

# Pen-testing remote VPN services over IP

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2003-11/0023.html>

---

**From:** Chris McNab ([chris.mcnab\\_at\\_trustmatta.com](mailto:chris.mcnab_at_trustmatta.com))

**Date:** 11/06/03

To: <[pen-test@securityfocus.com](mailto:pen-test@securityfocus.com)>

Date: Thu, 6 Nov 2003 19:21:50 -0000

Hi,

As part of some research I am undertaking recently, I'd like to know if any of you have any decent information relating to the following areas of \_remote\_ assessment of VPN services over IP.

The topics I have covered and documented fully so far include:

- IPsec enumeration, scanning for UDP/500 and using Roy Hills' tools (ike-scan) to identify the gateway
- Various overflows relating to ISAKMP / IKE packets being sent to UDP/500, as in MITRE CVE
- Offline aggressive mode IKE pre-shared key cracking, by sniffing VPN traffic and using IKECrack
- Check Point aggressive mode IKE username enumeration (using Roy Hills' fw1-ike-userguess over UDP/500)
- Check Point Telnet authentication service (TCP/259) user enumeration
- Check Point information leak attacks that reveal network interface addresses, over both TCP/256 and TCP/264
- Check Point RDP encapsulation filter bypass techniques, using UDP/259
- Offline Microsoft PPTP (TCP/1723) MS-CHAP challenge-response cracking

Two areas in which I've identified a need for tools are:

- Check Point brute force password grinding tool for FWZ or IKE, to compromise SecuRemote username/password combinations
- PPTP brute force tool, to compromise those user/password combinations also

Does anyone know of such offensive brute force tools, or techniques I have missed (against ISAKMP and Check Point)? if so, any input would be greatly appreciated.

Regards,

Chris

Chris McNab

## SecurityFocus Penetration: Pen-testing remote VPN services over IP

Technical Director

Matta

18 Noel Street  
London W1F 8GN

<http://www.trustmatta.com>

---

Network with over 10,000 of the brightest minds in information security at the largest, most highly-anticipated industry event of the year. Don't miss RSA Conference 2004! Choose from over 200 class sessions and see demos from more than 250 industry vendors. If your job touches security, you need to be here. Learn more or register at [http://www.securityfocus.com/sponsor/RSA\\_pen-test\\_031023](http://www.securityfocus.com/sponsor/RSA_pen-test_031023) and use priority code SF4.

---