Ministry of Higher Education
COLLEGES OF APPLIED SCIENCES
Information Technology DEPARTMENT
Course Title: Introduction to Security
Course Code: ITDR2108

Security Research Project Guidelines (10 Marks)

Aims of the project:

- Enhance student capability to learn and research beyond the lectures.
- Enhance student ability to work individually/group and represents his/her knowledge through the written report.
- Enhance student ability to work as group and represents their knowledge through the presentation.
- Enhance student creativity in applying all the concepts learnt in lectures and labs as core for the basic implementations needed for work environment.
- Enhance student ability to evaluate and audit any given security related case study and implement the required security system practically.
- Enhance student ability to work and implement within the time frame.

Team Size: 2

Report Structure:

- ✓ Cover page with (Unique "**Project Title**")
- ✓ Project Approval Form
- ✓ Marking Guide sheet
- ✓ Introduction
- ✓ Objectives
- ✓ Survey (Give 100 words of previous/ongoing research about the topic you have chosen. Include the Sources in the **References** page)
- ✓ Project Flow Diagram
- ✓ Implementation
- ✓ Result Interpretation (Tables, Statistics, Graph,.etc.)
- ✓ Conclusion
- ✓ References
- ✓ Appendices

Resources:

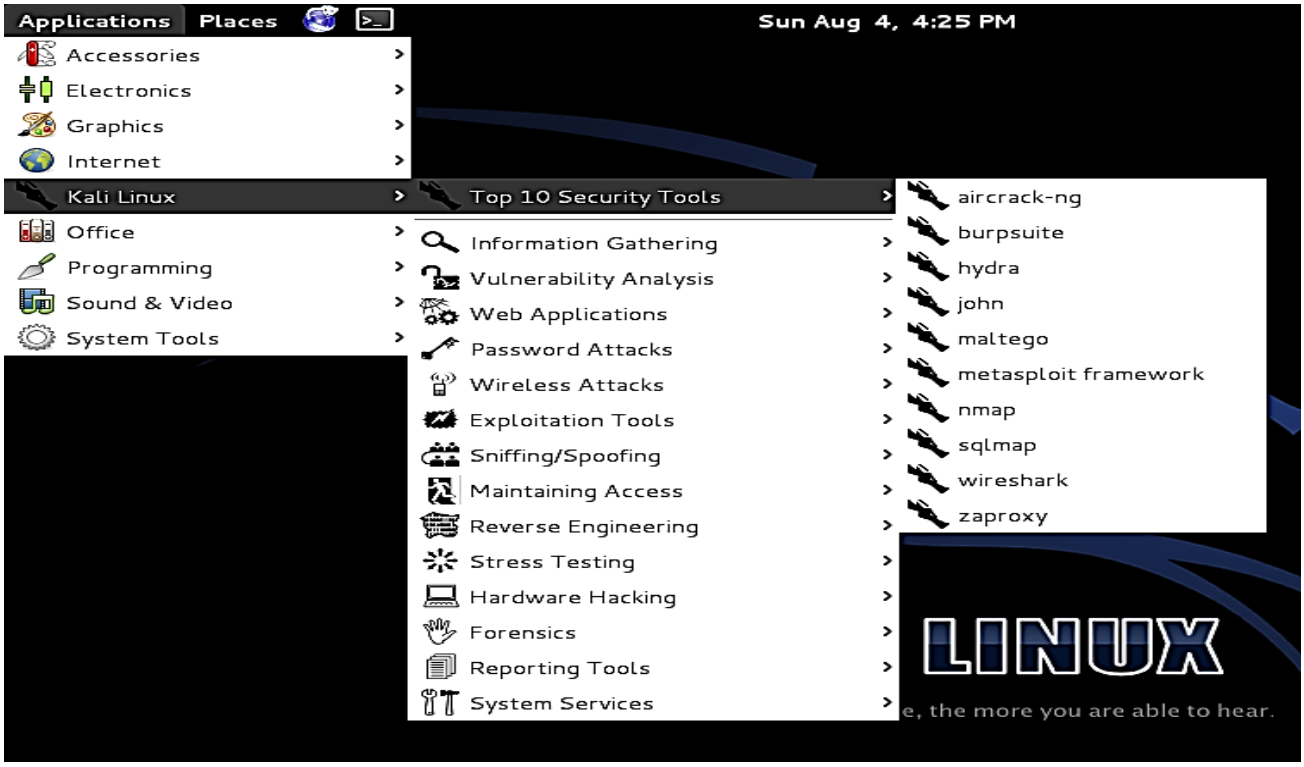
- ✓ Kali Linux, Windows XP, Windows Server2003
- ✓ **No GUI based tools allowed to present unless the tools have network implementation**
- ✓ Virtual Box/VM Ware
- ✓ Refer to Lectures and Labs.
- ✓ Refer to college library-you need to refer at least two books
- ✓ Technical Websites/Google Search/YouTube Videos
- ✓ Blackboard
- ✓ No internet allowed during the presentation

Report Format and Instructions:

- ✘ Total number of pages is between 15 to 30 pages (A4).
- ✘ Follow standard typeset format for report
- ✘ Use comb binding for the report, first and last page are transparent.
- ✘ Copy and paste is not allowed. You are expected to produce you own report.
- ✘ If there are two similar assignments, both will receive ZERO. It does not matter who copied from whom!
- ✘ It is recommended that you show your progress to your instructor to make sure you are on the right direction.
- ✘ Avoid submitting on the last day as you are doing so at your own risk. Never leave things to the last minute. You should always account for Internet connections problems and other problems that you might encounter on the last day.
- ✘ You must upload a softcopy of your report in **Blackboard Safe Assignment** to ensure no plagiarism.
- ✘ Submit hardcopy report during week-14, presentation at week-15.
- ✘ Submit hardcopy report to the course instructor two days before the presentation.

The Case Study Implementation: Telecommunication System

- Students are requested to discuss the current security system in a Telecom sectors and implement a solution to secure users' data.
- Students can discuss only one of many Wired or Wireless internet telecommunication services for this case study implementation.
- Student must choose "**A Project Title"** in relation with the attack and the prevention strategy. (Ex. "**Securing User Data from Network Spoofing**")
- Students must generate an attack on a user data in the telecom services using Linux KALI and Windows Client Virtual Environment.
- Students must choose one of the following types of attacks supported by the KALI Linux OS for experiments.
- ****No Internet allowed for presenting the project, Non-working or without implementation, projects will be disqualified.**



KALI Linux Supported Attacks

- Contrast your attack on the communication services in terms of user data Privacy, Availability, Integrity, Confidentiality, Non Repudiation, Vulnerability, Threats, Exploitations, and Risks.(Choose one or two to represent your attack)
- Students must provide ground truth samples for the attack.
- Students must address a solution to prevent the community from such attacks.
- Students must provide advises to the ISPs about preventive measures.

Project Overview and Approval

Project Name: Securing User Data from Network Spoofing

Abstract:

An introductory task of the project will include the general definitions of telecommunication services and in the context of network security, a spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage. It discusses the importance of User data and the services provided by the telecommunication operator. The types of services are used by the users and their limitations as well. Our team identified the possible attacks on the available services by network spoofing. In addition, the theoretical part will also allow us to understand the basic concepts like data Privacy, Availability, Integrity, Confidentiality, Non Repudiation, Vulnerability, Threats, Exploitations, and Risks. We decided to secure the data from Network spoofing and experiment the same using **KALI** and **Windows** client virtual environment. At the end of the experiment we prove that the Network spoofing is used for falsifying user data and gain access to it with examples. The practical and report parts are summarized in the following tabular form and the allocated tasks for each member of a group.

Task Allocating Schedule

Theoretical Task	Practical Task	Timeline	Done by
1. Problem statement 2. Choosing the attack 3. Configuration steps 4. Definitions 5. Example 6. Write the final report	1. Internal Network Implementation 2. Kali installation 3. Troubleshoot 4. Activate the attack	1-Mar-15	Ahmed
1. Implementation **2.** Understanding the attack **3.** Reports **4.** Submisions **5.** Example **6.** Write the final report	1. Install XP 2. Internal Network 3. Prove the attack 4. Troubleshoot the entire network	1-Mar-15	Khalid

Names:	**Khalid**	**Fahad**
IDs:	**2008299487**	**2008299295**
Group: 20		
Supervised by: Mr. Faizal	**Lecturer at the Information Technology Department**	
Approved?		**Instructor Signature**

Marking Guide sheet

(To be used by the Instructor)

Topic	
Student Name	**Student Name**

Evaluation Criteria

Criteria	Points to be observed	Marks for student 1	Marks for student 2
Content **(Max Marks=2)**	Is the content interesting and relevant? Is the topic supported with sufficient discussion?		
Display and delivery **(Max Marks=2)**	Have the presenters spoke key points, intro, and concluding remarks without reading? Is the presentation use sufficient text, pictures, graphs, etc to substantiate the topic? Is the topic delivered clearly?		
Technical **(Max Marks=4)**	**(Below kind of Questions the Instructor has to be prepared)** What kind of threat discussed in this document? What is the name of the attack? What is the target of the attack? What are the 5 important background of the attack? What are the solutions provided by you? What kind of software used by the attacker? What did you understand from the topic? How do you become victimized? Justify. **Lab demonstrations and basic troubleshooting.**		
Team Work **(Max Marks=1)**	Does the presentation reveal that all the members have worked as a team? Does the session prove that each member performed a task in the preparation of the presentation? Does everyone Contribute equally?		
Individual **(Max Marks=1)**	Are the presenters comfortable and fluent in the use of the presentation media? Is the presenter self-confident? Is the presenter able to answer any question in what his/her mate present?		
Total			