

# [Full-disclosure] Hacking Exposed Cisco Networks

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-12/msg01091.html>

---

- *From:* "Konstantin V. Gavrilenko" <[mlists@xxxxxxxxxx](mailto:mlists@xxxxxxxxxx)>
  - *Date:* Tue, 20 Dec 2005 18:05:26 +0200
- 

Hi List,

"Hacking Exposed Cisco Networks" was officially released yesterday. In the next couple of weeks it should be available in the shops. In the meantime you can download a sample chapter, get additional info about the book and download related tools from the book's official web page.

<http://www.hackingciscoexposed.com/>

-----The book outline-----

Defend against the sneakiest attacks by looking at your Cisco network and devices through the eyes of the intruder. Hacking Exposed Cisco Networks shows you, step-by-step, how hackers target exposed systems, gain access, and pilfer compromised networks. All device-specific and network-centered security issues are covered alongside real-world examples, in-depth case studies, and detailed countermeasures. It's all here: from switch, router, firewall, wireless, and VPN vulnerabilities to Layer 2 man-in-the-middle, VLAN jumping, BGP, DoS, and DDoS attacks. You'll prevent tomorrow's catastrophe by learning how new flaws in Cisco-centered networks are discovered and abused by cyber-criminals.

- \* Use the tried-and-true Hacking Exposed methodology to find, exploit, and plug security holes in Cisco devices and networks
- \* Locate vulnerable Cisco networks using Google and BGP queries, wardialing, fuzzing, host fingerprinting, and portscanning
- \* Gain network access using password and SNMP community guessing, Telnet session hijacking, and searching for open TFTP servers

## [Full-disclosure] Hacking Exposed Cisco Networks

- \* Use blackbox testing to uncover data input validation errors, hidden backdoors, HTTP, and SNMP vulnerabilities
- \* Find out how IOS exploits are currently written and whether an attacker can insert malicious code into the IOS binary itself and use Cisco router as an attack platform
- \* Block determined DoS and DDoS attacks using Cisco proprietary safeguards, CAR, and NBAR
- \* Prevent secret keys cracking, sneaky data link attacks, routing protocol exploits, and malicious physical access
- \* Abuse Cisco failover protocols, punch holes in firewalls, and break into VPN tunnels

I hope you enjoy the read.

--

Respectfully,  
Konstantin V. Gavrilenko

Arhont Ltd - Information Security

web: <http://www.arhont.com>  
<http://www.wi-foo.com>  
e-mail: k.gavrilenko@xxxxxxxxxxxx

tel: +44 (0) 870 44 31337  
fax: +44 (0) 117 969 0141

PGP: Key ID - 0x4F3608F7  
PGP: Server - keyserver.pgp.com

---

Full-Disclosure - We believe in it.  
Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>  
Hosted and sponsored by Secunia - <http://secunia.com/>