A.4

Level 1: Malware Definitions

Malware: is spread by a number of different mechanisms (routes of infection). Research and summarize each of the following attack methods.

Worm: A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it.

Virus: A computer virus is a type of malicious software that, when executed, replicates itself by modifying other computer programs and inserting its own code.

Exploit: An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic.

Phish: Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising as a trustworthy entity in an electronic communication

Explain how a worm is different from a virus.

In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate.

Research exploits in more detail and summarize two different exploit attacks.

In the realm of cybersecurity, exploits are malicious programs that take advantage of application software or operating system vulnerabilities. Such vulnerabilities represent critical security gaps for organizations and individual users alike, and software vendors are compelled to regularly issue patches that fix vulnerabilities discovered through their own internal quality testing or by application users themselves. Two examples of exploit attacks is with the recent discovery of people using the google chrome address bar for phishing purposes, or the discovery of a flaw found in the crypto currency Zcoin, which is claimed to now being put other crypto currencies in risk.

Once a computer is infected the malware may have one of many different effects. Research and summarize each of the following malware effects.

Ransom ware: Ransom ware is a type of malicious software from crypto virology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

Denial of Service (DoS):  A cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

Spyware: Spyware is software that aims to gather information about a person or organization, sometimes without their knowledge, that may send such information to another entity without the consumer's consent

Trojan: Trojan Horse hides malware in what appears to be a normal file. There are a wide variety of Trojan viruses on the Internet landscape that can perform an array of tasks. Most Trojans are typically aimed at taking control of a user’s computer, stealing data and inserting more malware on to a victim’s computer.

Research spyware in more detail and summarize two different spyware virus attacks.

Level 2: Updates & Protection

Firewall / Windows Firewall

Firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Software Updates / Automatic Updates

A software update, which is sometimes called a software patch, is a free download for an application, operating system, or software suite that provides fixes for features that aren't working as intended or adds minor software enhancements and compatibility.

Cookies / Security Certificates

A small text file (up to 4KB) created by a website that is stored in the user’s computer either temporarily for that session only or permanently on the hard disk (persistent cookie).Cookies provide a way for the website to recognize you and keep track of your preferences.

Level 3: Anti-Virus Products

Research a product

Norton Antivirus

List and explain major features

* One solution to protect your devices
* Provides protection against viruses, spyware, malware, and other online attacks
* Maintains your privacy, no matter what device you are using
* Avoids unsafe websites and suspicious downloads
* Lets you move protection from one device to another
* Lets you add more protection as you get more devices\*
* Easily locates lost or stolen smartphones and tablets