**Lesson 1 Key Terms**

* **adware** A general term for software that uses typical malware intrusion techniques to obtain marketing data or advertise a product or service.
* **availability**The efforts taken through policy, procedures, and design in order to create and maintain the accessibility of resources within a database environment.
* **back door** A method created during the programming of a worm in which access is gained into a system by avoiding normal security, which gives the creator of the worm undetected access into the system.
* **backup** An intentional copy of data, program files, and system configurations that is used to archive and store information in the event of network failure or malware attacks.
* **backup management plan** A process developed to ensure the safety of the data on a network.
* **black hat** Someone who breaks into computer networks without authorization and with malicious intent.
* **boot sector** An area of the hard disk that contains records necessary to the boot process of a computer.
* **boot sector virus** Malware that infiltrates a system by loading itself onto the boot sector of a hard disk via an infected floppy disk left in a floppy disk drive.
* **bot (software robot)**A form of malware that has the ability to perform a large array of automated tasks for an intruder at a remote location, ranging in severity from spamming a system to initiating DoS attacks on systems.
* **botmaster** An individual who controls a network of bots and who accumulates a number of bots and then rents these botnets to other intruders and cybercriminals for the purpose of spamming, phishing, and other more serious types of cybercrime.
* **botnet** A network of bots.
* **cold site** A facility that provides the basic necessities for rebuilding a network. A contract that involves a cold site would promise the use of a facility that provides water, power, air conditioning, or heat.
* **computer security** A set of established procedures, standards, policies, and tools that are used to protect a computer from theft, misuse, and unwanted intrusions, activities, and attacks.
* **computer virus** A form of malware intended to spread from one computer to another without detection.
* c**onfidentiality**The efforts taken through policy, procedure, and design in order to create and maintain the privacy and discretion of information and systems.
* **cracker** An individual who breaks into our networks without authorization with hopes to destroy and/or steal information.
* **database security** A set of established procedures, standards, policies, and tools that are used to protect data from theft, misuse, and unwanted intrusions, activities, and attacks.
* **data sending**Trojan Malware that obtains sensitive data from your computer and transmits it back to a cracker.
* **denial of service (DoS) attack**A concerted effort made by malware to keep system resources, such as Internet sites, from functioning correctly.
* **destructive**Trojan Malware that is installed on a computer with the intent to destroy a system as a whole by randomly deleting files and folders and corrupting the registry.
* **differential backup** An intentional copy of data, program files, and system  configurations that only saves the data that has changed since the last backup was complete.
* **disaster plan** A plan developed to ensure the quick reinstatement of a network that has fallen victim to a human or naturally caused disaster.
* **DNS poisoning** An intrusion where a cracker gains control over the DNS server and changes the domain name’s respective IP address, redirecting requests to sites that the cracker has built and maintains.
* **encryption** The transformation of data by using sophisticated algorithms in an attempt to make the data unrecognizable.
* **file-infected virus**A form of malware that will attach itself to an executable file that requires a user to run before it can propagate and corrupt the system.
* **file transfer protocol (FTP)** Trojan Malware that allows the attacker to use someone else’s computer as an FTP server.
* **full backup** An intentional copy of data, program files, and system configurations that stores all information, regardless of its critical nature, age, and prior backup activity.
* **grey hat** An individual or groups of individuals who waver between the classification of a hacker and a cracker, and who either act in goodwill or in malice.
* **hacker**Someone who has mastered the hardware and software of modern computer systems and enjoys the exploration and analysis of network security with no intent to intrude or cause harm.
* **hactivist** Hackers and crackers who use their extensive experience and skill to use networks to share their ideologies regarding controversial social, political, and economic topics.
* **Health Insurance Portability and Accountability Act (HIPAA)** Strict laws for health institutions throughout the United States that ensure the security and privacy of patient records by dictating the way in which files are accessed, stored, and transmitted on a network.
* **hijacking** A process in which Web sites are hacked into and rewritten to react differently to users than how the original Web site designer intended.
* **hot site** An exact replica of an organization’s network, or a mirror site, that promises the vendor will assume all responsibility for ensuring that the network is readily available in the event of a disaster.
* **hypertext transfer protocol (HTTP)**The portion of an Internet address that informs the browser what protocol is used to send the request for a particular Web site.
* **incremental backup**An intentional copy of data, program files, and system configurations that is conducted on only the data that has changed since the last full or incremental backup.
* **integrity** Efforts taken through policy, procedure, and design in order to create and maintain reliable, consistent, and complete information and systems.
* **logic bomb** Malware that can lie dormant until a specific predetermined variable is met, whose variables typically depend on the environment in which it resides.
* **macro** A small program that enables users to automate a large number of repeated processes within a document.
* **macro virus** Malware that can either be attached to a macro, or can replace a macro within a document, and that runs automatically when the document containing the infected macro is opened or closed.
* **malicious software** A programming code written and used by unauthorized intruders to perform a certain task on a computer.
* **malware** An abbreviation for the term malicious software.
* **misleading applications** Applications that deceive users into believing that their computer’s security has been breached, therefore tricking the user into downloading and purchasing rogue antivirus tools to remove the bogus breach.
* **multipartite virus** A form of malware that combines the characteristics of a boot sector virus with those of a file-infected virus.
* **network security** A set of established procedures, standards, policies, and tools that are used to protect data from theft, misuse, and unwanted intrusions, activities, and attacks.
* **nonresident virus** The general term for malware that requires users to initiate it by downloading a program or opening up an e-mail attachment.
* **operational information security** Ensures the secure operation of an organization through the development and reliability of an environment’s policies and procedures that focus on security policies, change management, update management, and disaster recovery plans.
* **OS upgrade**Installing a new version of an operating system onto a host or a server.
* **patch**A small program that is used to fix or update software programs or hardware devices.
* **payload** The component of a worm that holds all of the instructions on how to affect each computer that it encounters.
* **personal identifiable information (PII)** Personal information that identifies a person.
* **phishing** The attempt to obtain PII from people through the use of spoofed e-mail addresses and URLs.
* **polymorphism** The incidence of changing forms, or self-modification.
* **proxy**Trojan Malware that enables a cracker to use someone else’s computer to access the Internet in order to keep their identity hidden.
* **remote access and administration Trojan (RAT)** Malware that provides remote access capability to the cracker from whom the virus originated, who in turn is provided complete control of and access to someone else’s computer from a remote location.
* **resident virus** Malware that installs itself or takes residence directly in the main system memory of a computer.
* **script kiddie** Amateur crackers that use programs and scripts written by other people to infringe upon a computer network system’s integrity.
* **security policy** A document that defines the overall goal of security and identifies the scope of what to secure, as well as the roles and responsibilities of the people within the organization.
* **shared site agreement** An arrangement between companies with similar, if not identical, data centers.
* **signature** A pattern of characters that is identified for a specific family of viruses.
* **social engineer** An individual who uses human interaction to manipulate people into gaining access to systems, unauthorized areas, and confidential information.
* **software upgrade** A combination of a number of software or hardware packages that creates a new version of software.
* **spoofing** A process that involves hackers building Web sites to look identical to other popular sites in hopes of drawing in a user.
* **spyware** A general term for any software that intentionally monitors and records a user’s computer and/or Internet activities.
* **startup page** The Web site that is displayed when the Web browser is started.
* **time bomb (time-delayed virus)** Malware that can lie dormant until a specific variable is met, such as times, days, or specific days that are predetermined and written within its code.
* **transmission packet** Sensitive information about users or businesses compiled by spyware that is sent back to its original creators for use as they see fit.
* **Trojan (Trojan horse)**Malware that disguises itself and its harmful code and often hides within enticing programs such as software updates, games, and movies.
* **update** A change to a system that is added to software or firmware that is already installed on a network.
* **update management policy** A document that includes procedures for patch updates, software upgrades, OS upgrades, and firmware changes.
* **upgrade** Replacements for older versions of software or firmware.
* **warm site** A facility that contains the basic environmental concerns, as well as computers, connection firmware, and software devices necessary to rebuild a network system.
* **Web browser** An application that acts as a user interface of the Internet, allowing users to interact and view Web pages on the World Wide Web.
* **Web page** A document containing a specific programming language (e.g., HTML or JAVA) that is designed to be viewable on the World Wide Web.
* **white hat** An ethical hacker; hackers who use their extensive experience and knowledge to test systems and provide security consultation to others.
* **worm**Self-replicating malware that is able to harness the power of networks and use this power in its attacks against them.