 

19CS3041S – CRYPT ANALYSIS AND CYBER DEFENCE

SKILL WORKBOOK

TEAM CACD

KLEF | CRYPT ANALYSIS AND CYBER DEFENCE – 19CS3041S



**SKILLING WORKBOOK**

|  |  |
| --- | --- |
| STUDENT NAME |  |
| REG. NO |  |
| YEAR |  |
| SEMESTER |  |
| SECTION |  |
| FACULTY |  |

|  |
| --- |
| 1. **Installation of virtual box and Kali Linux.** |
| 1. **Implementation of Packet Capturing Using Airodump-ng** |
| 1. **Implementation of Social Engineering Using Ghost Phisher** |
| 1. **Implementation of Social Engineering Using Maltego** |
| 1. **Implementation of Password Cracking Using John the Ripper** |
| 1. **Implementation of Wi-fi Hacking Using Reaver** |
| 1. **Implementation of NMAP Tool** |
| 1. **Implementation of Vulnerability Analysis.** |
| 1. **Implementation of Man in the Middle Attack (Ettercap Tool)** |
| 1. **Implementation of Mobile Security Using APK Tool.** |
| 1. **Implementation of Web Application Security** |
| 1. **Implementation of Web Application Security (Paros)** |
| 1. **Implementation of SQL Injection Using SQL Map** |
| 1. **Implementation of Cross Site Scripting Attack.** |
| 1. **Exploiting Windows Machine using Metasploit** |

Table of Contents

**Organization of the STUDENT SKILL WORKBOOK**

The laboratory framework includes a creative element but shifts the time-intensive aspects outside of the Two-Hour closed laboratory period. Within this structure, each laboratory includes three parts: Preskill, In-skill, and Post-skill.

* 1. **Pre-Skill**

The Pre-skill exercise is a homework assignment that links the lecture with the skilling period - typically takes 2 hours to complete. The goal is to synthesize the information they learn in lecture with material from their textbook to produce a working piece of software. Prelab Students attending a two-hour closed laboratory are expected to make a good-faith effort to complete the Pre-skill exercise before coming to the lab. Their work need not be perfect, but their effort must be real (roughly 80 percent correct).

* 1. **In-Skill**

The In-skill section takes place during the actual skilling period. The First hour of the skilling period can be used to resolve any problems the students might have experienced in completing the Preskill exercises. The intent is to give constructive feedback so that students leave the lab with working Preskill software - a significant accomplishment on their part. During the second hour, students complete the In-skill exercise to reinforce the concepts learned in the Pres-kill. Students leave the lab having received feedback on their Pre-skill and In-skill work.

* 1. **Post-Skill**

The last phase of each skilling class is a homework assignment that is done following the skilling period. In the Post-skill, students analyse the efficiency or utility of a given system call. Each Post-lab exercise should take roughly 120 minutes to complete.

| **S. No** | **Date** | **Experiment Name** | **SKILLING EVALUATION** | | | **Viva Voce (10M)** | **Total** | **Faculty**  **Signature** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **EXECUTION (10M)** | **RESULT**  **(10M)** | **ANALYSIS**  **(10M)** |
| 1 |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |  |  |
| 7 |  |  |  |  |  |  |  |  |
| 8 |  |  |  |  |  |  |  |  |
| 9 |  |  |  |  |  |  |  |  |
| 10 |  |  |  |  |  |  |  |  |
| 11 |  |  |  |  |  |  |  |  |
| 12 |  |  |  |  |  |  |  |  |
| 13 |  |  |  |  |  |  |  |  |
| 14 |  |  |  |  |  |  |  |  |
| 15 |  |  |  |  |  |  |  |  |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SUBJECT CODE: 19CS3041S**

**CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK**

**1. Installing Virtual Box and Creating a Virtual install of Kali Linux**

**Date of the Session: \_\_\_/\_\_\_/\_\_\_ Session Time: \_\_\_\_\_to\_\_\_\_\_\_**

**Learning outcome**:

* Understanding of OS virtualization
* Understanding how to setup Virtual Box
* Understanding how to setup Kali Linux

## **Pre-Skill Task:**

1. Explain about OS virtualization?

2. Explain what is hypervisor?

3. Explain the Types of hypervisors?

## **In-Skill Task:**

*Harsha a* technology evangelist has just started learning about OS virtualization and interested in learning ethical hacking as Harsha a newbie in this you are requested by Harsha to help him to install Kali Linux in his computer using Virtual Box

**Solution:**

**Post-Skill Task:**

1. Why Kali Linux is newbie friendly for cyber Security enthusiast?
2. What are different types of Linux Distro’s available?
3. List some security focused Linux Distro’s available.

*(For Evaluator’s use only)*

|  |  |  |
| --- | --- | --- |
| |  | | --- | | Comment of the Evaluator (if Any) |  |  | | --- | | Evaluator’s Observation  Marks Secured: \_\_\_\_\_\_\_ out of \_\_\_\_\_\_\_\_  Full Name of the Evaluator:  Signature of the Evaluator Date of Evaluation: | |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SUBJECT CODE: 19CS3041S**

**CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK**

# 2. Implementation of Packet Capturing Using Airodump-ng

**Date of the Session: \_\_\_/\_\_\_/\_\_\_ Time of the Session: \_\_\_\_\_to\_\_\_\_\_\_**

## **Learning Outcomes:**

* To understand the concept of Data Sniffing over WIFI.
* To understand how to use Airodump-ng for Sniffing.

**Pre-Skill Task:**

1.What is Airodump-ng?

2.What is capture handshake?

**In-Skill Task:**

**1**.Ramesh wants to perform **“CRACKING WEP KEYS**” By using Monitor mode which was available in kali Linux. So, he wants to perform following operations:

1.Monitor mode using wifi-adapter

2.Capturing packets

3.Capturing ARP requests

Help him by doing those operations Successfully(If Possible include screenshots of those outputs)

**Solution:**

*(For Evaluator’s use only)*

|  |  |
| --- | --- |
| Comment of the Evaluator (if Any) | Evaluator’s Observation  Marks Secured: \_\_\_\_\_\_\_\_out of \_\_\_\_\_\_\_\_\_  Full Name of the Evaluator:  Signature of the Evaluator Date of Evaluation |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SUBJECT CODE: 19CS3041S**

**CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK**

# 3. Implementation of Social Engineering Using King Phisher

**Date of the Session: \_\_\_/\_\_\_/\_\_\_ Time of the Session: \_\_\_\_\_to\_\_\_\_\_\_**

## **Learning Outcomes:**

* To understand the concept of Phishing.
* To understand how to create Phishing websites.

**Pre-Skill Task:**

**1.** What are the dangers of Phishing attacks?

**2.** How can I identify a Phishing attack?

**3.** Briefly explain about different techniques of Phishing?

**4.** What are the psychological tricks that attackers employ so that people fall for the Phishing scheme?

**5.** How to avoid becoming a victim of a Phishing scam?

**In-Skill Task:**

**1**) Siddharth is a Computer Science Student and he is Naughty. He wants to fool his friend Siva by sending a Fake Mail by King Phisher tool. But he doesn’t know that how that tool Works.

a. He want to learn How the Tool (King Phisher ) Works .

So, Help Siddharth to understand how the Tool Work in a step by step process.

**Post-Skill Task :**

**1.** What is Ghost Phisher?

**2.** Name the dependencies that are required in the proper running of Ghost Phisher.

*(For Evaluator’s use only)*

|  |  |
| --- | --- |
| Comment of the Evaluator (if Any) | Evaluator’s Observation  Marks Secured: \_\_\_\_\_\_\_\_out of \_\_\_\_\_\_\_\_\_  Full Name of the Evaluator:  Signature of the Evaluator Date of Evaluation |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SUBJECT CODE: 19CS3041S**

**CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK**

# 4. Implementation of Social Engineering Using Maltego

**Date of the Session: \_\_\_/\_\_\_/\_\_\_ Time of the Session: \_\_\_\_\_to\_\_\_\_\_\_**

## **Learning Outcomes:**

* To understand vulnerabilities in social Engineering.
* To understand Maltego tool is used to explore the same.

**Pre-Skill Task:**

**1.** Help Shiny find the movie name that has ‘Dark’ in it’s name. Also find the cast those movies.

**2.** Surya tried very hard to get a job and applied for many companies but he didn’t get any job. One day he got an email offering a job “ reports@yahoo.com”, he wants to check whether the mail is an original one or a Spam so verify the mail whether it is real or fraud using “M**altego**” tool .

**In-Skill Task :**

**1.** Kavya heard about the sales in Myntra. She wants to find out the name servers of 'myntra.com'. She is also keen to know what other domains use these name servers. Help her in finding out the above mentioned using Maltego. Also help her get the email addresses these domains use and verify whether these mails exist or not.

*(For Evaluator’s use only)*

|  |  |
| --- | --- |
| Comment of the Evaluator (if Any) | Evaluator’s Observation  Marks Secured: \_\_\_\_\_\_\_\_out of \_\_\_\_\_\_\_\_\_  Full Name of the Evaluator:  Signature of the Evaluator Date of Evaluation |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SUBJECT CODE: 19CS3041S**

**CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK**

# 5. Implementation of Password Cracking Using John the Ripper

**Date of the Session: \_\_\_/\_\_\_/\_\_\_ Time of the Session: \_\_\_\_\_to\_\_\_\_\_\_**

## **Learning Outcomes:**

* To understand the concept of Data Sniffing through Wi-Fi.
* To understand the risks in Password cracking.

**Pre-Skill Task:**

**1.** Why the John the Ripper is easy for password cracking? Explain the modes of cracking in John the Ripper?

**2.** What are the advantages and disadvantages of John the Ripper?

**In-Skill Task:**

**1.** Two best friends started doing a project at last they made the project into a zip file with a password. Unfortunately by the presentation day they both forgot the password, so help them out by cracking the password using John the Ripper

*(For Evaluator’s use only)*

|  |  |
| --- | --- |
| Comment of the Evaluator (if Any) | Evaluator’s Observation  Marks Secured: \_\_\_\_\_\_\_\_out of \_\_\_\_\_\_\_\_\_  Full Name of the Evaluator:  Signature of the Evaluator Date of Evaluation |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SUBJECT CODE: 19CS3041S**

**CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK**

# 6. Implementation of Wi-Fi Hacking Using Reaver

**Date of the Session: \_\_\_/\_\_\_/\_\_\_ Time of the Session: \_\_\_\_\_to\_\_\_\_\_\_**

## **Learning Outcomes:**

* To understand the concept of Wi-Fi Hacking

**Pre-Skill Task:**

**1.**What is a Reaver attack?

**2.** What Reaver can do compared to other?

**3.** Is Reaver safe to use?

**In-Skill Task:**

1.Dheeraj is learning Reaver. As a beginner he wants to know the use of following commands in Reaver:-

i) Wash

ii) Reaver

2. Karun forgot his Wi-Fi password. He wants to know the password. Karun approached you for help. Help Karun by hacking the Wi-Fi using Reaver.

Write down the wireless interface names, monitor mode, ESSID, Channel, BSSID of the target and paste the screen shots of execution and the outputs.

Note:- Perform this experiment on your native Wi-fi, your home Wi-Fi preferably.

*(For Evaluator’s use only)*

|  |  |
| --- | --- |
| Comment of the Evaluator (if Any) | Evaluator’s Observation  Marks Secured: \_\_\_\_\_\_\_\_out of \_\_\_\_\_\_\_\_\_  Full Name of the Evaluator:  Signature of the Evaluator Date of Evaluation |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SUBJECT CODE: 19CS3041S**

**CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK**

# 7. Implementation of NMAP Scanning Technique

**Date of the Session: \_\_\_/\_\_\_/\_\_\_ Time of the Session: \_\_\_\_\_to\_\_\_\_\_\_**

## **Learning Outcomes:**

* To understand the concept Nmap Scanning Technique.
* To understand the need of Network Scanning.

**Pre-Skill Task:**

**1. Write a Nmap command to scan targets from a file.**

**2. Write a command to print a summary while sending and receiving every packet.**

**3.** **Write Nmap query for OS detection.**

**In-Skill Task :**

1. Vicky came to know that NMAP (Network Mapper) is a very versatile tool for Linux system/network administrators and is used for **exploring networks, perform security scans, network audit**and**finding open ports** on remote machine, Live hosts and Operating systems. So, he decided to work on the tool. Help him in performing the following scans:

a. Ping sweep

b. Port scan

c. TCP full open scan

d. TCP SYN scan

e. UDP scan

f. Version detection scan

g. OS detection scan and

h. Aggressive scan.

**Post-Skill Task :**

**1.** Billy is trying to understand how “–v” option is used in NMAP scanning technique. Explain him the use of the option “-v” by working on it.

*(For Evaluator’s use only)*

|  |  |
| --- | --- |
| Comment of the Evaluator (if Any) | Evaluator’s Observation  Marks Secured: \_\_\_\_\_\_\_\_out of \_\_\_\_\_\_\_\_\_  Full Name of the Evaluator:  Signature of the Evaluator Date of Evaluation |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SUBJECT CODE: 19CS3041S**

**CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK**

# 8. Implementation of Vulnerability Analysis Using Wireshark

**Date of the Session: \_\_\_/\_\_\_/\_\_\_ Time of the Session: \_\_\_\_\_to\_\_\_\_\_\_**

**Learning Outcomes:**

* To understand the Wireshark tool.
* To analyse the packets when we capture network traffic using Wireshark tool.

**Prerequisite: Wireshark Software  
Download:** [**https://www.wireshark.org/download.html**](https://www.wireshark.org/download.html) **Reference:** [**https://www.wireshark.org/docs/**](https://www.wireshark.org/docs/) **User Guide:** [**https://www.wireshark.org/docs/wsug\_html/**](https://www.wireshark.org/docs/wsug_html/)

**Pre–Skill Task:**

1. What is the main purpose of Wireshark tool?
2. How can we utilize the Wireshark tool and for what?
3. Describe about the each and every column in the top pane in Wireshark tool.

**In–Skill Task:**

1. How we can capture the data packets using the Wireshark tool? Mention the step by step process.
2. Analyze any packets that you capture and write down their information i.e., their source, destination along with its IP Address and to which protocol they belong to?

*(For Evaluator’s use only)*

|  |  |
| --- | --- |
| Comment of the Evaluator (if Any) | Evaluator’s Observation  Marks Secured: \_\_\_\_\_\_\_\_out of \_\_\_\_\_\_\_\_\_  Full Name of the Evaluator:  Signature of the Evaluator Date of Evaluation |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SUBJECT CODE: 19CS3041S**

**CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK**

# 9. Implementation of Man in the Middle Attack (Ettercap Tool)

**Date of the Session: \_\_\_/\_\_\_/\_\_\_ Time of the Session: \_\_\_\_\_to\_\_\_\_\_\_**

## **Learning Outcomes:**

* To understand MITM attack.
* To understand Kali Linux is used to explore the concept.

**Pre-Class:**

**1.** What is EtterCap?

**2.** List out user Interfaces provided by the EtterCap?

**3.** Write an example for Man in the Middle attack.

**4.** List the goals of ARP Spoofing.

**In-Skill Task:**

**1.** Monica and Jessica are exploring possible man in the middle attacks in cyber security in that process they learnt about ARP poisoning/spoofing. To demonstrate this they wanted to work with Ettercap, what could be the process or steps involved in this experiment, Demonstrate.

**Post-Skill Task:**

1.Explain the four modules in the Ettercap?

2. Is Ettercap a sniffing tool?

*(For Evaluator’s use only)*

|  |  |
| --- | --- |
| Comment of the Evaluator (if Any) | Evaluator’s Observation  Marks Secured: \_\_\_\_\_\_\_\_out of \_\_\_\_\_\_\_\_\_  Full Name of the Evaluator:  Signature of the Evaluator Date of Evaluation |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SUBJECT CODE: 19CS3041S**

**CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK**

# 10. Implementation of Mobile Security Using APK Tool.

**Date of the Session: \_\_\_/\_\_\_/\_\_\_ Time of the Session: \_\_\_\_\_to\_\_\_\_\_\_**

## **Learning Outcomes:**

* To understand the importance of Mobile security.
* To understand APK tool is used for mobile security.

**Pre-Skill Task:**

1. What are the needs of mobile security using APK tool?
2. What are the mobile apps testing tools?

3. How mobile security framework works?

**In-Skill Task:**

**1)** MOBILE SECURITY USING APK TOOL. Explore the following steps.

Task1: Installing process of APK tool?

Task2: Working of APK tool

Task 3: What is the conclusion of Working of APK tool?

*(For Evaluator’s use only)*

|  |  |
| --- | --- |
| Comment of the Evaluator (if Any) | Evaluator’s Observation  Marks Secured: \_\_\_\_\_\_\_\_out of \_\_\_\_\_\_\_\_\_  Full Name of the Evaluator:  Signature of the Evaluator Date of Evaluation |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SUBJECT CODE: 19CS3041S**

**CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK**

# 11. Implementation of Web Application Security Using Burp Suite.

**Date of the Session: \_\_\_/\_\_\_/\_\_\_ Time of the Session: \_\_\_\_\_to\_\_\_\_\_\_**

## **Learning Outcomes:**

* To understand the importance of Web Application Security.
* To understand how Burp suite is used for Web Security

**Pre-Skill Task:**

1. Sai wants to implement web application security using burp suite, help him with the required tools?
2. Install and configure burp suite and list out the features of Burp Suite?

**In-Skill Task:**

1. Find out all the requests sent to server when we access a particular URL(any URL)? And list those requests here.

2. Open the given URL, change the details entered by the user in that page (first name,

last name, user name) using parameter pampering.

*(For Evaluator’s use only)*

|  |  |
| --- | --- |
| Comment of the Evaluator (if Any) | Evaluator’s Observation  Marks Secured: \_\_\_\_\_\_\_\_out of \_\_\_\_\_\_\_\_\_  Full Name of the Evaluator:  Signature of the Evaluator Date of Evaluation |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SUBJECT CODE: 19CS3041S**

**CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK**

# 12. Implementation of Web Application Security (Paros)

**Date of the Session: \_\_\_/\_\_\_/\_\_\_ Time of the Session: \_\_\_\_\_to\_\_\_\_\_\_**

## **Learning Outcomes:**

* To understand the importance of Web Application Security.
* To understand how Paros is used for Web Security

**Pre-Skill Task:**

1.Paros is not only used by security experts for penetration testing for web applications but also by web developers, what are the features that Paros have that also help web developers?

2. As an aspiring security administrator, you might want to manually review the data to assess your Web site and identify security vulnerabilities. What are the few advanced features that Paros gives you?

3. Ram says that “ Just like other web application security tools paros can be used to find out the SQl- injection and XSS(Cross site Scripting ) vulnerability on a web application” Justify your statement?

**In-Skill Task:**

1. Why is it important for penetration testing tools on web applications. and how do you use Paros to validate vulnerabilities reports?

2. Write steps to implement Paros in your Kali Linux?

*(For Evaluator’s use only)*

|  |  |
| --- | --- |
| Comment of the Evaluator (if Any) | Evaluator’s Observation  Marks Secured: \_\_\_\_\_\_\_\_out of \_\_\_\_\_\_\_\_\_  Full Name of the Evaluator:  Signature of the Evaluator Date of Evaluation |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SUBJECT CODE: 19CS3041S**

**CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK**

# 13. Implementation of SQL Injection Using SQLMap

**Date of the Session: \_\_\_/\_\_\_/\_\_\_ Time of the Session: \_\_\_\_\_to\_\_\_\_\_\_**

## **Learning Outcomes:**

* To understand the concept SQL INJECTION using SQLmap.

**Pre-Skill Task:**

**1.** Satish is new to hacking field and he want to know about SQL injection and types of SQL injections. Briefly explain about SQL injection and its types.

**2.** Ramu has developed a web application on his own to sell products through online. He added all available products in his shop to database and day by day the online shopping is increasing and also the number of customers. Recently he heard that the data belongs to the customers of the shop which is behind his shop was leaked by some hackers. And he came to know that hackers use SQL injection to retrieve the data from the database. So, he also wants to check weather attackers able to use SQL injection to retrieve data from his website. Help him by explaining some methods to detect SQL Injection Vulnerabilities.

**In-Class Task:**

**1.** Given below is a testing and demo website for sqlmap practice.

<http://testphp.vulweb.com/listproducts.php?cat=1>

1. Find out the backend DBMS used in the mentioned website. Also list the databases present in it.
2. Now pick any database from the output and list the tables in it.
3. Search for the user name and passwords from those tables and try to login.

2. SUBTASK OF PREVIOUS WEBSITE:

1. Dump the artist names available in the database you found out.
2. In the previous question the vulnerable website was already given to you, instead, list one of the various ways through which we can identify vulnerable websites to access their databases and information.

*(For Evaluator’s use only)*

|  |  |
| --- | --- |
| Comment of the Evaluator (if Any) | Evaluator’s Observation  Marks Secured: \_\_\_\_\_\_\_\_out of \_\_\_\_\_\_\_\_\_  Full Name of the Evaluator:  Signature of the Evaluator Date of Evaluation |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SUBJECT CODE: 19CS3041S**

**CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK**

# 14. Implementation of Cross Site Scripting Attack.

**Date of the Session: \_\_\_/\_\_\_/\_\_\_ Time of the Session: \_\_\_\_\_to\_\_\_\_\_\_**

## **Learning Outcomes:**

* To understand about cross site scripting(xss).
* To apply cross site scripting(xss) for checking web application security.

**Pre-Skill Task:**

**1.** What is Cross Site Scripting?

**2.** List various types in Cross Site Scripting.

**3.** List out some websites which are enabled for Cross Site Scripting.

**In-Skill Task:**

**1.** Implement Cross Site Scripting for the following tasks in the given link below. And write the steps you have used for applying XSS:

Link : <http://www.xss-game.appspot.com/>

**Task 1:**

**Mission Description**

This level demonstrates a common cause of cross-site scripting where user input is directly included in the page without proper escaping.  
Interact with the vulnerable application window below and find a way to make it execute JavaScript of your choosing. You can take actions inside the vulnerable window or directly edit its URL bar.

**Mission Objective**

Inject a script to pop up a JavaScript **alert()** in the frame below.  
Link: <http://www.xss-game.appspot.com/level1>

**Task 2:**

Mission Description

Web applications often keep user data in server-side and, increasingly, client-side databases and later display it to users. No matter where such user-controlled data comes from, it should be handled carefully.  
  
This level shows how easily XSS bugs can be introduced in complex apps.

Mission Objective

Inject a script to pop up an **alert()** in the context of the application.  
  
**Note**: the application saves your posts so if you sneak in code to execute the alert, this level will be solved every time you reload it.

Link : <http://www.xss-game.appspot.com/level2>

*(For Evaluator’s use only)*

|  |  |
| --- | --- |
| Comment of the Evaluator (if Any) | Evaluator’s Observation  Marks Secured: \_\_\_\_\_\_\_\_out of \_\_\_\_\_\_\_\_\_  Full Name of the Evaluator:  Signature of the Evaluator Date of Evaluation |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SUBJECT CODE: 19CS3041S**

**CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK**

# 15. Implementation of Windows Exploit using Metasploit

**Date of the Session: \_\_\_/\_\_\_/\_\_\_ Time of the Session: \_\_\_\_\_to\_\_\_\_\_\_**

## **Learning Outcomes:**

* To understand Metasploit Framework
* How to setup payload for exploiting
* To understand Post exploitation techniques

**Pre-Skill Task:**

**1.** What are different types of modules does metasploit contains?

**2.** What are the different interfaces of metasploit?

**3.** Draw the architecture of Metasploit.

**In-Skill Task:**

**1.** Being a cyber security aspirant you want to join in KL University in cyber security and block chain specialization in order to confirm your seat you should clear basic entrance exam conducted by the University. Your problem statement is to exploit windows xp. All the best Happy Hacking!!

(Hint: You can use smb vulnerability)

*(For Evaluator’s use only)*

|  |  |
| --- | --- |
| Comment of the Evaluator (if Any) | Evaluator’s Observation  Marks Secured: \_\_\_\_\_\_\_\_out of \_\_\_\_\_\_\_\_\_  Full Name of the Evaluator:  Signature of the Evaluator Date of Evaluation |