Routine External and Internal "Hacking", An Important Part of Information Assurance

Introduction

One of Æsop's many fables was "The Hare and the Tortoise". In it, the Tortoise challenged the Hare to a race and the Hare, believing her assertion to be simply impossible, assented to the proposal; and they agreed that the Fox should choose the course and fix the goal. On the day appointed for the race the two started together. The Tortoise never for a moment stopped, but went on with a slow but steady pace straight to the end of the course. The Hare, lying down by the wayside, fell fast asleep. At last waking up, and moving as fast as he could, he saw the Tortoise had reached the goal, and was comfortably dozing after her fatigue. The moral of the story was that "Slow but steady wins the race."

Well, in the real world of information assurance, there is only a handful of "Tortoises" in the form of the systems administrators and security specialists, but hundreds of thousands of "Hares" in the forms of crackers, script kiddies, thieves and other undesirables. Slow and steady is only getting the "Tortoises" farther behind in the race against the legions of "Hares". In this case, fast and sneaky is winning the race. The good guys are generally overwhelmed by the myriad of ways the crackers continue to find to attack their systems and networks. They are in the defensive "fire fighting" mode while the crackers are still on the offense and picking up speed.
.

Now so far, I've only talked about outsiders who are trying to break into the firm's network and individual systems. There is also a whole slew of insiders who are trying to break into the firm's systems for devious purposes (and in many cases succeeding). Many people assume that the crackers are always outsiders but in a recent study of 1,238 companies, KPMG reported that 90 percent of the firms expected their e-commerce systems to be breached by crackers and warned that most attacks would be carried out by members of these firms' own staffs [1]. While you're busy guarding the front door, who is guarding the rest of the house?

It doesn't look good for the poor administrators and security officers unless they start enlisting the assistance of their own team of "hackers" to toughen them up, lend a helping hand and pick up their speed and stamina. Think of it this way, having what you believe to be good security in place is a lot like having what you believe to be a good disaster recovery plan in place. Unless you test it regularly, especially whenever you make changes to your operations, you just can't be sure that it will work as well as you believe it should.

Now why in the world would someone actually suggest that "hackers" are good for you when so many intrusion detection specialists, security officers and other members of corporate, university and government incident response teams work so hard to keep these kids, criminals and other low-lifes out of our networks and servers? Well for one thing, I'm using The Jargon Dictionary [2] term "hackers" which refers to a group of experts who enjoy the intellectual challenge of creatively overcoming or circumventing limitations without crossing the line into unethical or illegal activities. This contrasts sharply with "crackers" who enjoy breaking system and network security, vandalizing Web sites, committing theft and creating other havoc that systems administrators must deal with. I'll use these two distinctly different terms throughout this paper but in the general public, you'll have to get used to the idea that the terms "hackers" and "crackers" are used interchangeably.

If I'm Already Busy Trying to Keep Up With the Crackers, Why Do I Need Hackers?

That's an excellent question. The main reasons why you would want to have someone hack into your network or site from the outside using the same or similar tools as the crackers are to test the effectiveness of your router, proxy server, firewall and intrusion detection systems and to see if the hackers can break in through other means such as password cracking, back doors, social engineering or other means. If so, they will tell you in a detailed report just how far they were able to get and recommend ways to correct or at least reduce your vulnerabilities. This should give you an opportunity to fix the most significant vulnerabilities before a cracker takes advantage of them. By lending their skills to internal reviews of various in-house applications, they can also give you the unique perspective of what an "insider" might be able to do while you're busy guarding the perimeter against external crackers. Remember, most attacks are from the inside.

As the SANS Institute points out, a few software vulnerabilities account for the majority of successful attacks because the attackers are opportunistic, taking the easiest and most convenient routes first. Even so, SANS indicates that systems administrators have not corrected these flaws because they say that simply do not know which of the over 500 potential problems are the most dangerous, and they are too busy to correct them all. To help the administrators in this regard, SANS has published a continually updated "How to" for eliminating the ten most critical Internet security threats [3]. This should eliminate that excuse for many administrators but then again, ignorance is bliss.

Those threats currently include:

1) Berkeley Internet Name Domain weaknesses: nxt, qinv and in.named allow immediate root compromise;
2) vulnerable Common Gateway Interface (CGI) programs and extensions (e.g., ColdFusion) installed on Web servers;
3) remote procedure call (RPC) weaknesses in rpc.ttdbserverd (ToolTalk), rpc.cms (Calendar Manager), and rpc.statd that allow immediate root compromise;
4) RDS security hole in the Microsoft Internet Information Server (IIS);
5) Sendmail and Multipurpose Internet Mail Extensions (MIME) buffer overflows as well as pipe attacks that allow immediate root compromise;
6) sadmind and mountd;
7) global file sharing and inappropriate information sharing via Network Basic Input/Output System (NetBIOS) and Windows NT ports 135->139 (445 in Windows 2000), or UNIX Network File System (NFS) exports on port 2049, or Macintosh Web sharing or AppleShare/IP on ports 80, 427, and 548;

8) user Ids, especially root/administrator with no passwords or weak passwords;
9) Internet Message Access Protocol (IMAP) and Post Office Protocol (POP) buffer overflow vulnerabilities or incorrect configuration; and
10) default Simple Network Management Protocol (SNMP) community strings set to ‘public’ and ‘private’.

The extent of this “hacking”, who performs it and how often it is done is for the most part a resource question but this is not an area where you want to be too conservative. If you contract with an outside firm but define a very narrow scope assignment and bring in the lowest bidder as usual, you will get exactly what you paid for. In addition to the financial folks, your security and systems administration staff might actually be happy with the results because it will probably show very little and give the mistaken impression that everything is OK. What a waste.

There is also a question of whether you only want a “white hat test”, which is defined by some people as making use of commercial off the shelf (COTS) tools, a “black hat test” which makes use of actual cracker tools and techniques or a “grey hat test” that combines various features of white and black hat penetration testing [4]. I myself favor grey hat testing since it more thoroughly checks your operating environment against the wide array of attacks it may be subjected to on a daily basis. Of the COTS packages, the most well-known and one of the best is Internet Security Systems’ Internet Scanner. While not a cracker tool or a COTS, Nessus Security Scanner is very close to Internet Scanner in capability [5]. Some of its key developers are in NASA and Sun Microsystems so this open source software has a solid backing. With a limited amount of key word searching on your browser, you will find a large selection of COTS and cracker/hacker software.

My suggestion is that if you don’t already have an in-house hacking capability, you assemble a small team for this purpose, have them all at the very least attend the SANS GIAC Security Essentials course (and preferably the entire GIAC series), and then contract with an outside firm to have them attend an advanced, full-fledged penetration audit/hacking course. This course should preferably give the participants hands-on experience in hacking into a test or (under very controlled, supervised conditions) production network and let them each bring a portable computer full of hacker/cracker software back with them. The idea is to obtain the expertise and tools from an outside firm and bring them in-house for constant use and updating.

In my brief Web search, I found three firms that offer this type of training. Ernst & Young (E&Y) Security Professionals offers a five day, $5,000 per person “Extreme Hacking – Defending Your Site” course at various locations (or on-site if 18 or more individuals from one organization are attending) [6]. E&Y indicates that a strong understanding of TCP/IP and familiarity with both NT and Unix operating systems is required to attend the course. Foundstone, Inc. offers a four day, $3,500 per person “Ultimate Hacking: Hands-On” course (as well as a two day, $1, 995 mini-course) at various locations [7]. Attendees in the Foundstone courses need not be security experts, but one attendee, David Raikow, wrote an article that among other things, emphasized that without a good working knowledge of Windows and/or Unix networking concepts, students will quickly fall behind [8]. Finally, Canaudit, Inc. offers a four to five day, $12,500 per class

"The Ultimate Penetration Course" that has no prerequisites and is conducted on-site in order to have a team of your own security and audit personnel learn how to conduct a full penetration audit by actually conducting one on your network under the close supervision of the Canaudit instructors [9]. Canaudit also offers a four day, $945 per person course at various locations [10]. Mr. Raikow made another good point in that after you have trained this team, they will be eager to test their new skills and maybe even show off a little [8]. He said that this should not only be expected but also encouraged. He added that the team should also eventually get in the mode of testing new defensive techniques and equipment for the security and systems administration personnel before deployment. He therefore emphasized, and rightfully so, that the organization will need an "isolated test network" or laboratory to try new attacks and defenses without placing the production environment at risk. As we have covered in the GIAC Security Essentials class, even the most experienced hacker can accidentally crash a production system with even the most simple test. Doing such a test without the proper authorization is therefore just asking for trouble regardless of your intent.

The idea of having in-house hackers is not a new concept and the need for this helping hand has never been greater. In their 1995 paper, "Improving the Security of Your Site by Breaking Into it" [11], Dan Farmer and Wietse Venema emphasized that every day all over the world, computer networks and hosts are being broken into and that systems administrators are often unaware of the dangers presented by anything beyond the most trivial attacks. As the title suggests, the gist of their paper was that the best way to protect your own environment is to learn as much as possible about how it will probably be attacked, conduct the attacks yourself to learn what evidence they leave behind, and harden your network/system to prevent further attacks to the extent possible. However, in a recent interview on GIAC certification, Stephen Northcutt indicated that fewer than one in twenty security professionals has the core competence and the foundation of knowledge needed to perform their jobs and that most systems administrators have never been trained in security [12]. It's extremely difficult to conduct an attack yourself and learn from the experience if you don't know what you're doing. In fact, I believe that in order to maintain the proper separation of duties within an organization and to guarantee objectivity, individuals responsible for systems administration and security cannot also be responsible for penetration testing and other hacking and assurance functions.

Well great, now that you've spent a considerable amount of money to train a team of "hackers", set up a test network and possibly have a thorough external penetration test conducted, what else should you expect to obtain for your investment? The answer is three-fold. First, you can schedule periodic external penetration audits to ensure that previously discovered vulnerabilities have been resolved and that vulnerabilities covered in recent advisories have been addressed in the organization's operating environment(s). Second, you can use this capability in conjunction with normal information technology audits and security studies to ensure that the threats presented by "insiders" don't allow them to take advantage of vulnerabilities to exploit the organization's systems and applications for their own personal gain. Third, you give the security and systems administration personnel a helping hand in keeping track of security advisories, in "hardening" their servers and networks against attacks, in testing the effectiveness of their intrusion detection systems and as mentioned above, in testing new defensive techniques and equipment.

How can you keep this team staffed once it is set up? Attracting people from the outside consulting and penetration testing/audit firms or even from other organizations with their own hacking teams is probably out of the question since they are generally well paid, well traveled and well trained. For example, the Federal government has started a " Federal Cyber Service: Scholarship for Service" program where it offers $8,000 per year undergraduate scholarships and $12,000 per year graduate scholarships for two years of information assurance training. Upon graduation, recipients are required to work for a Federal agency for two years in a job that involves ensuring the protection of the U.S. information infrastructure [13].

You will probably have a lot of interested people from inside the organization since there is a considerable amount of prestige, fun and excitement associated with being a hacker. These in-house folks may in fact be your best bet assuming that you are willing to devote the training resources to bring them up to speed on information assurance and allow them to keep up-to-date on advances in software, hardware and techniques.

Hiring hackers straight from college (and even from high school) is one alternative since many of them probably know more about microcomputers, the Internet, Unix, NT and networking in general than many of the so called experts you already have on board. There is always considerable discussion about the wisdom of hiring a hacker/cracker because of the question of being able to trust them [14] and the fine line that exists between ethical/legal behavior and criminality [15]. The idea here is to find someone who appears to know the difference and who hasn't obtained a criminal record during this learning curve.

You have to remember that a good hacker would make an excellent cracker if it wasn't for the fact that they are ethical and remain within the law (or more realistically, they seldom cross the line and try not to leave a trail). When they **do** do things for the organization that would otherwise be unethical or illegal, they cover themselves with contracts, agreements, policies, procedures, job descriptions or other binding documentation that clearly shows that this is an unusual situation in which the organization **wants** them to do these things as a routine or one-time test.

Whether you bring people into the penetration testing team from within the organization or from the outside, this fine line between hacking and cracking makes it very important that you conduct thorough background checks on them as a condition of this assignment and that you ensure that there are detailed organization charts, job descriptions, policies, procedures, non-disclosure agreements and other documents that clearly define the "who, what, when, where and why" limits to their work. Members of this group will be tempted to "test" areas on their own just for the fun of it or to see if they can perform a successful penetration, so it must be very clear that they cannot use their status as team members to "freelance" or otherwise hack without specific authorization. That would be equivalent to "cracking" and would have to be dealt with firmly to ensure that these talented people know where to draw the line.

So how do you keep them productively busy in between hacking assignments? That's the easy part. Like good "Crackers", the team should be spending a considerable amount of time researching new hacking/ cracking tools and monitoring Usenet newsgroups on this subject. They should also be monitoring the Whitehats penetration testing, intrusion detection and network defense forums [16], distributing advisories on viruses, Trojan horses, worms, hoaxes, etc. throughout the organization, and ensuring that security and systems administration personnel are aware of security-related vendor advisories. Finally, the team will need to maintain their own test network to ensure that it at least comes close to duplicating the organization's production environment.

If anything, these individuals will be overworked but believe me, they will love every minute of it. Where else would they have a chance to be the good guy, the bad guy, the expert technician and the auditor all rolled into one? This is it. But you must be careful. If they're really good at it, their ego won't fit through most 36" doors!

Bibliography

[1] Neal, David (4/9/2001), Hackers work from within, ZDNetUK, http://www.zdnet.co.uk/news/2001/14/ns-22143.html

[2] The Jargon Dictionary, The Jargon File, version 4.2.2, (8/20/2000), http://info.astrian.net/jargon/

[3] How to Eliminate The Ten Most Critical Internet Security Threats, The Experts' Consensus", Version 1.32, (1/18/2001), http://www.sans.org.topten.htm

[4] Gula, Ron (July 1999), Broadening the Scope of Penetration Testing Techniques – "The top 14 things your ethical hackers for hire didn't test.", http://www.network-defense.com/papers/pentest.html

[5] Forristal, Jeff and Shipley, Greg (1/8/2001), Vulnerability Assessment Scanners, Network Computing, http://www.networkcomputing.com/1201/1201f1b1.html

[6] Ernst & Young eRISK SOLUTIONS, Extreme Hacking – Defending Your Site, http://www.ey.com/global/gcr.nsf/US/Extreme_Hacking_-_eSecurity_Solutions_-_Ernst_&_Young_LLP

[7] Boss, Shira J. (March 26, 2001), Companies Send Employees to 'Hacker' Workshops, Infowar.com, http://www.infowar.com/hacker/01/hack_032601b_j.shtml

[8] Raikow, David (April 10, 2001), Back to School, With a Vengeance, ZDNet, http://www.zdnet.com/filters/printerfriendly/0,6061,2706247-79,00.html

[9] Canaudit, Inc. Audits, Seminars, Consulting
http://www.canaudit.com/index.htm

[10] Canaudit Professional Development Weeks brochure,
http://www.canaudit.com/FTPRoot/ProWks.zip

[11] Farmer, Dan and Venema, Wietse (1995), Improving the Security of Your Site by Breaking Into it", http://pulhas.org/docs/improve_by_breakin.txt

[12] Can Security Certification Make a Difference? An Interview with Stephen Northcutt, SANS GIAC, http://www.sans.org/giactc/cert_dif.htm

[13] Federal Cyber Service: Scholarships for Service (SFS), A Federal Cyber Service Training and Education Initiative, NSF 01-11,
http://www.nsf.gov/pubs/2001/nsf0111/nsf0111.htm

[14] Sehn, Chad (August 22, 2000), Hackers and Crackers: Who Can We Trust", SANS Institute Information Security Reading Room,
http://www.sans.org/infosecFAQ/hackers/hackers.htm

[15] Thejian , Issues: Hiring hackers, the fine line between cult and criminal, Help Net Security, http://www.net-security.org/text/articles/thejian/hiring.shtml

[16] Max Vision's WHITEHATS forums, tools and arachnids database,
http://whitehats.com/index.shtml