INFS3617 Networking & Cyber Security

Sandbox Weekly Reflection

Name: Bevan Lui	**zID:** z5160501

Tutorial Week and Date: Week 3, Friday 11am, 6/3/2020

Explain <u>TWO</u> networking and/or cyber security concepts you have learned in your lab this week. Your description should be in the format provided below:

(1.1) Activity 2.2 Dynamic IP Assignment

Activity 2.2 involved using DHCP protocol to give a workstation an IP address automatically

(1.2)

The DHCP (Dynamic Host Control Protocol) is used to assign a local IP address to a device automatically. The way DHCP works is that the device will send a request to the server which will then offer an IP address to be accepted. In activity 2.2 we opened Wireshark to be able to observe this DHCP process that occurs when a device is getting assigned a local IP. The process of DHCP involves DHCP Discover, DHCP Offer, DHCP Request, DHCP Acknowledge for a device to be assigned an IP automatically. The DHCP Discover request is where the device would first send out a broadcast looking for a DHCP server to contact. The DHCP server will then send a DHCP Offer back to the device with a message that contains client IP address, subnet mask, default gateway IP address and IP lease time. After the device receives the offer, it means that there is a DHCP server on the same subnet and will broadcast a DHCP Request back to the server. This will request for network configuration data such as an IP address to use and accept the offer. The DHCP server that receives the DHCP request message will broadcast a DHCP Ack (acknowledge) and will transfer all the network configuration data and the IP address for the device, and finally the IP address is given to the device.

(2.1) Activity 4.1 - Observing NAT in action

Activity 4.1 involved changing the traffic from leaving from a private address to leaving from a public address to communicate over the internet.

(2.2)

This activity is an example of using NAT (Network Address Translation), NAT is used to remap private addresses to use a devices' public address to allow communication on the internet. NAT allows for example a business to appear to send all traffic from a single public IP address, while it is actually using one public IP for many devices instead of consuming hundreds and thousands of public IP addresses. This was observed in the activity as packets were sent from different terminals, but the packets sent out where identical with the same IP address as they are sent through a router. The router has NAT enabled and is replacing the workstations' IP with its own to connect to the internet and in NAT translation is retains where the traffic originated from so it can forward the traffic back to its origin in this case the device. NAT allows for a device with a private address with no access to the Internet to gain access to the internet through being provided with a public IP address that can connect to the internet.