NAME :- KRUNAL RANK

ROLL NO :- U18C0081

CLASS :- BTECH 4TH YEAR

SEMESTER :- 7

DIVISION :- B

U18CO081

27/07/21

CNS Tutorial 1

Ans 1.

i) Confidentiality : Confidentiality is equivalent to privacy and avoids the unauthorized disclosure of information. It involves the protection of data, providing access for those who are allowed to see it while disallowing others from learning anything about its content.

ii) Traffic flow confidentiality : These are ~~nos~~ techniques divised to hide the traffic pattern to prevent ~~sat~~ statiscal traffic analysis attacks.

iii) Integrity : Integrity refers to the methods for ensuring that the data is real, accurate and safeguarded from unauthorized user modification. Some examples to reinforce integrity are:- backups, checksums, data correcting codes.

iv) Availability : Availability is the property in which information is accessible and modifiable in a timely fashion by those authorized to do so. It is the determination of constant and reliable access to sensitive data. Some tools ~~to~~ to enforce availability are physical protections and redundant data stored in distant, remote data centers.

v) Nonrepudiation: Nonrepudiation is the assurance that someone cannot deny something. Typically, it refers to the ability to ensure that a party to a ~~consta~~ contract or a communication cannot deny the authenticity of their signature on a document ~~or~~

Ans 2:

Hackers:- A hacker is a computer expert that has the knowledge and deep understanding of the underlying ~~st~~ computer system and software, who uses the knowledge to subvert the system and violate the confidentiality, integrity or availability of the system data.

Crackers:- A cracker is a computer expert with deep understanding of the ~~underl~~ computer systems, who uses that knowledge to bypass the security of a software or network.

Script kiddies:- These are people who use existing scripts and codes to hack into a system, lacking the skill to write those codes on their own.

Spies:- Spies are the people who ~~are~~ unauthorizedly monitor the data on a network or in a system to obtain valuable secrets and sensitive information

Employees : Employees are the people who work for an organisation registered under the government. They are assigned tasks based on their skillset for which they are paid salaries.

Cyberterrorists :- Cyberterrorists are the experts who promote and are involved in cyberterrorism, cyber crimes and cyber harrassments. Their acts are either politically motivated or self motivated against information systems.

Ans3. An intrusion detection system is a system that monitors network traffic for suspicious activity and issues alerts when activity is discovered. It consists of 3 components:-

- Data preprocessor (audit data) :- This components involves in ~~Prep~~ preprocessing and organising data in order ~~to detect for existing malware signs~~ to analyse it later by the analyser. The preprocessor formats the incoming data according to pre-defined standards.

- Analyzer :- Analyzer is used to detect possible signatures of malware which are ~~as~~ matching to an existing database of such signatures in the incoming preprocessed data.

- Response engine :- Response engine is a component that is used as a failsafe if and when a malware or anomaly is detected in the incoming data.

Ans 4:

Security Approaches	Name of the Security Mechanism
Attack Deterrence	Notarization
Attack Prevention	Firewalls
Attack Deflection	Access Control.
Attach Avoidance	Digital Signature