

Review: SANS SEC550 Information Reconnaissance

Review by Justin Kallhoff, CISSP, C|EH, GPCI, GCIH et al

SANS Security 550 - Information Reconnaissance: Competitive Intelligence and Online Privacy

A pessimistic view of the Internet: A network that enables every human to be within a few milliseconds from every psychopath and criminal on earth.

Bryce Galbraith of Layered Security, a SANS certified instructor, has authored a new one-day course titled "Information Reconnaissance: Competitive Intelligence and Online Privacy." The course is designed to educate IT professionals on the risks associated with information disclosure. It also teaches the students tools, tips, and techniques that assist in discovering information.

The amount of our personal information that exists on the web today is staggering; our governments, corporations, phonebooks, colleges, Facebook, MySpace, and Twitter, are all guilty. According to Google, it is estimated the Internet grows a billion pages per day.

del.icio.us

Discuss in Forums {mos_smf_discuss:/root}

This reality affects everyone, and as society becomes more and more dependent on technology, the opportunities and challenges of information recon continue to expand at an exponential rate:

- Sensitive data disclosure is practically a daily occurrence.

- Hackers and thieves revel in the information they can harvest about their targets.

- Governments labor to keep sensitive information from falling into the wrong hands.
- Businesses struggle to keep intellectual property within their inner sanctum.
- Parents worry about the safety of their children online... and everywhere they go.
- Predators seek out their next victim.

Source: <http://www.sans.org/>

The tools and methodologies that Bryce has illustrated in SEC-550 made the computer geek in me say, "Oh, that's awesome." On the other hand, when I did searches on myself and organization, my tone changed to "Oh no!"

Security 550 is full of useful tools and hands-on exercises. For example, I had not heard of <http://www.pipl.com/> prior to Bryce's course. There is nothing like having every address you have lived at for the past 10 years, every phone number you have had, every building permit you have ever obtained, along with your family members, appear in front of you as a result of a single search query on the Internet. Awesome or ugly, depends on your perspective. To quote Page 2 of the courseware, "Information is power!"

The ability to harness the power of information on the Internet has many purposes. As a penetration tester, I can use the tools and information I learned in Security 550 to target an organization or individual more thoroughly and accurately. As a security professional tasked with protecting an organization, it is important that you're able to keep sensitive information from being leaked that could be used against the organization.

The paradigm shift that has occurred in the threat landscape, whereby attacks are increasingly targeting client-side applications, changes the risk associated with e-mail address disclosures. According to the 2009 Symantec Global Internet Security Threat Report, "In 2008, 95 percent of attacked vulnerabilities were client-side vulnerabilities." This trend is continuing in 2009, with browsers and various Adobe applications being highly targeted by attackers.

Valid email addresses provide an attacker with an easy gateway to workstations where client-side vulnerabilities typically are prevalent. It is difficult for organizations to keep up with the quantity of workstations and the quantity of vulnerabilities found on them. Combine the operational complexity of patching workstations with the challenge of training humans on the risks associated with information disclosure, we security practitioners have a real difficult problem to solve.

Based on the results we've discovered during the penetration tests performed at Infogressive, it is apparent that most organizations are not aware of the information they have publicly available, nor do they understand how it could be used against them. For example, we typically discover a number of valid e-mail addresses for organizations we test. Security 550 covers many of the methods we use for discovering email addresses for a particular organization. Maltego, pipl, whois data, social networking sites, and Google hacking are all very effective methods for finding e-mail addresses.

Typical employees do not understand the implications of data leakage and information disclosure. With big organizations it is very difficult to prevent it from happening 100% of the time. So the task is to become aware of leaks and either remediate it or mitigate it before it is used against you. Security 550 teaches the skills to proactively find information disclosure occurrences before they become bigger issues.

Information disclosure and privacy will continue to become larger problems for our connected world. As Web 2.0 technologies continue to grow exponentially, we will continue to see tools created in order to mine that data quickly and efficiently. As with all tools, they will be used by good guys in addition to some less ethical sources for their nefarious purposes. SANS Security 550 will better prepare IT professionals for dealing with some of these challenges now and into the future.

Justin Kallhoff

CISSP, C|EH, GPCI, GCIH, GSEC, GISP, GCWN, GCFA

Infogressive, Inc. | <http://www.infogressive.com>

Justin Kallhoff is the CEO of Infogressive, Inc., headquartered in Lincoln, Nebraska. Infogressive is a security-centric information technology consulting firm. His focus as CEO is growth, his commitment in the office and in the field are the vital and nurturing forces fueling Infogressive's success. Mr. Kallhoff earned his Bachelor of Science from the University of Nebraska. He worked for Alltel in a variety of technology roles including data engineering for six years. He also worked for Information Technology, Inc., a division of Fiserv, where he worked with financial institutions from around the country. Prior to founding Infogressive in Nebraska, Justin was a security consultant in the Chicago area. In his free time, Justin is a member of the ISSA – Lincoln Chapter, SANS GIAC Advisory Board, the FBI's Infragard program, and the Lincoln Young Professionals Group. He is an avid sports fan, absolutely loves to travel, enjoys cooking, and attends as many “geek conferences” as possible.