

WANTED: ETHICAL HACKERS

MANILA, August 29, 2004 (STAR) By Eden Estopace - Hackers, worms, viruses, malware, trojans, denial-of-service attacks – in layman's lingo, these are some of the threats that plague computers and computer networks all over the world.

Even as spending on network security has steadily risen in recent years and has taken up a much bigger share of IT budgets, global businesses remain vulnerable and constantly at risk to security breaches.

Computer viruses are also "getting smarter" and as the methods of spreading attacks reach higher levels of sophistication, warding off attacks has become the indefatigable task of a whole army of computer experts in a corporate setting.

In a report published Aug. 9 by CMPnetasia.com, a Hong Kong-based business-to-business content provider, 4,677 new viruses were written in the first six months of 2004 or an increase of 21 percent over the same period last year, according to Sophos, an anti-virus vendor.

The report also cited data from Trend Micro, another anti-virus vendor, that computer virus attacks cost global businesses a whopping \$65 billion in damages last year, also a dramatic increase from \$20-30 billion in 2002.

Since enterprises themselves and the Internet are gold mines of information with commercial value – client details, e-commerce transactions, credit card numbers, confidential data and source codes – the bad guys in the computer underworld will also have reasons to break into systems, not to mention the thrill of bringing down highly protected IT powerhouses such as Microsoft, which has been constantly besieged by all sorts of sneak attacks.

In the Philippines, the havoc wreaked by the infamous "I Love You" virus unleashed to the world by a young misguided computer programmer in 2000, crippling Internet access and obliterating files all the way to the Pentagon, still left traces of shame and fear of these enterprising computer outlaws.

Of hackers and crackers

The hacker computer culture has gone a long way since a bunch of tech-savvy kids learned how to jam phone lines in the late 70s. That today's generation of technical outlaws has steadily progressed as technology evolves is hardly a surprise. From the relatively simple skills of monitoring private calls, stealing credit card numbers, spying on each other's computers, and tapping into other people's Internet connections, hackers have creatively, even if malevolently,

honed their skills enough to crash commercial sites, wipe out corporate files and pull off million-dollar frauds.

These so-called cyber criminals, unlike their counterparts in the real world, are prowling on the loose in the information superhighway, as laws and regulations in the electronic frontier still have a lot of loose ends.

In cyber lingo, there is actually a big difference between a "hacker" and a "cracker." One who has a very high degree of computer knowledge and skills and who puts this talent into good use by learning more about programming languages and evolving computer technologies and breaking into supposedly secure systems to expose their vulnerabilities is called a hacker. On the other hand, a computer expert who uses the knowledge for malicious intent is called a "cracker." The difference lies in the intent.

Security experts are one in saying that to strengthen a network's defenses against persistent security threats hounding the IT world, countering a hack is still one of the best options for warding off threats.

By understanding hacker methodology and familiarizing one's self with all types of attacks, risk management is made easier for security teams.

Also called penetration testing, counter-hacking is simply the process of assessing the security of an organization's network and examining its vulnerabilities using professional methodology. The goal is to prevent an attack on the network by plugging the holes or vulnerabilities that are normally exploited by hackers or crackers.

However, since the thin line that divides ethical or professional hacking and malicious hacking is not yet very well-defined, enterprises are still uneasy about this whole idea of ethical hacking. Hiring someone to crack one's network still gives companies some misgivings.

But in recent years, professional courses and certifications on penetration have ushered in a new league of computer professionals, the so-called ethical hackers or penetration testers.

Professionalizing penetration testing

What does it take to be an ethical hacker? An understanding of network services such as TCP/IP, database, Web and mail services, a good grasp of the working and configurations of firewalls, IDS and wireless networks, hands-on experience in administering Windows, Linux, Unix or Novell Netware, and an advanced understanding of computer networks, including architecture, design and implementation.

Not everybody though can be a professional and certified penetration tester. As a penetration testing professional course opens next month in the Philippines, training organizers Mile2 and Training.net, which recently teamed up to offer the pioneer Certified Penetration Testing Professional (CTTP) program in the country, are implementing a rigid screening procedure for prospective students.

"This is to ensure that applicants work for legitimate companies and will not use the newly acquired skills for illegal or malicious attacks and will not use such tools in an attempt to compromise any computer system," said Wayne Burke, director and security consultant of Mile2 UK who flew in last July to conduct a free counter-hacker seminar and workshop for Filipino IT professionals.

The course, he said, is ideal for IT and information system auditors, risk managers, network professionals, security officers and consultants and vendor-based security experts who need to acquire broader penetration testing skills.

The extensive hands-on course, to be delivered over five training days beginning Sept. 6, is developed to address the training needs of IT professionals who are responsible for penetrating, analyzing and auditing the security of a network.

What makes the program unique, said Burke, is that the methodology focuses on the "how-to" of penetration testing in a vendor-neutral setting.

After the training, participants can take the certification exam which will allow them to join the league of world-class certified penetration testers who are experts in the area of information security management.

A cursory look at the five-day training syllabus reveals a broad overview of hacking techniques and all the attendant security problems in the IT world. Hacking Technique I includes lessons in exploiting targeted systems or networks to test levels of security and simulate the results of a real attack. This include, among others, intrusion detection system testing, password cracking, denial-of-service testing, application testing, exploit research, port scanning and firewall and access control testing.

Hacking Technique II tackles vulnerability scanning or lessons in identifying weaknesses in devices connected to a network. The module also examines vulnerabilities in Windows 2000/2003, Linux, Novell Netware, database servers, wireless LANs, firewalls and IDS, Web applications and malware.

Depending on the response of the Filipino IT community to this high-level training-workshop, Mile2 and Training.net are also poised to introduce other advanced computer courses such as Digital Forensics and Electronic Training and Open Source Intrusion Detection Systems (IDS) Training.

Reported by: [Sol Jose Vanzi](#)

© Copyright, 2004 by [PHILIPPINE HEADLINE NEWS ONLINE](#)
All rights reserved

[PHILIPPINE HEADLINE NEWS ONLINE \[PHNO\] WEBSITE](#)