**ASSIGNMENT 9**

**CRYPTOGRAPHY, HONEYPOTS, FAKE ACCESS POINTS**

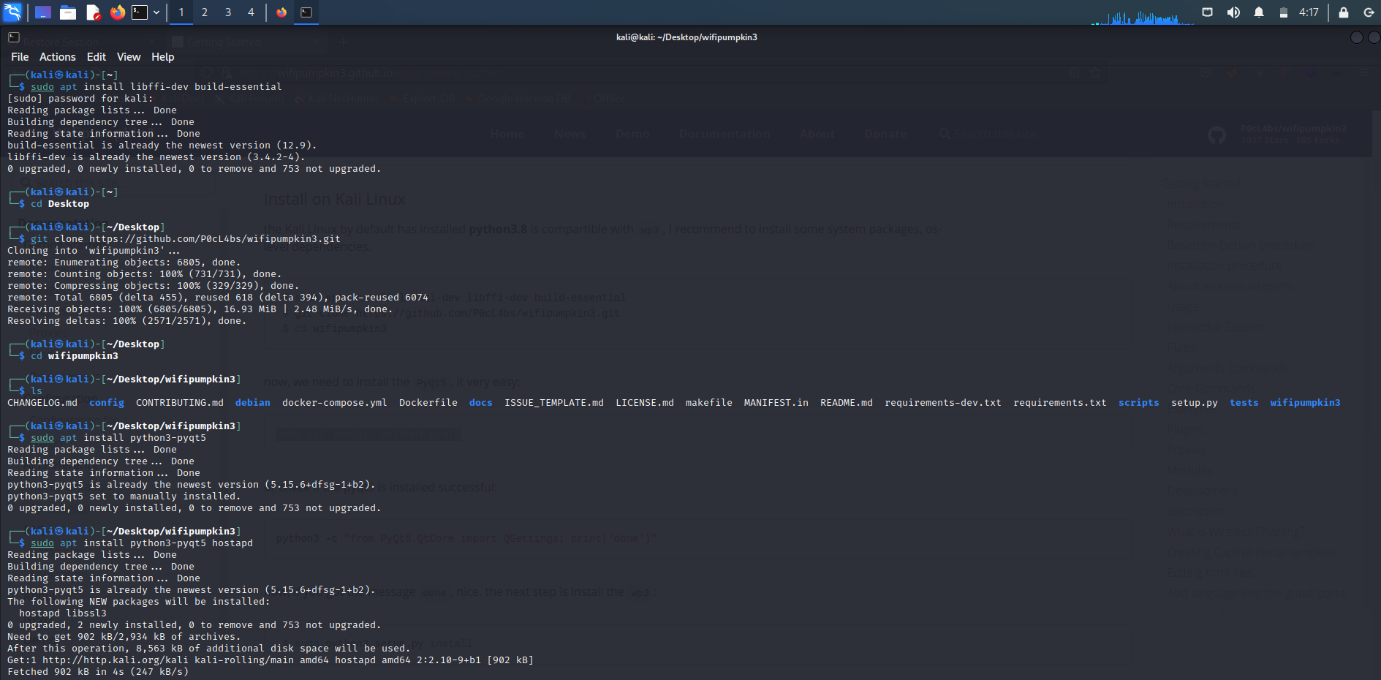
# **INDEX**

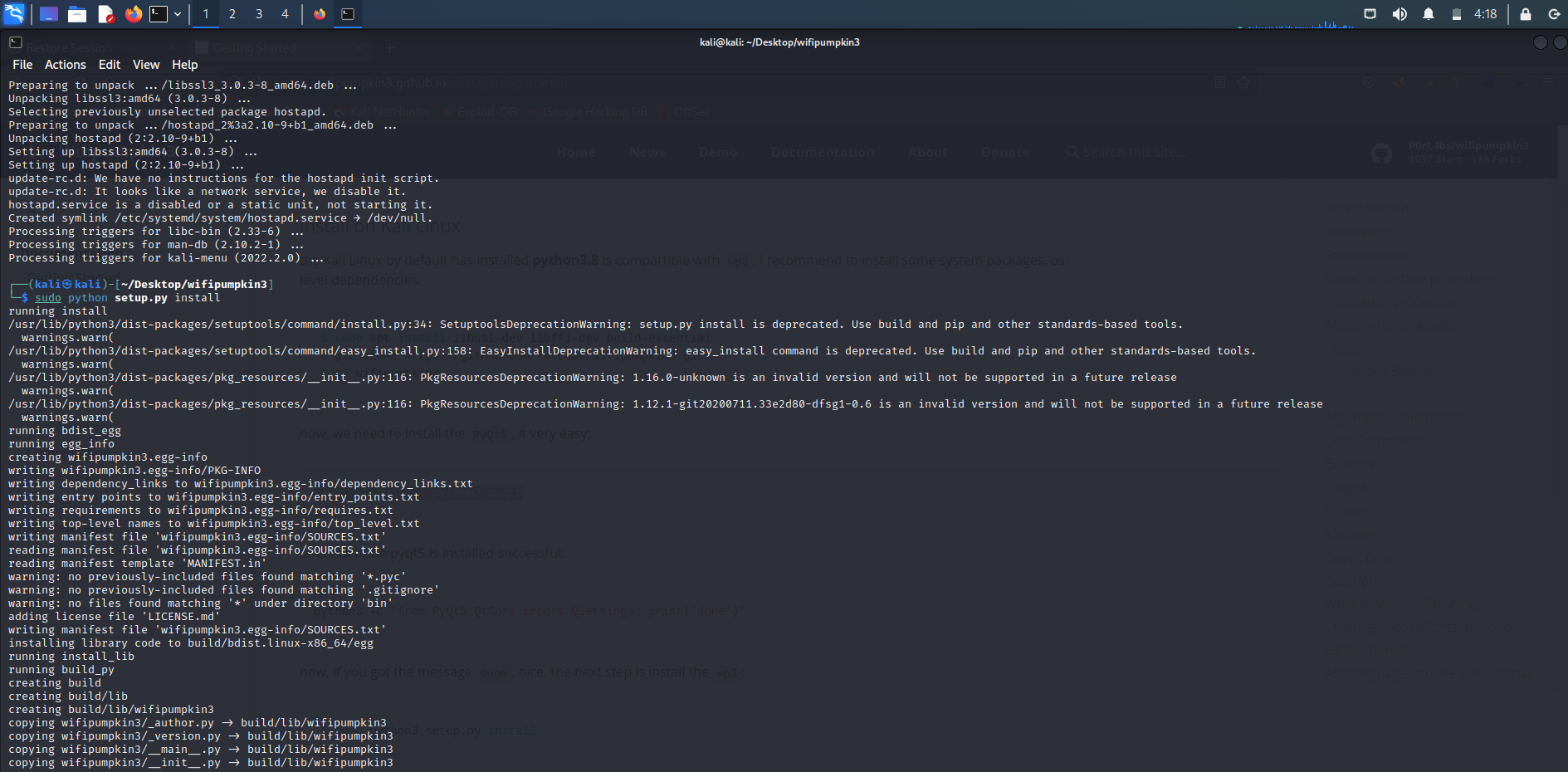
|  |  |  |
| --- | --- | --- |
| **SL NO** | **TOPIC** | **PAGE NO** |
| 1. | Installation of Wi-Fi Pumpkin | 2-3 |
| 2. | Creation of Fake Access Point | 3-4 |
| 3. | Summary Report of today’s lecture | 5-8 |

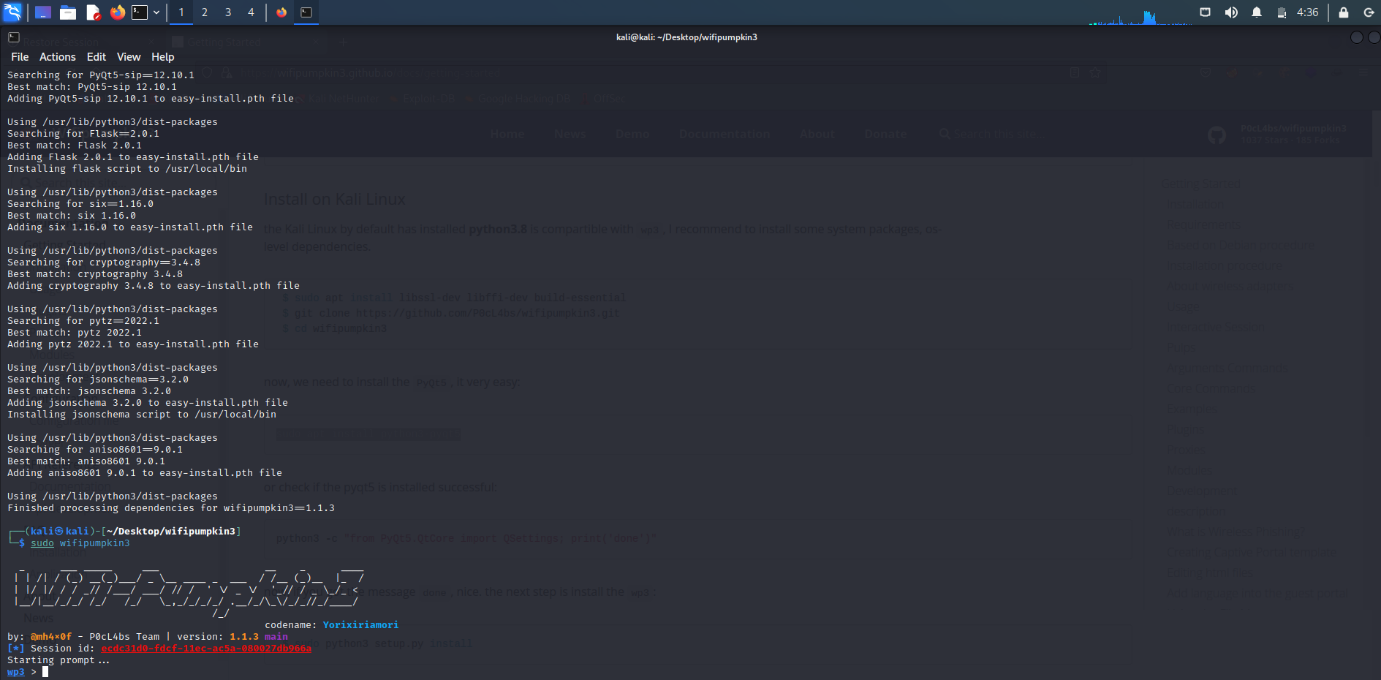
# **Topic: CRYPTOGRAPHY, HONEYPOTS ,FAKE ACCESS POINTS**

ASSIGNMENT 9(DAY 9) Date:06-07-2022

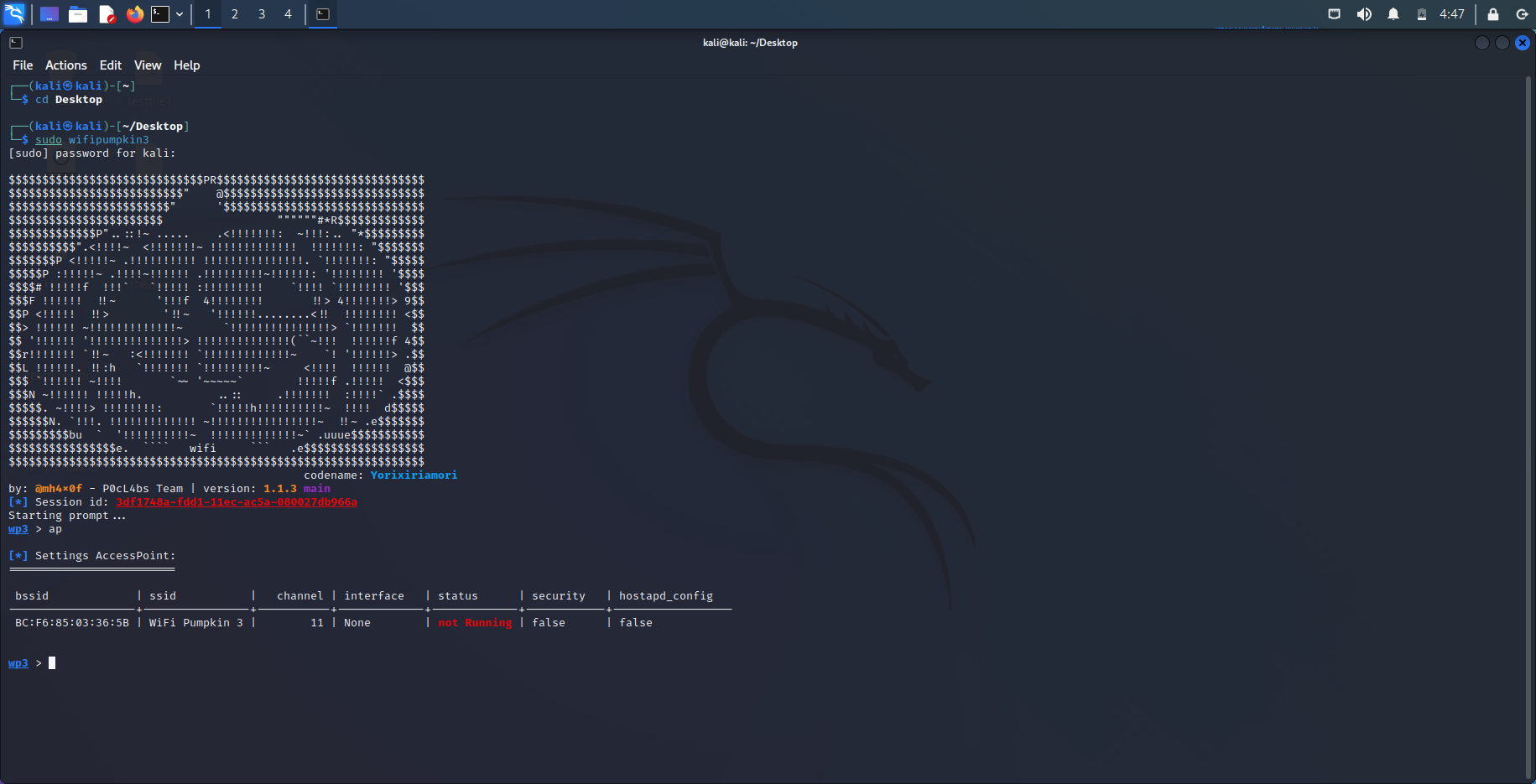
**1.Installation of Wi-Fi Pumpkin.**

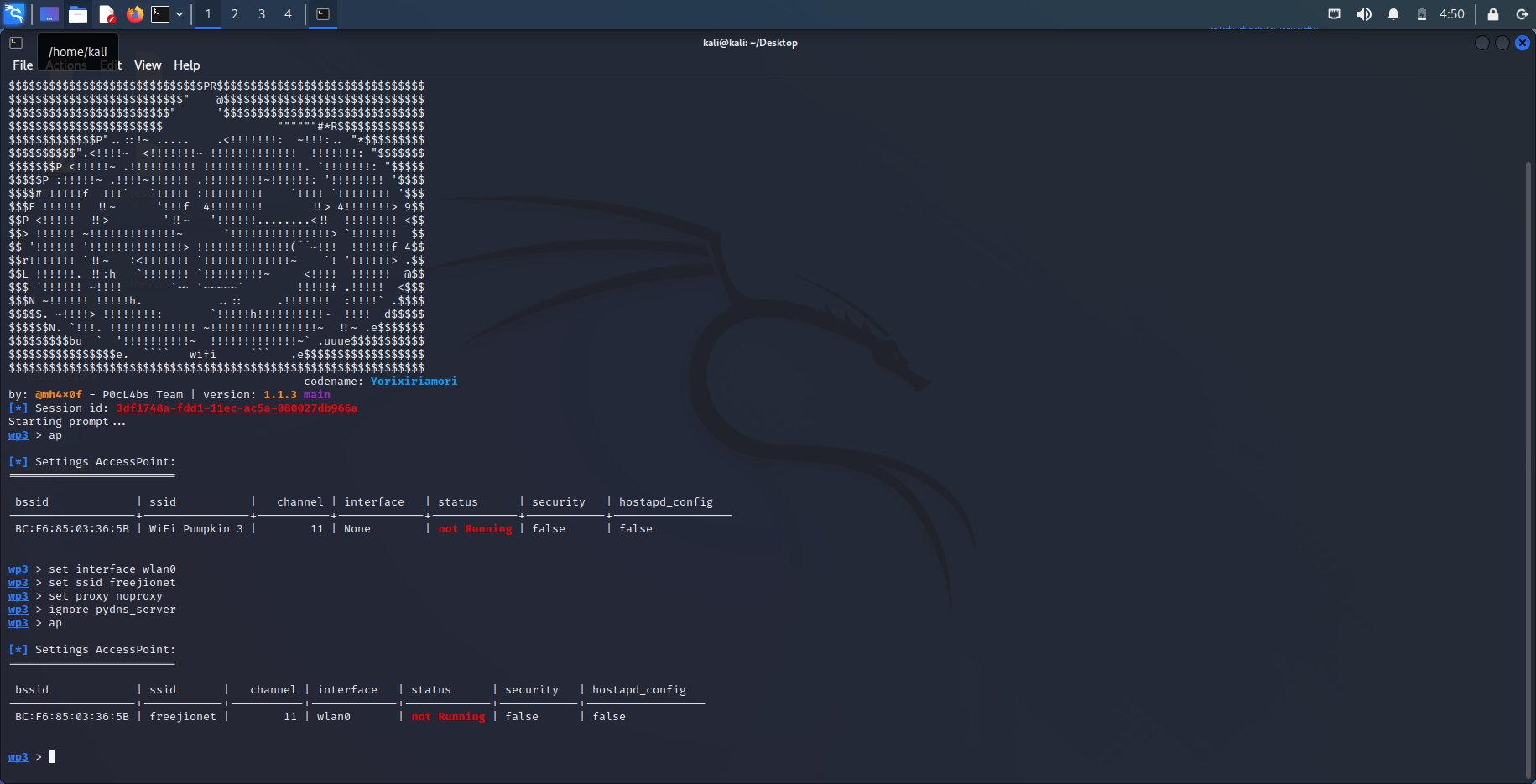
****

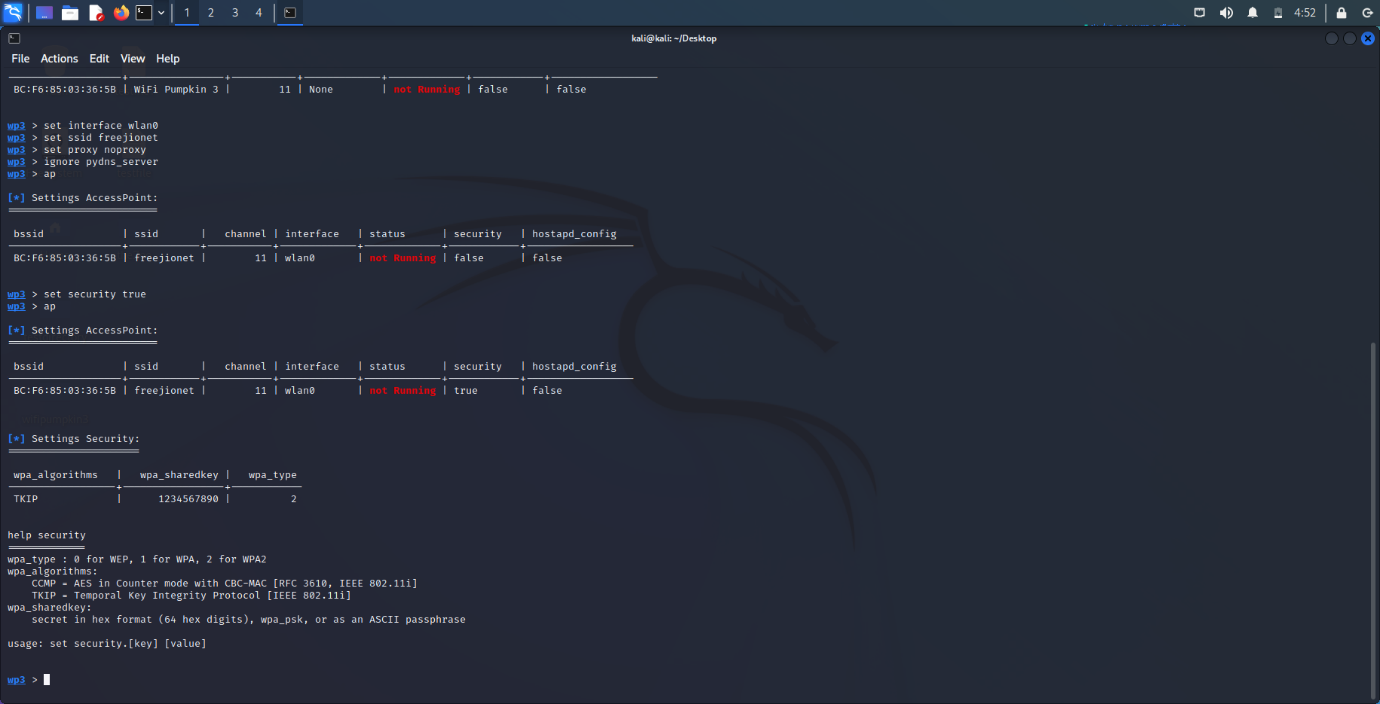
****

****

**2. Creation of fake access point.**

****

****

****

**3.Summary Report of today’s lecture.**

**CRYPTOGRAPHY**

* **What is a Cryptography?**
* **It is a science that uses mathematics to Encrypt or Decrypt the message. This method can keep the file safe even in most unsecured network like internet.**
* **Types of Cryptography**
* **Base 64**
* **Rot13**
* **Caesars Cipher**
* **Mono-Alphabetical Substitution Cipher**
* **MD5 Hash**
* **Triple DES**
* **RSA**
* **Blowfish**
* **AES**
* **Features of Cryptography**
* **Privacy/confidentiality**
* **Authentication**
* **Integrity**
* **Non-repudiation**
* **Key exchange**
* **Types of Cryptography**
* **Symmetric Key Cryptography**
* **It is an encryption system where the sender and receiver of the message use a single common key to encrypt and decrypt messages.**
* **Hash Functions**
* **A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain test to be recovered.**
* **Asymmetric Key Cryptography**
* **Here a pair of keys are used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption.**

**HONEYPOTS**

* **What is a Honeypot?**
* **A Honey Pot is an intrusion (unwanted) detection technique used to study hacker movement and interested to help better system defenses against later attacks usually made up of a virtual machine that sits on a network or single client.**
* **Three Goals of Honeypot:**
* **The virtual system should look as real as possible, it should attract unwanted intruders to connect to the virtual machine for study.**
* **The virtual system should be watched to see that it isn’t used for a massive attack on other systems.**
* **The virtual system should look and feel just like a regular system, meaning it must include files, directories and information that will catch the eye of the hacker**
* **How does a Honeypot work?**
* **Functions of Honeypot**
* **To divert the attention of the attacker from the real network, in a way that the main information resources are not compromised.**
* **To build attacker profiles in order to identify their preferred attack methods, like criminal profile.**
* **To capture new viruses or worms for future study.**
* **To identify new vulnerabilities and risks of various operating systems, environments and programs which are not thoroughly identified at the moment.**
* **Classification of Honeypot**
* **According to their Implementation Environment.**
* **Research honeypots**
* **They represent educational resources of demonstrative and research nature whose objective is centered towards studying all sorts of attack patterns and threats.**
* **Production honeypots**
* **Production honeypots are used to protect your network, they directly help secure your organization.**
* **According to their Level of Interaction.**
* **Low-Interaction**
* **Low-interaction honeypots are typically the easiest honeypots to install, configure, deploy, maintain, but customized to more specific attacks.**
* **There is no interaction with the underlying operating system**
* **High-Interaction**
* **High-interaction honeypots are the extreme of honeypot technologies.**
* **Provide an attacker with areal operating system where nothing is emulated or restricted.**
* **Advantages of Honeypots**
* **Small data sets of high value.**
* **Easier and cheaper to analyze the data**
* **Designed to capture anything thrown at them, including tools or tactics never used before**
* **Require minimal resources**
* **Work fine in encrypted or IPv6 environments**
* **Can collect in-depth information**
* **Conceptually very simple**
* **Disadvantages of Honeypots**
* **Can only track and capture activity that directly interacts with them**
* **All security technologies have risk**
* **Building, configuring, deploying and maintaining a high-interaction honeypot is time consuming**
* **Difficult to analyze a compromised honeypot**
* **High interaction honeypot introduces a high level of risk**
* **Low interaction honeypots are easily detectable by skilled attackers**

**FAKE ACCESS POINT**

* **What is Fake Access Point?**
* **Any unauthorized device that provides wireless access implemented using software, hardware, or a combination of both.**
* **It can be intentional or unintentionally set up.**
* **How Fake Access Point works?**
* **Effects of Fake Access Point**
* **Security risk.**
* **In a corporate environment it allows unauthorized access to the network.**
* **They are misconfigured and lack security features**
* **Rogue AP on network = (logically) LAN jack of your network hanging out of the premises.**
* **RF signal spillage of Rogue AP provides access to wired enterprise network from outside of the premises**
* **Prevention and Detection of Fake Access Point**

**NAME: I PRASANTI**

**SIC: 20BCEA56**

**BRANCH: CEN**