

CURSO ONLINE DE CIBERSEGURIDAD__

Especialidad Administración de
Sistemas de Ciberseguridad

Taller 3

Unidad 5. Seguridad en
administración de sistemas



VICEPRESIDENCIA
PRIMERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL

 **incibe**

INSTITUTO NACIONAL DE CIBERSEGURIDAD



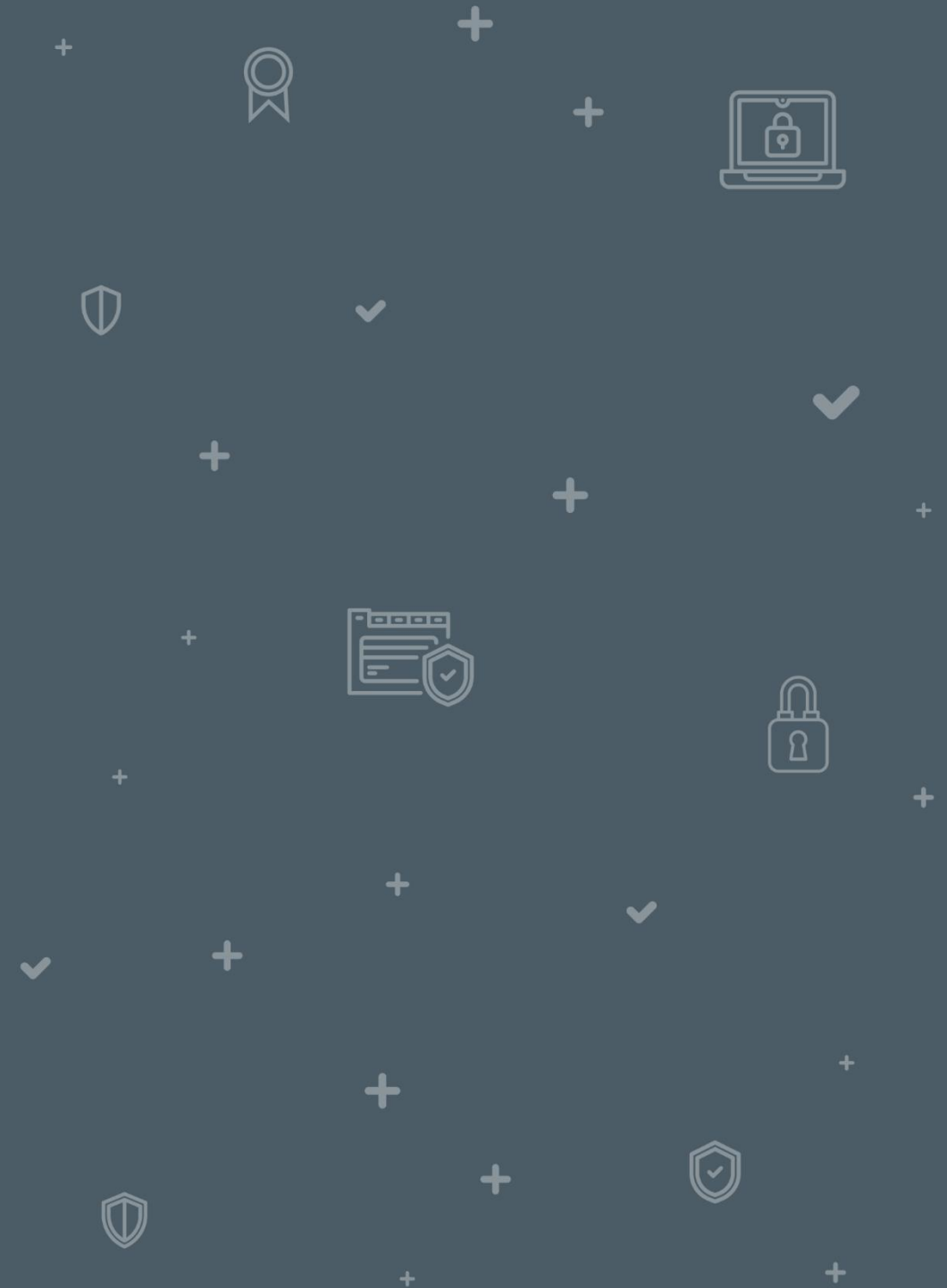
Contenidos

1	LOS ATAQUES POR FUERZA BRUTA Y DICCIONARIO	3
2	CONSIDERACIONES PREVIAS	5
3	ENUNCIADO EJERCICIO PRÁCTICO 1	14
4	SOLUCIONARIO EJERCICIO PRÁCTICO 1	16

Duración total del taller: 1 hora

LOS ATAQUES POR FUERZA BRUTA Y DICCIONARIO

1



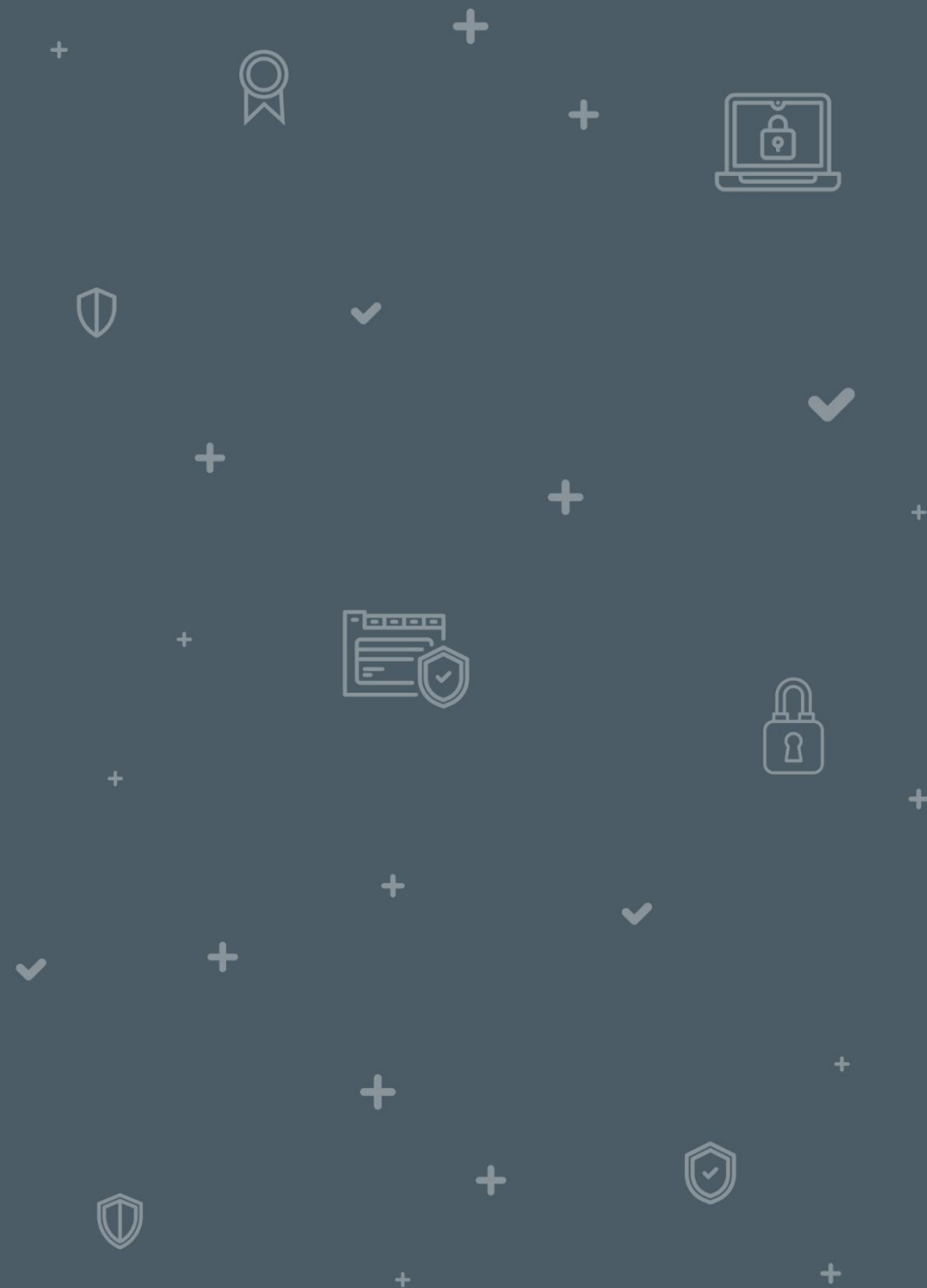
1 LOS ATAQUES POR FUERZA BRUTA Y DICCIONARIO

En este taller, vas a utilizar la herramienta **John the Ripper**, una herramienta para crackear los *hashes* MD5, SHA-1, etc., de las contraseñas por fuerza bruta y por diccionario. Esta herramienta es de las más populares en el ámbito de realizar ataques por fuerza bruta.

El ejercicio práctico consistirá en crackear un *hash* obtenido de un archivo .zip con contraseña, el cual se quiere descomprimir para ver el contenido.

2

CONSIDERACIONES PREVIAS



2 CONSIDERACIONES PREVIAS

- En primer lugar, abre tu máquina Kali Linux y comprueba que la herramienta John the Ripper está instalada y actualizada.
 - Para ello, abre una terminal y ejecuta el comando **sudo apt install john**.

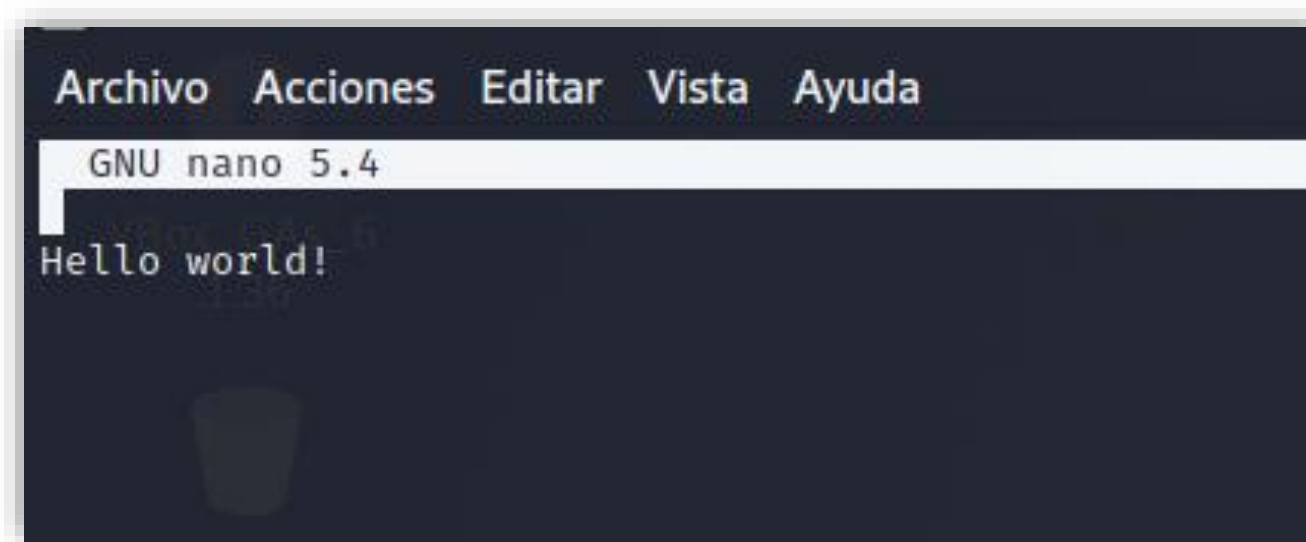
```
(incibe@kali)-[~]Escritorio
└─$ sudo apt install john
[sudo] password for incibe:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
john ya está en su versión más reciente (1.9.0-Jumbo-1+git20211102-0kali3+b1).
fijado john como instalado manualmente.
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
```

Ilustración 1: Ejecución del comando sudo apt install john.

- Una vez que has comprobado que la herramienta está instalada y actualizada, puedes comenzar a utilizarla.

2 CONSIDERACIONES PREVIAS

- A continuación, crea un archivo comprimido con contraseña para poder utilizarlo como ejemplo. Para ello, crea un archivo de texto con cualquier contenido aleatorio, y dale el nombre que quieras, nosotros le hemos dado el nombre «Test.txt». Con el comando **nano** abrirás el editor de texto e introducirás el texto.



```
Archivo  Acciones  Editar  Vista  Ayuda
GNU nano 5.4
Hello world!
```

Ilustración 2: Ejecución del editor de texto con el comando *nano*. Introducción de un contenido aleatorio.

2 CONSIDERACIONES PREVIAS

- Guarda el archivo de texto pulsando «Ctrl + O» y ciérralo con «Ctrl + X».
- Ahora, comprime el archivo de texto con contraseña.
 - Para ello, utiliza el comando **sudo zip --encrypt nombre_archivo_comprimido.zip nombre_fichero_creado.extensión**
 - En nuestro caso, el comando es el siguiente **sudo zip --encrypt Test.zip Test.txt**

```
(incibe@kali)-[~/Descargas]
$ sudo zip --encrypt Test.zip Test.txt
[sudo] password for incibe:
Enter password:
Verify password:
  adding: Test.txt (stored 0%)
```

Ilustración 3: Ejecución del comando
sudo zip --encrypt Test.zip Test.txt

2 CONSIDERACIONES PREVIAS

- En este caso, se añade **sudo**, ya que se necesitan permisos de administrador para comprimir este archivo, por lo que te solicitará la contraseña de *root* de tu equipo y después la contraseña que quieras poner al archivo .zip.
- Para comprobar que se ha realizado bien la compresión del archivo utiliza el comando **unzip** indicando el nombre del archivo a descomprimir. A continuación, te solicitará la contraseña que has introducido anteriormente.

```
(incibe@kali)-[~/Descargas]  
$ unzip Test.zip  
Archive:  Test.zip  
[Test.zip] Test.txt password: 
```

Ilustración 4: Solicitud de contraseña.

2 CONSIDERACIONES PREVIAS

- Con el archivo comprimido con contraseña, ya puedes obtener el *hash* de la contraseña que elegiste para el archivo .zip.
 - Para ello, introduce en la terminal el comando **zip2john Test.zip > hash.tmp**

```
(incibe@kali)-[~/Descargas]
$ zip2john Test.zip > hash.tmp
ver 1.0 efh 5455 efh 7875 Test.zip/Test.txt PKZIP Encr: 2b chk, TS_chk, cmplen=26, decmplen=14, crc=BE51019F ts=6092 cs=6092 type=0
```

Ilustración 5: Ejecución del comando zip2john Test.zip > hash.tmp

2 CONSIDERACIONES PREVIAS

- Ya tienes el *hash* guardado en el documento que, en este caso, se ha denominado **hash.tmp**. Ahora ya puedes intentar crackearlo.
- Al ser un archivo comprimido, el *hash* que crea la herramienta de la contraseña es un tipo especial denominado PKZIP, el cual solo puede crackearse con la herramienta John the Ripper de la siguiente manera: **sudo john hash.tmp**

```
(incibe@kali)-[~/Descargas]
$ cat hash.tmp
Test.zip/Test.txt:$pkzip$1*2*2*0*1a*e*be51019f*0*42*0*1a*6092*0c77641cbfd9bed963b12c5ce063c930514fda60e72d3cb20861*$/pkzip$:Test.txt:Test.zip::Test.zip
```

Ilustración 6: Archivo hash.tmp

2 CONSIDERACIONES PREVIAS

```
(incibe@kali)-[~/Descargas]
$ sudo john hash.tmp
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
admin (Test.zip/Test.txt)
1g 0:00:00:00 DONE 2/3 (2022-08-18 13:16) 6.250g/s 172000p/s 172000c/s 172000C/s 123456..Peter
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Ilustración 7: Comando sudo john hash.tmp

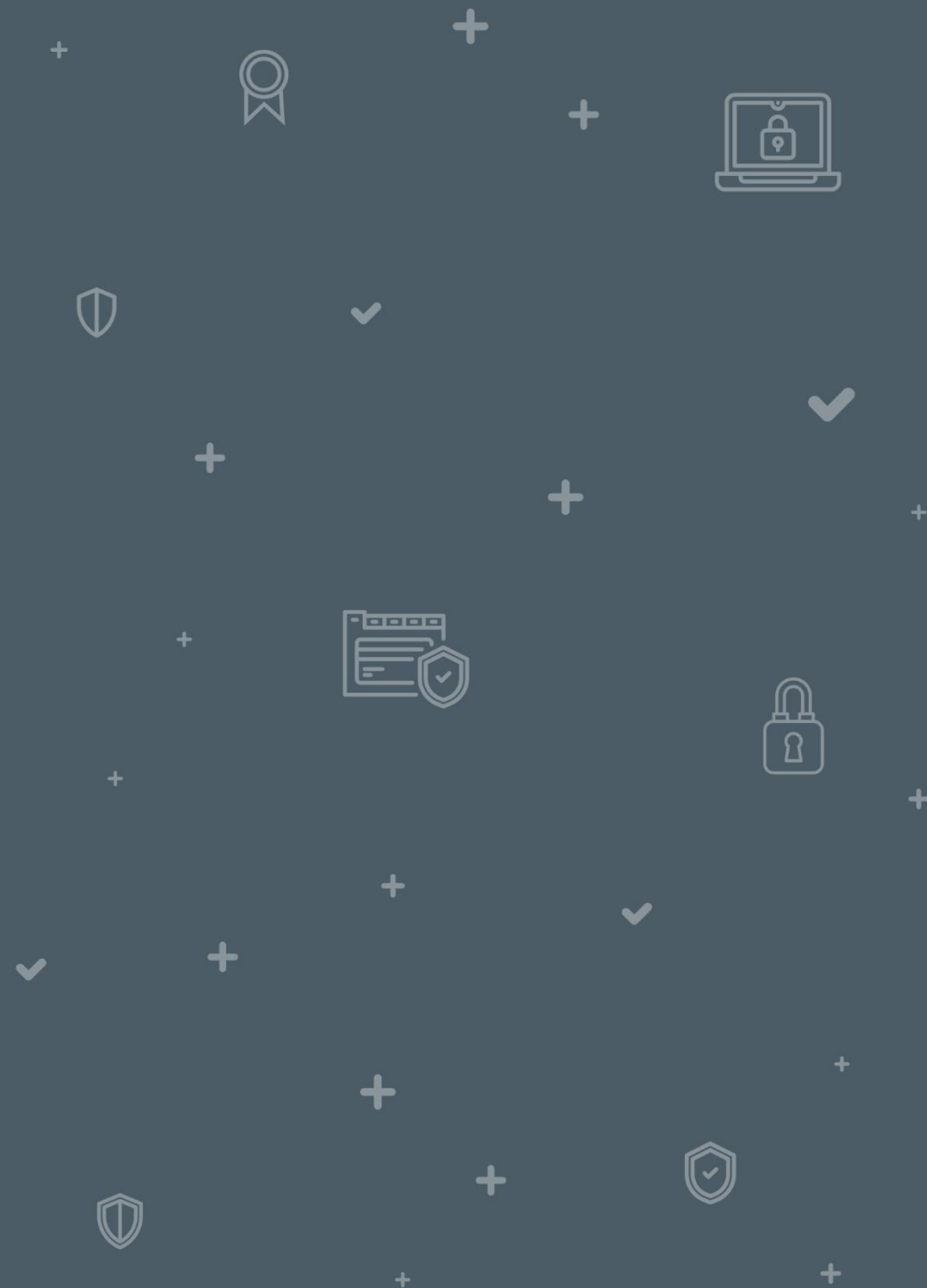
2 CONSIDERACIONES PREVIAS

- Como se puede observar, se ha crackeado el *hash* y muestra la contraseña que se introdujo anteriormente. En este caso, es una contraseña sencilla y a la herramienta no le ha llevado mucho tiempo crackearla, pero el tiempo dependerá de qué dificultad tenga la contraseña.



3

ENUNCIADO EJERCICIO PRÁCTICO 1



ENUNCIADO EJERCICIO PRÁCTICO 1

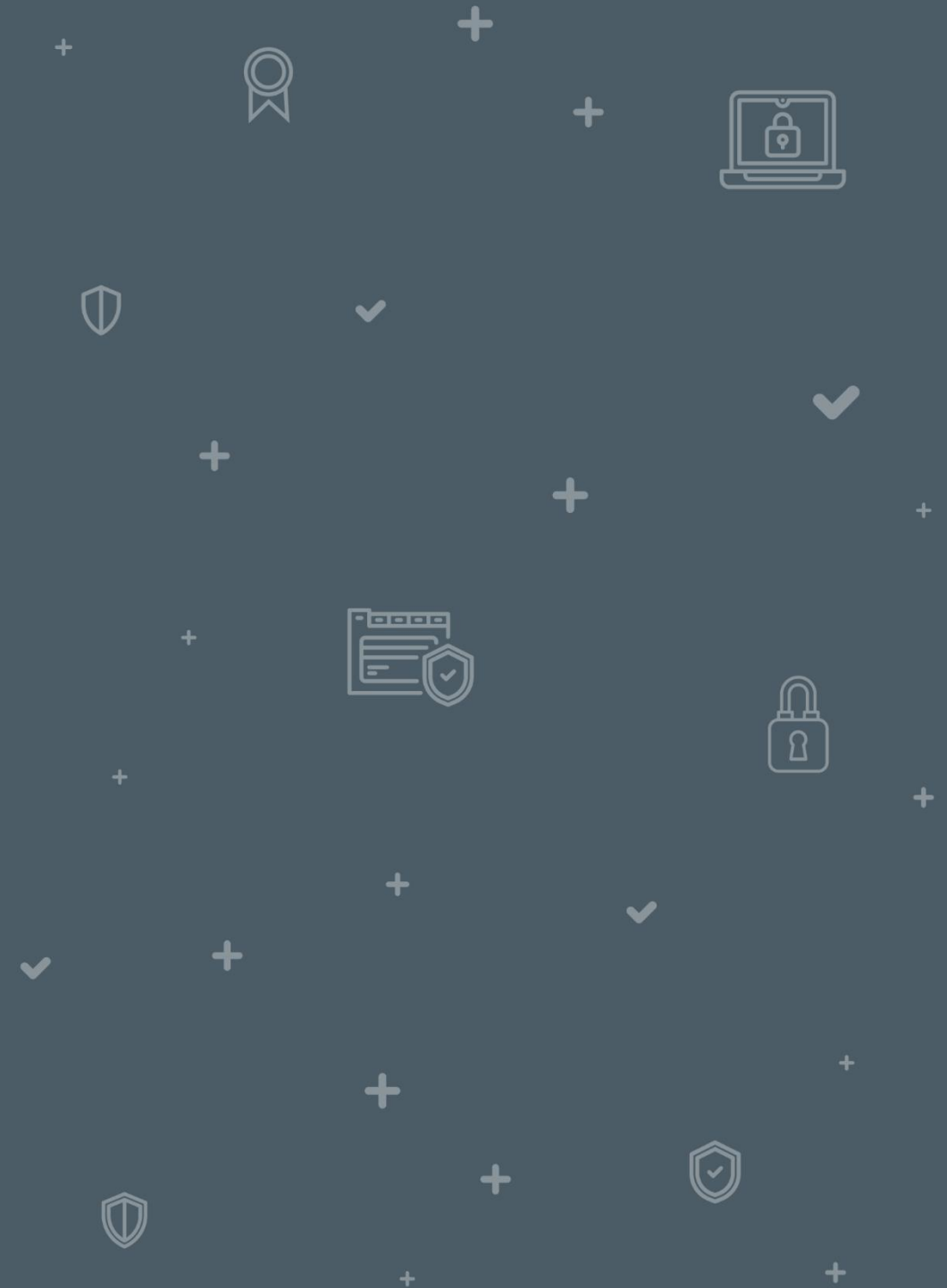


Para la realización de este taller, los alumnos tendrán que descargarse el archivo «Taller 3_Atques por fuerza bruta y diccionario.zip» que encontrarán entre los recursos descargables de la unidad.

Con este archivo «Taller 3_Atques por fuerza bruta y diccionario un archivo.zip» deberás obtener el *hash* y crackearlo. Primero, tendrás que descargarlo o bien introducirlo en la máquina virtual Kali Linux.

4

SOLUCIONARIO EJERCICIO PRÁCTICO 1



4 SOLUCIONARIO EJERCICIO PRÁCTICO 1

- Este archivo solicita una contraseña para descomprimirlo.
 - En primer lugar, obtén el *hash* de este archivo para poder trabajar con él más adelante.
 - Para ello, utilizarás la herramienta John the Ripper con la que conseguirás obtener el *hash* de la contraseña del archivo .zip.
 - Accede al directorio en el que se encuentre el archivo comprimido.
 - Para conseguir el *hash* del archivo debes ejecutar el comando **zip2john Taller 3_Atques por fuerza bruta** y diccionario un **archivo.zip > hash.tmp**

```
(incibe@kali)-[~/Escritorio]  
$ zip2john Incibe.zip > hash.tmp  
ver 2.0 efh 5455 efh 7875 Incibe.zip/INCIBE.pdf PKZIP Encr: TS_chk, cmplen=27080, decmplen=31832, crc=77C1A614 ts=5476 cs=5476 type=8
```

Ilustración 8: Ejecución del comando zip2john
Taller 3_Atques por fuerza bruta y diccionario un archivo.zip > hash.tmp

4 SOLUCIONARIO EJERCICIO PRÁCTICO 1

- Una vez tengas este *hash*, con el comando **john** se ejecutará el crackeo de este mismo *hash*. El tiempo de ejecución dependerá de la dificultad de la contraseña.

```
(incibe@kali)-[~/Escritorio]
$ sudo john hash.tmp
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
1234 run 2 OpenMP(Incibe.zip/INCIBE.pdf)
lg0:00:00:00 DONE 2/3 (2022-08-17 13:16) 6.250g/s 235700p/s 235700c/s 235700C/s 123456..Peter
Use the "--show" option to display all of the cracked passwords reliably
Session completed. Processing the remaining buffered candidate passwords, if any.
```

Ilustración 9: Ejecución del comando john para crackear el *hash*.

¡GRACIAS!



GOBIERNO
DE ESPAÑA

VICEPRESIDENCIA
PRIMERA DEL GOBIERNO

MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL



INSTITUTO NACIONAL DE CIBERSEGURIDAD

