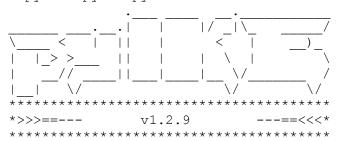
sudo python pyike.py 10.100.140.35 -T1



- [>] Checking options...
- [>] Running pre-scan checks....
- [+] Checking all target ports are open before attempting IKE scan (default).
- [+] Using light intensity (45 transforms (-T1) with PSK only).
- [+] Using 45 transforms on 1 target(s).
- [>] Testing 10.100.140.35:
- [+] 10.100.140.35:500/udp is open checking for Aggressive Mode....
- [+] 10.100.140.35 Aggressive Mode Handshake returned (Validation: ike-scan -M -A --id=fakegroup --trans=1,2,1,2 10.100.140.35 -P)
- [+] Running implementation check (slow):
- [+] 10.100.140.35 Implementation guess: Cisco VPN Concentrator or PIX 7.0 (Validation:ike-scan -M --trans=1,2,1,2 --showbackoff 10.100.140.35)
- [+] RESPONDER HASH:

fb9ae07b5bb9556ccc473af1673212d6e7e6505e375c8794e84b7a808f960dca24b84f905695c12 53d3407a178cf92bd13793bcce068969fdff99608880e9d09fe6dee3397a6d76723ca935a627d43 274d13388fd70ceaa9db158f50d668be0a47536755ad1acfcf3e801a9fad5d6c6bfc977c2411df5 b2aaacc530e96fb48b6:d3dc1a6a89d6d283fc2299909608197f7f0a1f85cdcb2b0f8514d5f9f26 1d6f89ca29db136b366d1092f54f068d926468fa3a19a1eeb34063001a9394b8a8843e11dc44a59 5727556a7eba5c4274871e56fba0d7c9401317fd12f3c77d10a59d9e2547834be60c12b0e52e5c8 d58f1a00ead73c1c0982478f20d6472eab64907:8e8dec2d444234e0:0fa3f32c5aea6483:00000 001000000010000002c01010001000000240101000080010001800200028003000180040002800b 0001000c000400007080:01110000c3c29203:05c6de3ef9e629d202c0ebf60773463f108352fc: 1997742102405e5a68ddc4915292605df2f335ad:919f6bfec54b8f470f1309890809ab3a1f62fd ff

- [*] Note that unless the group ID is correct, the responder hash (hash_r)
 returned
- [*] from CISCO devices is an anti-enumeration feature, and will not be crackable.
- [-] Other transform options allowing Aggressive Mode handshakes on this host (from the T1 list of 45 transforms):

```
(--trans=5,2,1,2)
(--trans=7/128,2,1,2)
(--trans=7/192,2,1,2)
```

- [+] Conclusion: 10.100.140.35 supports Aggressive Mode.
- [+] 1 server(s) found supporting Aggressive Mode.