

## LAN Switch Security: What Hackers Know About Your Switches

Review by Chris Gates, CISSP, GCIH, C|EH, CPTS

In addition to his regular column, Chris Gates does some great work on EH-Net including participating in our growing forums as well as doing various book reviews. He is back with a quick look at a recently released security title by Cisco Press that Chris describes as, "Should be required reading for Pentesters.&rdquo; So let's begin his review...

LAN Switch Security: What Hackers Know About Your Switches provides enough information to leverage the most common layer 2 attacks a pentester would be interested in; MAC Flooding, VLAN Hopping, DTP attacks, and CDP Snarfing along with plenty of switching protocol details for the Cisco ninja wannabe.

Free Sample Chapter Available Below - "Attacking the Spanning Tree Protocol"

[del.icio.us](#)

[Discuss in Forums {mos\\_smf\\_discuss:Book Reviews}](#)

"LAN Switch Security: What Hackers Know About Your Switches" By Eric Vyncke and Christopher Paggen, Published by Cisco Press. ISBN: 978-1587052569; Published: September 16, 2007; Pages: 360; Edition: 1st.

[Click here to download Chapter 2, "Attacking the Spanning Tree Protocol"](#)

With the exception of the white paper for the tool Yersinia there isn't much in the way of resources out there for conducting Layer 2 attacks and certainly nothing written to the technical level of LSS.

The discussion of Layer 2 attacks in the first few chapters of this book are excellent and easily worth the price of the book especially if you are responsible for securing switches or just breaking into and abusing them. Chapter 4's ("Are VLANs Safe?") discussion on Dynamic Trunking Protocol is probably the most valuable for pentesters. The chapter covers using Yersinia to (hopefully) turn the port the attacker is connected to into a trunk port. This enables the attacker to see all traffic on all VLANs (pretty handy). In addition to exceptional background material on switching protocols and information on breaking the different switching protocols the book gives us quality information on securing those same protocols to include a good chunk of the IOS commands to implement the recommended changes.

#### Pros

- All the chapters using Yersinia for attacks and the overview of Yersinia
- The structure (Technology Overview, Discussion of the Vulnerability, Remediation) of each chapter works well
- Plenty of Cisco IOS command line specifics to get the job done
- Really good overviews of the switching protocols, how to break them, and how to secure them
- Discussion of data planes and control planes

#### Cons

- Check out the cons of Richard Bejtlich & Stephen Northcutt...all valid
- No discussion of minimum lab requirements to set up a lab to reproduce the attacks
- I lost interest from part II onward, probably because most of the attacks don't give you much (if any) in the way of privileges and it got fairly deep into switching protocols I don't usually deal with and the book seems to drift. I'm not sure what happened but the book doesn't end as strong as it begins.
- Some repeating of material in different chapters

Rating: 4 Stars

I gave the book 4 stars mostly due to editing issues, lack of lab guidance to reproduce the attacks, and the fact that I lost interest in the book toward the end. Even though I lost interest toward the end I still recommend this book for anyone interested in breaking Layer 2 or securing it.

Chris Gates is an Ethical Hacker Network Columnist and VP of operations for LearnSecurityOnline. For his day job, he currently works as a penetration tester for a large government contractor. In the past he worked for the US Army as a

signal officer and over the years has worked with various satellite communications systems, worked with various deployable communications packages that allowed network connectivity in remote locations, served as a system and network administrator and as an Information Assurance Security Officer. Chris also holds his CompTIA A+, Network+, Security+ Certifications and is a Microsoft Certified Professional (MCP) for Server 2003.

Check out his blog:

<http://carnal0wnage.blogspot.com/>