

Book Review: Ninja Hacking

Review by Ryan Linn, CISSP, MCSE, GPEN

“Ninja Hacking,” the new book by Thomas Wilhelm and Jason Andress, is not a typical book about hacking and penetration testing. Experienced penetration testers who want to learn cutting-edge penetration techniques will find few references to little-known penetration tools or techniques presented in bland technical format. The book doesn’t rely on pun-filled humor, either.

Ninja Hacking is targeted at individuals who have an interest in the warriors of feudal Japan and want a serious philosophical exploration on how those warrior’s techniques map into modern cyber-warfare. For penetration testers who want to know how to be Ninjas, Ninja Hacking creates a framework for becoming a feudal Japanese warrior in cyberspace. Each chapter discusses a new piece of the puzzle, and, while you won’t achieve mastery from this book alone, the building blocks are laid that should allow an inspired reader to know what additional areas need to be researched.

Free Download Below of Chapter 5: Disguise

RUaNinja?

Test your ninja skills & win signed copies. See Forum Thread for Details.

del.icio.us

Discuss in Forums {mos_smf_discuss:Book Reviews}

Download Chapter 5: "Disguise"

Exclusive for EH-Net Readers:

20% Off All Syngress Books!!

Use Code: 50467

Without turning into a how-to manual, Wilhelm and Andress do a good job exposing the reader to the world of the Ninja and then mapping the cutting-edge skills of the leaders in penetration testing to those of the Zukin (the penetration tester who leverages unorthodox techniques). A good mix of history and hacking ensures even those who have no interest in the historical aspect will still get ideas for how to take penetration tests to the next level. This reference is broad enough to inspire almost everyone, but that breadth comes at the cost of not being deep enough to allow for expert mastery of any of the individual skills. By the end of this book the reader should know how to become the Ninja penetration tester and should be able to intelligently discuss the relationship between the feudal Ninja to the Ninjas of today.

The book is peppered with historical parables designed to shed light on modern security scenarios and stoke interest in the material. These scenarios may make explanation of aspects of penetration testing easier to understand for non-pentesters, and they should make experienced security experts think. The book covers a broad range of concepts, from contrasting the philosophies of the Ninja and Samurai classes using stories about specific feudal lords and clan leaders to examining the rules of engagement according to Sun Tzu's Art of War. Throughout, these researched components are not only used to examine concepts of penetration and defense but also to question the cookie-cutter methodologies found in many penetration tests. However, those who aren't interested in Ninjas can skip the first 2 chapters and go directly into the chapters about stealth and misdirection and will still be able to understand the references in most of the book.

By examining penetration testing using a point of view which is not bound by the traditional rules of war, Wilhelm and Andress are able to examine what sets apart traditional penetration testers from the leaders in the field. The authors do not focus on explicit programs or tools which grant the latter an advantage. Rather, they explain how the Zukin can achieve better results than a traditional penetration tester. Approaching a problem from the mindset of an intruder who wants to obtain access without being detected changes the field of play for penetration tests in significant ways that this book is not afraid to explore. Modern techniques for advanced information gathering, social engineering, misdirection, and even sabotage are defined as extensions of the Ninja philosophy for covert and open operational tactics. Discussion of disguise, impersonation, surveillance and social engineering begins with exploration of how these techniques were leveraged by the feudal warriors.

Overall, Ninja Hacking has excellent relevant material and a significant amount of Ninja lore and history. While this book is not a technical reference, it is an excellent choice for someone who has an interest in Ninjas or someone who is looking for inspiration to think differently about penetration testing and security concepts. The mappings for traditional Ninja skills to the skills of today are mostly well-coupled and are always relevant to how the leaders in the field are addressing security today.

Editing assistance provided by Heather Pilkington of the Infosec Insanity blog.

Ryan Linn, CISSP, MCSE, GPEN - Ryan is currently an Information Security Engineer at SAS Institute. Employed in the computer industry since 1997, he has held positions ranging from web developer to Unix Systems Programmer at a large university to his current position in Information Security. Ryan has been responsible for working with large scale deployments of various flavors of *nix, high availability web and database clusters, as well as for application programming in high availability environments. In the past few years, Ryan has incorporated Windows security into his responsibilities, and is now part of the team responsible for information security globally in one of the largest privately held software companies in the world.