Enterprise Security Architecture
BS-SE (13)

Name: BABAR KAMAL
ID: 5507

Question 1:
Answer:

a) **Security Policy:** Security policy is a compromise that an organization decides to adopt between absolute security and absolute access.
   - Who can get in or out.
   - Where they can go.
   - When they can get in or out
   - What they can bring in or carry out
   - Physical access
   - Protecting management station

b) **Vulnerability Window:** The time gap between the 1st attack and until you get ready to face it, It indicates how vulnerable you are. Higher the window size, the more vulnerable you are.

c) **Ping of Death:** Type of attack on a computer system that involves sending a malformed or otherwise malicious ping to a computer. Exploits bugs on UNIX, windows, Mac OS. Host crashes when large ping packet arrives ICMP echo > 64kb
   Solution:
   - OS patch can correct the problem
   - No longer an attack

d) **Security Proxy:** Proxy is a program which intercepts packets, examines content and takes some action to safeguard the server. Firewall goes beyond packet filtering and circuit relay.
   -Detect forbidden content.
   Each packet is stripped of its wrapping analyzed, processed, re-wrapped and forwarded.
   -Add some delay as well.

Question 2:
Answer:

a) **Total access vs no access:**
   - Users want the world to be at their fingertip.
   - System admin want to stop as much as.
   - The best way to survive is to have no access.
   - We need compromise
     Answer is: Security Policy

b) **Confusion vs diffusion:**

- Diffusion dissipates statistical structure of plaintext over bulk of ciphertext.
- Confusion makes the relationship between ciphertext and keys as complex as possible.

c) **Hacker vs Cracker:**

Hacker:

- A hacker is a person intensely interested in the arcane and recondite workings of any computer operating system.
- Hackers are most often programmers.
- Hackers obtain advanced knowledge of operating systems and programming languages.
- They might discover holes within systems and the reasons for such holes.

Cracker:

- Cracker is one who breaks into or otherwise violates the system integrity of remote machines with malicious intent.
- Having gained unauthorized access, crackers destroy vital data, deny legitimate users service, or cause problems for their targets.
- Crackers can easily be identified because their actions are malicious.

d) **Intruder Detection vs intruder prevention:**

Intruder Detection:

- Use all sorts of login to check for vulnerabilities.
- Cannot prevent attack but could detect after pr when immerging
- Too complicated need lot of vigilance
- Passive security

Intruder Prevention:

- Prevent before it happens
- Active Security
- Need more processing power
- Methods:
  - -Protocol anomaly detection
  - -Signature based detection
  - -Behaviour based detection
- Prevention is better than detection

Question 3:
b) Answer:

TRANSPOSITION CIPHER:
Message: UNIVERSITY
Code: UNSYNEIIRT

U	V	S	Y
N	E	I	
I	R	T	

RAIL FENCE CIPHER:
Message**:** UNIVERSITY
Code**:** U E T N V R I Y I S

Question 3:

c) Answer:

DES: is most widely used in block cipher in the world, adopted in 1977 by NBS as FIPS PUB 46, It encrypts 64 bit data using 56 bit key, it has widespread use. Uses simple logic operations and it has been considerable controversy over its security.

DES Feistel cipher structure:

- Horst feistel devised the feistel cipher.
  -Based on concept of invertible product cipher
- Partition input block into two halves
  - Process through multiple rounds which perform a substitution on left data half based on round function of right half and subkey
  - Then have permutation swapping halves.
- Implements Shannon's S-P net concept.

Design Parameters:

- Block size
- Key size
- Number of rounds
- Subkey generation algorithm
- Round function
- Fast software en/decryption
- Ease of analysis

----------THE END----------