INTRODUCTION

Perhaps the real difference between the Jedi and the Sith lies only in their orientation; a Jedi gains power through understanding, and a Sith gains understanding through power.

—Darth Sidious

THE PECULIARITIES AND HARDSHIPS OF CISCO-RELATED ATTACKS AND DEFENSES

Some *hackers* (in a loose meaning of this battered term) try to understand everything about the internal workings of a system or protocol they have targeted, and only then do they begin the exploitation. Others try to break it using all means at their disposal and learn about the system in the process of breaking it. The methodologies we describe in this book can appeal to the followers of both paths. At the end of the day, it is the results that count, and an approach that works best for the attacker would be embraced by him or her as true. In our specific case, the result is usually called *enable*.

An attacker who goes after Cisco networking devices can be a CCIE Security consultant, performing a legitimate security audit. He can be a renegade system programmer, armed with disassembly tools and searching for great fame or equally great stealth. She might be an experienced network engineer with an arsenal of powerful sniffing and custom packet generating utilities, with a craving for the takeover of the whole network via an unknown glitch in a proprietary protocol design. Or, perhaps a novice hacker has just discovered what really runs the modern Internet and wants to experiment with these mysterious and powerful hosts. As the person responsible for the security of a network, you have to be ready to cope with all types of attackers and everything they can throw at the target. As a security auditor, you have to be capable of emulating all kinds of attackers, understanding their mentality, approaches, methods, and techniques. Only by starting the audit while behaving like the lowest denominator of cracker, and ending it acting like a highly professional Black Hat, can a penetration tester do a proper external or internal risk assessment of the audited network.

This is not easy. First of all, everything related to Cisco systems and protocols hacking is only beginning to emerge from the shadows. You won't find a lot of comprehensive information about this online, and this book is the world's first printed literature source entirely devoted to this issue. Another difficulty you (and the attackers) will inevitably encounter is the great variety of Cisco devices and versions of the operating systems that they run—routers, switches, firewalls, VPN concentrators, IDS sensors, wireless access points, and so on. They run various versions of IOS, CatOS, PIX OS, and even general purpose operating systems such as Solaris and Linux. To make things more difficult, many OS versions are specifically bound to the hardware they run on for efficiency and optimization reasons. This is particularly important for a highly skilled attacker trying to write a shellcode for his exploit.

When Next Generation (NG) IOS appears and good old CatOS eventually dies out, truly cross-platform exploits for Cisco routers and switches may become possible. For now, an exploit will work against a specific platform only, and a hacker would need to spare some time and effort to find offset addresses for different IOS versions running on that particular platform. It should be noted that network administrators in general seem to be somewhat conservative and not truly eager to update the operating systems of their routers and switches. We have encountered many cases of IOS 11.X and CatOS 4.X still running on the audited hosts. Thus, older IOS and CatOS versions are here to stay for quite a while, even after the much talked about IOS NG is released.

On the defenders' side, the differences between the system versions mean that some countermeasures will be available on the systems you control, and some won't. Moreover, the same safeguard could be configured on distinct system versions using different commands or variations of the same command. This makes the device and the overall network defense a rather complicated task. A lot of material, mostly from Cisco itself, has been released on the subject of securing Cisco devices and whole networks, but blindly typing the commands mentioned in the manual does not help the administrator to understand the full impact or implications of the attack these commands may prevent. Thus, the incentive to spend time on thoroughly configuring existing security features and patching the known flaws may run very low. What is needed is an all-around Cisco security resource, providing a professional description and systematic balanced approach to both attack and defense. We have strived to adhere to this requirement as much as possible and hope that this book will meet at least some of your expectations.

We have also tried to dispel common mythology surrounding the peculiarities of Cisco device and network security and halting the development of this important information security field. The harmful myths currently circulating within the world security community, from corporate security managers to lowly script kiddies, are many and include the following:

- Cisco routers, switches, PIX firewalls, and so on are secure by default and can't really be broken into, unless they are badly misconfigured.
- To the contrary, Cisco routers are very easy to break into (this opinion is common among the "Telnet password and SNMP community guessing crowd," a part of the "hooded yob" populating so-called "underground channels").

- Running the IOS privileged EXEC mode `auto secure no-interact` command will automatically sort out all your security headaches, even if you don't know much about router security.
- The cracking underground is not really familiar with Cisco network appliances and rarely selects them as targets.
- There is little the intruders can do with a taken over Cisco router and nothing they can do with an "owned" Catalyst switch. At worst, they will erase both Flash and NVRAM.
- An intruder cannot preserve his access to an owned Cisco router or other device without leaving telltale signs in its configuration file.
- Data link layer attacks are for weirdoes. You can do the same things with ARP spoofing, right?
- Crackers can bring down the whole Internet via a BGP-based attack, and it is easy to do.
- To the contrary, BGP is completely secure and unbreakable. Proprietary routing protocols are also very secure, since their full specifications are not known to attackers.
- Buffer overflow attacks against IOS are impractical and too difficult to execute. Writing exploits against this system is an extreme form of rocket science, known only to the few remaining Illuminati.
- Patching the IOS binary image to inject malicious code is also next to impossible. Such an image won't be accepted by the router or won't function properly.
- Attacking another router from (not through!) a hacked router? That's impossible! Cisco cross-platform worm? You must be joking!

Whether you prefer to gain power through understanding or understanding through power, we hope that the contents of this book will convince you that these statements are, to put it politely, rather economical with the truth, which often lies somewhere in the middle.

ALL THE POWER OF HACKING EXPOSED AND MORE

This tome is written in the best tradition of the *Hacking Exposed* series. However, we've included a few differences, such as the way risk ratings are handled.

The topic of Cisco-related hacking isn't exactly the most researched topic. Many potential security threats and attack algorithms described here are little-known or new and were discovered during the process of writing this book. To do this, we assembled a tiny testing and research Cisco network, consisting of three 2500 and two 2600 series routers, Catalyst 2950 and 5000 series switches, PIX 515E and PIX 501 firewalls, a 3000 series VPN concentrator, and an Aironet 1200 wireless access point. We have also employed a couple of Gentoo and Debian Linux machines running Quagga and various attack and network monitoring/analysis tools mentioned through the book. A maximum

effort was made to test all the presented methods and techniques on this network. In addition, some of the published data, of course, is based on our hands-on experience as penetration testers, network security administrators, and architects.

Also, when working on the book, we discovered that the current arsenal of open source Cisco security auditing tools is rather limited. So we had to write some new tools and scripts to close such gaps and *make the theoretical practical* (an old L0pht motto, for those who don't remember). They are available under the GPL license at the book's companion web site, *http://www.hackingexposedcisco.com*, to anyone interested. The time for the entire project was restricted, and it was not possible to complete everything that was initially planned. Thus, some of the code had to join the TODO list queue and will hopefully be finished by the time this book hits the shelves, or soon afterward. So, do visit the site for the updates, including new security tools and research observations.

Easy to Navigate

A standard tested and tried *Hacking Exposed* format is used through this book:

This is an attack icon.

This icon identifies specific penetration testing techniques and tools. The icon is followed by the technique or attack name and a traditional *Hacking Exposed* risk rating table:

Popularity:	*The frequency with which we estimate the attack takes place in the wild. Directly correlates with the Simplicity field. 1 is the most rare, 10 is used a lot, N/A is not applicable (the issue was been discovered in a testing lab when writing this book).*
Simplicity:	*The degree of skill necessary to execute the attack. 10 is using a widespread point-and-click tool or an equivalent, 1 is writing a new exploit yourself. The values around 5 are likely to indicate a difficult-to-use available command line tool that requires knowledge of the target system or protocol by the attacker.*
Impact:	*The potential damage caused by successful attack execution. Usually varies from 1 to 10; however, this particular book does have a few exemptions to this rule. 1 is disclosing some trivial information about the device or network, 10 is getting enable on the box or being able to redirect, sniff and modify network traffic.*
Risk Rating:	***This value is obtained by averaging the three previous values. In a few cases, where the Popularity value equals N/A, only the Simplicity and Impact numbers are averaged.***

So, what are the exceptionally high Impact values supplied in some specific cases in Chapters 10 and 14? Imagine an attack that may lead to thousands of networks being compromised or large segments of the Internet losing connectivity or having their traffic redirected by crackers. It is clear that the impact of such an attack would be much higher than gaining enable on a single host or redirecting and intercepting network traffic on a small LAN. At the same time, attacks of such scale are neither common nor easy to execute without having a significant level of skill and knowledge. Thus, their Popularity and Simplicity values would be quite low, and even if the Impact value equals 10, the overall Risk Rating is going to be lower, as compared to easier to execute attacks that do not present a fraction of the threat. This does not represent a real-world situation, and a logical solution to rectify this problem is to inflate the underrated Impact field value, so that the overall Risk Rating is at the maximum or, at least, close to it.

We have also use these visually enhanced icons to highlight specific details and suggestions, where we deem it necessary:

This is a countermeasure icon.

Where appropriate, we have tried to provide different types of attack countermeasures for different Cisco platforms, not just the IOS routers. Such countermeasures can be full (upgrading the vulnerable software or using a more secure network protocol) or temporary (reconfiguring the device to shut down the vulnerable service, option, or protocol). We always recommend that you follow the full countermeasure solution; however, we do recognize that due to hardware restrictions, this may not be possible every time. In such a situation, both temporary and incomplete countermeasures are better than nothing. An incomplete countermeasure is a safeguard that only slows down the attacker and can be bypassed—for example, a standard access list can be bypassed via IP spoofing, man-in-the-middle, and session hijacking attacks. In the book, we always state whether the countermeasure is incomplete and can be circumvented by crackers.

The Companion Web Site

Expressing great care about the precious time of the reader, we have created a separate online resource specifically for the book. It contains the collection of the new code mentioned in the book and not available anywhere else. As to the rest of the utilities covered in the book, each one of them has an annotated URL directing you to its home

site. In case the future support of the utility is stopped by the maintainer, we will make the latest copy available at *http://www.hackingexposedcisco.com*, so you won't encounter a description of a nonexisting tool in the book. We also plan to post any relevant future observations and ideas at this web site.

HOW THE BOOK IS ORGANIZED

This book is split into three completely different parts. Each part can be read without even touching the remaining two—so if the reader is interested only in the issues described in the selected part, he or she may consult only that part.

Part I. "Foundations"

The first part is introductory and gives the reader a taste of real-world Cisco devices and network security. None of the chapters in it deals with detailed attack techniques; thus, the usual *Hacking Exposed* Attack icons and Risk Rating boxes are absent. The majority of information in this part is defender-oriented, with a strong emphasis on the need for security to be built in to the network design from its earliest stage.

Chapter 1. "Cisco Network Design Models and Security Overview"

We begin the book by looking at the network as a whole and outlining how different network topologies, architectures, and designs can affect its security from both defender and attacker perspective.

Chapter 2. "Cisco Network Security Elements"

A logical continuation of the previous chapter, this chapter provides a comprehensive review of all common Cisco security appliances, applications, and device security features. The selection is staggering.

Chapter 3. "Real-World Cisco Security Issues"

This chapter is fully devoted to attackers: their motivations, aims, things they may do with the "owned" devices, and the general hacker's perspective of Cisco appliances and networks. It ends up by laying the foundations for professional, independent Cisco device and network penetration testing.

Part II. "'I Am Enabled': Hacking the Box"

This part is the core of the book and describes how an attacker would first enumerate the whole network, and then pick up specific targets, enumerate them with great precision, launch an appropriate attack, gain and preserve enable-level access, and proceed with further devastating attacks through or from the hacked Cisco devices.

Chapter 4. "Profiling and Enumerating Cisco Networks"

In this chapter, various Cisco-related network enumeration tricks not described in other *Hacking Exposed* volumes are shown. A heavy emphasis is placed on routing protocols, in particular BGPv4. Some of the demonstrated methods can directly handle the device access to a lucky cracker.

Chapter 5. "Enumerating and Fingerprinting Cisco Devices"

Here we review passive, semi-active, and active methods of precise enumeration of various standalone Cisco devices, from casual routers to VPN concentrators and wireless access points. Plenty of examples are provided, together with the recommendations on how to hide your box from the cracker's eyes.

Chapter 6. "Getting in from the Outside: Dead Easy"

The methods described in this chapter in great detail may not be very exciting, but they surely work, and that is how the majority of Cisco devices in the real world fall into even the most inexperienced attacker's hands.

Chapter 7. "Hacking Cisco Devices: The Intermediate Path"

Learn how hackers can discover input validation, information leak, and denial of service vulnerabilities of Cisco devices employing classical Black Box techniques, such as packet fuzzing. The two most common Cisco management services, SNMPd and web interface, are used to illustrate this approach in practice.

Chapter 8. Cisco IOS Exploitation: The Proper Way

Find out how working buffer overflow exploits for Cisco IOS are constructed using a real-life example. We jokingly call this chapter "FX for Dummies"—however, there is far more to it than meets the eye.

Chapter 9. "Secret Keys Cracking, Social Engineering and Malicious Physical Access"

If a purely technical means of gaining access has failed, crackers can use social engineering tricks to gain physical access to a Cisco device, retrieve the configuration file, and crack the encrypted passwords. This chapter offers a welcome break between two technically heavy and skill-demanding chapters (8 and 10).

Chapter 10. "Exploiting and Preserving Access"

Here the myth of "attackers not being able to do a lot with the hacked Cisco router or switch" receives heavy battering. The most skilled intruders can actually hide the malicious code inside of the IOS binary image or even write a cross-platform IOS worm. On the countermeasures side, Cisco forensics are discussed.

Chapter 11. "Denial of Service Attacks Against Cisco Devices"

Denial of service attacks against or through Cisco hosts are common, and this book would not be complete without covering this topic. Apart from the attacks themselves, we also explain how to use Cisco proprietary safeguards to stop even the most devastating distributed denial of service assaults.

Part III. "Protocol Exploitation in Cisco Networking Environments"

In the final part of the book, we shift our attention from attacking the device to attacking the protocol. A fine art of protocol exploitation can handle intruders full control over the network traffic without any direct access and reconfiguration of the hosts deployed.

Chapter 12. "Spanning Tree, VLANs, EAP-LEAP, and CDP"

Data link layer attacks are not well known to unskilled crackers. They are sly and can easily slip under the watchful eye of an IDS, handling the attacker both stealth and power.

Chapter 13. "HSRP, GRE, Firewalls, and VPN Penetration"

Moving to the higher network layers, the crackers can abuse Cisco failover and tunneling protocols, punch holes in firewalls, and hack into supposedly secure VPN tunnels. Don't succumb to a false sense of security—just having a firewall or a VPN deployed is insufficient to stop a skilled attacker from doing his dastardly deeds.

Chapter 14. "Routing Protocols Exploitation"

Who controls the routing protocol controls the network. What else can be said? Pay special attention to BGP attacks, because they are a megalomaniac cracker's bonanza.

Part IV. "Appendixes"

The appendixes provide additional technical material necessary for using some of the described concepts and techniques in practice.

Appendix A. "Network Appliance Security Testing Template"

This is the actual step-by-step template we developed from scratch for thorough security beta-testing of standalone network appliances, including those made by Cisco.

Appendix B. "Lab Router Interactive Cisco Auto Secure Configuration Example"

A live router example of the IOS `auto secure` configuration is provided to help network administrators use this reasonably recent IOS security feature, while avoiding any unnecessary configuration changes.

Appendix C. "Undocumented Cisco Commands"

Here we present the first-ever printed press catalog of these mysterious commands for different Cisco-made operating systems, which can be helpful for both attackers and defenders alike. The secret enable-engineer mode commands taken from our testing CatOS switch are included.

A FINAL MESSAGE TO OUR READERS

We could not describe all the existing Cisco-related attacks in a single book and apologize if something has gone amiss. In the first place, compiling a comprehensive paper database of things that anyone can find by searching the SecurityFocus web site wasn't our goal. Our true aim was to describe how things work and why they work this way in a logical and sequential manner. In other words, we hope to "teach the person to fish instead of feeding him every day." Hopefully, after reading this tome, you will be able to understand how new vulnerabilities in Cisco operating systems and protocols are discovered and attack methodologies and code are developed. This is proactive security in action—if you do manage to grasp all the concepts in this book, you will never meet these emerging threats unprepared.

We don't know which path have you decided to take—it is your personal choice and personal responsibility. Just remember that the eternal information security battle is never fought between systems, protocols, or applications. In all cases, it happens between humans—attackers and defenders. And whoever knows and understands more will invariably emerge victorious.