SCAN

Certification

New Software Security Cert Targets Managers

(ISC)² announced in late September a new software security credential that targets security architects, IT and project managers rather than strictly just coders.

The Certified Secure Software Lifecycle Professional cert has been in development for two years at (ISC)². It will be a standalone cert; holders do not need a CISSP to take the course. The first exam will be available in June; the program will be released in May.

"We're not trying to turn a security officer into a programmer," says new (ISC)² executive director Hord Tipton. "We want him to know enough about how software is developed, what best practices need to be in applications and be able to sit with a coder and explain why the extra time and money needs to be spent to implement a security best practice." ›

–MICHAEL S. MIMOSO

Malware

ISPs Dropping Hosting Provider Atrivo

Atrivo, an Internet hosting provider that has been accused by many of being a haven for malware suppliers, has been having a rough go lately.

Throughout September, the company was variously dropped by its upstream providers, brought back online and then dropped again. Company officials have denied repeatedly that they provide services to malware authors, but the Shadowserver Foundation found that more than 22,000 malware binaries were making connections to Atrivo's network.

Shadowserver also found that at least three botnets known to launch DDoS attacks were being hosted on Atrivo's network, and that there were only 11 other networks getting more connections from malware binaries than Atrivo. ›

–DENNIS FISHER

| Internet Security |

How to Pwn a Company Without Really Trying

Your network might have the latest and greatest security gear, go through penetration tests every quarter and be locked down tighter than Guantanamo Bay. But if your company or any employee has any sort of Web presence, Chris Gates can find a way in.

Gates, a penetration tester, is one of a growing crop of hired guns who are more like private investigators than typical security consultants and use nontraditional methods for gathering information on a target and finding ways into its network. At the ToorCon show in September, Gates said that with a little bit of know-how and an armory of freely available tools, today's penetration testers can get more information on a company and its employees than they can by using traditional security-assessment methods.

"You can do all of this without sending any non-standard traffic to the customer's network," Gates says.

Gates uses a variety of tools in his work, including email harvesters such as Goog-mail.py, and the program Metagoofil, which can pull metadata from Word documents, PDFs and other documents. The tool can identify the author of a document, who has edited it and even their email addresses, if they're available. But his favorite weapon is Maltego, an open source tool that gathers information on specific people or companies and finds the relationships between various targets. The application also displays the relationships in a variety of ways to graphically represent how various entities are interconnected.

"I can start with simple mail and name servers, get the names of all of the domains on those servers, move on to netblocks and so on," Gates says. "I can turn email addresses into real names, which can be very useful."

And very worrisome, if you're an IT security manager. ›

–DENNIS FISHER

EVENTS

Dec

FinSec 2008
www.misti.com/default.asp?page=65&Return=70&ProductID=7474
DEC. 2-3 • New York City
State of Arizona CISO David VanderNaalt and Jason Witty of Bank of America will deliver keynote speeches at this event designed for financial security professionals.

Data Protection: Securing Data in Motion, in Use and in Storage
Hosted by Information Security
http://events.techtarget.com/datatheft/?Offer=SEdpMevent12
DEC. 10 • Boston
This one-day event explores security and storage technologies that address data leakage, data protection and data governance.

SANS Cyber Defense Initiative 2008
www.sans.org/cdi08/
DEC. 10-16 • Washington, D.C.
Training includes pen testing and ethical hacking, forensics, auditing, Web app security, hacker techniques and training for the CISSP exam.