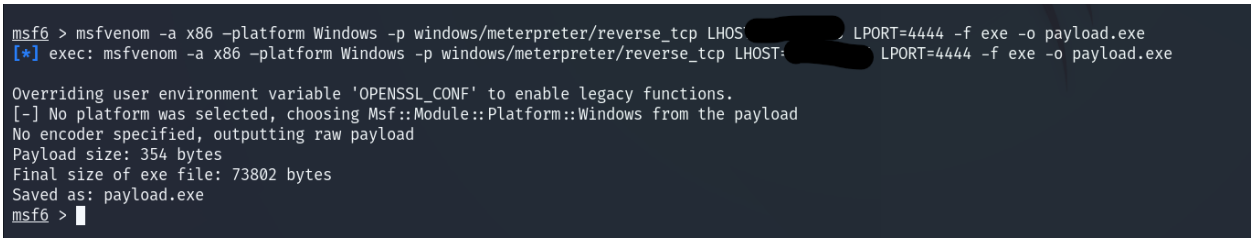
Metasploit- Remote Code Execution (RCE)

Remote Code Execution (RCE) in the Metasploit Framework refers to the process of exploiting vulnerabilities in remote systems to execute arbitrary code. Metasploit, a popular penetration testing tool, allows security professionals to identify and exploit RCE vulnerabilities by leveraging its vast library of exploits and payloads. When an RCE vulnerability is identified, Metasploit can be configured to target the vulnerable system by setting appropriate parameters such as the target IP address, port, and specific exploit details. Once configured, Metasploit's payload, which can be a reverse shell or meterpreter session, is delivered to the target. This allows the attacker to execute commands on the remote system, potentially gaining unauthorized access and control. The flexibility and extensive database of Metasploit make it a vital tool for demonstrating the impact of RCE vulnerabilities, aiding in vulnerability assessments, and reinforcing the importance of securing systems against such critical flaws.

Examples: -

1. Open msfconsole in order to create a .exe file.

2. Use the below code in order to create a window's payload.



3. As you can see we have successfully, created the windows payload.