NIS
Network and Information Security
&
SIC
Security in Computing

What is NIS and SIC about ?

- SIC and NIS is about studying the Network Security.
- It is about what is Information
- What is Attack
- What is defense
- What are the protocols
- What is authentication, Authorization and Accessibility
- Cryptography
- Access Controls

What is Information?

- Information is an asset of any organization.
- Information is classified according to the sensitivity and its vulnerability for theft or misuse
- Loss or theft of confidential information could violate the privacy of individuals, reduce the company's competitive advantage, or cause damage to the company
- In order to protect their data against any security threats using
  - Risk Assessment Methodology to identify its critical resources and possible areas of risk
  - If any risks are identified then the company should develop an extension plan to mitigate the attacks.
  - A Company should also have Business Continuity Plan and Disaster Recovery Plan ready so that the business operations can be continued in case of a Security attack.

What is Computer Security?

- Before Computer Security, What is Security?
- Security is about protection of assests.
- Security in case of Computer systems can be distinguished as follows:
  - Prevention:- Taking measures that prevent your assets from being damaged.
  - Detection:- Taking measures that allow you to detect if the asset is under damage, how it has been changed and who has cause the damage.
  - Reaction:- Taking measures that allow you to recover your assets or to recover from damage of your assets.

What is Computer Security?

- Lets illustrate it:-
- Prevention:- Use encryption when placing an order in an E-Commerce Website. Rely on the merchant to perform some checks on the caller before accepting a credit card order. Don’t use your card number on the Internet.
- Detection:- A transaction that you did not authorize appears on the Credit Card Statement.
- Reaction:- You can ask for a new card number. The cost of the fraudulent transaction may have to be covered by the card holder, the merchant where the fraudster made the purchase, or the card issuer.

Network Security Basics:-

- In Computer Security, there are 3 aspects which we need to see how information can be compromised.
- 1. Confidentiality:- Prevention of unauthorized disclosure of information
- 2. Integrity:- Prevention of unauthorized modification of information
- 3. Availability:- Prevention of unauthorized withholding of information or resources. e.g.:- Denial of Service
- 4. Accountability:- Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party.

Risk and Threat Analysis

- Security Policies:- A statement that defines the security objectives of an organization; it has to state what needs to be protected; it may also indicate how this is to be done
- This also includes ISO certifications
- What is Risk?
- Risk is associated with the consequences of uncertain events.

Risk and Threat Analysis

- Assets:-
  - First thing in IT system is to value the assets includes:-
    - Hardware- Laptop, computers, smart cards, etc.
    - Software:- applications, operating systems, website, database management system, source code, etc.
    - Data and Information:- essential data for running and planning your business, design documents, digital content.
    - Reputation
  - Assets such as hardware may cost monetary replacement costs
  - For Data or information leaks may lead to loss in clients or customers and may cause loss to the profits

Risk and Threat Analysis

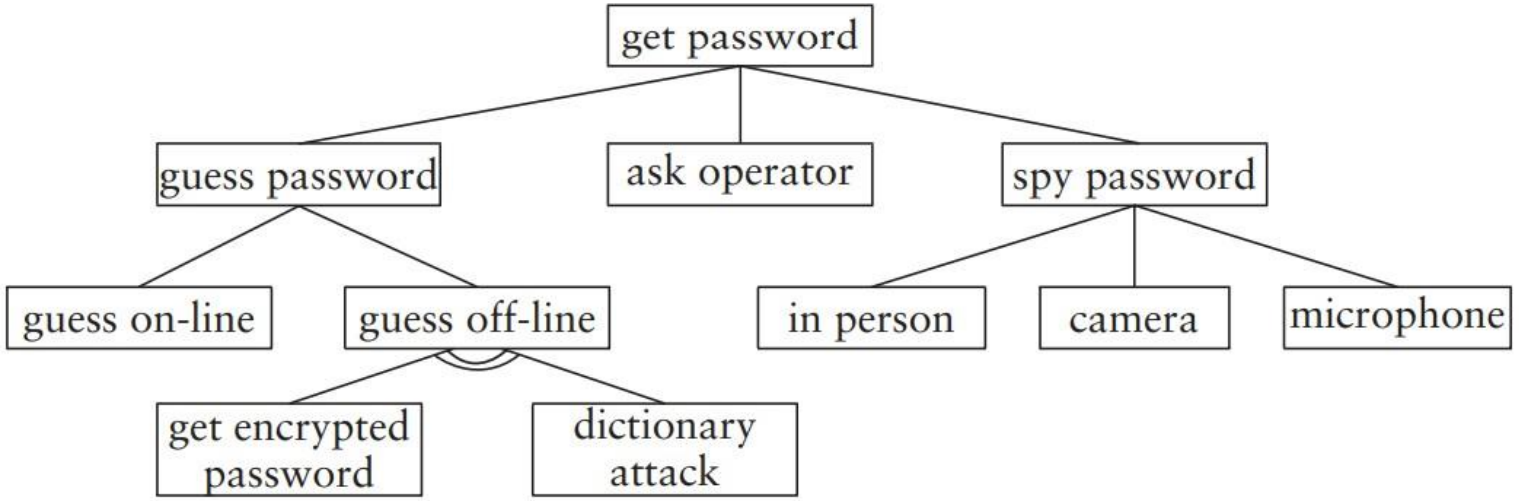
- Threats:-
  - Threat is an undesirable negative impact on your assets. There are various ways of recognizing the threats.
  - We can categorize the threats according to the agents and assets
    - Spoofing identities
    - Tampering the data
    - Repudiation
    - Information Disclosure
    - Denial of Service
    - Elevation of privilege

Risk and Threat Analysis

- Vulnerabilities:-
  - Vulnerabilities are the weakness of the system that could be accidentally or intentionally exploited to damage assets.
  - accounts with system privileges where the default password, such as ‘PASSWORD’ has not been changed;
  - weak firewall configurations that allow access to vulnerable services.
  - Risk analysis team should measure the criticality of the vulnerabilities.
  - *Vulnerability scanners* provide a systematic and automated way of identifying vulnerabilities.

Risk and Threat Analysis

- Attacks:-
  - An attack is a sequence of steps which a attackers uses to damage a particular system.
  - It starts with gathering the information needed to move on to gain privileges on one machine, from there jump to another machine, until the final target is reached.
  - To get a full picture of its potential impact, a forest of attack trees can be constructed. Attack trees are a formalized and structured method for analyzing threats



Countermeasures

- Result of risk analysis is a prioritized list of threats, together with recommended countermeasures to mitigate the risk.
- This will help us to get the ROSI (Return of Security Investment)
- Countermeasures can be installing firewall, proxy server, anti virus, authentication protocols , Access Control , etc.

Thank you so much for hearing with Patience