router(config)#
HQ_Router(config)#
HQ_Router(config)#end
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#copy run start
%SYS-5-CONFIG_I: Configured from console by console
```

Copy Paste

Una vez cargado el script de configuracion del router es necesario acceder a la computadora de Selly, para ello primero nos aseguraremos de que esta tenga una direccion ip y no una direccion APIPA que asigne automaticamente el SO:



Configuramos la dirección ip de Sally utilizando un servidor DHCP:



Ahora conectamos a Sally al servidor ftp de Gotham:

```

C:\>
C:\>ftp 10.44.2.254
Trying to connect...10.44.2.254
Connected to 10.44.2.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>put FTPupload.txt

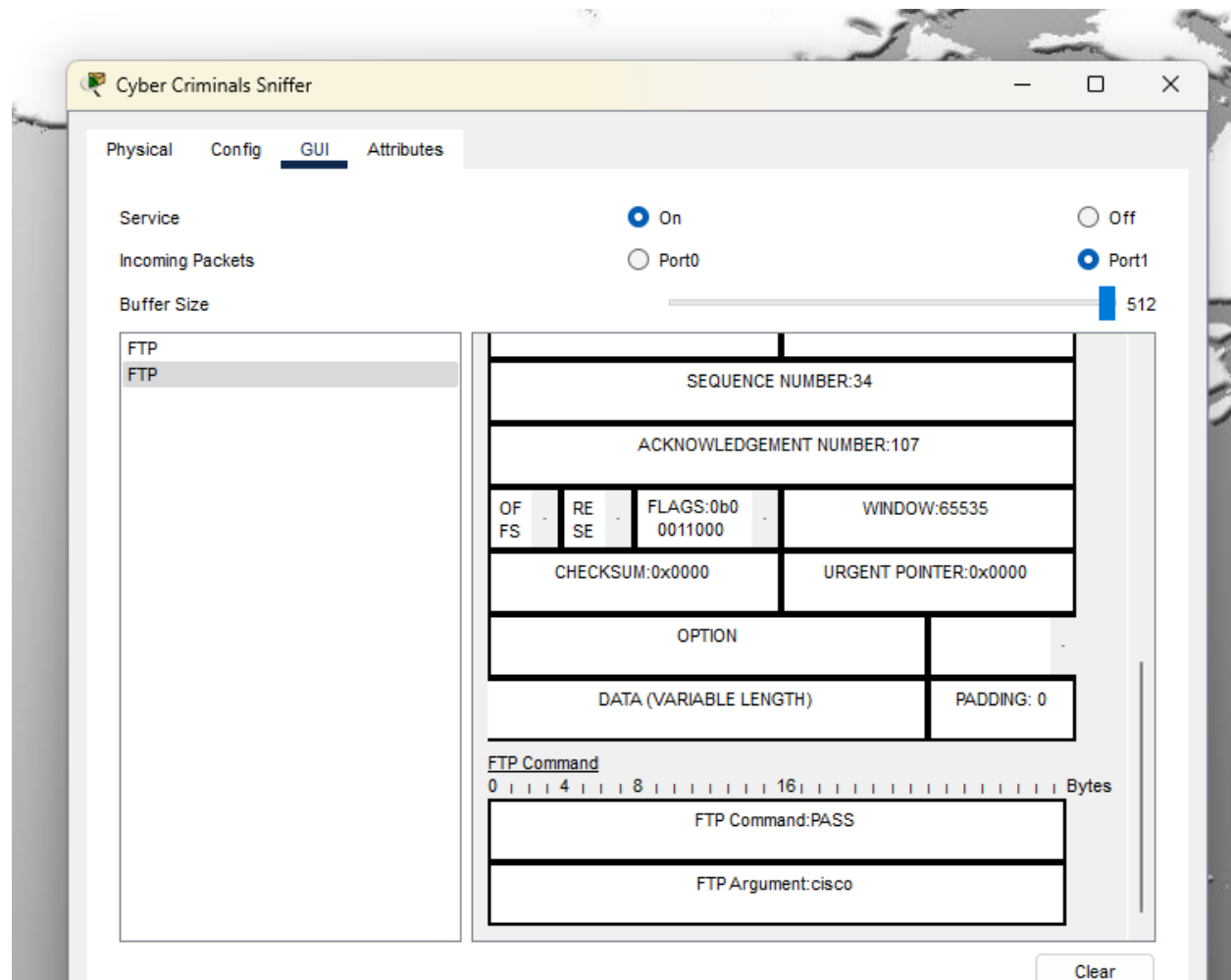
Writing file FTPupload.txt to 10.44.2.254:
File transfer in progress...

[Transfer complete - 1575 bytes]

1575 bytes copied in 0.02 secs (78750 bytes/sec)
ftp>

```

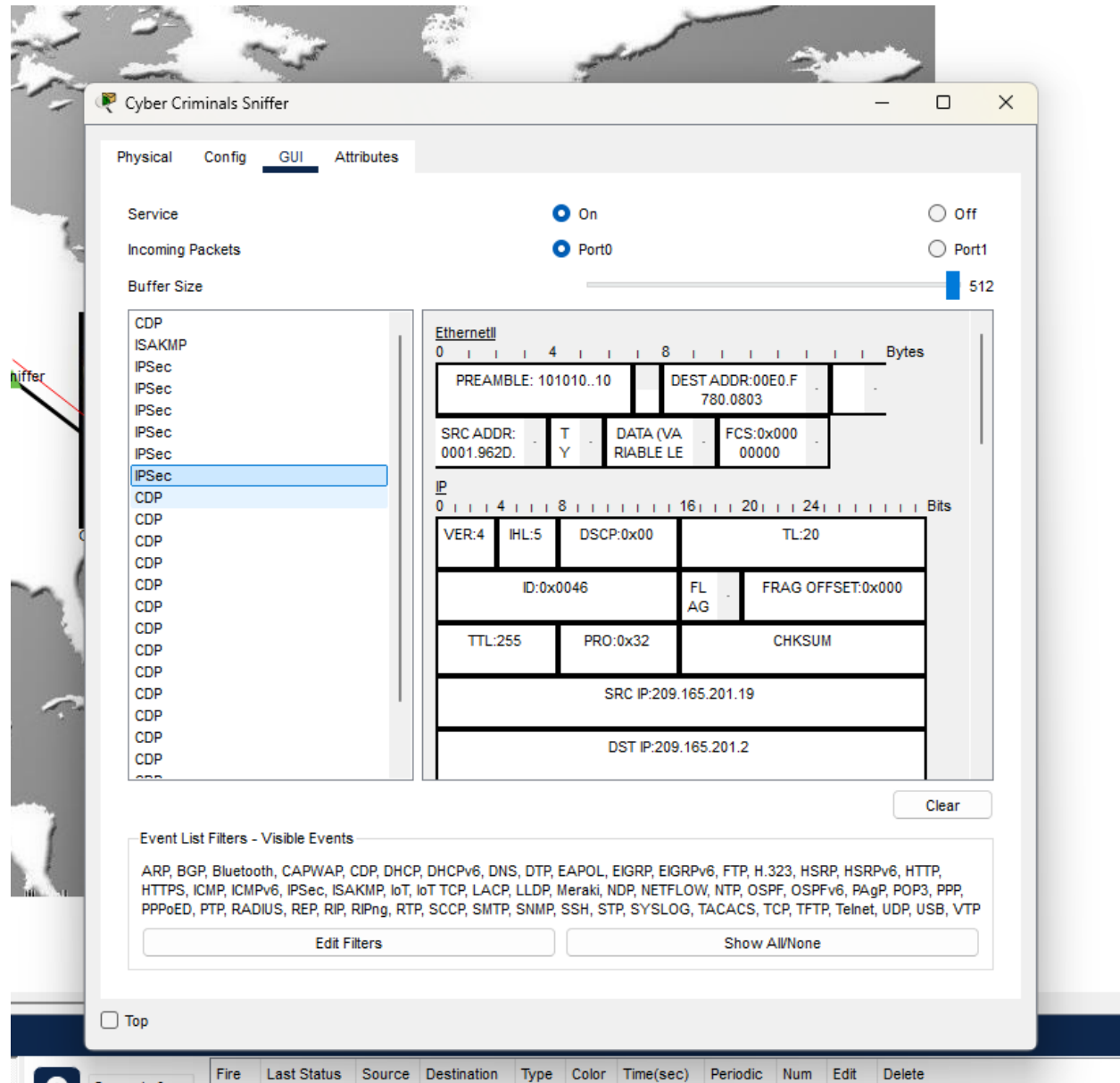
Y subimos el archivo llamado FTupload.txt, la practica nos indica que debemos revisar en el sniffer de red si es que hubo algún cambio o si se detectó algún paquete nuevo:



¿Como se puede haber no hubo ningún nuevo paquete detectado, la practica nos hace preguntarnos hay algún paquete FTP proveniente de la dirección ip de Sally?, Y si no es así explique

La respuesta es sencilla, no viajan aparentemente ningún dato FTP en la red, pero si recordamos el funcionamiento de IPSEC es decir que encapsula los datos mediante los conceptos de paquete portadora, paquete operador y paquete transporte y por tanto si colocaríamos un sniffer de red en el VPN Gateway es posible verificar que transitan paquetes FTP después de su des encapsulación.

Para comprobar esta hipótesis y afirmar que en realidad si transmiten paquetes IPSEC en la red (ya que con el filtrado FTP por defecto no aparecen limpiaremos los filtros y nos encontraremos con:



Debilidades detectadas:

Las credenciales no son cifradas y no se implementan políticas de acceso para el router HQ_Router

```
HQ_Router#sh run | include pass
no service password-encryption
crypto isakmp key vpnpass address 209.165.201.19
HQ_Router#
```

Como se puede apreciar en la imagen

Además se puede acceder al modo de configuración del router sin requerir credenciales de acceso, una forma de solucionar esto seria habilitándolas tanto en las interfaces fuera de línea como en las interfaces virtuales y en general cualquier acceso que se pueda utilizar para conectarse al router.

Además es necesario ingresar mensajes de aviso que la conexión a este dispositivo solo es autorizada para el personal con los permisos suficientes, una política de seguridad mas avanzada seria el implementar servidores TACACS+ y RADIUS así como el protocolo SYSLOG para poder mantener un registro de las modificaciones realizadas en los dispositivos intermediarios.

Otra vulnerabilidad observada es la no deshabilitación del protocolo CDP que como sabemos es utilizado para descubrir dispositivos cisco, este protocolo puede dar cabida a un ataque de reconocimiento en el que se identifique la versión de router usada y se ejecuten exploits conocidos para esa versión de cisco IOS

```
HQ_Router#show cdp ne
HQ_Router#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID      Local Intrfce   Holdtme    Capability   Platform     Port ID
ISP            Gig 0/1         166        R           C2900        Gig 0/0
Switch         Gig 0/0         166        S           2960         Fas 0/5
HQ_Router#
```

Instalación de pgp

Para ello primero se procedera a actualizar la lista de repositorios que se poseen en el so

```
(wizard23@DESKTOP-DL1SVJD)-[/mnt/c/Users/user 2]
$ gpg
Could not find command-not-found database. Run 'sudo apt update' to populate it.
gpg: command not found

(wizard23@DESKTOP-DL1SVJD)-[/mnt/c/Users/user 2]
$ sudo apt update
Get:1 http://mirrors.ocf.berkeley.edu/kali kali-last-snapshot InRelease [41.5 kB]
Get:2 http://mirrors.ocf.berkeley.edu/kali kali-last-snapshot/main amd64 Packages [19.7 MB]
21% [2 Packages 5,606 kB/19.7 MB 28%]
```

```
(wizard23@DESKTOP-DL1SVJD)-[/mnt/c/Users/user 2]  
$ sudo apt search gnupg | grep gnupg
```

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

```
gnupg/kali-last-snapshot 2.2.43-7 all  
gnupg-agent/kali-last-snapshot 2.2.43-7 all  
gnupg-l10n/kali-last-snapshot 2.2.43-7 all  
gnupg-pkcs11-scd/kali-last-snapshot 0.10.0-4 amd64  
gnupg-pkcs11-scd-proxy/kali-last-snapshot 0.10.0-4 amd64  
gnupg-utils/kali-last-snapshot 2.2.43-7 amd64  
gnupg1/kali-last-snapshot 1.4.23-2 amd64  
gnupg1-l10n/kali-last-snapshot 1.4.23-2 all  
gnupg2/kali-last-snapshot 2.2.43-7 all  
libgnupg-interface-perl/kali-last-snapshot 1.04-2 all  
libgnupg-perl/kali-last-snapshot 0.19-5 all  
libmail-gnupg-perl/kali-last-snapshot 0.23-4 all  
php-gnupg/kali-last-snapshot 1.5.1-3+b1 amd64  
php-gnupg-all-dev/kali-last-snapshot 1.5.1-3 all  
php8.2-gnupg/kali-last-snapshot 1.5.1-3+b1 amd64  
python3-gnupg/kali-last-snapshot 0.5.2-2 all  
sequoia-chameleon-gnupg/kali-last-snapshot 0.8.0-5 all
```

```
(wizard23@DESKTOP-DL1SVJD)-[/mnt/c/Users/user 2]  
$ sudo apt install gnupg
```

```
(wizard23@DESKTOP-DL1SVJD)-[/mnt/c/Users/user 2]  
$ sudo apt install gnupg
```

Installing:

gnupg

Installing dependencies:

dirmgr gnupg-utils gpg-agent gpgconf libassuan0 libnph0t64
gnupg-l10n gpg gpg-wks-client gpgsm libksba8 pinentry-curses

Suggested packages:

pinentry-gnome3 tor gpg-wks-server parcimonie xloadimage sdaemon pinentry-doc

Summary:

Upgrading: 0, Installing: 13, Removing: 0, Not Upgrading: 0
Download size: 3,457 kB
Space needed: 11.6 MB / 1,025 GB available

Continue? [Y/n] y

```
Get:1 http://http.kali.org/kali kali-last-snapshot/main amd64 libassuan0 amd64 2.5.6-1+b1 [50.4 kB]  
Get:2 http://kali.download/kali kali-last-snapshot/main amd64 gpgconf amd64 2.2.43-7 [119 kB]  
Get:4 http://kali.download/kali kali-last-snapshot/main amd64 libnph0t64 amd64 1.6-3.1 [17.9 kB]  
Get:5 http://kali.download/kali kali-last-snapshot/main amd64 dirmgr amd64 2.2.43-7 [363 kB]  
Get:6 http://kali.download/kali kali-last-snapshot/main amd64 gnupg-l10n all 2.2.43-7 [701 kB]  
Get:9 http://kali.download/kali kali-last-snapshot/main amd64 gpg-agent amd64 2.2.43-7 [248 kB]  
Get:11 http://kali.download/kali kali-last-snapshot/main amd64 gnupg all 2.2.43-7 [375 kB]  
Get:13 http://kali.download/kali kali-last-snapshot/main amd64 gnupg-utils amd64 2.2.43-7 [500 kB]  
Get:10 http://mirrors.jevincanders.net/kali kali-last-snapshot/main amd64 gpgsm amd64 2.2.43-7 [250 kB]  
69% [Connecting to mirror.0xem.ma (76.69.228.187)] [10 gpgsm 66.4 kB/250 kB 27%] [Connecting to kali.mirror.rafa.ca]
```

Crearemos un directorio con un archivo py que tendrá un simple “hola mundo”

```
(wizard23@DESKTOP-DL1SVJD)~  
$ mkdir pruebaCifrado  
  
(wizard23@DESKTOP-DL1SVJD)~  
$ cd pruebaCifrado/  
  
(wizard23@DESKTOP-DL1SVJD)~/pruebaCifrado  
$ ls  
  
(wizard23@DESKTOP-DL1SVJD)~/pruebaCifrado  
$ echo "print('hello world')" >> hello.py  
  
(wizard23@DESKTOP-DL1SVJD)~/pruebaCifrado  
$ cd ..
```

Ahora utilizaremos pgp para cifrar el archivo

```
(wizard23@DESKTOP-DL1SVJD)~  
$ gpg -c pruebaCifrado/hello.py
```

GPG automaticamente nos generara un archivo con extensión .gpg

```
(wizard23@DESKTOP-DL1SVJD)~  
$ ls pruebaCifrado/  
hello.py  hello.py.gpg
```

La opción -c indica que utilizaremos un cifrado simétrico


```

$ gpg -h
gpg (GnuPG) 2.2.43
libgcrypt 1.11.0
Copyright (C) 2023 g10 Code GmbH
License GNU GPL-3.0-or-later <https://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Home: /home/wizard23/.gnupg
Supported algorithms:
Pubkey: RSA, ELG, DSA, ECDH, ECDSA, EDDSA
Cipher: IDEA, 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH,
        CAMELLIA128, CAMELLIA192, CAMELLIA256
Hash: SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224
Compression: Uncompressed, ZIP, ZLIB, BZIP2

Syntax: gpg [options] [files]
Sign, check, encrypt or decrypt
Default operation depends on the input data

Commands:

-s, --sign                make a signature
--clear-sign              make a clear text signature
-b, --detach-sign         make a detached signature
-e, --encrypt              encrypt data
-c, --symmetric            encryption only with symmetric cipher

```

Como lo indica la ayuda del comando, ahora bien las credenciales usadas para el cifrado del archivo fueron hello world en l337 es decir: “H3110 W0r1D”

Ahora para el proceso de descifrado se usara:

```

(wizard23@DESKTOP-DL1SVJD)~$ gpg -d pruebaCifrado/hello.py.gpg
gpg: AES256.CFB encrypted data
gpg: encrypted with 1 passphrase
print('hello world')

```

Como se puede observar se hizo uso de AES256 como indica gpg

Investigación sobre PGP una forma de cifrar y enviar información de forma segura en la web

La seguridad de la información es un aspecto crítico en el mundo digital de hoy.

Con la creciente preocupación por la privacidad y la integridad de los datos, herramientas como GnuPG se han vuelto indispensables. GnuPG, o GNU Privacy Guard, es una solución de cifrado y firma digital que ofrece múltiples capas de seguridad para la comunicación y el almacenamiento de información. A continuación, exploraremos sus características clave y cómo contribuyen a una infraestructura de seguridad robusta.

Cifrado de Datos con GnuPG

El cifrado de datos es fundamental para proteger la información confidencial. GnuPG utiliza la criptografía de clave pública, que como sabemos, implica un par de claves: una pública y una privada. El remitente utiliza la clave pública del destinatario para cifrar el mensaje o archivo, asegurando que solo el destinatario pueda descifrarlo con su clave privada correspondiente. Este proceso garantiza que la información solo sea accesible para las partes previstas, protegiéndola de accesos no autorizados.

La Importancia de la Firma Digital

La firma digital es otro componente esencial de la seguridad en GnuPG. Al firmar digitalmente un archivo o mensaje, el remitente asegura que el contenido es auténtico y no ha sido alterado desde su origen. Esto se logra utilizando la clave privada del remitente para crear la firma. Cualquier persona con acceso a la clave pública del remitente puede verificar esta firma, lo que añade una capa adicional de verificación y confianza.

Las firmas digitales proporcionan no solo integridad, sino también autenticación. Dado que solo el propietario de la clave privada puede generar una firma válida, los destinatarios pueden confiar en que los datos recibidos son genuinos y provienen de la fuente declarada. Esta característica es crucial para evitar la suplantación de identidad y garantizar la autenticidad de la comunicación.

GnuPG también juega un papel vital en la preservación de la integridad de los datos. Las firmas digitales permiten a los usuarios detectar cualquier modificación no autorizada de los datos durante su tránsito. Si los datos se alteran, la firma no coincidirá al ser verificada, alertando a los destinatarios de una posible brecha de seguridad, otro aspecto que cubre la herramienta es la gestión de claves es un aspecto fundamental del uso de GnuPG. La herramienta proporciona mecanismos para la creación y administración de pares de claves, así como para el mantenimiento de un anillo de claves, que es un conjunto de claves públicas de otros usuarios. Esto facilita el intercambio seguro de claves públicas y establece una red de confianza entre los usuarios, este punto se discutirá un poco más adelante.

En resumen, GnuPG es una herramienta poderosa que ofrece soluciones integrales para la seguridad de la información. Desde el cifrado de datos hasta la gestión de claves, GnuPG ayuda a los usuarios a proteger su información y a mantener la confidencialidad, la autenticidad y la integridad de sus comunicaciones en el ciberespacio.

Existe una guía que nos blinda los pasos básicos a seguir si queremos aprender sobre la auto defensa en los correos electrónicos, en ella se habla sobre muchos aspectos incluyendo la web de confianza que es

una forma que incita a los usuarios a firmar las firmas de otros usuarios con los que se frecuenta enviar mensajes, esto para autenticar que un usuario es quien dice ser y no un suplantador de identidad, en la documentación de la herramienta se menciona que GPG fue una herramienta utilizada por Edward Snowden para exfiltrar datos confidenciales de la NSA, incluso de alguna forma, se creo un bot para enseñar a los usuarios a firmar y enviar información de correos electrónicos cifrados a este programa con el mismo nombre del personaje.

GPG hace uso de de servidores de claves los cuales son como una especie de directorio a la cual se puede subir la clave publica con el objetivo de hacer que cualquier persona pueda enviarle mensajes, incluso gpg tiene un api que puede ser invocada en algún lenguaje de programación para darle seguridad a algunos componentes del sistema.

Conclusiones:

En conclusión, la seguridad de la información es un aspecto crítico en la gestión de redes y sistemas informáticos. La práctica ha demostrado que el cifrado de credenciales es esencial para proteger la confidencialidad de la información, especialmente cuando se transmiten datos sensibles a través de protocolos inseguros como FTP. La implementación de IPSEC con cifrado AES y autenticación HMAC se presenta como una solución robusta para mitigar los riesgos asociados con la captura de credenciales en texto plano.

Además, la identificación de vulnerabilidades en la configuración de dispositivos de red resalta la necesidad de adoptar medidas de seguridad más estrictas, como la implementación de autenticación fuerte y el uso de servidores TACACS+ o RADIUS para el control de acceso. La eficacia de IPSEC en la protección de datos es indiscutible, aunque su uso sin GRE puede presentar limitaciones en el tránsito de paquetes de enrutamiento, lo que sugiere la necesidad de configuraciones adicionales para adaptarse a diferentes entornos de red.

Por último, el cifrado con GPG y el uso de firmas digitales han probado ser métodos efectivos para asegurar la autenticidad e integridad de los datos, elementos fundamentales en sistemas donde la privacidad es de suma importancia. Estas prácticas subrayan la relevancia de una estrategia de seguridad integral que no solo se enfoque en la protección de la infraestructura de red, sino también en la seguridad de los datos en sí.

La seguridad informática es un campo en constante evolución, y estas prácticas son un recordatorio de la importancia de mantenerse actualizado con las últimas tendencias y tecnologías para proteger eficazmente la información en la era digital.

Referencias:

4. *Redes empresariales, Seguridad y Automatización -Introducción*. (n.d.).

<https://contenthub.netacad.com/ensa-dl/6.0.1?lng=es-XL>

5, *Email Self-Defense - a guide to fighting surveillance with GnuPG encryption*. (n.d.).

<https://emailselfdefense.fsf.org/en/index.html#step-6c>

1. Schneier, B. (2015). **Applied Cryptography: Protocols, Algorithms, and Source Code in C** (20th anniversary ed.). Wiley.

2. Stallings, W. (2017). **Cryptography and Network Security: Principles and Practice** (7th ed.). Pearson.