Medusa- Wordlist Brute Forcing SSH

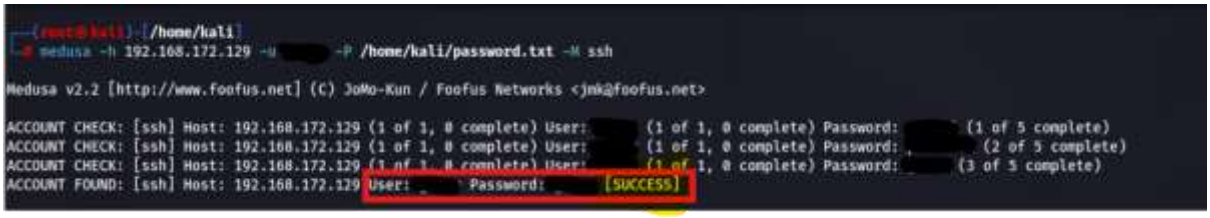
A wordlist brute-force attack is a method used in cybersecurity to gain unauthorized access to a system by systematically trying a large number of potential passwords. The attack utilizes a precompiled list of common or likely passwords, known as a wordlist, to attempt logging into a target system. Unlike a traditional brute-force attack, which tries every possible combination of characters, a wordlist brute-force attack leverages a curated list of words, phrases, or passwords, significantly speeding up the process by focusing on the most probable passwords. This technique is commonly used against various authentication mechanisms, such as login forms, encrypted files, and network services like SSH. It relies on the assumption that users often choose weak, common, or predictable passwords. Tools like John the Ripper, Hydra, and Medusa are frequently employed to automate these attacks, testing each password in the wordlist against the target system until access is gained or the list is exhausted. While effective, this attack method is illegal without explicit permission and is typically used in penetration testing to evaluate and improve system security.

Medusa is a powerful and flexible open-source tool designed for performing rapid, parallel brute-force login attacks against a variety of network services. It is widely used in the

cybersecurity field for penetration testing and security assessments. Medusa supports numerous protocols, including SSH, FTP, HTTP, POP3, and many more, making it versatile for different types of authentication mechanisms. Its ability to perform multiple login attempts simultaneously makes it highly efficient, significantly reducing the time required to complete an attack compared to sequential methods. Medusa's modular design allows for easy addition of new services and its command-line interface provides users with robust control over attack parameters, such as specifying the target IP, port, username, and password list. However, like all penetration testing tools, Medusa should be used responsibly and legally, only against systems for which the tester has explicit permission. Its effectiveness in identifying weak or default credentials makes it a valuable asset in enhancing the security posture of systems by highlighting vulnerabilities that need addressing.

Examples: -

1. In order, perform wordlist brute force attack on a target user we will use medusa tool.
   For this attack we should have information of target user IP address, Username and a wordlist to perform the wordlist attack.



   Here, we use -h to define the host/target IP address. After that -u for the target's user name. Then -P is for the path of our wordlist. In the end we use -M for setting the mode in our case it is SSH.

   In this attack scenario, we pass the target IP address and it's user name so that we can perform a wordlist Brute Force attack over it and get login credentials for the SSH login.