Extra Black box Vancuver

Sudo arp-scan --localhost

Trovato ip : 192.168.56.101

```
└─$ 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

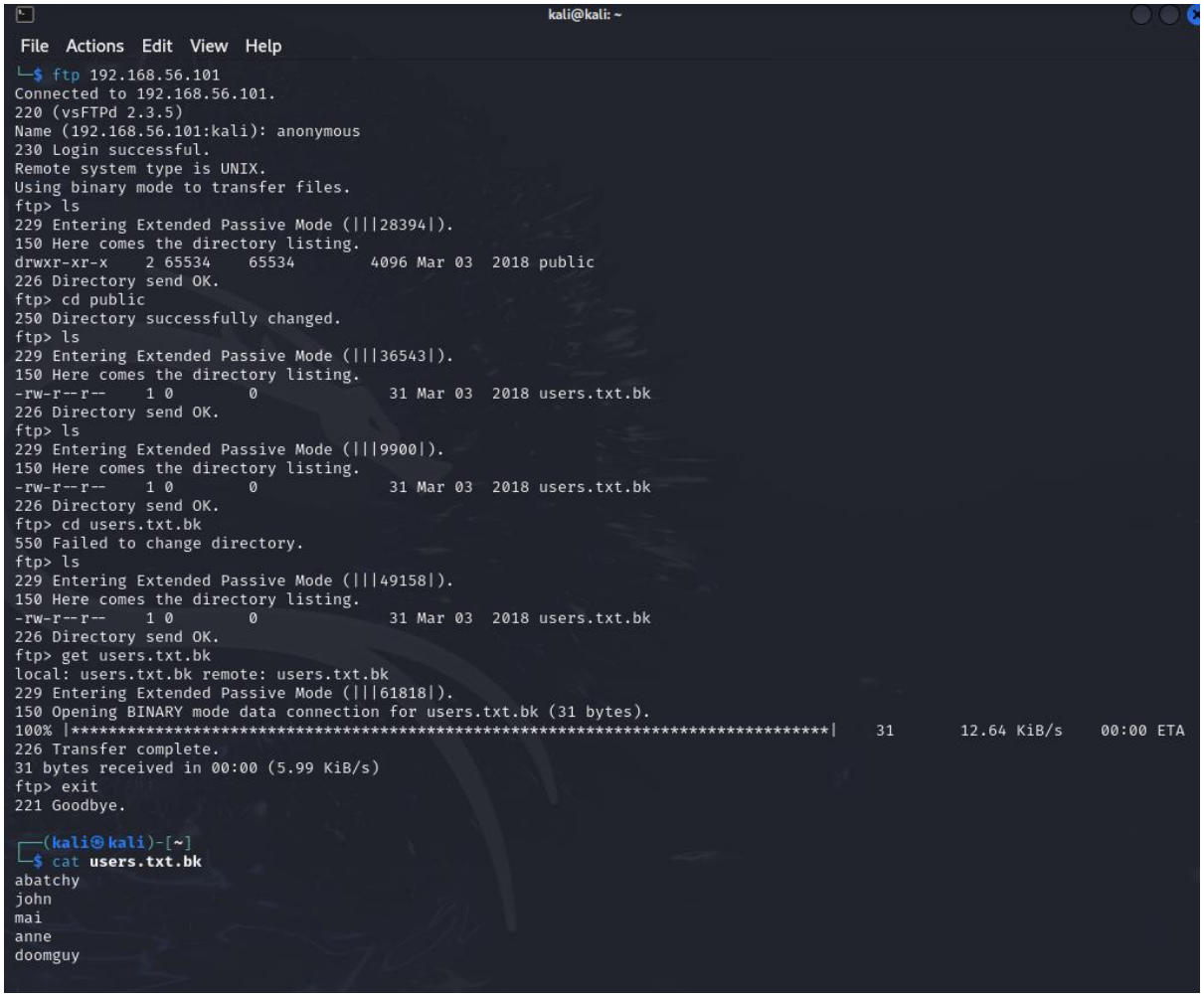
-A: Abilita il rilevamento del sistema operativo e dei servizi.

-sC: Usa script Nmap standard per ulteriori informazioni.

-sV: Determina le versioni dei servizi in esecuzione.

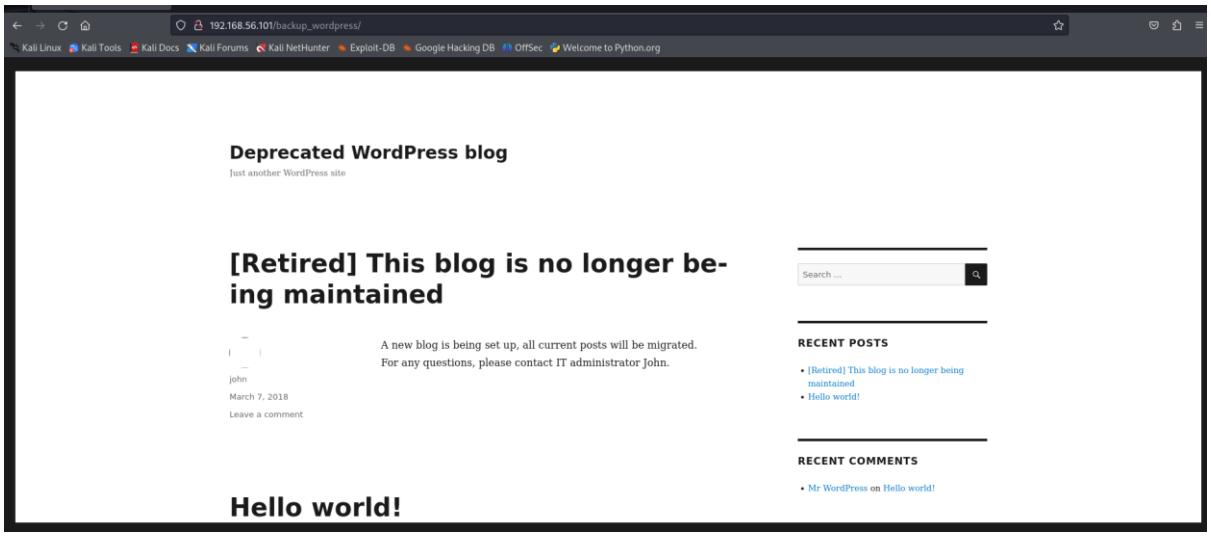
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A -sC -sV 192.168.56.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 12:16 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.0011s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
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:
|   STAT:
| 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 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 85:9f:8b:58:44:97:33:98:ee:98:b0:c1:85:60:3c:41 (DSA)
|   2048 cf:1a:04:e1:7b:a3:cd:2b:d1:af:7d:b3:30:e0:a0:9d (RSA)
|_  256 97:e5:28:7a:31:4d:0a:89:b2:b0:25:81:d5:36:63:4c (ECDSA)
80/tcp open  http    Apache httpd 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)

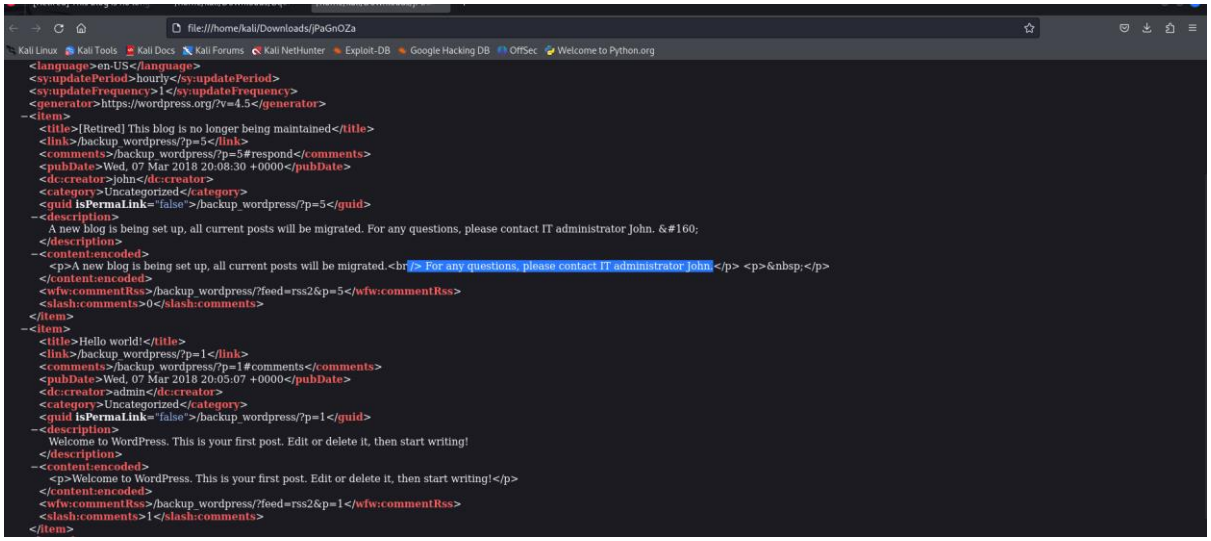


-Test accesso ftp con credenziali anonymous , ottengo accesso alla dir pubblic e scarico il file users.txt.bk e leggo il contenuto con cat

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/