ITN-263

Lab 02 - Add a route

Last modified: 6 Sep 2021

Scenario

Your goal is to log into the target machine using freddie / clauseses as credentials. Unfortunately, the network isn’t configured properly (it’s missing a route). You’ll need to fix it.

If (at any point in the below) you become stuck, be sure to read the man pages for the commands involved (e.g., “man route”, “man ifconfig”, “man ip”). Also, searching Google may help.

Set up

This lab requires the use of the telnet client. You’ll need to install it via:

```
apt-get update
apt-get upgrade -y
apt-get install -y telnet
```

Steps

1) Right-click on the link in RTB’s Lab 02 to access your workstation. (credentials = root / toor)

2) Open a terminal window and use the “ifconfig” command to determine your desk’s IP and netmask. Use the following to find the other machine in your network segment.

```
for i in {1..254};do (ping -c 1 192.168.10.$i > /dev/null && echo 192.168.10.$i &); done
```

> **Note**
>
> If only “192.168.10.1” (which is your desk’s IP) is listed in the results, re-run the script a few times.

> **Note**
>
> If you use “255”, instead of “254” in the above, you’ll receive a warning about pinging the broadcast address. If this happens, just press Enter.

Since there’s only one other IP in the network segment, it’s probably safe to assume that it’s the router between your workstation and the target machine.

Enter the discovered IP as the answer to the first question in RTB’s Lab 02.

3) The IP address of the target machine is 192.168.122.38 and uses the same netmask. If you attempt to ping it, at this point, you’ll receive a “network is unreachable” error.

```
root@VABeach:~# ping -c 1 192.168.122.38
connect: Network is unreachable
```

Using the information you’ve gathered so far, you should be able to create a route command so that you can reach the target system.

Add a route to your machine, so that you can reach the target IP. The syntax for it is:

```
route add -net NET_IP netmask NETMASK gw GATEWAY_IP
```

where: - “NET_IP” is the network IP range for the target. (Hint: it will end in “.0”, vice “.38”.) - “NETMASK” is in the “dotted quad’ format (e.g.,”255.255.255.0“). - “GATEWAY_IP” is the IP address of the router, through which the target can be accessed. (This is the IP that you detected in Step #2.)

Enter the routing statement as the answer to the second question in RTB Lab 02.

4) Telnet to the target machine and find the flag. Enter the flag as the answer to question 3 in RTB Lab 02. The credentials are: freddie / clauseses

5) It is important to note that the “route” command is being deprecated (i.e., will be removed in future Linux distributions). It is being replaced by the “ip route” command.

Read the man page for the “ip” command. Determine the missing piece from the following:

```
ip route add MISSING_PIECE via GATEWAY_IP
```

where: - “MISSING PIECE” is the new routing information. - “GATEWAY_IP” is the address you used (above) as the gateway IP address.

Enter the missing piece information as the answer to question 4 in RTB Lab 02.

Troubleshooting

1) You can show your current routes by running one of the following:

```
route -n
ip route
```

2) If you’ve made mistakes when entering routing statements, you can remove individual routes using one of the following syntaxes:

```
route del -net NET_IP netmask NETMASK gw GATEWAY_IP
ip route del ROUTE via GATEWAY_IP
```

Simply put, you need to re-run the command while using “del” instead of “add”. A quick way of doing this is to press the up-arrow key until you reach the route that you want to remove and replace “add” with “del”.

3) As it’s stated in the worksheet, you’ll use the following syntax:

route add -net IPRANGE netmask NETMASK gw GATEWAYIP

where:

- IPRANGE is the network segment in which the web server resides
- NETMASK is the netmask for the network segment in which the web server resides
- GATEWAYIP is the IP address in desk’s local network segment, through which you have to go to reach the web server

> **Note**
>
> IPRANGE almost always ends in “.0”

> NETMASK for class C-sized segments is 255.255.255.0
>
> The worksheet gives you the IP address of the web server. 192.168.x.x network segments are almost always 255.255.255.0