Vulnerability Management in Practice: Contribution of Qualys to the ACCESS Project for Enhanced Cybersecurity

Megha M Moncy
ACCESS STEP (Cybersecurity Intern)
NCSA - University of Illinois at Urbana Champaign
Indiana University
memoncy@iu.edu

***Abstract*—In a digital landscape fraught with vulnerabilities, the careful selection of vulnerability management solutions is vital. This paper presents a comprehensive analysis of the implementation and evolution of Qualys in the ACCESS project, encompassing both summer and fall terms of a cybersecurity internship at NCSA. Initially focusing on Qualys' selection for its cost-effectiveness, seamless integration, and robust threat detection, the study then expands to the fall term, detailing advancements in asset management, enhanced reporting, and refined vulnerability analysis. The integration of these new strategies alongside initial implementations illustrates a proactive, dynamic approach to cybersecurity challenges. The findings offer valuable insights for similar vulnerability management endeavors, emphasizing the importance of continuous adaptation and improvement in cybersecurity practices.**

***Index Terms*—Vulnerability Management, Cybersecurity, ACCESS, Qualys, Vulnerability Detection, Security Scanning**

I. Introduction

In recent years, the digital landscape has seen a significant surge in reported cybersecurity vulnerabilities, exemplified by the Common Vulnerabilities and Exposure (CVE) system [1]. This increasing complexity, amplified by rapid technological advancements and the rise of sophisticated cyber-threats, underscores the urgent need for robust cybersecurity measures. As the digital environment grows more intricate, the task of maintaining data security and system integrity escalates in both importance and difficulty, making the adoption of effective cybersecurity strategies imperative. [2].

One critical aspect of cybersecurity is vulnerability management. Vulnerabilities are weaknesses or flaws in systems, networks, or applications that can be exploited by malicious actors to gain unauthorized access, compromise data integrity, or disrupt operations [3]. Among the various vulnerability management solutions available in the market, Qualys has emerged as a leading platform widely adopted by organizations. The ACCESS project, an ongoing initiative, has chosen Qualys as its preferred vulnerability management solution. The findings of this research contribute to the existing body of knowledge by providing valuable insights into the selection and implementation of vulnerability management solutions, with a specific focus on Qualys in the context of the ACCESS project. This paper not only discusses the initial selection of Qualys due to its efficiency and effectiveness but also extends to cover the strategic enhancements made during the fall term. These include the optimization of asset management processes and improved reporting mechanisms, signifying a proactive approach to evolving cybersecurity challenges. The integrated analysis aims to offer valuable insights for organizations navigating similar cybersecurity landscapes, emphasizing the importance of adaptability and strategic planning in vulnerability management. Furthermore, a comparative analysis with other vulnerability management solutions will be conducted to gain insights into the key factors influencing the choice of a suitable platform.

II. RESEARCH OBJECTIVES AND QUESTIONS

The primary objective of this research is to evaluate the adoption and practical utilization of Qualys as the vulnerability management solution for the ACCESS project at NCSA - University of Illinois at Urbana Champaign. This research aims to comprehensively assess the implementation and evolution of the Qualys platform within the ACCESS project across two internship terms. The primary goal is to understand the factors influencing the selection of Qualys and to evaluate its effectiveness in managing cybersecurity threats over an extended period. Specifically, the paper seeks to answer the following questions:

- What were the driving factors behind choosing Qualys as the vulnerability management solution for ACCESS, and how have these factors evolved over time?
- In what ways was Qualys implemented and integrated within the ACCESS project's cybersecurity framework during both terms, and what enhancements were made?
- How effectively has Qualys addressed cybersecurity threats within the ACCESS project, considering both initial implementation and subsequent optimizations?

III. METHODOLOGY

This research followed a comprehensive and systematic methodological approach, incorporating various techniques to gain a comprehensive understanding of the adoption and utilization of Qualys within the ACCESS project. The methodology consisted of the following five steps:

A. In-depth Literature Review

This critical first step involved exhaustive research to understand the underlying concepts and practices of vulnerability management, its significance in the cybersecurity landscape, and the functionalities of various vulnerability management solutions currently available in the market. The review particularly focused on the role and attributes of Qualys as a tool of choice for several organizations, including our test environment. The review enabled a well-grounded understanding of the broader context of vulnerability management and the ongoing academic and industry dialogue around this topic.

B. Practical Experimentation with Qualys

The subsequent step involved hands-on experimentation with the Qualys platform in a real-world environment. By leveraging the ACCESS project's infrastructure, we gained practical experience with Qualys, exploring its features, performance, integration capabilities, and overall user experience. This hands-on approach provided valuable insights into the platform's functionalities and allowed for a more practical assessment of its effectiveness in vulnerability management.

C. Development of the Spreadsheet

A significant milestone in our methodology was the construction of a detailed spreadsheet that served as a transition management tool from XSEDE to ACCESS. This task involved aggregating essential data such as host names, IP addresses, and other relevant information from Qualys, Syslog, and Nagios. The aim was to establish a system that could validate the status of services across these platforms by attributing a 'Yes' or 'No' status. This aspect of the methodology highlighted our intent to create a versatile, efficient, and comprehensive vulnerability management scope for the ACCESS.

D. New Business Units and Role Optimization

In the fall term of the ACCESS project, the establishment of new business units marked a significant shift in the project's organizational structure. These units were designed with specific roles and responsibilities to streamline asset management and improve overall cybersecurity efficiency. This strategic reorganization allowed for more precise and focused management of security tasks. Unit Managers were empowered with tailored rights and responsibilities, enhancing their ability to manage their units autonomously while aligning closely with the project's overarching security protocols. This restructuring not only improved operational efficiency but also reinforced the project's resilience against cybersecurity threats.

E. Scanning and Reporting Enhancements

Furthermore, the ACCESS project's scanning schedules were meticulously refined for greater precision in identifying vulnerabilities. This was a strategic shift towards more proactive and preemptive cybersecurity measures. Additionally, the reporting system underwent a comprehensive overhaul, transitioning to a more detailed and analytical format. These enhanced reports provided in-depth insights into the project's security landscape, highlighting active hosts and potential vulnerabilities. This advancement in reporting enabled a more rapid and focused response mechanism, improving the project's ability to effectively manage and mitigate cybersecurity threats.

F. Data Analysis and Service Index Integration

The adoption of sophisticated data analysis methods, particularly the use of detailed spreadsheets, significantly enhanced the project's ability to correlate scan results with the Service Index. We utilized a bash script to collect the necessary data from the Service Index website and extract additional details to feed into our spreadsheet task. This meticulous approach allowed for a thorough comparison, ensuring comprehensive coverage and accuracy in the vulnerability scanning process. It was instrumental in identifying and rectifying any discrepancies between expected and actual scan outcomes. Such a detailed analytical process was crucial in aligning the project's scanning activities with its overall security objectives, thereby ensuring a robust and effective cybersecurity framework. Our data-driven approach resulted in a significant increase in the number of hosts being scanned, approximately by 20%, thereby enhancing the project's vulnerability scanning scope.

IV. DETAILED EVALUATION OF THE VULNERABILITY MANAGEMENT SOLUTION-QUALYS

A. Qualys

Qualys offers a cloud-based solution for vulnerability management that includes real-time visibility of IT assets, continuous monitoring, and vulnerability prioritization based on threat intelligence. The platform's key features include a comprehensive IT asset inventory, real-time vulnerability detection, vulnerability prioritization, and integrated patch management. The University of Illinois and NCSA prefer Qualys due to its convenience, cost-effectiveness, and the regular updates for detecting emerging threats.

B. Patching and Responsibility

The patching process for identified vulnerabilities occurs in cycles, depending on the host. For example, Kerberos hosts undergo patching on a monthly cycle. Upon identification of a high-severity vulnerability during these scans, the protocol involves raising Jira tickets. By checking the service index, we identify the party responsible for the host and direct the ticket to them. Essentially, the patching is the responsibility of whoever manages the machine.

C. Reporting Frequency Across Different Services

The frequency of Qualys reports varies across services. For ACCESS, a separate weekly report is generated. In contrast, the National Center for Supercomputing Applications (NCSA) receives daily reports from Qualys, underscoring the dynamic nature of the security environment and the need for frequent checks.

D. Security Analyst Meetings and Critical Response

During the regular security analyst meetings, we review these Qualys reports and evaluate the criticality of the identified vulnerabilities. If a vulnerability is deemed critical, a remediation ticket is raised immediately. For non-critical issues, we typically rely on the usual patching cycle of the machines, trusting the responsible parties to address them in due course.

V. Overview of the Current Quarter's Report

The latest quarterly report illustrates the efforts made in identifying and remedying vulnerabilities within the system. This graph (Fig. 1) details the key findings, progress, and current status of vulnerabilities as identified through Qualys.

Graphical Representation of Vulnerabilities by Severity: A graph is provided in the report, categorizing vulnerabilities by severity levels. The absence of Severity 5 in ACCESS indicates that there are no current threats at this level. The report identifies one instance of Severity 4, showcasing the control over high-severity vulnerabilities.

Trend Analysis Since Last Scan: The numbers (-2, -8, +39) represent the change in the trend of vulnerabilities since the last scan. An increase of +39 might indicate the discovery of new, lower-severity issues or changes in the classification of existing vulnerabilities. A decrease of -8 and -2 indicates successful mitigation in other severity levels. Specifically, the -2 for Severity 5 signifies that there were previously two hosts identified with vulnerabilities of this level. The reduction to zero indicates that these particular Severity 5 vulnerabilities have been successfully addressed and patched.

Ongoing Efforts and Next Steps: The report may also provide insight into ongoing efforts to address current vulnerabilities and plans for future scans and improvements. Key stakeholders should continue to monitor these trends and take proactive measures to maintain a robust security posture. This quarter's report demonstrates significant progress in identifying and rectifying vulnerabilities within the system. Continuous monitoring and an agile response to new and existing threats will ensure the security and integrity of the system moving forward.

VI. Results

The findings from the research on Qualys' implementation within the ACCESS project were both illuminating and affirming, highlighting the platform's tangible contributions to vulnerability management.

A. Enhancement of Scanning Capabilities

The data revealed an impressive 20% increase in the number of hosts being scanned since implementing Qualys. This substantial enhancement is a testament to Qualys' robust scanning capabilities and its efficiency in identifying potential vulnerabilities across a wide range of hosts.

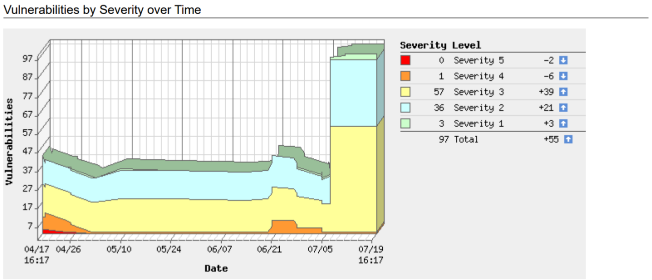

Fig. 1. Vulnerability Scanning Report in Qualys

B. Transition from XSEDE to ACCESS

The development and utilization of a comprehensive spreadsheet facilitated the smooth transition from XSEDE to ACCESS. The spreadsheet served as an essential tool in aggregating critical data such as host names, IP addresses, and other pertinent information. This meticulous organization and tracking allowed for an identification of gaps in the host lists from Qualys, Syslog, and Nagios, and ensured the seamless inclusion of these hosts into the Qualys scanning process.

C. Reporting Efficiency

The differentiated reporting structure, ranging from weekly reports for Access to daily reports NCSA, showcased Qualys' adaptability to meet varying security needs. This tailored approach ensures that security checks are both frequent and contextually appropriate, based on the risk profile of different segments of the organization.

D. Successful Vulnerability Mitigation

The graphical representation of vulnerabilities by severity and the subsequent trend analysis were instrumental in visualizing the control over high-severity vulnerabilities. The data revealed successful mitigation, specifically the reduction of Severity 5 vulnerabilities from two hosts to zero, indicating that these vulnerabilities had been effectively addressed and patched.

E. Business Unit Reorganization and Role Redefinition

The implementation of new business units and role optimization yielded significant results. The primary outcome was the reduced necessity to assign Global Admin status to personnel for accessing the complete range of ACCESS resources. This streamlined access management meant that interns and new users could be effectively assigned to the ACCESS-CI Business Unit, granting them visibility into all relevant asset groups without needing higher-level administrative privileges. This reorganization achieved the end goal of simplified yet secure access control, enhancing operational efficiency and security within the ACCESS project.

VII. Discussion

The choice of Qualys as the vulnerability management system for the ACCESS project was largely influenced by its pre-existing deployment within the University of Illinois, its cost-efficiency, the smoothness of its integration with Splunk, and its consistent updates for detecting vulnerabilities. The familiarity of the staff with Qualys obviated the need for substantial retraining, accelerating its adoption for the ACCESS project. Additionally, its cost-effectiveness was demonstrated as NCSA was able to procure Qualys at the same rate as the university, providing significant financial benefits and avoiding costs related to adopting a new platform.

Furthermore, Qualys's commitment to continuous updates and vulnerability detection, keeping pace with evolving cyber threats, reinforced its position as a reliable choice for vulnerability management. The practical integration of Qualys within the ACCESS project was also highly effective, as seen from the development of a detailed spreadsheet to facilitate the transition from XSEDE to ACCESS. This spreadsheet, which contained critical information such as host names and IP addresses, identified missing hosts from Qualys, Syslog, and Nagios lists, enabling their seamless inclusion into Qualys's scanning process. As a result, the number of hosts scanned increased by approximately 20%, underscoring the improved scope and efficacy of vulnerability management. Further into the project, the introduction of new business units and redefined roles marked a pivotal advancement. This restructuring streamlined access management and enhanced security control, demonstrating a proactive adaptation to the evolving cybersecurity landscape.

VIII. Future Work

The current research offers a thorough assessment of Qualys in the ACCESS project, yet future studies could delve deeper into its long-term effects on the project's security posture. Exploring how Qualys adapts to new vulnerabilities and its ongoing effectiveness in protecting against threats will deepen understanding of its long-term benefits. Additionally, a detailed cost-benefit analysis of Qualys could provide insights into its economic impact, balancing the costs against the financial risks mitigated through enhanced security measures. Moreover, with the rapid evolution of cybersecurity technologies, there's potential for future research to investigate the integration of emerging technologies like machine learning and artificial intelligence with Qualys. This exploration could focus on how these technologies might enhance threat detection and mitigation, further advancing the project's cybersecurity capabilities.

IX. CONCLUSION

In the rapidly evolving landscape of cyber threats, the need for comprehensive and robust security measures has never been greater. This study underscores the critical role that vulnerability management plays in fortifying cybersecurity infrastructure [4]. The implementation and enhancement of Qualys within the ACCESS project demonstrate its capabilities in real-time threat detection and efficient management, proving it to be a valuable asset in cybersecurity. Furthermore, the study takes an in-depth look at various vulnerability management solutions, with a particular focus on the Qualys platform. Our research reveals that while no solution is without its shortcomings, Qualys stands out for its adaptability and resilience in the face of new and emerging threats. The platform's continuous innovation and ability to provide real-time threat detection, vulnerability prioritization, and efficient patch management contribute to its robustness, making it an invaluable tool in the broader context of vulnerability management and cybersecurity. The project's progression, especially with the strategic reorganization and technological advancements, showcases a multifaceted approach to tackling modern cyber threats.

Future research could explore enhancements to the Qualys platform and other solutions, including improving real-time detection capabilities, streamlining the user interface, increasing customization options, and integrating artificial intelligence and machine learning in vulnerability management [5]. Research can also focus on the development of predictive models for threat detection and the evaluation of emerging authentication protocols.

Acknowledgment

This material is based upon work supported by the National Science Foundation under Grant No. 2138307. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Moreover, I am profoundly grateful to my supervisors, Christopher Clausen and Jacob Gallon, for their unwavering support and expertise throughout my tenure as an ACCESS STEP intern in Cybersecurity at NCSA. Equally, I extend my heartfelt appreciation to Professor Gary Schwebach for his immense patience and nurturing guidance that has transformed this journey of my Independednt Study into an invaluable learning experience.

References

[1] Syed, R. (2020). Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system. Information & Management, 57(6), 103334.

[2] Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. Arabian Journal for Science and Engineering, 45, 3171-3189.

[3] Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 65-88.

[4] Ansari, M. F., Dash, B., Sharma, P.,& Yathiraju, N. (2022). The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review. International Journal of Advanced Research in Computer and Communication Engineering.

[5] Ansari, M. F., Dash, B., Sharma, P.,& Yathiraju, N. (2022). The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review. International Journal of Advanced Research in Computer and Communication Engineering