Important Computer Security Terms & Terminology:

Access Control: Access Control ensures that resources are only granted to those users who are entitled to them.

Access Control List (ACL): A mechanism that implements access control for a system resource by listing the identities of the system entities that are permitted to access the resource.

Access Control Service: A security service that provides protection of system resources against unauthorized access. The two basic mechanisms for implementing this service are ACLs and tickets.

Access Management Access: Management is the maintenance of access information which consists of four tasks: account administration, maintenance, monitoring, and revocation.

Account Harvesting: Account Harvesting is the process of collecting all the legitimate account names on a system.

Active Content: Program code embedded in the contents of a web page. When the page is accessed by a web browser, the embedded code is automatically downloaded and executed on the user's workstation. Ex. Java, ActiveX (MS)

Activity Monitors: Activity monitors aim to prevent virus infection by monitoring for malicious activity on a system, and blocking that activity when possible.

Address Resolution Protocol (ARP): Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address to a physical machine address that is recognized in the local network. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

Advanced Encryption Standard (AES): An encryption standard being developed by NIST. Intended to specify an unclassified, publicly-disclosed, symmetric encryption algorithm.

Algorithm: A finite set of step-by-step instructions for a problem-solving or computation procedure, especially one that can be implemented by a computer.

Adware: The difference between Adware and Spyware is very subtle. Both Adware and Spyware is installed without the user's permission on a machine. An Adware's main purpose is to display targeted ads based on the user behavior it is tracking.

It is not uncommon for people to confuse "adware" with "spyware" and "malware", especially since these concepts overlap. For example, if one user installs "adware" on a computer, and consents to a tracking feature, the "adware" becomes "spyware" when another user visits that computer, and interacts with and is tracked by the "adware" without their consent.

Authentication: Authentication is verifying who you are. There are numerous ways to implement authentication; each has pros and cons. The most widely implemented authentication mechanism is by password. Various other authentication mechanisms are as follows:

- Digital Certificate, such as those used in the X.509 format. This is when a message is encrypted with a private key. The message can be decrypted by a public key and validated against a certificate of authority. Unfortunately, the private key is usually protected by a symmetrically encrypted key, specifically, a password.

- Hardware token, such as SecurID. The hardware token generates a random number at a specified time interval using a proprietary algorithm. This number is synchronized with an authenticating server, and combined with a personal PIN composed of alphanumeric characters. The randomly generated number expires after the next number is generated preventing its reuse.
- Biometric Technologies such as voice pattern recognition, Iris/Retina scanning, and fingerprinting are the new wave of authentication technologies. Problems such as losing or forgetting your hardware token, password, or digital certificate become a thing of the past.

Authorization: Authorization is granting or denying access to a service based on who you say you are. Authorization is often tightly integrated with authentication, and thus often confused with authentication. Authorization depends on being able to authenticate an identity, but checks that identity against an access control list to grant or deny access. The access control list can be stored in a configuration in a file, in non-volatile RAM, or in a distributed database such as LDAP, Active Directory, or NetWare Directory Services.

Integrity: Integrity is the process of validating that the data provided by an authenticated source has not been changed. This is often done by running an algorithm over a set of selected data to produce a hash or message digest. This value is then protected by encrypting it and attaching it to the original data. The process of computing the hash, encrypting it, and attaching it to the original data is called digitally signing data.

To validate that the integrity has not been compromised, a new hash or message digest is computed and compared to the decrypted value. If they match, there is no way the data could have been modified without the key used to protect the data originally. Theoretically, only the original person/company would have access to that key. This allows you to validate the digital signature on the data.

BackDoor: A backdoor is a program designed to give access to the attacked host at a later point of time. These backdoors use well known ports such as 80 or 445. However the most common port used by Backdoor programs is 6667 or the port used by Internet Relay Chat(IRC) which is a camping ground these days for Botnet farmers. These backdoors are used by attackers when launching DDoS attacks.

Black Box Penetration Testing: In this model, there is no interaction between the company and the tester. This means no interviews, no network layouts…nothing. This is the better form of testing as this does not warn the employees who might behave more vigilantly than they might otherwise have been. This form of testing allows a company to see how it might respond to an attack as well as get a better assessment of its security policies as the employees are not forewarned.

Blue Screen of Death (BSoD): When a Windows NT-based system encounters a serious error, the entire operating system halts and displays a screen with information regarding the error. The name comes from the blue color of the error screen.

Buffer Overflow: A buffer overflow occurs when a program writes more data in memory than it was initially allotted (buffer space). In the example shown below, a buffer overflow is caused if a user enters a string of more than 20 characters. 19 or less does not cause an overflow.

Certificate: An electronic document attached to someone's public key by a trusted third party, which attests that the public key belongs to a legitimate owner and has not been compromised. Certificates are intended to help you verify that a file or message actually comes from the entity it claims to come from.

Certificate Authority (CA): A trusted third party (TTP) who verifies the identity of a person or entity, then issues digital certificates vouching that various attributes (e. g., name, a given public key) have a valid association with that entity.

Computer Virus: A Virus is a computer program which attaches itself to an executable file or an application. A computer virus is not standalone and needs a host file or program to work or replicate.

Compliance: Government or industry imposed regulations and best practices.

Cookie: A text file passed from the Web server to the Web client (a user's browser) that is used to identify a user and could record personal information such as ID and password, mailing address, credit card number, and more. A cookie is what enables your favorite Web site to "recognize" you each time you revisit it.

Cracker: A person who break into computer systems with the intent of doing harm or destroying data.

Denial-of-service attack: A denial-of-service attack (DoS attack) is an attempt to make a computer resource unavailable to its intended users. Typically the targets are high-profile web servers, and the attack attempts to make the hosted web pages unavailable on the Internet.

Digital Signature or digital signature scheme: is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

Distributed Denial-of-service attack (DDoS): A distributed denial of service attack (DDoS) occurs when multiple compromised systems flood the bandwidth or resources of a targeted system, usually a web server(s). Script kiddies use them to deny the availability of well known websites to legitimate users. More sophisticated attackers use DDoS tools for the purposes of extortion — even against their business rivals.

Encryption: the process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

Hacker: Originally used to describe a computer enthusiast who pushed a system to its highest performance through clever programming, the term hacker through media portrayal has evolved and often confused with "cracker" as someone who tries to access a computer or a network without prior approval of the systems owner.

Hacking: The U.S. Dept. of Justice defines Hacking as "All illegal access to a computer or a network".

Key: A piece of information (a parameter) that determines the functional output of a cryptographic algorithm or cipher. Without a key, the algorithm would produce no useful result. In encryption, a key specifies the particular transformation of plaintext into cipher text, or vice versa during decryption. Keys are also used in other cryptographic algorithms, such as digital signature schemes and message authentication codes.

Malware: Malware is any malicious software designed to disrupt the working of a network. Virus, worms and Trojans fall under the category of Malware.

Personally Identifiable Information (PII): Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Ping-of-Death attack: A ping of death (abbreviated "POD") is a type of attack on a computer that involves sending a malformed or otherwise malicious ping to a computer. A ping is normally 64 bytes in size; many computer systems cannot handle a ping larger than the maximum IP packet size, which is 65,535 bytes. Sending a ping of this size often crashes the target computer.

Penetration Test: In a Penetration test, you the tester are trying to break into a network and gain access to their systems, trying to understand and find its weakest link.

Phishing: The use of e-mails that appear to originate from a trusted source to trick a user into entering valid credentials at a fake website. Typically the e-mail and the web site looks like they are part of a bank the user is doing business with.

Ports: A port is a logical component of the TCP connection. Learning more about ports will help you better defend your network by closing off ports and services which are not required. Remember, if a port is open, even something like port 80 which you use to access the internet, if you can get out, then a Hacker can get in.

Policy: Company imposed rules regarding access and editorial control at the file level.

RootKit: A root kit is a collection of programs that intruders often install after they have compromised the root account of a system. RootKits are the deadliest of the Trojan horses as they are almost impossible to detect because of their ability to hide and integrate within the OS.

Spyware: Spyware is a program or software that resides on an infected computer and collects various information about the users without their informed consent. This personal information is secretly recorded with a variety of techniques, including logging keystrokes, recording Internet web browsing

history, and scanning documents on the computer's hard disk. Purposes range from overtly criminal (theft of passwords and financial details) to the merely annoying (recording Internet search history for targeted advertising, while consuming computer resources)

Security Test: In a security test, you perform a penetration test of a network and then offer solutions to the company and help them tweak their security policies and procedures besides helping them patch up any vulnerabilities and help them secure their network.

Safety: Safety is the need to ensure that the people involved with the company, including employees, customers, and visitors, are protected from harm.

Scavenging: Searching through data residue in a system to gain unauthorized knowledge of sensitive data.

Secure Electronic Transactions (SET) Secure Electronic Transactions is a protocol developed for credit card transactions in which all parties (customers, merchant, and bank) are authenticated using digital signatures, encryption protects the message and provides integrity, and provides end-to-end security for credit card transactions online.

Secure Shell (SSH): Program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another.

Secure Sockets Layer (SSL): A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection.

Security Policy: A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

Sensitive Information: As defined by the federal government, is any unclassified information that, if compromised, could adversely affect the national interest or conduct of federal initiatives.

Separation of Duties: The principle of splitting privileges among multiple individuals or systems.

Server: A system entity that provides a service in response to requests from other system entities called clients.

Session: A session is a virtual connection between two hosts by which network traffic is passed.

Session Hijacking: Take over a session that someone else has established.

Social Engineering: Utilizing publically facing information including social media, public records, etc. to launch a highly targeted attack against an individual (usually a high ranking official within an enterprise) with the goal of accessing sensitive enterprise data from the inside.

TCP three-way handshake: TCP is a connection oriented protocol where the sender doesn't send any data until the destination acknowledges back to the sender. This whole process is called a three-way handshake where the Sender first sends the receiver a SYN packet. The receiver then acknowledges that

it is listening to the sender by sending back a SYN-ACK packet. Finally, the sender sends an ACK packet, thus initiating data transfer.

Trojan: A Trojan is basically a program that disguises itself as a valid or useful computer application or program. These Trojan horses then install a backdoor or a rootkit designed to give entry to the hacker at a later point of time.

White box Penetration Testing: In this model of Penetration Testing, the pen tester has an idea what the network layout/topology looks like along with any applications, switches, routers and OS's running the company's servers. You are also given the opportunity to talk to the company's security analysts and other regular employees.

Worm: A Worm is a computer program that can replicate and propagate itself without the need for a host.