Assignment 1

1. List all symmetric key algorithms.

DES :-
Data Encryption Standard (DES) It is a block cipher published by NIST. It is an implementation of Feistal Cipher. It uses 16 round feestal structure. It has an effective key length of 56 bits

Triple DES:-
Triple DES is an encryption technique which uses 3 instances of DES on same plain text. It uses three different types of key choosing techniques in first all used keys are different and in second 2 keys are same and one is different. and in third all keys are same.

AES!-
Advanced Encryption Standard (AES) is atleast 6 times faster than Triple DES. It is iterative rather than Feistal Cipher. It computes all permutation on bytes rather than bits. It treats the 128 bits of a plaintext block as 16 bytes.

2. List all asymmetric key algorithms.

RSA:- It is an asymmetric key algorithm. and is considered as most secure in encryption. It has following features!-

1. It is a popular exponentiation in a finite field over integers including prime numbers.
2. The integers used by this method are sufficiently large making it difficult to solve

- There are two sets of keys used : private & public

Diffie Hellman Key Exchange:-
It is a method of securely exchanging cryptographic keys over a public channel. It is a method of digital encryption, that uses number raised to the power to produces decryption keys on the basis of components that are never directly. trans

3. List the algorithm for message digest.

1. MD5:-
It is a one way cryptographic algorithms. Its family comprises of hash functions. MD2, MD4, MD5. and MD6. It have been widely used in the software worldwide. For example Servers often provide a pre computed MD5 checksum of all files

2- Secure Hash Function (SHA)
The original version of SHA is SHA 0, a 160 bit Hash function was published by the NIST. SHA1 is the most widely used of the existing algorithms. It is employed in several widely used applications and protocols. including Secure Socket Layer (SSL) security.

Assignment 2:-

Discuss briefly

a) PII (Personally Identifiable Information)

- PII identifiable is an data that could potentially identify a specific individual.
- Any information that can be used to distinguish one person from another and can be used for deanonymizing previously anonymous data can be considered as PII.

b) Us Privacy Act of 1974

- It establishes a code of affair information practices that govern the collection, maintenance and use and dissemination of information about individuals that is maintained in systems of records by federal agencies.

c) FOIA:-

It generally provides any person with the statutory right, enforceable in court to obtain access to Government. Information in executive branch agency records.

This right to access is limited when such information is protected from disclosure by one of FOIA's nine statutory exemptions.

d) FERPA:-

The Family Educational Rights and Privacy Act (FERPA) is a federal law that affords parents the right to have access to their children's education records, the right to seek to have

the records amended and the right to have some control over the disclosure of personally identifiable information from the education record.

e) CFAA :-
It stands for Computer Fraud and Abuse Act. It imposes criminal and civil liability for unauthorized access or damage to a protected computer. This law reaches every computer connected to the internet and non networked computers used by the US govt & financial institutions.

f) COPAA
Childrens Online Privacy Protection Rule imposes certain requirements on operators of websites or online services directed to children under age of 13 years and on operators of other web-sites or online services that have actual knowledge that they are collecting personal information online from child under 13 yrs.

g) VPPA :-
Video Privacy Protection Act was created to prevent what it refers to as "wrongful" disclosure of video tape rental or sale records to cover items such as media games and the future DVD. It makes any video tape service provider that discloses rental information outside the ordinary course of ~~bu~~ business liable for up to $2500 in actual damages.

h) HIPAA:-
The Health Insurance Portability and Accountability Act required the Secretary of the US department of Health and Services to develop regulations protecting the privacy and Security of certain health information.

i) GLBA:-
The Gramm Leach Bliley Act is also known as Financial Modernization Act of 1999. It requires law that requires financial institutions to explain how they share and protect their customer private information.

j) PCI DSS:-
The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure all Companies that accept, process, store or transit credit card information maintain a secure environment

k) FCRA:-
The Foreign Contribution Regulation Act lasts certain obligation on banks in regard to acceptance of foreign inward remittances for onward credit to the accounts of association in India.
These are applicable to all the scheduled commercial Banks.

b) FACTA:- The Fair and Accurate Credit Transactions Act (FACT Act) was enacted in 2003 and amends the Fair Credit Reporting Act (FCRA) a federal law that regulates, in part who is permitted to access your consumer report information. and how it can be used. The Act entitles consumers to obtain one free copy of their consumer files from certain customer reporting agencies during each 12 month period.

Assignment :- 3

State the full form for:-

1. RADIUS :-
   Remote Authentication Dial-in User Services

2. TACAS:-
   Terminal Access Controllee Access Control System.

3. L2TP & PPTP.
   Layer 2 Tunneling Protocol
   Point-to-Point Tunneling Protocol.

4. PPP
   Point to Point Protocol.

5. EAP
   Extensible Authentication Protocol.

6. CHAP
   Challenge - Handshake Authentication Protocol.

7. NTLM:
   New Technology LAN Manager.

8. PAP
   Password Authentication Protocol.

9. SSH
   Secure Shell.

10. LDAP

Lightweight Directory Access Protocol.

Assignment 4.

1. List the name of software for.

1. Firewall.
ZoneAlarm, PeerBlock, Private Firewall, Norton, AVS Firewall, Tinywall, System Mechanic Ultimate Defense, OpenDNS Home, Glasswire

2. Intrusion Detection and Prevention.
McAfee Network Security Platform, Trend Micro Tipping Point, Hillstone NIPS, MazeTrace Enterprise Immune System.

3. Antivirus:-
PCProtect, SCANGUARD, NORTON, MacKEEPER

4. Packet Sniffing
Wireshark, Kismet, Fiddler, Tcpdump, Ethereage

2. State any 10 security software used by ethical hackers.

1. Wireshark
2. Metasploit
3 Nessus
4 Aircrack
5 Snort
6. Cain and Abel
7. Back Track
8 10. Netcat
9. tcp Dump
10. John the Ripper.

3. What is the role of CERT?

Reactive:-

1. Provides a single point of contact for reporting local problems.
2. Assist the organisational constituency and general computing in preventing and handling computer security incidents.
3. Share information and lessons with CERT/CC other CERT's.
4. Incident Response
5. Provide 24x7 security service.
6. Offer recovery procedures.
7. Artifact Analysis.
8. Incident tracing.

Proactive:-

1. Issues security guidelines
2. Vulnerability analysis and response
3. Risk Analysis
4. Collaboration with vendors
5. National Repo. of and a referral policy for cyber instructions.
6. Profiling hackers
7. Conduct training
8. Interact with vendors and others at large to
9. investigate and provide solutions for incidents

4. List OSA OWASP Top ten.

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
6. Broken Access Control
6. Security Misconfiguration
7. Cross Site Scripting
8. Insecure Deserialization
9. Using components with known Vulnerabilities
10. Insufficient Logging and Monitoring.