

www.internetnews.com/commentary/article.php/3776876

[Back to Article](#)

No/Low/High-Tech Hacking: It All Matters

By Sean Michael Kerner

October 9, 2008

COMMENTARY: I spent a few days this week at the SecTor conference in Toronto, an event that isn't quite the Black Hat of the North (though maybe we could call it the Black Toque of the North). What made this event interesting for me is the mix of technology approaches discussed, ranging from no-tech hacking to the super-powerful, software-based methods.

Listening in to the various presentations, I came to a conclusion that may well be obvious, but still needs to be repeated. Whether no-, low- or high-tech, all methods of hacking need to be part of enterprise security efforts. Furthermore, it's unacceptable to simply think that hacking is just an offensive approach to security. As the old adage goes, the best defense is a good offense.

At the no-tech end of the scale, there is Johnny Long, who not coincidentally is the author of a book titled "No-Tech Hacking." At InfoSec, Long repeated a presentation he gave in 2007 at Black Hat Las Vegas, humorously detailing how, using the power of observation and the naiveté of others, he could profile people and gain access to supposedly secure buildings.

"We have a tendency to get so into the technology of the industry, that's all we can see," Long told the SecTor audience. "Solutions can be complex, but hackers need to be clever and they don't need to have tech. Bad guys can break your stuff without using technology."

It's an important lesson that Long preaches, from protecting your laptop from prying eyes (a technique Long referred to as "shoulder surfing") to ensuring that personally identifiable information is kept out of sight. Sure, it sounds like good, simple common sense, and it is -- so don't let it slide in your own organization.

In terms of low-tech hacking, the basic tool of perimeter security for most of recorded human history has been some form of lock (door lock, padlock or otherwise). In a standing-room only session at SecTor, security researcher Deviant Ollam (yes, he goes by that name) explained to the delight of the audience how easy it was to pick many common locks with simple tools.

Ollam noted that in the U.S., lock manufacturers have their own self-regulated rating system for the quality of locks, while in Europe, the rating system is regulated by police authorities. The difference, in Ollam's view, is that in Europe, there is great transparency about the security quality of a lock.

The point of the discussion was not so much a how-to on lock-picking, but rather, a wake up call about physical security. You can have safer and better locks that are more difficult for an attacker to penetrate. It's all a matter of awareness and choice.

From a purely IT perspective, remember that if your servers are behind a locked door and that door lock gets picked, well, those servers could be at risk from a low-tech hacker.

Physical and low-tech security approaches aside, there are high-tech approaches to hacking that are a real threat, too. The Metasploit Framework is an intricate technology approach to hacking that attempts to gain access from the packet level and upwards.

With the upcoming Metasploit 3.2 release that security researcher H. D. Moore discussed at SecTor, automating complex attacks against browsers, applications and wireless access points will actually become even more efficient.

Metasploit is not introducing new vulnerabilities that enterprises need to deal with. What Metasploit does is it makes vulnerabilities more transparent to enterprises by demonstrating how easy it is use known vulnerabilities to exploit a variety of technologies.

All of these no-, low- and high-tech hacking techniques need to be part of IT security considerations. Any one of them could be the proverbial "weak link" that topples an application or lets an attacker steal an identity. Rather than thinking negatively of some of these approaches as "hacker" tools, think of hacking in a more responsible security sense.

Don't wait for the bad guys to use their tools to hack your stuff -- use the tools to hack your own stuff to see where vulnerabilities may lie. Ignorance is not an option. You can empower yourself to make the right security choices to find and fix security issues whether they are simple or complex.

JupiterOnlineMedia.

internet.com

EARTHWEB



mediabistro.com

graphics.com

Search:

Find

Jupitermedia Corporation has two divisions: Jupiterimages and JupiterOnlineMedia

Jupitermedia Corporate Info

Copyright 2008 Jupitermedia Corporation All Rights Reserved.
Legal Notices, Licensing, Reprints, & Permissions, Privacy Policy.

Advertise | Newsletters | Tech Jobs | Shopping | E-mail Offers

Solutions

Whitepapers and eBooks

Microsoft Article: Will Hyper-V Make VMware This Decade's Netscape?
Microsoft Article: BitLocker Encryption on Windows Server 2008
Go Parallel Article: Intel Thread Checker, Meet 20 Million LOC
IBM Whitepaper: Innovative Collaboration to Advance Your Business
Internet.com eBook: Real Life Rails
Avaya Article: Call Control XML - Powerful, Standards-Based Call Control
Tripwire Whitepaper: Seven Practical Steps to Mitigate Virtualization Security Risks
Internet.com eBook: The Pros and Cons of Outsourcing
Internet.com eBook: Best Practices for Developing a Web Site

IBM CXO Whitepaper: The 2008 Global CEO Study "The Enterprise of the Future"
Avaya Article: Call Control XML in Action - A CCXML Auto Attendant
Go Parallel Article: James Reinders on the Intel Parallel Studio Beta Program
IBM CXO Whitepaper: Unlocking the DNA of the Adaptable Workforce--The Global Human Capital Study 2008
Adobe Acrobat Connect Pro: Web Conferencing and eLearning Whitepapers
Go Parallel Article: Getting Started with TBB on Windows
HP eBook: Storage Networking , Part 1
MORE WHITEPAPERS, EBOOKS, AND ARTICLES

Webcasts

Go Parallel Video: Intel(R) Threading Building Blocks: A New Method for Threading in C++
HP Video: Is Your Data Center Ready for a Real World Disaster?
Microsoft Partner Portal Video: Microsoft Gold Certified Partners Build Successful Practices
HP On Demand Webcast: Virtualization in Action
Go Parallel Video: Performance and Threading Tools for Game Developers

Rackspace Hosting Center: Customer Videos
Intel vPro Developer Virtual Bootcamp
HP Disaster-Proof Solutions eSeminar
HP On Demand Webcast: Discover the Benefits of Virtualization
MORE WEBCASTS, PODCASTS, AND VIDEOS

Downloads and eKits

Microsoft Download: Silverlight 2 Software Development Kit Beta 2
30-Day Trial: SPAMfighter Exchange Module
Red Gate Download: SQL Toolbelt

Iron Speed Designer Application Generator
Microsoft Download: Silverlight 2 Beta 2 Runtime
MORE DOWNLOADS, EKITS, AND FREE TRIALS

Tutorials and Demos

IBM IT Innovation Article: Green Servers Provide a Competitive Advantage
Microsoft Article: Expression Web 2 for PHP Developers--Simplify Your PHP Applications

MORE TUTORIALS, DEMOS AND STEP-BY-STEP GUIDES