

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.

```
(root@kali)-[/home/kali]
# ike-scan 192.168.1.1
Starting ike-scan 1.9.5 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
1:----- Main Mode Handshake returned HDR=(CKY-R=0000000000000000) (8 transforms)

Ending ike-scan 1.9.5: 1 hosts scanned in 0.026 seconds (39.20 hosts/sec). 1 returned handshake; 0 returned notify
```

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

```
(root@kali)-[/home/kali]
# ike-scan 192.168.1.0/24
Starting ike-scan 1.9.5 with 135 hosts (http://www.nta-monitor.com/tools/ike-scan/)
1:----- Main Mode Handshake returned HDR=(CKY-R=0000000000000000) (8 transforms)

Ending ike-scan 1.9.5: 135 hosts scanned in 22.180 seconds (6.09 hosts/sec). 1 returned handshake; 0 returned notify
```

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).

```
(root@kali)-[/home/kali]
# ike-scan --trans=1,1,5,2,2 192.168.1.1
WARNING: Ignoring extra transform specifications past 4th
Starting ike-scan 1.9.5 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
1:----- Main Mode Handshake returned HDR=(CKY-R=0000000000000000) SA=(Enc=DES Hash=MD5 Auth=RSA_RevEnc Group=2:modp1024 LifeType=Seconds LifeDuration(4)=0x00007080)

Ending ike-scan 1.9.5: 1 hosts scanned in 0.015 seconds (68.47 hosts/sec). 1 returned handshake; 0 returned notify
```

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

```
(root@kali)-[/home/kali]
# ike-scan -v 192.168.1.1
DEBUG: pkt len=336 bytes, bandwidth=56000 bps, int=52000 us
Starting ike-scan 1.9.5 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
1:----- 5 Main Mode Handshake returned HDR=(CKY-R=0000000000000000) (8 transforms)

Ending ike-scan 1.9.5: 1 hosts scanned in 0.010 seconds (100.84 hosts/sec). 1 returned handshake; 0 returned notify
```