Security Glossary - from CMU/SEl-2OO8-SR-O17 – Appendix.

Access control: Access control ensures that resources are only granted to those users who are entitled to them [SANS 2oo3].

Access control list: A list of access control entries apply to an entire object, a set of the object's properties or an individual property of an object, and that define the access granted to one or more security principals [Tulloch 2oo3].

Artifact: The remnants of an intruder attack or incident activity. These could be software used by intruder(s), a collection of tools, malicious code, logs, files, output from tools, status of a system after an attack or intrusion [West-Brown 2oo 3].

Attack: An action conducted by an adversary, the attacker, on a potential victim. A set of events that an observer believes to have information assurance consequences on some entity, the target of the attack [Ellison 2oo3].

Auditing: The information gathering and analysis of assets to ensure such things as policy compliance and security from vulnerabilities [SANS 2oo3].

Authentication: The process of determining whether someone or something is, in fact, who or what it is declared to be [SearchSecurity 2oo8].

Authorization: The process of granting a person, computer process, or device access to certain information, services, or functionality. Authorization is derived from the identity of the person, computer process, or device requesting access, which is verified through authentication [Tulloch 2oo3].

Availability: The property of a system or a system resource that ensures it is accessible and usable upon demand by an authorized system user. Availability is one of the core characteristics of a secure system [Tulloch 2oo3].

Back door: A hardware or software-based hidden entrance to a computer system that can be used to bypass the system's security policies [Tulloch 2 oo3].

Breach: Any intentional event where an intruder gains access that compromises the confidentiality, integrity, or availability of computers, networks, or the data residing on them [CERT/CC 2oo4].

Brute force: A cryptanalysis technique or other kind of attack m ethod involving an exhaustive procedure that tries all possibilities, one by one [SANS 2oo3].

Cache poisoning: Malicious or misleading data from a remote name server is saved [cached] by another name server. Typically used with DNS cache poisoning attacks [SANS 2oo3].

Confidentiality: The property that information is not made available or disclosed to unauthorized indi- viduals, entities, or processes (i.e., to any unaut horized system entity) [SANS 2oo3].

Control: An action, device, procedure, or technique that removes or reduces vulnerability.

Corruption: A threat action that undesirably alters system operation by adversely modifying system functions or data [SANS 2oo3].

Cracker: Someone who breaks into someone else's computer system, often on a network, by- passes passwords or licenses in computer programs, or or in other ways intentionally breaches computer security [SearchSecurity 2oo8].

Denial-of-service (DoS) attack: An attempt of a malicious (or unwitting) user, process, or system to prevent legitimate users from accessing a resource (usually a network service) by exploiting a weakness or design limitation in an information system. Examples of DoS attacks include flooding network connections, filling disk storage, disabling ports, and removing power [Tulloch 2oo3].

Disaster recovery plan: A plan that helps a company recover data and restore services after a disaster [Tulloch 2oo3].

Disclosure: A component of the notice principle, wherein a company should make available its data handling practices, including notices on how it col lects, uses, and shares personally identifiable information [Tulloch 2oo3].

Disgruntled employee: A person in an organization who deliberately abuses or misuses computer systems and their information [Alberts 2oo3].

Encryption: The cryptographic transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used [SANS 2oo3].

Fault tolerance: [The property of] a computer system or component designed so that, in the event that a component fails, a backup component or procedure can immediately take its place with no loss of service. Fault tolerance can be provided with software, embedded in hardware, or provided by some combination [SearchSecurity 2oo8].

Firewall: A security solution that segregates one portion of a network from another portion, allowing only authorized network traffic to pass through according to traffic-filtering rules [Tulloch 2oo3].

Hacker: Someone who engages in the activity of hacking computer programs, systems, or net- works [Tulloch 2oo3].

Integrity: For data, the property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner [Allen 1999].

Intrusion: An attempt to compromise a system or network [Tulloch 2oo3].

Intrusion detection system: A combination of hardware and software that monitors and collects system and network information and analyzes it to determine if an attack or an intrusion has occurred. Some IT systems can automatically respond to an intrusion [Allen 1999].

Liability: The responsibility of someone for damage or loss [West-Brown 2oo3].

Malware: Programming or files that are developed for the purpose of doing harm. Thus, malware includes computer viruses, worms, and Trojan horses [Webopedia 2oo8].

Man-in-the-middle attack: A computer attack during which the cyber criminal funnels communication between a consumer and a legitimate organization through a fake website. In these attacks, neither the consumer nor the organization is aware that the communication is being illegally monitored. The criminal is, in effect, in the middle of a transaction between the consumer and his or her bank, credit card company, or retailer [BSA 2oo8].

Non-repudiation: A technique used to ensure that someone performing an action on a computer cannot falsely deny that they performed that action [Tulloch 2oo3].

Patching: The process of updating software to a new version that fixes bugs in a previous version [SANS 2oo3].

Physical security: Security measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment [Guttman 1995].

Privacy: The quality or condition of being secluded from the presence or view of others [Dictionary.com 2008].

Recovery: A system's ability to restore services after an intrusion has occurred. Recovery also contributes to a system's ability to maintain essential services during intrusion [Ellison 2oo3].

Risk: The product of the level of threat with the level of vulnerability. It establishes the likelihood of a successful attack [SANS 2oo3].

Spoof: Making a transmission appear to come from a user other than the user who performed the action [Microsoft 2005].

Stakeholder: Anyone who is a direct user, indirect user, manager of users, senior manager, operations staff member, support (help desk) staff member, developer working on other systems that integrate or interact with the one under development, or maintenance professionals potentially affected by the development and/or deployment of a software project [Ambler 2004].

Stealthing: A term that refers to approaches used by malicious code to conceal its presence on an infected system [SANS 2003].

Survivability: The capability of a system to complete its mission in a timely manner, even if significant portions are compromised by attack or accident. The system should provide essential services in the presence of successful intrusion and recover compromised services in a timely manner after intrusion occurs [Mead 2003].

Target: The object of an attack, especially host, computer, network, system, site, person, organization, nation, company, government, or other group [Allen 1999].

Threat: A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cau se harm [SANS 2oo3].

Threat assessment: The identification of the types of threats that an organization might be exposed to [SANS 2003].

Threat model: Used to describe a given threat and the harm it could to do a system if it has a vulnerability [SANS 2003].

Trust: Determines which permissions other systems or users have and what actions they can perform on remote machines [SANS 2oo3].

Virus: A hidden, self-replicating section of computer software, usually malicious logic, which propagates by infecting—i.e., inserting a copy of itself into and becoming part of—another program. A virus cannot run by itself; it requires that its host program be run to make it active [SANS 2003]. Compare worm.

Vulnerability: Anything that gives an attacker the opportunity to perform an exploit.

Worm: Self-propagating malicious code that can automatically distribute itself from one computer to another through network connections. A worm can take harmful action, such as consuming network or local system resources, possibly causing a denial-of-service attack [Microsoft 2005]. Compare virus.