**SYSTEM SECURITY AND AUDIT**

**Lesson 1:**

Introduction.

What is system Security and audit

This is a protection of information systems from theft or damage to  hardware, software and information as well as the disruption of services that they provide

**Objectives of learning system security and audit**

1. importance
2. Develop a strategy for pursuit of career in information security
3. Understand information security in business
4. Protects computes, networks of organizations

C. I. A (Confidentiality, integrity, authenticity, availability) - - - > goals of system security

**Goals of computer security**

1. Come up with strategies for prevention, detection and recovery of data and information
2. provide services for confidentiality, integrity, availability and authenticity

**12 principles of security**

i) there is no such thing as absolute security

-given enough time, skills and tools, a hacker can break any system security

ii) the 3 security goals (CIA) Protect the confidentiality of data,

--no unauthorized access to information is permitted and accidental disclosure of sensitive information

--Preserve integrity of data. This keeps data pure and trustworthy and protects data from intentional and accidental changes

--promotes availability of data for authorized use

iii) defense  in depth of a strategy

--Implements security in overlapping layers that provide the 3  elements that secure assets.. Prevention, detection, recovery

Iv) When left on their own, people tend to make the worst security decisions

V) functionality  and assurance requirement - - functionality requirement  describes what a system should do while assurance requirement describes how functionality systems  should be implemented and tested

What is verification? - - process of confirming that one or more predetermined requirements are met

What is validation? - - This is the correctness or quality of the mechanism used to meet the requirements stated above

Vi) security through obscurity  is not an answer

vii) risk management.. Security is not concerned with eliminating all threats but eliminating known threats and minimizing loses. Risk analysis and management are central in securing systems. They place an economic value on assets to best determine appropriate counter measure that protect them from loses

Vulnerability – this is a known problem within a system or program

Exploit – this is taking advantage of a specific vulnerability or weak point

Attacker – this is the link between vulnerability and an exploit

Viii) Security controls

Security mechanism servers the purpose by preventing a compromise, detecting that a compromise is underway and responding to a compromise why it is happening or after it had been discovered.

ix) complexity is the enemy of security - - the more complex the system gets the harder it is to secure

X) fear, uncertainty and doubt do not work in selling security

XI) People. Process and technology are all needed - - this are essential elements of security practices including operations, applications, physical security, and cryptography

Xii) open disclosure of vulnerability is good for security

**COMPUTER SECURITY ARCHITECTURE**

What is a threat?

This is an event or action that might violate the security of information system.

A threat is a possible danger that might explore an vulnerability.

Components of threats

1. A target – this is the aspect of security that might be attacked-security services ie CIA
2. Agent-this is the person or organisation originating the threat

**Characteristics of an agent**

1.access – they have access to your network

2 motivation – whats the motive behind the attack

3.knowledge – this is the level and type of information the agent has about the target

4.event – type of action that passes the threat

3.Attacks – this is an assult om system security that is derived from an intelligent threat ie intelligent act that is deliberaye attempt to evade security services and violate the security policy of a system

What hackers exploit to break into a system

1. Buffer overflows
2. Open file sharing
3. Weak passwords
4. Programming flows, bad programming

**How hackers behave :**

1. Select target using ip lookup tools
2. Able to identify potential vulnerable services
3. Map network for accessible services
4. Bruteforce- guessing passwords
5. Install remote administrative tools
6. They wait for admin to login and capture passwords
7. They use password to access the remaining part of network

**-**the osi security architecture focus on security attacks, mechanisms and services

**Security mechanism**

**-**this is a process or device that is designed to prevent, detect or recover from secirity attack

**Security services**

**------**

**.**

-setvices that enhance security of data processinf system and information transfer of an organization

**Types of attacks**

1.passive attacks eg eavesdropping or monitoring of transmissions eg release of messages and traffic analysis

2. Active attacks – modification of the data stream or crstion of false streams eg replay, DdoS, modification of messages

**Threats**

**Type of threats**

1. Disclosure
2. **Diception or acceptance of false data**
3. **Disruption or prevention of correct operation**
4. **Usurpation or anauthorised access**
5. **Masquerating – inpefsonation of one entity to another**
6. **Rep-this is a false denial that an entity..**
7. **Denial of receipt.**
8. **Delay**
9. **Denial of service**

**Anauthorised interception of info. It is afrom of disclosire.**

**It involves an entity listening**

**Security policy**

This is a formal statement of the rules bywhicj people who afe fiven access to an organizations assets, technology amd informstion assets mist abide

1. To inform usrrs staff anx managers of their obligatofy requiremtns for protecting technologu anfd informagion.
2. Specify the mechanisms throygh this requiremnets must ne met
3. It provides a baseline from which it will acquire ro configure and audit compurer systems and neteork for compliace
4. Spell out corporate position on private  issues and intellectual property jssues

Individuals that matter in creating

1. Site security administrator
2. IT staff
3. Adminstrarors of large user groups
4. Security incident response team
5. Representatives of security group
6. Legal counsellor
7. The corporate management

Characteistics of a good security  policy

1. Must be implementable tjrough sytstem admin procedures
2. It must be enforciable with seciriry tools
3. Must clearly define  the key areas of responsibilty for users, administrators and management

Componrts

1. Purchasing guidelines. Access policy which defines access rights and privileges
2. Accountabilty polocy. This defines
3. Authentication policy. This is established through peffective password policy.
4. Availabilty statement.
5. Violations reporting policy.
6. Supporting infkrmation which provide users, staff, and management with contact information for each type of policy violations amd guidelines

Security mechnisms

1. Encipherment. This is a use of algorithm to transfrom data into a form which is not readilty intelligeable
2. Digital signatures. This is data appemded to data unkt thay allows a recipient to prove the source and integrity of the data
3. Access control. This are mechanism that enforce access rights to resources
4. Data integrity.
5. Authentication exchange. Mechanism intended to ensure the jdentity of an entity  by means of informstion exchange
6. Traffic padding. Inserion of bits into gsps to frustrate teaffic analysis
7. Routing control. Involves selecting secure routes
8. Notarization. The use of a third party to assure certain properties of data exchange

Mechanisms not specific to osi /pervasive

1. Trusted functionality
2. Event detection. Detect seciruty relevant event
3. Security audit trail. Data collected to keep record of ssystem activity
4. Security label. Names and securiy attributes of a resource
5. Security recovery. Takes recovery actions