SECURITY IS SEXY

By Darlene Storm | Follow

About |

Most security news is about insecurity, hacking and cyber threats, bordering on scary. But when security is done right, it's a beautiful thing...sexy even. Security IS sexy.

OPINION

Dirty little secrets revealed by ethical hackers

Computerworld | OCT 10, 2011 1:47 PM PT

Dirty little secrets can be the best kind, especially when revealed by insiders with the real scoop. This year, thanks to LulzSec and AntiSec hackers, there were numerous high profile sites attacked which highlighted poor security standards. The hacks were then followed up with postings of the pillaged digital dirt, acting like a global eye-opener for how very insecure companies are.

The inside of A list hackers are penetration testers, the ethical version of elite hackers who get to play like bad boys sneaking into a system. These ethical hackers pentest the security of networks or computer systems for potential vulnerabilities that could be used by malicious attackers. Some of my friends who make a living as pentesters enjoy the fact that they get to feel a bit dirty like black hats trying to break in, yet still get to be a white hat with noble intent.

At the security conference Derbycon last weekend, two ethical hackers Chris Gates (carnal0wnage), a Partner/Principal Security Consultant LARES, and Rob Fuller (mubix), a Penetration Tester at Rapid7, gave a very interesting talk called The Dirty Little Secrets They Didn't Teach You In Pentesting Class.

I had the pleasure of interviewing Chris Gates about Dirty Little Secrets for pentesters:

Did all the recent breaches and high-level of anti-sec attacks help prove the point that pentesting of old may not be dead but it seems to be "out-dated?" That traditional security assessment exploitation needs to evolve from the primary use of automated tools like vulnerability scans, or smash and grab tactics, to thinking like a stealthy attacker?

Gates: *I think so. Companies have become very good at catching their pentesters but horrible at catching real attackers in their networks. Thus the problem is obviously that we are doing a poor job training them with their pentests. At a minimum we need to perform data driven pentests where the goal is to obtain some piece of data in the network, but a better approach is a capability driven assessment where we emulate varying levels of attackers, see which one is successful, raise our defenses to detect and respond to that threat and then repeat the process.*

An attacker has persistence and determination to steal the data if they can. If the real goal is "to test the client's ability to detect and respond to various levels of attackers," does that mean security testing today should embrace more of an old-school capture the flag mentality?

Gates: Like Chris Nickerson (CEO/Founder of Lares) says "how do you know you can take [illegible] a fight?" Right now companies spar with the equivalent of a 5 year old after we place the scope restrictions and lack of a good "goal" for the testers. This essentially shapes the outcome of their pentest to the results and outcome they want and not necessarily an accurate view of the network or company's security posture. If you want to fight with the big boys you have to train your way up and not influence your test or sparing partner with undue restrictions. The Penetration Execution Standard (PTES) is working to address some of this, especially with the Threat Modeling section.

In regards to a better way to pentest, you list Intelligence Gathering, Foot Printing, Vulnerability Analysis, Exploitation, Post Exploitation, and Clean Up. Yet exploitation is much less important that post-exploitation. In fact, you give "exploitation" about the same importance as "clean up." Is that because an attacker will not necessarily stop after finding one vulnerability?

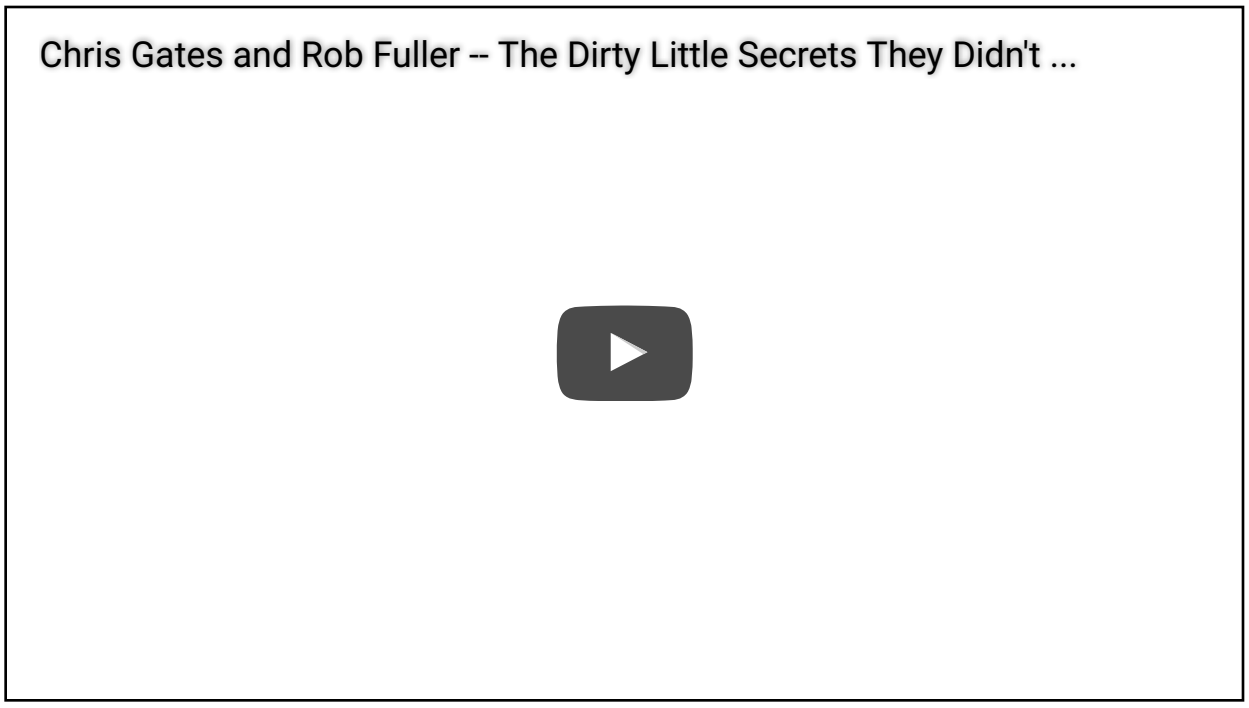
Gates: Right now because we are so vulnerability focused for our pentests, the number of vulnerabilities discovered/used/possible tends to overshadow what access I gain with those vulnerabilities, how those vulnerabilities got there, what I can get to or how long I stay in a network after I leverage those vulnerabilities. Attackers will do what it takes to get to what they are after instead of taking that missing patch, getting 200 shells with metasploit, taking a screenshot then hi-fiving their buddies and calling it a day. We tend to focus on throwing that screenshot of a metasploit shell in the report (Scan-->Exploit-->Report) instead of digging into a network to go after what makes the company money. Information Gathering, Footprinting, and Post Exploitation are highlighted in the talk because that's what attackers do and something most pentests DON'T allocate time for.

Post-exploitation includes focusing on the way attackers work such as searching for the gold, the "money shot." A stealthy attacker is going in for the "money" kill and may lurk there undetected for long periods of time while working on escalating privileges, locating the best data to steal, leaving a backdoor, moving data around laterally before actually making off with it. Is that the reason you shared all the slick tricks and best case scenarios in The Dirty Little Secrets They Didn't Teach You In Pentesting Class?

Gates: The first part of the talk on doing things differently is the most important part of the talk. The whole exploitation tips/tricks are merely a facilitator to the re-education of the industry to actually test like attackers operate.

You give numerous good, better and best scenarios. Are the "best" considered the "dirty little secrets" not taught in pentesting class?

Gates: The "best" stuff was the code Rob (@mubix) wrote to help us with pentests we were on. Like we said in the talk, do what works for you. If the new code helps you in tough spots...great!



The Dirty Little Secrets video above was also posted on IronGeek by Adrian Crenshaw who helps organize Derbycon. Previously we covered Crenshaw's wickedly hilarious Funnypots and Skiddy Baiting presentation. I hope you enjoy Dirty Little Secrets as well.

Image credit: Sophos

To express your thoughts on Computerworld content, visit Computerworld's Facebook page, LinkedIn page and Twitter stream.

Darlene Storm (not her real name) is a freelance writer with a background in information technology and information security.