

AuditOne Advisory

From Bud Genovese, Chairman

Just in case you may have missed it, below is an important article on Network Penetration Testing written by our AuditOne technology experts that appeared in the November/December 2010 Technology issue of WIB's *Western Independent Banker* magazine. Please forward this article to the appropriate IT staff in your bank.

The highly credentialed information security professionals of AuditOne and our sister company, Insight Risk Consulting, deliver regulatory compliant, up-to-date technology audits including comprehensive IT, GLBA, and Network Vulnerability Assessments including internal and external penetration testing. When you need banking-specific information technology expertise to keep your bank's network safe and sound, contact me to discuss our cost-effective solutions. Thank you. --Bud

Network Security Demands both Internal and External Penetration Testing

By Nigel Sampson and Len Filppu

As part of the information security risk management process required by regulators, proper network vulnerability assessments should test both external and internal penetration controls. But even though the vast majority of hack attacks occur from within an organization, many banks are not including internal penetration testing in their annual risk management program.

External facing firewalls and intrusion detection systems should not be the last line of defense against attacks. Just because a device cannot be compromised, does not mean the network is not vulnerable to attack.

Frequency of Internal Attacks

Cisco Systems, one of the leading network security device manufacturers, writes in the first chapter of its publication *Network Security 101* that 80 percent of attacks occur from inside the network, normally by disgruntled employees. Microsoft designed numerous security features for their servers to thwart internal attacks. For example, a policy allows the default administrator account called "Administrator" to be renamed because Microsoft knows that the first account an internal attacker is likely to look for on the network is "Administrator."

What is Penetration Testing?

Penetration testing examines devices for configuration issues such as missing or incorrectly coded configurations. In some cases, penetration testing exposes a missing security device such as an Intrusion Detection System, an Intrusion Prevention System or a firewall.

Basics of External Penetration Testing

External penetration testing consists of attempting to compromise external interfaces including routers and firewalls. It also tests the fallibility of the email system. It tests whether the server provides relaying and email validation...two common weakness exploited by spammers. Testing an institution's website reveals internal email addresses that are valid, and internal email addresses that can be used for email spamming and pretexting.

Basics of Internal Penetration Testing

Internal penetration testing includes numerous elements. The larger the institution, the more targets require proper testing. Devices that are tested for weaknesses include servers, managed switches, internal router interfaces, internal firewall interfaces, and intrusion detection systems. Testing is not relegated to just looking for unnecessary open ports, but also for login pages, file transfer capabilities, and open shares.

Internal Attacks

How can banks be attacked internally? With the proliferation of wireless capabilities and the miniaturization of Wireless Access Points, it is now possible to hide hacking tools almost anywhere. A janitor could hook a wireless access to an unused office, or hide the ports behind by a desk or boxes. Internal attackers can be off-site, constantly scanning the network for information. It is far easier than most people think to crash a server. Disgruntled employees can download tools and software to create a denial-of-service attack. The “ping of death” overloads the server with requests to make sure it’s still active. If the server is inundated with these requests, it has no time to do anything else. Another type of internal attack does not require any special software. Web management interfaces to managed switches are often left with default username and passwords. Basically, hackers can use a default username such as “Administrator” with a password of “Password” to gain access to all the ports on the switch. This can allow trespassers to shut down all the ports, just like turning off the switch remotely.

What Can Banks Do?

The first step bank management should take is to ensure that its IT staff is informed and aware of the threats and issues surrounding internal penetration testing. IT staff can leverage existing security measures such as group policies in active directory, Virtual Local Area Network and Media Access Control address filtering on switches, and ensure all directories have the appropriate permissions. Banks can encourage IT staff to earn basic network certifications such as Microsoft Certified System Engineer and Cisco Certified Network Administrator. Also, seminars on network security are worth attending, especially ones regarding Internet banking and remote deposit capture.

There are many software applications that provide detailed analysis, but it’s one thing to find a network compromise, and it’s another to provide a solution to fix it. Experience counts when analyzing data. Look for independent risk management consulting firms that have CISSP and CISA-certified technology experts who provide both internal and external penetration testing as part of network vulnerability assessments.

Don’t Leave the Back Door Open

As regulators increasingly expect thorough information security risk assessments from banks, it is critical to include proper internal penetration testing. Cutting costs by performing only external vulnerability testing is like buying a steel door with deadbolts for the front of your house while leaving the back door open for anyone in the neighborhood to come and go as they darn well please.

Bud Genovese is Chairman of AuditOne LLC, a California-based internal audit firm that focuses only on banks and their service providers. Mr. Genovese pioneered the concept of providing comprehensive, affordable, independent internal audit and credit review services by gathering wide-ranging, extraordinary expertise within one firm. AuditOne now serves over 160 clients throughout the Western United States, and nationally. Contact Bud Genovese at 408-980-8099 or bud.genovese@audit-one.com