Capture The Flag

SSH

I.E.S Fernando III - 6 mayo 2022

01
¿QUÉ ES SSH?

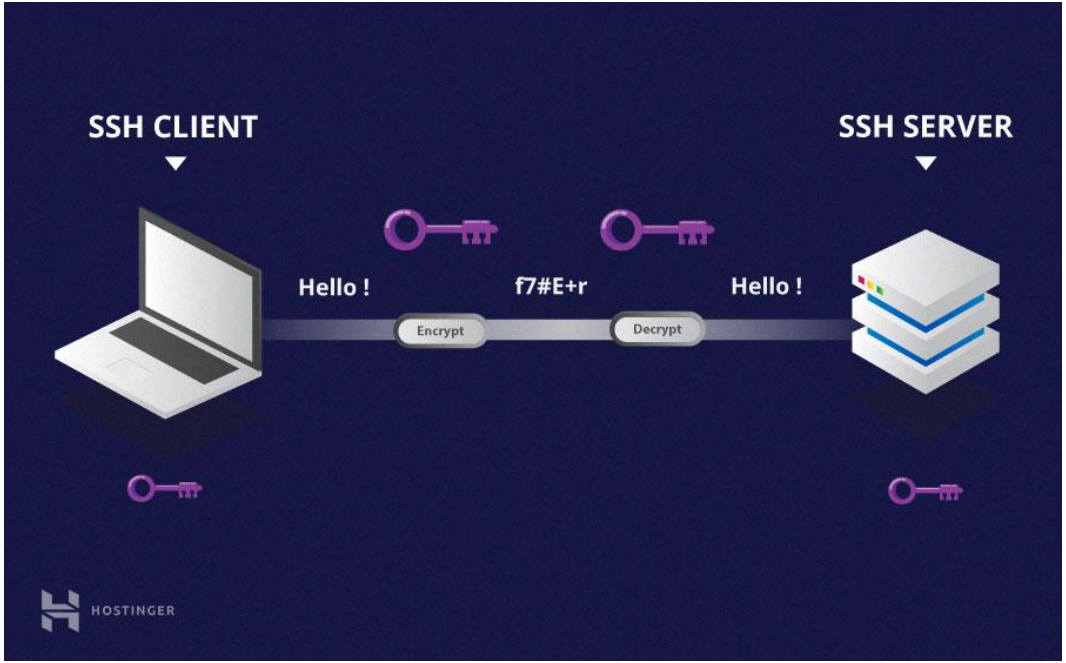
Secure SHell (SSH)

Protocolo de administración remota que permite a los usuarios **controlar y modificar servidores remotos** de Internet a través de un mecanismo de **autentificación**

02

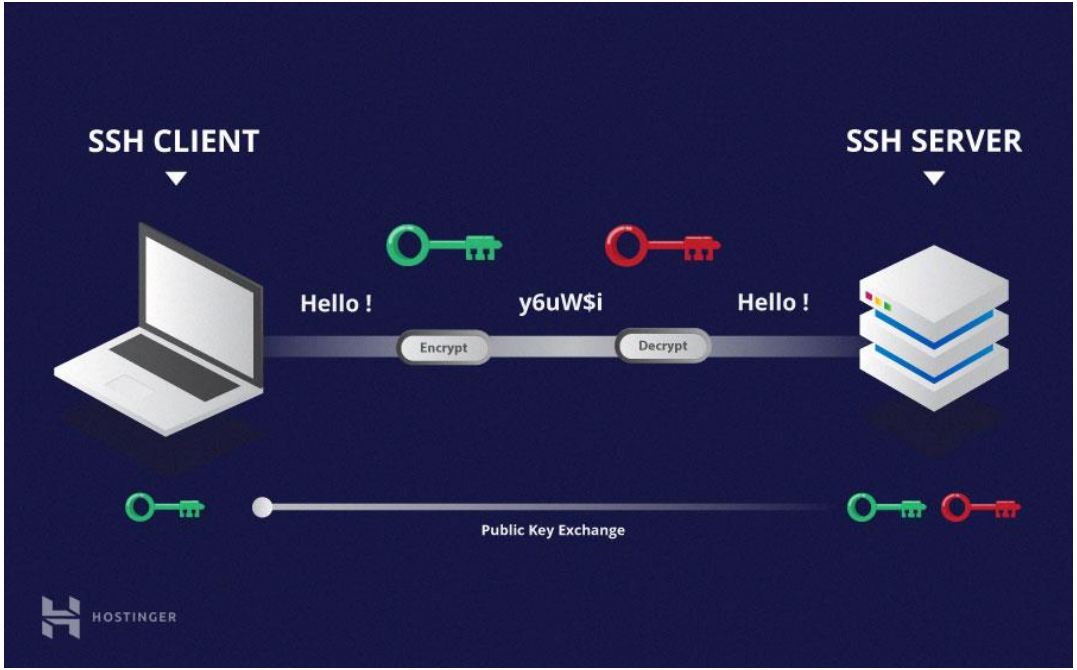
CIFRADOS

Cifrado simétrico (clave secreta)



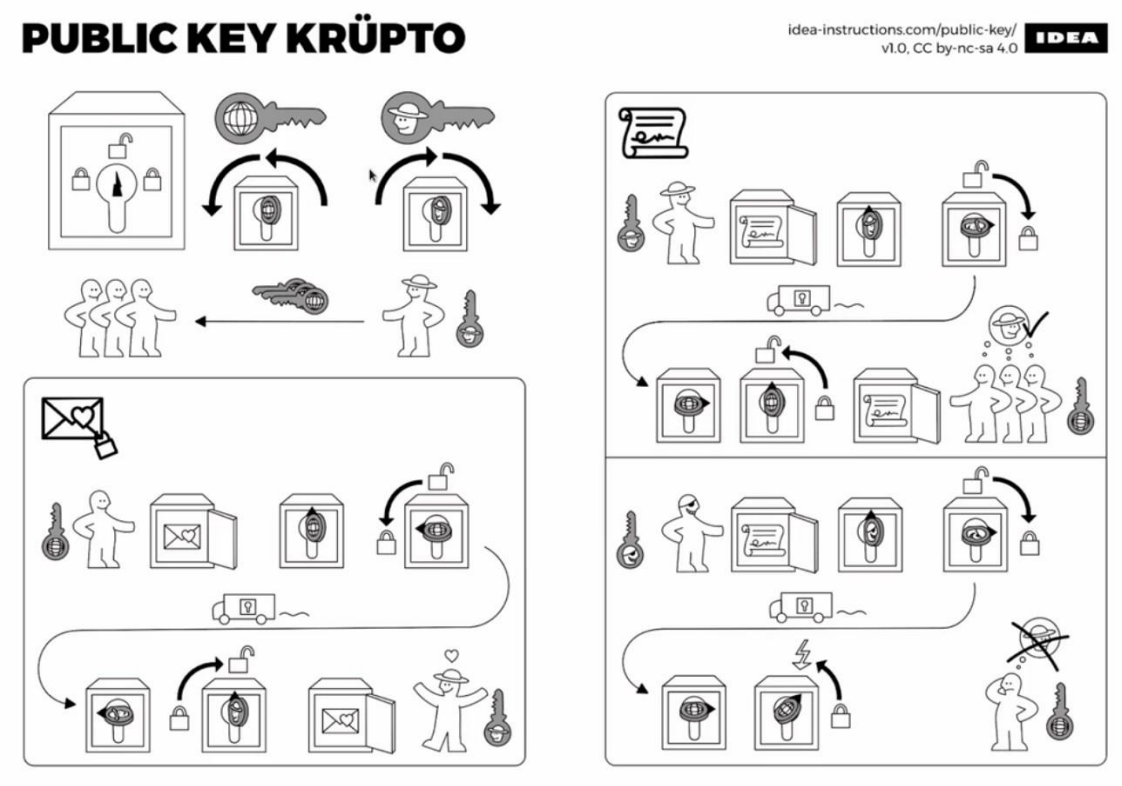
Fuente: https://www.hostinger.es/tutoriales/que-es-ssh

Cifrado asimétrico (par de claves pública-privada)



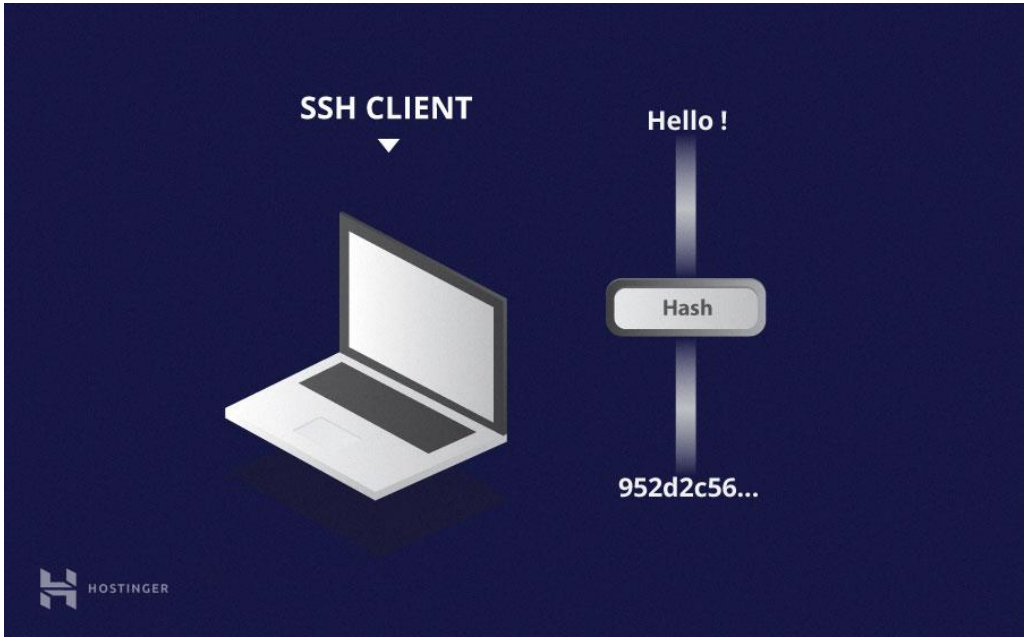
Fuente: https://www.hostinger.es/tutoriales/que-es-ssh

Cifrado asimétrico (par de claves pública-privada)



Fuente: https://idea-instructions.com/public-key/

Hashing



Fuente: https://www.hostinger.es/tutoriales/que-es-ssh

03

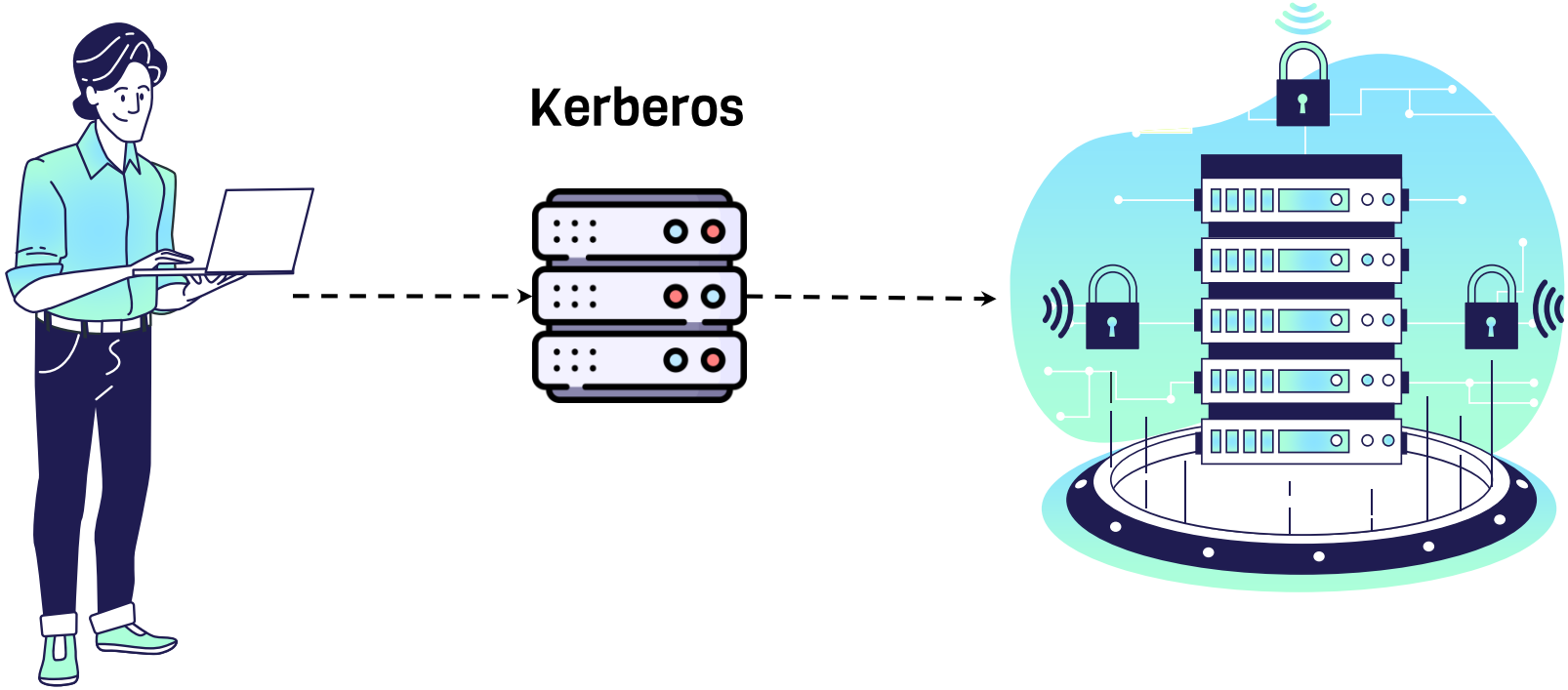
FORMAS DE AUTENTICACIÓN

Contraseña

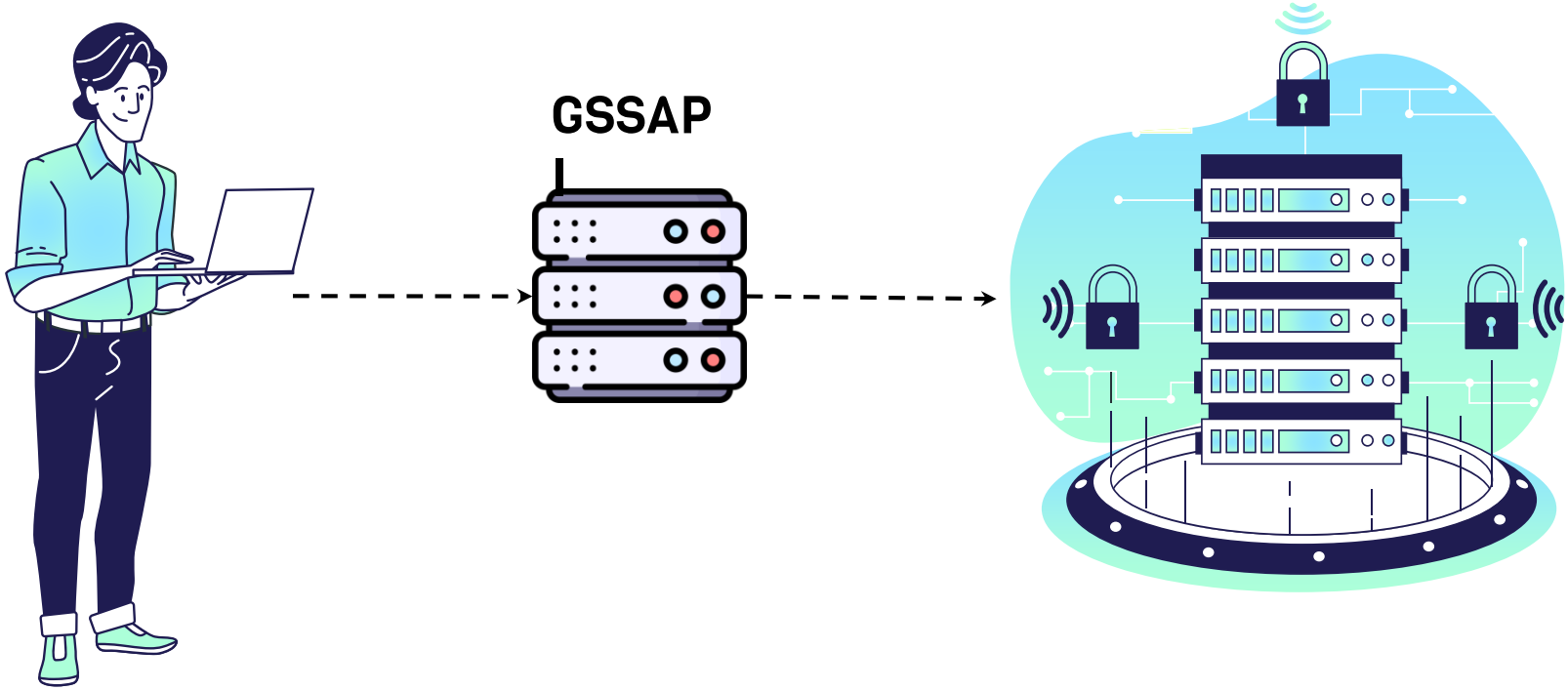
Usuario: Pepe
Contraseña: ********

Clave pública

Servidor kerberos



GSSAPI



04

¿CÓMO FUNCIONA?

NEGOCIACIÓN Y AUTENTICACIÓN

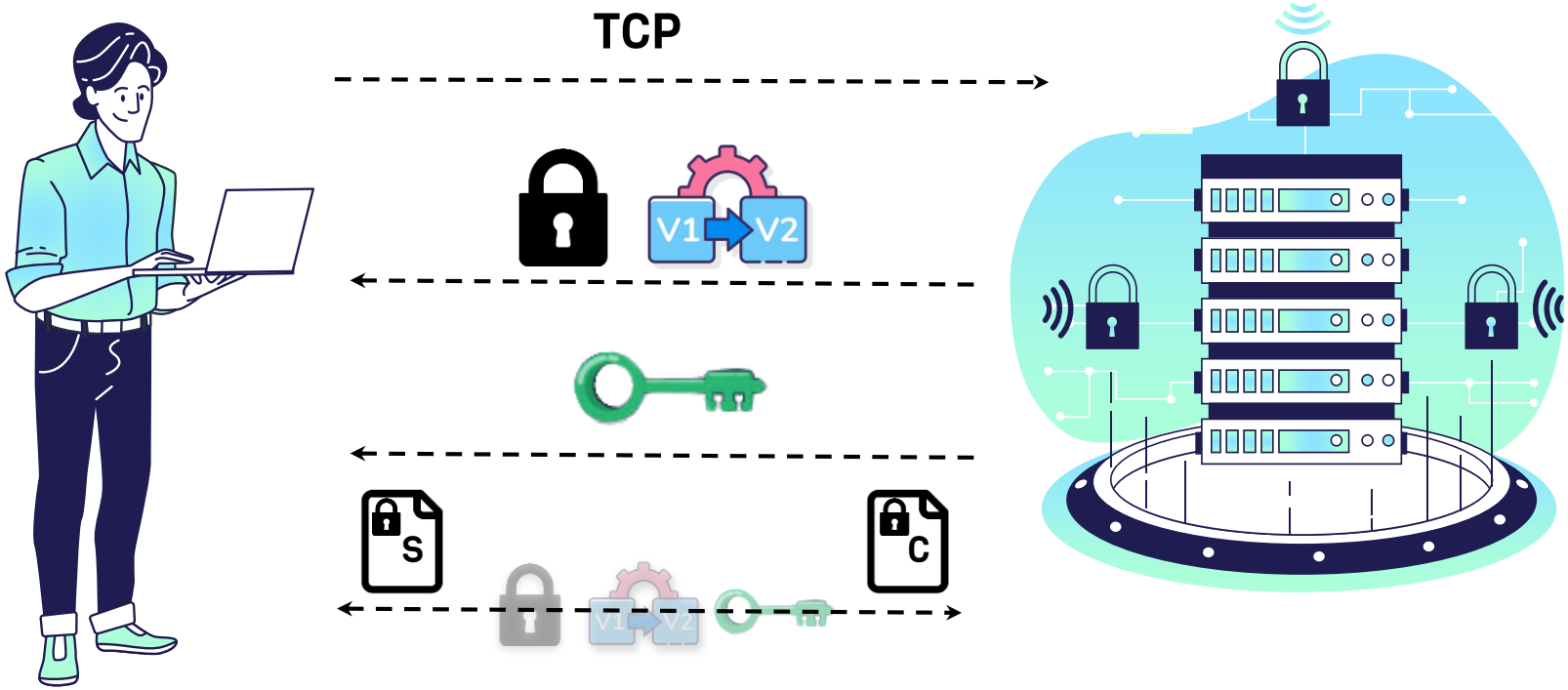
1

NEGOCIACIÓN

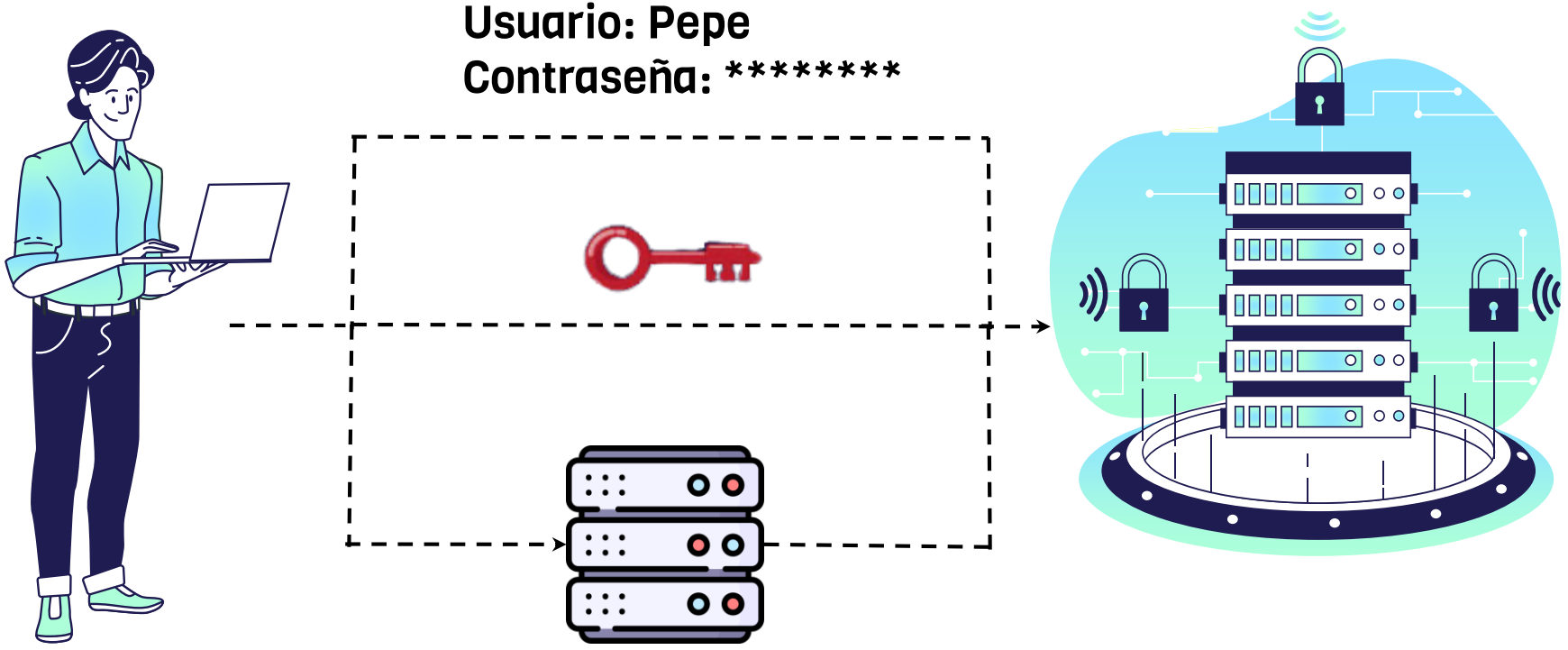
2

AUTENTICACIÓN

Fase 1: NEGOCIACIÓN



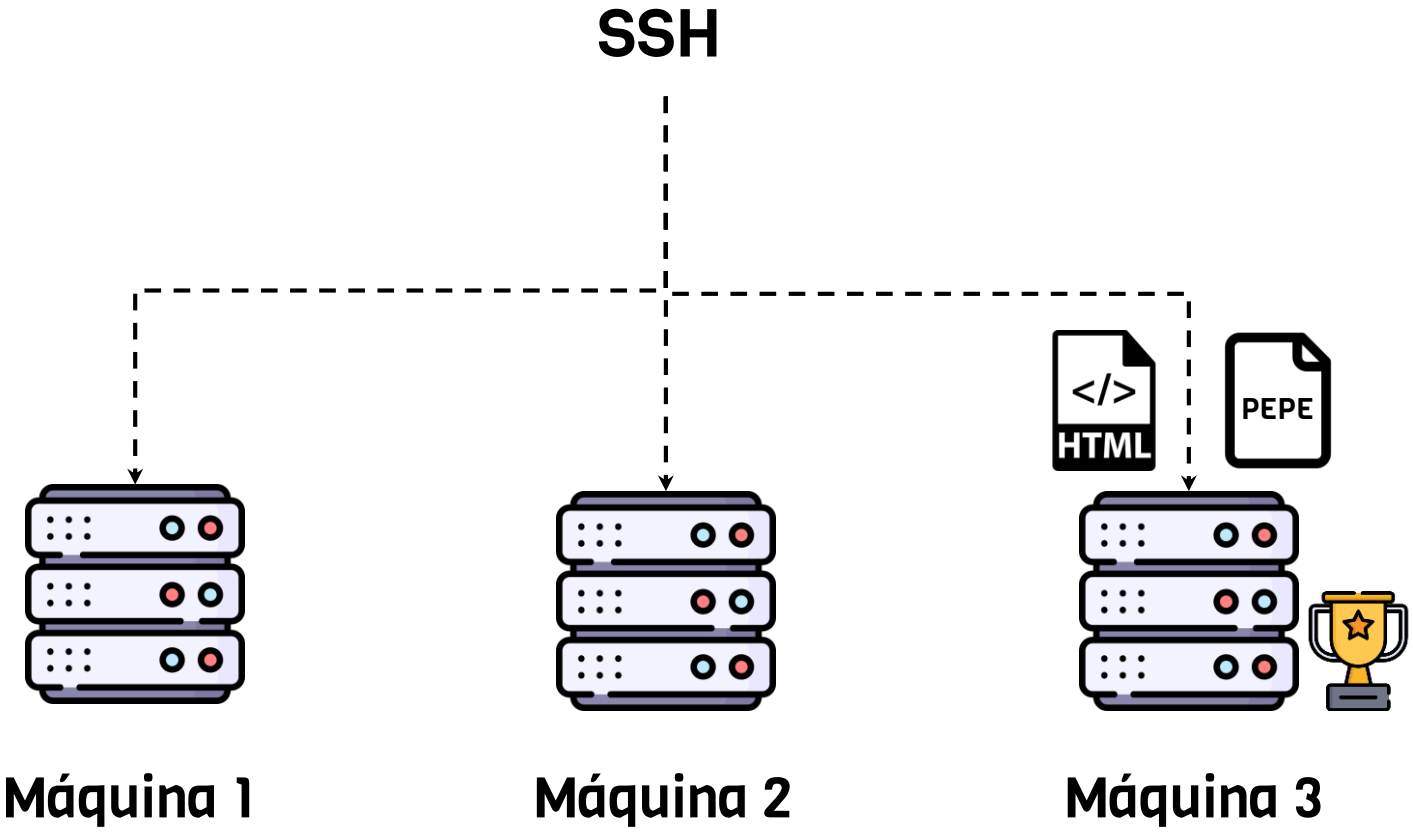
Fase 2: AUTENTICACIÓN



05

CTF SSH

CTF SSH



PRIMERA PRUEBA

- Máquina 1
  - Host: falcondptoinformatica.synology.me
  - Puerto: 22
  - Usuario: Eladio, Ana, Loli, Guillermo, Antonio, Carlos
  - Contraseña: Se encuentra entre las 200 contraseñas más utilizadas en España en el año 2020 (fichero pass_csv.csv)

- Araña en Java que realice un ataque de diccionario para conseguir el usuario y la contraseña de la máquina
- Conexión SSH mediante terminal a la máquina 1
- Abrir o descargar el fichero *instrucciones_máquina_2.txt* para ver la siguiente prueba

ANEXO I

Cómo utilizar SSH

Autenticación con usuario y contraseña

```
ssh usuario@maquina -p <puerto>
```

Autenticación con usuario y contraseña

Ejemplo

```
ssh paco@192.168.0.56
```

```
ssh isabel@serverdpto.me -p 56
```

Autenticación con clave pública

Generar claves

```
ssh-keygen -t <algoritmo>
```

Autenticación con clave pública

Ejemplo

```
ssh-keygen -t ecdsa
```

Autenticación con clave pública

Copiar clave pública (Linux)

```
ssh-copy-id -i <ruta_fichero_identidad> usuario@maquina
```

Autenticación con clave pública

Ejemplo

```
ssh-copy-id -i id_ecdsa paco@192.168.0.56
```

Autenticación con clave pública

Copiar clave pública (Windows)

```
type <fichero_clave_pub> | ssh usuario@maquina "cat >> .ssh/authorized_keys"
```

Autenticación con clave pública

Ejemplo

```
type id_ecdsa.pub | ssh paco@192.168.0.56 "cat >> .ssh/authorized_keys"
```

Autenticación con clave pública

Conexión indicando clave privada

```
ssh -i <ruta_clave_privada> usuario@maquina -p <puerto>
```

Autenticación con clave pública

Ejemplo

```
ssh -i ~/.ssh/miclaveprivada paco@192.168.0.56
```

Transferencia de ficheros

```
scp usuario@maquina_origen:ruta usuario@maquina_destino:ruta
```

Transferencia de ficheros

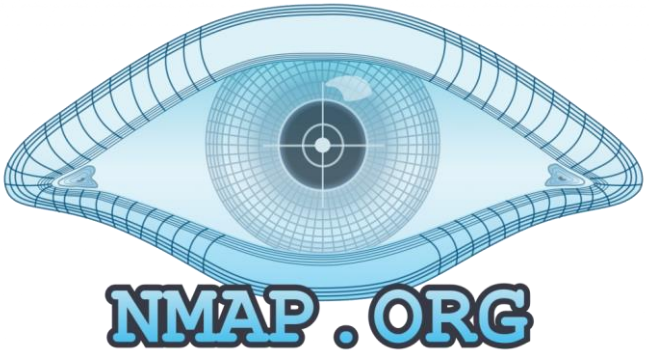
Ejemplo

```
scp paco@192.168.0.56:/home/paco/examen.docx .
```

```
scp ./notas.xslx paco@192.168.0.56:/home/paco/
```

ANEXO II

Cómo utilizar Nmap



Escaneo de puertos con Nmap

Puertos más comunes

namp <dirección-ip>

Escaneo de puertos con Nmap

Ejemplo

namp 192.168.0.56

namp serverdpto.me

Escaneo de puertos con Nmap

Rango de puertos

namp -p <p-inicio>-<p-fin> <dirección-ip>

Escaneo de puertos con Nmap

Ejemplo

namp -p 0-400 192.168.0.56

Escaneo de servicios con Nmap

```
namp -sV <dirección-ip>
```

Escaneo de servicios con Nmap

Ejemplo

namp -sV 192.168.0.56

ANEXO III

Github

!SUERTE!