IKE-Scan

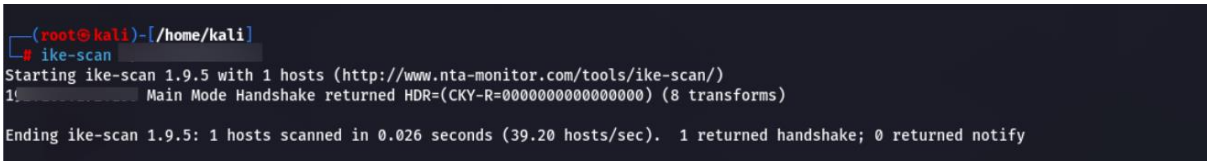
IKE-Scan is a command-line tool used for discovering, fingerprinting, and testing IPsec VPN servers by sending IKE packets and analyzing the responses. It can be useful for network security assessments and penetration testing.

ike-scan does two things:

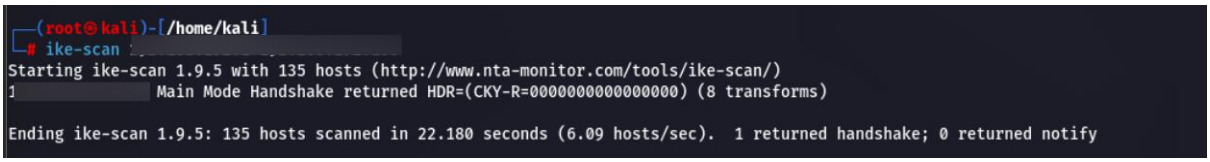
- **Discovery:** Determine which hosts are running IKE. This is done by displaying those hosts which respond to the IKE requests sent by ike-scan.
- **Fingerprinting:** Determine which IKE implementation the hosts are using. This is done by recording the times of the IKE response packets from the target hosts and comparing the observed retransmission backoff pattern against known patterns.

Examples: -

1. To scan for a single IP we will use ike-scan command along with the target IP Address.



2. To scan for a range of IP we will use ike-scan command along with the target IP Address.



3. IKE-Scan can send requests with a specific IKE policy. For example, to use Main Mode with a specific encryption algorithm (3DES), hash algorithm (SHA1), and authentication method (PSK).

4. To get the output in a detail view we will use -v command.