Global Information Assurance Certification Paper

The virtues of Security through Obscurity

Joseph V. Gibbs III
October 18, 2000

A Good Idea

Way back when, in the pre-dawn of computer security, people began to wonder how to protect their data. “Well,” someone might have said, “computers are complex and hard to understand. They probably won’t even be able to use it, let alone find my data.” Similar ideas continued to emerge and become popular, like running services at odd port numbers or keeping cryptographic algorithms secret. Even today, many people take comfort in the knowledge that they are “too small to notice”, “too hard to find”, or “just don’t have anything worth stealing.”

Or Perhaps Not

As it turns out, things don’t really work that way. Most crackers, even if not formally educated, are very comfortable on computers and tend to posses a vast working knowledge of their target systems. But intimacy with the nuances of TCP/IP is not necessary; script kiddies are testimony to that. One well-versed individual creates a tool, and suddenly there is a host of well-armed attackers beating at your doorstep (or more accurately, slipping effortlessly through the cracks!)

A simple port scan will locate services at odd ports. A small business that has a web page but does not conduct e-commerce may not have anything to steal on that network, but what about a denial of service attack? What if that web page is altered to contain incorrect, illegal, or slanderous content? Home users connected via cable modem or DSL are sure that no one wants to attack them until they find that their box is hosting an IRC server for crackers, or worse, actively scanning and attacking other sites.

But then Again

Clearly, there is no security to be obtained from obscurity, right? But it sure was nice to see that the Pretty-Park virus didn’t know what to do with the obscure, freeware mail client that my wife was using when that nasty critter showed up on our doorstep. I think she had to Cntrl+Alt+Delete to kill the runaway process, but that was it. On the other hand, Norton didn’t stop it either. At least not until I tried to save it to disk to scan it manually. Then I got all kinds of warnings! Granted, we were just lucky, but perhaps obscurity deserves a second look. In fact, two weapons in the modern security professional’s arsenal use obscurity: NAT and split DNS.

Network Address Translation (NAT) can be used to hide your entire IP address space from the rest of the world. This allows you to connect out and use the Internet as you please, but attackers cannot reach into your precious network by initiating a connection from outside the NAT.

Split-DNS is a security technique for the domain name service (DNS) where two DNS servers are used with the purpose of hiding the names of the hosts in your internal network while still providing enough information that customers can reach the hosts you want them to see.

Both of these techniques are designed to hide information from the would-be attacker. Sure, once the attacker gets behind the box running NAT and/or reaches the internal DNS server, he has access to all of the information you were trying to hide. However, he must spend time probing and such after penetrating your network. Had this information been publicly available, he would already know which internal hosts he wanted to attack, come prepared, and move immediately. Hopefully your intrusion detection system (IDS) detects the attack and your security staff has time to follow the documented security policy while the attacker is wasting time trying to find his next target.

Defense in Depth

So maybe you cannot bet the farm on obscurity, but smoke and mirrors can definitely play a part in your defense-in-depth strategy. Let's take a look at other ways obscurity is used to supplement many of the security mechanisms guarding your treasures. As it turns out, there are quite a few places where a little sleight of hand can serve your goals. Here is a short list:

Bannering: Many services will supply their name and version number when you connect to them. Intruders can use that information to make looking up an exploit easier and more accurate. Turn these off whenever possible, or at least remove the name and version.

Naming Conventions: Consider the intruder that has managed to reach your internal domain name server. She'll have a much easier time choosing a target if she finds a host named payroll than if all of the hosts are called wksxx. Take that into account when choosing a naming convention for the hosts on your network.

Hiding the Guards: Most network based intrusion detection systems support a stealth mode. That is, they strive to be undetectable on the network. Take advantage of this capability whenever possible. You might also consider keeping the existence of an IDS hidden from most of your employees. You may be legally obligated to inform them that their actions are being monitored, but there is no need to disclose the name and version of the product, the hosts and network segments covered, and the log archival procedures.

Anti-Scan Techniques: Some people like to configure their firewalls and surrounding routers such that it is difficult to even tell that a firewall is present when scanned from the outside. A hardened target can only take so much punishment before it falls. Protecting it from attack by removing it from the enemy's notice can be worthwhile. This is particularly true for home users with cable or DSL. Those boxes don't normally offer services, so configuring a home-firewall to pretend that it isn't there can go a long way to keeping their box from falling to a cracker.

Compartmentalization: The developers have no reason to be snooping around on the boxes used by the marketing or payroll personnel. Consider partitioning the network such that segments are separated on a need-to-know basis. And if your security plan calls for the payroll segment to sit behind an extra firewall, why not use split DNS there too?

Encryption: How often do you telnet to a host and login as root? Hopefully never! You use secure shell (SSH) instead. Why? To protect the password. You are hiding it in case someone has installed an unauthorized sniffer in your network. You may not be able to remove the data from view, but you are at least making it hard to read.

Document Control: Dumpster diving is still a common practice. Policies and procedures need to be in place to ensure that documents, however insignificant, containing information about the network configuration, security, user names, and any other critical information are properly destroyed. Again, we are working to keep information out of an intruder's hands.

Social Engineering: This topic is admittedly only weakly related to obscurity. However, if your employees are properly educated about security such that they can recognize and evade most social engineering attempts, then you have strengthened the shroud of mystery you've thrown over your network.

Conclusion

So, is there such a thing as security through obscurity? Not really, but obscurity can play a part in defense-in-depth. This paper is merely a reminder that in the age of information warfare, information is key. And your efforts to keep it out of the hands of an intruder can be the difference between a smoking firewall and a good night's sleep.

Reference

Zwicky, Elizabeth and Russell, Deporah. "Getting a handle on Internet Security." URL: http://www.ladysharrow.ndirect.co.uk/Internet/getting_a_handle_on_internet_sec.htm

Priestly, Matthew. "Obscurity as Security." 17 August 1999.
URL: http://slashdot.org/features/99/08/17/1327246.shtml

Fuller, Edward. "Denial of Service Attack." 6 April 2000.
URL: http://www.sans.org/infosecFAQ/dos.htm

McLaughlin, Bryan. "Network Address Translation." 10 September 2000.
URL: http://www.sans.org/infosecFAQ/net_add.htm

Holland, Jeff. "DNS Security." 23 July 2000.
URL: http://www.sans.org/infosecFAQ/DNS_sec.htm

Turrell, Timothy. “IDS.” 13 September 2000.
URL: http://www.sans.org/infosecFAQ/IDS.htm

Zych, Tina. “Personal Firwalls: What are they, how do they work?” 22 August 2000.
URL: http://www.sans.org/infosecFAQ/personal_fw.htm

Cassidy, Michael. “Document Security: An Ignored Computer Security Vulnerability.” 11 September 2000. URL: http://www.sans.org/infosecFAQ/doc_sec.htm

Orr, Chris. “Social Engineering: A Backdoor to the Vault.” 5 September 2000.
URL: http://www.sans.org/infosecFAQ/backdoor.htm

Palumbo, John. “Social Engineering: What is it, why is so little said about it and what can be done?” 20 July 2000. URL: http://www.sans.org/infosecFAQ/social.htm

“The Secure Shell Community Site.” URL: http://www.ssh.org

Elnitiarta, Raul and Chien, Eric. “PrettyPark.Worm.” Symantec AntiVirus Research Center. 1 June 1999 (28 February 2000)
URL: http://www.symantec.com/avcenter/venc/data/prettypark.worm.html

Garfinkel, Simson. “Security Through Obscurity.” 12 November 2000.
URL: http://www.wideopen.com/story/101.html

“Appendix A, California Internet Voting Task Force, Technical Committee Recommendations.” URL: http://www.ss.ca.gov/executive/ivote/appendix_a6.htm