SETTING UP A DMZ:

In this module, we have created a DMZ and configured an Apache TomCat Web Server in DMZ.

Toolkit Used:

Workstation Operating System	Lubuntu 15.04
External Network Interface Cards	Quantity: 2 (LAN + DMZ) Manufacturer: TP-LINK Model Number: TF-3200
Switches	Quantity: 1 Manufacturer: D-LINK Model Number: DES-10008A

DMZ Setup Steps with Screenshots:

1. Installed another TP-Link TF-3200 NIC in the Workstation for DMZ in addition to LAN NIC in the previous module.

2. Edited the `/etc/udev/rules.d/70-persistent-net.rules` file and renamed the new NIC interface name as DMZ for the sake of our own convenience.

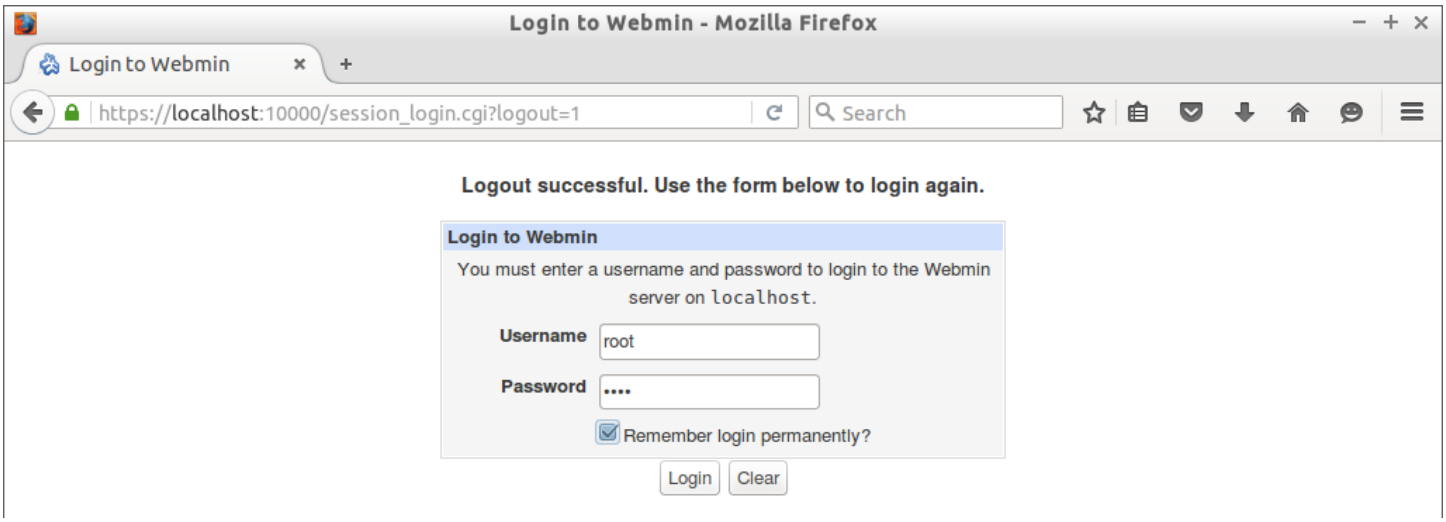
3. Added the DMZ interface configuration to the `/etc/network/interfaces` file.

```
iface DMZ inet static
        address 192.168.1.1
        netmask 255.255.255.0
        broadcast 192.168.1.255
        network 192.168.1.0
        gateway 192.168.1.1
```

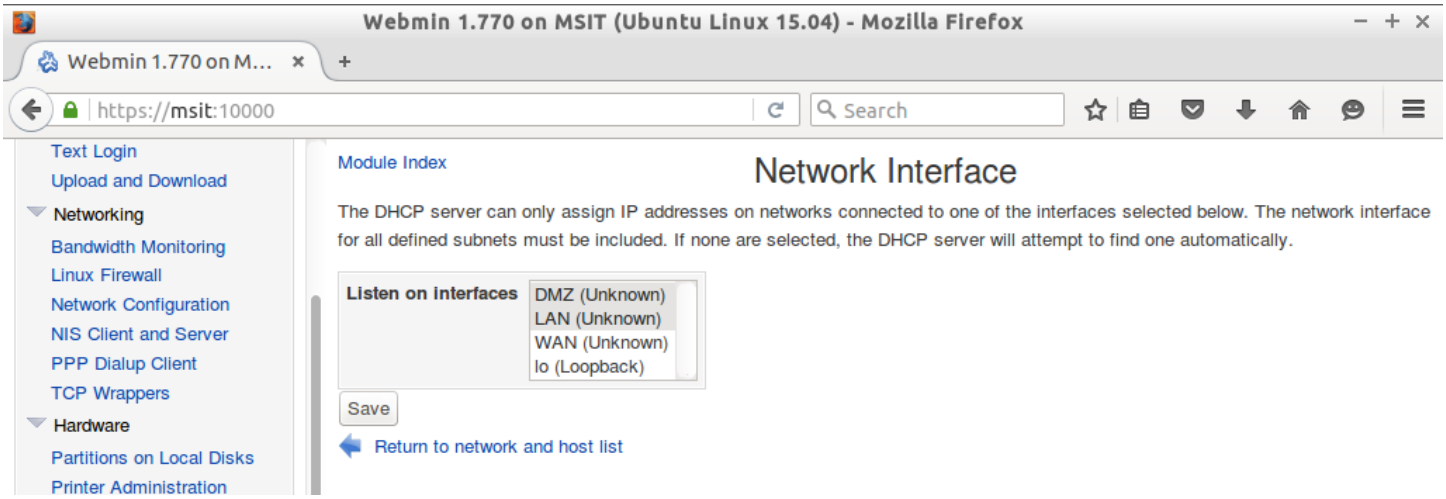
4. Edited the `/etc/dhcp/dhcpd.conf` file to append the DMZ subnet details.

```
dhcpd.conf
File  Edit  Search  Options  Help
#
# Sample configuration file for ISC dhcpd for Debian
#
# Attention: If /etc/ltsp/dhcpd.conf exists, that will be used as
# configuration file instead of this file.
#
#


ddns-update-style ad-hoc;
ddns-update-style interim;

default-lease-time 600;
max-lease-time 7200;

#LAN
subnet 192.168.0.0 netmask 255.255.255.0 {
    authoritative;
    option broadcast-address 192.168.0.255;
    range 192.168.0.10 192.168.0.100;
    option domain-name-servers 218.248.255.145 , 14.139.5.5 , 8.8.8.8 , 8.8.4.4;
    option routers 192.168.0.1;
    default-lease-time 600;
    max-lease-time 7200;
}

#DMZ
subnet 192.168.1.0 netmask 255.255.255.0 {
    authoritative;
    option broadcast-address 192.168.1.255;
    range 192.168.1.50 192.168.1.100;
    option domain-name-servers 218.248.255.145 , 14.139.5.5 , 8.8.8.8 , 8.8.4.4;
    option routers 192.168.1.1;
    default-lease-time 6000;
    max-lease-time 72000;
}
```

5. Login to the Webmin interface with the root account.



6. Listen to both Interfaces LAN and DMZ such that both interfaces are up and running to provide DHCP services to their respective clients.

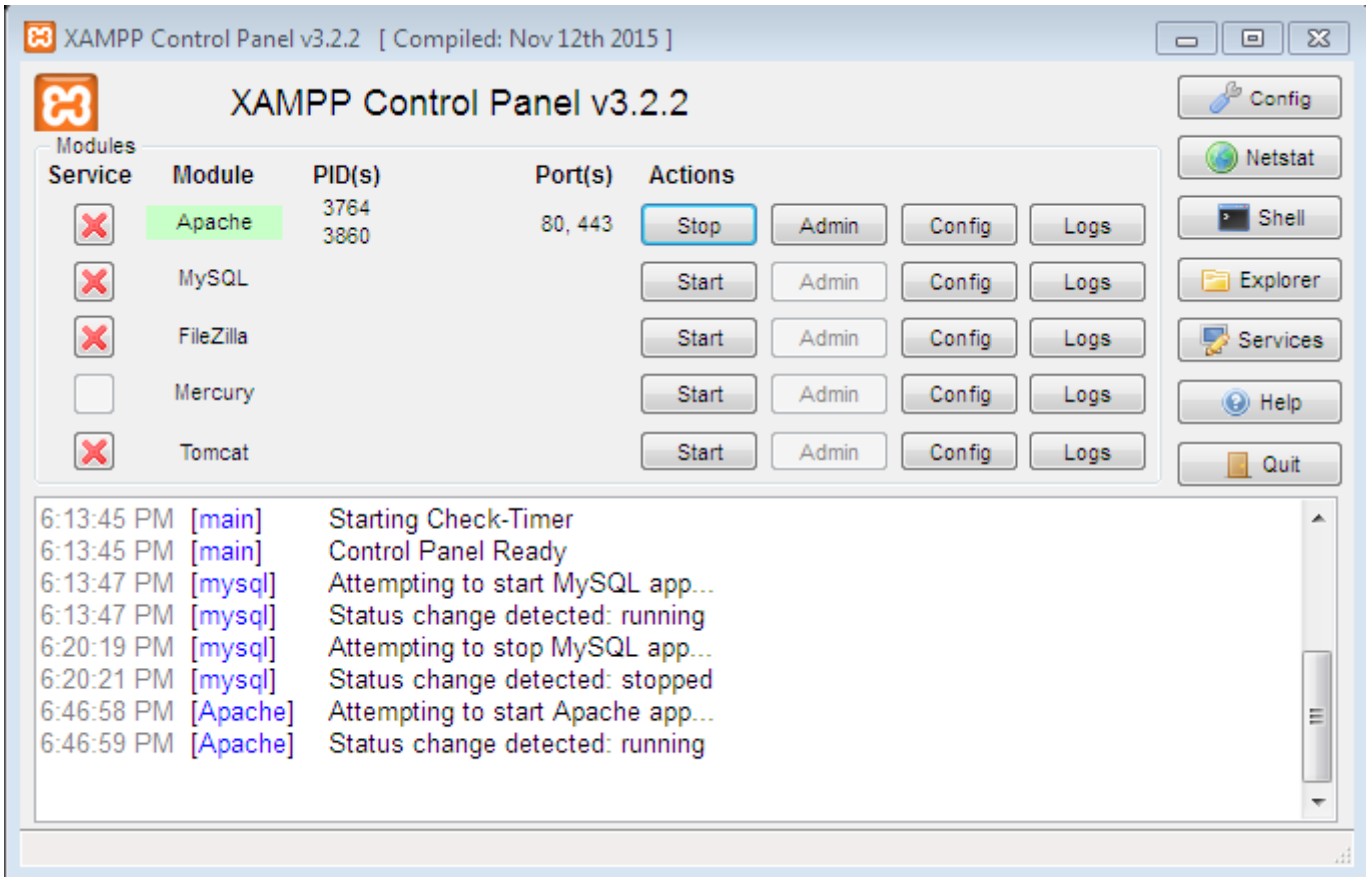


7. Start the DHCP server from the Webmin.

8. Add a new workstation in the DMZ network such that it works as a Web Server.
   a. The workstation we obtained from the MSIT Lab has Windows 7 pre-installed in it and it is in new condition. So, we have considered Win7 to install apache web server.

```
C:\Users\JNTUCC>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6ca2:fe6c:36b:2a6e%11
   IPv4 Address. . . . . . . . . . . : 192.168.1.52
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter isatap.{285EFB39-D3FF-460C-8C35-9552546FB82E}:
```

   b. Installed XAMPP and started the Apache Web Server.



9. Add the required IPTABLES rules such that the LAN Users must be able to communicate with the Web Server in DMZ.

- `iptables -A FORWARD -i LAN -o DMZ -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT`
- `iptables -A FORWARD -i DMZ -o LAN -m state --state ESTABLISHED,RELATED -j ACCEPT`

- `iptables -A FORWARD -i DMZ -o WAN -m state --state ESTABLISHED,RELATED -j ACCEPT`
- `iptables -A FORWARD -i WAN -o DMZ -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT`

- `iptables -t nat -A PREROUTING -p tcp -i WAN -d 10.66.20.18 --dport 80 -j DNAT --to-destination 192.168.1.52`

10. The webserver in DMZ is now accessible to the LAN users.

    a. `192.168.0.13` accessed the Apache Web Server at `192.168.1.52` can be observed in the below screenshot.

DATABASE SERVER SETUP IN LAN (on `192.168.0.12`):

1. MySQL DB server was installed on `192.168.0.12`.

```
root@H3M4:/home/sr1k4n7h# ifconfig
eth0      Link encap:Ethernet  HWaddr 74:e6:e2:18:25:d9
          inet addr:192.168.0.12  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::76e6:e2ff:fe18:25d9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:309956 errors:0 dropped:1123 overruns:0 frame:0
          TX packets:92007 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:272717480 (260.0 MiB)  TX bytes:18250655 (17.4 MiB)
```

```
root@H3M4:/home/sr1k4n7h# mysql -uroot -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 40
Server version: 5.5.46-0+deb8u1 (Debian)

Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.
```

2. Enabled the remote access to the MySQL server by editing the `/etc/mysql/my.cnf` file.

```
[mysqld]
#
# * Basic Settings
#
user            = mysql
pid-file        = /var/run/mysqld/mysqld.pid
socket          = /var/run/mysqld/mysqld.sock
port            = 3306
basedir         = /usr
datadir         = /var/lib/mysql
tmpdir          = /tmp
lc-messages-dir = /usr/share/mysql
#skip-external-locking
#
# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
# bind-address          = localhost
# bind-address          = 192.168.1.52
```

3. Granted remote access privileges to the root user.

```
mysql> SHOW grants;
+-----------------------------------------------------------------------+
| Grants for root@localhost                                             |
+-----------------------------------------------------------------------+
| GRANT ALL PRIVILEGES ON *.* TO 'root'@'localhost' WITH GRANT OPTION |
| GRANT PROXY ON ''@'' TO 'root'@'localhost' WITH GRANT OPTION        |
+-----------------------------------------------------------------------+
2 rows in set (0.00 sec)
```

4. Restarted the MySQL server on `192.168.0.12`.

```
root@H3M4:/home/sr1k4n7h# /etc/init.d/mysql restart
[ ok ] Restarting mysql (via systemctl): mysql.service.
```

5. MySQL server is in `192.168.0.12` up and running.

Accessibility according to the given requirements:

1. Add the IPTABLES rule on the router such that the Web Server (192.168.1.52) on DMZ can access the Database server on LAN (192.168.0.12).

```
target     prot opt source               destination
root@MSIT:/home/inf053c# iptables -A INPUT -p tcp -s 192.168.1.52 --sport 1024:65535 -d 192.168.0.12 --dport 3306 -m state --
state NEW,ESTABLISHED -j ACCEPT
root@MSIT:/home/inf053c#
```

2. Finally, Web Server (192.168.1.52) on DMZ is able to access the DB Server (192.168.0.12) in LAN.

```
Administrator: XAMPP for Windows
# mysql -u root -h 192.168.0.12 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 39
Server version: 5.5.46-0+deb8u1 (Debian)

Copyright (c) 2000, 2015, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases
    -> ;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| IS_SPEC            |
| mysql              |
| performance_schema |
+--------------------+
4 rows in set (0.00 sec)

MySQL [(none)]> exit
Bye

JNTUCC@JNTUCC-PC c:\xampp
#
```