kioptrix 2

ip address : --- 192.168.31.141 00:0c:29:44:48:e6   1   60 VMware, Inc.

---

nmap

```
nmap  -Pn -n -A -p- 192.168.31.141
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-11 15:05 EDT
Stats: 0:01:39 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.90% done; ETC: 15:06 (0:00:00 remaining)
Stats: 0:01:39 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.90% done; ETC: 15:06 (0:00:00 remaining)
Nmap scan report for 192.168.31.141
Host is up (0.0011s latency).
Not shown: 65528 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 3.9p1 (protocol 1.99)
| ssh-hostkey:
|   1024 8f:3e:8b:1e:58:63:fe:cf:27:a3:18:09:3b:52:cf:72 (RSA1)
|   1024 34:6b:45:3d:ba:ce:ca:b2:53:55:ef:1e:43:70:38:36 (DSA)
|_  1024 68:4d:8c:bb:b6:5a:bd:79:71:b8:71:47:ea:00:42:61 (RSA)
|_sshv1: Server supports SSHv1
80/tcp   open  http       Apache httpd 2.0.52 ((CentOS))
|_http-server-header: Apache/2.0.52 (CentOS)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
111/tcp  open  rpcbind    2 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2           111/tcp  rpcbind
|   100000  2           111/udp  rpcbind
|   100024  1           768/udp  status
|_  100024  1           771/tcp  status
443/tcp  open  ssl/https?
|_ssl-date: 2019-09-11T15:56:07+00:00; -3h09m44s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_64_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
631/tcp  open  ipp        CUPS 1.1
| http-methods:
|_  Potentially risky methods: PUT
|_http-title: 403 Forbidden
771/tcp  open  status     1 (RPC #100024)
3306/tcp open  mysql      MySQL (unauthorized)
MAC Address: 00:0C:29:44:48:E6 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.30
Network Distance: 1 hop

Host script results:
|_clock-skew: mean: -3h09m44s, deviation: 0s, median: -3h09m44s

TRACEROUTE
```

HOP RTT   ADDRESS
1   1.13 ms 192.168.31.141

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 121.57 seconds

dirb

START_TIME: Wed Sep 11 15:07:21 2019
URL_BASE: http://192.168.31.141/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.31.141/ ----
*** Calculating NOT_FOUND co + http://192.168.31.141/cgi-bin/ (CODE:403|SIZE:290)
+ http://192.168.31.141/index.php (CODE:200|SIZE:667)
==> DIRECTORY: http://192.168.31.141/manual/
+ http://192.168.31.141/usage (CODE:403|SIZE:287)

---- Entering directory: http://192.168.31.141/manual/ ----
*** Calculating NOT_FOUND co ==> DIRECTORY: http://192.168.31.141/manual/de/
==> DIRECTORY: http://192.168.31.141/manual/developer/
==> DIRECTORY: http://192.168.31.141/manual/en/
==> DIRECTORY: http://192.168.31.141/manual/faq/
==> DIRECTORY: http://192.168.31.141/manual/fr/
==> DIRECTORY: http://192.168.31.141/manual/howto/
==> DIRECTORY: http://192.168.31.141/manual/images/
+ http://192.168.31.141/manual/index.html (CODE:200|SIZE:7234)
==> DIRECTORY: http://192.168.31.141/manual/ja/
==> DIRECTORY: http://192.168.31.141/manual/ko/
+ http://192.168.31.141/manual/LICENSE (CODE:200|SIZE:11358)
==> DIRECTORY: http://192.168.31.141/manual/misc/
==> DIRECTORY: http://192.168.31.141/manual/mod/
==> DIRECTORY: http://192.168.31.141/manual/programs/
==> DIRECTORY: http://192.168.31.141/manual/ru/
==> DIRECTORY: http://192.168.31.141/manual/ssl/
==> DIRECTORY: http://192.168.31.141/manual/style/

---- Entering directory: http://192.168.31.141/manual/de/ ----
+ http://192.168.31.141/manual/de/de (CODE:301|SIZE:319)
==> DIRECTORY: http://192.168.31.141/manual/de/developer/
+ http://192.168.31.141/manual/de/en (CODE:301|SIZE:319)
==> DIRECTORY: http://192.168.31.141/manual/de/faq/
+ http://192.168.31.141/manual/de/fr (CODE:301|SIZE:319)
==> DIRECTORY: http://192.168.31.141/manual/de/howto/
==> DIRECTORY: http://192.168.31.141/manual/de/images/
+ http://192.168.31.141/manual/de/index.html (CODE:200|SIZE:7317)
+ http://192.168.31.141/manual/de/ja (CODE:301|SIZE:319)
+ http://192.168.31.141/manual/de/ko (CODE:301|SIZE:319)
+ http://192.168.31.141/manual/de/LICENSE (CODE:200|SIZE:11358)
==> DIRECTORY: http://192.168.31.141/manual/de/misc/
==> DIRECTORY: http://192.168.31.141/manual/de/mod/
==> DIRECTORY: http://192.168.31.141/manual/de/programs/
+ http://192.168.31.141/manual/de/ru (CODE:301|SIZE:319)
==> DIRECTORY: http://192.168.31.141/manual/de/ssl/
==> DIRECTORY: http://192.168.31.141/manual/de/style/

---- Entering directory: http://192.168.31.141/manual/developer/ ----
+ http://192.168.31.141/manual/developer/index.html (CODE:200|SIZE:4770)

---- Entering directory: http://192.168.31.141/manual/en/ ----
+ http://192.168.31.141/manual/en/de (CODE:301|SIZE:319)

```
==> DIRECTORY: http://192.168.31.141/manual/en/developer/
+ http://192.168.31.141/manual/en/en (CODE:301|SIZE:319)
==> DIRECTORY: http://192.168.31.141/manual/en/faq/
+ http://192.168.31.141/manual/en/fr (CODE:301|SIZE:319)
==> DIRECTORY: http://192.168.31.141/manual/en/howto/
==> DIRECTORY: http://192.168.31.141/manual/en/images/
+ http://192.168.31.141/manual/en/index.html (CODE:200|SIZE:7234)
+ http://192.168.31.141/manual/en/ja (CODE:301|SIZE:319)
+ http://192.168.31.141/manual/en/ko (CODE:301|SIZE:319)
+ http://192.168.31.141/manual/en/LICENSE (CODE:200|SIZE:11358)
==> DIRECTORY: http://192.168.31.141/manual/en/misc/
==> DIRECTORY: http://192.168.31.141/manual/en/mod/
==> DIRECTORY: http://192.168.31.141/manual/en/programs/
+ http://192.168.31.141/manual/en/ru (CODE:301|SIZE:319)
==> DIRECTORY: http://192.168.31.141/manual/en/ssl/
==> DIRECTORY: http://192.168.31.141/manual/en/style/

---- Entering directory: http://192.168.31.141/manual/faq/ ----
+ http://192.168.31.141/manual/faq/index.html (CODE:200|SIZE:3564)

---- Entering directory: http://192.168.31.141/manual/fr/ ----
+ http://192.168.31.141/manual/fr/de (CODE:301|SIZE:319)
==> DIRECTORY: http://192.168.31.141/manual/fr/developer/
+ http://192.168.31.141/manual/fr/en (CODE:301|SIZE:319)
==> DIRECTORY: http://192.168.31.141/manual/fr/faq/
+ http://192.168.31.141/manual/fr/fr (CODE:301|SIZE:319)
==> DIRECTORY: http://192.168.31.141/manual/fr/howto/
==> DIRECTORY: http://192.168.31.141/manual/fr/images/
+ http://192.168.31.141/manual/fr/index.html (CODE:200|SIZE:7234)
+ http://192.168.31.141/manual/fr/ja (CODE:301|SIZE:319)
+ http://192.168.31.141/manual/fr/ko (CODE:301|SIZE:319)
+ http://192.168.31.141/manual/fr/LICENSE (CODE:200|SIZE:11358)
==> DIRECTORY: http://192.168.31.141/manual/fr/misc/
==> DIRECTORY: http://192.168.31.141/manual/fr/mod/
==> DIRECTORY: http://192.168.31.141/manual/fr/programs/
+ http://192.168.31.141/manual/fr/ru (CODE:301|SIZE:319)
==> DIRECTORY: http://192.168.31.141/manual/fr/ssl/
==> DIRECTORY: http://192.168.31.141/manual/fr/style/

---- Entering directory: http://192.168.31.141/manual/howto/ ----
+ http://192.168.31.141/manual/howto/index.html (CODE:200|SIZE:5685)
^C> Testing: http://192.168
```

nmap http-enum

```
map -Pn -n -p80 --script=http-enum 192.168.31.141
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-11 15:10 EDT
Nmap scan report for 192.168.31.141
Host is up (0.00086s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|   /icons/: Potentially interesting directory w/ listing on 'apache/2.0.52 (centos)'
|_  /manual/: Potentially interesting folder
MAC Address: 00:0C:29:44:48:E6 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 7.90 seconds
```

searchsploit

```
earchsploit apache 2.0.52
---------------------------------------- ----------------------------------------
 Exploit Title                          |  Path
                                        | (/usr/share/exploitdb/)
```

-- --
Apache 2.0.52 - GET Denial of Service | exploits/multiple/dos/855.pl

searchsploit cups 1.1 | grep "remote"
CUPS 1.1.x - '.HPGL' File Processor Buf | exploits/linux/remote/24977.txt
CUPS 1.1.x - Negative Length HTTP Heade | exploits/linux/remote/22106.txt

nikto

nikto -h 192.168.31.141
- Nikto v2.1.6

+ Target IP: 192.168.31.141
+ Target Hostname: 192.168.31.141
+ Target Port: 80
+ Start Time: 2019-09-11 15:14:48 (GMT-4)

+ Server: Apache/2.0.52 (CentOS)
+ Retrieved x-powered-by header: PHP/4.3.9
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Apache/2.0.52 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ Uncommon header 'tcn' found, with contents: choice
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ Server may leak inodes via ETags, header found with file /icons/README, inode: 357810, size: 4872, mtime: Sat Mar 29 13:41:04 1980
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8725 requests: 1 error(s) and 17 item(s) reported on remote host
+ End Time: 2019-09-11 15:15:58 (GMT-4) (70 seconds)

+ 1 host(s) tested

mysql

```
?php
        mysql_connect("localhost", "john", "hiroshima") or die(mysql_error());
        //print "Connected to MySQL<br />";
        mysql_select_db("webapp");

        if ($_POST['uname'] != ""){
                $username = $_POST['uname'];
                $password = $_POST['psw'];
                $query = "SELECT * FROM users WHERE username = '$username' AND password='$password'";
                //print $query."<br>";
                $result = mysql_query($query);

                $row = mysql_fetch_array($result);
                //print "ID: ".$row['id']."<br />";

        ----------------------------------------------------------------------------------------------------------
```

bash-3.00# mysql -u john -p --execute="show databases"
mysql -u john -p --execute="show databases"
Enter password: hiroshima

```
+----------+
| Database |
+----------+
| mysql    |
| test     |
| webapp   |
+----------+
```