WIRELESS SECURITY

HACKING THE HACKERS

Posted by Kent Woodruff in Wireless Security on Aug 31, 2011 10:54:57 AM

Hacker conferences are pretty interesting. The two big conferences, DEFCON and Black Hat, serve as a platform for hackers to get together, discuss their craft, party like rock stars, and occasionally share a bit of code. When you're attending a hackers' conference, you get a little careful about logging onto networks, but imagine *operating* a network at a hotel or conference center that's hosting a hackers' convention. It must be difficult for event planners to sell DEFCON and Black Hat to hotels and convention centers.

We found ourselves at DEFCON in Las Vegas a few weeks ago to see how our network security services would stand up to the hackers. Logging onto a network during DEFCON to see how your network security tools work is a little like stepping into a snake pit with a vial full of antidote you've created. You know you can trust your product, but still, you don't want to get bit.

The good news for us was, we didn't get bit too badly. There wasn't as much activity or threats on the network as we thought there might be, and we had a lot of opportunities to identify small threats quickly. For example, it used to be a big thing to put out proof-of-concept code releases, and the newly-acquired code would wreak havoc on networks nearby, but now we're seeing fewer attack tools coming out that impact the on-site network.

Gone phishing

There was one afternoon, though, were we got a run for our money. A workshop on wireless hacking included detailed how-to information, a live CD and some hardware. Twenty minutes after the workshop ended, we saw a flurry of activity on the network:

> *The two repeated attacks were AP beacon floods and what appeared to be a KARMA attack. In reviewing the packets, the AP flood appeared to be MDK3 running in default mode. Lots of spoofed MAC addresses and crazy SSID's. The KARMA attack didn't seem to include the backend setup required for a full blown Karmetasploit, sslstrip, driftnet or others, as we never received a DHCP response.*

If you can read that last paragraph fluently, then perhaps you're OK in defending your own networks from these kinds of attacks. If you need a bit more explanation. This particular attack was a phishing attack and it illustrated an important point: Phishing attacks like these focus on the client directly and circumvent the infrastructure. Most IT security people aren't necessarily looking at their Wi-Fi space, so even users who are on the wired network that leave their wireless card activated are really susceptible to this kind of attack.

Hacking is mainstream now

We learned a few things at DEFCON. There are some savvy hackers out there, and there are some savvy network security products designed to catch the hackers. It's a cat-and-mouse game that will continue for as long as there is code to write and networks to exploit. To keep up with hackers, we've got to pretend there's a DEFCON and a Black Hat conference every day, and constantly stay on top of the latest techniques the hackers are using to threaten the integrity of networks big and small.

We were glad to see how our latest updates performed under the pressure of DEFCON this year, and we're already working on tools to help the airspace around next year's show – and for every day in-between.

We'd be happy to put on our White Hat and show you how our security services can help you. Visit our Air Defense Solutions site for more information.

Note: On September 27, join Kent Woodruff and Andre Kindness of Forrester Research for a live webinar, **Exterminate Rogues from Your Network: Techniques for Comprehensive Rogue Detection and Elimination**. *Learn more about the webinar or sign up now to participate.*

49128 Views

Tags: wi-fi, wlan, security, wireless, breach, mobile, hack, hacking, attacks, services, enterprise_solutions, wireless_infrastructure, motorola_solutions, network_protection, netowrk_security_breach, wirless_security

0 Comments

There are no comments on this post