INFS3617 Networking & Cyber Security

Sandbox Weekly Reflection

Name: Bevan Lui	**zID:** z5160501
Tutorial Week and Date: Week 8, Friday 11am, (Thursday, 9/4/2020)	
Explain TWO 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 Basic Exploit*

Observing the use of asymmetric cryptography to access a remote machine as the root

*(**1.2**)*

Asymmetric cryptography, in the case of the activity SSH, is used to provide remote access to a machine that is more secure than logging on using a password. It involves the existence of a public and a private key, the public key is placed onto the machine that you want to be able to remotely access, and public SSH key encrypted messages can only be decrypted with your own private key. The keys are related mathematically but cannot be derived from each other making it difficult for anyone to get the other key from knowing the other. In the activity the remote vulnerable machine couldn't be accessed via SSH, however there was an opening in the security to access the root directory of the file server with incorrectly set up permissions, this allowed for copying our public SSH key into the vulnerable machine to allow access into the system. After copying our SSH public key, was now able to access the remote machine via SSH as the root giving full control of the system. The system was able to be accesses because of asymmetric cryptography, as we knew the private key for the public SSH key that was copied into the vulnerable machine's root directory, so was able to decrypt and authenticate to enter the system.

*(**2.1**) Activity 3 Firewalls*

Observing the use of firewalls through using Iptables as a stateful firewall

*(**2.2**)*

Firewalls are used to monitor and control the incoming and outgoing network flows based on a set of criteria, firewalls can be on devices installed between networks or on the host machine itself. They act as the very first layer of defence to stop others from accessing services that shouldn't be. In the case of the activity the criteria for the firewall was the IP and the ports having to match. This is done by using the INPUT chain on the Filter table one of many from Iptables. A stateful firewall can be configured from Iptables, the rules can be defined in any way you want to match multiple criteria, as the rules are looked at in a certain order. In the activity we were able to observe allowing two ports for the firewall criteria after reopening the firewall, after configuring the firewall to block all the ports due to the machine being compromised to flush out the attackers.