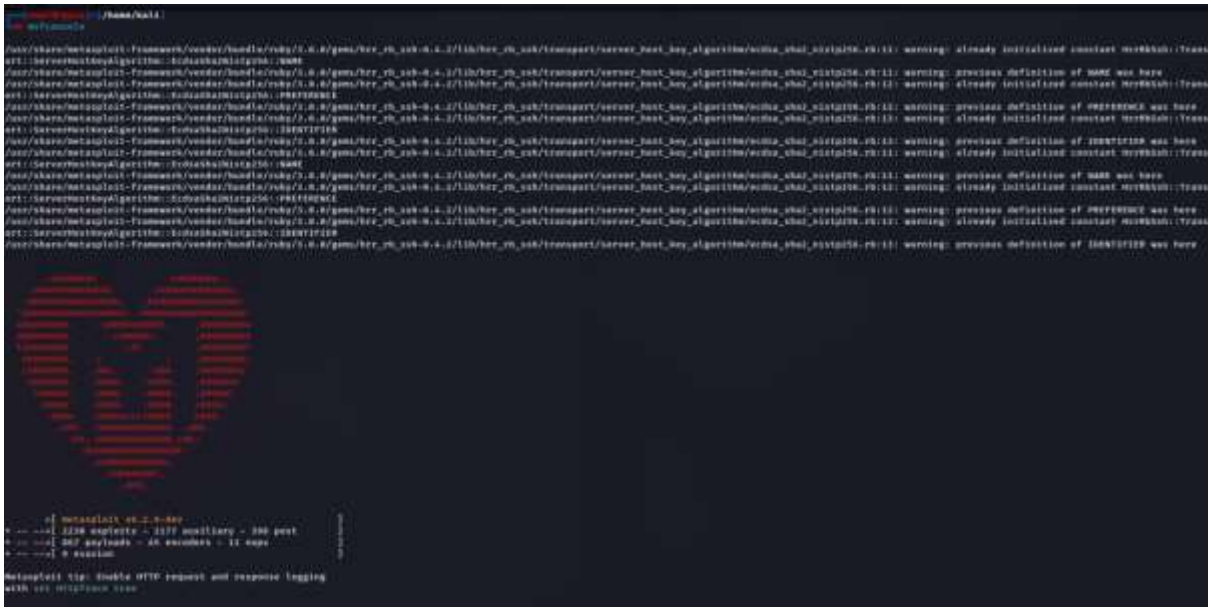
Metasploit- Auxiliary Scan

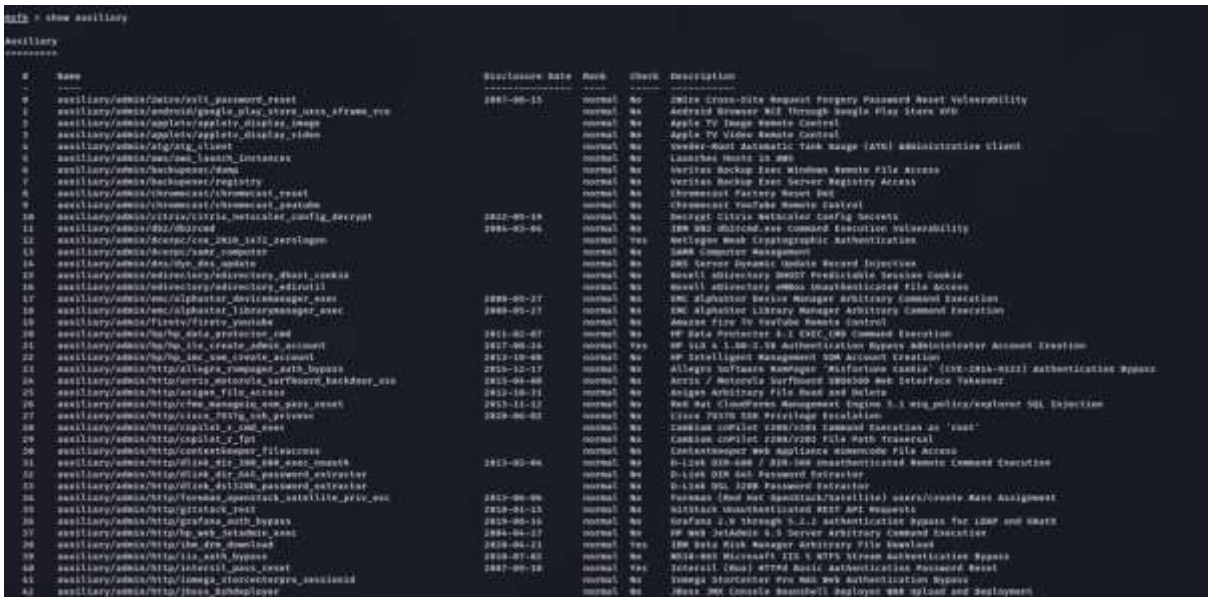
An auxiliary scan in the context of Metasploit refers to the process of using auxiliary modules to gather information about a target network or system without exploiting vulnerabilities. Unlike exploit modules, which are designed to exploit vulnerabilities and gain unauthorized access, auxiliary modules perform a variety of tasks such as network scanning, service enumeration, vulnerability assessment, and information gathering. These modules help security professionals and penetration testers to map out the network, identify active hosts, determine the services and versions running on those hosts, and uncover potential security issues that need attention. For example, an auxiliary scan can be used to detect open ports, identify operating system versions, discover network shares, and even check for weak passwords. This information is crucial for understanding the target environment and planning further penetration testing activities. Auxiliary scans are a fundamental part of the reconnaissance phase in a security assessment, providing a comprehensive overview of the target's security posture without causing disruption or alerting the target.

Example: -

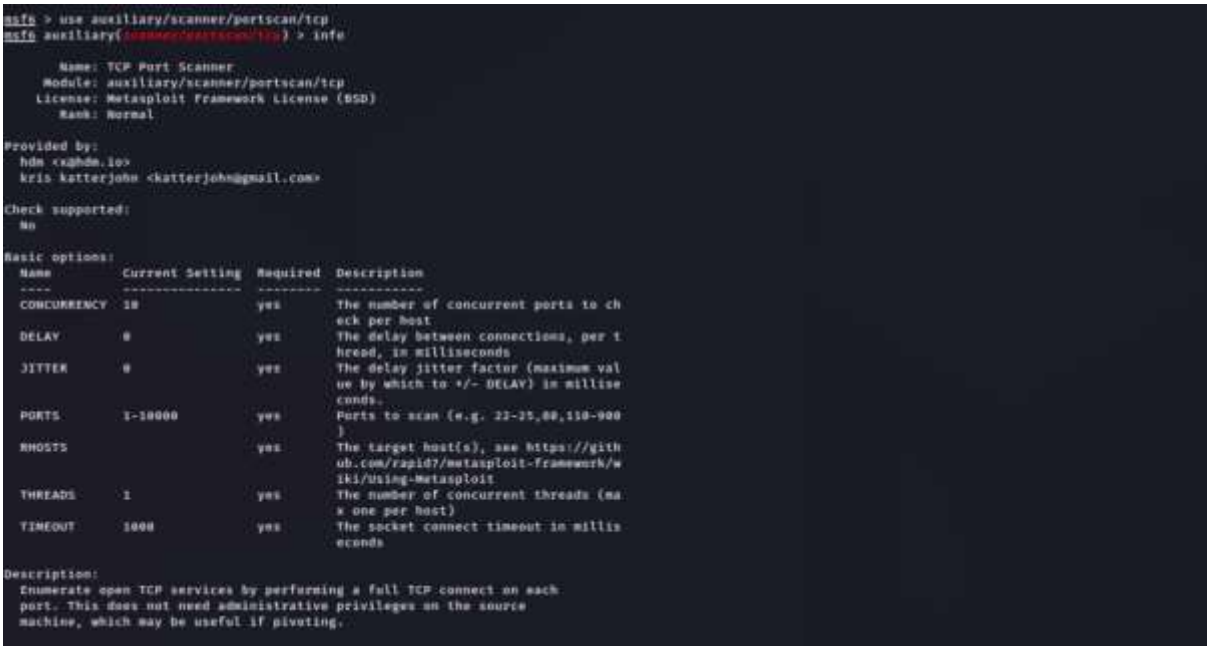
1. Firstly, open the msfconse inside the terminal.



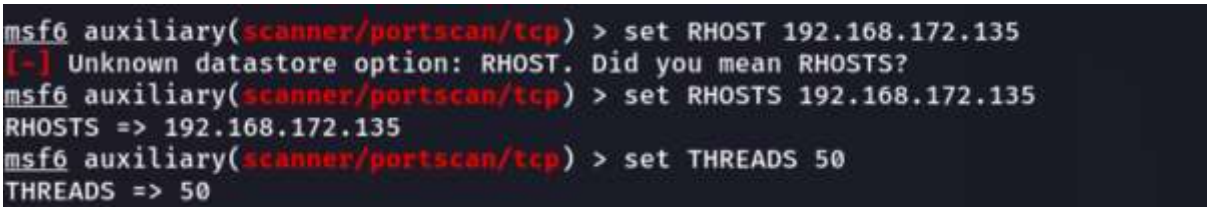
2. Now we will list all the auxiliary by using show auxiliary command.



3. Now out of list we have to choice scanner/portscan/tcp option.



4. Now we have to define our target.



5. At last use run command to perform the scan.