Project Report

Track : Cyber Security with IBM QRadar

Team ID : LTVIP2024TMID11398

Team Size : 4

Team Leader : BHARGAVA SAI JETTI

Team member : AVALA JYOTHEESHWAR RAO

Team member : BHAVANI SIVA CHARAN CHITTI

Team member : CHITRADA PAVAN

College: Dr.L.B. Degree & P.G. College

Project : Understanding Cyber Threats: Exploring the Nessus and Beyond scanning tools

INTRODUCTION -

Overview:

"Understanding Cyber Threats: Exploring the Nessus and Beyond scanning tools" delves into the realm of cybersecurity vulnerability assessment. It provides an in-depth exploration of two prominent scanning tools: Nessus and Beyond.

1. Nessus:
    a. Nessus is one of the most widely used vulnerability assessment tools, known for its comprehensive scanning capabilities.
    b. It performs network vulnerability scanning to identify security issues, misconfigurations, and potential threats within a network infrastructure.
    c. Nessus employs a vast database of known vulnerabilities and continuously updates its plugins to keep pace with emerging threats.
    d. The tool provides detailed reports on discovered vulnerabilities, prioritizing them based on severity levels and offering remediation recommendations.
2. Beyond:
    a. Beyond represents a newer generation of vulnerability assessment tools, designed to address the evolving landscape of cyber threats.
    b. It goes beyond traditional vulnerability scanning by incorporating advanced features such as machine learning, threat intelligence integration, and predictive analytics.
    c. Beyond aims to provide not only vulnerability detection but also proactive threat identification and mitigation capabilities.
    d. The tool leverages AI and analytics to detect anomalous behaviors, zero-day vulnerabilities, and potential attack patterns that traditional scanners might overlook.

Purpose:

The project "Understanding Cyber Threats: Exploring the Nessus and Beyond scanning tools" serves several purposes and offers numerous benefits:

1. Vulnerability Assessment: The primary purpose is to conduct thorough vulnerability assessments of network infrastructures and systems. By utilizing tools like Nessus and Beyond, organizations can identify weaknesses, misconfigurations, and potential entry points for cyber threats.
2. Risk Management: Through comprehensive scanning, organizations can assess their security posture and prioritize remediation efforts based on the severity of

vulnerabilities detected. This helps in effective risk management by allocating resources to address the most critical security issues first.

3. Security Compliance: Many industries and regulatory bodies require organizations to adhere to specific security standards and compliance frameworks. Utilizing scanning tools like Nessus and Beyond aids in meeting these compliance requirements by identifying and addressing security gaps.
4. Incident Prevention: By proactively identifying vulnerabilities, organizations can take preventive measures to mitigate the risk of security incidents such as data breaches, unauthorized access, or system compromise.
5. Enhanced Security Awareness: Through the detailed reports generated by these scanning tools, organizations gain insights into their security posture and potential areas of improvement. This enhances security awareness among stakeholders, enabling informed decision-making and proactive security measures.
6. Continuous Monitoring: Nessus and Beyond support continuous monitoring of network security by regularly scanning for new vulnerabilities and emerging threats. This proactive approach helps organizations stay ahead of cyber threats and adapt their security strategies accordingly.
7. Integration with Security Operations: These scanning tools can be integrated into broader security operations, including incident response processes and security information and event management (SIEM) systems. This integration enhances overall security orchestration and response capabilities.
8. Resource Optimization: By automating the vulnerability assessment process, organizations can optimize resource utilization and reduce manual efforts required for security testing. This frees up security personnel to focus on more strategic security initiatives.

LITERATURE SURVEY -

Existing Problem:

The existing problem addressed by vulnerability assessment tools like Nessus and Beyond is the pervasive threat of cyber attacks due to vulnerabilities present in network infrastructures and systems. These vulnerabilities can be exploited by threat actors to gain unauthorized access, steal sensitive data, disrupt operations, or cause other malicious activities. The challenge lies in identifying and mitigating these vulnerabilities effectively to minimize the risk of security breaches.

Proposed solution:

Existing approaches and methods to solve this problem include:

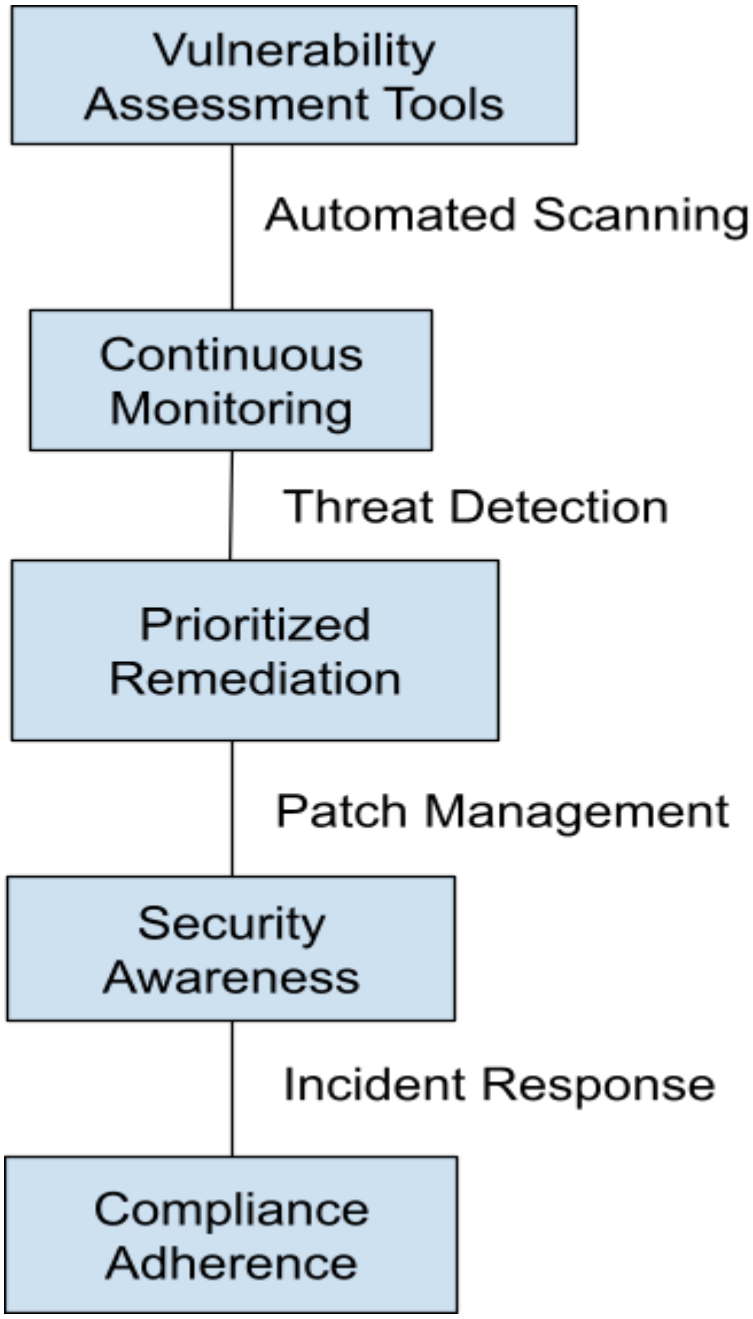
1. Manual Penetration Testing: Traditional manual penetration testing involves skilled security professionals manually assessing networks, systems, and applications for vulnerabilities and potential security weaknesses. While effective, this approach is time-consuming, resource-intensive, and may not scale well for large or complex environments.
2. Automated Vulnerability Scanning: Tools like Nessus, Beyond, and others automate the process of vulnerability assessment by scanning networks, systems, and applications for known vulnerabilities, misconfigurations, and security gaps. These tools leverage databases of known vulnerabilities and continuously updated plugins to identify potential threats.
3. Continuous Monitoring: Implementing continuous monitoring solutions allows organizations to proactively detect and respond to security threats in real-time. This involves monitoring network traffic, system logs, and other security data sources for signs of suspicious activity, anomalous behavior, or indicators of compromise.
4. Threat Intelligence Integration: Integrating threat intelligence feeds into vulnerability assessment tools enhances their capabilities by providing

insights into emerging threats, zero-day vulnerabilities, and attack trends. This enables organizations to prioritize remediation efforts based on the most relevant and imminent threats.

5. Patch Management: Establishing robust patch management processes ensures that software, operating systems, and other components are regularly updated with the latest security patches and fixes. Patch management helps mitigate known vulnerabilities and reduces the attack surface exposed to potential threats.
6. Security Awareness Training: Educating employees and stakeholders about cybersecurity best practices, threat awareness, and safe computing habits is essential for mitigating human-related security risks. Security awareness training helps build a culture of security within the organization and reduces the likelihood of successful social engineering attacks.
7. Security Frameworks and Standards: Adhering to established cybersecurity frameworks and standards, such as NIST Cybersecurity Framework, ISO/IEC 27001, and CIS Controls, provides a structured approach to managing cybersecurity risks. These frameworks offer guidelines, controls, and best practices for implementing effective security measures.
8. Incident Response Planning: Developing and regularly testing incident response plans ensures that organizations are prepared to respond effectively to security incidents and data breaches. Incident response planning involves defining roles and responsibilities, establishing communication protocols, and conducting tabletop exercises and simulations.

THEORETICAL ANALYSIS -

Block diagram:



Hardware / Software designing:

Hardware Requirements:

1. Server: A powerful computer to run the vulnerability assessment tools.
2. Network Equipment: Routers, switches, and firewalls for network communication.
3. Storage: Enough space to store scan results and backups.
4. Workstations: Computers for security personnel to use the tools.

Software Requirements:

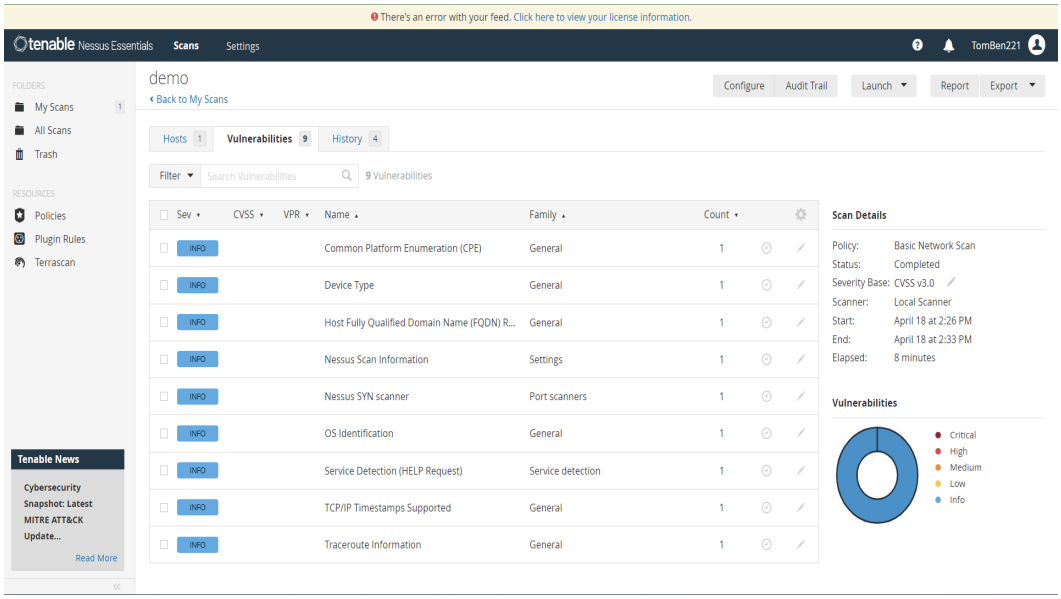
1. Vulnerability Assessment Tools: Nessus, Beyond, or similar software.
2. Operating System: Windows Server, Linux (like Ubuntu), or macOS for the server.
3. Database: Software to store scan results, like MySQL or PostgreSQL.
4. Security Software: Antivirus and endpoint security for protection.
5. Patch Management: Software to update systems with security patches.
6. Documentation and Reporting Tools: Software to document procedures and generate reports.
7. Training Resources: Materials to train personnel on using the tools.

RESULT -

For this project we used two sites one as practice and another as target

The practice site is Acunetix - http://testphp.vulnweb.com/

The following is the result of nessus scan on this site

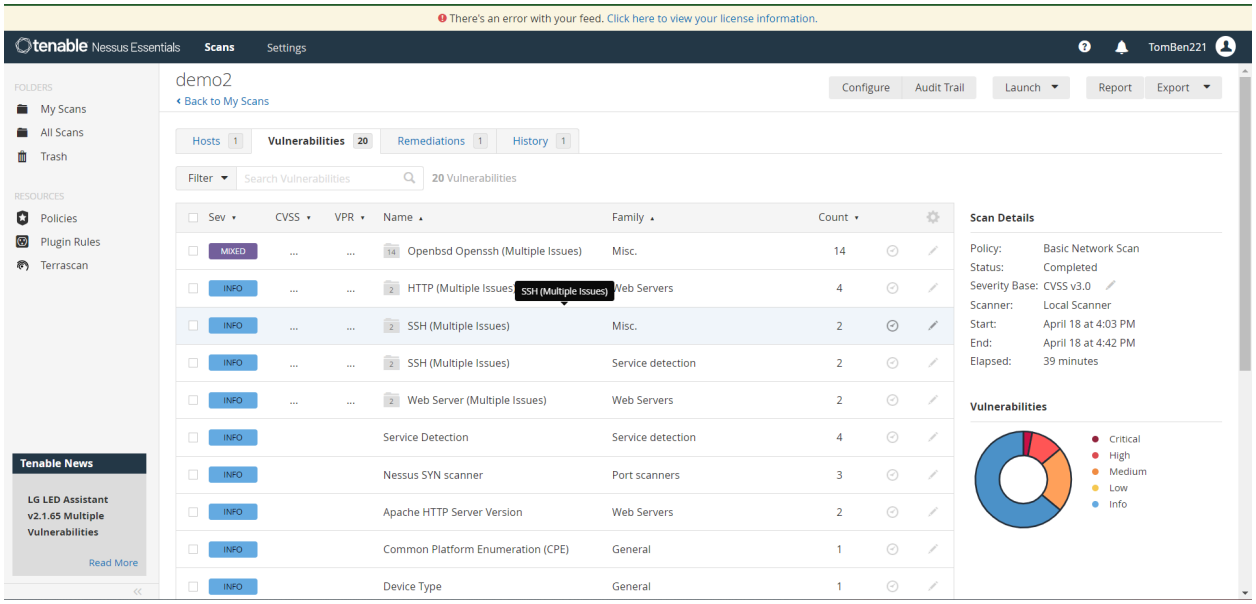


We have encountered total nine vulnerabilities, they are

1. Common Platform Enumeration (CPE)
2. Device Type
3. Host Fully Qualified Domain Name (FQDN) Resolution
4. Nessus Scan Information
5. Nessus SYN scanner
6. OS Identification
7. Service Detection (HELP Request)
8. TCP/IP Timestamps Supported
9. Traceroute Information

The target site is bWAPP - http://www.itsecgames.com/

The following is the Nessus scan result on this site



We have encountered total 20 vulnerabilities, they are

1. Openbsd Openssh (Multiple Issues)
2. HTTP (Multiple Issues)
3. SSH (Multiple Issues)
4. SSH (Multiple Issues)
5. Web Server (Multiple Issues)
6. Service Detection
7. Nessus SYN scanner
8. Apache HTTP Server Version
9. Common Platform Enumeration (CPE)
10. Device Type
11. Drupal Software Detection
12. Host Fully Qualified Domain Name (FQDN) Resolution
13. Nessus Scan Information
14. Open Port Re-check
15. OS Identification
16. OS Security Patch Assessment Not Available
17. Patch Report
18. SolarWinds Server & Application Monitor (SAM) Detection
19. Target Credential Status by Authentication Protocol - No Credentials Provided
20. Traceroute Information

ADVANTAGES & DISADVANTAGES -

The advantages and disadvantages of using vulnerability assessment tools like Nessus and Beyond:

Advantages:

1. Automated Scanning: These tools automate the process of identifying vulnerabilities, saving time and effort compared to manual assessments.
2. Comprehensive Coverage: They scan network infrastructures, systems, and applications thoroughly, uncovering a wide range of security issues.
3. Continuous Monitoring: Vulnerability assessment tools support continuous monitoring, allowing organizations to stay vigilant against emerging threats.
4. Prioritized Remediation: They prioritize vulnerabilities based on severity, enabling organizations to focus on fixing critical issues first to mitigate risks effectively.
5. Compliance: Using these tools helps organizations comply with industry standards and regulations by identifying and addressing security gaps.
6. Threat Intelligence Integration: Some tools integrate threat intelligence feeds, providing insights into emerging threats and enhancing detection capabilities.
7. Reporting and Analysis: They generate detailed reports with actionable insights, facilitating informed decision-making and remediation planning.

Disadvantages:

1. False Positives/Negatives: Vulnerability assessment tools may produce false positives (incorrectly identifying vulnerabilities) or false negatives (missing actual vulnerabilities), requiring manual verification.
2. Resource Intensive: Scanning large or complex environments can be resource-intensive, requiring powerful hardware and adequate network bandwidth.
3. Limited Scope: They may not detect all types of vulnerabilities, especially zero-day exploits or advanced persistent threats (APTs) not yet known to the tool's database.
4. Complexity: Configuring and managing vulnerability assessment tools effectively requires expertise and may be challenging for organizations with limited cybersecurity resources.
5. Dependency on Updates: Tools rely on regularly updated vulnerability databases and signatures, so outdated or incomplete data may impact their effectiveness.
6. Potential Disruption: Scanning activities may disrupt normal network operations or trigger false alarms in intrusion detection systems (IDS) or firewalls.
7. Cost: Some advanced vulnerability assessment tools may have significant upfront costs, licensing fees, or ongoing subscription fees, which may be prohibitive for smaller organizations.

APPLICATIONS -

Vulnerability assessment tools like Nessus and Beyond can be applied across various areas and industries to enhance cybersecurity posture and mitigate risks. Here are some key areas where this solution can be effectively applied:

1. Enterprise Networks: Large organizations with extensive network infrastructures can use vulnerability assessment tools to identify and address security vulnerabilities across their systems, servers, and applications.
2. Small and Medium-sized Businesses (SMBs): SMBs can benefit from vulnerability assessment tools to conduct regular security scans and prioritize remediation efforts based on their resource constraints and risk tolerance.
3. Critical Infrastructure: Industries such as energy, transportation, and healthcare rely on critical infrastructure that is susceptible to cyber threats. Vulnerability assessment tools help identify and mitigate vulnerabilities to safeguard essential services and infrastructure.
4. Government Agencies: Government agencies at the local, state, and federal levels can use vulnerability assessment tools to assess the security posture of their IT systems and networks and comply with cybersecurity regulations and mandates.
5. Financial Services: Banks, financial institutions, and fintech companies handle sensitive financial data and are prime targets for cyber attacks. Vulnerability assessment tools help identify and remediate vulnerabilities to protect customer information and maintain regulatory compliance.
6. Healthcare: The healthcare industry faces growing cybersecurity threats, especially with the digitization of patient records and medical devices. Vulnerability assessment tools help healthcare organizations identify and mitigate vulnerabilities to protect patient data and ensure the integrity of medical systems.
7. Education Institutions: Colleges, universities, and K-12 schools store large amounts of sensitive information, including student records and research data. Vulnerability assessment tools help educational institutions identify and address security vulnerabilities to protect sensitive information and maintain data privacy.
8. Retail and E-commerce: Retailers and e-commerce businesses collect and process vast amounts of customer data, making them attractive targets for cybercriminals. Vulnerability assessment tools help identify and remediate vulnerabilities in online platforms, payment systems, and backend infrastructure to protect customer information and maintain trust.
9. Manufacturing and Industrial Control Systems (ICS): Manufacturing facilities and industrial control systems (ICS) are increasingly connected to the internet, making them vulnerable to cyber attacks. Vulnerability assessment tools help identify and mitigate security risks in industrial networks and control systems to prevent disruptions to production and ensure worker safety.
10. Cloud Environments: Organizations leveraging cloud services and infrastructure can use vulnerability assessment tools to assess the security of their cloud environments, identify misconfigurations, and ensure compliance with cloud security best practices.

CONCLUSION -

In conclusion, the project "Understanding Cyber Threats: Exploring the Nessus and Beyond scanning tools" has provided valuable insights into the realm of cybersecurity vulnerability assessment. Through an exploration of prominent scanning tools like Nessus and Beyond, the project aimed to enhance our understanding of cyber threats and the methodologies used to mitigate them.

Throughout the project, several key findings and outcomes have emerged:

1. Importance of Vulnerability Assessment: Vulnerability assessment plays a crucial role in identifying and mitigating security vulnerabilities across network infrastructures, systems, and applications. Automated scanning tools like Nessus and Beyond offer efficient ways to conduct comprehensive vulnerability assessments.
2. Comprehensive Scanning Capabilities: Nessus and Beyond provide comprehensive scanning capabilities, enabling organizations to identify a wide range of security issues, misconfigurations, and potential threats within their IT environments.
3. Continuous Monitoring and Threat Detection: Integrating continuous monitoring and threat intelligence feeds enhances the detection capabilities of vulnerability assessment tools, enabling organizations to stay ahead of emerging threats and vulnerabilities.
4. Prioritized Remediation and Patch Management: Prioritizing vulnerabilities based on severity and criticality allows organizations to focus their remediation efforts on addressing the most significant security risks first. Effective patch management processes ensure timely deployment of security patches and updates to mitigate vulnerabilities.
5. Security Awareness and Incident Response: Educating employees and stakeholders about cybersecurity best practices and establishing robust incident response plans are essential components of a proactive cybersecurity strategy. Security awareness training and incident response planning help organizations detect, respond to, and mitigate security incidents effectively.

FUTURE SCOPE -

Looking ahead, there are several potential enhancements that can be made to further improve the effectiveness and efficiency of vulnerability assessment practices:

1. Integration with Threat Intelligence Platforms: Enhancing vulnerability assessment tools with seamless integration with threat intelligence platforms would enable organizations to leverage real-time threat intelligence data to prioritize vulnerabilities based on active threats and emerging attack trends.
2. Advanced Analytics and Machine Learning: Incorporating advanced analytics and machine learning algorithms into vulnerability assessment tools can improve detection accuracy, reduce false positives, and identify anomalous behavior indicative of potential security threats more effectively.
3. Automation of Remediation Tasks: Implementing automation capabilities within vulnerability assessment tools to automate remediation tasks, such as applying security patches, reconfiguring settings, and implementing security controls, can streamline the remediation process and reduce manual intervention.
4. Enhanced Reporting and Visualization: Enhancing reporting capabilities with interactive dashboards, visualization tools, and customized reporting templates can provide stakeholders with actionable insights and facilitate better decision-making regarding vulnerability management and risk prioritization.
5. Container and Cloud Security: Enhancing vulnerability assessment tools to support container and cloud-native environments would enable organizations to assess security risks associated with modern application architectures more effectively and ensure the security of cloud-based assets.
6. IoT and OT Security: Extending vulnerability assessment capabilities to include Internet of Things (IoT) devices and operational technology (OT) systems would address the growing security challenges associated with interconnected smart devices and industrial control systems.
7. Enhanced Compliance and Policy Management: Strengthening compliance and policy management capabilities within vulnerability assessment tools to align with industry-specific regulations, standards, and internal security policies would help organizations maintain compliance and demonstrate adherence to security best practices.
8. Threat Simulation and Red Teaming: Integrating threat simulation and red teaming capabilities within vulnerability assessment tools would enable organizations to conduct simulated cyber attacks and penetration testing exercises to evaluate their security defenses and identify potential weaknesses proactively.
9. Collaboration and Integration with Security Ecosystem: Enhancing interoperability and integration capabilities to facilitate seamless collaboration with other security solutions and ecosystem partners, such as SIEM platforms, incident response tools, and security orchestration platforms, would enable organizations to orchestrate end-to-end security workflows more effectively.

10. Continuous Improvement and Feedback Mechanisms: Establishing mechanisms for continuous improvement based on feedback from security practitioners, vulnerability researchers, and industry stakeholders would ensure that vulnerability assessment tools evolve to address emerging threats, technological advancements, and changing organizational needs effectively.

BIBLIOGRAPHY -

The following are taken for a reference to complete this project

1. Roesch, M. (2000). Snort: Lightweight Intrusion Detection for Networks. In LISA '99: Proceedings of the 13th Systems Administration Conference (pp. 229–238). USENIX Association.
2. Beale, J., & Pearce, A. (2007). Nessus Network Auditing (2nd ed.). Syngress.
3. Clements, K., Shieh, A., & Liu, J. (2013). Nessus, Snort, and Ethereal Power Tools: Customizing Open Source Security Applications (2nd ed.). Syngress.
4. Khan, A., Raza, A., & Khan, S. U. (2018). Cyber Threat Intelligence: Concepts, Methodologies, Tools, and Applications. IGI Global.
5. Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.
6. National Institute of Standards and Technology (NIST). (2019). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. NIST Cybersecurity Framework.
7. National Vulnerability Database (NVD). (n.d.). Retrieved from https://nvd.nist.gov/
8. Tenable Network Security. (n.d.). Nessus Documentation. Retrieved from https://docs.tenable.com/nessus/
9. Beyond Security. (n.d.). BeyondTrust Documentation. Retrieved from https://www.beyondsecurity.com/documentation/
10. Open Web Application Security Project (OWASP). (n.d.). OWASP Top Ten. Retrieved from https://owasp.org/www-project-top-ten/