NETWORK SECURITY (CS6500) - Tutorial 4a

Rebecca Bloomwood is addicted to online shopping, and this is well known to her colleague Mr Derek Smeath. Derek decides to take advantage of this fact and makes a deal with a rival company *shophere.com* of a famous e-commerce website *shopher.com*. Since they are in the same organisation, Derek can see when Rebecca is trying to access the shopping website. Derek's task is to make sure that Rebecca shops only from the website *shophere.com*. One way to achieve this is that whenever Rebecca tries to access *shopher.com*, Derek redirects her to website *shophere.com*, but he realised that it is very tiresome to redirect her for every request. Your task is to assist Derek in achieving a long-lasting effect that always redirects Rebecca to *shophere.com*.

You will need to configure the DNS server BIND(9), which is pre-installed in pre-built Ubuntu virtual machine image. For further configuration you can follow these steps:

Step 1: Create the named.conf.options file. The DNS server needs to read the /etc/bind/ named.conf configuration file to start. This configuration file usually includes an option file called /etc/ bind/named.conf.options. Please add the following content to the options file, if not already there:

```
options{
        dump-file       "/var/cache/bind/dump.db";
    };
```

It should be noted that the file /var/cache/bind/dump.db is used to dump DNS server's cache.

Step 2: Assume that we own a domain: *shopher.com*, which means that we are responsible for providing the definitive answer regarding *shopher.com*. Thus, we need to create a zone in the DNS server by adding the following contents to /etc/bind/named.conf.

```
zone "shopher.com" {
        type master;
        file "/var/cache/bind/shopher.com.db";
        };

zone "0.168.192.in-addr.arpa" {
        type master;
        file "/var/cache/bind/192.168.0";
        };
```

Step 3: The file name after the file keyword in the above zones is called the zone file. The actual DNS resolution is put in the zone file. In the /var/cache/bind/ directory, compose the following shopher.com.db zone file. You can modify and use the file shopher.com.db given in Moodle.
We also need to set up the DNS reverse lookup file. In the directory /var/cache/bind/, compose a reverse DNS lookup file called 192.168.0 for shopher.com domain: The file is given in Moodle.

Step4: Now we are ready to start the DNS server. Run the following command:
% sudo service bind9 restart

On the user machine, we need to change the DNS server. We achieve this by changing the DNS setting file /etc/resolv.conf of the user machine:

nameserver 192.168.0.10 # the IP of the DNS server you just set up

Note: make sure this is the only nameserver entry in your /etc/resolv.conf. Also note that in Ubuntu, /etc/resolv.conf may be overwritten by the DHCP client if you change the network.

Questions :

1. Describe the attack technique that you have adopted.
2. Modify the given file udp.c to send the spoof DNS response.
3. Write down the challenging part of this lab, if any.

Submission:

1. The modified udp.c file which is used in the attack.
2. Detailed lab report along with screenshots showing the output of ‘dig’ command before and after the attack.