

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



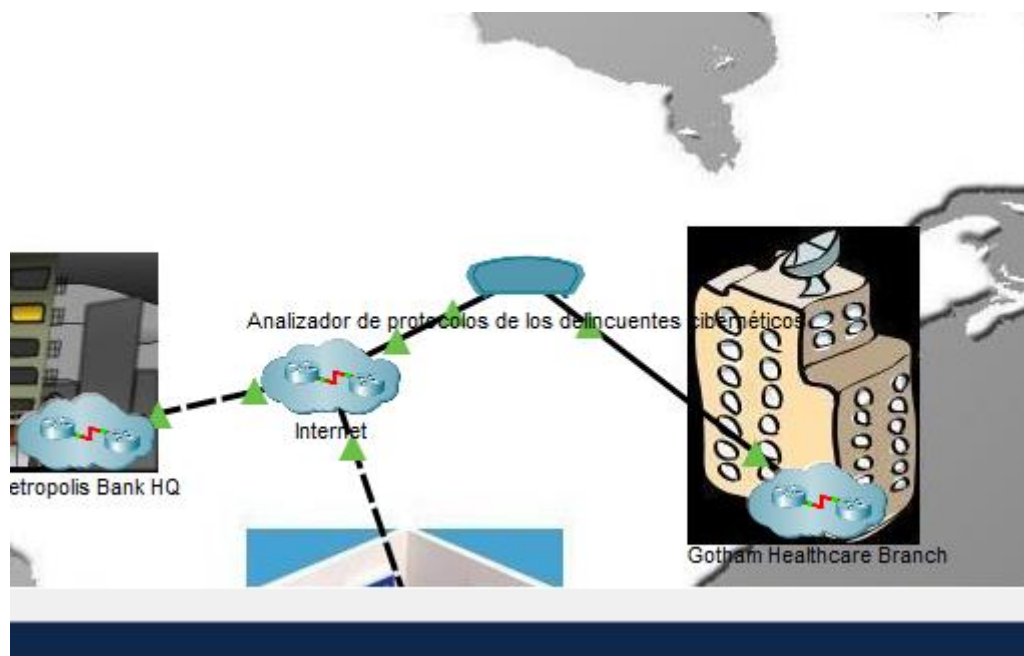
introducción

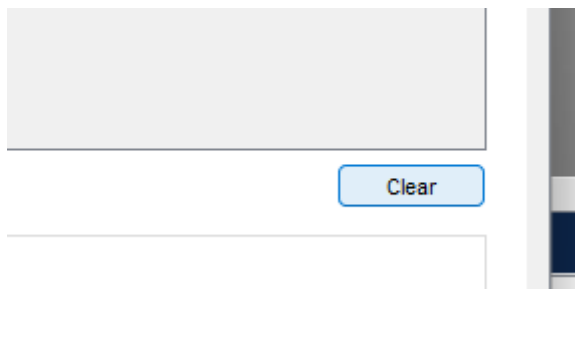
En esta práctica, nos adentramos en la configuración y análisis de un medio de transporte VPN dentro de un entorno corporativo simulado. El objetivo principal es identificar y comprender los elementos criptográficos que aseguran la transferencia de datos a través de redes inseguras. Mediante el uso de 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

The network diagram shows a central 'Metropolis Bank HQ' connected to 'Office 1'. The HQ has a 'Router in Ambrico' and an 'HQ Router'. Office 1 has a 'Switch_1' and a 'Sally' computer. A 'Network Closet' contains a 'Switch_2' and an 'FTPWeb' server. IP addresses 10.44.0.0/24 and 10.44.1.0/24 are indicated. The interface includes a toolbar, a status bar with 'Time: 00:01:51.777', and a 'PLAY CONTROLS' section with buttons for 'Event List', 'Realtime', and 'Simulation'.

PT Activity: 00:04:10

y enviar el tráfico de FTP cifrado. La asignación de direcciones IP, la configuración de direcciones de servicio ya están completas. Utilizará un dispositivo cliente en Bank HQ para transferir datos de FTP cifrados y no cifrados.

Parte 1: enviar tráfico de FTP no cifrado

Paso 1: acceda al analizador de protocolos de delincuentes cibernéticos

- Haga clic en el Analizador de protocolos de delincuentes cibernéticos en la ficha GUI.
- Haga clic en el botón Borrar para eliminar todas las entradas de tráfico pos el analizador de protocolos.
- Minimice el Analizador de protocolos de delincuentes cibernéticos.

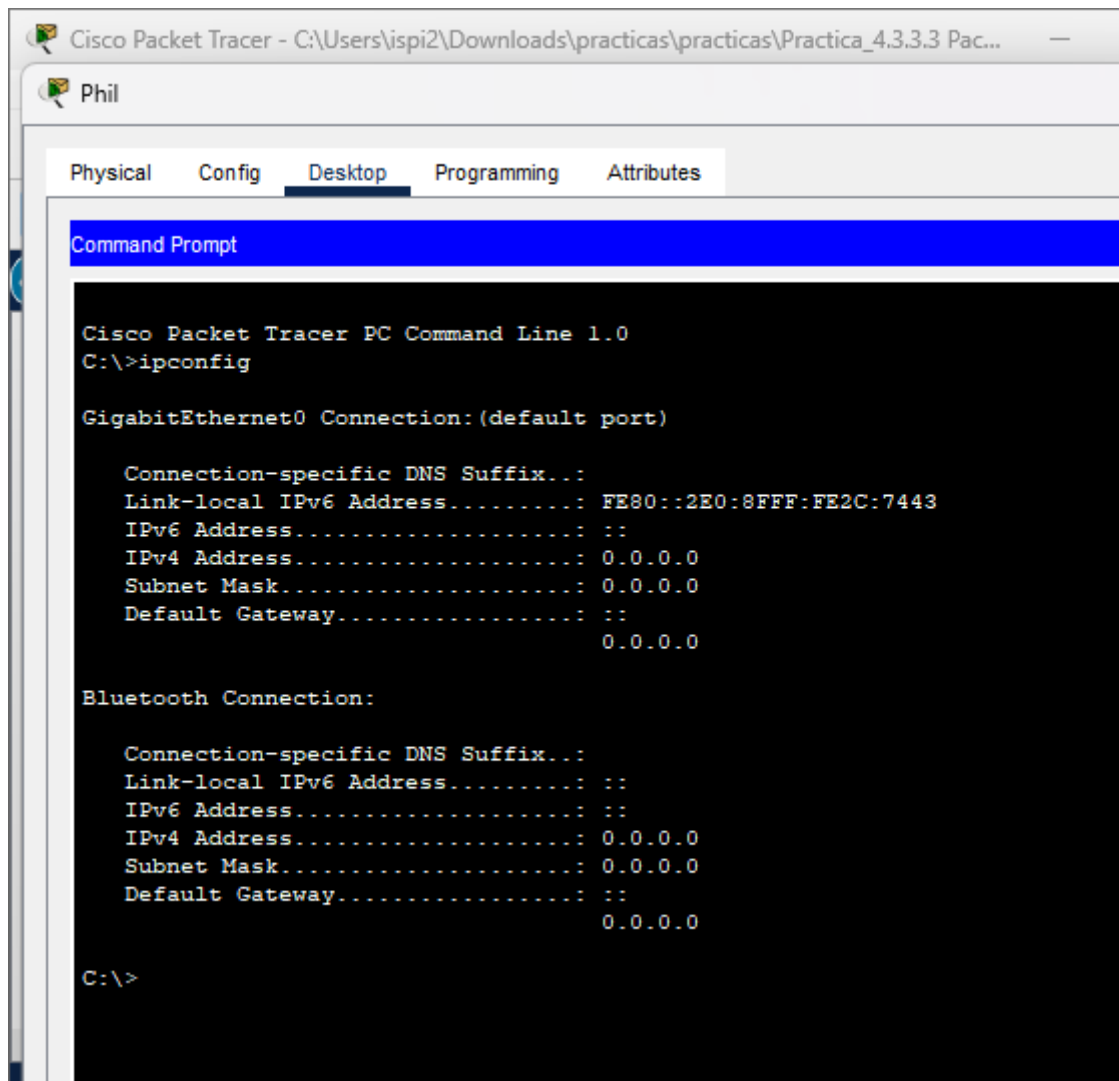
Paso 2: conéctese al servidor Public_FTP mediante una conexión insegura.

- Haga clic en el sitio Metropolis Bank HQ y luego haga clic en la pc portátil
- Haga clic en la ficha Escritorio y luego haga clic en Petición de ingreso d
- Utilice el comando ipconfig para ver la dirección IP actual de la computado
- Conéctese al servidor Public_FTP en Gotham Healthcare Branch al introc 209.165.201.20 en la petición de ingreso de comandos.
- Introduzca el nombre de usuario cisco y la contraseña publickey para inici servidor Public_FTP.
- Utilice el comando put para cargar el archivo PublicInfo.txt al servidor Pub

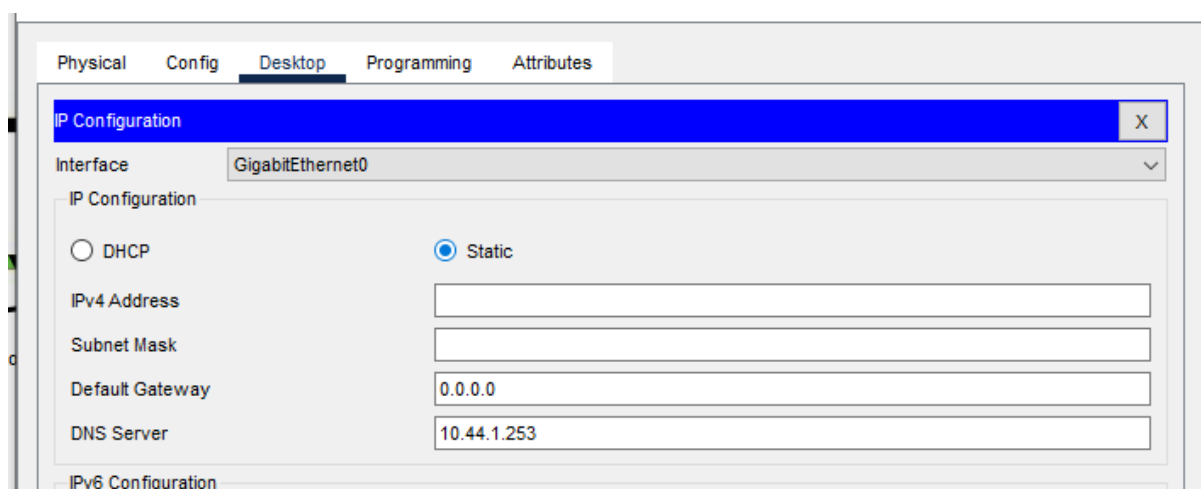
Paso 3: vea el tráfico en el analizador de protocolos de delincuer cibernéticos.

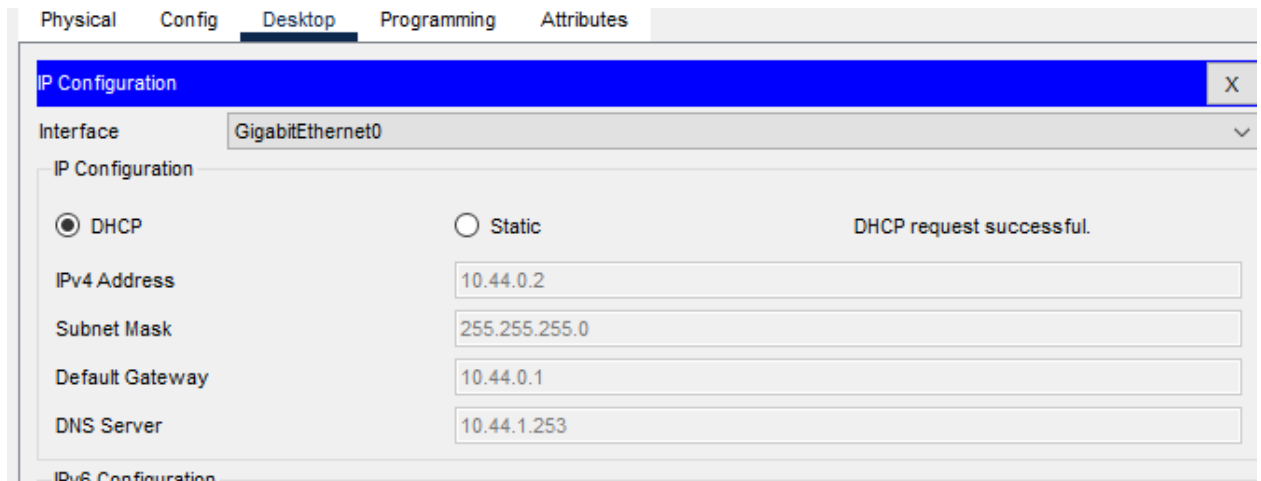
- Maximice el Analizador de protocolos de delincuentes cibernéticos que previamente.
- Haga clic en los mensajes de FTP que se muestran en el analizador de prot desplácese hasta la parte inferior de cada uno.

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 logeo 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:

```
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>
ftp>
ftp>dir

Listing /ftp directory from 209.165.201.20:
```

```
Invalid or non supported command.
ftp>
ftp>put PublicInfo.txt

Writing file PublicInfo.txt to 209.165.201.20:
File transfer in progress...

[Transfer complete - 346 bytes]

346 bytes copied in 0.01 secs (34600 bytes/sec)
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:

Physical Config **GUI** Attributes

Service ☒ On ☐ Off

Incoming Packets ☐ Port0 ☒ Port1

Buffer Size

FTP

FTP

FTP

FTP

FTP

FTP

FTP

FTP

FTP

FTP

FTP

FTP

FTP

FTP

FTP

ACKNOWLEDGEMENT NUMBER:53			
OFFSET: 0x0	RESERV ED: 0	FLAGS:0b00011000	WINDOW:65535
CHECKSUM:0x0000		URGENT POINTER:0x0000	
OPTION			
DATA (VARIABLE LENGTH)		PADDING: 0	
FTP Command			
0 4 8 16 Bytes			
FTP Command:USER			
FTP Argument:cisco			

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

Physical Config **Desktop** Programming Attributes

106

IP Configuration

Dial-up

Terminal

Command Prompt

Web Browser

PC Wireless

Open the VPN client application.

VPN

Traffic Generator

MIB Browser

Cisco IP Communicator

ara así cifra

Physical Config **Desktop** Programming Attributes

VPN Configuration X

VPN

GroupName: VPNGROUP

Group Key: 123

Host IP (Server IP): 209.165.201.20

Username: phil

Password: ••••••••

Connect

Introduciremos los datos de conexión al vpn

Physical Config **Desktop** Programming Attributes

VPN Configuration X

Client IP: 10.44.2.200

Disconnect

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 multicasts 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 realizar 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 clave 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.

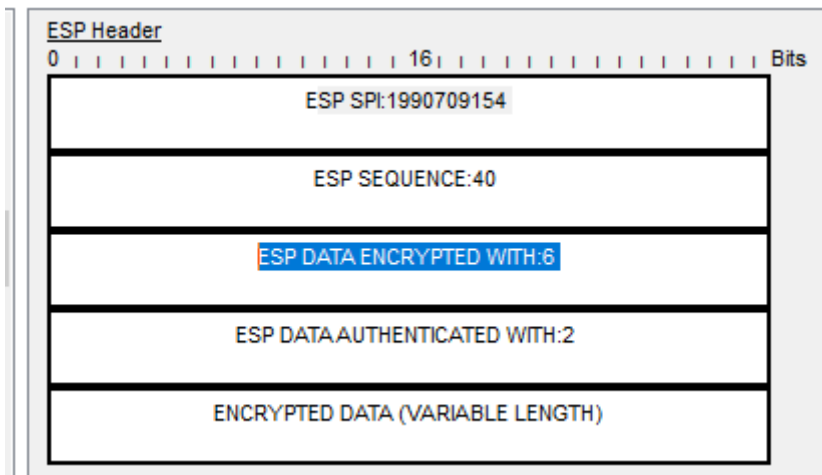
IPSEC provee de múltiples formas de funcionamiento o configuraciones:

- **AH:** este es el encabezado de autenticación únicamente proporciona la confidencialidad de los datos, pero el texto se transporta como no cifrado
- **ESP:** permite la autenticación y cifrado de los datos, permite ocultar tanto la dirección de envío 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 sería 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

```

Default Gateway.....: 10.44.0.1

Bluetooth Connection:

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::
Tunnel Interface IP Address.....: 10.44.2.201

C:\>ping 10.44.2.201

Pinging 10.44.2.201 with 32 bytes of data:

Reply from 10.44.2.201: bytes=32 time=9ms TTL=127
Reply from 10.44.2.201: bytes=32 time=11ms TTL=127

```

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

```
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>
```

Subiremos nuevamente el archivo private info.log

```
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 PrivateInfo.txt

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

[Transfer complete - 668 bytes]

668 bytes copied in 0.1 secs (6680 bytes/sec)
ftp>
```

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 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 <input type="checkbox"/> RE <input type="checkbox"/> FS <input type="checkbox"/> SE <input type="checkbox"/>	FLAGS:0b0010000 WINDOW:65535
	CHECKSUM:0x0000	URGENT POINTER:0x0000
	OPTION	
	DATA (VARIABLE LENGTH)	
	PADDING: 0	
	Clear	

Event List Filters - Visible Events

Physical	Config	GUI	Attributes
Service		<input checked="" type="radio"/> On <input type="radio"/> Off	
Incoming Packets		<input type="radio"/> Port0 <input checked="" type="radio"/> 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 IPsec ISAKMP	DATA (VARIABLE LENGTH)		
	ISAKMP		
	0 4 8 16 Bits		
	INITIATOR COOKIE:0x0000000000000000		
	RESPONDER COOKIE:0x0000000000000000		
	NEXT PAYL OAD: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



```
wizard23@DESKTOP-DL1SVJD: /mnt/c/Users/user 2
(Message from Kali developers)
This is a minimal installation of Kali Linux, you likely
want to install supplementary tools. Learn how:
  https://www.kali.org/docs/troubleshooting/common-minimum-setup/
(Run: "touch ~/.hushlogin" to hide this message)
(wizard23@DESKTOP-DL1SVJD)-[/mnt/c/Users/user 2]
$ openssl genrsa -out keyprivada.pem 2048
(wizard23@DESKTOP-DL1SVJD)-[/mnt/c/Users/user 2]
$ _
```

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

```

$ cat keyprivada.pem
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKggggSkAgEAAoIBAQDsRYN6B/obgi2v
Tv7Pmw7MnRJZN5SKvnnv+1VWRE+YPwV0FLjiaEuu7sbHLEAlY0NARYhCthdPy2jd/
0gs2FC4zpYvAN4yiCDHxRM/KgHR0LzjRQkDx967WxeWo0IqaDVyyKiM0QD6kIdxA
6kQfWSYsuA09vbiZi6HhyWq/Acw2b8RGaZnZafNVayDcwbNhd06E29GZRKHf4yQ7
YFFoB2TssS+XH2DS1LHCm7/UQRCx0anHDWze/8Pz6BIydS1MD3ToRCf4xFjZky0l
IIJ6/Iz0cAnrUgj3FB12i6w97ASjRvCYG/4jREXsxMmH+9Gj9sUlaLtBxDRf24k2
52vB4bzPAGMBAECggEAD35BcFucjXg8Wa4S7HctAcLdBKet4Gk8RUXynfhRkj/q
QyA0Svopph2xXHD5Ra0muTUWheJsMxUXJZUW8h1hqDZXUyvxV2C1Ma6C97LzrXrQ
PXycOKG2v90rSyYdqJtutCoqM89wrB+iS0lxXSLh6cFS8PUDaWiS19uq2cqa4wjR
7Ubycq4AQUJ2Ai8pfAaCocAPWT5j1YY2Ge67ECRBLBD9W6q+5geixIfCafU0BQxV
Cd1z7Ui+zFQmCz+mEulhrfCIpI0Qo7q/3NZYHg3u8HDh490h21NBjBbIA/f7T4jw
HmXAHbuOmjsCjB0NV9pf4tR5hsICjBPBvVwGNeC0pQKBgQD/kSW//6MmkTwAq4TL
vvKk3grCHlyj93r2L8yMhdMSSR63BB/11ci9qEzFz0SgyBi7N1uoOrYjB14QoG0S
6eR1ZM6HPE3V8WC5U50tb9SzMpGmEcy9txLbphqdGL3A2ZwpNHmeo4mVeCIrT+l
uBKxYNRYn6I8NkFKibgqFerJ+wKBgQDsQ/8nTXp+xjnzK00Z9bpVT830298FhpA7
nly0SUU60d5LWQ9ojzpuCBvADf8A8ySofyoVBEYMrkrH2ovKw+UH/RZ17jDsPPia
Rr1iqF/tQHPEpmiV0TYFDYZMUO/iI0dOwwOgkNBQY7b83vPdPFs7VvNCH9J8SFKB
Fu8+svgUPQKBgQCHL9VjMauw3AR8aj5NtI0PzvCr7HmetmuRzIkMEEItmwYnU4RA
ezy7rk0mG5MYxZ/ncIoIfD4aw2xTqTjpV1XcmK1y9eBKemtrDFHC6vrwpqmdHDIV
cGXpdPAK57nt5huLHHR30X5eIvEp+1L+q1cgAxNwacjcxupUrnL/uCZBfwKBgQCe
388GuTITzEm2wYEIvJX5cvr7dAnAkdZczyubKdx4+8PH3N9FF3Dn0DWgtUSLhK0F
F2h0d3H2rUGx63mQAfTLahAb1mutCjjwh7A2fET45jSS/AqVF74lojCXJnYB3iD0
NIeevNe6P1X1Z11aFFx891qQ9v+7QmlwEs9DzaxPGQKBG1+fU5CWNVVoYhA7jpJ
44INGBuUGJkjdJVK2K/lfTaG1zVFwyrC6q3RS6f8/XS8RlWxapEPJv0sdqgST0j
1MBH7ySB098Hgisi7ndqcCFRAvtOVVgH2xYPndR/Q3uEZnWqs2dd16leTXBgijHQ
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+z5s0
zJ0SWTeUir57/pVVkRPmD8FdBS44mhLru7GxyxAJctDQEWIQRyXT8to3f9ILNhQu
M6WLwDeMoggx8UTPyoB0Ti840UJA8feu1sXlqNCKmg1csiojNEA+pChcQ0pEH1km
ErgNPb24mYuh4clqvWMMNm/ERgMzWwzVWsg3MGzYXTuhNvRmUShxeMk02BRaAdk
7LLPlx9gtSxwpu/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>