Luke Evans

February 20th, 2021

Lab 4 – DNS

User: 10.0.2.4

DNS Server: 10.0.2.5

Attacker: 10.0.2.15

*Part I: Setting Up a Local DNS Server*

*1.1: Configure the User Machine*

On the user machine, we edit the head file to change our DNS server to 10.0.2.5. The head file is located at /etc/resolvconf/resolv.conf.d/head:

*A screenshot of a computer

Description automatically generated with low confidence*

In order for our change to take affect we must refresh our DNS setting. To do this we use the command sudo resolvconf -u. Then we ping google.com and check we can resolve the IP and reach the site:

Text

Description automatically generated

If we sniff the packets with wireshark, we can see that our user machine uses 10.0.2.5 as its local DNS server:

Graphical user interface, application

Description automatically generated

Observation: In this task, we set up our local server VM to act as our DNS server. In order to make the user VM use our local DNS server we had to edit the /etc/resolvconf/resolv.conf.d/head file and specify our nameserver as our DNS server IP. After we refreshed our DNS settings we tested our configuration by pinging [www.google.com](http://www.google.com). Using wireshare, we were able to sniff the packets and see that the DNS queries were in fact being sent to IP 10.0.2.5 which is our local DNS server.

Explanation: Changing the DNS server on Linux can be done by chaning the nameserver location by editing the heads file located in /etc/resolvconf/resolv.conf.d/ directory. This will allow us to run attacks on our local DNS server.

*1.2: Set up a Local DNS Server*

Options for our bind DNS server are configured in /etc/bind/named.conf.options:

Text

Description automatically generated

When we ping [www.google.com](http://www.google.com) we can see that the server VM is used by our User VM as the local DNS server:

Graphical user interface, application

Description automatically generated

Observation: In this task we setup our DNS server on our server VM. We had to configure disabling dnssec and changed the name of our cache dump file to dump.db. Bind 9 was already configured in our prebuilt image so I only had to check that the configuration settings were correct. Just as in the previous step, when pinging google.com, our server VM is used by the User VM as our local DNS server. This is shown from the screenshot from wireshark.

Explanation: We setup our server VM to serve as our local DNS server for our user machine. This will allow us to simulate DNS attacks on computers on the same LAN.

*1.3: Host a Zone in the Local DNS Server*

First, we create our zones in /etc/bind/named.conf file. These two zone specify forward and reverse lookup for example.com:

Text

Description automatically generated

Next, we need to setup our forward lookup zone file that we specified above as example.com.db:

Text

Description automatically generated

Lastly, we need to setup the reverse lookup file:

Text

Description automatically generated

To test our configuration, we restart out bind server and then run the dig example.com command from our user VM:

Text, letter

Description automatically generated

Observation: For this task we configured hosting a zone on our DNS server. The domain that we are hosting is [www.example.com](http://www.example.com). In the above screenshots, we show the files that we created for our DNS records and routing information. In order for our changes to take affect, we had to restart our DNS server. To test our setup, we ran dig [www.example.com](http://www.example.com) from the user VM to see that it routes to the local IP.

Explanation: Bind setting up the appropriate bind configurations, we can direct web addresses to use our local IP address. They can then be queried on our DNS server by using the dig command from a machine that is configured to use our server as the local DNS server.