LAB 4 - Exposing Network Services - NAT, Firewalls & Port Forwarding

Commonly an organization will have a special subnet setup where all their networking services run. For instance, many companies host an internal web server. When a user wants to access a page on this internal web server, their traffic is routed to the corporate subnet where this server is hosted. The network administrator places a *firewall* between this special subnet and the rest of the network. Many networks will have a *Network Address Translation* service running between this special network segment and the rest of the network. This allows the server subnet to be addressed with a different IP Address schema than the rest of the network. The security team will open specific ports on the firewall, which will only allow specific traffic to pass onto the server subnet.

In this lab we will configure our server as an internal web server. We'll reconfigure our Virtual Box network to mimic this type of internal subnet. Then we'll open ports through Virtual Box to allow other hosts on our internal network access this web server. Finally we'll use Wireshark to sniff our HTTP connection with the web server.

Prerequisites

Completion of Lab 2 will prepare you for completing this lab.
Lab 3 is recommended, but not required at this point.

Backing Up a VM (again)

Throughout these labs we'll be making configuration changes to our Ubuntu Server installation. It can be easy to break our server, but we don't have to worry about that, VirtualBox allows us to backup the current state of our server. It's strongly suggested that you backup your virtual server now. Here are a few online resources that cover this process:
https://www.youtube.com/watch?v=xqNIvyZlHts

https://www.osradar.com/how-to-backup-vms-on-virtualbox/

Setting Up Virtual Box NAT

We are trying to simulate a corporate network that exists on a subnet behind a firewall and a NAT service. We will setup Virtual Box so your guest operating system is behind a NAT service. Your host machine (and local network) will act as the rest of the corporate network.

If your Virtual Box guest machine is set in “Bridged” mode, you’ll need to change that now. You may need to stop your guest machine before you can make the changes in Virtual Box:
https://geek-university.com/oracle-virtualbox/configure-nat-networks/

Removing Static IP Address & Resetting DHCP

In a previous lab we set our guest operating system up with a static IP Address. We now need to undo that change. Please reconfigure your guest OS to use DHCP instead of Static IP Addresses:
https://www.server-world.info/en/note?os=Ubuntu_20.04&p=dhcp&f=2

Network Address Translation (NAT)

Our VM is running behind a NAT service. This means our VM is using a different IP Address space than our host machine. Virtual Box provides NAT translation in this case. This is an excellent introduction to what NAT is doing on the network:
https://computer.howstuffworks.com/nat.htm

Port Forwarding

Now We want to Port Forward two ports. We want to be able to access Port 22 (for SSH) and Port 80 (for Web Server) on our guest operating system. But we are going to use Port Forwarding to allow this access. Here is a fairly good discussion on Port Forwarding:

https://superuser.com/questions/284051/what-is-port-forwarding-and-what-is-it-used-for

Now, Port Forward host port 4990 to guest port 22, and forward host port 4995 to guest port 80.

Here are some good instructions on Port Forwarding in Virtual Box: https://www.howtogeek.com/122641/how-to-forward-ports-to-a-virtual-machine-and-use-it-as-a-server/

You should now be able to SSH into your guest machine using your host machine's IP Address and Port 4990.

If you have access to your network router settings, you can enable access to your server from the internet by port forwarding port 4990 and port 4995 to your host machine.

Setting Up A Web Server On Ubuntu 20.04

Linux has many options for web servers. Nginx can be setup with one command:
https://www.tecmint.com/install-nginx-on-ubuntu-20-04/

Bring up a browser on your host machine. And go to http://127.0.0.1:4995
If you see the following, Nginx was successfully installed:

Demo File To Use On Web Server

Create /var/www/html/index.html and add the following text to it:

```
<html>
    <body>
    <p> HUMBOLDT STATE UNIVERSITY- THIS IS A TEST </p>
    <p> x11551155x11551155x </p>
    </body>
</html>
```

Load http://127.0.0.1:4995 and you should see the following:

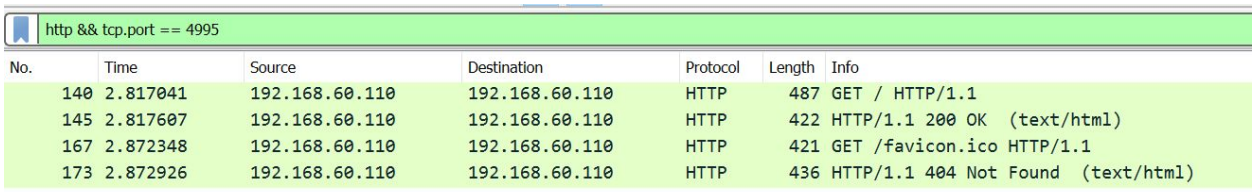
HUMBOLDT STATE UNIVERSITY- THIS IS A TEST

x11551155x11551155x

You'll be able to look for this string in your HTTP packets!

Wireshark – Collecting Packets from an HTTP Transaction

Run Wireshark. Setup the following filter: "*http && tcp.port == 4995*" and listen for traffic on all interfaces. Now, in the background, reload your http://127.0.0.1:4995 page. If no traffic shows up on wireshark you may need to use http://MY-HOST-IP:4995 instead of your 127.0.0.1 loopback address. Sometimes Windows versions of wireshark are unable to listen for loopback addresses. You should see results similar to this:



Deliverables:

1. Wireshark Export File
    - Save your wireshark capture, and upload the file to LAB4 on Canvas.
    - Make sure your capture shows both an HTTP GET request, and an HTTP Response.
    - If your capture takes too long, your file will grow too large for Canvas to appreciate. I would recommend that if your capture is more than 250k in size that you try to do it again, but quicker.

Instructions for Deliverables

Preparing For Future Labs

In a future lab we will use wireshark to decode and analyze different protocols as they are running on the network. Today we've learned to sniff specific packets from specific protocols. Using this tool we will be able to record, reconstruct and analyze many types of network traffic.