LOCK-PICKING THE eDOOR: KNOWING HOW HACKERS FIND THE WEAKEST LINK

RAPID7 SECURITY

FOR MORE INFORMATION ABOUT NEXPOSE, VISIT

WWW.RAPID7.COM

LOCK-PICKING THE eDOOR: KNOWING HOW HACKERS FIND THE WEAKEST LINK

Is it possible to predict the probability that a system in an organization's network will become compromised by a cyber-attack? The weakest link lies somewhere in the electronic business processes, but it is difficult to know exactly where it is located, what it looks like, and how likely it is to be found. Access, programming and communications are typically used in many phases of a business process, therefore understanding the actual threat is complex.

We generally think of unpatched workstations as the likely target of malicious attacks, but even completely secure systems can become compromised as a result of stolen or guessed user IDs and passwords, configuration errors, user-installed software such as iTunes™, adware or spyware, corporate policy violations, and employee data theft and fraud.

In advancing development of NeXpose, Rapid7's robust solution for investigating and reporting electronic vulnerabilities, we've taken the product to the next level of vulnerability management because we recognize that there are many avenues for potential hacker attacks that have yet to be explored and no real defined risk model for existing vulnerabilities.

There is a report on credit card data theft in the *New York Times* ("Main Street in the Cross Hairs," July 26, 2005). The article recounts how criminals used "drive-by" wireless eavesdropping techniques to acquire credit card information on thousands of customers as purchases were made at four major retail outlets in a Florida shopping area. The thieves singled out stores with strong wireless signals and weakly protected data. Yet another weak link in the communications chain to be accounted for!

The number and types of vulnerabilities in an enterprise present risks that can clearly compromise systems. Because business processes rely on networks of interconnected systems, it takes only the weakest link to cause a business interruption or affect a company's reputation.

USING ARTIFICIAL INTELLIGENCE TO DETERMINE RISK

Criminals access systems using a variety of techniques and then use those systems as launching points for illegal activities. To understand how they are able to succeed, we've modeled these techniques using NeXpose, an Enterprise Vulnerability Management system which incorporates an expert system (AI) engine called Jess® (http://herzberg.ca.sandia.gov/jess/)[1]. Just as a hacker gains advantage with each piece of information he extracts about a network, the expert system takes each piece of information extracted and builds a knowledge base of facts about the environment it explores. With the database of facts, the expert system can then deliver complex results, revealing how information obtained on a specific vulnerability, such as an admin ID discovered in a system, can be used to create a different vulnerability that would not necessarily be discovered by traditional penetration tools and therefore, dig deeper into the targeted network. The expert system is able to operate as a hacker can and can link facts together and predict with greater accuracy how systems may be compromised. Understanding which systems in your network are high risk systems enables you to reduce research and administration costs of vulnerability assessment and remediation and more accurately evaluate the riskiest systems in your networked environment in order to take precautionary measures to reduce the likelihood of an attack.

---

[1] *Jess and the Jess design are registered trademarks of Sandia National Laboratories. Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the U. S. and other countries*

As the time from vulnerability discovery to exploit shortens - just several days between discovery and worm release in the most recent cases - knowing the systems with the highest potential risk is an important factor for managing your exposure. Without this knowledge, the approach generally taken is to apply all available fixes to a specific system. Because there are so many systems and numerous possible firmware upgrades, this approach is an expensive and near impossible proposition. Understanding the potential risk of a system enables you to optimize the use of expensive administrative resources and direct them to the most important tasks.

Hackers who discover vulnerabilities may release information about them before the vendor has released a fix, generating the possibility of so called "zero-day" vulnerabilities. There are vendors' products containing vulnerabilities that only hackers know about, creating threats that are extremely difficult to discern. Since both companies and vendors are unaware what their vulnerabilities truly are, acquiring "intelligence" about vulnerabilities in the network environment can ensure the right security measures are taken to prevent attack.

THE COMPILATION OF RISK

As the number of interconnected devices expands exponentially across enterprises and the world, so do the opportunities for vulnerabilities to be exploited for criminal gain. NeXpose and its internal expert system engine provide knowledge of how vectors between systems may increase risk. NeXpose also counteracts the intensifying complexity that thousands of interconnected devices can create by scaling to the density of the environment. In a large environment, NeXpose can scale accordingly, continuing to filter and analyze the opportunities for a compromise to occur.

Aircraft accidents can be the result of a number of coincidental events that combine to create an unanticipated and unwanted outcome. Carelessness with systems administration often leads to the same outcome in the networked world. NeXpose tests hundreds of ways of accessing information to determine how systems may be broken into by a hacker. When access to one system leads to access of another, a link has been uncovered that can be exploited without detection. Using this knowledge, risk scores can be calculated to describe the contribution of a specific system to the susceptibility of attack.

When all the systems in a network are evaluated as a whole, the risk scores represent a highly accurate ranking of which systems need remediation first.

CONCLUSION

Companies with thousands of systems have a difficult time understanding the scope of their exposure to malicious attacks. By exploring the relationships within networks of systems — how risk in a single system can impact the entire enterprise — NeXpose is able to deliver a critical assessment of risk. NeXpose can also target specific vulnerabilities within those networks to create risk profiles of individual systems, deepening our understanding of how networks of related systems can create and increase risk.

ABOUT RAPID7

Rapid7 was founded in 1999 by a team of software industry veterans who were major contributors to product development and subsequent growth and success at Percussion Software, Bond Technologies and Stride & Associates. Since introduced, NeXpose has been sold to corporate enterprises, Global 2000 companies, and government entities, and serves the full range of vertical markets across the U.S. and abroad. Rapid7 is headquartered in Boston, MA, with offices in California and the United Kingdom. For more information on the company and its product, NeXpose, visit the **Rapid7 web site**. To try NeXpose in your environment today, visit the **NeXpose download page** of our web site.