INFORME DE PENTESTING

RESULTADOS DE THEHARVESTER:

```
Read proxies.yaml from /etc/theHarvester/proxies.yaml
*******************************************************************
*                                                                 *
* | |_| |__   ___     /\  /\__ _ _ _____  _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \   / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/  / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___|  \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.5.1                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: ua.es

■[94m[*] Searching Yahoo.

[*] No IPs found.

[*] Emails found: 2
----------------------
dfae@ua.es
info@csidiomas.ua.es

[*] Hosts found: 21
---------------------
autentica.cpd.ua.es
ciencias.ua.es
csidiomas.ua.es
cvnet.cpd.ua.es
derecho.ua.es
economicas.ua.es
educacio.ua.es
eps.ua.es
fae.ua.es
fcsalud.ua.es
gasterra.ua.es
gcloud.ua.es
ice.ua.es
is.ua.es
lletres.ua.es
```

pca.ua.es
s.ua.es
seuelectronica.ua.es
si.ua.es
web.csidiomas.ua.es
web.ua.es

HOSTS Y PUERTOS ABIERTOS:

- Host: 10.10.1.1, Estado: up
- Host: 10.10.1.50, Estado: up
  - Puerto: 21, Protocolo: tcp, Estado: open
  - Puerto: 22, Protocolo: tcp, Estado: open
  - Puerto: 23, Protocolo: tcp, Estado: open
  - Puerto: 25, Protocolo: tcp, Estado: open
  - Puerto: 53, Protocolo: tcp, Estado: open
  - Puerto: 80, Protocolo: tcp, Estado: open
  - Puerto: 111, Protocolo: tcp, Estado: open
  - Puerto: 139, Protocolo: tcp, Estado: open
  - Puerto: 445, Protocolo: tcp, Estado: open
  - Puerto: 512, Protocolo: tcp, Estado: open
  - Puerto: 513, Protocolo: tcp, Estado: open
  - Puerto: 514, Protocolo: tcp, Estado: open
- Host: 10.10.1.51, Estado: up

INFORMACIÓN DEL SISTEMA OPERATIVO:

- Host: 10.10.1.1
- Host: 10.10.1.50
  - Nombre OS: Linux 2.6.9 - 2.6.33, Precisión: 100
    - Tipo: general purpose, Vendedor: Linux,
    - Familia OS: Linux, Generación: 2.6.X
- Host: 10.10.1.51

RESULTADOS DEL EXPLOIT:

--- Resultado de 'hostname' ---
metasploitable

--- Resultado de 'whoami' ---
root

--- Resultado de 'pwd' ---
/home

--- Resultado de 'ls' ---
ftp
msfadmin
service
user

--- Resultado de 'cat /etc/passwd' ---
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh

bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false