(I) What is IDS?

Model Answer :

IDS (Intrusion Detection System) monitors the traffic on a computer network to detect any suspicious activity

(II) What are the services provided by IPSec?

Model Answer :

1. Access control
2. Connectionless integrity
3. Data origin authentication
4. Rejection of replayed packets.

(III) Distinguish between MAC and Hash function.

Model Answer :

MAC:
In Message Authentication Code, the secret key shared by sender and receiver. The MAC is appended to the message at the source at a time which the message is assumed or known to be correct.
Hash Function:
The hash value is appended to the message at the source at time when the message is assumed or known to be correct. The hash function itself not considered to be secret.

(IV) Define integrity and non repudiation.

Model Answer :

Integrity: Service that ensures that only authorized person able to modify the message.
Non repudiation: This service helps to prove that the person who denies the transaction is true or false.

(VII) What is the difference between message authentication and one-way hash function.

Model Answer :

A hash function, by itself, does not provide message authentication. A secret key must be used in some fashion with the hash function to produce authentication. A MAC, by definition, uses a secret key to calculate a code used for authentication.

(VIII) Define Virus.

Model Answer :

Computer Viruses is defined as the malicious software programs that damage computer program entering into the computer without the permission of the users, and also run against the wishes of the users. They are replicated by themselves. Viruses are so dangerous and malicious that they can be automatically copied and pasted from memory to memory over and over.
Types of virus:
Boot sector Virus Macro virus Multipartite Virus Stealth virus.

(IX) Define Authentication.

Model Answer :

Authentication is the process of determining whether someone or something is, in fact, who or what it declares itself to be. Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server.

(X) Mention any three hash algorithms.

Model Answer :

MD5 (Message Digest version 5) algorithm.
:SHA_1 (Secure Hash Algorithm).
RIPEMD_160 algorithm.

(XI) What is Stream Cipher in Cryptography?

Model Answer :

A Stream Cipher is used for symmetric key cryptography, or when the same key is used to encrypt and decrypt data. Stream Ciphers encrypt pseudorandom sequences with bits of plaintext in order to generate ciphertext, usually with XOR.

(XII) Define five modes of operations of Block Cipher.

Model Answer :

i. Electronic Codebook(ECB)
ii. Cipher Block Chaining(CBC)
iii. Cipher Feedback(CFB) iv. Output Feedback(OFB) v. Counter(CTR).

2. .List all the information mentioned in a Digital ID.Also,mention the minimal requirement of Digital ID. [5]

Model Answer :

The information contained in a Digital ID depends on the type of Digital ID and its use. At a minimum, each Digital ID contains
Owner's public key
Owner's name or alias
Expiration date of the Digital ID
Serial number of the Digital ID
Name of the certification authority that issued the Digital ID
Digital signature of the certification authority that issued the Digital ID.

3. Explain the working of caesar Cipher. [5]

Model Answer :

The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique. Itâ€™s simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.

Thus to cipher a given text we need an integer value, known as a shift which indicates the number of positions each letter of the text has been moved down.
The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,â€¦, Z = 25. Encryption of a letter by a shift n can be described mathematically as.

$E_n(x)=(x+n) \mod 26$
(Encryption Phase with shift n)

$D_n(x)=(x-n) \mod 26$
(Decryption Phase with shift n)

4. What are the steps in virus removal process? [5]

Model Answer :

Virus should be removed form the system by scanning process. The steps include in this process are,
1. Backup your data
2. Check to ensure that other factors aren't causing your problem
3. Gather your antivirus tools
4. Reboot in Safe Mode
5. Run your scans.
6. Test your computer

5. What is the difference between HTTP and HTTPS [5]

Model Answer :

Key Difference between HTTP and HTTPS
HTTP lacks a security mechanism to encrypt the data, whereas HTTPS provides SSL or TLS Digital Certificate to secure the communication between server and client.
HTTP operates at the Application Layer, whereas HTTPS operates at Transport Layer.
HTTP by default operates on port 80, whereas HTTPS by default operates on port 443.
HTTP transfers data in plain text, while HTTPS transfers data in cipher text (encrypt text).
HTTP is fast as compared to HTTPS because HTTPS consumes computation power to encrypt the communication channel.

6. What is Distributed Denial of service attack? [5]

Model Answer :

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices.

From a high level, a DDoS attack is like an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination.

7 (a) List the basic comparison between Symmetric & Asymmetric Encryption. [5]

Model Answer :

Basis of Comparison Symmetric Encryption Asymmetric Encryption:
Encryption key Same key for encryption & decryption Different keys for encryption & decryption
Performance Encryption is fast but more vulnerable Encryption is slow due to high computation
Algorithms DES, 3DES, AES and RC4 Diffie-Hellman, RSA
Purpose Used for bulk data transmission Often used for securely exchanging secret keys.

7 (b) State the difference between IDS & IPS. [5]

Model Answer :

IDS is Intrusion Detection System and it only detects intrusions and the administrator has to take care of preventing the intrusion. Whereas, in IPS i.e., Intrusion Prevention System, the system detects the intrusion and also takes actions to prevent the intrusion.

7 (c) How is Encryption different from Hashing? [5]

Model Answer :

Both Encryption and Hashing are used to convert readable data into an unreadable format. The difference is that the encrypted data can be converted back to original data by the process of decryption but the hashed data cannot be converted back to original data.

8 (a) What protocols fall under TCP/IP Layer of OSI Model? [5]

Model Answer :

TCP/IP TCP/IP Protocol Examples
Application NFS, NIS+, DNS, telnet, ftp, rlogin, rsh, rcp, RIP, RDISC, SNMP and others
Transport TCP, UDP
Internet IP, ARP, ICMP
Data Link PPP, IEEE 802.2
Physical Network Ethernet (IEEE 802.3) Token ring, RS-232, others.

8 (b) What is SSL & TLS? [5]

Model Answer :

SSL is meant to verify the senderâ€™s identity but it doesnâ€™t search for anything more than that. SSL can help you track the person you are talking to but that can also be tricked at times.

TLS is also an identification tool just like SSL, but it offers better security features. It provides additional protection to the data and hence SSL and TLS are often used together for better protection.

8 (c) What is Email spoofing? [5]

Model Answer :

Email spoofing is the creation of email messages with a forged sender address. The term applies to email purporting to be from an address which is not actually the sender's; mail sent in reply to that address may bounce or be delivered to an unrelated party whose identity has been faked.

9 (a) [8]

What are the different types of password attack?

Model Answer :

Phishing Attacks.
Credential Stuffing Attacks.
Brute Force Attacks.
Dictionary Attacks.
Password Spraying Attacks.
Keylogger Attacks.
Man-In-The-Middle Attacks.
Rainbow Table Attacks.

9 (b) What is the Digital Signature? [4]

Model Answer :

A digital signature is a mathematical technique used to validate the authenticity and integrity of a digital document, message or software. It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security.

9 (c) What is non repudiation? [3]

Model Answer :

Non-repudiation is the assurance that someone cannot deny the validity of something. Non-repudiation is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data. In other words, non-repudiation makes it very difficult to successfully deny who/where a message came from as well as the authenticity and integrity of that message.

10 (a) What is proxy chain? [7]

Model Answer :

Proxy Chaining is connecting two or more proxy servers to obtain the intended page. We can use as many proxies as we want. Letâ€™s see an example as shown below:

User â€"â€"â€"â€"> Proxy1 â€"â€"â€"â€"> Proxy2 â€"â€"â€"â€"> Proxy3 â€"â€"â€"â€"> Proxy4â€"â€"â€"â€"> Webpage

The user connects to proxy1 and from there to the next proxies as specified by the user until it finally reaches the destination.
When the destination end searches for the IP, the Proxy4 IP is displayed as the userâ€™s IP.
While using proxy chaining we have to make sure that the entire proxy server included in the chain is working properly.
If any proxy IP fails to work, this means the connection canâ€™t be established.
Then, we have to replace the damaged proxy with a new one or exclude the damaged IP and connect the rest forming a new chain.
Sometimes it can be a bit difficult to figure out which proxy has mis functioned if you are using too many proxies.

10 (b) How to secure wireless networks Protocols [8]

Model Answer :

Wired Equivalent Privacy (WEP)

Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access 2 (WPA 2)

Wi-Fi Protected Access 3 (WPA 3)

WEP stands for Wired Equivalent Privacy, and WPA stands for Wireless Protected Access. WPA2 is the second version of the WPA standard. Using some encryption is always better than using none, but WEP is the least secure of these standards, and you should not use it if you can avoid it.

11 (a) Why is Cyber Crime increasing at a huge extent day by day? [7]

Model Answer :

Cyber Crime is increasing day by day every year because of the following reasons:

Cyber Crime is easy to accomplish. A person having good knowledge of computer hacking can do Cybercrime.
There is a lower risk of getting caught in Cybercrime.
A cyber attackers can get huge money for their little work.
Cyber attackers can target thousands of victims.
With the introduction of cryptocurrencies, money laundering is getting easier.

11 (b) What are the main goals of Cyber Security? [8]

Model Answer :

The main objective of cyber security is to protect data from cyber-attacks. It follows a principle called CIA trio. It is a security sector that provides a triangle of three connected principles. The CIA model is used to help organizations to develop policies for their information security architecture. There are three main components Confidentiality, Integrity, and Availability of this CIA model. One or more of these principles is broken when it finds a security breach. This model provides a security paradigm to guide individuals through many aspects of IT security.