EFFECTIVE VULNERABILITY MANAGEMENT USING QUALYSGUARD

ICTN 6823
BOYD AARON SIGMON
EAST CAROLINA UNIVERSITY

Abstract

In the Information Security field, being proactive is often better than being reactive, especially when it comes to the ever-growing vulnerabilities in today's software and operating systems. In order for an organization to be proactive, implementing an effective vulnerability management program is a necessity and can drastically reduce the amount of risk and incidents associated with cyber security attacks.

For an organization to achieve the objectives of an effective vulnerability management program, the implementation of an automated vulnerability management tool called QualysGuard is proposed. QualysGuard is vulnerability scanner and tracking system that can also inventory all software, assets, and services on a network.

In addition to implementing the tool, policies for the program must be developed with deadlines set to address vulnerabilities in a reasonable amount of time. Addressing the most critical patch-related vulnerabilities is imperative so utilizing custom reporting will present users with only the vulnerabilities that can be remediated by patching. This will set easy achievable goals, help asset owners learn the tool and filter out the more difficult to understand vulnerabilities, as well as drastically reduce the risk of cyber attacks on the organization.

1. Introduction

IETF RFC 2828 defines the term vulnerability as "A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy" [10]. Vulnerability management is defined as the "cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities, especially in software and firmware" [11]. In order to implement an effective vulnerability management program, the implementation of an automated vulnerability management tool called QualysGuard and the use of custom reporting are needed. QualysGuard is the market leader in vulnerability management tools. The product allows you to perform vulnerability scanning, asset discovery, inventory, compliance monitoring, and threat protection all from a single easy to use interface. This paper will show the process that should be followed to ensure the program is successful and help you greatly reduce security risk.

2. Why Vulnerability Management Is Needed

According to the 2015 HP Cyber Risk Report, "44 percent of known breaches came from vulnerabilities that are 2-4 years old" [4]. This is a prime example of why implementing an effective vulnerability management program should be an essential part of any information security program. By taking this proactive approach, you will greatly reduce risk to cyber security attacks and provide safeguards when other controls, such as firewalls and intrusion detection systems fail to prevent incidents. In a whitepaper by SecureState, the author states that "the lack of a Vulnerability Management Program ultimately could result in a breach because vulnerabilities attackers use to compromise

networks are not being addressed in your environment. Without a Vulnerability Management Program your security team is blind to the technical risk to which your company may be exposed" [3].

By implementing the QualysGuard tool, it will help you achieve and automate the process for the first four objectives of the SANS 20 Critical Security Controls, which are the most important and most effective defense mechanisms to protect against cyber security attacks. Those objectives include inventorying approved assets and software, using secure configurations for hardware and software, and doing continuous vulnerability detection and remediation [2]. Before implementation can begin, the most important step of the process is to develop policy and timelines around your Vulnerability Management program, as well as establish roles and responsibilities. Every user involved in the vulnerability management process should clearly understand the expectations of the organization, know their role in the process, and fully comprehend the deadlines set to remediate vulnerabilities.

According to Qualys, "80% of vulnerability exploits are available within 60 days after news announcements of vulnerabilities" [6], so making sure vulnerabilities are remediated in a reasonable amount of time is essential to prevent systems from being compromised. The below example shows the timelines put in place by the State of North Carolina in the Statewide Information Security Manual for NC agencies [8].

- "High-level risk" vulnerabilities must be mitigated as soon as possible. It is recommended that "High-level risk" vulnerabilities be mitigated within 7 days, but must be remediated within 21 days.

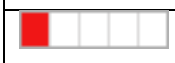
- "Medium-level risk" vulnerabilities must be mitigated within thirty (30) days
- "Low-level risk" vulnerabilities must be mitigated within ninety (90) days

As you establish timelines for remediation in your policy, it is recommended to start with having users only remediate Urgent and Critical level vulnerabilities that have a patch available. The reason why is vulnerability data can be very cumbersome for most end-users, especially, because vulnerability assessments usually identify an extremely large number of vulnerabilities that are ranked by severity. The severity of each vulnerability is ranked by using the CVSS (Common Vulnerability Scoring System), and then QualysGuard presents the vulnerability as Urgent, Critical, Serious, Medium, or Low.

By using custom reporting in QualysGuard, this will ensure that users have a clear understanding of what vulnerabilities should be addressed and make the data very easy to understand. This will give your program a quick win, drastically reduce the number of vulnerabilities on your network, and greatly reduce your organization's risk. In an article by InfoWorld, Grimes states "more than 80 percent of all publicly known exploits have patches available on the day of the vulnerability's public disclosure" [9].

Table 2.1 shows the severity levels in QualysGuard that vulnerabilities are ranked against.

Table 2.1

Severity	Level	Description
	**Minimal**	Intruders can collect information about the host (open ports,

		services, etc.) and may be able to use this information to find other vulnerabilities.
	**Medium**	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
	**Serious**	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
	**Critical**	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
	**Urgent**	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands,

		and the presence of backdoors.

In addition to custom reporting, QualysGuard also has a built-in ticketing system that can be used to automatically assign tickets to the asset owner for vulnerabilities that match the policy. By using the ticketing system, you can create tickets for only the vulnerabilities that you want users to remediate and assign a due date. Tickets are automatically closed when a re-scan occurs that no longer shows the vulnerability present on the asset. If tickets are not closed by the due date, then they will show up as overdue. Also, end-users can also use the ticketing system to efficiently report false positives by submitting written proof into the ticket. Once the ticket has been flagged as a false positive, it is closed, but can be manually re-opened by the QualysGuard administrator.

3. Implementing QualysGuard

Now that we have an understanding of why a vulnerability management program is needed, we can discuss how the technical steps of how the QualysGuard vulnerability management tool should be implemented. Following this process will ensure an effective automated deployment.

3.1. Asset Identification & Inventory

One of the most important steps of the process is to take inventory of all approved assets on your network and successfully identify each asset owner. QualysGuard maintains that inventory by creating a database entry for each IP address it performs a vulnerability scan on. The inventory contains important information such as IP address, hostname, operating system, installed software, and open ports.

3.2. Discovery Scans

Before you can begin the vulnerability-scanning phase, you must run what is called a discovery scan. A discovery scan is a lightweight scan that only looks at a limited number of ports to identify asset information, such as DNS name, NETBIOS name, Operating System, as well as the Router that device uses. Discovery scans should be scheduled to run on every subnet in your network weekly. Once you have your approved asset list, this will help you to identify newly connected assets or rouge devices.

3.3. Identify Assets & Assign Owners

Once the discovery scans have completed, you can then begin the process of identifying each asset owner. QualysGuard will allow you to assign an asset owner to each individual IP address and you can assign the assets to an Asset Group. Asset Groups are a critical component of the QualysGuard architecture, as you will use them to assign user permissions, schedule vulnerability scans, classify business risk, and to create remediation policies, if you choose to implement the ticketing system. It is recommended to create separate Asset Groups for critical systems, servers, workstations, network devices, as well devices that are in-scope for compliance purposes.

3.4. Scheduled Vulnerability Scanning

The next step of the implementation process is to setup scheduled authenticated vulnerability scans to run against each Asset Group weekly. This will keep the vulnerability data relevant and close remediated vulnerabilities faster, as well as have accurate searchable asset information. Authenticated scanning in QualysGuard is

extremely important because it helps the scanner accurately identify the system and it's vulnerabilities, as well as reduces the number of false positives. QualysGuard supports the use of SSH keys, domain credentials, and standalone, as well as integration with CyberArk Password Vault.

When performing vulnerability scanning for the first time on your network, it is recommended to run the scans on a test system first to prevent a possible unplanned outage of a service. QualysGuard's standard scan settings test about 1900 tcp ports and 180 udp ports, and isn't very disruptive to systems. If you find systems that are being affected by the Standard Scan settings, then you will have to build a new Option Profile that you can configure to scan the system slowly one port at a time, rather than in parallel.

3.5. Custom Reporting & Ticketing

At this point in the process, you should have scans running at various times throughout the week and should be seeing some vulnerability numbers in the QualyGuard interface. The scan data under the Scans tab is the place where most users go to look at the scans. That data is the raw scan data and can overwhelm most end users who are not familiar with remediating vulnerabilities. This is why you should train your users to use custom reporting.

Based on the vulnerability management policy your organization has established, it is recommended that you build custom reports to show only the vulnerabilities that you want the asset owners to remediate. Those custom reports can be scheduled to run

weekly and can be sent as a PDF to an email address, or viewed in the QualysGuard interface. You can also use the custom reports to search through all assets on your network for a single vulnerability, which can be extremely useful if a particular vulnerability becomes a hot topic in the news.

In addition to the custom reporting, you can also setup the internal ticketing system to assign tickets to asset owners based on the same criteria as the custom reports. This is very useful to track remediation progress and assign due dates based on the timelines established in the vulnerability management policy. Asset owners can also use the tickets to report false positives, which can later be reviewed and approved by the program administrator.

4. Conclusion

Vulnerability management is a critical part of a security program and can be very difficult to implement. By deploying QualysGuard in your environment and using custom reporting to only show patch-related vulnerabilities, your organization can easily implement an effective program that significantly reduces your organization's risk to a majority of cyber attacks.

5. References

1. Hoel, M. (2013, December 22). Framework for building a Comprehensive Enterprise Security Patch Management Program. Retrieved July 21, 2016, from https://www.sans.org/reading-room/whitepapers/threats/framework-building-comprehensive-enterprise-security-patch-management-program-34450

2. CIS Critical Security Controls. (n.d.). Retrieved July 21, 2016, from https://www.sans.org/critical-security-controls/

3. McCully, G. (n.d.). Retrieved July 21, 2016, from http://www.securestate.com/Insights/Documents/WhitePapers/9 half signs your vul mgmt program failing.pdf

4. Security Threat Landscape Still Plagued by Known Issues, says HP. (2015, January 1). Retrieved July 21, 2016, from http://www8.hp.com/us/en/hp-news/press-release.html?id=1915228&pageTitle=Security-Threat-Landscape-Still-Plagued-by-Known-Issues,-says-HP#.VQ3hrWTF9K5

5. Palmaers, T. (2013, March 23). Implementing a vulnerability management process. Retrieved July 21, 2016, from http://www.sans.org/reading-room/whitepapers/threats/implementing-vulnerability-management-process-34180

6. Qualys. (2004, January 1). Guide to Effective Remediation of Network Vulnerabilities. Retrieved July 21, 2016, from https://www.qualys.com/docs/guide_vulnerability_management.pdf

7. Mell, P., Bergeron, T., & Henning, D. (2005, November 1). Creating a Patch and Vulnerability Management Program. Retrieved July 21, 2016, from http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf

8. Statewide Information Security Manual. (2015, January 1). Retrieved July 21, 2016, from https://www.scio.nc.gov/library/pdf/SISM-1-2015.pdf

9. Grimes, R. (2013, July 23). Stop 80 percent of malicious attacks now. Retrieved July 21, 2016, from http://www.infoworld.com/article/2611443/security/stop-80-percent-of-malicious-attacks-now.html

10. Shirey, R. (2000, May). Request for Comments: 2828. Retrieved July 21, 2016, from https://www.ietf.org/rfc/rfc2828.txt

11. Vulnerability management. (n.d.). Retrieved July 21, 2016, from https://en.wikipedia.org/wiki/Vulnerability_management