PreSkill:-

1.What is the objective of implementing Wi-Fi hacking using Reaver?
The objective is to exploit vulnerabilities in Wi-Fi Protected Setup (WPS) to retrieve a Wi-Fi network's WPA/WPA2 passphrase.

2.What is the purpose of Reaver in Wi-Fi hacking?
Reaver is used in Wi-Fi hacking to brute-force the WPS PIN, ultimately allowing access to the Wi-Fi network's security key.

3.What is WPS and how does it contribute to Wi-Fi vulnerability?
WPS is a feature designed to simplify the connection process, but it can be exploited by attackers to bypass Wi-Fi security by guessing the PIN.

4.Describe the process followed by Reaver to exploit WPS vulnerabilities.
Reaver repeatedly guesses the WPS PIN, leveraging the fact that the PIN can be broken into two parts, making it easier to brute-force.

5.What precautions should be taken before conducting Wi-Fi hacking using Reaver?
Ensure you have legal permission to test the network, and be aware that using Reaver can disrupt the Wi-Fi service and is illegal on unauthorized networks.

VIVA:-

1.**Are there any legal implications associated with Wi-Fi hacking using Reaver? Explain.**
Yes, using Reaver on unauthorized networks is illegal and can result in severe legal consequences, including fines and imprisonment.

2.**What are some countermeasures that can be implemented to protect against Reaver attacks?**
Disable WPS on your router, use strong WPA2 encryption, and regularly update your router's firmware to protect against Reaver attacks.

3.**Can you suggest alternative tools or techniques for Wi-Fi penetration testing apart from Reaver?**
Alternative tools include Aircrack-ng for WPA/WPA2 cracking and Wifite for automated Wi-Fi auditing.

4.**How does the implementation of Wi-Fi hacking using Reaver help raise awareness about Wi-Fi security?**
It demonstrates the vulnerabilities of WPS, encouraging users to secure their networks by disabling WPS and using strong encryption methods.

5.**In what scenarios can the knowledge gained from implementing Wi-Fi hacking using Reaver be useful from a security perspective?**
It’s useful for security professionals in penetration testing, helping them identify and mitigate Wi-Fi security weaknesses in a controlled, legal environment.