**DOS ATTACKS**

The ICMP echo response packets generated in response to a ping flood using randomly spoofed source addresses is known as backscatter traffic.

Flooding attacks flood the network link to the server with a torrent of malicious packets competing with valid traffic flowing to the server.

The standard protocol used for call setup in VoIP is the Session Initiation Protocol.

Requests and responses are the two different types of SIP messages.

A HTTP flood refers to an attack that bombards Web servers with HTTP requests.

During a reflection attack, the attacker sends packets to a known service on the intermediary with a  spoofed source address of the actual target system and when the intermediary responds, the response is  sent to the target.

In reflection attacks, the spoofed source address directs all the packets at the desired target and any responses  to the intermediary.

Amplification attacks are a variant of reflector attacks and also involve sending a packet with a spoofed  source address for the target system to intermediaries.

The best defense against broadcast amplification attacks is to block the use of IP-directed broadcasts.

The four lines of defense against DDoS attacks are: attack prevention and preemption, attack detection  and filtering, attack source traceback and identification and attack reaction.

Since filtering needs to be done as close to the source as possible by routers or gateways knowing the  valid address ranges of incoming packets, an ISP is best placed to ensure that valid source  addresses are used in all packets from its customers.

A captcha is a graphical puzzle used to attempt to identify legitimate human initiated interactions.

To respond successfully to a DoS attack a good incident response plan is needed that includes details of how to  contact technical personal for your ISP(s).

If an organization is dependent on network services it should consider mirroring and replicating these  servers over multiple sites with multiple network connections.

A denial of service is an action that prevents or impairs the authorized use of networks, systems, or applications  by exhausting resources such as central processing units, memory, bandwidth, and disk space.

**INTRUSION DETECTION**

The three classes of intruders are masquerader, clandestine user and misfeasor.

A misfeasor is a legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges.

Computer Emergency Response Teams are cooperative ventures that collect information about system vulnerabilities and disseminate it to systems mangers.

Intrusion Detection is a security service that monitors and analyzes system events for the purpose of finding, and providing real-time warning of attempts to access system resources in an unauthorized manner.

An IDS comprises three logical components: analyzers, user interface and sensors.

The threshold detection approach involves defining thresholds, independent of user, for the frequency of occurrence of various events.

Profile-based anomaly detection focuses on characterizing the past behavior of individual users or related groups of users and then detecting significant deviations.

Signature detection techniques detect intrusion by observing events in the system and applying a set of rules that lead to a decision regarding whether a given pattern of activity is or is not suspicious.

A distributed IDS consists of three main components: host agent module, central manager module, and LAN monitor agent module.

A network based IDS monitors traffic at selected points on a network or interconnected set of networks.

The Intrusion Detection Message Exchange Requirements (RFC 4766) document defines requirements for the Intrusion Detection Message Exchange Format (IDMEF).

The functional components of an IDS are: data source, sensor, analyzer, administration, manager, and operator.

The security policy is the predefined formally documented statement that defines what activities are allowed to take place on an organization’s network or on particular hosts to support the organization’s requirements.

Honeypots are decoy systems that are designed to lure a potential attacker away from critical systems.

A Snort installation consists of four logical components: packet decoder, detection engine, logger, and alerter.

**FIREWALLS AND INTRUSION PREVENTION**

The firewall is inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter to protect the premises network from Internet-based attacks.

A packet filtering firewall applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet.

The source IP address is the IP address of the system that originated the IP packet.

An intruder transmitting packets from the outside with a source IP address field containing an address of an internal host is known as IP address spoofing.

The SOCKS protocol is an example of a circuit-level gateway implementation that is conceptually a “shim-layer” between the application layer and the transport layer and does not provide network-layer gateway services.

Identified as a critical strong point in the network’s security, the bastion host serves as a platform for an application-level or circuit-level gateway.

A personal firewall controls the traffic between a personal computer or workstation on one side and the Internet or enterprise network on the other side.

A VPN uses encryption and authentication in the lower protocol layers to provide a secure connection through an otherwise insecure network, typically the Internet.

IPSec protocols operate in networking devices, such as a router or firewall, and will encrypt and compress all traffic going into the WAN and decrypt and uncompress traffic coming from the WAN.

A host-based IPS makes use of both signature and anomaly detection techniques to identify attacks.

Pattern matching scans incoming packets for specific byte sequences (the signature) stored in a database of known attacks.

Traffic anomaly watches for unusual traffic activities, such as a flood of UDP packets or a new service appearing on the network.

Snort Inline adds three new rule types: drop, reject, and Sdrop.

A single device that integrates a variety of approaches to dealing with network-based attacks is referred to as a UTM system.

The firewall follows the classic military doctrine of defense in depth because it provides an additional layer of defense.

**BUFFER OVERFLOW**

A buffer overrun is a condition where more input is placed into a buffer or data holding area than the capacity allocated and thus overwrites other information.

At the basic machine level, all of the data manipulated by machine instructions executed by the computer processor are stored in either the processor’s registers or in memory.

UNIX was one of the earliest operating systems written in a high-level language.

A stack buffer overflow occurs when the targeted buffer is located on the stack, usually as a local variable in a function’s stack frame.

The function of the shellcode was to transfer control to a user command line interpreter that gave access to any program available on the system with the privileges of the attacked program.

One of the restrictions on the content of shellcode is that it has to be position independent, which means that it cannot contain any absolute address referring to itself.

Compile time defenses aim to harden programs to resist attacks in new programs.

Run time defenses aim to detect and abort attacking existing programs.

The openBSD project produces a free, multiplatform 4.4BSD-based UNIX-like operating system.

Stackshield, Return Address Defender and Stackguard are GCC compiler extensions that insert additional function entry and exit code.

Off-by-one attacks can occur in a binary buffer copy when the programmer has included code to check the number of bytes being transferred, but due to a coding error, allows just one more byte to be copied than there is space available.

In 1996 Aleph One published “Smashing the Stack for Fun and Profit” in Phrack magazine, giving a step-by-step introduction to exploiting stack-based buffer overflow vulnerabilities.

A buffer overflow can occur as a result of a programming error when a process attempts to store data beyond the limits of a fixed-sized buffer and consequently overwrites adjacent memory locations.

Guard pages can be placed between stack frames or between different allocations on the heap to provide further protection against stack and heap overflow attacks, but at cost in execution time supporting the large number of page mappings necessary.

The attacker can specify the return address used to enter code as a location somewhere in the run of NOPs, which is called a NOP sled.

**SOFTWARE SECURITY**

“Failure to Preserve SQL Query Structure” is in the Insecure Interaction Between Components CWE/SANS software error category.

Defensive programming is a form of design intended to ensure the continuing function of a piece of software in spite of unforeseeable usage of the software.

Program input refers to any source of data that originates outside the program and whose value is not explicitly known by the programmer when the code was written.

Two key areas of concern for any input are the size of the input and the meaning and interpretation of the input.

A number of widely used standard C library routines compound the problem of buffer overflow by not providing any means of limiting the amount of data transferred to the space available in the buffer.

Program input data may be broadly classified as textual or binary.

In the SQL injection attack the user supplied input is used to construct a SQL request to  retrieve information from a database.

Cross site scripting attacks are most commonly seen in scripted Web applications.

A variant where the attacker includes malicious script content in data supplied to a site is the XSS reflection vulnerability.

10. The process of transforming input data that involves replacing alternate, equivalent encodings by one common value is called canonicalization.

11. The major advantage of fuzzing is its simplicity and its freedom from assumptions about the expected input to any program, service, or function.

12. A race condition occurs when multiple processes and threads compete to gain uncontrolled access to some resource.

13. UNIX related systems provide the chroot system function to limit a program’s view of the file system to just one carefully configured section that is known as a chroot jail.

14. If privileges are greater than those already available to the attacker the result is a privilege escalation.

15. The principle of least privilege strongly suggests that programs should execute with the least amount of privileges needed to complete their function.

**INTERNET SECURITY PROTOCOLS AND STANDARDS**

S/MIME is a security enhancement to the MIME Internet e-mail format standard, based on technology from RSA Data Security.

S/MIME content-types support four new functions: enveloped data, signed data, clear-signed data, and signed and enveloped data.

A digital signature is formed by taking the message digest of the content to be signed and then encrypting that with the private key of the signer.

A signed data message can only be viewed by a recipient with S/MIME capability.

The default algorithms used for signing S/MIME messages are SHA-1 and the DSS.

The default algorithms used for encrypting S/MIME messages are the triple DES and a public-key scheme known as ElGamal.

If encryption is used alone, radix-64 is used to convert the ciphertext to ASCII format.

Domain Keys Identified Mail is a specification for cryptographically signing e-mail messages, permitting a signing domain to claim responsibility for a message in the mail stream.

The message user agent is housed in the user’s computer and is referred to as a client e-mail program or a local network e-mail server.

The domain name system is a directory lookup service that provides a mapping between the name of a host on the Internet and its numerical address.

The SSL record protocol provides two services for SSL connection: message integrity and confidentiality.

The alert protocol is used to convey SSL-related alerts to the peer entity.

A security association is uniquely identified by three parameters: security parameter index, protocol identifier, and IP destination address.

IP-level security encompasses three functional areas: authentication, confidentiality, and key management.

IPsec provides two main functions: a combined authentication/encryption function called Encapsulating security payload and a key exchange function.

**INTERNET AUTHENTICATION APPLICATIONS**

Biometric systems are automated methods of verifying or recognizing identity on the basis of some physiological or behavioral characteristic.

A software utility initially developed at MIT and available both in the public domain and in commercially supported versions, Kerberos is the defacto standard for remote authentication.

An alternative to each server being required to confirm identities of clients who request service is to use an authentication server that knows the passwords of all users and stores them in a centralized database.

A full-service Kerberos environment consisting of a Kerberos server that has the user ID and password of all participating users in its database and shares a secret key with each server, all users and servers being registered with the Kerberos server, is referred to as a Kerberos realm.

The issuer unique identifier is an optional bit string field used to identify uniquely the issuing CA in the event the X.500 name has been reused for different entities.

Public key infrastructure is the set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography.

The certification authority is the issuer of certificates and certificate revocation lists.

Key pair recovery allows end entities to restore their encryption/decryption key pair from an authorized  key backup facility.

The focus of identity management is defining an identity for each user, associating attributes with the identity,  and enforcing a means by which a user can verify identity.

In a generic identity management architecture a principal is an identity holder.

In a generic identity management architecture data consumers are entities that obtain and employ data  maintained and provided by identity and attribute providers, often to support authorization  decisions and to collect audit information.

Security Assertion Markup Language is an XML-based language for the exchange of security information between online  business partners.

WS security is a set of SOAP extensions for implementing message integrity and confidentiality in Web  services.

In Kerberos, the ticket granting server decrypts the ticket and authenticator, verifies the request, and creates  ticket for requested server.

The ticket contains the user’s ID, the server’s ID, a timestamp, a lifetime after which the ticket is  invalid, and a copy of the same session key sent in the outer message to the client.

**WIRELESS NETWORK SECURITY**

The security requirements are: confidentiality, integrity, availability, authenticity, and accountability.

The wireless environment consists of three components that provide point of attack: the wireless client, the transmission medium, and the wireless access point.

A man-in-the-middle attack involves persuading a user and an access point to believe that they are talking to each other when in fact the communication is going through an intermediate attacking device.

A denial of service attack occurs when an attacker continually bombards a wireless access point or some other accessible wireless port with various protocol messages designed to consume system resources.

A network injection attack targets wireless access points that are exposed to non-filtered network traffic, such as routing protocol messages or network management messages.

The principal threats to wireless transmission are disruption, eavesdropping and altering or inserting messages.

Like TKIP, CCMP provides two services: message integrity and data confidentiality.

Two types of countermeasures are appropriate to deal with eavesdropping: signal-hiding techniques and encryption.

The lowest layer of the IEEE 802 reference model is the physical layer.

The fields preceding the MSDU field are referred to as the MAC header.

The field following the MSDU field is referred to as the MAC trailer.

The two services involved with the distribution of messages within a DS are distribution and integration.

The 802.11i RSN security specification defines the following services: authentication, privacy with message integrity, and access control.

There are two types of keys: pairwise keys used for communication between a STA and an AP and group keys used for multicast communication.

At the top level of the group key hierarchy is the group master key.