INT-407 → Information Security and Privacy

CA-1, SET-B.

Name: Mohammad Faisal
Reg No: 11702044 Roll No. B02, SECTION: KE027

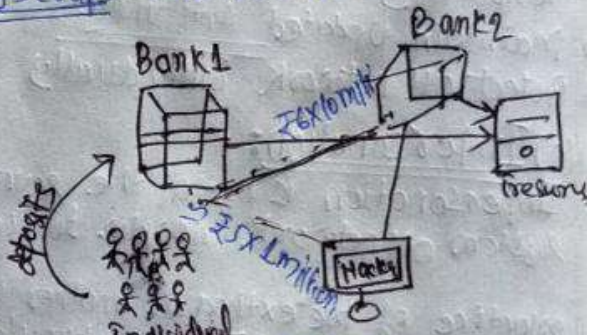
Ans (1) (a) **Salami Attack**: Salami attack is a form of financial cyber attack where the criminal takes an amount of money that is so insignificant that a sigal case is completely unnoticed.

- The amount of money taking in every case is very little (say ₹5), however the number of cases would be large.

Experts views

one school of security expert → slicing the data thin - like Salami

other argues → building up a significant objects or amount from tiny scraps - like a salami.



Ex: ₹10.cr

How / Cause of Salami attack

It is often used to carry out illegal activities.

The attacker uses an online database to seize the information of customers (credit cards details etc) deducting very little amount from every account over a period of time.

Customers remain unaware of attack hence very few complaint launched.

Previous Cases / Examples

January 1993, four executives of a rental car franchies in florida were charged with defraud at least 47,000 customers using salami attack.

In 2008, a man was arrested for fraudulently creating 58,000 accounts from online brokerage firm using salami attack.

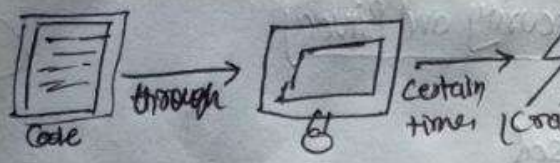
Prevention / Conclusion

Don't store any personal bank information like credit card, debit card in any online websites.

Most important track your money over a define period of time.

(b) Logic Bomb: It is a piece of code inserted into an operating system or any software application that implements a malicious function after a period of time limit or specific condition are met.

Many security reports says Logic bombs are often used with viruses, worms and trojan horses to time them to do maximum damage before being noticed.



Common malicious actions that logic bombs are able to comit include data curruption, file del
or hard drive clearing.

How / Cause of logic bomb

Secretly inserted into the Computer network through the use of malicious code.
Code inserted in the form of virus, worms, or Trojan horses lies dormant and typically undetect
Trigger occured, it may be positive or negative, but demanded and destroy the system.

Prevention / Conclusion

Previous Cases: In USA, March 2002, there was a day when 2000 of the company's servers w
down, about 17000 brokers across the country unable to trade, Nearly 400 branches are
affected. Many files are deleted.

There are some suggestion which prevents us from logic bombing.
(i) Periodically scan the all files, including compressed files,
(ii) maintain Updated Anti virus
(iii) Protect all network individually (iv) Braving Protecting data accessibility.

(c) Impersonation:

Impersonation is one of the several social engineering tools used to gain access to a
system or network inorder to commit fraud, industorial espionage or identity thef

practice of pretexting as another person with the goal of obtaining information or access
to a person, Computer or Company's systems.

Impersonator Role

(i) Posing as a fellow employee
(ii) employee of a vendor or auditor
(iii) a new employee request help
(iv) as someone in authority.

Previous Cases:

(i) Billionaire Robbed through Impersonation. (In 2007)
(ii) Fake delivery man beats and Robs 90 year Old. (In 2009)

Prevention / Conclusion:

Verification is the key for prevention of impersonation.
Awareness is the key as many email impersonation.
Constantly monitoring your digital footprint and social media account is neccassary.

(d) Spoofing: According to the network security, a spoofing attack is a situatio
in which a person or program successfully identifies as another by faisify data,
to gain an illegitimate advantage.

Examples: (i) Common email spoofing attack (ii) Caller ID spoofing attacks
(iii) Domain name System (DNS) by attackers.

How/Causes of Spoofing

- typically take advantage of trusted relationship by impersonating a person or organisation
- whale phishing attacks that feature email spoofing
- A careful spoofing attack can have serious consequences.
- Gain Unauthorized network access bypass access control.

IP address spoofing attacks

- **Caller ID spoofing attack**
  - Call Number with specific Geographic location
  - give up sensitive information
- **Email address**
  - phishing attack
  - Spear attack
- **Website spoofing**
  - dangerous links to be clicked
  - login credential approval
- **ARP Spoofing**
  - Address Resolution Protocol (ARP)
  - MAC address with a legitimate IP address
  - exchange of tokens
- **DNS server attack**
  - MITM attack
  - malware issues arises
  - IP address control.

Protection against Spoofing

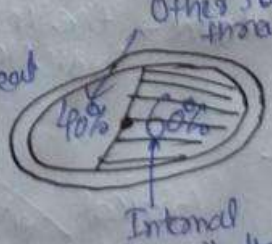
(i) Turn on your scam filter
(ii) Don't click the links or open attachement in emails
(iii) login through separate tab or window
(iv) Invest in a good cybersecurity Program.

(2) Ans: **Security threat**: A potential for violation of security, which exists when there is an entity, circumstance, capability, action or event that could cause harm.

Example: an attacker modifies the database, A remote attacker runs command on server.

Types of Security threats

1. **Internal Security threats:**
   - Internal threats occurs when someone has authorized access to the network with either an account on a server or physical access to the network.
   - Can be internal to the organization as the result of employee action or failure of an organisation.
   - 60% of the security threats are due to the internal security threat



Ex:- In Facebook: A security engineer abused his access to stalk women.

2. External security threats:

External threats can arise from individuals or organisations working outside a company. they do have authorized access to the computer system or network.

- External attacks occur through connected networks (wire and wireless), Physical intrusion or a partner network.
- This threat is detected by the IDS (Intrusion Detection System)

Example: Eavesdropping, Data breaches etc.

3. Unstructured security threats:

Unstructured threats often involve unfocused assaults on one or more network system, often by individuals with limited or developing skills.

- Created by inexperienced individual or information leaked from network by inexperienced individual.

Example: unstructured threats are only executed with the intent of testing and challenging a hacker's skills can still do serious damage to a company

4. Structured security threats:

Structured threats come from hackers who are highly motivated and technically competent.

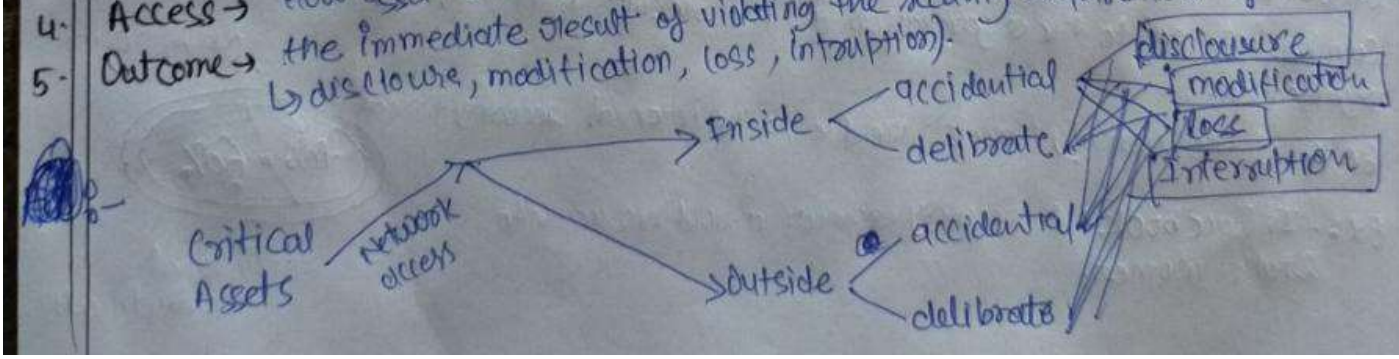
- Knows system vulnerabilities and can understand and develop exploit code and scripts.
- Understand, develop and use sophisticated hacking techniques to penetrate unsuspecting business.

Examples: Often involved with the major fraud and theft cases reported to law enforcement agencies.

Threat Profile: Threat profile is the identification and analysis of the threat to the organization.

Key components basis comprise following items.

1. Assests → value to the organisation (Information in electronic or physical form)
2. Actor → who or what may violate the security requirements (Confidentiality, integrity availability) of an assest.
3. Motive → Indication of whether the actor's intentions are deliberates or accidental.
4. Access → How asset will be accessed by the actor (Network access, physical access)
5. Outcome → the immediate result of violating the security requirement of an assest, ↳ disclosure, modification, loss, interruption).



(3) Ans difference between security threats (Information level Vs Network level)

Information level threat	Network level threat
(1) Information threat is potentially possible influence or impact on an automated system with subsequent damage to someone's needs	(1) Network level threat include information gathering sniffing, Spoofing and denial of Service.
(2) Shortcoming of software or hardware	(2) Code and SQL injection attacks
(3) Structure of automated system in the information flow.	(3) Privilege escalation, man-in the middle attacks
(4) Inaccuracy of information exchange Protocol and interface	(4) Insides threats that is penetrate the network in order to harm.
(5) factors weaking information security.	(5) Advanced persistent attacks.
Protection	**Protection**
↳ Integrity towards the database.	Cynet 360 is the holistic security solution that Protects against across the network.
↳ Confidentiality restricts access to information resources	↳ Blocking suspicious behavior
↳ Authencity shows trusted person is save	↳ UBA-a real time analysis on behaviour of networks.
↳ Accessibility - Public information with authorized access.	↳ Uncover Hidden threats

(4) Ans :- Information Classification is a process in which organisations asses the data that they hold and the level of protection it should be given.

↳ to grant who is going to see and who is not ?

following are the factors which associated with the classification

(1) **Unclassified : Unrestricted**
this is the default and refers to information that Can be release individuals without clearance.
for example: In US, Homeland security praised U.S. terror threat level data.

(2) **Confidential :**
It is applied to information, the unauthorized disclosure of which reasonably Could be expected to cause damage the organisation security.

(3) **Secret :** This is the third level securityclassification, when its unauthorized disclosure would cause "serious damage" to organisation security.

- Most of the information classified is held at secret sensitivity.

Ex:- Google, Microsoft, Amazon is having payroll related documents in that level of classification

(4) Top secret:

- It is the highest classification
- Unauthorized disclosure of which reasonably could be expected to cause "exceptionally grave damage" to the organization security is able to identify
- Ex:- It is believed that 1.4 million Americans have top secret clearances.

(5) Sensitive but unclassified:

- Any information which the loss and misuse, or unauthorized access to of modification of which adversely affect the national interest or organisation street.
- It is also refered as SBU unit.

(5) Ans:- difference between Virus, Worm and Trojan Horse:

	Virus	Worm	Trojan Horse
①	Virus is the software or computer program that connect itself to other software or computer program to ruin computer system.	① Worms replicated itself to cause slow down the computer system	① Trojan horse neither than replicate capture some important information about a computer system or a computer network.
②	Virus replicates itself	② Worms are also replicates itself	② But Trojan horse does not replicate itself
③	Virus can't be controlled by remote	③ Worms can be controlled by remote	③ Like worms, Trojan horse is slow in comparison of both virus and worms.
④	Spreading rate of virus are moderate.	④ While spread rate of worms are faster than virus and trojan	④ Trojan spread is moderate
⑤	The main objective of virus is to modify information	⑤ main objective of worms to eat the system resources	⑤ Trojan horse's main objective is to steal the information.
⑥	Viruses are executed via executable file (.exe)	⑥ worms are executed via weakness in system	⑥ Trojan horse executes through a program and interpts as utility software.

END of the QUESTION ANSWER sheet