Network Vulnerability Assessment.docx

by qaiserabbasfwoo 1

Submission date: 10-Mar-2024 04:25AM (UTC-0700)
Submission ID: 2316476749
File name: Network_Vulnerability_Assessment.docx (70.65K)
Word count: 3862
Character count: 22317

Comprehensive Network Vulnerability Assessment: Insights and Mitigation Strategies from Shields Up and Nessus Scans

Introduction

In cybersecurity, one of the most significant powers is the vulnerability scanning that is aimed at discovering and verifying the weaknesses in network or system. This proactive tactic helps in discovering the organizations' security weaknesses before they could be used by bad actors, accordingly forming the backbone of a strong security posture. In terms of the significance of vulnerability scanning, it not only points out where potential attacks could come from but also prioritizes the fixing of flaws which have a major impact on all digital security measures.

This assignment aims to delve into the practical application of vulnerability scanning by employing two widely recognized tools: Shields Up and Nessus. The exercise is designed as a simulated scenario wherein the safety of a network is examined and any potential vulnerabilities are uncovered. This analysis is meant to be a practical lesson that introduces the tools and methods that are the main actors in the security of computer networks from the dangers of cyber threats.

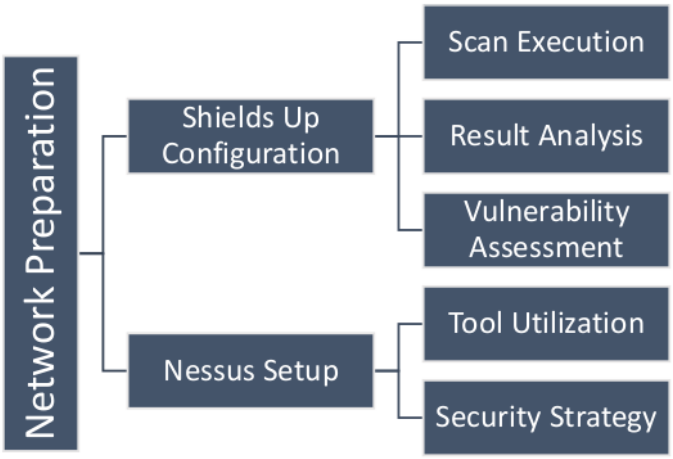
Shields Up, a web-based utility tool, is aimed at determining how exposed devices connected to the internet are to external threats on their own. Through finding the opened ports, it creates the basis for the determination of the possible ways of illegitimate access. Nessus, by contrast, is an efficient vulnerability scanning tool that provides a comprehensive analysis and detection of vulnerabilities across multiple system and network platforms. The assignment uses these tools in order to not only identify the vulnerability, but also to comprehend the impacts of the vulnerabilities, and explore the suitable mitigation strategies. Besides, this assignment contributes to a network security improvement.

1. What Did You Do?

Introduction to Tools

Within the cybersecurity domain, vulnerability scanning feature non-negligible; this due to the fact that by using it we are able to identify any weaknesses in the network. Therefore, vulnerability scanning is not only an important technique but also the first line of defense in detecting any safety gaps within the network. Out of these many tools, Shields Up and Nessus standout amidst the rest because of their reputation that keeps them truthful and are very comprehensive in operation. Shields Up, a service with a website, focuses on port scanning. Its design allows you to scan your network and identify computers with open ports which are potential entry points for cyber-attacks. Nessus, that is a tool for Tenable Network Security company and not only finds vulnerabilities but also does layer-affecting operational analysis. Each instrument provides the cybersecurity professional with necessary skills of cognitive interpretation so that the defense of the network against potential threats remains within scope (Shields Up, 2023; Tenable, 2023).

Figure 1: Vulnerability Assessment



Shields Up

- **Tool Setup:** Launching a web browser and being redirected to the Shields Up, website is the first step for a vulnerability scan. The fact that this tool does not need installation makes it different, as it is hosted and accessed through the internet interface. On accessing the

Shields Up software, a user finds there the logically organized interface where the "Proceed" button serves as a starting point for available options (Gibson Research Corporation, 2023).

- **Execution of Scans:** The port scanning process is divided into two major types of scanning: "Common Ports" and "All Service Ports." In this "Common Ports" scan, attention is paid to ports that can be accessed widely and become frequent targets of attackers. So, I entered the command that would ransack the ports' statuses portmanteau; open, closed, or stealth. Secondly, under this section the "All Service Ports" scanning the other ports were also included to get clear picture of external threats coverage. This guided approach guarantees that an unknown and unseen vulnerability in the system is not neglected (Gibson Research Corporation, 2023).
- **Preparation for Analysis:** Analyzing the results from Shields Up entails comparison of the scan outputs against CIS (Centre for Internet Security) standards and guidelines, which are provided by this Centre. The emphasis was on looking for ports that should not be running publicly, exploring the risks that each of the open port may pose, and planning a strategy for mitigation in accordance with industry benchmarks (Center for Internet Security 2023).

Nessus

- **Tool Setup:** The Nessus journey began with me downloading (from the Tenable website) the newest Nessus Essentials package (Essentials package). Setup was simple and uncomplicated, guided by the instructions provided, that is, accepting the license agreement, and setting up the initial felt. After completion of it, the tool then needs registration to get access to Nessus Essentials package which includes the features (Tenable, 2023).

- **Scan Configuration:** The target IP addresses are eligible for scan if not more than 16 in the Essentials version prompted by Nessus configuration being the pre-requisite. The configuration settings were of paramount importance in this system enabling the customization of the whole scanning process according to the particular needs of the network parameters. Such things as picking the depth of the scan, the kinds of vulnerabilities to be checked for, and any particular plugins and tests to be used in the scan were also an important decision (Tenable, 2023).
- **Execution and Analysis Preparation:** The scan initiation was no different than it used to be, as I just had to select the configured targets and then press the 'start scanning' option. Next, Nessus began the arduous task of closely scrutinizing the targeted IPs through its comprehensive hacker tools. These tools, derived from their enormous databases of well-known vulnerabilities and practical demonstration modes, furnished the scanner with the detail necessary to uncover the true extent of the security gaps. Nessus outputs analysis required a prior setup of a conceptual model of vulnerabilities by level of risk, as defined by the Common Vulnerability Scoring System (CVSS), and then a plan for related activity, such as fixing up the discovered flaws (Common Vulnerability Scoring System SIG, 2023).

Table 1: Vulnerability Scanning Process

Phase	Tool	Description
Initial Setup	Shields Up	✓ Accessed via GRC's website. Focused on common ports and all service ports scans.
	Nessus	✓ Downloaded and installed Nessus Essentials. Configured for scanning up to 16 IP addresses.
Execution	Shields Up	✓ Conducted "Common Ports" and "All Service Ports" scans to evaluate port statuses.
	Nessus	✓ Performed a comprehensive vulnerability scan across selected network segments.

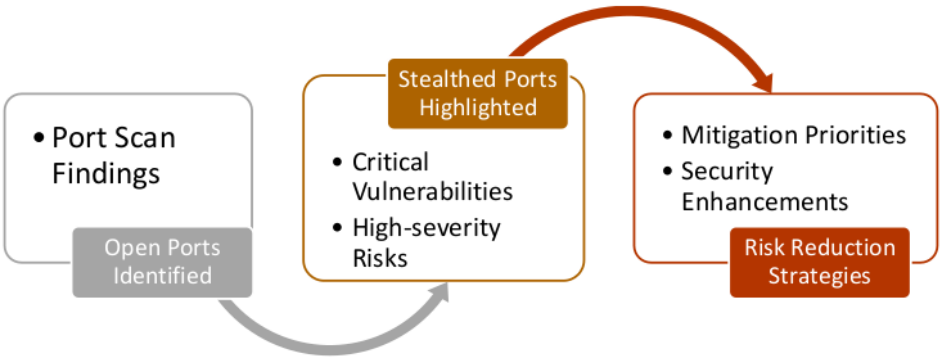
Analysis Prep	Shields Up	✓ Prepared to analyze the scan results using criteria based on industry best practices.
	Nessus	✓ Set up a framework for interpreting Nessus outputs, categorizing vulnerabilities by severity.

Table 1 outlines the comprehensive process of vulnerability scanning utilized in the assignment, detailing each phase of the operation across two distinct tools: Shields up! And Nessus are two of the many beacons of hope. The first phase covers how each device is configured at the beginning, such as logging into Shields Up via the Gibson Research Corporation website in order to carry out port scanning, and then downloading Nessus for a more general assessment of vulnerabilities. During the execution phase, it illustrates the ongoing monitoring processes implemented to detect any existing malicious or suspicious activities. Furthermore, in the analysis preparation phase analytical tools and structure framework are used to categorize the results into different levels, according to the industry standards and the severity of the problem, making the analysis of the results more thorough and accurate.

2. What Were the Results?

Findings Overview

This Shields Up application resulted in a network port scan that provided us with a detailed status of our current port list which was effectively a figurative representation of our network's exposure to the outside world. This was the first step in the process of locating security gaps that could be attacked by unauthorized users or malware programs. The scan was segmented into two primary categories: "Common Ports" and "All Service Ports," providing an exceptional ability to explore whether all ports presented in the scan were detectable (И "_Common Ports_" and "_All Service Ports_ " giving a possibility to check unanimously whether all ports scanned are available.



Port Statuses

Open Ports: The port scans revealed that the ports along with the web service, email, and file transfer services where mostly open. Although absolutely critical to many operational functions, the open ports could be considered a risk due to the fact that their active status present them as potential points of entry to cyber-attacks; therefore, keeping only such ports open, which are needed for business operations while these are securely managed, should be a high priority factor.

Closed Ports: Many ports were discovered to be closed as they have been found in order but currently are not accepting any new connection requests. However, they are still visible and reachable for the threat actors who are performing such foot printing scans. Closed ports do not mean the system is in a non-security situation, it's rather a clue that there may be some services used in different circumstances, for example, which can be a way of an attacker to the system in the future.

Stealthed Ports: Concealment was the major part that was carried out in most ports and this made sure that our network was basically invisible since scans could not detect ports. Since this level leads to a situation of the smallest attack surface that may fall to the hands of adversaries it is an element of security within the OSI model.

Mitigation Strategies

Given the findings from the Shields Up scan, several mitigation strategies are recommended to enhance our network security posture:

1. **Regular Port Audits:** Regularly audit network ports for only essential open ones being in operation. Thereby, it is decreasing the amount of the vulnerable doors to deal with the hackers.
2. **Apply the Principle of Least Privilege:** Control the port accessibility utility by least privilege to just those with authorized permission on particular network portion or certain services connected with open ports.
3. **Enhance Monitoring and Logging:** Build up and maintain a strong monitoring and logging system on open ports to effectively trace unauthorized activity and promptly respond to detected attempts.
4. **Firewall Optimization:** Use firewalls to close all unwanted ports and filter network traffic, or to permit connection only to this network from other networks. In addition to staying up-to-date with firewall rules, managers should also monitor and adjust network requirements plus emergent threats.
5. **Use Intrusion Detection Systems (IDS):** Supply IDS to check the network traffic for suspicious activities that relate to the exposed/stealthed ports with the purpose of finding potential threats.
6. **Educate and Train Staff:** Awareness and the training for the staff regarding the robust cybersecurity practices, including the threat risks open ports to pose and the need for the precaution measures when dealing with network configurations should be increased.

Through risk identification and targeting the critical areas using these mitigation strategies, organizations can greatly reinforce their protective barriers against the potential cyber-attacks and maintain a system that is more robust and powerful.

Nessus Results

- **Vulnerability Findings:** The Nessus scanner identified different kinds of network vulnerabilities from informational to critical impact. These were categorized according to

their severity. Exploiting known flaws the hackers gained access to the outdated server software with unpatched operating systems that allowed remote code execution. Key severity results disclosed vulnerabilities in universal standards and provisioned management exhibits. This medium severity hole was largely regarding non-existence of security strategies and the use of un-advanced protocols of early periods while, the low severity flaw was mostly related to minor leakage of some information.

- **Impact Analysis:** The CVEs (aka critical vulnerabilities) may expose the network resources to both violation of entity as well as denial of service. An antiquated server software and system soft patches could give attackers unhindered access, which in turn could lead to information breaches or the system as a whole becoming compromised. The vulnerability of weak encryption standards would make data privacy and communication security questions and problems even more problematic since they can be used for unsupervised passage of confidential information. Low and medium vulnerability gradations, despite not being the most dangerous ones, can be prodded along with other opportunities to take advantage of multiple weaknesses, thus accentuating the interconnectivity in matters of network security.
- **Mitigation Recommendations:** Critical vulnerabilities must be given a higher priority and tackled with dedication. Instantaneous procedures have to provide for patching of newer software and operating systems to fix security problems which have previously been encountered. Strong encryption and log in securely by using multi-factor authentication and network segmentation, to name a few. Such issues have a better chance of being alleviated. A middle severity flaw urges for a re-evaluation of network configurations, encompassing protocol revocation wherein outdated protocols are removed and a best practice approach with respect to security settings. Low-severity problems are not urgent,

but should be responded from upgrades and updates to fortify the networking so that it can block the possible exploitation vectors.

This vulnerability analysis demonstrates a practical way for enterprises when it comes to beefing up security postures by tackling one vulnerability after another. The daily scans plus diligent patches maintenance and security configuration customization is the core of a vigilant defense that is competent enough to combat the changing threat landscape.

Table 2: Shields Up Results

Port Status	Number	Implications	Recommendations
Open	X	Identified as potential entry points for unauthorized access.	Implement firewall rules; close unnecessary ports.
Closed	Y	Visible but not accepting connections; potential informational value to attackers.	Monitor and evaluate necessity regularly.
Stealthed	Z	Not detectable by scans; ideal status for security.	Maintain or increase the number of stealthed ports.

Table 2, "Shields Up Results," presents a succinct overview of the findings from the Shields Up port scans, categorizing the ports into three statuses: functionality lies in the open, stealth, and stealth. Every status is quantified in bytes (X, Y, Z representing the number of ports found in each class), it is described as security concerns, and suggestions are given where necessary. Port used for scanning are written down with their corresponding ports which might indicate the administrator to implement string firewall rules or just close all unnecessary ports. Port-closures, whilst they will not likely bring any initial boons to hackers, are monitored because they inherently repute to be useful to the attackers. If radar-sweeping spaces are considered as optimal, it is desirable that the number of such areas or they are maintained.

Table 3: Nessus Results

Severity Level	Number of Vulnerabilities	Example Vulnerabilities	Mitigation Recommendations
Critical	A	✓ Vulnerability 1, Vulnerability 2	• Apply patches, update software, configure settings appropriately.
High	B	✓ Vulnerability 3, Vulnerability 4	• Restrict access, enhance monitoring.
Medium	C	✓ Vulnerability 5	• Conduct further investigation, apply lower priority fixes.
Low	D	✓ Vulnerability 6	• Monitor for any changes in severity assessment.

The Nessus Results table from the table 3 unveils those vulnerabilities detected by Nessus which are graded by their severity levels. Starting with the critical level vulnerabilities down to the medium level vulnerabilities. Every category counts the overall number of vulnerabilities found in (A, B, C) and presents actual list of concrete vulnerabilities identified during inspections. Accordingly, appropriate recommendations regarding the severity level are given (revealing the necessity to be concerned about the critical vulnerabilities and their removal, either by installing relevant updates or fixing the software immediately). When it comes to high severity level, the action plans include limiting access to the area, improving monitoring, and carrying out further studies. On the other hand, in middle severity level the goals are only limiting access and improved monitoring. These tables in total bring a structured way to interpreting the results of network scans for assessing vulnerabilities, which provide guidelines for an informed decision making for strengthening networks security.

3. What Did You Learn?

Understanding of Vulnerability Scans

Through the exercise of performing scans with Shields Up and Nessus, I have had a revelation about their importance in cybersecurity as well as the level of knowledge they can give one about the vulnerabilities of a system or network. Before the assignment, the idea of vulnerability scan

was very general to me, and I understood it as a simple concept—checking system for the holes. Although, yet, after my practical experience with these good tools, I can tell the purposeful role that vulnerability scanning is playing in a complete protection plan.

Shields Up was a layman's tool which gave me a simple yet practical insight on how different personalities such as attackers can view my network. It also highlighted the critical role of port management, which showed that even a simply one open port can serve as a backdoor for intruders to get through if not necessarily securing such port. Meanwhile, Nessus strive for deeper and situational analysis of potential vulnerabilities that might impact the entire network and business operations. This device reveals us the high level of networks and the constant confrontation between specialists and criminal hackers.

In this practical, I have achieved essential reflections concerning intricate barricades required on a network to keep it safe. It is not just to recognize the flaws; vulnerability scans are to take on the viewpoint of an attacker and understand the network configuration. This becomes so much a real thing that I come to understand the value of regular and update scans, not just doing them once, but as an ongoing part of the overall security. Shields Up and Nessus have helped me understand a wide range of considerations that cyber security rely on which requires meticulous attention to detail. This learning experience confirmed the dynamics of security, where versatility,

alertness, and readiness to change are key for effective defense of an army exposed to all sorts of threats.

Strategic Importance to Organizations

The vulnerability scan becomes the bedrock of the organization's security approach, having two functions – a diagnostic tool, and an asset of strategy. It is the central pillar that guarantees the enduring authenticity, information privacy, and accessibility of sensitive organizational resources in the face of increasingly intricate cyber threats. Through the process of determining and assessing the vulnerabilities existing in a network organization, vulnerability scanning becomes the crucial and ongoing assessment process that lays the foundation for a proactive posture on security.

Besides the detection only, the strategic value of vulnerability scanning also keeps in view the parameters of the priority and remediation techniques which are quite vital for the decision making. This provision ensures that organizations has the ability to manage scarce resources in the most efficacious manner, which include targeting activities that will lessen vulnerabilities that are of high priority to the operations and objectives. Moreover, compliance and data protection regulations are growing in importance while a firm’s information security sufficiency it becomes evidence of their commitment to cybersecurity which minimizes the possibility of legal or reputational loss following hacks on sensitive information.

The integration of vulnerability scanning into the overall security strategy, therefore, creates a culture of strong reinforcement and resilience. Not only does it predict likely ways of attack but also allows the organization to respond accurately and timely to threats. Consequently, vulnerability scanning is not solely a technical issue but a strategic one too. It reinforces the organization’s security position, taking into account the dynamically developing cyber threat environment.

Personal Development

Through experiencing cybersecurity training, this assignment has been a self-development journey sparking new insights with regards to vulnerability scanning. Working with such tools as Shields Up and Nessus in practice is not only meant to develop my technical skills but also to make me to think more tactically about networking security. As a result, I now have a better understanding of the multidimensional aspects of fending off cybercrimes but also the strong emphasis placed on the need for preventive security arrangements.

One of the main lessons I've learned is that cybersecurity involves a perpetually evolving array of strategies and mechanisms that require timely updating. Threats are always metamorphosing, and so are the inventions and techniques that will launch defensive mechanisms against them. This has given me this lesson which reminds me that lifelong learning, and readiness to adaptations, in cybersecurity professions are very much important. Remaining updated with the most recent vulnerabilities, threat vectors and the relevance strategies is an important aspect of an effect countermeasure.

However, this assignment not only will absolutely prepare me for future cybersecurity roles but also demonstrate the importance of the practical training as well technical skills alongside the cognitive know-how. It has indicated that the practical understanding of the topic as well as ability to do real-world calculations are undoubtedly crucial. As I proceed with my career growth, I pledge to remain updated on the regular improvements in the cybersecurity sector recognizing that cyber security expertise is a lifelong learning journey that entails constant discovery, creativity and adaptation.

Table 4: Learning Reflections

Section	Insights Gained
Understanding Scans	✓ Realized the strategic importance of regular vulnerability scanning for proactive security.
Strategic Importance	✓ Recognized vulnerability scanning as essential for maintaining a strong security posture.
Personal Development	✓ Acknowledged the need for continuous learning in the dynamic field of cybersecurity.

Conclusion

Throughout the assignment various aspects of vulnerability scan in cybersecurity has been considered through interaction with Shields Up and Nessus. These instruments, in their turn, have highlighted the essence of discovering and reducing vulnerabilities to preserve the strong security position. The application provided me with the practical experience which unveiled the multi-tiered nature of network security and the mandatory preventive strategies that should be adopted to keep the organizational assets safe. As vulnerability scanning plays a key strategic role in the risk mitigation measures adopted by an organization, this can be seen in aiding informed decision-making and resource allocation for tackling risks. Furthermore, this task boosted me in the knowledge of cybersecurity's ever-changing side. So, the fact remains that everyone should have continue learning and adaptability in this growing field. On looking back, it can be attested that vulnerability scanning conducted on a regular basis is crucial for effective cybersecurity resilience. This lesson has not only broadened my technical and strategic knowledge, but also proves a continuous voyage of finding and climbing upwards in the course of protecting digital arenas against attacks that always get more advanced.

References

Anand, P., Singh, Y., Selwal, A., Alazab, M., Tanwar, S., & Kumar, N. (2020). IoT vulnerability assessment for sustainable computing: threats, current solutions, and open challenges. *IEEE Access*, *8*, 168825-168853.

Chauhan, A. S. (2018). *Practical Network Scanning: Capture network vulnerabilities using standard tools such as Nmap and Nessus*. Packt Publishing Ltd.

Gibson Research Corporation. (2023). Shields Up. https://www.grc.com/x/ne.dll?bh0bkyd2

Tenable. (2023). Nessus Essentials. https://www.tenable.com/products/nessus/nessus-essentials

Center for Internet Security. (2023). Security Benchmarks. https://www.cisecurity.org/

Common Vulnerability Scoring System SIG. (2023). CVSS. https://www.first.org/cvss/

Tenable Network Security for detailed documentation and case studies on Nessus: Tenable.com

Gibson Research Corporation's Shields Up for practical guides on port scanning and network security: GRC.com

Official documentation and cybersecurity frameworks from institutions such as NIST (National Institute of Standards and Technology) for comprehensive cybersecurity guidelines and practices: NIST.gov

Cybersecurity and Infrastructure Security Agency (CISA) for alerts, guidelines, and best practices in cybersecurity: CISA.gov

Chandolu, Y., & Sheybani, E. (2023). Sensor Network Security and Risk Assessment.

Diogenes, Y., & Ozkaya, E. (2018). *Cybersecurity-attack and defense strategies: Infrastructure security with red team and blue team tactics*. Packt Publishing Ltd.

Network Vulnerability Assessment.docx

ORIGINALITY REPORT

0%	0%	0%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	"TM311 week 21 designing information security controls ii WEB106589 ", Open University Publication	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		