Institute of Public Administration
Communication and Network Security
Group 1
Homework (1) Solution

Question (1)
Mention the unintentional components in protocol specifications, protocol implementations, or other types of software that are exploitable by attackers.

Solution:
Loopholes.
Flaws.
Defects.

Question (2)
Define a Cryptanalysis concept.

Solution:
Cryptanalysis is the art and science of finding useful information from ciphertext data without knowing the decryption keys.
For example, in a substitution cipher that substitutes plaintext letters with ciphertext letters, if a ciphertext message reveals a certain statistical structure, then one may be able to decipher it.

Question (3)
List the common types of attackers.

Solution:
- Black-hat hackers.
- Script kiddies.
- Cyber spies.
- Employees.
- Cyber terrorists.

Question (4)
What are the basic components of security model?

Solution:
- Cryptosystems.
- Firewalls.
- Antimalicious-software software (AMS software).
- Intrusion detection systems (IDS system).

Question (5)
List the most common online security resources.

Solution:
- CERT.
- SANS Institute.
- Microsoft Security.
- NTBugtraq.

Question (6)
Name one secure network protocol, which can be used instead of telnet to manage a router?

Solution:
SSH

Question (7)
Provide a reason as to why https should be used instead of http.

Solution:
HTTP sends data in clear text whereas HTTPS sends data encrypted.

Question (8)
Which protocol does https uses at the transport layer for sending and receiving data?

Solution:
TCP

Question (9)
_____ ensures that information is correct and that no unauthorized person or malicious software has altered that data.

Solution:
Integrity

Question (10)
_____ ensures that only authorized parties can view information.

Solution:
Confidentiality