Muhammad Izham Bin Norhamadi
B032020039

Lab 7

Exercise 1

1- Definition of Antivirus

Antivirus software is a computer program used to prevent, detect and remove malware.

2- Antivirus Important features

Some of the important features in antivirus are virus and threat protection, real-time threats scanning and web protection.

3- How often to run an anti virus scan

Depending on the sensitivity and importance of a system, we can schedule the frequency of virus scanning to make sure the system is clear of any malicious softwares. Home users typically has the virus scan scheduled once every week during the weekend.

Exercise 2

1- Definitions

Password Policy

A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. A password policy is often part of an organization's official regulations and may be taught as part of security awareness training.

Account Lockout Policy

Account lockout threshold policy setting determines the number of failed sign-in attempts that will cause a user account to be locked. A locked account cannot be used until an admin reset or until the number of minutes specified by the account lockout duration policy setting expires.

Audit Policy

Provides information about basic audit policies that are available in Windows and links to information about each setting. The basic audit policy settings are:

- Audit account logon events
- Audit account management
- Audit directory service access
- Audit logon events
- Audit object access
- Audit policy change
- Audit privilege use
- Audit process tracking
- Audit system events

User Right Assignment

User Rights Assignment covers both the privileges and user rights that have been assigned to user accounts. Privileges determine the type of system operations that a user account can perform whereas account rights determine the type of logon that a user account can perform

Exercise 3

1. The importance of configuring firewall settings

Firewall policy configuration is based on network type, such as public or private, and can be set up with security rules that block or allow access to prevent potential attacks from hackers or malware.

2. Block all incoming connections and notify user for blocked program

Block all incoming connections blocks all incoming data connections to the computer, including all of the programs on the whotelist of connections that's normally allowed. Notify user for blocked program is the default option for firewall, where windows firewall notify user for any suspicious movement on the network. It is more secured to block all incoming connections but softwares or services that requires connection may unable to perform in this firewall setting.

3. Inbound and Outbound rules

Inbound rules filter traffic passing from the network to the local computer based on the filtering conditions specified in the rule, which typically are someone from outside your computer that wants to initiate a connection such as a server receiving requests from user.

Outbound rules filter traffic passing from the local computer to the network based on the filtering conditions specified in the rule. These rules are so that you can let some programs use the internet and block others such as the web browser.