IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Exploring Optimal Approaches to Vulnerability Assessment Through Manual Testing and Automated Tools

[1]Prashik Shinde, [2]Yuvraj Singh Rathore, [3]Mansi Sonawane
[1]MSc CS, [2]MSc CS, [3]MSc CS
[1]B. K. Birla College, Kalyan, [2]B. K. Birla College, Kalyan, [3]B. K. Birla College, Kalyan

Abstract: Vulnerability assessment, in simple terms, is the process aimed at protecting sensitive data, resources, systems, or infrastructures from attacks by identifying weaknesses that can be exploited. A risk management process is how the self-assessment in its complexity, defines the risk following the degree of its impact and the possibility of use. To determine the presence or absence of vulnerabilities, it is important to choose between employing automated tools and performing manual testing and know which way is the best for the aimed performance within the specific time.

This research paper will focus on the qualitative evaluation of the processes regarding vulnerability assessment with a focus on automated tools and manual testing to appropriately meet the requisite output volume and quality. It is expected that most of the findings will be helpful in promptly addressing the relevant scenarios and timelines to apposite vulnerability assessment methods. To do that, the study will focus on applying both approaches to see what is more efficient in what conditions.

A thorough study has revealed that the automated testing approach can be time-consuming and involves a lot of effort. Manual testing, otherwise, tends to focus on specific types of vulnerabilities but is faster. The ideal approach will seek to combine the two testing strategies into a hybrid approach, which is expected to strike the best possible balance. This will also provide a complete reporting mechanism that meets regulatory requirements and ensures that timely reports are available.

Keywords: automated tools, manual testing, vulnerability assessment, etc.

I. Introduction

In a world where modern cyber threats continue to grow in sophistication, effective protection of any digital infrastructure is becoming even more imperative. The growing connectivity of computers through Internet, the increasing extensibility and the unbridled growth of the size and complexity of systems have made system security a bigger problem now than in the past.[1] Vulnerability is the intrinsic and dynamic feature of an element at risk (community, region, state, infrastructure, environment etc.) that determines the expected damage/ harm resulting from a given hazardous event and is often even affected by the harmful event itself.[2] One of the most critical activities in this respect is vulnerability assessment so that vulnerabilities in various systems can be located, assessed, and ranked.[3] Vulnerability assessment depends on various factors such as appropriate theoretical concepts and quality and adequacy of information gathered.[4] Several literature reviews target a specific subset of penetration testing, and vulnerability assessments, such as web-based penetration testing[5], cloud device penetration testing[6], and penetration testing enhanced by AI (Artificial Intelligence)[7].[8] There are various approaches available to conduct the vulnerability assessment activity. This procedure, too, has changed over duration with two advancements: Firstly, through the efforts of human resource, i.e., manual testing approach and then through the assistance of machines, i.e., automated testing approach. Manual testing, on the other hand, depends on the skills and knowledge of people, whereas automated systems are quick and efficient, especially for large systems. Both approaches have strengths and weaknesses and it is seldom that a single technique is used effectively to carry out a comprehensive vulnerability assessment. This study aims to discuss and examine how manual penetration testing and vulnerability assessment automated tools can complement each other in the process of vulnerability assessment in the existing threat environment.

This paper carries out a comparative study between automated tools and manual penetration testing about the identification of vulnerabilities. The paper commences by detailing some basic concepts of concepts that bear on vulnerability assessment which includes its scope, methods, objectives, and relevance in the field of cybersecurity given the fact that changes in cybersecurity threats are incessant. The paper also describes manual testing as being carried out by humans who engage in procedures that are time-consuming such as penetration testing and security auditing as opposed to having an automated system that scans the systems based on preset conditions. The two put-forward methodologies have their merits and demerits, for instance, manual methods are more context-sensitive and flexible but tend to be slow and sometimes prone to biases while automated methods, on the other hand, are fast and consistent but may generate false alarms or miss even some of the minor defects. This research aims to justify the optimal efficiency that integrates both methodologies. This plan will be furthered through the creation of a strategy that will allow for concurrent use of automated scanning and naked-eye testing which is expected to furbish the processes of a company regarding its context and risk level. The effectiveness of these approaches will be assessed through detection and false positive rates, cost and time efficiency, as well as efficacy towards organizational security. Real-time case studies will illustrate how this integration has been successfully implemented in various environments with different tools and outcomes. Ultimately, the paper aims to provide organizations with recommendations that will enhance the effectiveness of their vulnerability assessments and, consequently, contribute to the development of stronger security strategies and improved risk management practices.

II. METHODOLOGY

The research adopts a common protocol for the evaluation of the different techniques of Vulnerability Assessment (VA) Most of the sections include the following steps: -

1. Literature Review
   The purpose of this paper was to present the results of existing studies, with particular emphasis on methods, tools, and techniques of Vulnerability Assessment (VA), a systematic review was performed. This also assisted in recognizing the problems in the knowledge base of the area and specified the scope of research of the present study.
2. Learning the Automated VA Tools
   Determined were tools for the development of an automated process of the VA. This is about setting up the tools, scanning using the tools, and understanding how to read the outcomes for practical experience.
3. Manual Method of Passing through VA
   At the same time, we analyzed the way the WA is performed without the employment of automated machines, namely, using manual penetration testing, vulnerability scanning, and areas concerned with other branches of security testing. The aim was to retrieve the approximate patterns of a real attack to investigate the effectiveness of the manual technique with that of automation.
4. Both Approaches are implemented
   This also involved developing environments for testing automated as well as manual techniques of VA. For instance, the automated tools were used to prepare reports on areas of weakness, whereas in the manual, each weakness was tested. Thereafter the records made were compared.
5. Comparison of Reports Substitutively, reports were made for the two testing methods, the automated tools and the manual tool followed by their cross-comparison. This was done by considering several key aspects, such as the quantity of discovered vulnerabilities, their characteristics, and the time in which these data could be collected.
6. Conclusion and Inference The possible advantages and disadvantages of these two methods were also brought into focus in terms of the comparative analysis. The last part of the research is dedicated to some conclusions

made from this comparison and more useful lessons on how VA can be done and possible gaps for further studies or improvement.

III. Implementation and Analysis

For the entirety of the research, the following tools and technologies were used:

1. Nmap
2. Tenable Nessus Essential
3. Oracle VirtualBox
4. Metasploitable Linux 2

To begin with, the researchers installed the Metasploitable Linux 2 in Oracle VirtualBox. They then proceeded to scan the system and produce reports, as well as an automatic vulnerability assessment using the Advanced Scan feature of Tenable Nessus Essential. This operation took an amount of time of two hours and thirty-six minutes but gave a comprehensive report on the vulnerabilities encountered.

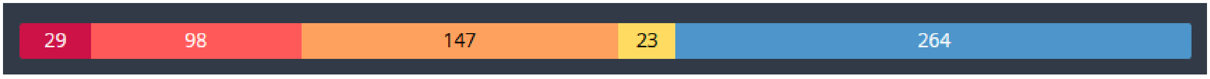

Figure 1

This figure is 1 which depicts the ‘complete with a color code’ list of vulnerabilities that were missed by the tool.

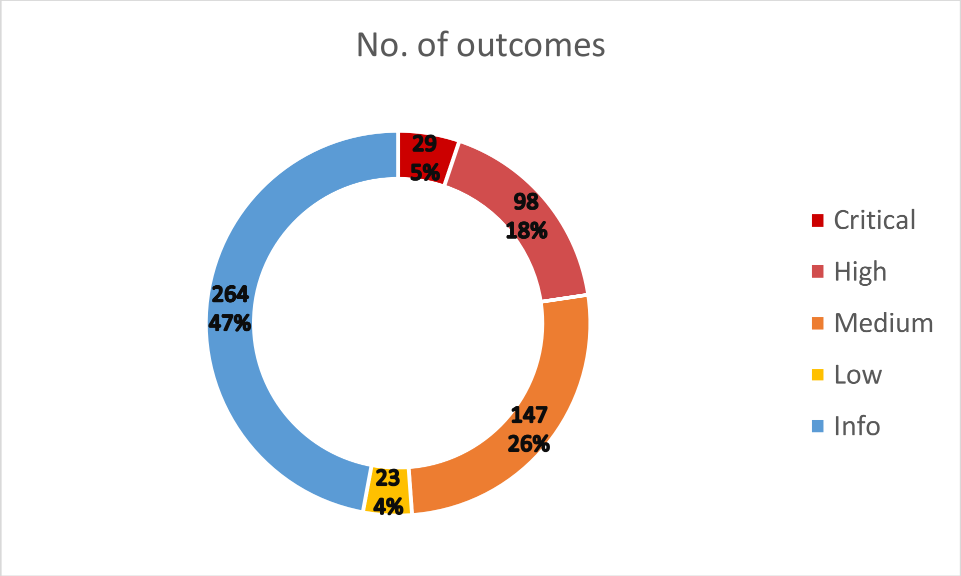

Figure 2

According to Figure 2, a summary of the vulnerabilities identified using the automated vulnerability assessment tool Tenable Nessus Essential is shown. In variance, out of about 23 homemade tested open anchorages, only the factual exploitative anchorages are meant to be linked through penetration testing, which was relatively quick to analyze and took less than a minute.

Because the two methods have been perpetrated, the following logical perceptivity was gathered regarding each system.

Automated Vulnerability Assessment Advantages: Nessus Essentials

1. Volume and Scope of Vulnerability Coverage

- Coverage: Nessus software guarantees a broad vulnerability coverage by performing a complete vulnerability scan and discovering other weaknesses, including common vulnerabilities, exposures, configuration vulnerabilities, and compliance-related issues. It has weaknesses in identifying known vulnerabilities, zero-day vulnerabilities, configuration vulnerabilities, obsolete software and protocols, and weaknesses there is a lot of information for future remediation planning.
- Built-In Vulnerability Correlation: Nessus has known vulnerability databases (CVE and CVSS) that explain how each vulnerability can be exploited alongside its CVSS rating. This correlation provides a detailed range of views that would take significant effort and time to obtain manually.

2. Accelerated Speed and Automation of Complicated Scanning

- Simultaneous: Automated and Consistent: Complex scans can be efficiently done through Nessus since complex scans executed on different systems and assets will produce the same results, helping to achieve uniformity in vulnerability detection. This consistency in the performance of multiple scan results helps reduce human error and helps in setting a definite baseline for the outcomes of each scan.
- Time for Large-Scale Scanning Reduced: Nessus performs extensive scans much faster automatically than manually in networks that contain large numbers of thousands of assets even though one automated scan takes hours. This is because automation enables cross-scanning of many systems at the same time which is impossible with manual evaluations.

3. More Reports that are Detailed and Customization Possibilities

- Comprehensive Reports Accompanied with Severity Graphs: Nessus produces in-depth reports with a standard degree of severity graph which persons in charge of the security teams can rely on to prioritize their efforts (the graph can be critical high medium and low) and helps in categorizing vulnerabilities based on the risk levels. These reports also come with user-friendly graphs and tables that depict historical data on security trends.
- Reporting To Customized Reporting for Different Audiences: Reports can be cut differently to meet different needs including that of the security departments which require detailed technical documents while the administration requires a few lines with key points highlighted. This flexibility enhances communication across teams and ensures that everyone is on the same page regarding the security posture.
- Compliance-Specific Reporting: Nessus offers templates and frameworks that align with industry regulations (e.g., PCI-DSS, HIPAA, NIST). These compliance-focused reports assist security teams in preparing for audits and documenting adherence to regulatory requirements with minimal extra effort.

4. As to Contextual Remediation Guidance

- Capabilities Placing Remediating Action: Nessus provides detailed and succinct remediation details, which makes it possible for security teams to respond quickly to the vulnerabilities they have discovered. Such recommendations often contain links to the vendor patches, suggestions on the settings, and how to deal with certain threats.
- Exploitation Potential as the Basis of Evaluation: Nessus monitors the potential of vulnerabilities to be exploited to determine those that are capable of being exploited in practice. This assures that those issues that need to be fixed most urgently are dealt with first.

5. Revisioning & updates tracking the threat’s history.

- Vulnerability & security database with the stress on ‘updating’. For example, Nessus will always be able to detect recent vulnerabilities as Nessus continues to offer its old database for potential threats and simply integrates any newer ones whenever they come along. This consistent update of the vulnerability database helps the security teams to mitigate novel threats.
- Apprehension of Threat Intelligence: Nessus Essentials can work with many Tenable products (such as Tenable.io) to enhance its threat intelligence and thus improve detection. New threats can also be detected by working with other security solutions (e.g. SIEM and SOAR) and extending, even more, its role in a suite of cyber security measures.

6. Scalability for Large Environments

- Efficient for Large-Scale Network Security: Nessus has a good degree of scaling across many systems and hence is useful for large companies with large distributed networks and geographical coverage. It offers companies and head offices a chance and ease to manage policies and supervise the vulnerability monitoring state of all assets from a single location across the spectrum.
- Supports Distributed Scanning: Nessus is designed to work in distributed setups with remote scan units meaning that the software is best suited for firms with different physical setups or with a strong virtualization exciton.

7. Resource Optimization and Integration with Other Security Tools

- Integration with Incident Response and SIEM Systems: Nessus incorporates SIEM (Security Information and Event Management) systems, enabling the system to automatically respond to incidents by sending out alerts resulting from assessing vulnerabilities. This integration helps reduce the barriers to managing vulnerabilities and improve how fast an incident can be addressed.

- Efficient Use of Security Resources: Automated tools limit the need for active manual supervision, enabling security analysts to spend their time determining the best ways to eliminate vulnerabilities instead of seeking such vulnerabilities. Such a resource deployment makes the most of a minimal security workforce.

Automated Vulnerability Assessment Disadvantages: Nessus Essentials

1. High Initial and Operational Costs

- License and Subscription Fees: Despite the availability of a free version, Nessus Essentials has the possibility of upgrading to some premium tiers. More often than not, premium licenses and subscription fees attract hefty amounts, with big organizations being the target of these fees. This amount tends to create budgetary limitations, especially in small to mid-sized organizations.
- Potential Need for Additional Software/Modules: Apart from many organizations utilizing a Tenable cloud environment module or an on-premise Tenable server managing one, additional operational cost is incurred due to the module necessity. This necessitated bundling modules tends to increase the total cost.

2. Network and System Resource Demand

- High System and Network Usage During Scans: Nessus basic lifecycle scans can achieve this by conducting an exhaustive scan on an entire network which utilizes a lot of system resources. Scanning can also intimidate workloads on the network and systems without the right scanning scheduling.
- Longer Scanning Duration for Comprehensive Scans: However, in proper undertakings, it is possible for an extension scan to be completed in a few hours but this may vary depending on the size of the network, hitting up to days. From your setting, the estimate was approximately 2 hours and 36 minutes were necessary to perform the host scan. This long scan range could impede rapid vulnerability discovery in time-critical situations.

3. Security Concerns

- Automated Scanning Tool Dependence: Using an automated tool like Nessus on its own presents risks since there are gaps that the automation will never be able to comprehend without a human touch such as logical errors and one-off misconfigurations. The lack of a sledgehammer approach could potentially lead to arrogance in the organizations, overlooking the necessity for slow techniques.
- Security Blind Spots: There are even times when Nessus might generate false positives, i.e., boreholes that can be considered non-existent in the geographic region of interest and some other times even generate real penetrations. These inaccuracies require extra verification and validation that is often manual in nature or tool-secondary.

4. Contextual Factors of Complex Systems' Exploiting Capability Remains Unknown

- Missing Exploitability Cypher - Contextual gap on Exploitability: Nessus has all of the capabilities to find deficiencies but most of the time takes into consideration the context of the risk of that deficiency (such as all configurations, types of usage, and context) which can be decisive in the level of actual exploitability out there in the wild. In simple words, not all high-rated deficiencies will get exploited, and similarly, not all low-rated deficiencies will remain low risk due to frustration in configurations.
- Does Not Address All Types of Vulnerability: Nessus Essentials targets common vulnerabilities and configuration weaknesses but specific vulnerabilities or some of the insider threats may be overlooked and these are best through manual testing, physical security assessments, or behavioral analytics.

5. Demands Daunting Skilled Interpretation of Results

- Dependency on Experienced Personnel: The analysis of Nessus results is dependent upon skilled analysts. As much as Nessus can specify certain details related to the weaknesses, such details can be misinterpreted or misunderstood creating a situation where an effort to address the issues, for instance of low priority, but none of the crucial ones, is made.
- Challenges in Handling Vast Amounts of Outputs: Quite a few of Nessus Essentials outputs come in the form of bulky and comprehensive reports. For example, it is expected to produce hundreds of findings that have several risk levels e.g. Critical, High, Medium, Low, and Informational that need trained people to separate the relevant findings from the rest and rank them in order of relevance.

6. Use and need to make Regular Changes in the Environment

- Nessus Needs to be Regularly Updated So That Security Can be Maintained: Unfortunately, Nessus depends very much on a regular update to be able to reflect the current vulnerabilities. In short, where there has been a lapse in updates, the chances of missing out on scanning effectiveness improve since newly mooted weaknesses will not be able to be included.

- Interruption in the Functionality of Nessus is a Possibility: Because they are sometimes necessary changes, the addition of changes to Nessus updates means that some productive functionality in terms of scanning and other security measures has to be postponed for a certain time. Also for environments that are air-gapped or have very high restrictions, the dependency of Software on external internet access will pose problems.

7. Customized Processes to Meet Scoped Assessment Requirements are not available.

- Flexible Customization for Variant Scenarios is Lower than Manual Approaches: Nessus has its advanced scanning techniques but there aren't many flexible options when seen from the perspective of manual testing wherein specific instructions can be focused on selective testing narratives or cones. Complex setups with distinctive designs may require additional independent assessment to address designated risk scenarios.
- Completely obviate the need for Hybrid Methods: While Nessus Essentials is an impressive suite that strives to provide an effective baseline, it does not fulfill the requirement for the hybrid methodologies including social engineering, physical security, or application dependence testing that are crucial for security assessments in certain, risky environments.

Advantages of Performing Manual Vulnerability Assessment With Nmap

1. Quick and Effective in Port Scanning Activities

- Scan Activity Owns Speed Edge: Nmap is capable of scanning hosts for active and open ports in a short time. You know in your enclosed assessment, it took less than a minute to perform the scan, which is beneficial in dynamic situations or in massive network traffic environments where prompt examination is required.
- Assessment on the Fly: The users, through Nmap, can scan the structure of the network and there is an opportunity to see the overview of what services and devices may need testing which saves a lot of time in such scenarios. This gives an edge in times of emergencies such as active security threats or environments when constant scanning has to be done.

2. Uses Little Resources and Has a Lightweight Profile

- Minimal System and Network Weight: An important tool scan is virtually imperceptible when it comes to network and operational burdens. This nature of lightweight materials is beneficial for the scanning of the production environment as even delays will affect business processes so well.
- Computational Resources Are Economized: The application works lean in terms of CPU and memory, making it possible to run on smaller systems or workloads distributed across system instances without the need for additional hardware.

3. Specialization and Modification of Scanning

- Multiple Scanning Facilities: Nmap has different scan types (SYN, TCP Connect, TCP, ICMP, etc.) and parameters that, when included, prove useful in meeting specific scanning needs. For instance, a SYN scan may be employed in situations where stealth is a key concern while service version detection gives hints about the software useful that is available on open ports.
- Available for various circumstances: Nmap is quite useful as it enables security analysts to carry out leur scans on almost any network configuration such as screened or firewalled networks and modify their scans to fit the type of network, size as well as security objectives.

4. Economical and Easily Accessible

- Completely Free and Open Source: As Nmap is open-source, it can be used by organizations that do not have any resources. This free availability is very useful to smaller organizations or educational institutions that cannot afford expensive automated tools easily and effectively to check and scan networks and systems securely without any worries over finances.
- Virtually No Limitations with Community: Nmap is a popular open-source software thus the developer and user community is huge. This community offers help in the form of documentation, videos, and Nmap tutorials, extensions that greatly help security professionals to know more about Nmap and how to use it as well as improve the existing Nmap features.

5. Useful for Network Mapping & Reconnaissance

- Network Topology Visualization: Nmap plays a crucial role in determining and classifying network structure, especially with regards to the inter-relationship between devices, recognition of phantom devices or effects, and configuration of the structure. This ability to map out networks is fundamental in appreciating how the different elements of a network perform, which is useful in promotional defense measures.
- Host Discovery and Asset Management: Nmap is useful even in the management of assets in a critical security process, through the detection of all hosts that are active in a network. Awareness of what is on the network helps organizations in asset configuration management oversight and policy enforcement compliance.

6. Minimizes Dependence on Automated Tools

- Manual Verification of Findings: Because of the manual Nmap scanning, analysts can confirm and check the results brought about by automated scans, hence reducing false warnings from such automated tools. In this manner, a security team would be able to enhance the accuracy of determining the seriousness of the findings by going through several open ports or services.

7. Nmap has Displayed More Than Adequate Control of the Scanning Procedure

- Granular Control for Experienced Users: In experienced users, such restrictions do not apply as such users can control every single aspect of the scan including its depth, when it is conducted, and what specific commands are sent to avoid being detected. Such fine-grained control could be an advantage when used in highly sensitive environments or in a penetration test context where stealth and precision are essential.

Cons of Manual Vulnerability Assessment with Nmap

1. Fails to Identify the Vulnerability Itself in Several Instances

- It Cannot Directly Determine the Existing Vulnerabilities: The purpose of Nmap is to perform reconnaissance on open ports and services yet does not specifically highlight CVEs or similar policies that might apply to those services. Although the information regarding the open ports is somewhat helpful, one would still need to conduct further research and triangulation upon the information to discern the threats posed.
- Security practitioners must correlate the open ports and the services that were detected with databases of known vulnerabilities: Time and effort are required to confirm the existence of vulnerabilities with specific Exploit-DB, CVE, CVSS, and several other databases. Alternatively, the risk of making an error at the level of analysis remains high hoping it does not turn out to be one of the most detrimental consequences.

2. Needs Abundant Skill and Knowledge

- Understanding is Important: When using Nmap effectively, it is essential to know about network concepts, services, and various scan types. If a scan is not configured properly, it will return partial or inaccurate results, and a novice may miss critical information.
- Results Imagineering is a Complex Activity: To be able to correctly interpret Nmap results, one must be ready to analyze service banners, relate the open ports to the structure of the arrangement, and interpret the importance of these designs. Team members without such skills run the risk of underestimating the degree of the finding or overestimating exploitable configurations.

3. Scant Reporting and Analysis Caps

- No Native Reporting Features: Nmap does not have any reporting features. It does not give analysts the option to export or create templates for external reports on a scan. This is contrary to automated tools that do not require much effort from the deadline to prepare. Nmap does not provide any reading in terms of the number of excessive vulnerabilities, which means that the analyst has to do everything from scans.
- Lack of Reporting of Suggested Remediation Techniques: Unlike this other type of tool, Nessus specifically offers a description of the vulnerabilities together with a proposed how to fix them, Nmap can only offer information on the services that are running. Security personnel will have to understand the data and look for relevant measures on their own, which will make the whole process complex.

4. The Cost of Manual Work Associated with Comprehensive Assessment

- It's Unbearable in Great Ecosystems: Although Nmap is efficient when a single scan is conducted, performing comprehensive audits of large networks with hundreds or thousands of assets is resource-consuming. Because manual scanning and analysis over large networks has been time-consuming, scalability has been limited.
- Something Purpose-built is Either Very Hard or Possible: Some aspects of vulnerability assessments using Nmap include configuration and compliance checks and deep vulnerability coverage. For this purpose,

organizations would be required to purchase other tools or undertake manual checks to augment Nmap which adds more time and complexity.

5. There Is the Risk of Omitted Context-Sensitive Vulnerabilities

- May Warrant Network Configuration Restrictions: Certain network contexts or patterns of behavior whereby certain vulnerabilities exist that Nmap may not be able to recognize. Some of these weaknesses may be applicable at the application layer or may be multi-vector in nature, which cannot be performed by Nmap default scans resulting in a potential coverage security gap.
- Assumes Exploitability is Not Provided in Such Situations: Though the Nmap tool displays enabled ports, the software does not address how exploitable those ports are in the application context, practices, and configuration. As such security teams might not develop a clear and comprehensive view about the situation where the open ports found in the scan are all exploitable or not.

6. New Vulnerabilities Not Added Through Automated Updates

- Serious Manual Updates Source Of Threat Intelligence: As Nmap does not include automatic updates as automated tools, security analysts are required to manually update new techniques or insights related to new threats, further necessitating a continuous learning and upkeep need for the individual or system.
- Advanced Threats Still Undetected: Deep scanning of the NMAP tool shouldn’t be relied upon to detect advanced threats like the ones that need an authentication scan or those that employ deep protocol inspection techniques. Without additional plug-ins, some vulnerabilities, particularly the ones regarding security segmentation of certain environments, may go undetected and not subject to indentation further analysis.

7. Poor Performance in Compliance and Regulatory Performance Measurement And Reporting.

- Compliance Framework Check Not Available: Nmap does not conduct regulatory checks against any frameworks – PCI-DSS, HIPAA, or NIST. Organizations that have to follow compliance will have to seek out other applications for compliance reporting, owing to Nmap features no templates, policies, or standards that are inside the automated compliance tools.
- Non-standardized feedback is a Significant Drawback During the Auditing Process: The enormous disadvantage is that Nmap does not create standard reports meaning that the general findings might be hard to file during the course of submission of the findings for compliance audit. The absence of standardized reporting may hinder efforts to comply with regulatory obligations or, provide sufficient evidence for audits.

IV. Result and Discussion

Following is the comparative analysis of the both of the approaches:

Aspect	Automated Vulnerability Assessment (Tenable Nessus Essentials)	Manual Assessment (Nmap)
Detection Depth	Comprehensive detection of known vulnerabilities, misconfigurations, and compliance issues.	Limited to open ports and basic service detection.
Vulnerability Scope	Broad coverage, including OS, applications, and network vulnerabilities.	Focused primarily on network services and open ports.
Reporting	Detailed, standardized reports with severity ratings and actionable remediation steps.	Basic output with limited detail; lacks structured reporting.
Speed of Assessment	Takes hours for comprehensive scans (e.g., 2 hours 36 minutes in your case).	Extremely fast, typically under a minute for initial scans.
Resource Consumption	High resource usage during scans, can impact system performance.	Low resource consumption; minimal system impact.

False Positives/Negatives	Possible false positives; occasionally misses nuanced vulnerabilities.	Risk of human error; may miss complex vulnerabilities.
Contextual Awareness	Correlates vulnerabilities with CVSS scores and threat intelligence.	Limited context; relies on the operator's understanding.
Customization	Limited customization of scans; mainly uses predefined templates.	Highly customizable commands and scripts for targeted tests.
Remediation Guidance	Provides actionable recommendations and links to patches.	No built-in remediation guidance; requires manual research.
Compliance and Regulatory Support	Supports compliance reporting with templates for various standards (e.g., PCI-DSS).	Lacks structured compliance reporting.
Integration Capabilities	Integrates with SIEMs and other security tools for streamlined workflows.	Limited integration capabilities; primarily a standalone tool.
Scalability	Scales well for large organizations with distributed assets.	Less effective for large networks; manual efforts can become unmanageable.
Skill Level Required	Basic technical skills needed for execution required skilled personnel for effective interpretation and action on findings.	Advanced technical skills are needed for execution as well as deeper skills for analysis.
Frequency of Updates	Regular updates to the vulnerability database; require internet access.	No automatic updates; relies on manual verification of findings.
Operational Costs	Higher initial and operational costs due to licensing and maintenance.	Low cost; primarily dependent on manpower and tools.
Time to Results	Longer time to obtain comprehensive results due to scan duration.	Immediate results for initial reconnaissance.
Historical Analysis	Tracks historical data for vulnerability trends over time.	Limited historical context unless manually logged.
Operational Flexibility	Less flexible in adapting to unique scenarios; may need manual validation.	Highly adaptable; can test specific hypotheses or configurations.
Security Posture Improvement	Provides a holistic view of security posture; helps prioritize risks.	Useful for targeted assessments but may miss the broader context.

Table 1

V. Conclusion

Automated Vulnerability Assessment (Tenable Nessus Essentials)

1. Depth and Scope: Nessus employs in-depth detection and scanning processes in all strategies, including scanning for security compliance for application and operating system vulnerabilities, outdated software, and other misconfigurations. It utilizes a vast number of vulnerability databases (CVE, CVSS, etc.) to cross-reference and assess vulnerabilities contextually.
2. Speed and Efficiency: Large networks can be quickly evaluated by automated scans (although hours-long scans are necessary), as they are able to assess the whole network quickly. For example, the scoping study established a scanning time of close to 2 hours and 36 minutes, indicating the time savings for large-scale operations.
3. Reporting and Guidance: Nessus provides detailed vulnerability assessment and security measures with remediation steps and documentation based on compliance requirements, classifying the vulnerabilities according to the degree of their threat. Structured reports are essential to the stakeholders for security risk priorities and their management.
4. Resource Requirements: Scanning processes that would otherwise require human involvement are recurring contacts with Nessus, a tool that can automate the process and still make it useful in some unique instances. There are also quite a few system and network resources required for the scan which generally does not help in enhancing the overall system performance. License costs, updates, and maintenance may also add up to substantial costs these are even more pronounced in larger institutions.
5. Skill Level and Interpretation: A moderately effective use of Nessus, effectively being able to yield positive results, requires managed expertise to understand the delivered output, and most importantly undertake the needed remediation practice. There is also the chance that some assets will be automated to the extent that security gaps may arise as some vital vulnerabilities are ignored.
6. Integration and Scalability: Several employee-based vulnerability scanners require additional input in the form of configured security policies. However, Nessus does link well and is a fully functioning tool in addition to other security tools such as SIEM systems and they can grow well with larger organizations and offer centralized oversight of vulnerability assessments across numerous locations or networks.

Manual Assessment (Nmap)

1. Speed and Flexibility: Nmap enables a very quick scanning of hosts and networks, which is often less than a minute for first scans. Due to its flexibility, security analysts can adapt the commands to be used for only specific sections of the reconnaissance targeting certain assets or configurations.
2. Resource Efficiency: Manned evaluations are generally less resource-intensive and help reduce the effect on the network. This comes in handy when the traffic is high or in situations where the adequacy of resources is limited.
3. Customizability: The Nmap tool allows the determination of the scanning and testing parameters, therefore, providing a chance for security analysts to make informed tests about the environment and the probable risks.
4. Reporting Limitations: The information that has been derived from Nmap lacks adequate details and has normal attempts which leads analysts to have to manually interpret the results. The unavailability of a formal report makes it impossible to report effectively to stakeholders regarding the status of security.
5. Contextual Analysis: Manual assessments are quite dependent on the analyst's skills and experience, which might help them in being able to grasp the context of the environment and are targets of abuse. This strategy, however, is vulnerable to human fallibility and neglect, such that, important vulnerabilities that would have unaided tools are likely to be overlooked.
6. Historical Tracking and Updates: There are no built-in facilities in Nmap that are used for countering historical data or automatic updates so the security teams have to wait for the findings to be logged and verified over some time.

The comparative analysis indicates that while automated vulnerability assessment tools available, for instance, Tenable Nessus Essentials are appropriate for large area networks, their operation and interpretation are effective only with competent, skilled personnel and specialized resources. Consequently, their robust technical reporting together with integration capabilities adds value to organizations that are focused on maintaining a strong security posture.

On the other hand, this cannot be said for manual assessment techniques employing tools like Nmap which are resource-efficient and proficient at reconnaissance but do possess the depth and detailed reporting framework synonymous with their automated counterparts. They are suited for selective assessments and can augment automated tools in forming a holistic vulnerability management program.

Best Practice Recommendation: To obtain the best results, organizations are encouraged to adopt a mixed approach that employs both automated and manual assessments. By adopting this approach, security managerial teams can cover the weaknesses of each of the conducted techniques in regards to the scope of damage and the concerned types of attacks. In doing so, security teams enhance their security posture and take appropriate measures to mitigate complications owed to vulnerabilities.

VI. Reference

[1] S. Shah and B. M. Mehtre, “An overview of vulnerability assessment and penetration testing techniques,” *J. Comput. Virol. Hacking Tech.*, vol. 11, no. 1, pp. 27–49, Feb. 2015, doi: 10.1007/s11416-014-0231-x.

[2] A. Fekete, M. Damm, and J. Birkmann, “Scales as a challenge for vulnerability assessment,” *Nat. Hazards*, vol. 55, no. 3, pp. 729–747, Dec. 2010, doi: 10.1007/s11069-009-9445-5.

[3] W. Moret, “Vulnerability Assessment Methodologies: A Review of the Literature”.

[4] N. Nirupama, “Risk and vulnerability assessment: a comprehensive approach,” *Int. J. Disaster Resil. Built Environ.*, vol. 3, no. 2, pp. 103–114, Jul. 2012, doi: 10.1108/17595901211245189.

[5] M. Mirjalili, A. Nowroozi, and M. Alidoosti, “A survey on web penetration test,” vol. 3, no. 6, 2014.

[6] A. S. Al-Ahmad, H. Kahtan, F. Hujainah, and H. A. Jalab, “Systematic Literature Review on Penetration Testing for Mobile Cloud Computing Applications,” *IEEE Access*, vol. 7, pp. 173524–173540, 2019, doi: 10.1109/ACCESS.2019.2956770.

[7] N. Milosevic, A. Dehghantanha, and K.-K. R. Choo, “Machine learning aided Android malware classification,” *Comput. Electr. Eng.*, vol. 61, pp. 266–274, Jul. 2017, doi: 10.1016/j.compeleceng.2017.02.013.

[8] F. Heiding, S. Katsikeas, and R. Lagerström, “Research communities in cyber security vulnerability assessments: A comprehensive literature review,” *Comput. Sci. Rev.*, vol. 48, p. 100551, May 2023, doi: 10.1016/j.cosrev.2023.100551.