Marshall Eddy

CS332-002

Vincent Skimmer

1 March 2017

Automated Scripts

For vulnerability management, policy management is critical. Eneterprise policies start at the top of an organization and require executive oversight. Policies determine the nature of controls used to ensure security, such as standard configurations for all security devices and applications including antivirus, firewall and intrusion prevention. Policies and controls also should include

servers, network services, applications and endpoint PCs. New software tools can automate some aspects of policy management and enforce configurations on endpoint devices. Automation saves time, improves accuracy and lowers total cost of ownership.

You need to find vulnerabilities before you can fix them. This step sets an evaluation baseline by creating and maintaining a current database of all IP devices attached to the network. Organizations should categorize assets by business value to prioritize vulnerability remediation. Elements in the database include all hardware, software, applications, services and configurations. Tracking this level of detail provides two benefits. The data enable your organization to identify which vulnerabilities affect particular subsets of the IT infrastructure. An accurate inventory ensures that you select and apply the correct patches during remediation. The tracking inventory also helps speed the scanning process because it limits scans to relevant devices, software and services affected by particular vulnerabilities. Discovering devices, software and services and tracking this inventory can be done manually. You can also automate the entire discovery and tracking inventory process with an on demand vulnerability management service like QualysGuard.

A vulnerability scan tests the effectiveness of security policy and controls by examining network infrastructure for vulnerabilities. The scan systematically tests and analyzes IP devices, services and applications against known security holes. A post-scan report reveals actual vulnerabilities and states what needs fixing. There are many options for scanning. Some require software applications you install and maintain, such as the Nessus public domain scanner. These require lots of time and carry typical operational overhead. A Web-based on demand solution such as QualysGuard does the scans for you over the Internet. It works without special software or hardware. Another advantage to a Web- “Qualys’ on demand model is like turning on a light – immediate visibility into ranked vulnerabilities and the fastest path to remediation, preventing attacks before they occur.” Robert S. Paszko Director of Security DuPont Categorize assets by business value to prioritize vulnerability remediation Qualys, Inc. Vulnerability Management Page 5 based service is being always up-to-date with the most recent vulnerabilities. You shouldn’t have to worry about updates to scanning technology because it’s a key part of the vulnerability management system.

The comparison process helps to minimize false positives. With some vulnerability scanning and intrusion detection systems, for example, false positives can dull the results of accurate alarms if vulnerabilities do not match what’s in your inventory. To eliminate inaccurate hits and the resulting waste of time chasing down false positives, compare your organization’s IP inventory against industry standard vulnerability databases such as the Common Vulnerabilities and Exposures (www.cve.mitre.org) list and NIST’s ICAT Metabase (www.icast.nist.gov). CVE provides a comprehensive list of publicly known vulnerabilities, an analysis of authenticity of new vulnerabilities, and a unique name for each vulnerability. ICAT takes CVE to the next level with detailed information about each vulnerability. Also use the SANS Top 20 and CERT Advisories (www.scans.org/top20.html and www.cert.org/advistories/). QualysGuard automatically does the comparison against industry standard vulnerability databases and other public and private lists of vulnerabilities.

Fixing security problems is the result of vulnerability management. Traditional manual processes for applying patches and other remediation are slow and expensive. Sometimes the high cost of patching coupled with the high volume of patches released by vendors encourages organizations to delay remediation. Organizations may delay updates – even for critical patches – until multiple patches or service packs are available, or until arrival of a regular monthly, quarterly or annual update process. Unfortunately, delay can be a fatal strategy “As a Web-based solution, QualysGuard enables us to perform security audits as often as necessary, spot vulnerabilities immediately as they are added to the QualysGuard database, and work proactively to remediate them. This helps us secure all our network entry points, enforce ICI security policies and assists us in meeting federal requirements.” Paul Simmonds Dir. of Global Information Security ICI Qualys, Inc. Vulnerability Management Page 6 so it’s important to remediate vulnerabilities as quickly as possible. Automated patch management and software distribution solutions can help speed this process and keep costs to a minimum. Rollback capability allows organizations to efficiently ensure use of appropriate software versions. Integrating patch management with other automated vulnerability management processes is beneficial. Open XML application programming interfaces enable integration of QualysGuard with third party remediation and patch management software such as Arcsight, Citadel and GuardedNet.

References

<https://www.qualys.com>

<http://www.tutorialspoint.com/penetration_testing/penetration_testing_quick_guide.htm>