VLab 11

Required discussion questions for this week are:

1.3.2.1: Windows server backup

1.4.1: Damage to the system could cause both the original and the backup location to be destroyed.

1.4.2: You can use a USB or optical disk as alternative locations for backup storage. An advantage is that is portable and does not have to stay in one location, a disadvantage is that it’s easy to lose.

1.4.3: Full backup: copies all data to a storage medium, regardless of whether the data is new or changed.

            Incremental backup: copies only data that has changed since the last full or incremental backup.

            Differential backup: copies only data that has changed since the last full backup.

2.2.6.1: To ensure that backups are not corrupt or damaged and that they are actually being run

2.2.9.2: Files and folder

2.3.1: Yes

2.3.2: rpcapd

2.4.1: Files, you can browse volumes included in this backup and select files and folder.

Volumes, You can restore an entire volume, such as all data stored on C:

System State, You can restore just the system state.

3.2.1:

 1: Virus, code added to legitimate programs activated when the program is run, then writes itself to memory and runs instead of the legitimate program.

2: Worm, replicates quickly, which can cause high bandwidth consumption and resource overload. It carries a payload, can carry out an action such as deleting files or stealing data.

3.2.2: Stealthy, malicious software program designed to conceal itself in a system and allows remote access and control of a system without detection by the user or security programs.

3.2.3: Eicar files are standardized test file for signature based virus detection software.  These files are not viruses, but simulate a virus based on the code structure of the file. They are recognized and  marked as an infected file.