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 2 Configuración de un medio de transporte VPN.

Fecha:

02/10/2024

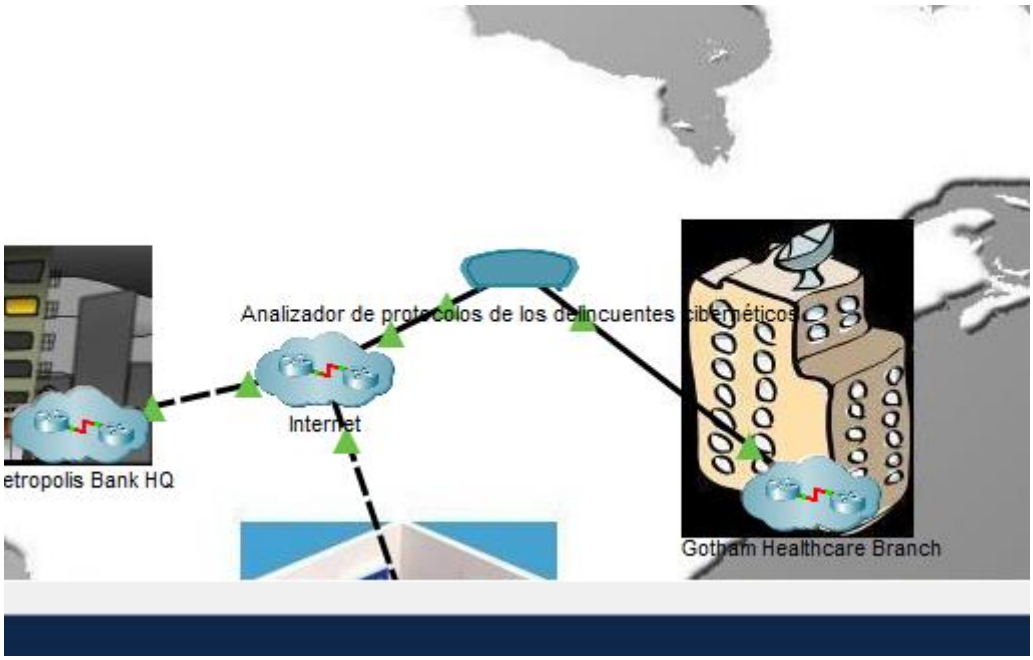
introducción

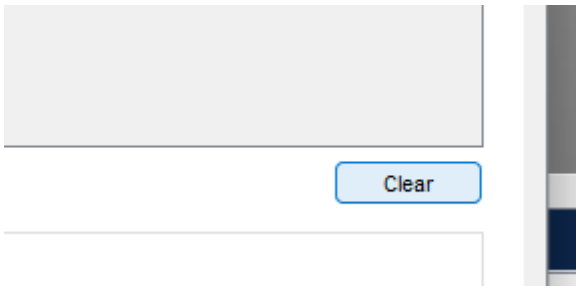
En esta práctica, nos adentramos en la configuración y análisis de un medio de transporte VPN dentro de un entorno corporativo simulado. El objetivo principal es identificar y comprender los elementos criptográficos que aseguran la transferencia de datos a través de redes inseguras. Mediante el uso de herramientas como sniffers de red y protocolos de seguridad como IPSEC y GRE, se exploran los riesgos asociados a la transferencia no cifrada de información y cómo los VPNs proveen una solución efectiva al encapsular y proteger los datos. Esta práctica busca no solo desarrollar una VPN funcional, sino también resaltar la importancia de los mecanismos criptográficos en la seguridad de la información.

Configuración de un medio de transporte VPN

Identificación de los elementos criptográficos dentro del sistema corporativo simulado:

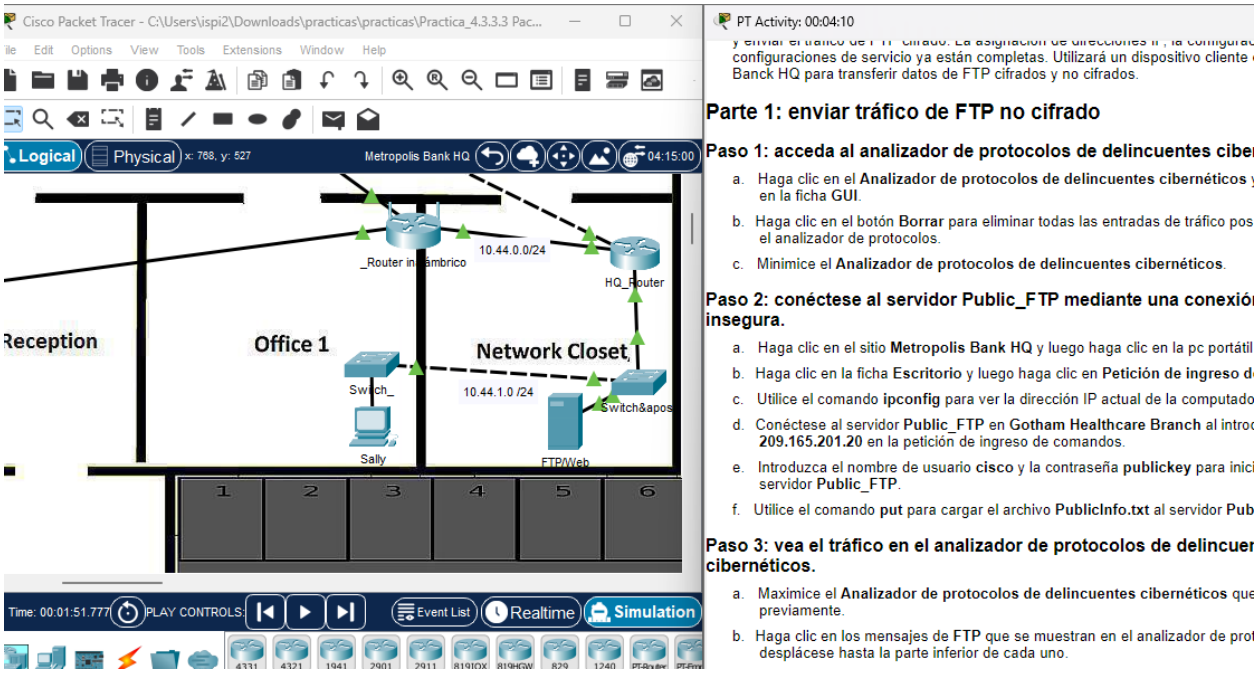
La practica inicia solicitando que inicialicemos el analizador de protocolos de los delincuentes informáticos, esto no es mas que un sniffer de red que capturara los paquetes enviados por la red



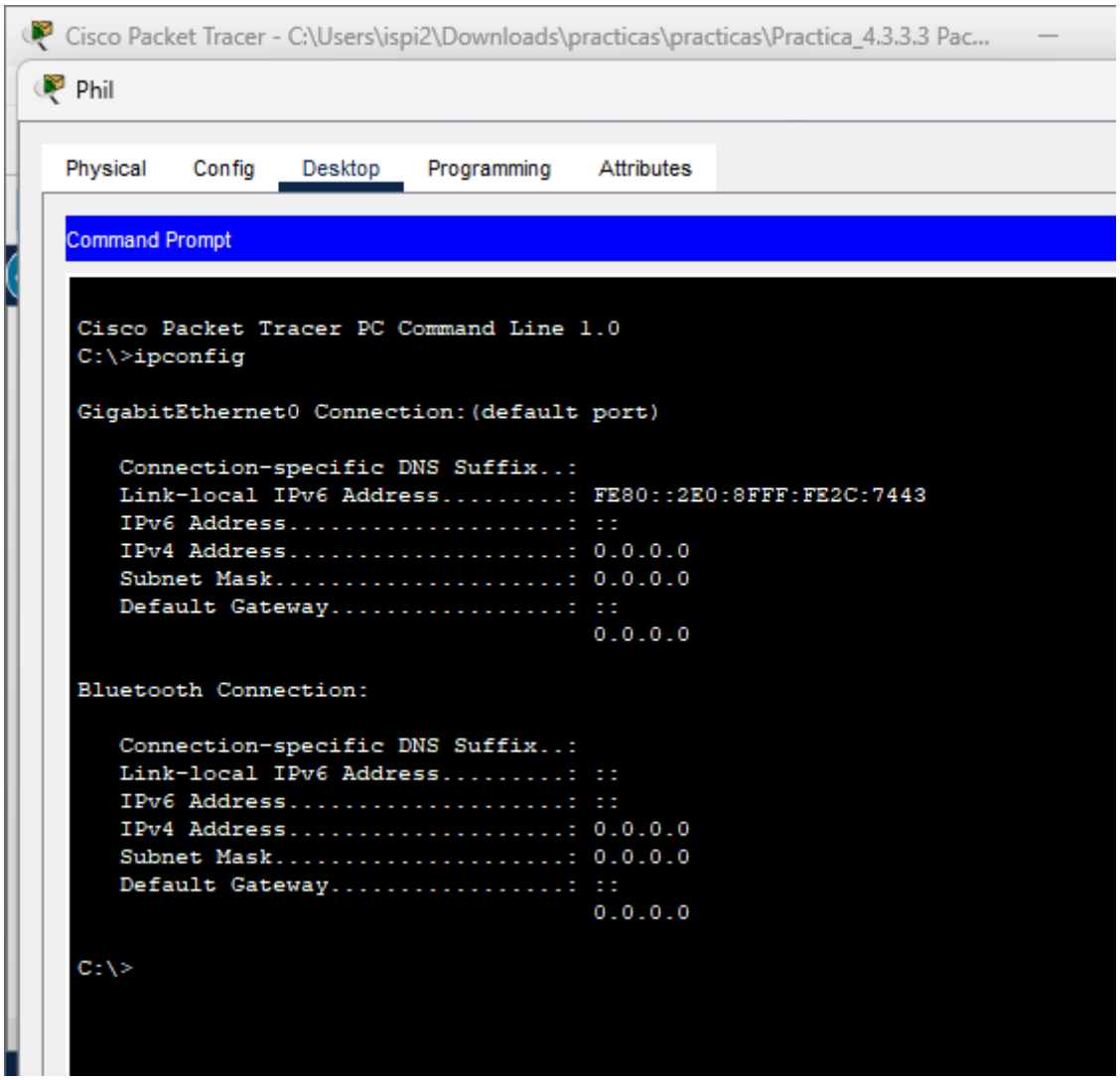


Al darle en clear limpiamos las previas entradas que se pudieron haber generado en el dispositivo

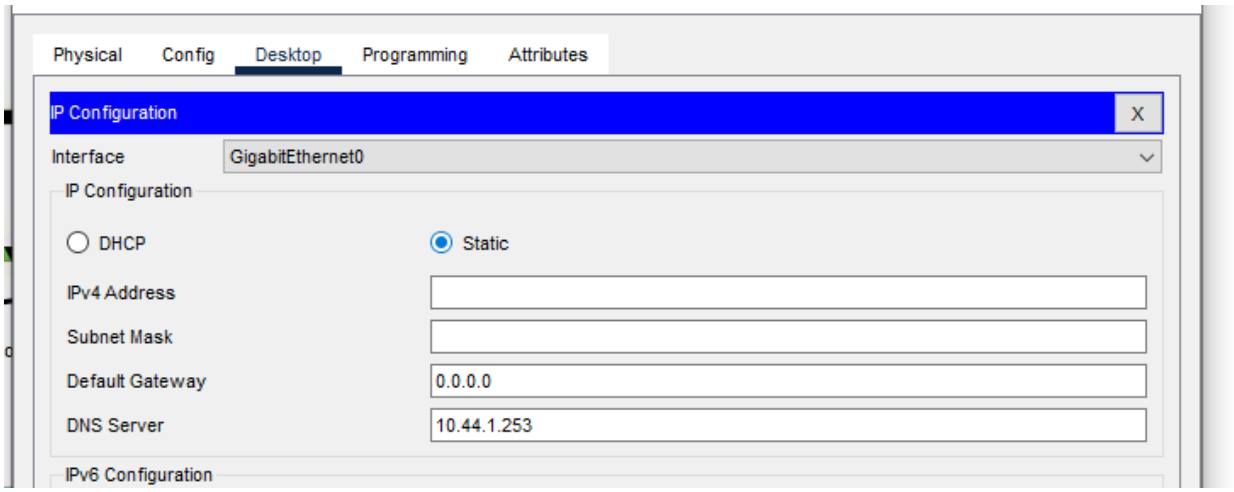
La practica señala que es necesario acceder a la computadora de phil

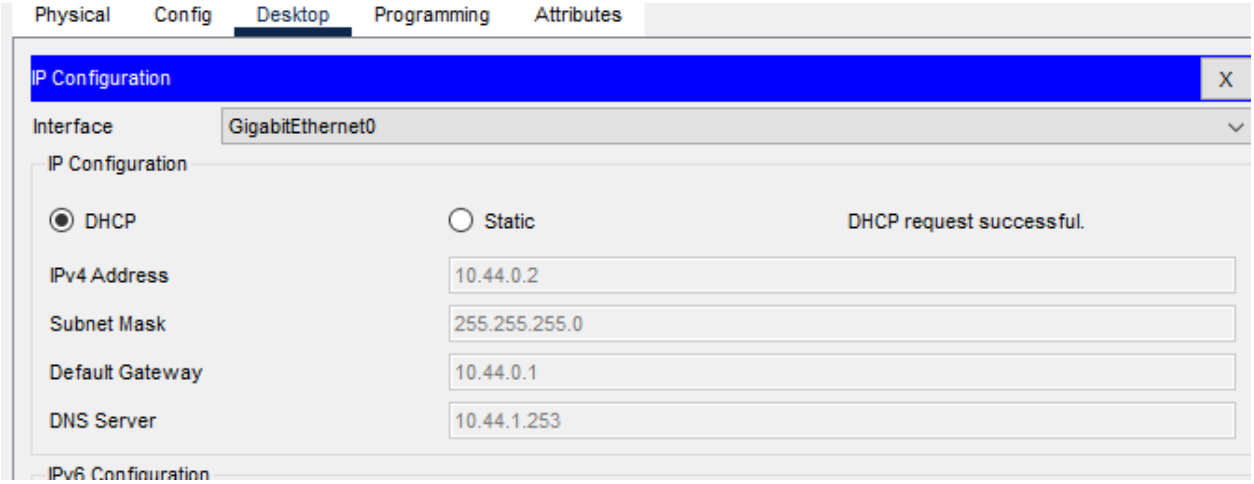


Accederemos a la computadora de phil

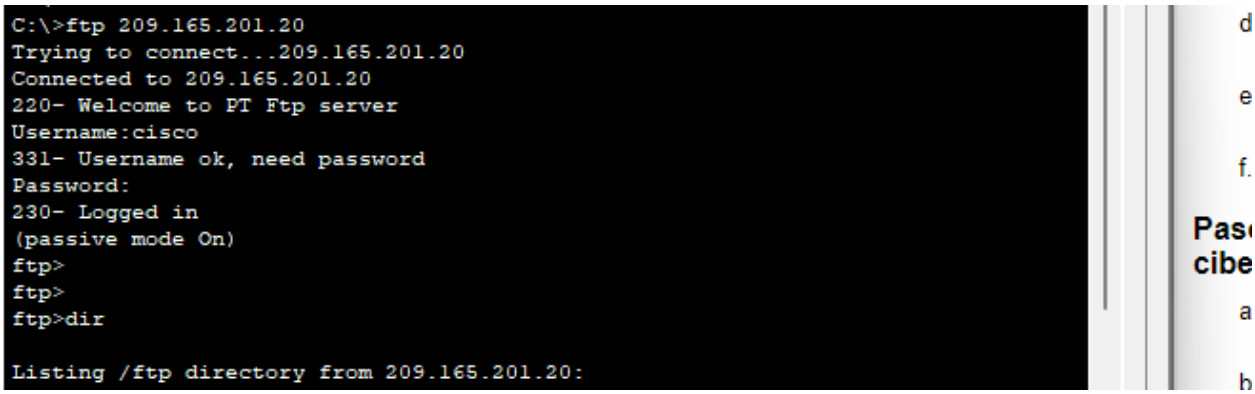


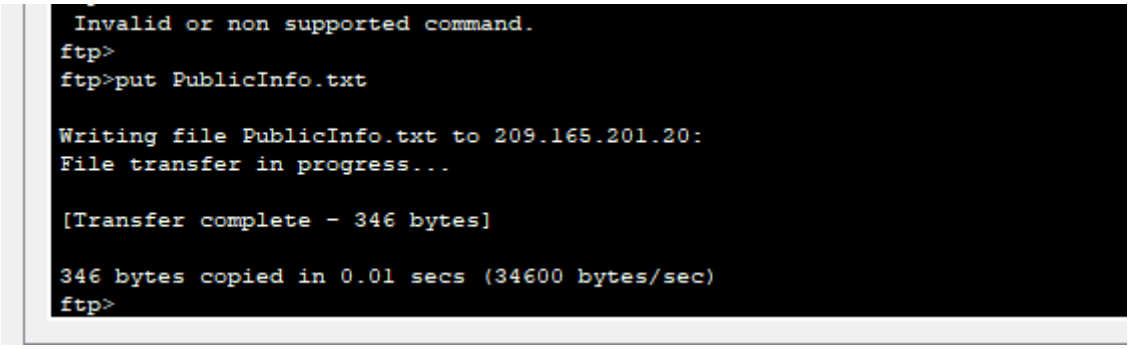
Primero para ello verificamos si se posee alguna dirección ip, en este caso no es así por que la dirección ip de la computadora está configurada con una dirección APIPA, debemos habilitar la obtención dinámica de una dirección ip por medio de un servidor DHCP





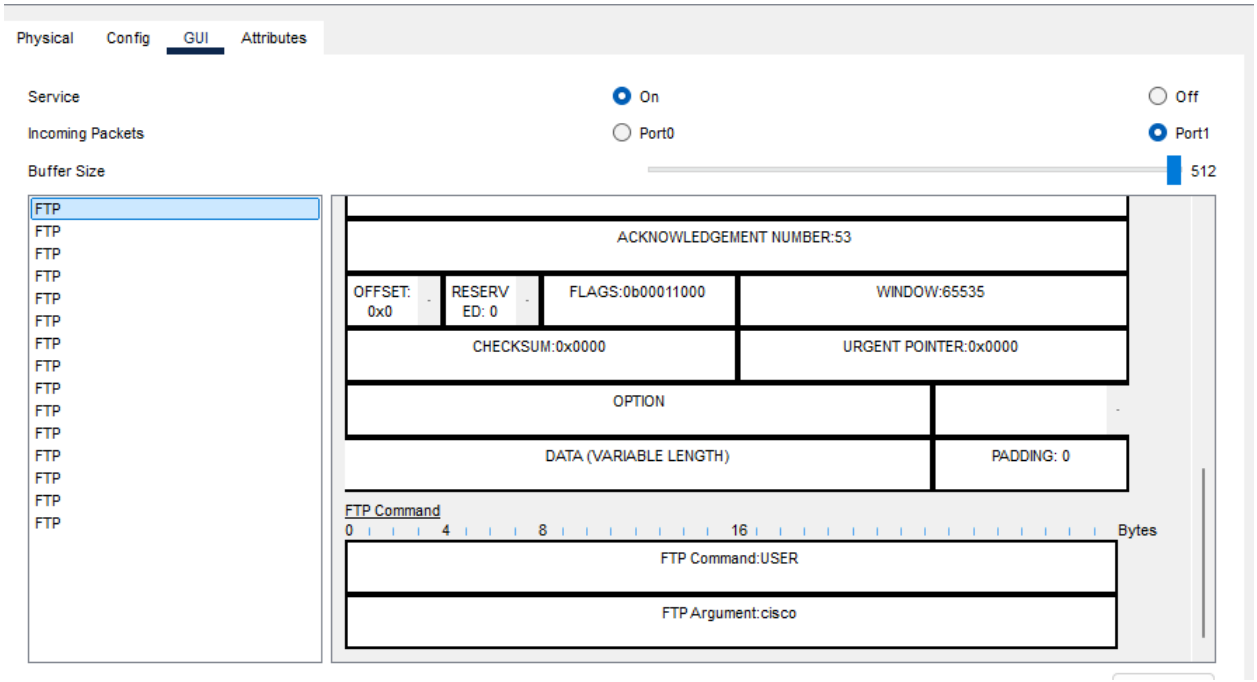
La petición fue exitosa ahora con la dirección ip podremos conectarnos a el servidor FTP, sin embargo aquí hay una implicación de seguridad, FTP no es un protocolo destinado a la transferencia de archivos de forma segura, se desaconseja su uso principalmente porque no solo el contenido transferido es visible en texto plano sino que lo mismo sucede con el loggeo con las credenciales pertinentes por lo tanto al hacer uso de Sniffer de red se podrán ver las credenciales que se utilizan para acceder a ftp:



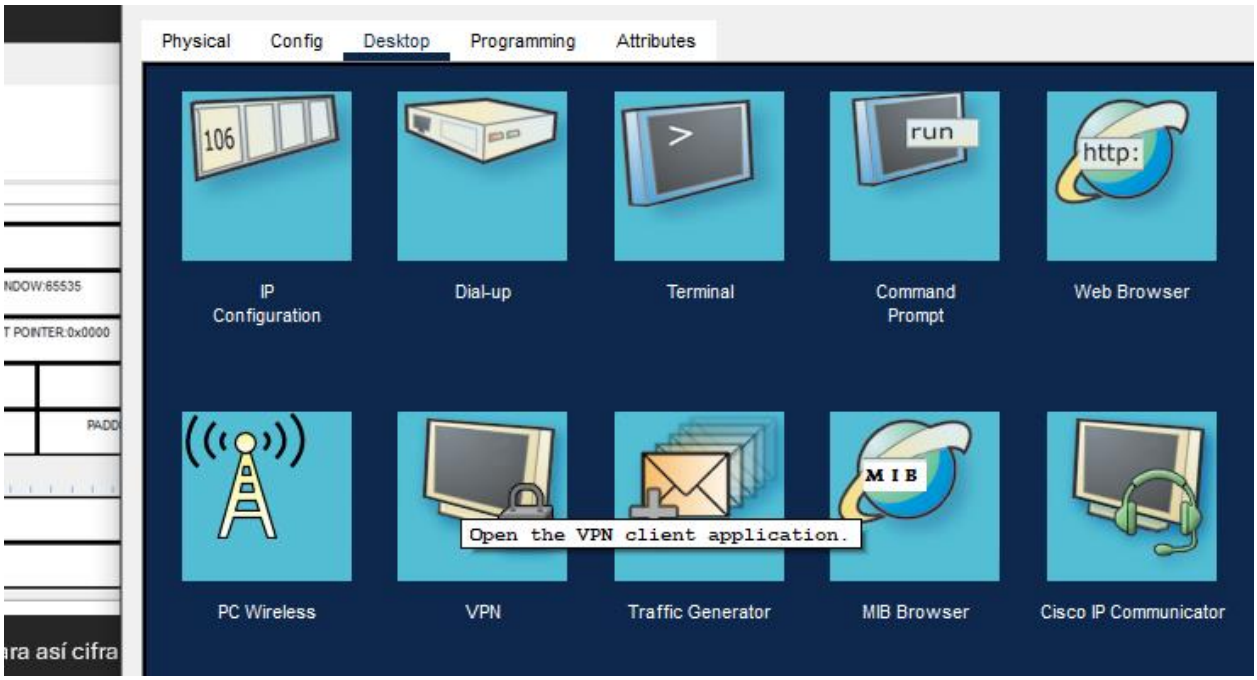


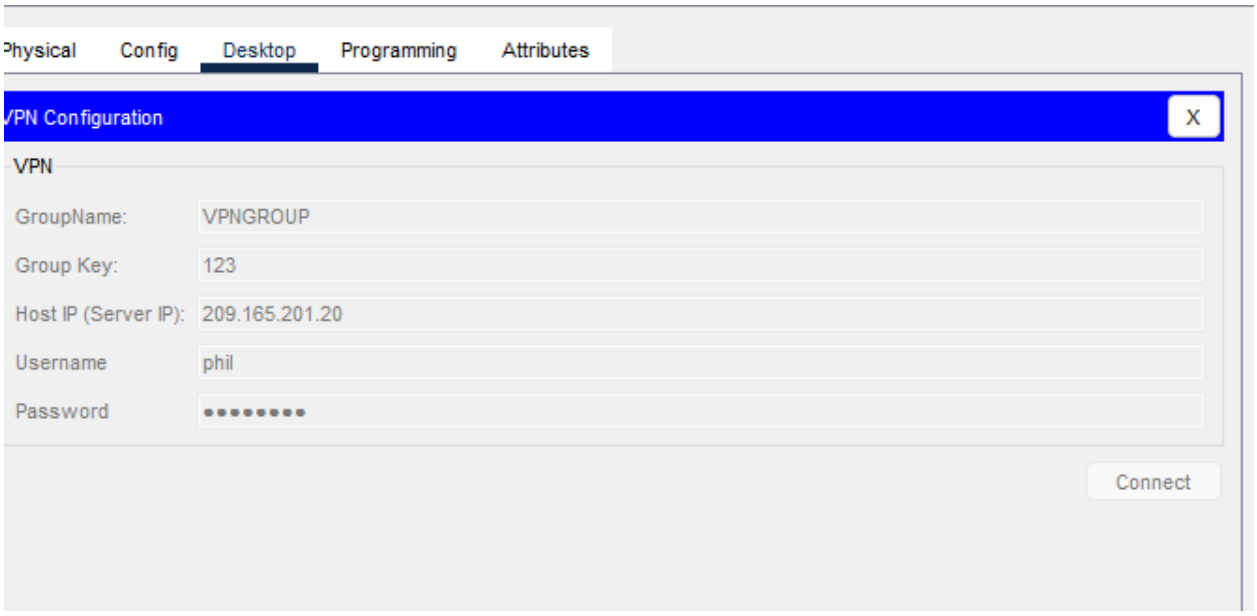
Para demostrar este punto nos loggeamos y subimos el archivo PublicInfo.txt al servidor con el verbo put

Ahora si como lo demarca la practica vamos al sniffer de red, podemos ver las credenciales que se utilizaron para acceder al servicio FTP, esto involucra una grave falta a la confidencialidad de los datos transmitidos:

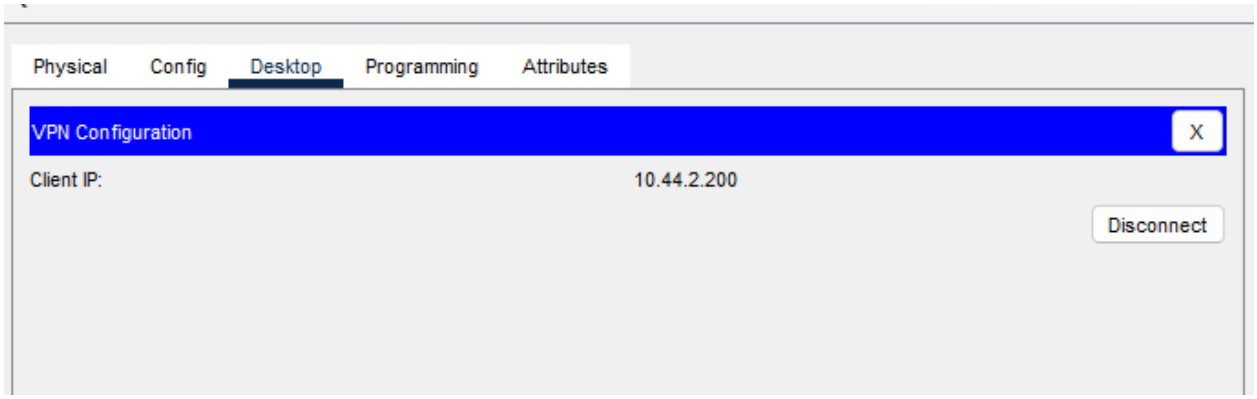


La practica exige que conectemos la computadora de bob a una vpn para así cifrar los datos del trafico de red





Introduciremos los datos de conexión al vpn



Y finalmente nos conectaremos, en este punto podemos preguntarnos, ¿ como funcionan los VPN, es decir que protocolos suelen utilizarse para su funcionamiento? Y ¿que clase de cifrados utilizan?

Existen varios enfoques para crear una vpn uno de ellos es el uso del protocolo GRE (Generic Routing Encapsulation) , el cual es un protocolo desarrollado por cisco, es posible utilizar el protocolo GRE con el protocolo IPSEC para poder transmitir datos punto a punto o sitio a sitio, como lo mencionan en cisco existen 2 tipos de VPN de sitio a sitio y de acceso remoto

Los Vpn de sitio a sitio son como la vpn mencionada anteriormente, es decir se debe de configurar la puerta de enlace para la realización de la VPN, ahora bien, en contra parte existen las VPN de acceso remoto.

Como sabemos IPSEC soporta todas las aplicaciones basadas en IPSEC compatibles utiliza una fuerza o longitudes de cifrado de 256 bits sin embargo como sabemos es difícil las conexiones ya que los equipos que utilizan IPSEC deben configurar parámetros específicos en sus equipos como ocurre en este caso

IPSEC también puede ser implementado de sitio a sitio el funcionamiento de esto es por medio de como se mencionó anteriormente el encapsulamiento de los datos de un paquete es decir el tomar un protocolo y envolverlo en otros parámetros, ¿por que utilizar un protocolo sobre otro? Es decir por que usar GRE para encapsular un paquete IPSEC que finalmente encapsule los datos del paquete o datagrama, esto es debido a que hay ocasiones en las que se requiere enviar los paquetes multicas para información de control de la red

Ahora bien IPSEC se caracteriza por hacer uso de AES, sin embargo como sabemos ese tipo de cifrado es simétrico, por lo que, para poder realiazzr una negociación de claves IPSEC implementa IKE el cual es un protocolo orientado al intercambio de claves, ike puede hacer uso de múltiples formas de autenticación de los datos como puede ser el uso de biométrica o claves PSK).

IPSEC hace pleno uso del esquema DiffHellman es decir un método para poder intercambiar claves usadas para cifrar los datos, IPSEC está estrechamente relacionado con OAKLEY el cual es un protocolo que es implementado por IKE o Internet Key Exchange

PSK es una clave secreta en la cual se utiliza un canal seguro, estas PSK utilizan cifrado simétrico como puede ser el uso de AES

Las psk en general se combinan con otros parámetros, sin embargo existe otra forma de autenticación en el caso de los datos del vpn, como se ha explorado hasta este momento otra forma es utilizando las firmas RSA, como sabemos es posible firmar datos por medio de una calve pública o privada, en el caso de RSA es posible usarlo para crear los CA o certificados de autenticación, herramientas como PGP, un ejemplo de esta actividad se retomara en una sección posterior donde con esta herramienta generaremos una clave pem y exploraremos los parámetros y funcionalidades de la herramienta openssl, el protocolo IKE impera este tipo de mecanismo de autenticación.

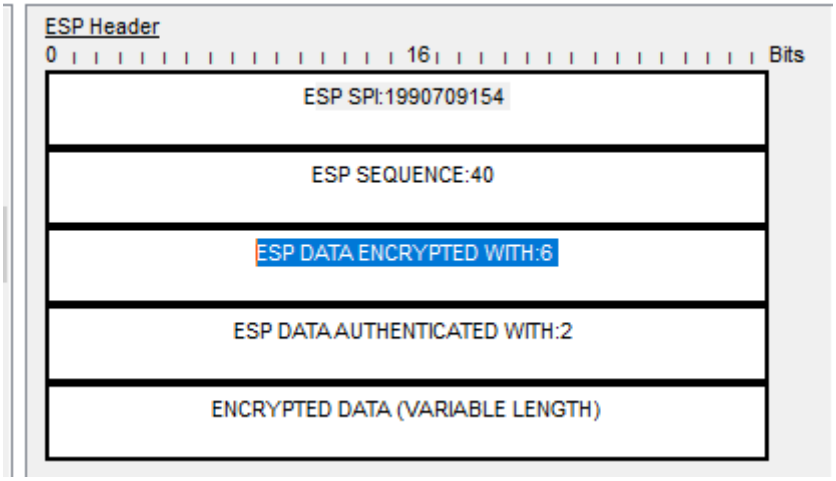
IPSEC provee de múltiples formas de funcionamiento o configuraciones:

- **AH:** este es el encabezado de autenticación únicamente proporciona la confidencialidad de los datos, pero el texto se transporta como no cifrado
- **ESP:** esp permite la autenticación y cifrado de los datos, permite ocultar tanto la dirección de envió como de recepción, impera la selección de algún modo de cifrado (DES,3DES, AES,SEAL) así como algún modo para poder gestionar la integridad de los datos (uso de algoritmos SHA o MD5), autenticación (firmado de datos con RSA o PSK) y algún mecanismo para establecer un canal seguro (como puede ser el uso de DH)

Existe una tercera forma o configuración de IPSEC el cual es ESP + AH esta forma es utilizada para solo seleccionar una forma o mecanismo de confidencialidad de los datos (un cifrado vaya) y un mecanismo de establecimiento de un canal seguro de comunicación (DiffHellman)

Ahora bien existe la pregunta, ¿qué mecanismo se ocupa en la práctica?

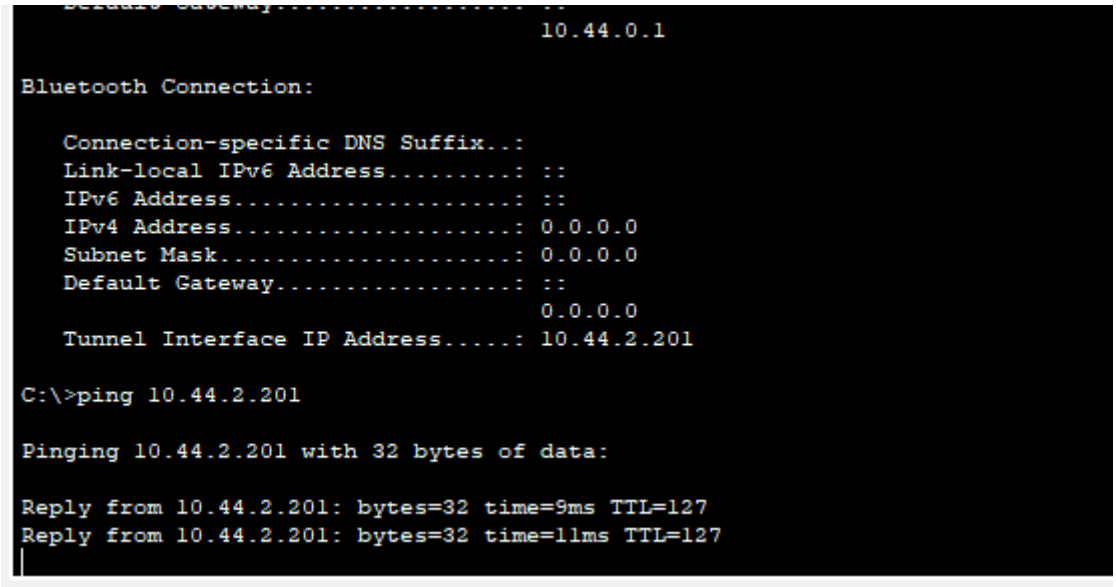
Los paquetes están cifrados utilizando 3DES como se muestra en el paquete



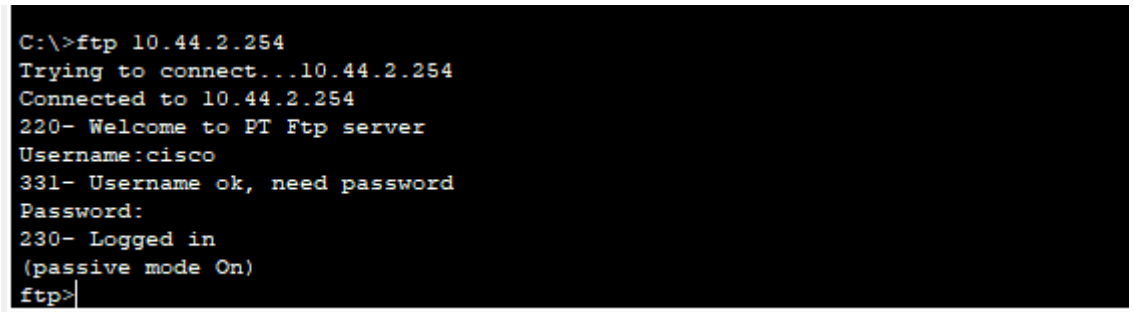
Utilizan el modo ESP, ESP DATA AUTHENTICATED WITH: 2 significa que los datos encapsulados en ESP están siendo autenticados utilizando el algoritmo HMAC-MD5-96. Esto asegura que los datos no han sido alterados en tránsito y que provienen de una fuente confiable. Sin embargo, es **importante mencionar que MD5 ya no es considerado un algoritmo de hash seguro**, por lo que muchas implementaciones modernas prefieren usar alternativas más seguras como HMAC-SHA-256.

En resumen, una implementación de una política de seguridad para mejorar este aspecto en la red seria el implementar otro método de autenticación como HMAC-SHA-256 además de erradicar el uso de un servidor FTP y pasar a una implementación segura de este protocolo como puede ser el uso de TFTP.

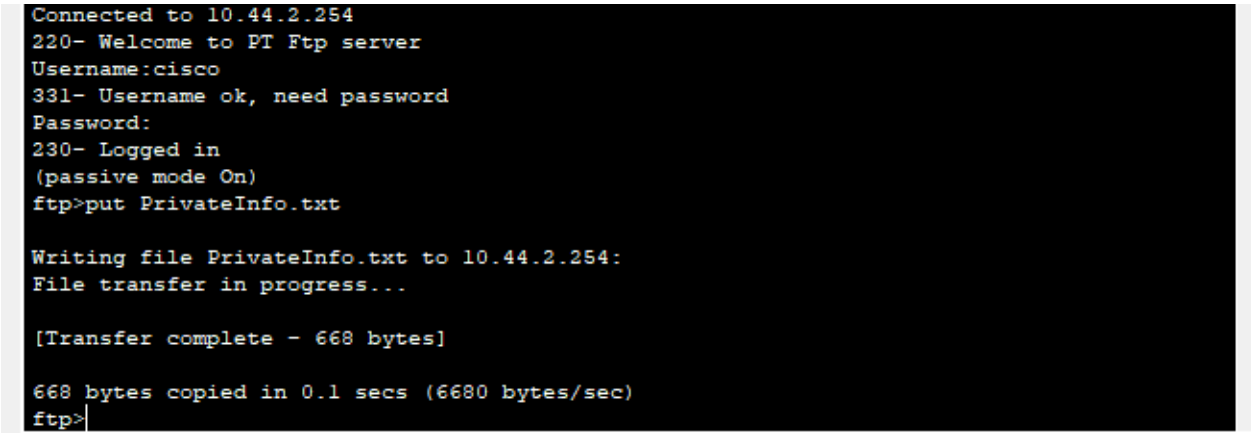
Prosiguiendo con la práctica, realizaremos un ping para comprobar que los datos se hayan enviado con éxito, como podemos observar se muestra una dirección ip adicional la dirección de túnel ip esta dirección nos demarcara la dirección ip que retorna la vpn como nuestro identificador en la red



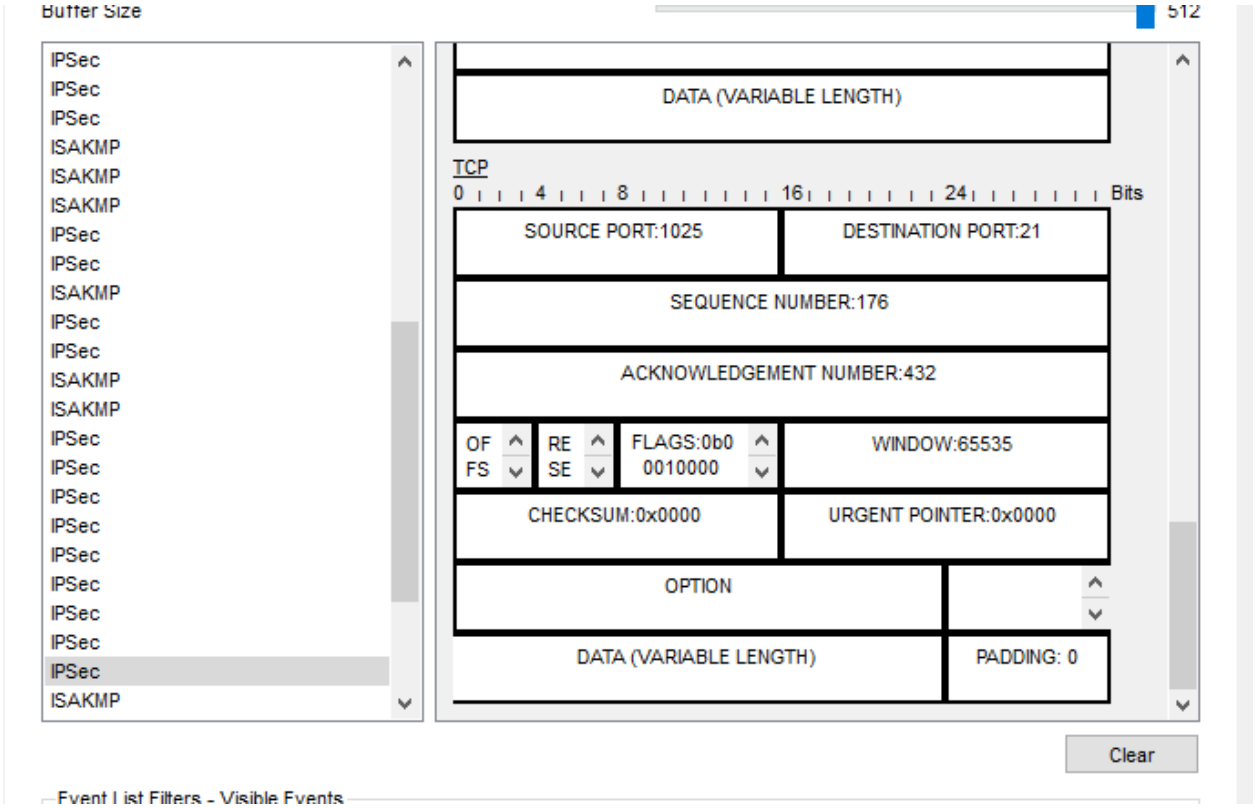
Verificamos que la conexión sea exitosa y a continuación ingresaremos a ftp y transmitiremos datos, para posterior verificar en el sniffer si estos datos son registrados por los atacantes

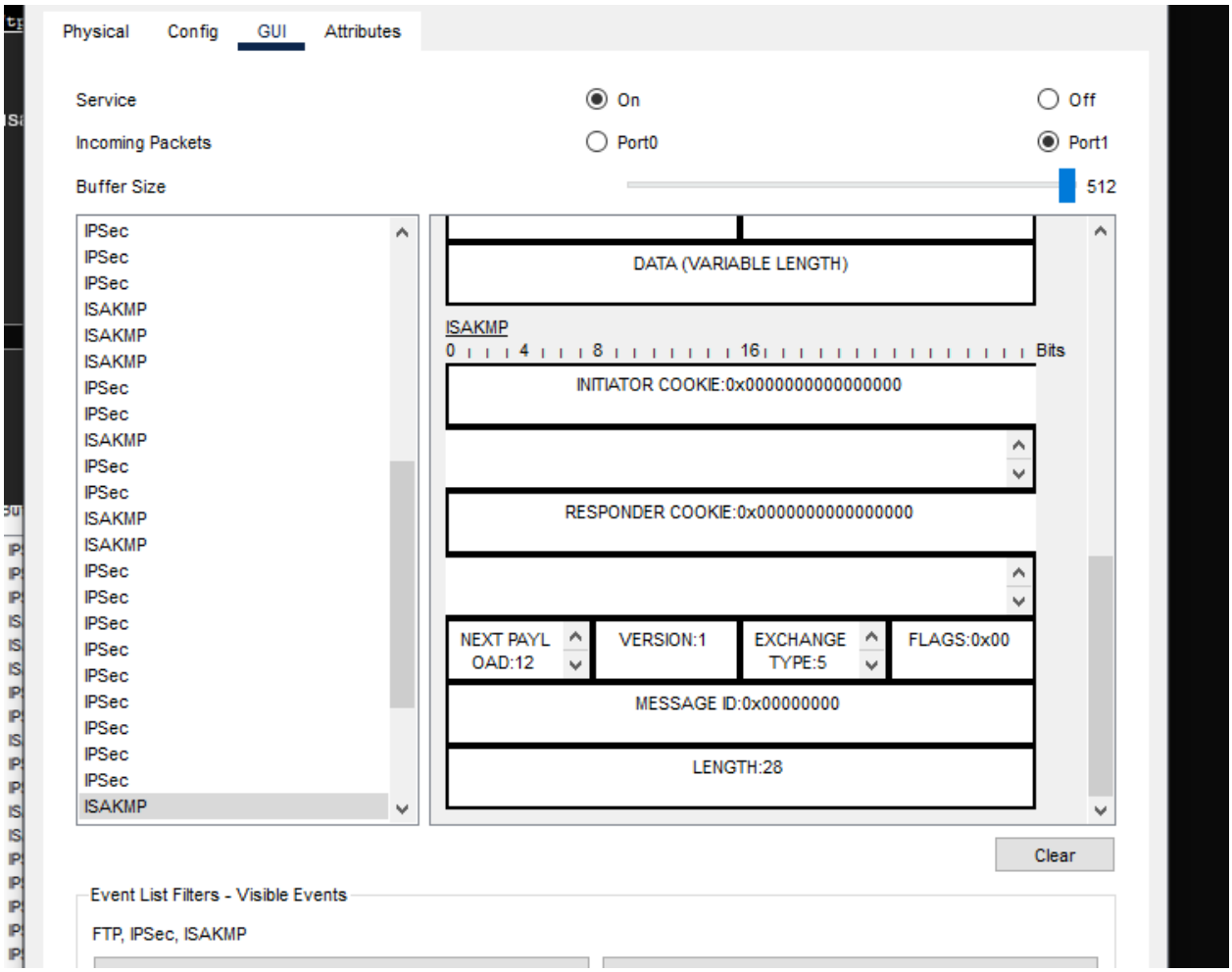


Subiremos nuevamente el archivo private info.log



Si usamos el sniffer de red solo veremos paquetes IPSEC y ISAKMP


Buffer Size
512
IPSec
IPSec
IPSec
ISAKMP
ISAKMP
ISAKMP
IPSec
IPSec
ISAKMP
IPSec
IPSec
ISAKMP
ISAKMP
IPSec
IPSec
IPSec
IPSec
IPSec
IPSec
IPSec
IPSec
IPSec
ISAKMP
DATA (VARIABLE LENGTH)
TCP
0 4 8 16 24 Bits
SOURCE PORT:1025
DESTINATION PORT:21
SEQUENCE NUMBER:176
ACKNOWLEDGEMENT NUMBER:432
OF FS
RE SE
FLAGS:0b0 0010000
WINDOW:65535
CHECKSUM:0x0000
URGENT POINTER:0x0000
OPTION
DATA (VARIABLE LENGTH)
PADDING: 0
Clear
Event List Filters - Visible Events


Physical
Config
GUI
Attributes
Service
On
Off
Incoming Packets
Port0
Port1
Buffer Size
512
IPSec
IPSec
IPSec
ISAKMP
ISAKMP
ISAKMP
IPSec
IPSec
ISAKMP
IPSec
IPSec
ISAKMP
ISAKMP
IPSec
IPSec
IPSec
IPSec
IPSec
IPSec
IPSec
IPSec
IPSec
ISAKMP
DATA (VARIABLE LENGTH)
ISAKMP
0 4 8 16 Bits
INITIATOR COOKIE:0x0000000000000000
RESPONDER COOKIE:0x0000000000000000
NEXT PAYLOAD:12
VERSION:1
EXCHANGE TYPE:5
FLAGS:0x00
MESSAGE ID:0x00000000
LENGTH:28
Clear
Event List Filters - Visible Events
FTP, IPSec, ISAKMP

¿Existen mensajes de FTP que muestran la contraseña de Internet o la carga del archivo PrivateInfo.txt?

No existen paquetes que puedan incluso indicar el uso del protocolo ftp al IPSEC encapsular los datos

Creación de clave publica .pem con openssl

Como parte del contenido de la practica se demanda el hacer uso de Kali Linux y por ello mismo haremos uso de wsl para ejecutarlo

Para ello usaremos el comando openssl genrsa -out keyprivada.pem 2048

Esto nos generara una clave privada con el nombre del archivo keyprivada.pem

```
└─$ cat keyprivada.pem
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDsRYN6B/obgi2v
Tv7Pmw7MnRJZN5SKvnv+lVWRE+YPwV0FLjiaEuu7sbHLEAly0NARYhCthdPy2jd/
0gs2FC4zpYvAN4yiCDHxRM/KgHROLzjRQkDx967WxeWo0IqaDVyyKiM0QD6kIdxA
6kQfWSYSuA09vbiZi6HhyWq/Acw2b8RGAzNZafNVayDcwbNhdO6E29GZRKHF4yQ7
YFFoB2Tsss+XH2DS1LHCm7/UQRCx0anHDWze/8Pz6BIydS1MD3ToRCf4xFjZky0l
IIJ6/Iz0cAnrUgj3FBl2i6w97ASjRvCYG/4jREXsxMmH+9Gj9sUlaLtBxDRf24k2
52vB4bzPAgMBAAECggEAD35BcFucjXg8Wa4S7HctAcLdBKet4Gk8RUXynfhRkj/q
QyA0Svopph2xXHD5RaOmuTUWheJsMxUXJZUW8h1hqDZXUyvxV2C1Ma6C97LzrXrQ
PXycOKG2v9OrSyYdqJtutCoqM89wrB+iS0lxXSLh6cFS8PUDaWIsI9uq2cqa4wjR
7Ubycq4AQUJ2Ai8pfAaCocAPWT5j1YY2Ge67ECRBlBD9W6q+5geixIfCafU0BQxV
Cdlz7Ui+zFQmCz+mEulhrfCIpI0Qo7q/3NZYHg3u8HDh490h21NBJBbIA/f7T4jW
HmXAHbuOmjsCJb0NV9pf4tR5hsICjBPBvVwGNeC0pQKBgQD/kSW//6MmkTwAq4TL
vvKk3grCHlyj93r2L8yMhdMSSR63BB/11ci9qEzFzOSgyBi7N1uoOrYjB14QoG0S
6eRlZM6HPE3V8WC56U5Otb9SzMpGmEcy9txLbphqdGL3A2ZwpNHmeo4mVeCIrT+l
uBKxYNRYn6I8NkFKibgqFerJ+wKBgQDsq/8nTXp+xjnzkO0Z9bpVT83O298FhpA7
nlY0SUU6Od5LWQ9ojzpuCBvADf8A8ySofyoVBEYMrkrH2ovKw+UH/RZ17jDsPPia
Rr1iqF/tQhPEpmiV0TYFDYZMUO/iI0dOwwQgkNBQY7b83vPdPFs7VvNCH9J8SFKB
Fu8+svgUPQKBgQCHL9VjMauw3AR8aj5NtI0PzvCr7HmetmuRzIkMEEItmwYnU4RA
ezy7rkomG5MYxZ/ncIoIfD4aW2xTqTjpV1XcmK1y9eBKemtrDFHC6vrwpqmdHDIV
cGXpdPAk57nt5huLHHR30X5eIvEp+1L+q1cgAxNwacjcxupUrnL/uCZBfwKBgQCe
388GuTITzEm2wYEIvjX5cvr7dAnAkdZczyubKdx4+8PH3N9FF3Dn0DWgtUSLhK0F
F2hOd3H2rUGx63mQAfTLahAb1mutCjjwh7A2fET45jSS/AqVF74lojCXJnYB3iDO
NIeevNe6P1XlZl1aFFxB91qQ9v+7QmlwEs9DzaxPGQKBgG1+fU5CWNZVoYhA7jpJ
44INgBuuGJkjkdJVK2K/lfTaGlzVFwyrC6q3RS6f8/XS8RlWxapEPJvOsdqgST0j
1MBH7ySB098HgiSi7ndqcCfRAVtOVVgH2xYPndR/Q3uEZnWqs2ddl6leTXBgijHQ
pPxLQgPtj8dSxmWGz2TNMhDN
-----END PRIVATE KEY-----
```

La key privada esta codificada en base64 que posteriormente posee un formato binario

Ahora en base a esta clave privada generaremos una clave publica

```
┌──(wizard23㉿ DESKTOP-DL1SVJD)-[/mnt/c/Users/user 2]
└─$  openssl rsa -pubout -in keyprivada.pem -out keypublica.pem
writing RSA key

┌──(wizard23㉿ DESKTOP-DL1SVJD)-[/mnt/c/Users/user 2]
└─$ cat keypublica.pem
```

```
┌──(wizard23㉿ DESKTOP-DL1SVJD)-[/mnt/c/Users/user 2]
└─$ cat keypublica.pem
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA7EWDegf6G4Itr07+z5sO
zJ0SWTeUir57/pVVkRPmD8FdBS44mhLru7GxyxAJctDQEWIQrYXT8to3f9ILNhQu
M6WLwDeMoggx8UTPyoB0Ti840UJA8feu1sXlqNCKmg1csiojNEA+pCHcQOpEH1km
ErgNPb24mYuh4clqvwHMNm/ERgMzWWnzVWsg3MGzYXTuhNvRmUShxeMkO2BRaAdk
7LLPlx9g0tSxwpu/1EEQsdGpxw1s3v/D8+gSMnUtTA906EQn+MRY2ZMtJSCCevyM
9HAJ61II9xQZdousPewEo0bwmBv+I0RF7MTJh/vRo/bFJWi7QcQ0X9uJNudrweG8
zwIDAQAB
-----END PUBLIC KEY-----
```

Podemos observar que posee el mismo formato.

Conclusiones

La práctica concluye demostrando la relevancia de los VPNs en la protección de datos corporativos, especialmente frente a posibles ataques que puedan comprometer la confidencialidad y autenticidad de la información. A través de la implementación de IPSEC y la observación del funcionamiento de protocolos como ESP, se comprueba cómo se cifran y autentican los datos, mitigando riesgos comunes en redes no seguras. Asimismo, se reconoce la importancia de avanzar hacia sistemas más seguros, eliminando prácticas inseguras como el uso de FTP sin cifrado. En resumen, esta experiencia enfatiza la necesidad de implementar soluciones robustas de seguridad, como VPNs y cifrados avanzados, para proteger la integridad de los sistemas corporativos.

Referencias:

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.

3. Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography Engineering: Design Principles and Practical Applications*. Wiley.

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