Global Information Assurance Certification Paper

Jim Sherrill
SANS Security Essentials GSEC Practical Assignment Version 1.2e

Title
Oh Answer, Where Are Thou? or Gee, There's a Lot to Know

Main Text

I am new to this industry and I consider it a daunting landscape. Information Security is the never-ending process of trying to assure the confidentiality, integrity, and availability of your stuff. Why "never-ending?" Because the softwares, hardwares, configurations, vulnerabilities, and people *change*. These changes will probably modify the perceived risks and therefore we have to act. There are multiple threats to every aspect of information, for example, our servers could be hacked in many ways. People, insiders or outsiders, could:

- Gain access to a workstation and attack the server
- Hijack an inside computer's modem connection to the Internet and bypass the firewall completely
- Install a sniffer device on a network wire and capture password and other packets
- Boot an operating system from a bootable CDROM and change, copy, or delete any file
- Fool someone into revealing server passwords ("I am trying to verify last night's backup and I have to log in as admin - can you help me get into the box?")
- Create web or mail traffic that gets through the firewall and affects workstations or servers
- Entice an employee to visit a web page that captures the name and password entered by the employee and then use this information to gain access to the servers
- Unplug the servers and walk out the door

Some ways are harder and less probable than others, but even more server attacks are possible. Now, let's consider many threats to other information elements, such as e-mail, web, domain name service, router, firewall, server and desktop operating systems, business applications, virus scan, backup, recovery, document storage, credit card readers, accounts receivable and payable, air conditioning controls, distributed process control systems, computer-controlled manufacturing tools, packaging, shipping, telephone, building security, fire warning and suppression, power distribution, an so on. Ow, my head hurts - but this list of elements is not even close to complete!

The SANS instruction drilled the defense-in-depth concept deep into my brain but these layers of risk-reducing defenses must change with the threats. So we have to

build up the defensive layers and then continually monitor the results and risks. Then, based on business decisions or industry best practices, we must modify, replace, or add layers.

The telegraph lasted over one hundred and fifty years, from early experiments in the late 1830s to its last uses in Mexico in 1992. The telegraph dramatically increased message velocity, up to ten words per minute in early practice. Likewise, the various media that we enjoy and endure, especially the Internet, have increased communications to incredible rates. Both telegraph and typical Internet transmissions, however, provide no assurance about the quality or accuracy of the transmitted information.

However, a large number of web sites provide information that helps everyone, good and bad. I searched for hacking information and I was nearly drowned by the resulting lists of sites. For example, see:

http://infosyssec.master.com/texis/master/search/+/Top/Computers/Hacking.

Here is a list of the "top 50" (measured by who?) hacking sites, including enthusiastic banners like “Download Trojans!”

http://www.cyberarmy.com/t-50/index.shtml

The bad guys naturally use the hacking information and tools to break into systems and then view or use the resources. The good guys have to use this knowledge to increase the security of their resources and reduce the risk of loss. Some of the information that I found is outdated for most organizations, like ways to hack into a standard installation of Windows NT 3.5.1, but every site also had relevant information about current systems.

Many sites offer advice on hacking, such as getting around firewalls. One site handily informs us that the major categories of getting through firewalls are:

> Insider: There's someone inside the company (you, girl/boy-friend, chummer) who installs the backdoor. This is the easiest way of course.
>
> Vulnerable Services: Nearly all networks offer some kind of services, such as incoming email, WWW, or DNS. These may be on the firewall host itself, a host in the DMZ (here: the zone in front of the firewall, often not protected by a firewall) or on an internal machine. If an attacker can find a hole in one of those services, he's got good chances to get in. You'd laugh if you'd see how many "firewalls" run sendmail for mail relaying ...
>
> Vulnerable External Server: People behind a firewall sometimes work on external machines. If an attacker can hack these, he can cause serious mischief such as the many X attacks if the victim uses it via an X-relay or sshd. The attacker could also send fake ftp answers to overflow a buffer in the ftp client

software, replace a gif picture on a web server with one which crashs netscape and executes a command (I never checked if this actually works, it crashs, yeah, but I didn't look through this if this is really an exploitable overflow). There are many possibilities with this but it needs some knowledge about the company. However, an external web server of the company is usually a good start. Some firewalls are configured to allow incoming telnet from some machines, so anyone can sniff these and get it. This is particulary true for the US, where academic environments and industry/military work close together.

Hijacking Connections: Many companies think that if they allow incoming telnet with some kind of secure authentication like SecureID (secure algo?, he) they are safe. Anyone can hijack these after the authentication and get in ... Another way of using hijacked connections is to modify replies in the protocol implementation to generate a buffer overflow (f.e. with X).

Trojans: Many things can be done with a trojan horse. This could be a gzip file which generates a buffer overflow (well, needs an old gzip to be installed), a tar file which tampers f.e. ~/.logout to execute something, or an executable or source code which was modified to get the hacker in somehow. To get someone running this, mail spoofing could be used or replacing originals on an external server which internal employees access to update their software regulary (ftp xfer files and www logs can be checked to get to know which files these are). (van Hauser)

Want to crack passwords for most popular programs? No problem, you have plenty of help, such as Joe Peshel's Key Recovery Page: http://members.aol.com/jpeschel/crack.htm . How about steganography? Neal Johnson provides much content and links at: http://isse.gmu.edu/%7Enjohnson/Steganography/ .

A Problem

As an example of a hole in defense-in-depth, I gathered all of this information from behind a firewall. This firewall is configured to block access to sites in a "Hacking" category! My successful surfing is more evidence that defense in depth is necessary and insufficient to reduce risks. To provide sufficiency, we have to combine three elements:

- Best practices
- Continuous monitors
- Frequent updates

No individual security element, such as our firewall's prohibited website database, can completely protect even parts of our information. To add more depth to this particular defense, we have to

- Create a policy that describes acceptable use of Internet access

- Educate employees about the policy (who, what, when , where, and why)
- Enforce the policy as written
- Monitor attempts that the firewall policy denies
- Track web sites that the firewall allowed (or at least try to)
- Update the denied sites database regularly
- Send in allowed sites that should be blocked to the database vendor
- Watch for, evaluate, and use improved methods of controlling web content

We have to create a similar task list for each element in the defense layers. Ow, my head hurts again. But, too bad, because that is the price to pay for "information security" and all the risks that our definition of this phrase creates.

More Topics
Let's review e-mail, the mainstay application of computers. Peter Gutmann outlines the same main requirements that SANS teaches:

- Confidentiality
- Authentication
- Integrity

He then adds other requirements which are applicable not only to e-mails but also to other business documents and transactions:

- Non-repudiation
- Proof of submission
- Proof of delivery
- Anonymity
- Revocability
- Resistance to traffic analysis

Many of these are difficult or impossible to achieve (italics added) (Gutmann)

Other than "difficult or impossible," we are in good shape.... Using best practices, seeking new solutions, and using these improved technologies are mandatory in e-mail and all other information elements. Of course, the new technologies have new threats and so the cycle must continue.

What about social engineering? Social engineering is similar to the "con-man hustles," like in the movie *The Sting* or Rasputin's influence over Tsaritsa Aleksandra. This gaping security hole exists because humans generally want to be helpful. People do not often question someone who asks for assistance or someone who sounds or looks

like they are in power. Even the appearance of belonging (like wearing the appropriate clothing for an inside salesperson/mechanic/director) erodes suspicion, causing people to not question a stranger's appearance. For example, so many contractors flow through our buildings that unless we enforced our Visitor Policy, we could not tell who was an employee, contractor, casual visitor, or criminal. Naturally, there are holes in the policy that we cannot fill; someone could gather the policy details from an employee through social engineering techniques ("Hi, I had a meeting with the Director of HR about the copier maintenance, what was his name? Oh, that's right, Bill, well, he told me to get signed in but...") and then fake their way in as a copier repair person. Of course, even with our policy, we are not really sure of who is who. We cannot rest 100% assured that we are secure with our policy, but it makes the bad guy's job harder. Because this threat is caused by a common human trait, as opposed to a technology, I consider social engineering to be the most dangerous and long lasting threat.

In an interesting paper on the psychological elements of social engineering, Rusch describes six factors that help accomplish social engineering feats, using "peripheral routes to persuasion."

- Authority - being obedient to higher powers
- Scarcity - wanting something that is in short supply or only available for a limited time
- Liking and similarity - liking those who are like you
- Reciprocation - wanting to pay back someone, even if we did not ask for what we got
- Commitment and consistency - carrying out your promises
- Social proof - seeing what others are doing or saying (Rusch)

You cannot even trust some authentic-looking web pages - visit the test link at http://www.thetopoftheworld.com/spartanhorse/ to see an example that would probably not succeed against those in the information security business, but since it would work on a large number of people that we support, the problem remains ours. Many sources promote training as the best defense for social engineering but I think that this defense must include education and experience. Most training consists of a session with projected slides, a notebook with copies of the slides, and a presenter, hopefully a subject matter expert. To increase the likelihood of learning the content, the teacher has to engage the audience by allowing participation. The audience should be able to make comments and discuss the topics. Real examples bring the content to life. For example, sending a test virus to all employees, after proper permission and warning, could vividly demonstrate the effective level of an employee's virus protection.

The virus world provides more concrete examples of how defense-in-depth and social engineering can collide, with sometimes expensive results. I started using computers in 1988 and I "got" two viruses in ten years; both were harmless Word macro viruses which I got from infected files on floppy discs. In contrast, modern worms like I LOVE YOU and W32.Sircam.Worm@mm spread with a nearly exponential growth (at least until countermeasures slow the spread). These malicious code payloads spread much

too fast for the anti-virus products to stop immediately. As fast as these anti-virus experts are, they cannot stay ahead of threats that they do not know about. With a strong router, firewall, and anti-virus policy, employees will still double-click attachments that can contain harmful code. Why?

"As long as there are users who can be fooled, malware will continue to plague us. So far we've been very lucky that the malware has been largely benign and too primitive to avoid even the most trivial forms of detection." (Curtin, Ellison, & Monroe)

They propose multiple steps (not just "training") to reduce the tricking of "users":

> Educate
> People who use computers need to understand the risks associated with computing. Some will resist, saying they need not know what the difference is between a Word document and a VBScript file in order to accomplish their jobs. They must be corrected and helped to understand the need to compute responsibly.
> Guide
> People who use computers need to be guided. That means a clear articulation of policy. Buzzword-laden corporate newspeak does not count. Rather than trying to cover every single case, establish general principles that easily translate into practices, without regard to the technology that happen to be popular at the second that the policy was drafted.
> Assist
> Only after the users have been educated and guided will technology be able to help curb the flow of malware. Technology itself can always be circumvented by users, so do not attempt to skip directly to this step. (Curtin, Ellison, & Monroe)

Conclusion

We reviewed the complex environment of information security and looked at several elements of security practices. The Internet serves a double-sided sword role, providing large amounts of both information and threats. But people also act in the double-edged role: they can build sturdy, secure systems and they can also topple them by falling prey to social engineering attacks. Only diligent and continuous cycles of do, study, and improve (for people and systems) will reduce risk to acceptable levels.

References

van Hauser. “Placing Backdoors Through Firewalls v1.5.” URL: http://www.xillusion.net/home/firewall/Backdoors%20in%20Firewalls.htm (25 Jul 2001)

Rusch, Jonathan. “The "Social Engineering" of Internet Fraud.” URL: http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm (24 Jul 2001)

“CIAC Notes Number 94-03a 94_07_06.” URL: http://www.ciac.org/ciac/notes/Notes03a.shtml#Engineering (24 Jul 2001)

VIGILANTe.com, Inc. “Social Engineering.” URL: http://www.vigilante.com/inetsecurity/socialengineering.htm (24 Jul 2001)

Gutmann, Peter. University of Auckland. URL: http://www.cryptoapps.com/~peter/part3.pdf (25 Jul 2001)

Berg, Al. “Cracking a Social Engineer.” URL: http://packetstormsecurity.org/docs/social-engineering/soc_eng2.html (25 Jul 2001)

Harl. “People Hacking: The Psychology of Social Engineering.” 05/07/97 URL: http://cybercrimes.net/Property/Hacking/Social%20Engineering/PsychSocEng/PsySocEng.html (24 Jul 2001)

Curtin, Matt. Ellison, Gary. Monroe, Doug “Why Anti-Virus Software Cannot Stop the Spread of Email Worms” May 11, 2000 URL: http://www.interhack.net/pubs/email-trojan/ (23 Jul 2001)

“Milestones in Telegraphic History.” DOTS and DASHES, Volume XV Nos. 1-4, 1987 URL: http://members.tripod.com/morse_telegraph_club/images/newpage1.htm (24 Jul 2001)

Palace Biographies: Rasputin URL: http://www.alexanderpalace.org/palace/Rasputin.html (25 Jul 2001)