Glossary of Terms

Access - Ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.

Access Control List (ACL) - A register of: 1. users (including groups, machines, processes) who have been given permission to use a particular system resource, and 2. the types of access they have been permitted.

Access Point - A device that logically connects wireless client devices operating in infrastructure to one another and provides access to a distribution system, if connected, which is typically an organization's enterprise wired network

Active Content - Software in various forms that is able to automatically carry out or trigger actions on a computer platform without the intervention of a user.

Administrative Account (Admin/Root/Super User) - A user account with full privileges on a computer.

Advanced Encryption Standard (AES) - The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. This standard specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits

Antivirus Software - A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents.

Asymmetric Keys - Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.

Audit Log - A chronological record of system activities. Includes records of system accesses and operations performed in a given period.

Authentication - Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Authentication Mechanism - Hardware-or software-based mechanisms that force users to prove their identity before accessing data on a device.

Authentication Protocol - A defined sequence of messages between a Claimant and a Verifier that demonstrates that the Claimant has possession and control of a valid token to establish his/her identity, and optionally, demonstrates to the Claimant that he or she is communicating with the intended Verifier.

Banner - Display on an information system that sets parameters for system or data use.

Banner Grabbing - SOURCE: CNSSI-4009 Banner Grabbing – The process of capturing banner information—such as application type and version—that is transmitted by a remote port when a connection is initiated.

Biometric - A measurable physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics.

Biometric System - An automated system capable of: 1) capturing a biometric sample from an end user; 2) extracting biometric data from that sample; 3) comparing the extracted biometric data with data contained in one or more references; 4) deciding how well they match; and 5) indicating whether or not an identification or verification of identity has been achieved.

Blacklisting - The process of the system invalidating a user ID based on the user's inappropriate actions. A blacklisted user ID cannot be used to log on to the system, even with the correct authenticator. Blacklisting and lifting of a blacklisting are both security-relevant events. Blacklisting also applies to blocks placed against IP addresses to prevent inappropriate or unauthorized use of Internet resources.

Block Cipher - A symmetric key cryptographic algorithm that transforms a block of information at a time using a cryptographic key. For a block cipher algorithm, the length of the input block is the same as the length of the output block.

Block Cipher Algorithm - A family of functions and their inverses that is parameterized by a cryptographic key; the function maps bit strings of a fixed length to bit strings of the same length.

Blue Team –

1. The group responsible for defending an enterprise's use of information systems by maintaining its security posture against a group of mock attackers (i.e., the Red Team). Typically the Blue Team and its supporters must defend against real or simulated attacks 1) over a significant period of time, 2) in a representative operational context (e.g., as part of an operational exercise), and 3) according to rules established and monitored with the help of a neutral group refereeing the simulation or exercise (i.e., the White Team).

2. The term Blue Team is also used for defining a group of individuals that conduct operational network vulnerability evaluations and provide mitigation techniques to customers who have a need for an independent technical review of their network security posture. The Blue Team identifies security threats and risks in the operating environment, and in cooperation with the customer, analyzes the network environment and its current state of security readiness. Based on the Blue Team findings and expertise, they provide recommendations that integrate into an overall community security solution to increase the customer's cyber security readiness posture. Often times a Blue Team is employed by itself or prior to a Red Team employment to ensure that the customer's networks are as secure as possible before having the Red Team test the systems.

Boundary Protection Device - A device with appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (ii) provides information system boundary protection.

Brute Force Password Attack – A method of accessing an obstructed device through attempting multiple combinations of numeric and/or alphanumeric passwords.

Buffer Overflow – A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system.

Buffer Overflow Attack - A method of overloading a predefined amount of space in a buffer, which can potentially overwrite and corrupt data in memory.

Certificate - A digitally signed representation of information that 1) identifies the authority issuing it, 2) identifies the subscriber, 3) identifies its valid operational period (date issued / expiration date).

In the information assurance (IA) community, certificate usually implies public key certificate and can have the following types:

cross certificate – a certificate issued from a CA that signs the public key of another CA not within its trust hierarchy that establishes a trust relationship between the two CAs.

encryption certificate – a certificate containing a public key that can encrypt or decrypt electronic messages, files, documents, or data transmissions, or establish or exchange a session key for these same purposes. Key management sometimes refers to the process of storing, protecting, and escrowing the private component of the key pair associated with the encryption certificate.

identity certificate – a certificate that provides authentication of the identity claimed. Within the National Security Systems (NSS) PKI, identity certificates may be used only for authentication or may be used for both authentication and digital signatures.

Clear Text - Information that is not encrypted.

Command Line Interface (CLI) – A text-based way to interface with a workstation.

Common Vulnerability Scoring System (CVSS) - An SCAP specification for communicating the characteristics of vulnerabilities and measuring their relative severity

Credential - An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a Subscriber.

Cross Site Scripting (XSS) – A vulnerability that allows attackers to inject malicious code into an otherwise benign website. These scripts acquire the permissions of scripts generated by the target website and can therefore compromise the confidentiality and integrity of data transfers between the website and client. Websites are vulnerable if they display user supplied data from requests or forms without sanitizing the data so that it is not executable.

Cryptography - Is categorized as either secret key or public key. Secret key cryptography is based on the use of a single cryptographic key shared between two parties. The same key is used to encrypt and decrypt data. This key is kept secret by the two parties. Public key cryptography is a form of cryptography which makes use of two keys: a public key and a private key. The two keys are related but have the property that, given the public key, it is computationally infeasible to derive the private key

[FIPS 140-1]. In a public key cryptosystem, each party has its own public/private key pair. The public key can be known by anyone; the private key is kept secret

Demilitarized Zone (DMZ) - Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

Exploit Code – A program that allows attackers to automatically break into a system.

Flooding - An attack that attempts to cause a failure in a system by providing more input than the system can process properly.

Graphical User Interface (GUI) – An interactive desktop that allows the user to interface with installed software graphically.

Industrial Control System (ICS) - An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems (SCADA) used to control geographically dispersed assets, as well as distributed control systems (DCS) and smaller control systems using programmable logic controllers to control localized processes.

Insider Threat - An entity with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service.

Intrusion Prevention System (IPS) – System(s) which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.

Man in the Middle - A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association.

Network Access Control (NAC) - A feature provided by some layer 3 network devices that allows access based on a user's credentials and the results of health checks performed on the telework client device.

Network Address Translation (NAT) - A routing technology used by many firewalls to hide internal system addresses from an external network through use of an addressing schema.

Operating System (OS) Fingerprinting - Analyzing characteristics of packets sent by a target, such as packet headers or listening ports, to identify the operating system in use on the target.

Packet Sniffer - Software that observes and records network traffic.

Phishing - Deceiving individuals into disclosing sensitive personal information through deceptive computer-based means.

Port Scanning - Using a program to remotely determine which ports on a system are open (e.g., whether systems allow connections through those ports).

Proxy - An application that “breaks” the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it. Note: This effectively closes the straight path between the internal and external networks, making it more difficult for an attacker to obtain internal addresses and other details of the organization’s internal network. Proxy servers are available for common Internet services; for example, a Hyper Text Transfer Protocol (HTTP) proxy used for Web access, and a Simple Mail Transfer Protocol (SMTP) proxy used for email.

Proxy Server - A server that services the requests of its clients by forwarding those requests to other servers.

Red Team - A group of people authorized and organized to emulate a potential adversary’s attack or exploitation capabilities against an enterprise’s security posture. The Red Team’s objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment.

Remediation - The act of correcting a vulnerability or eliminating a threat. Three possible types of remediation are installing a patch, adjusting configuration settings, or uninstalling a software application.

Replay Attack - An attack that involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access.

Risk Assessment - The process of identifying, prioritizing, and estimating risks. This includes determining the extent to which adverse circumstances or events could impact an enterprise. Uses the results of threat and vulnerability assessments to identify risk to organizational operations and evaluates those risks in terms of likelihood of occurrence and impacts if they occur. The product of a risk assessment is a list of estimated potential impacts and unmitigated vulnerabilities. Risk assessment is part of risk management and is conducted throughout the Risk Management Framework (RMF).

Symmetric Key - A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code.

References –

CNSSI-4009 The Committee on National Security Systems Instruction No 4009

Federal Information Security Management Act (FISMA) P.L. 107-347, December 2002.

NISTIR 7298 Revision 2