Introduction to Information Security and Forensics

Assignment 01

Distribution Date: 17-10-2022

Due Date: 25-10-2022

Instructions:

- Submit this assignment by turning in in the reply of this assignment on Microsoft Teams with the file title **"YourRegNo_YourName_YourSection_AssignmentNo".** Incorrect title can harden to find your email from inbox, and you may get **0** marks.
- Late submission is not allowed (Time has fixed on Microsoft Teams). Late submission request with any excuse will be strictly denied.
- Don't copy any material from Internet and don't share your assignment with your colleges. If anyone fail to compliance this policy, he/she will be awarded **0** marks**.**
- You will have to submit MS Word file in attachment. If it is required to submit any snap or screenshot, place it in Word document with appropriate caption.
- Don't forget to add citation if you are getting help form a websites or books.
- Your assignment report should be well formatted according to the standard format. Submit assignment report in APA format. You can easily find template and examples of APA format from Internet

Marks Distribution

APA Format	5
Citation	5
Questions	40
Total	**50**

Q1

Hands on Projects: Different Hands-on projects are mentioned in the end of chapter 01 of recommended book (Comptia Security + Guide to Network Security Fundamentals). Complete following projects. Take screenshot of each step and submit in assignment.

1. Project 1-1: Examining Data Breaches—Textual
2. Project 1-3: Scanning for Malware Using the Microsoft Safety Scanner
3. Project 1-5: Creating a Virtual Machine of Windows 10 for Security Testing

---

Q2

What are the default passwords? Why can following configuration cause serious security concerns?

1. Default Configurations
2. Misconfigurations
3. Weak Configurations

Why are insider attacks considered as most lethal attacks?

Q3

Briefly describe the functionality of following Kali Linux commands with screenshots. Remember, you should run these commands in correct format. Elsewise, you will be marked **0**.

1. **Ipconfig**
2. **Ping www.google.com**
3. **Ping -c4 www.google.com**
4. **Ping6 -c4 localhost**
5. **Arp -a**
6. **Tracert**
7. **Nslookup**
8. **Netstat**

END