3.1 Develop an ethical hacking plan to identify and test weaknesses.

Ethical hacking plan to identify and test weaknesses :

1. Planning
2. Reconnaissance
3. Scanning
4. Gaining access
5. Maintaining access
6. Clearing tracks
7. Reporting

1.**Planning** – First identify a scope based on the organization's rule and regulations to know the limitation while performing ethical hacking. Then develop a plan to identify weaknesses and define the target/system to be tested. Then set a time frame for this ethical hacking test.

2. **Reconnaissance** – also known as Footprinting involves the initial stage of information gathering. Identify the target information such as IP Address, subdomains, System type and OS version. Perform passive and active reconnaissance.

3 . **Scanning** - Scan the network to identify potential vulnerabilities, open ports, and services. Appliable approaches include port scanning to identify open ports and services, vulnerability scanning to identify weaknesses that can be exploited, banner grabbing to know the versions and configurations of services running on open ports.

4. **Gaining Access** – Exploit previously identified vulnerabilities and execute technical actions to gain access to the target system. Methods – exploits known software vulnerabilities in operating systems, applications or websites, perform brute force attacks, credential thefts such as phishing, keylogging, or password cracking.

5. **Maintaining Access** – maintain control over the compromised system to assess the potential risks and impact. Strategies – backdoors, privilege escalation, Trojans or RATs (remote access Tools).

6. **Clearing Tracks** – Cover traces and evidences of hacking activities on the target system or network. Delete any signs of intrusion and ensures the ethical hacking engagement is concealed to protect the integrity and confidentiality of the process.

7.**Reporting** – Write report on every vulnerabilities found during the ethical hacking process and recommend solutions to minimize the weaknesses and improve the network security.