SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING-IOT Including CS&BCT

COURSE NAME : **19SB402**- NETWORKING AND CYBERSECURITY

II YEAR / III SEMESTER

Unit II- **SECURITY THREATS**

Topic : **Target Assets and vulnerability**

Assets:

➢ It is any data (or) device (or) other component of an organisations system that is valuables.

E.g. Employee -> Computer, Company phone.

➢ Org most common assets are Intermutior assets.

Like: Database, Physical Files.

➢ It can be refers to "A".

Threats:

➢ It is an incident.

➢ It is could negatively affect on assets.

  E.g. Any assets are accessed by unauthorized party.

Vulnerability: (Weak spots)

➢ It is a weak spots within your environment and your assets.

Security Vulnerability:

➢ It is a weakness, flow (or) error found within a security system.

E.g.

1. Broken Authentication – Exp.

2. SQL Injection.

3. Cross site scripting.

4. Cross site Request Forgery.

5. Security Misconfiguration.

Data Leak:

➢ It is occurs when data is accidentally leaked from within an org

➢ Data Leakage is usually the result of mistake.

    E.g.

    Sending a confidential message (or) mail to the wrong email.

Data Leak:

Step1: (Characterization)

Analyse assets & criticality screen assets (or) consequence identity critical assets.

Step2: (Threat Assessment)

Analyse threats & assets attractive. Determine target assets.

Step3: (Vulnerability Assessment)

Conduct Scenario analysis. Determine act specific consequences and vulnerability.

Data Leak:

Step4: (Risk Evaluation)

Assess risk against security criteria.

Step5: (Risk Treatment)

Evaluate security upgrades as required.

Determine residual risk.

Any Queries

Thank You!