

IT WEEK

IT NEWS FOR CONNECTED NETWORKS

Volume 1 Number 7

Hackers Are On The Prowl

By: Harry J. Segal

Are Your Valuables Safe?

You spent your IT budget wisely over the past several years. Your patch management solution rolls fixes out to the entire enterprise faster than you can say *vulnerability*. Your firewall is outfitted with more bells and whistles than this year's luxury sedan. And next up on your wish list is one of those new multi-port multi-gigabit security appliances that will stop dead *any and all* worms - whether emanating from the Internet or from a road warrior's laptop plugged into the network. So why would a vulnerability assessment even be a blip on your budget planner?

An objective evaluation of your network security will uncover the *real* issues that make your network vulnerable. Whether faced with the alphabet soup of federal regulations, individual state laws, or a CEO who occasionally appears at your door in a sweat having just read about the latest hack of eBay or the New York Times, it may be time to re-evaluate your preconceived notions of what a vulnerability assessment is.

The first step in understanding the vulnerability assessment process is to define a *vulnerability*. SANS, the world's largest information security certification organization, states, "Vulnerabilities are the gateways by which threats are manifested." While this may sound slightly obtuse on the surface, it is important to understand the concept. A vulnerability may be a missing patch, but it is also an account with excessive privileges or a weak or missing password.

A Vulnerability Assessment is Not Just a Fancy Name for Patch Verification!

A commonly held misconception is that a vulnerability assessment merely reveals missing patches. While this is one area of risk that should be analyzed, a quality vulnerability assessment will provide a comprehensive evaluation of a broad range of risks.

One technology that has helped reduce the vulnerabilities present on corporate networks is enterprise patch management. These systems automate operating system and application patching, giving the network administrator control over the process. When coupled with patch verification tools such as Microsoft's Baseline Security Analyzer, the net-

"hackers and worms often take care of the low-hanging fruit first."

While assessing a well-known sporting goods retailer's e-commerce site, there were no vulnerabilities or missing patches uncovered using the vulnerability scanning tools. But further investigation by the auditor discovered a default administrative account with a well-known default password that provided full access to all sales transactions, including customer credit card information!

work administrator now has powerful tools at his disposal. Corporate IT departments should take advantage of these tools, but it is equally important to evaluate vulnerabilities that go beyond patch levels.

A commonly-discovered vulnerability that is easily exploitable is unnecessary services running on servers, routers and other network devices. For example, even if the Telnet service on your core switch is up to date and contains no known weaknesses, Telnet is an inappropriate protocol to use for the sensitive task of managing a switch due to the lack of security features - such as encryption - in the telnet protocol. Keeping patches up to date is a crucial step in reducing risks but as this example points out, it is only part of the story.

Another misconception is that a vulnerability assessment simply involves running a few vulnerability scanning tools from the Internet. While some security firms offer *scanning services*, these services represent only a subset of an external (Internet-based) vulnerability assessment. A scanning service typically delivers a report containing a list of vulnerabilities discovered by the scanning tool and general information about the vulnerabilities. In a properly conducted external vulnerability assessment, the auditor should evaluate the vulnerabilities in the context of your servers and eliminate false positive results. Finally, the assessment results should be presented with specific guidance for remediation of the vulnerabilities uncovered.

“...having breached the system, the auditor could snoop on any video conference!”

External and Internal Vulnerability Assessments vs. Penetration Tests

Most organizations focus their security resources on their Internet gateways and publicly-accessible servers. If you have a single VPN connection to another network that is not under your direct control, or you allow users to connect to the corporate network through a VPN, discard the concept of your network having an “inside” and “outside.” Any network that is not under your direct control including remote end users should be considered un-trusted. When you allow connections from an un-trusted network or host to your internal or trusted network, there is no longer an “edge” to your network.

Although the *edges* of your network have become blurred, an external vulnerability assessment is by definition performed from the Internet and therefore should have no access to your non-public network resources. A more intensive look at your network security is obtained by the auditor connecting directly to your internal network. An *internal* vulnerability assessment delivers substantially more insight into your network than an *external* vulnerability assessment. Connecting directly to your network, the auditor can assess the security of the infrastructure of all network resources beginning at the physical layer – the routers and switches - all the way up to the SQL server that houses your payroll information.

Sometimes confusion arises over terminology. For example, the term *vulnerability assessment* is generally considered interchangeable with *security audit*. Another term that adds confusion is a *penetration test*, which has the implied goal of “penetrating” the security of your network rather than only *identifying* network vulnerabilities. During a penetration test, the auditor attempts to circumvent the security features of network resources by *exploiting* one or a small number of discovered vulnerabilities. A penetration test may provide an eye-opening demonstration of the possible implications of your network’s vulnerabilities to senior management or a board of directors. However, it may be more sensible and productive to concentrate on *identifying and correcting* vulnerabilities through a vulnerability assessment rather than expending resources on a penetration test that breaches your network security. There is plenty of evidence that vulnerabilities place your network at risk – why pay a security firm to prove it?

During the first fifteen minutes of a vulnerability assessment for a multi-national law firm, the auditor uncovered a *weak username and password combination* that allowed full remote access to the law firm’s network as if he were one of their attorneys!

Newly Deployed Technology Challenges Security

In recent years, IT staffs have generally been downsized while the volume of technology overseen by the IT department has grown at a rapid pace. Wireless networks, VoIP, web-enabled applications, IP-based video conferencing, and VPNs connecting both remote users and even partners’ networks, are just a few of the recent technologies that

are commonplace today. In many instances, third-party integrators or manufacturers help with the initial deployment and hopefully perform a level of knowledge transfer, but the rest is left up to you!

Tight resources and the continued deployment of new technology make it difficult, if not impossible, for your IT staff to completely understand all the technologies that are in place on your network. Even more challenging is recognizing the unnecessary risks these technologies introduce to your network.

Vulnerability assessments have shown that early adopters of technology are often employing software containing vulnerabilities. A recently completed vulnerability assessment discovered that the client's VoIP gateway that was installed nine months earlier contained a vulnerability unknown even to the manufacturer.

The vulnerability was found in an embedded web server used for controlling and managing the VoIP gateway. Easily exploited, this vulnerability would allow a malicious user or hacker to disable the entire VoIP system! Had the VoIP gateway been fully integrated into the client's network, the vulnerable gateway could have been used as a "jumping off" point to attack other network resources.

Clearly, in today's IT pressure cooker environment, it is hard to imagine having your staff adequately trained *and* devoting the time to discover even more obvious vulnerabilities. These conditions point out the importance of having an objective third party that understands security risks evaluate your environment.

What Will Your Vulnerability Assessment Uncover?

So you are warming up to the idea of having a vulnerability assessment completed and now you want to know what to expect in the end? The scope of your vulnerability assessment will greatly influence the final report.

What your external vulnerability assessment will encompass, depends in large part on what services you publicly host. For example, smaller organizations may only have a single email server, router, firewall, and possibly a web or FTP server, exposed to the Internet. Often, the IT manager of a small business with a limited Internet presence develops an, "I don't have anything a hacker wants," mentality and operates as if security risks do not represent true business risks. Yet, when pressed to consider the impact of a prolonged outage of their email server, suddenly the benefits of preventative measures such as vulnerability assessments become obvious.

Larger organizations are likely to have numerous web, application, and database servers at key corporate locations and at co-location or hosting facilities. And having transitioned portions of their wide area network to site-to-site VPN technology, many organizations have *multiple* Internet gateways to secure.

The more common vulnerabilities found during an external vulnerability assessment include poorly configured border routers with extraneous services running and web servers that have not been hardened properly prior to

"It is analogous to the story of two CIO's hiking in the woods."

An on-line services provider with a mission-critical, offsite server farm first contacted Networks Unlimited two years ago to perform an external vulnerability assessment. The company had never been audited before, and selected the Massachusetts-based security firm after interviewing several candidates. According to the company's senior network administrator, within the first hour of the audit there were some big surprises, which required immediate attention. "Web-based administrative tools on a core switch were accessible to the Internet – a serious error we needed to quickly correct." The company has just recently completed its third audit, and continues to reap benefits. "Our latest audit was both an internal and external assessment. It uncovered several oversights in both server and network security configurations. We are committed to having security assessments performed on an annual basis. We believe this is a critical component in protecting our confidential customer information and keeping our servers operating flawlessly."

deployment and are also missing patches. An external assessment exposes a portion of firewall mis-configurations, but comprehensive firewall configuration checking requires a close review of the firewall's rules.

In addition to vulnerability testing of network devices, including servers, switches and a representative sample of workstations, the internal vulnerability assessment generally incorporates much more, such as a review of your written security policies or a detailed report on the permissions granted to every user on the network.

Vulnerability assessments often uncover services and applications running that place your network at risk of disruption or unauthorized access. Some common examples include management protocols such as SNMP, web-based management tools for servers and other network resources, and network devices running default and insecure configurations.

Security issues are occasionally discovered that were not on IT's radar prior to an assessment. Task or application-specific servers that are provided by a vendor as part of a package for ACD, VoIP, and departmental applications are sometimes improperly maintained for fear of "breaking them" or due to the expectation that the vendor is maintaining them properly. One recent vulnerability assessment at a bank discovered serious vulnerabilities in multiple servers that were the responsibility of the client's primary data processing services vendor! The bank had excluded the servers from earlier vulnerability assessments on the assumption the well-respected vendor employed strong security procedures.

Aside from enhancing security, vulnerability assessments may identify methods for improved network stability and performance. Removing unnecessary services and hardening the configuration of your core network can greatly reduce the impact an infected computer or malicious user can have on your network.

LDIO (Let's Do It Ourselves)

At this point, you may be asking, "why not do this with our internal resources?" IT departments should be assessing their network for vulnerabilities as part of their normal operations, but it is critical to have an objective third party with expertise in network security assessing your network on a periodic basis. The frequency of these third-party assessments will vary based on the findings of an initial vulnerability assessment, the dynamics of your environment, the skill level and availability of your IT staff, the value you place on your network and the data it contains, your budget, and finally the risks associated with a security breach.

With a third-party vulnerability assessment, problems that are often swept under the carpet because a project has been *completed* and your staff is onto the next project can be brought to light and solved. It is very difficult for an interested party such as an employee to properly weigh the risks vs. rewards and avoid being influenced by departmental politics or friendships.

As you know all too well, there is often significant internal pressure to rapidly deploy a new application or server to meet tight deadlines, leaving little room for system maintenance much less a thorough security vetting. An objective third party will look at the security implications of a given configuration - divorced from the business need of the configuration - allowing you to make in-

Wishing to ensure that it was properly protecting its information assets, a diversified mining company had its first audit performed at the end of 2003. Several vulnerabilities were discovered. Realizing the importance of these discoveries, the IT staff quickly went to work - starting with the high-severity risks - until all remediation was completed. According to the company's CIO, "Having a third-party help identify and explain why vulnerabilities were of high, medium, or low risk, added valuable knowledge for our IT staff." Follow up validation was performed to make sure all issues had been properly addressed.

At the end of 2004, in its most recent audit of the mining company, Networks Unlimited determined that a few new security issues had surfaced during the year, requiring IT's attention. But even with his technical services team doing an "impressive job", the company's CIO plans to expand the scope of future security assessments. "We need to continue our work with Networks Unlimited and have them conduct internal and external security audits on an annual basis. Even if the assessments confirm that we are doing a good job, it is best practice to continue validating the management of security risks. Having these assessments performed keeps us on our toes and helps us stay proactive. Security now plays a bigger role in our minds and we do a better job of deploying systems the first time around!"

formed decisions on acceptable levels of risk.

During a recent vulnerability assessment intended to target a client's Internet gateway and public services, the auditor discovered a video conferencing system installed outside the client's firewall. For proper operation, multiple ports were required to be open to the video conferencing system from the Internet. The client was uncomfortable placing a device that required substantial public access on his internal network or DMZ and chose to instead have it placed outside the firewall. Once the video conferencing system was up and running, it had largely been ignored. The device worked and due to its location, a security breach of the system would not affect the client's corporate network. The vulnerability assessment uncovered several services running that enabled remote management of the video conferencing system. The auditor was able to compromise the system through the use of a default management account present on the system. The client's pride in knowing that even though the auditor was able to break into the system - *his network was safe* - faded when he realized having breached the system, the auditor could snoop on any video conference! Later discussions determined that the client was following vendor setup recommendations in response to the client's security concerns about the video conferencing system's need for multiple open ports. In the end, changing a few default settings greatly enhanced the security of the video conferencing system.

Do we or don't we have a vulnerability assessment performed?

Recognizing that sophisticated automated scanning tools are readily available to hackers and malicious users, and that worms rapidly propagate affecting thousands of systems in minutes, your goal should be to ensure your network is not one of the *easy targets*. Like so many activities in life, hackers and worms often take care of the *low-hanging fruit* first. With many organizations leaving themselves vulnerable - there's plenty to choose from!

It is analogous to the story of two CIO's who are hiking in the woods. All of a sudden, a bear starts chasing them. They climb a tree, but the bear starts climbing up the tree after them. The first CIO gets his sneakers out of his knapsack and starts putting them on. The second CIO says, "What are you doing???"



The first CIO responds "I figure when the bear gets too close, we'll have to jump down and make a run for it."

The second CIO says "Are you crazy? You can't outrun a bear."

And the first CIO, grinning, says, "I don't have to outrun the bear - I only have to outrun you!"

Harry J. Segal, President & Founder, Networks Unlimited

Prior to founding Networks Unlimited, Harry Segal was vice president of sales at Microcom, a manufacturer of modems that was best known for its invention of the error-correcting protocol still used in today's dial-up modems. His career in the computer industry began over 30 years ago with Data General Corporation. He holds a bachelor's degree in information and computer science from Georgia Tech. He can be contacted at harry.segal@networksunlimited.com.

Founded in 1985, Networks Unlimited, Inc. serves the needs of mid-market organizations across a variety of industries - financial, health care, manufacturing, legal, retail, and online services.

A privately-held company based in Hudson, Mass., the firm is today recognized as one of the nation's foremost systems integrators and information technology consulting firms specializing in information security.

Networks Unlimited offers its customers a full-service approach to systems integration and consulting that includes security audits, managed security services, security policy development, regulatory compliance, and security infrastructure deployment and support.

Networks Unlimited deploys systems that protect critical information and valuable network resources. It helps customers avoid the disruption and the detrimental impact of security breaches, and comply with regulations, such as Sarbanes-Oxley, HIPAA, and Graham-Leach-Bliley.

Further information is available at their web site: www.networksunlimited.com