

Information Gathering

1) Found open ports

```
(vigneswar@VigneswarPC)-[~]
$ tcpscan 10.10.11.161
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-07 19:04 IST
Nmap scan report for 10.10.11.161
Host is up (0.21s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   3072 ea:84:21:a3:22:4a:7d:f9:b5:25:51:79:83:a4:f5:f2 (RSA)
|_   256 b8:39:9e:f4:88:be:aa:01:73:2d:10:fb:44:7f:84:61 (ECDSA)
|_   256 22:21:e9:f4:85:90:87:45:16:1f:73:36:41:ee:3b:32 (ED25519)
80/tcp    open  http      uvicorn
|_ http-server-header: uvicorn
|_ fingerprint-strings:
|_   DNSStatusRequestTCP, DNSVersionBindReqTCP, GenericLines, RTSPRequest, SSLSessionReq, TLSSessionReq, TerminalServerCookie:
|_   HTTP/1.1 400 Bad Request
|_   content-type: text/plain; charset=utf-8
|_   Connection: close
|_   Invalid HTTP request received.
|_   FourOhFourRequest:
|_   HTTP/1.1 404 Not Found
|_   date: Sat, 07 Sep 2024 17:46:18 GMT
|_   server: uvicorn
|_   content-length: 22
|_   content-type: application/json
|_   Connection: close
|_   {"detail":"Not Found"}
|_   GetRequest:
|_   HTTP/1.1 200 OK
|_   date: Sat, 07 Sep 2024 17:46:03 GMT
|_   server: uvicorn
|_   content-length: 29
```

2) Checked the website

```
10.10.11.161 - Chromium

10.10.11.161 x +
← → ↻ ⚠ Not secure 10.10.11.161
Pretty-print ☐
{"msg":"UHC API Version 1.0"}
```

3) Found endpoints

```
vigneswar@VigneswarPC: ~  
(vigneswar@VigneswarPC)~  
$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u 'http://10.10.11.161/FUZZ' -ic  
v2.1.0-dev  
-----  
:: Method      : GET  
:: URL         : http://10.10.11.161/FUZZ  
:: Wordlist     : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt  
:: Follow redirects : false  
:: Calibration : false  
:: Timeout     : 10  
:: Threads     : 40  
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500  
-----  
[Status: 200, Size: 29, Words: 4, Lines: 1, Duration: 219ms]  
docs [Status: 401, Size: 30, Words: 2, Lines: 1, Duration: 210ms]  
api  [Status: 200, Size: 20, Words: 1, Lines: 1, Duration: 225ms]  
[Status: 200, Size: 29, Words: 4, Lines: 1, Duration: 206ms]  
[WARN] Caught keyboard interrupt (Ctrl-C)
```

File Edit View Search Tools Help
1. 10.10.11.161
HTTP/1.1 200 OK
date: Sat, 07 Sep 2024 17:46
server: uvicorn
content-length: 29
2) Checked the website
10.10.11.161
Notsecure 10.10.11.161
Pretty-print
(JavaScript API Version 1.0*)