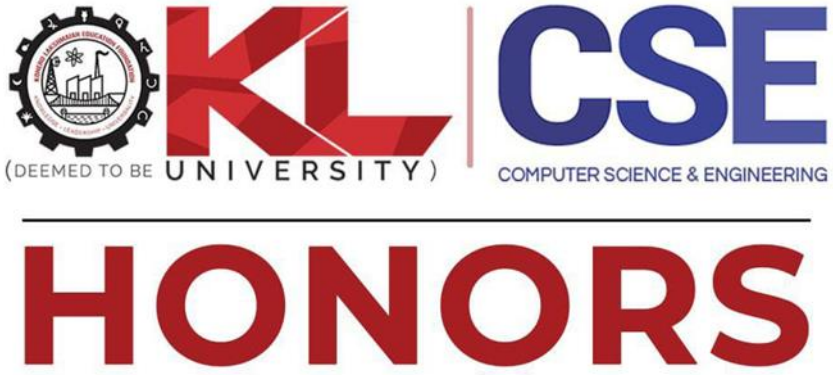
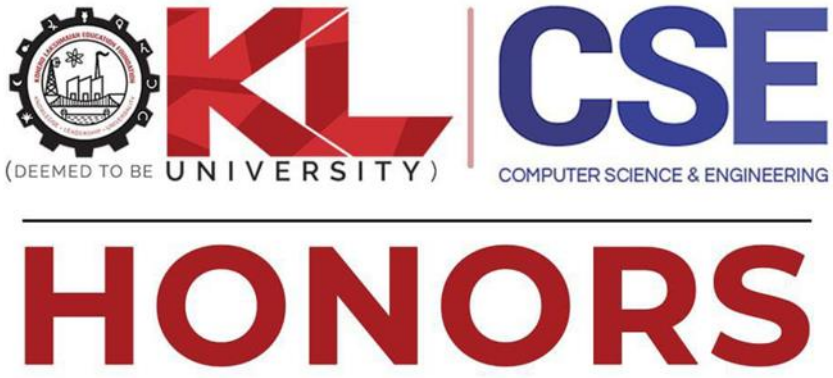


20CS3041AA – CRYPT ANALYSIS AND CYBER DEFENCE

SKILL WORKBOOK

TEAM CRYPT ANALYSIS AND CYBER DEFENCE

KONERU LAKSHMAIAH EDUCATION FOUNDATION |
20CS3041AA – CRYPT ANALYSIS AND CYBER DEFENCE



SKILLING WORKBOOK

STUDENT NAME	RAMU SINGAMSETTY
REG. NO	
YEAR	3
SEMESTER	1
SECTION	
FACULTY NAME	

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, eachlaboratory includes three parts: Pre-skill, In-skill, and post-skill.

a. 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).

b. 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 Pre-skill exercises. The intent is to give constructive feedback so that students leave the lab with working Pre-skill 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.

c. 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 (50M)	Faculty Signature
			EXECUTION (10M)	RESULT (10M)	ANALYSIS (20M)			
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								

S. No	Date	Experiment Name	SKILLING EVALUATION			Viva Voce (10M)	Total (50M)	Faculty Signature
			EXECUTION (10M)	RESULT (10M)	ANALYSIS (20M)			
11								
12								
13								
14								
15								

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SUBJECT CODE: 20CS3041AA
CRYPTANALYSIS 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?

It is the process of intalling a virtual operating system on the existing host operating system using virtualization techniques and suitable softwares

2. Explain what is hypervisor?

Hypervisor is a software that installs and runs the virtual machines and supports the virtualisation of the guest operating system.

3. Explain the Types of hypervisors?

There are mainly two types of hypervisors namely Bare metal and hosted.

Bare metal: The type of hyoervisor which makes the guest os to run on the physical components of the system i.e it also runs the software on the physical configuration of the system.

Hosted Hypervisor: Unlike the bare metal type this hypervisor runs the virtual machine as a computer program rather than running parlelly on the physical configuration of the system.

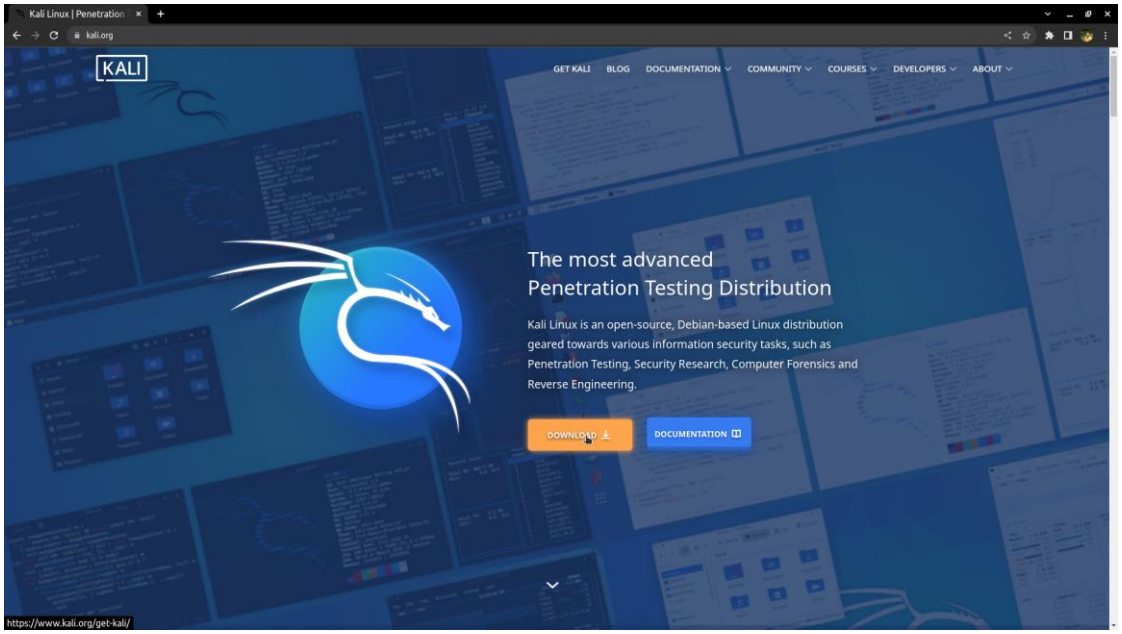
In-Skill Task:

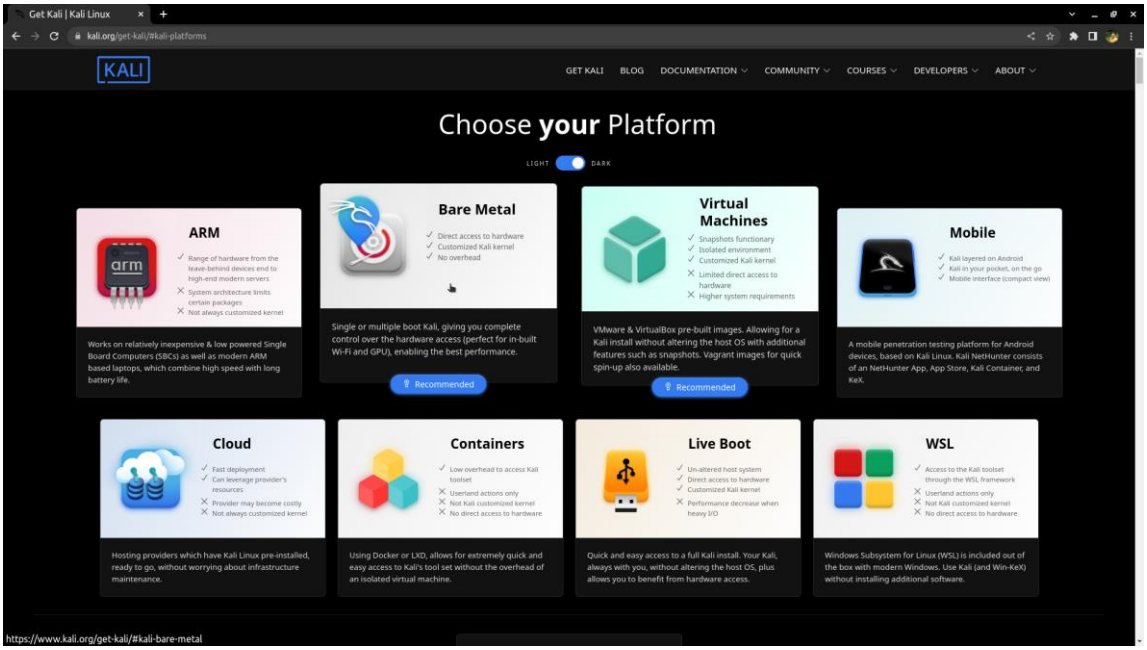
Harsha a technology evangelist has just started learning about OS virtualization and interested in learning ethical hacking as Harsha a newbie in this you was requested by Harsha to help him to install Kali Linux in his computer using Virtual Box

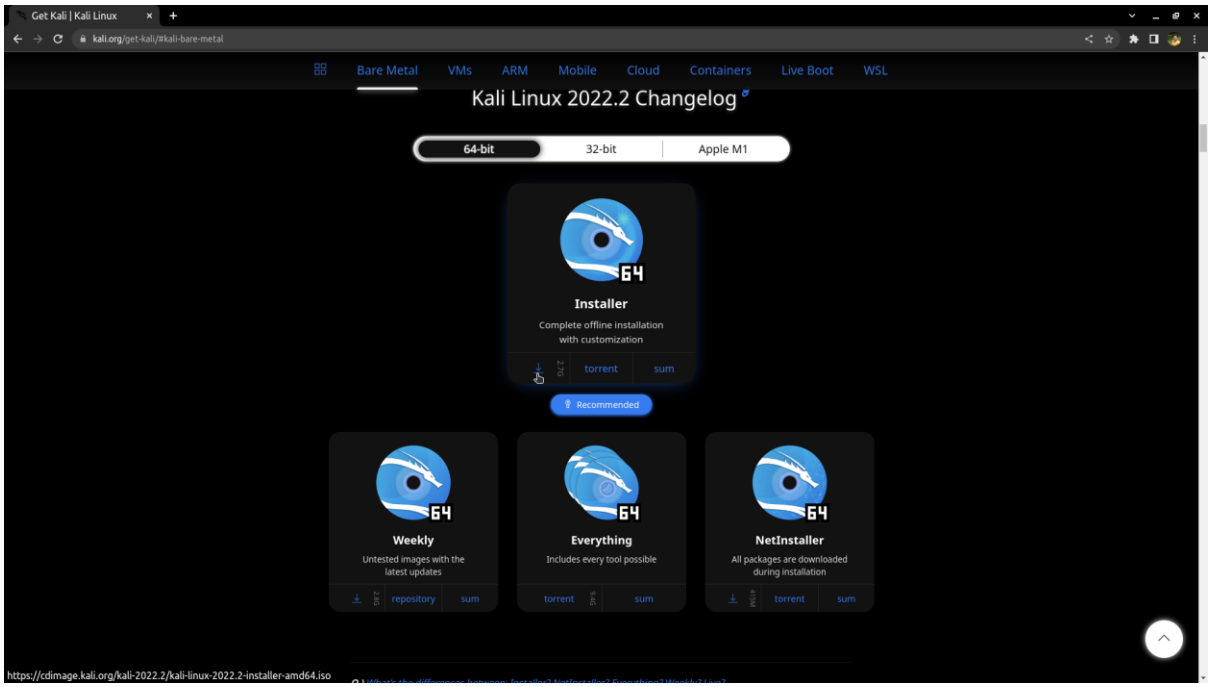
Writing space for the Problem:(For Student's use only)

Solution:

Download the virtual image from the official kali website and select bare metal. Kali.org



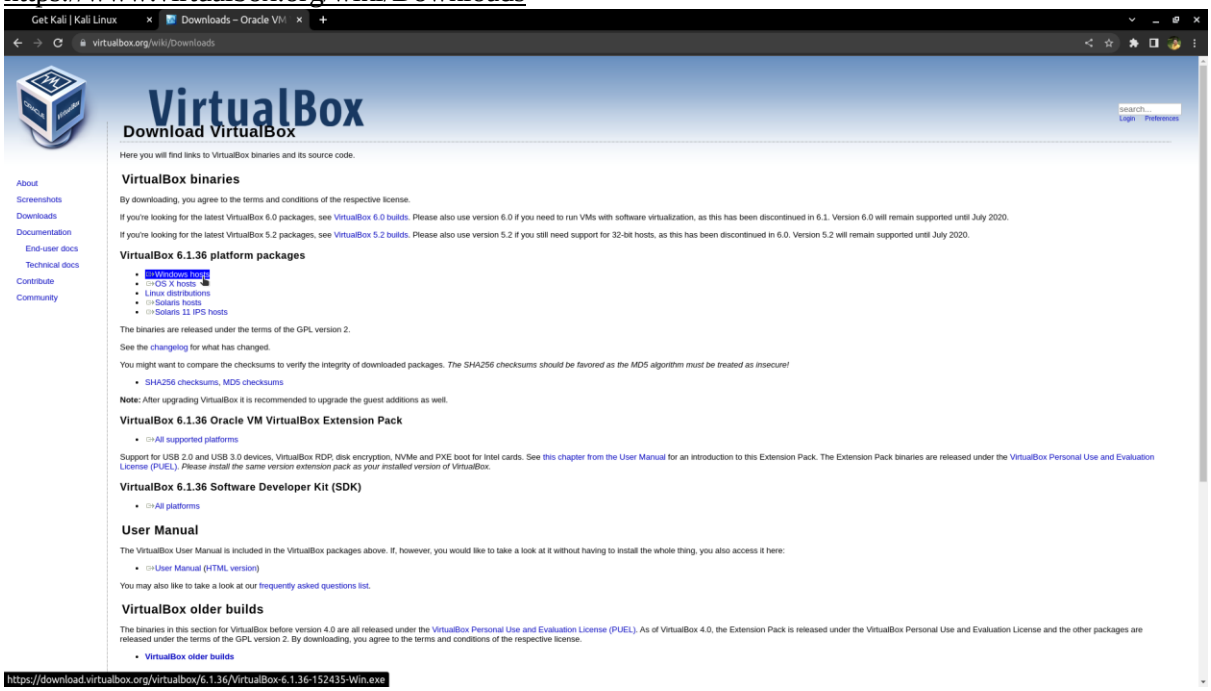

Get Kali | Kali Linux
kali.org/get-kali/#kali-platforms
KALI
GET KALI
BLOG
DOCUMENTATION
COMMUNITY
COURSES
DEVELOPERS
ABOUT
Choose your Platform
LIGHT
DARK
ARM
Range of hardware from the leave-behind devices end to high-end modern servers
System architecture limits certain packages
Not always customized kernel
Works on relatively inexpensive & low powered Single Board Computers (SBCs) as well as modern ARM based laptops, which combine high speed with long battery life.
Bare Metal
Direct access to hardware
Customized Kali kernel
No overhead
Single or multiple boot Kali, giving you complete control over the hardware access (perfect for in-built Wi-Fi and GPU), enabling the best performance.
Recommended
Virtual Machines
Snapshots functionary
Isolated environment
Customized Kali kernel
Limited direct access to hardware
Higher system requirements
VMware & VirtualBox pre-built images. Allowing for a Kali install without altering the host OS with additional features such as snapshots. Vagrant images for quick spin-up also available.
Recommended
Mobile
Kali layered on Android
Kali in your pocket, on the go
Mobile interface (compact view)
A mobile penetration testing platform for Android devices, based on Kali Linux. Kali NetHunter consists of an NetHunter App, App Store, Kali Container, and KeX.
Cloud
Fast deployment
Can leverage provider's resources
Provider may become costly
Not always customized kernel
Hosting providers which have Kali Linux pre-installed, ready to go, without worrying about infrastructure maintenance.
Containers
Low overhead to access Kali toolset
Userland actions only
Not Kali customized kernel
No direct access to hardware
Using Docker or LXD, allows for extremely quick and easy access to Kali's tool set without the overhead of an isolated virtual machine.
Live Boot
Un-altered host system
Direct access to hardware
Customized Kali kernel
Performance decrease when heavy I/O
Quick and easy access to a full Kali install. Your Kali, always with you, without altering the host OS, plus allows you to benefit from hardware access.
WSL
Access to the Kali toolset through the WSL framework
Userland actions only
Not Kali customized kernel
No direct access to hardware
Windows Subsystem for Linux (WSL) is included out of the box with modern Windows. Use Kali (and Win-KeX) without installing additional software.
https://www.kali.org/get-kali/#kali-bare-metal



https://www.kali.org/get-kali/#kali-bare-metal

Now let us install the virtual box

https://www.virtualbox.org/wiki/Downloads



Install the virtualbox as with the same installation steps as any other software.

Post-Skill Task:

1. Why Kali Linux is newbie friendly for cyber Security enthusiast?
   Because it has all the components that a newbie needs like, friendly ui and easy to use

2. What are different types of Linux Distro's available?
   We have other os like Ubuntu, Feroda, Arch Linux, Parrot os, mint, Solarix, etc.

3. List some security focused Linux Distro's available.
   We have other security focused linux distro's like Parrot os, Black Arch Linux, Backbox linux etc.

(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: 20CS3041AA
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?

Airodump-ng is a penetration testing tool which captures raw data packets which might be useful for further analysis.

2.What is capture handshake?

Handshake is a process of establishing connection between two systems or between a system and a router. Capturing handshake means getting the handshake file which consists of the various keys in order to connect to the access point.

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

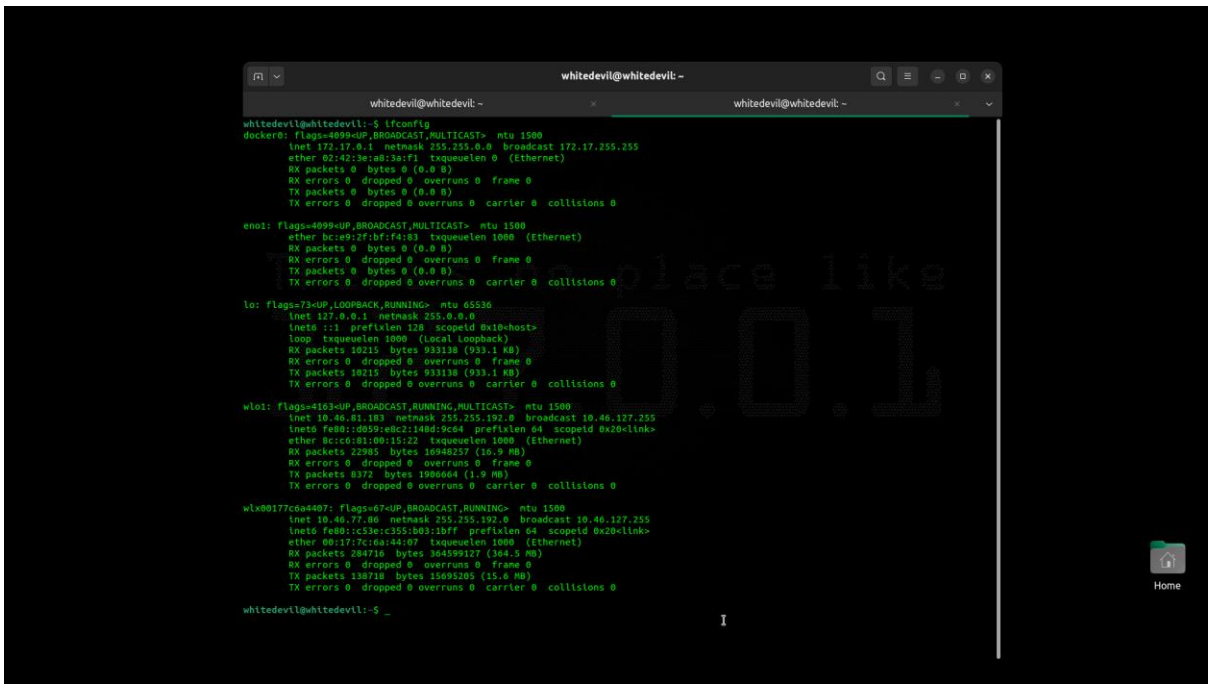
Help him by doing those operations Successfully(If Possible include screenshots of those outputs)

Solution:

1. Monitor mode using wifi-adapter

For this we need to use ifconfig and we need to know the device/ interface name.

Go to terminal and hit ifconfig and enter it shows the list of interfaces and its status.



in my case the adapter's name is "wlx00177c6a4407"

For putting the device into monitor mode, we need to execute the following command

ifconfig wlx00177c6a4407 down && iwconfig wlx00177c6a4407 mode monitor && ifconfig wlx00177c6a4407 up

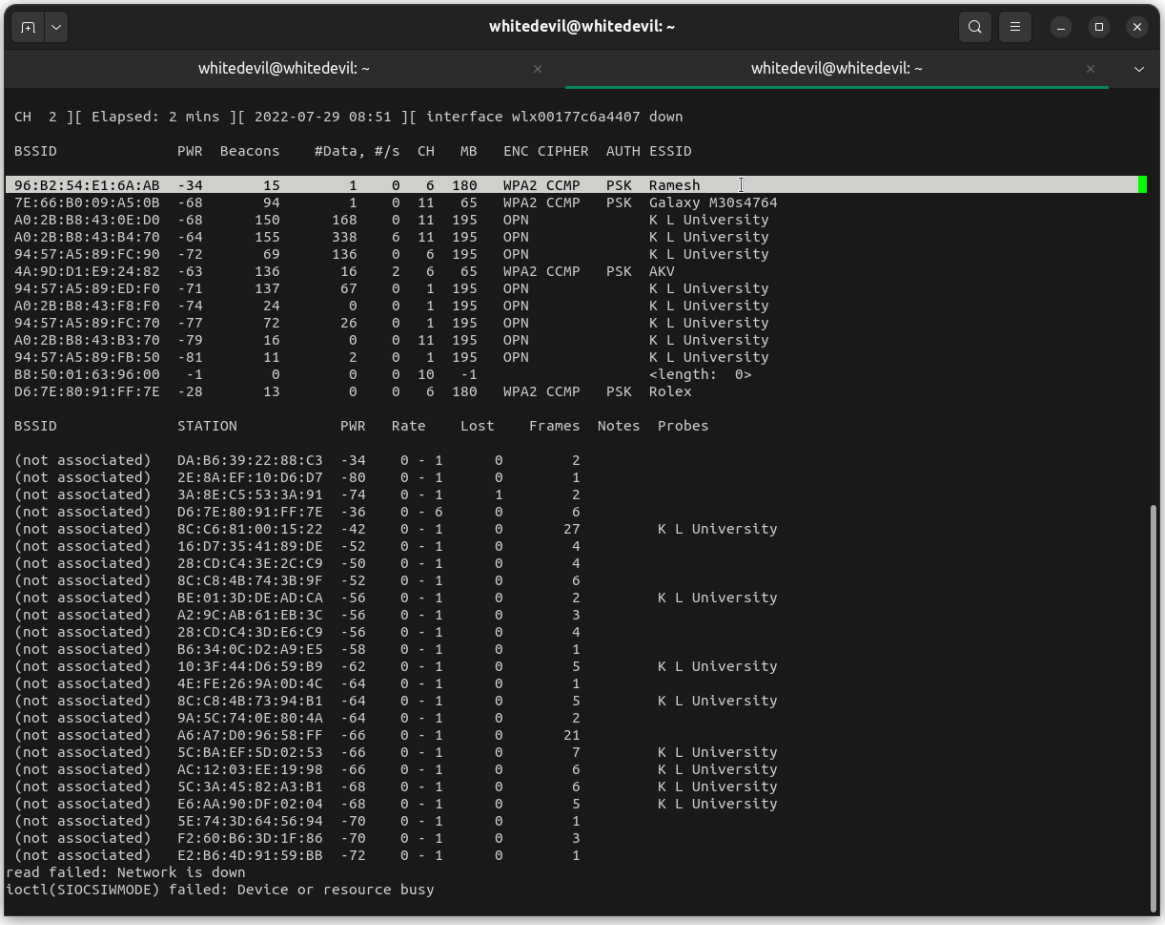
2.

For capturing packets we need the following details: bssid, channel and interface name

for knowing the bssid:

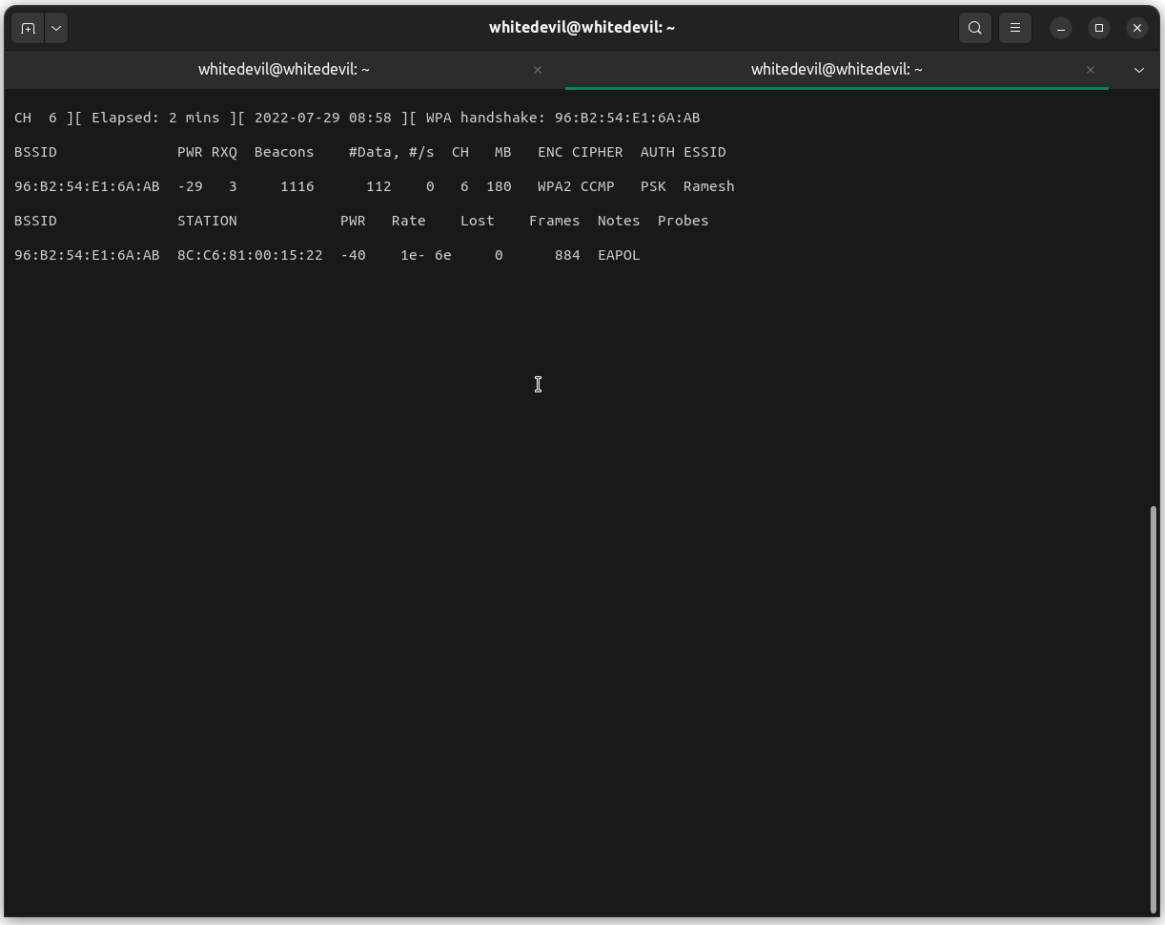
Command: airodump-ng --interface interfacename

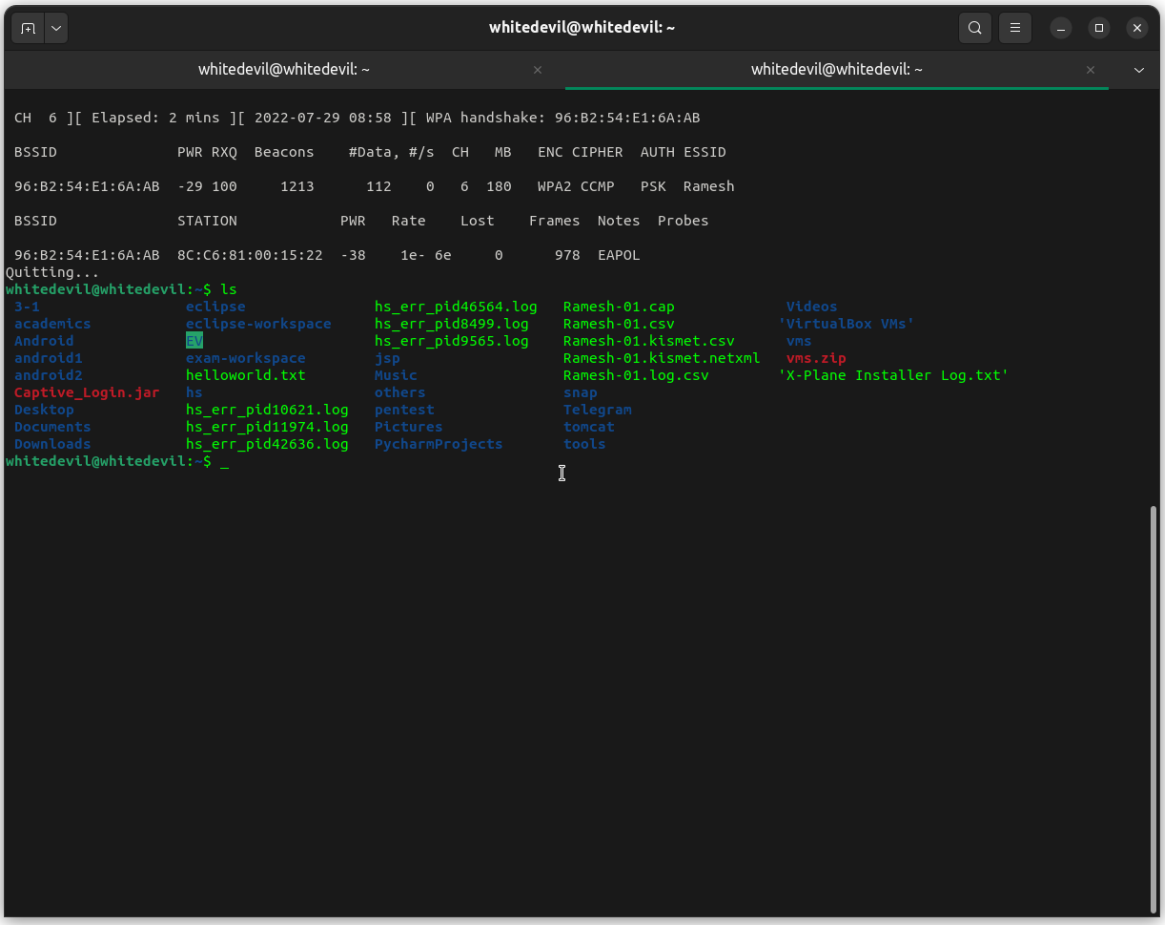
example: airodump-ng --interface wlx00177c6a4407



So we got our bssid, channel, interface name, now we can start capturing packets.

Command: airodump-ng --bssid 96:B2:54:E1:6A:AB --channel 6 wlx00177c6a4407 --write Ramesh


whitedevil@whitedevil: ~
whitedevil@whitedevil: ~
whitedevil@whitedevil: ~
CH 6][Elapsed: 2 mins][2022-07-29 08:58][WPA handshake: 96:B2:54:E1:6A:AB
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
96:B2:54:E1:6A:AB -29 3 1116 112 0 6 180 WPA2 CCMP PSK Ramesh
BSSID STATION PWR Rate Lost Frames Notes Probes
96:B2:54:E1:6A:AB 8C:C6:81:00:15:22 -40 1e- 6e 0 884 EAPOL



We can observe the files of Ramesh which are out captured files with various information.

3.

(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: 20CS3041AA
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: 20CS3041AA
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.

1. Go to transforms and click on transform hub search for tmdb

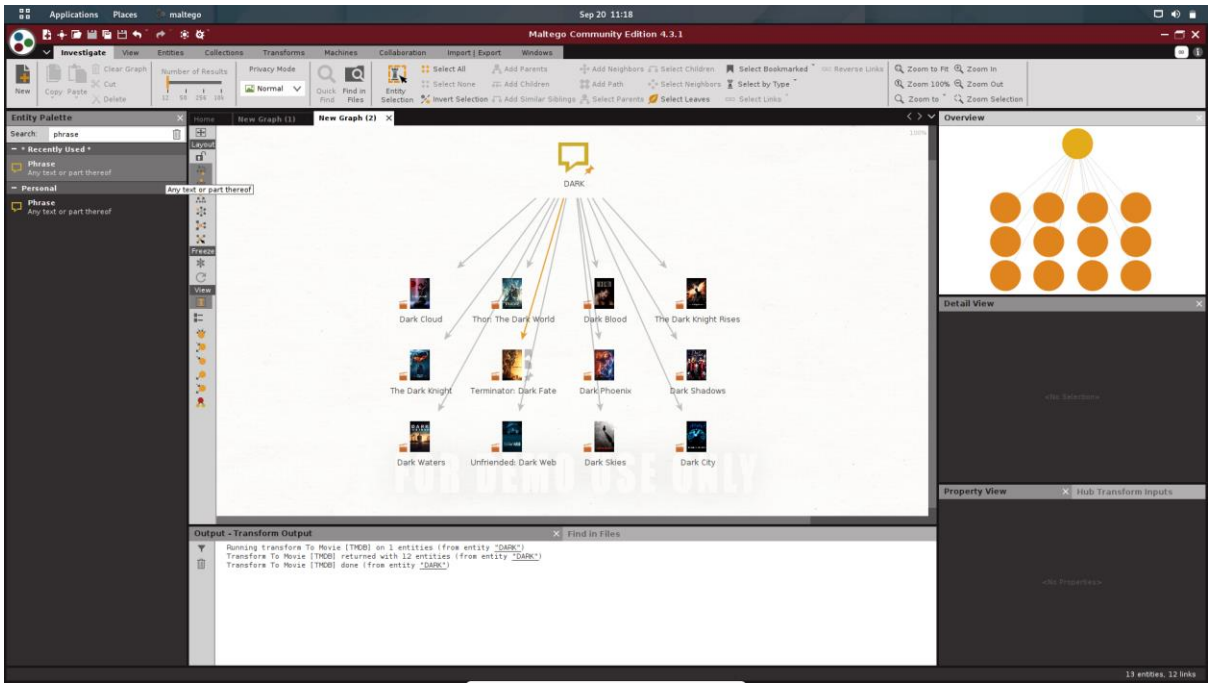
2. install the transform

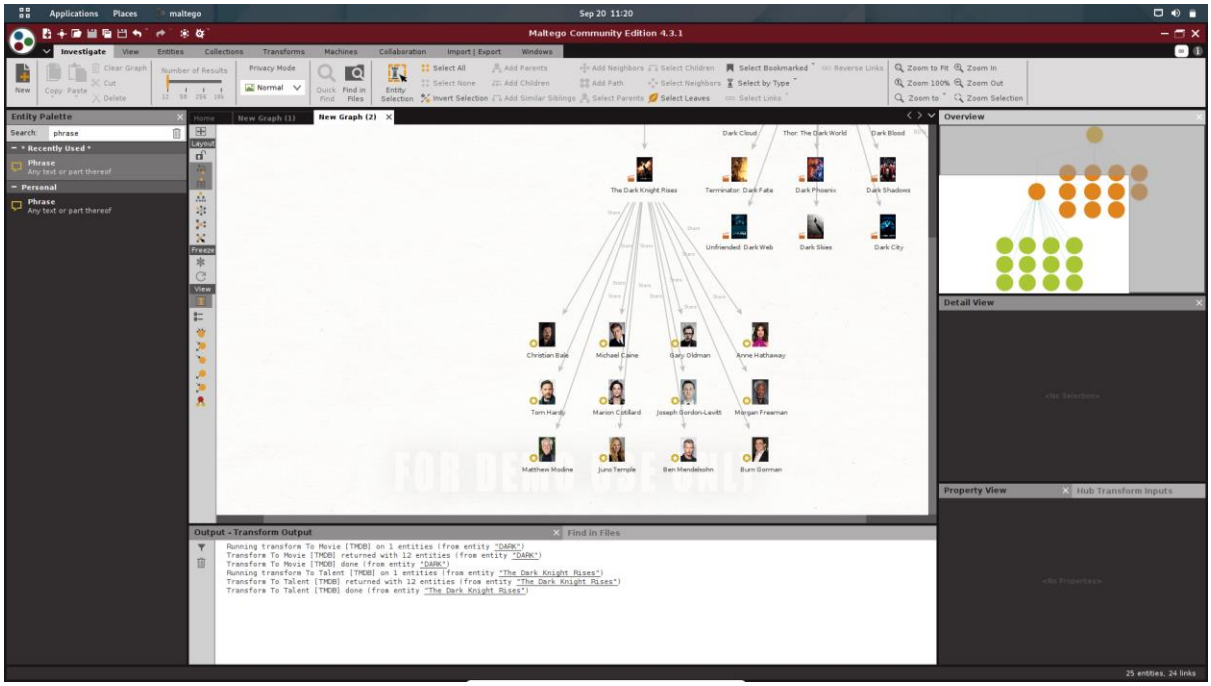
3. go to investigate and select phrase

4. drag and drop and change name to DARK

5. right click and search tmdb transform and click on that

6. select some movie and right click and select to talent for getting the cast of the movie




Applications
Places
maltego
Sep 20 11:20
Maltego Community Edition 4.3.1
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Entity Palette
Search:
phrase
* Recently Used *
Phrase
Any text or part thereof
Personal
Phrase
Any text or part thereof
Home
New Graph (1)
New Graph (2)
Layout
Freeze
View
Dark Cloud
Thor: The Dark World
Dark Blood
The Dark Knight Rises
Terminator: Dark Fate
Dark Phoenix
Dark Shadows
Unfriended: Dark Web
Dark Skies
Dark City
Christian Bale
Michael Caine
Gary Oldman
Anne Hathaway
Tom Hardy
Marion Cotillard
Joseph Gordon-Levitt
Morgan Freeman
Matthew Modine
Juno Temple
Ben Mendelsohn
Burn Gorman
Overview
Detail View
Property View
Hub Transform Inputs
Output - Transform Output
Find in Files
Running transform To Movie [TMDB] on 1 entities (from entity "DARK")
Transform To Movie [TMDB] returned with 12 entities (from entity "DARK")
Transform To Movie [TMDB] done (from entity "DARK")
Running transform To Talent [TMDB] on 1 entities (from entity "The Dark Knight Rises")
Transform To Talent [TMDB] returned with 12 entities (from entity "The Dark Knight Rises")
Transform To Talent [TMDB] done (from entity "The Dark Knight Rises")
25 entities, 24 links

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 .

1. open new case
2. select email in entity
3. change the name
4. right click on the entity
5. search for email transform
6. select verify and fraud check mail address

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.

Open new case

Select domain entity

Change the domain name to mynthra

Right click and select to domains

(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: 20CS3041AA
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

Create a zip file with a password

Once the password is set and zip is put it into the kali machine

Open terminal

Commands:

Zip2john example.zip > hash.txt

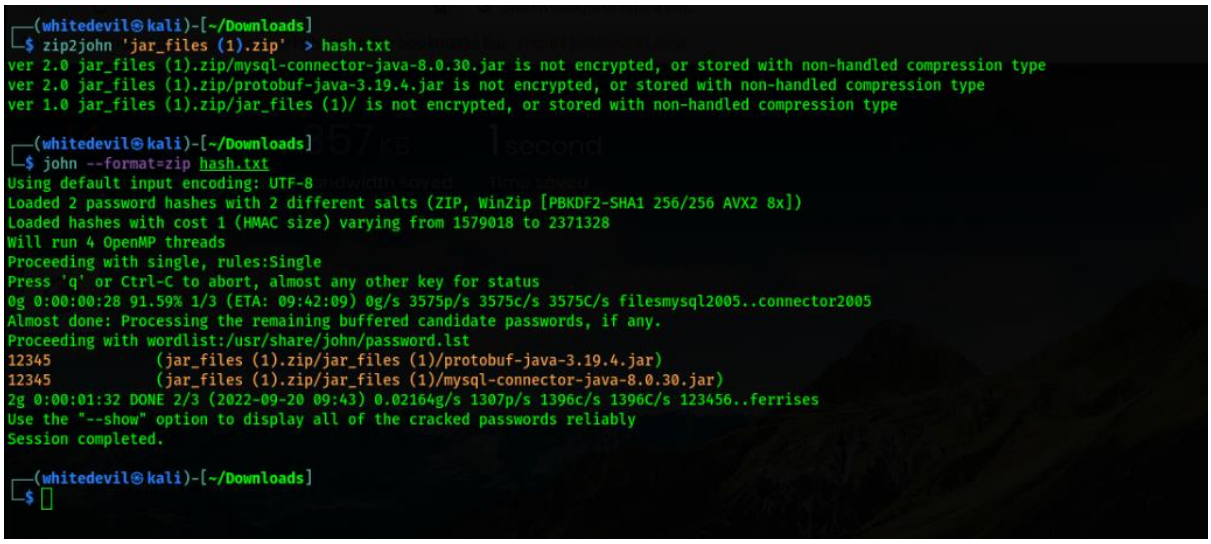
/*This command creates the hash of the password and obtains the salts of the same*/

John --format=zip hash.txt

/*This checks for the hash and makes brute force using the rockyou.txt wordlist*/

** put an easy password to the zip not a complex one

** better put a password from the rockyou.txt file



(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: 20CS3041AA
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?

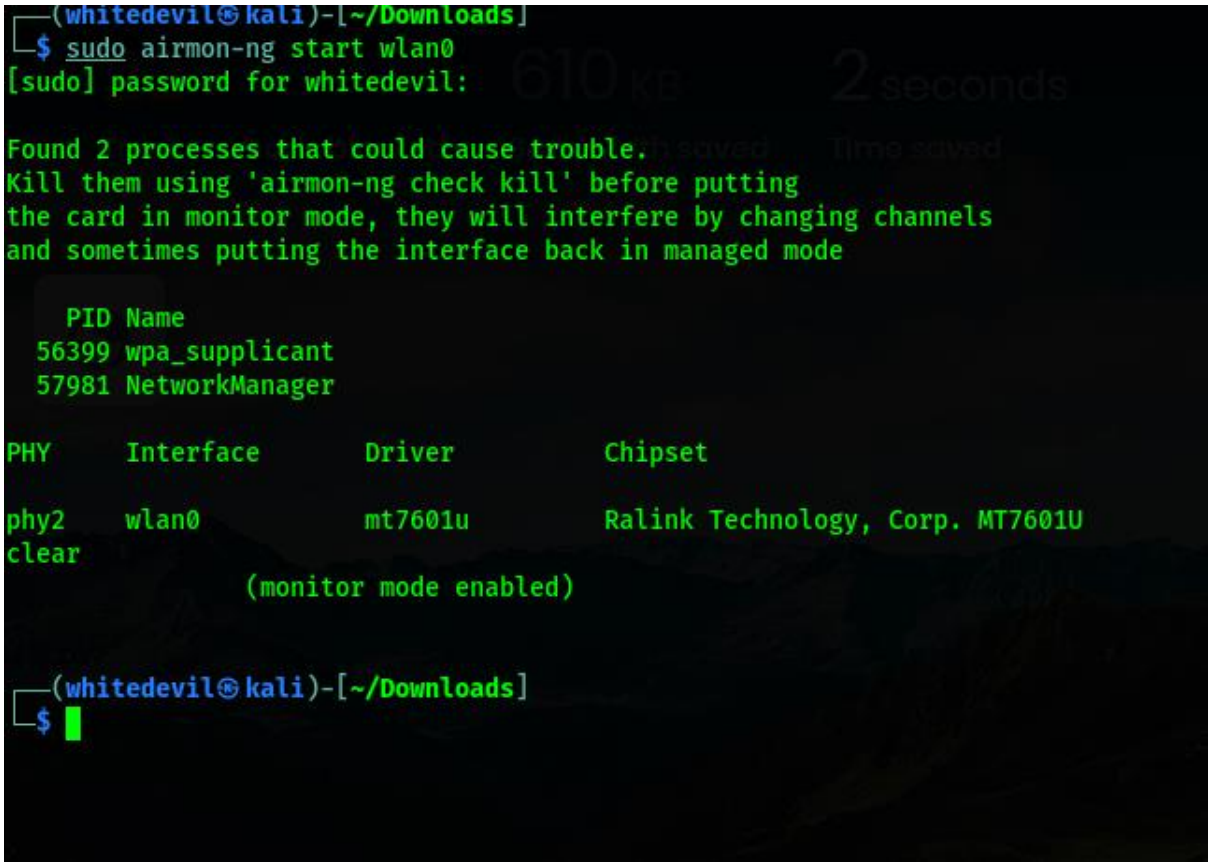
3. Is Reaver safe to use?

In-Skill Task:

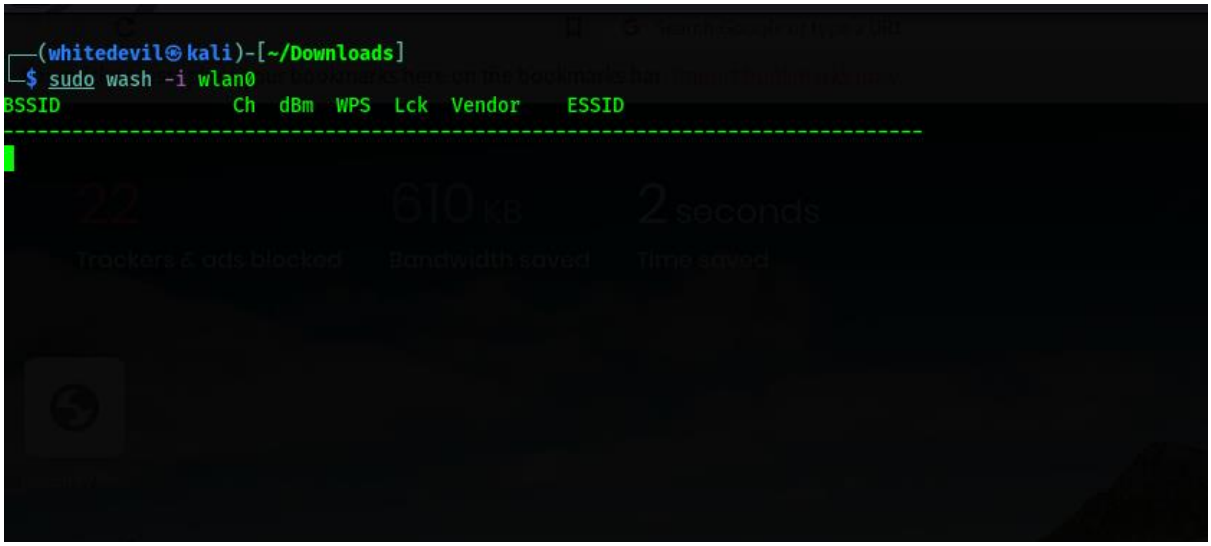
1.Dheeraj is learning Reaver. As a beginner he wants to know the use of following commands in Reaver:-

i) Wash
ii) Reaver

** “airmon-ng start wlan0” this command puts the wireless interface into monitor mode



Then we need to monitor the networks:
“Sudo wash -I wlan0” this displays the available networks in a detailed way



“reaver -i wlan0 -c 6 -b 00:45:7f:82:03 -vv”

This command starts to test the wps pin connection in Wi-Fi and tries to connect to the Wi-Fi for that we need to give some input such as:

-c the channel of the wifi which will be shown during wash

-b is the bssid of the network which is also displayed in the wash

-vv stands for verbrose mode which works gret while testing a difficult network

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.

Same as 1st qn

(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: 20CS3041AA
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**,** performing security scans**,** netwoauditsdit and finding open ports on a remotmachinesne, Live hosts and Operating systems. So, he decided to work on the tool. Help him in performing the following scans:

a. Ping sweep nmap -sP ipaddr range

b. Port scan namp ipaddr

c. TCP full open scan: nmap -sT ipaddr

d. TCP SYN scan : nmap -sS ipaddr

e. UDP scan : nmap -sU ipaddr

f. Version detection scan : sudo nmap -sV ipaddr

g. OS detection scan and : sudo nmap -O ipaddr

h. Aggressive scan.: Namp –A ipaddr

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: 20CS3041AA
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
Reference: https://www.wireshark.org/docs/
User Guide: 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.

    1. Open terminal
    2. Sudo wireshark
    3. Wireshark gui is shown up
    4. Select the interface
    5. Select start in top left corner
    6. It starts to capture the packets

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?

Do the same as 1st and just write down them

(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: 20CS3041AA
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: 20CS3041AA
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: 20CS3041AA
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: 20CS3041AA
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: 20CS3041AA
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

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

2. SUBTASK OF PREVIOUS WEBSITE:

a) Dump the artist names available in the database you found out.

b) 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: 20CS3041AA
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: 20CS3041AA
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