IPsec Enumeration

IPsec is the most commonly implemented technology for both gateway-to-gateway (LAN-to-LAN) and host to gateway (remote access) enterprise VPN solutions. IPsec provides data security by employing various components like ESP (Encapsulation Security Payload), AH (Authentication Header), and IKE (Internet Key Exchange) to secure communication between VPN end-points.

Most IPsec based VPNs use ISAKMP (Internet Security Association Key Management Protocol), a part of IKE, to establish, negotiate, modify and delete Security Associations (SA) and cryptographic keys in a VPN environment.

Enumeration with Nmap

- Lets start our enumeration using nmap.

```
sudo nmap -sU -p 500 192.168.29.141
```

Like the previous section, i wasn't able to find any machine that has IPSec installed and running. So, keep adding the techniques to the notes.

IPSec Enumeration using ike-scan

Next we will see how we can perform enumeration with ike-scan.

ike-scan is a command-line tool that comes pre-installed in kali and is used for discovering, fingerprinting, and testing IPsec VPN servers. It sends IKE (Internet Key Exchange) packets to target hosts and displays any responses received.

- To extract the hash, or preshared key, we can run the following command as long as Aggressive mode is enabled.

```
ike-scan --aggressive <targetIP>
```

- To extract some details about the VPN configuration, such as what hashing format and encryption algorithms that are being used.

```
ike-scan -M <targetIP>
```

- To confirm whether or not the VPN is using IKE version 2, you can run the following command. If it returns successful output, then you know IKEv2 is in use.

```
ike-scan -M -2 <targetIP>
```

One thing to note here is that, the Nmap scans across an established IPSEC connection will need to run with `-sT` flag to get accurate results. The default for Nmap is to run with SYN scans (`-sS`) with sudo.
