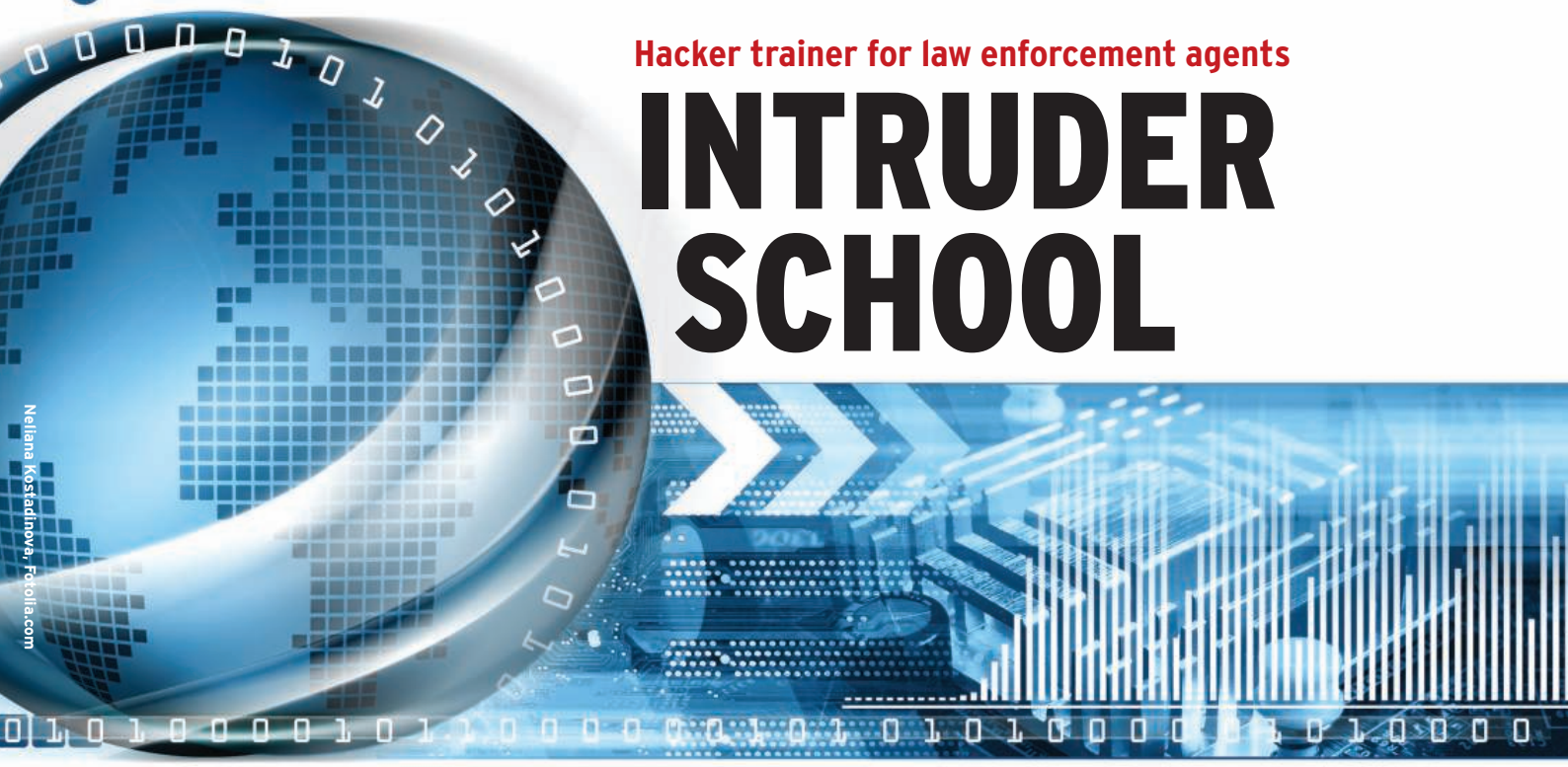

Hacker trainer for law enforcement agents

INTRUDER SCHOOL

A former intrusion specialist is training a gathering of European law enforcement agents in how the bad guys work on the Internet. Contributing editor Markus Feilner stops in for a lesson in attack techniques. **BY MARKUS FEILNER**

November 2008. Freiburg is supposed to be Germany's "sunniest city," but today, on my way to a special forensics conference, the rain is constant. Tobi, an ex-hacker who is now a forensics expert and trainer, is training 20 representatives from a smattering of European law enforcement agencies (Figure 1). The sessions over the next few days will cover topics such as rootkits, CSS scripting attacks, and browser compromise. The participants will also learn how attackers use professional software to create, distribute, and administer botnets, trojans, and viruses.

Even showing up for this event invites some legal risk. German law forbids such training. Yet many agencies feel it is impossible to maintain IT security without an understanding of the tools used by professional intruders.

The whole problem is that the criminal world isn't too worried about statutes. A well-trained and highly organized community of intrusion specialists even distributes user-friendly software to aspiring beginners so that anyone can get in the game. One of the agents groans, "By now, any mouse-pusher or script kiddie can practice his art at breakneck speed."

Eager to learn, the students set themselves an intense schedule for the next three days. Soon, the participants have words like Metasploit, MPack, and DreamDownloader reverberating through their heads.

Settling In

Tobi is visibly pleased with Linux Magazine's presence. The chemistry works; it takes no more than a minute before a greeting turns into a conversation about the advantages of the nVidia GeForce graphics card. However, it's not about games, it's about how the card's performance is especially suited for cracking passwords.

Companies from Russia and Eastern Europe, especially the older Soviet states, provide much of the sample hacker software Tobi is demonstrating in the course (Figure 2). For instance, ElcomSoft [1], which is headquartered in Moscow, makes a business of cracking passwords with the nVidia GeForce graphics card.

Admittedly, Tobi's first contact with law enforcement wasn't quite voluntary. When the Phatbot attacks were happening a few years ago, he was at the wrong place at the wrong time – that is, on the wrong server and under criminal police surveillance because he maintained contact with the malware originators. "Some of the guys behaved pretty badly, even bragging on the web! No wonder they were caught." Tobi survived the or-

Figure 1: Law enforcement agents from all over Europe learn from a hacker how to take control of Windows computers and build botnets.

Figure 2: In the foreground, Tobi; in the background is his adopted father, forensics expert Hans-Peter M., who won't keep his eyes off him for more than a second near his PC.

Figure 3: "Everyone leaves tracks, nobody is perfect": Swiss agents at forensics training in Freiburg, Germany.

deal, but you can tell the experience left its marks.

Tobi's hacker name is Newroot, and he writes his e-mail address like graffiti. These days, he works for one of Germany's leading pen testing and security service firms. At work, he hacks the newest aerotechnology software, outwits the firmware for VoIP phones, and informs international forensics experts about the newest software tricks.

Tools of the Trade

According to Tobi, "It takes just a few simple things to make it hard for attackers, but most admins aren't even aware of them. Just mount the right partitions with *nonsuid* and *nonexec*, and your attacker has a bad hair day. Or set the append-only attribute on logfiles or in the Bash history. It's hard to wipe away your tracks, especially when a cron job is picking them up on another system."

It doesn't take long before he starts listing a score of "gray area" websites that admins need to be aware of: InvisibleThings [2], Matasano [3], the Fake Name Generator [4], and the Milw0rm exploit database. He uses sites like these regularly in his training to build rootkits or demonstrate the newest Internet Explorer bug. Even seasoned Microsoft fans are speechless when Tobi shows, inside of two minutes using Metasploit or BackTrack, how an attacker on the local net can take over a Windows machine and get a full root shell on the MS server. Windows has enough back doors, says Tobi, that an attacker who knows the right websites can really do some damage [5].

To understand the damage introduced by client-side bugs and buffer overflows in the browser, Tobi introduces BeEF, the Browser Exploitation Framework [6]. BeEF is a professional tool designed to demonstrate the real-time effect of browser vulnerabilities. Tobi then directs the participants to the Open Web Application Security Project (OWASP) [7] [8].

The group studies the various ways to take control of a Windows client, examining the differences among stored, reflected, and DOM-based cross-site scripting [9]. Tobi also shows how to integrate a JavaScript script from a third web page and then leave the script in the guestbook of a foreign, unprotected site. With holes like the IFrame Tag Buffer Overflow Exploit in Internet Explorer, it's only a small step to take complete control of the Windows computer.

The agents take in the demonstrations with amazing calm. "Oh yeah, what we're seeing here is just the tip of the iceberg," one officer shrugs. "The reporting rate from victims is so pathetically bad because no one wants to admit they've fallen into a trap or that an attacker compromised their supposedly secure enterprise net."

His colleagues on the Swiss team (Figure 3) take a more positive approach: "Totally correct. But everyone makes mistakes. Every attacker, no matter how skilled, leaves tracks. That's where we come in." Denying the attacker a shell with admin privileges might make an attack more difficult, but Tobi shows that this isn't enough to thwart a determined intruder. The attack can still continue with help from professional solutions like MPack and DreamDownloader. "Redirecting the browser to your page is wonderfully transparent in the background over the IFrame tag, and the Windows user won't have a clue …. The port is open, and we can install whatever program we want." Even automation is easy. With a remote administration tool like Poison Ivy [10], execute a few mouse clicks, package the newly created trojan with DreamDownloader, infiltrate the Windows system with MPack, and you've got yourself a botnet.

Rainy Night

The training is almost over, and it's beginning to get dark in Freiburg; The rain won't subside. Why hasn't anyone hacked the weather? ■

INFO

[1] ElcomSoft: *http://www.elcomsoft.com*

[2] InvisibleThings: *http://www.invisiblethings.org*

[3] Matasano Security: *http://www.matasano.com/log*

[4] Fake Name Generator: *http://www.fakenamegenerator.com*

[5] E-learning CD for Web Security: *http://www.badstore.net*

[6] BeEF: *http://www.bindshell.net/tools/beef*

[7] OWASP: *http://www.owasp.org*

[8] OWASP Top Ten Project: *http://www.owasp.org/index.php/OWASP_Top_Ten_Project*

[9] Cross-site-scripting: *http://en.wikipedia.org/wiki/Cross-Site_Scripting*

[10] Poison Ivy: *http://www.poisonivy-rat.com*