Threats are attacks carried out. **False**

Security mechanisms typically do not involve more that one particular algorithm or protocol. **False**

Contingency planning is a functional area that primarily requires computer security technical measures. **False**

The first step in devising security services and mechanisms is to develop a security policy. **True**

Triple DES takes a plaintext block of 64 bits and a key of 56 bits to produce a ciphertext block of 64 bits. **False**

Like the MAC, a hash function also takes a secret key as input. **False**

Public-key algorithms are based on simple operations on bit patterns. **False**

AES uses a Feistel structure. **False**

One desirable property of a stream cipher is that the ciphertext be of the same length as the plaintext. **True**

Key distribution can be achieved for 2 parties A and B by third party selecting the key and physically delivering it to A and B. **True**

**System integrity** assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

A flaw or weakness in a system’s design, implementation, or operation and management that could be exploited to violate the system’s security policy is a **vulnerability.**

A **passive attack** is an attempt to learn or make sue of information from the system that doesn’t affect system resources.

**Ciphertext** is the scrambled message produced as output.

On average, **¾** of all possible keys must be tried in order to achieve success with a brute-force attack.

**Message authentication** is a procedure that allows communicating parties to verify that received or stored messages are authentic.

Digital signatures and key management are the 2 most important application of **public-key** encryption.

The exact substitutions and transformations performed by the algorithm depend on the **secret key**.

The most widely used encryption scheme is based on the **DES** adopted in 1977 by the National Bureau of Standards.

**CTR** mode is typically used for general-purpose block-oriented transmission and is useful for high-speed requirements.

SHA-1 is considered to be very secure. **False**

HMAC can be proven secure provided that the embedded has function has come reasonable cryptographic strengths. **True**

The Diffie-Hellman algorithm depends for its effectiveness on the difficulty of computer discrete logarithms. **True**

A token is the best means of authentication because it cannot be forged or stolen by an adversary. **False**

Depending on the supplication, user authentication on a biometric system involves either verification or identification. **True**

Memory cared store and process data. **False**

The authentication function determines who is trusted for a given purpose. **False**

External devices who is trusted for a given purpose. **False**

The default set of rights should always follow the rule of least privilege or read-only access. **True**

Traditional RBAC systems define the access rights of individual users and groups of users. **False**

A **brute-force** attack involves trying all possible private keys.

Although the **timing** attack is a serious threat, there are simple countermeasures that can be used such as constant time calcs, random delays or binding computations.

**RSA** was the first published public-key algorithm.

Presenting or generating authentication information that corroborates the binding between the entity and the identifier is the **identification step.**

The **user education** strategy is when users are told the importance of using hard to guess passwords and provided with guidelines for selecting strong passwords.

To counter threats to remote authentication, systems generally rely on some form of **challenge-response** protocol.

**Access control** implements a security policy that specifies who or what may have access to each specific system resource and the type of access that is permitted in each instance.

**DAC** is the traditional method of implementing access control.

**RBAC** is based on the roles the users assume in a system rather than the user’s identity.

An approval to perform an operation on 1 or more RBAC protected objects is **permission.**

An essential component of many buffer overflow attacks is the transfer of execution to code, known as **shellcode,** supplied by the attacker and often saved in the buffer being overflowed.

The possibility of overwriting the saved frame pointer and return address forms the core of a stack overflow. **True**

A **stack frame** is a structure where data are usually saved on the stack.

Shellcode is not specific to a particular processor architecture. **False**

A stack buffer overflow attack is also referred to as **stack smashing**.

The x86 Assembly Language Instruction NOP means **no operation or do nothing instruction.**

**Environment variables** are a collection of string values inherited by each process from its parent that can affect the way a running process behaves.

A stead reduction in memory available on the heap to the point where it is completely exhausted is known as a **memory leak.**

The difference between defensive programming and normal practices is that everything is assumed. **False**

To counter XSS attacks a defensive programmer needs to explicitly identify any assumptions as to the form of input and to verify that any input data conform to those assumptions before any use of the data. **False**

Programmers often make assumptions about the type of inputs a program will receive. **True**

There is a problem anticipating and testing for all potential types of non-standard inputs that might be exploited by an attacker to subvert a program. **True**

Incorrect handling of program **input** is one of the most common failings in software security.

Bots starting from a given HTTP link and then following all links on the provided website in a recursive way is called **spidering.**

**Application-based** bandwidth attacks attempt to take advantage of the disproportionally large resource consumption at a server.

The attacker needs access to a high volume network connection for a SYN spoof attack. **False**

A denial-of-service attack is an attempt to compromise availability by hindering or blocking completely the provision of some service. **True**

In a **DNS amplification** attack, the attacker creates a series of DNS requests containing the spoofed source address for the target system.

The SYN spoofing attack targets the table of TCP connections on the server. **True**

A SIP flood attack exploits the fact that a single INVITE request triggers considerable resource consumption. **True**

The IDS component responsible for collecting data is the user interface. **False**

**RFC 4767** is a document that describes the application level protocol for exchanging data between intrusion detection entities.

Snort can perform intrusion prevention but not intrusion detection. **False**

Anomaly detection is effective against misfeasors. **False**

**Insider attacks** are among the most difficult to detect and prevent.

A **Markov proces**s model is used to establish transition probabilities among various states.

A packet filtering firewall is typically configured to filter packets in both directions. **True**

The **tiny fragment** attack is designed to circumvent filtering rules that depend on TCP header information.

The primary role of the personal firewall is to deny unauthorized remote access to the computer. **True**

A **circuit-level** gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host.

One disadvantage of a packet filtering firewall is its simplicity. **False**

The firewall may be a single computer system or a set of two or more systems that cooperate to perform the firewall function. **True**

Typically the systems in the **DMZ** require or foster external connectivity such as a corporate Web site, an email server or a DNS server.

DKIM is designed to provide an email authentication technique that is transparent to the end user. **True**

Most browsers come equipped with SSL and most web servers have implemented the protocol. **True**

IPsec can assure that **a router advertisement comes authorized, update isn’t forged and a redirect message comes from the original router.**

As and alternative the RSA public-key encryption algorithm can be used with either the SHA-1 or the MD5 message digest algorithm for forming signatures. **True**

The **protocol identifier** field in the outer IP header indicates whether the association is an AH or ESP security association.

DKIM has been widely adopted by a range of email providers and many Internet service providers. **True**

A benefit of IPsec is **below the transport layer, no need to revoke keying material, and can provide security for individual users.**

**Computer Security** is the protection afforded to an automated information system in order to attain  
the applicable objectives of preserving the integrity, availability, and confidentiality of  
information system resources.  
2. Confidentiality, Integrity, and Availability form what is often referred to as the **CIA triad**.  
3. A loss of **availability** is the disruption of access to or use of information or an information  
system.  
4. In the United States, student grade information is an asset whose confidentiality is regulated  
by the **FERPA**.  
5. A(n) **attack** is a threat that is carried out and, if successful, leads to an undesirable  
violation of security, or threat consequence.  
6. A(n) **countermeasure** is any means taken to deal with a security attack.  
7. Misappropriation and misuse are attacks that result in **usurpation** threat consequences.  
8. The assets of a computer system can be categorized as hardware, software, communication  
lines and networks, and **data**.  
9. Release of message contents and traffic analysis are two types of **passive** attacks.  
10. Replay, masquerade, modification of messages, and denial of service are example of  
**active** attacks.  
11. Establishing, maintaining, and implementing plans for emergency response, backup  
operations, and post disaster recovery for organizational information systems to ensure the  
availability of critical information resources and continuity of operations in emergency situations  
is a **contingency** plan.  
12. A(n) **risk** assessment is periodically assessing the risk to organizational operations,  
organizational assets, and individuals, resulting from the operation of organizational information  
systems and the associated processing, storage, or transmission or organizational information.  
13. The OSI security architecture focuses on security attacks, **mechanisms** and services.  
14. A **digital** **signature** is data appended to, or a cryptographic transformation of, a data unit that  
allows a recipient of the data unit to prove the source and integrity of the data unit and protect  
against forgery.  
15. Security implementation involves four complementary courses of action: prevention,  
detection, response, and **recovery**.

Also referred to as single-key encryption, the universal technique for providing confidentiality  
for transmitted or stored data is **symmetric** **encryption**.  
2. There are two general approaches to attacking a symmetric encryption scheme:  
cryptanalytic attacks and **brute**-**force** attacks.  
3. The **decryption** algorithm takes the ciphertext and the secret key and produces  
the original plaintext.  
4. A **cryptanalytic** attack exploits the characteristics of the algorithm to attempt to deduce a specific  
plaintext or to deduce the key being used.  
5. A **block cipher** processes the plaintext input in fixed-size blocks and produces a block of  
ciphertext of equal size for each plaintext block.  
6. A **stream cipher** processes the input elements continuously, producing output one element at a time.  
7. Public-key encryption was first publicly proposed by **Diffie and Hellman** in 1976.  
8. The two criteria used to validate that a sequence of numbers is random are independence and  
**uniform distribution.**  
9. A **back-end appliance** is a hardware device that sits between servers and storage systems and encrypts all data going from the server to the storage system and decrypts data going in the opposite direction.  
10. In July 1998 the **Electronic Frontier Foundation (EFF)** announced that it had broken a DES encryption using a special  
purpose “DES cracker” machine.  
11. The simplest approach to multiple block encryption is known as **electronic codebook** mode, in which  
plaintext is handled *b* bits at a time and each block of plaintext is encrypted using the same key.  
12. A **pseudorandom** stream is one that is unpredictable without knowledge of the input key and which  
has an apparently random character.  
13. The **public and private key** is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption.  
14. **Library-based tape encryption** is provided by means of a co-processor board embedded in the tape drive and tape  
library hardware.  
15. The purpose of the **Diffie-Hellman Key Agreement** algorithm is to enable two users to securely reach agreement about a shared secret that can be used as a secret key for subsequent symmetric encryption of  
messages.

An authentication process consists of the **identification** step and the verification step.

2. Voice pattern, handwriting characteristics, and typing rhythm are examples of **dynamic** biometrics.

3. A **shadow password file** is a separate file from the user IDs where hashed passwords are kept.

4. With the **proactive password** **checking** strategy a user is allowed to select their own password, but the system checks to see if the password is allowable.

5. The technique for developing an effective and efficient proactive password checker based on rejecting words on a list is based on the use of a **bloom** filter.

6. Objects that a user possesses for the purpose of user authentication are called **tokens**.

7. Authentication protocols used with smart tokens can be classified into three categories: static, dynamic password generator, and **challenge-response.**

8. A **biometric** authentication system attempts to authenticate an individual based on his or her unique physical characteristics.

9. The **retinal pattern** is the pattern formed by veins beneath the retinal surface.

10. A host generated random number is often called a **nonce**.

11. **Eavesdropping**, in the context of passwords, refers to an adversary’s attempt to learn the password by observing the user, finding a written copy of the password, or some similar attack that involves the physical proximity of user and adversary.

12. In a **Trojan Horse** attack, an application or physical device masquerades as an authentic application or device for the purpose of capturing a user password, passcode, or biometric.

13. A **denial-of-service** attack attempts to disable a user authentication service by flooding the service with numerous authentication attempts.

14. A **cardholder** is an individual to whom a debit card is issued.

15. The **verification** step is presenting or generating authentication information that corroborates the binding between the entity and the identifier.

X.800 defines **access control** as the prevention of unauthorized use of a resource,  
including the prevention of use of a resource in an unauthorized manner.  
2. An independent review and examination of system records and activities in order to test for  
adequacy of system controls, to ensure compliance with established policy and operational  
procedures, to detect breaches in security, and to recommend any indicated changes in control,  
policy and procedures is a(n) **audit**.  
3. **Role based** access control controls access based on the roles that users have within the system  
and on rules stating what accesses are allowed to users in given roles.  
4. **Discretionary** access control controls access based on the identity of the requestor and on access  
rules stating what requestors are or are not allowed to do.  
5. The basic elements of access control are: subject, **object** and access right.  
6. Basic access control systems typically define three classes of subject: owner, **group** and  
world.  
7. A discretionary access control scheme is one in which an entity may be granted access rights  
that permit the entity, by its own volition, to enable another entity to access some resource.  
8. The **super user** ID is exempt from the usual file access control constraints and has system  
wide access.  
9. A **session** is a mapping between a user and an activated subset of the set of roles to which  
the user is assigned.  
10. Role hierarchies make use of the concept of **inheritance** to enable one role to implicitly  
include access rights associated with a subordinate role.  
11. A **prerequisite** dictates that a user can only be assigned to a particular role if it is already  
assigned to some other specified role and can be used to structure the implementation of the least  
privilege concept.  
12. **Object** functions provide the capability to create, delete, and maintain RBAC elements  
and relations.  
13. The NIST model defines two types of role hierarchies: general role hierarchies and  
**limited** hierarchies.  
14. **Static** Separation of Duty enables the definition of a set of mutually exclusive roles, such  
that if a user is assigned to one role in the set, the user may not be assigned to any other role in the  
set.  
15. The **administrative** functions include the following: create a user session with a default set of  
active roles; add an active role to a session; delete a role from a session; and check if the session  
subject has permission to perform a request operation on an object.

A **DBMS** is a suite of programs for constructing and maintaining the database and for  
offering ad hoc query facilities to multiple users and applications.  
2. In a relational database columns are referred to as **attributes**.  
3. A **view** is the result of a query that returns selected rows and columns from one or more  
tables.  
4. **SQL** is a standardized language that can be used to define schema, manipulate, and  
query data in a relational database.  
5. With **ownership-based** administration the owner (creator) of a table may grant and revoke access  
rights to the table.  
6. In a **centralized** administration a small number of privileged users may grant and revoke  
access rights.  
7. In addition to granting and revoking access rights to a table, in a **decentralized** administration  
the owner of the table may grant and revoke authorization rights to other users, allowing them to  
grant and revoke access rights to the table.  
8. In a discretionary access control environment database users are classified into three broad  
categories: administrator, end user other than application owner, and application **owner**.  
9. The information transfer path by which unauthorized data is obtained is referred to as an  
10. A **statistical** database is one that provides data of a statistical nature such as counts and  
averages.  
11. When using the **data swapping** method attribute values are exchanged (swapped) between records  
in sufficient quantity so that nothing can be deduced from the disclosure of individual records.  
12. The **user** is a human entity that presents requests (queries) to the system.  
13. **Cloud Computing** is a model for enabling ubiquitous, convenient, on-demand network access to a  
shared pool of configurable computing resources that can be rapidly provisioned and released with  
minimal management effort or service provider interaction.  
14. A \_\_\_\_\_\_\_\_\_\_ cloud infrastructure is made available to the general public or a large industry  
group and is owned by an organization selling cloud services.  
15. The \_\_\_\_\_\_\_\_\_ model provides a predefined environment for the cloud subscriber that is shared  
with other tenants, typically through tagging data with a subscriber identifier.

A **rootkit** is a set of programs installed on a system to maintain covert access to that system with administrator (root) privileges while hiding evidence of its presence.

2. A **blended attack** uses multiple methods of infection or propagation to maximize the speed of contagion and the severity of the attack.

3. A computer **virus** is a piece of software that can “infect” other programs or any type of executable content and tries to replicate itself.

4. Sometimes referred to as the “infection vector”, the **infection mechanism** is the means by which a virus spreads or propagates.

5. Sometimes known as a “logic bomb”, the **trigger** is the event or condition that determines when the payload is activated or delivered.

6. The four phases of a typical virus are: dormant phase, triggering phase, execution phase and **propagation** phase.

7. During the **triggering** phase the virus is activated to perform the function for which it was intended.

8. A **stealth** virus is explicitly designed to hide itself from detection by anti-virus software.

9. **Mobile** code refers to programs that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.

10. A **drive-by-download** is when a user views a Web page controlled by the attacker that contains a code that exploits the browser bug and downloads and installs malware on the system without the user’s knowledge or consent.

11. A **botnet** is a collection of bots capable of acting in a coordinated manner.

12. A bot can use a **keylogger** to capture keystrokes on the infected machine to retrieve sensitive information.

13. Countermeasures for malware are generally known as **anti-virus** mechanisms because they were first developed to specifically target virus infections.

14. Developed by IBM and refined by Symantec, the **digital immune system** provides a malware detection system that will automatically capture, analyze, add detection and shielding, or remove new malware and pass information about it to client systems so the malware can be detected before it is allowed to run elsewhere.

15. **Generic decryption** technology is an anti-virus approach that enables the anti-virus program to easily detect even the most complex polymorphic viruses and other malware, while maintaining fast scanning speeds.

A symmetric encryption scheme has five ingredients: plaintext, encryption algorithm, ciphertext, decryption algorithm and **secret key.**

2. **Cryptanalysis** is the process of attempting to discover the plaintext or key.

3. A **block** cipher processes the input one block of elements at a time, producing an output block for each input block.

4. A **stream** cipher processes the input elements continuously, producing output one element at a time as it goes along.

5. An encryption scheme is **computationally secure** if the cost of breaking the cipher exceeds the value of the encrypted information and/or the time required to break the cipher exceeds the useful lifetime of the information.

6. The **AES** was issued as a federal information-processing standard and is intended to replace DES and 3DES with an algorithm that is more secure and efficient.

7. **RC4** was designed in 1987 by Ron Rivest and is a variable key-size stream cipher with byte-oriented operations.

8. “The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext” is a description of the **CBC** mode of operation.

9. Unlike ECB and CBC modes, **CTR** mode requires only the implementation of the encryption algorithm and not the decryption algorithm.

10. The most powerful, and most common, approach to countering the threats to network security is **encryption**.

11. With **end-to-end** encryption the encryption process is carried out at the two end systems.

12. With **link** encryption each vulnerable communications link is equipped on both ends with an encryption device.

13. For symmetric encryption to work the two parties to an exchange must share the same **key**, which must be protected from access by others.

14. All encryption algorithms are based on two general principles: substitution and **transposition**.

15. The three most important symmetric block ciphers are: 3DES, AES, and **DES**.

The Secure Hash Algorithm (SHA) was developed by the **NIST** and published as a federal information processing standard (FIPS 180) in 1993.

2. Versions of SHA, with hash value lengths of 256, 384, and 512 bits, (SHA-256, SHA-384, and SHA 512) are collectively known as **SHA-2**

3. The evaluation criteria for the new hash function are: security, **cost** and algorithm and implementation characteristics.

4. **HMAC** has been issued as RFC 2014, has been chosen as the mandatory-toimplement MAC for IP Security, and is used in other Internet protocols, such as Transport Layer Security.

5. One of the first public-key schemes, **RSA** was developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman.

6. **Timing attacks** are alarming for two reasons: they come from a completely unexpected direction and they are a ciphertext-only attack.

7. Four possible approaches to attacking the RSA algorithm are: brute force, timing attacks, **mathematical** attacks, and chosen ciphertext attacks.

8. NIST has published FIPS PUB 186, which is known as the **DSS**.

9. The purpose of the **secret key** algorithm is to enable two users to exchange a secret key securely that can then be used for subsequent encryption of messages.

10. One of the simplest hash functions is the **XOR** of every block.

11. “Must support hash value lengths of 224, 256,384, and 512 bits” and “algorithm must process small blocks at a time instead of requiring the entire message to be buffered in memory before processing it” are requirements for **SHA-3.**  
12. If speed is a concern, it is fully acceptable to use **MD5** rather than SHA as the embedded hash function for HMAC.

14. The security of any MAC function based on an embedded hash function depends in some way on the **cryptographic** strength of the underlying hash function.

15. Perhaps the most widely used public-key algorithms are **RSA** and DiffieHellman.

**SHA-1** is not very secure

A **token** can be forged or stolen by an adversary

The **authentication** process does not determine who is trusted for a given purpose

**Diffie Hellman** was the first published public key algorithm

Presenting or generating authentication info that corroborates the binding between the entity and the identifier is the **verification** step.

Challenge threats to remote user authentication, systems rely on some form of **challenge-response** protocol.

**DAC** is the traditional method of implementing access control

**RBAC** is based on the roles the users assume in a system rather than the user identity

An approval to perform an operation on one or more RBAC protected objects is **permission**

**ECB** is every 64 bits independently with the same key

**CBC** is an XOR with the next 64 bits of plaintext and the previous 64 bits of ciphertext

**CTR** – every block of plaintext is XOR with an encrypted counter. The counter is incremented for each subsequent block

Programmers use **backdoors** to debug and test their programs

Replay, masquerade, modification of messages, and denial of service are example of **active** attacks.  
  
An example of  **masquerade** is an attempt by an unauthorized user to gain access to a system by posing  
as an authorized user.

**Privacy** assures that individuals control or influence what information related to them may be  
collected and stored and by whom and to whom that information may be disclosed.

In the United States, student grade information is an asset whose confidentiality is regulated by the **FERPA**.

A(n) **passive attack** is an attempt to learn or make use of information from the system that does not  
affect system resources.

Release of message contents and traffic analysis are two types of **passive** attacks.

Contingency planning is a functional area that primarily requires computer security technical measures. **False**

Combined one byte at a time with the plaintext stream using the XOR operation, a **keystream** is the output of the pseudorandom bit generator.

Symmetric encryption is used primarily to provide confidentiality. **True**

Digital signatures and key management are the two most important applications of **public-key** encryption.

The **decryption algorithm** is the encryption algorithm run in reverse.

Triple DES takes a plaintext block of 64 bits and a key of 56 bits to produce a ciphertext block of 64  
bits. **False**

The strength of a hash function against brute-force attacks depends solely on the length of the hash  
code produced by the algorithm. **True**

A message authentication code is a small block of data generated by a secret key and appended to a  
message. **True**  
  
 A good technique for choosing a password is to use the first letter of each word of a phrase. **True**

Each individual who is to be included in the database of authorized users must first be **enrolled** in the system.   
  
User authentication is a procedure that allows communicating parties to verify that the contents of a  
received message have not been altered and that the source is authentic. **False**

User authentication is the basis for most types of access control and for user accountability. **True**

**Hand geometry** systems identify features of the hand, including shape, and lengths and widths of fingers.

Enrollment creates an association between a user and the users biometric characteristics. **True**

A constraint is a defined relationship among roles or a condition related to roles. **True**

A concept that evolved out of requirements for military information security is **mandatory access control**.

External devices such as firewalls cannot provide access control services. **False**

An auditing function monitors and keeps a record of user accesses to system resources. **True**

The main innovation of the NIST standard is the introduction of the RBAC System and Administrative  
Functional Specification, which defines the features required for an RBAC system. **True**

**Constraints** provide a means of adapting RBAC to the specifics of administrative and security policies  
in an organization.

**Data perturbation** is when the data in the SDB can be modified so as to produce statistics that cannot be  
used to infer values for individual records.

A census database is an example of a pure statistical database. **True**

In a relational database rows are referred to as **tuples**.

SQL Server allows users to create roles that can then be assigned access rights to portions of the database. **True**

To create a relationship between two tables, the attributes that define the primary key in one table must appear as attributes in another table, where they are referred to as a foreign key. **True**

Random-sample query is a simple output perturbation technique. **True**

A bot propagates itself and activates itself, whereas a worm is initially controlled from some central  
facility. **False**

In addition to propagating, a worm usually carries some form of payload. **True**

Packet sniffers are mostly used to retrieve sensitive information like usernames and passwords. **True**

A macro virus infects executable portions of code. **False**

The term computer virus is attributed to **Fred Cohen** .

A program that is covertly inserted into a system with the intent of compromising the integrity or  
confidentiality of the victims data is **malware**.

A brute-force approach involves trying every possible key until an intelligible translation of the ciphertext into plaintext in obtained. **True**

A **permanent key** is a key used between entities for the purpose of distributing session keys.

AES uses a Feistel structure. **False**

The most widely used encryption scheme is based on **DES** the adopted in 1977 by the National  
Bureau of Standards.

Plaintext is the scrambled message produced as output. **False**

Symmetric encryption is also referred to as secret-key or single-key encryption. **True**

The operations performed during a round consist of circular shifts, and primitive Boolean functions  
based on DSS, MD5, SHA, and RSA. **False**

A **chosen ciphertext** type of attack exploits properties of the RSA algorithm.

SHA-3 algorithms must be designed to resist any potentially successful attack on SHA-2 functions. **True**

Unlike RSA, DSS cannot be used for encryption or key exchange. **True**

The  **RSA** scheme has reigned supreme as the most widely accepted and implemented approach  
to public-key encryption.

The appeal of HMAC is that its designers have been able to prove an exact relationship between the  
strength of the embedded hash function and the strength of HMAC. **True**

**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.

A **poison packet** triggers a bug in the system’s network handling software causing it to crash and the  
system can no longer communicate over the network until this software is reloaded.

In a **DNS amplification** attack the attacker creates a series of DNS requests containing the spoofed source  
address for the target system.

Given sufficiently privileged access to the network handling code on a computer system, it is difficult  
to create packets with a forged source address. **False**

When a DoS attack is detected, the first step is to **identify the attack**.

In both direct flooding attacks and **SYN spoofing attacks** the use of spoofed source addresses results in response packets being scattered across the Internet and thus detectable.

A characteristic of reflection attacks is the lack of **backscatter** traffic.

A **network-based IDS** monitors network traffic for particular network segments or devices and analyzes network, transport, and application protocols to identify suspicious activity.

Intrusion detection is based on the assumption that the behavior of the intruder differs from that of a  
legitimate user in ways that can be quantified. **True**

The objective of the intruder is to gain access to a system or to increase the range of privileges accessible  
on a system. **True**

The IDS component responsible for collecting data is the user interface. **False**

**Insider attacks** are among the most difficult to detect and prevent.

The **analyzer** is responsible for determining if an intrusion has occurred.

A **VPN** consists of a set of computers that interconnect by means of a relatively unsecure  
network and makes use of encryption and special protocols to provide security.  
   
**Direction** control determines the direction in which particular service requests may be initiated and  
allowed to flow through the firewall.  
   
**Service** control determines the types of Internet services that can be accessed, inbound or outbound.  
   
The firewall may be a single computer system or a set of two or more systems that cooperate to perform  
the firewall function. **True**  
   
**Stateful matching** scans for attack signatures in the context of a traffic stream rather than individual packets.  
   
A prime disadvantage of an application-level gateway is the additional processing overhead on each  
connection. **True**

**Run-time** defenses involve changes to the memory management of the virtual address space of  
processes that act to either alter the properties of regions of memory or to make predicting the location  
of target buffers sufficiently difficult to thwart many types of attacks.  
   
Buffer overflows can be found in a wide variety of programs. **True**  
   
21 An essential component of many buffer overflow attacks is the transfer of execution to code, known as  
**shellcode**, supplied by the attacker and often saved in the buffer being overflowed.  
   
A **stack frame** is a structure where data are usually saved on the stack.  
   
In 2004 the  **Sasser Worm** exploited a buffer overflow in Microsoft Windows 2000/XP Local Security  
Authority Subsystem Service.  
   
The x86 Assembly Language Instruction NOP means **no operation or do nothing instruction** .  
   
Programmers often make assumptions about the type of inputs a program will receive. **True**  
   
Many computer security vulnerabilities result from poor programming practices. **True**  
   
The correct implementation in the case of an atomic operation is to test separately for the presence of  
the lockfile and to not always attempt to create it. **False**  
   
**Environment variables** are a collection of string values inherited by each process from its parent that can affect the way a running process behaves.  
   
A **command injection** attack occurs when the input is used in the construction of a command that is subsequently executed by the system with the privileges of the Web server.  
   
Software security is closely related to software quality and reliability. **True**  
  
The **mail submission agent** accepts the message submitted by a message user agent and enforces the policies of the hosting domain and the requirements of Internet standards.  
  
IPsec can assure that **a router advertisement comes from an authorized router, a routing update is not forged, a redirect message comes from the router to which the initial packet was sent**  
   
33 An ADMD is an Internet e-mail provider. **True**  
   
The **MDA** is responsible for transferring the message from the MHS to the MS.  
   
35 At its most fundamental level the Internet mail architecture consists of a user world in the form of **MUA**  
   
36 ESP supports two modes of use: transport and **tunnel**.  
  
The ticket-granting ticket is not reusable. **False**  
The ticket-granting ticket is encrypted with a secret key known only to the AS and the TGS. **True**  
   
**Kerberos** requires that a user prove his or her identity for each service invoked and, optionally,  
requires servers to prove their identity to clients.  
  
CMP, defined in RFC 2510, is designed to be a flexible protocol able to accommodate a variety of  
technical, operational, and business models. **True**  
   
Federated identity management makes use of a number of standards that provide the building blocks  
for secure identity information exchange across different domains or heterogeneous systems. **True**  
   
A principal element of an identity management system is  **workflow automation, delegated administration, and authentication**.  
   
Initialization begins the process of enrolling in a PKI. **False**  
Company wireless LANs or wireless access points to wired LANs in close proximity may create overlapping transmission ranges. **True**  
A wireless access point is a **cell tower, Wi-Fi hot spot, wireless access point to a LAN or WAN**   
A **pre-shared key** is a secret key shared by the AP and a STA and installed in some fashion outside the  
scope of IEEE 802.11i.  
The smallest building block of a wireless LAN is a **BSS**.  
The MPDU exchange for distributing pairwise keys is known as the **4-way handshake**.  
The MAC service data unit contains any protocol control information needed for the functioning of the  
MAC protocol. **False**  
Any device that contains an IEEE 802.11 conformant MAC and physical layer is a basic service set. **False**