A Project Report on

NETWORK VULNERABILITY ASSESSMENT

By

Bheema Shreya (20AT1A3546)
Kuruba Arjun(20AT1A0206)
Omkar Reddy(21AT5A0203)

Under the Guidance of

Dr.T.Tirupal **(M.Tech.,Ph.D)**
Associate Professor

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

G. PULLAIAH COLLEGE OF ENGINEERING AND TECHNOLOGY (Autonomous)

(Approved by AICTE | NAAC Accreditation with ‘A’ Grade | Accredited by NBA (ECE, CSE, EEE, CE) | Permanently Affiliated to JNTUA)

ACKNOWLEDGEMENTS

I Am extremely grateful to Chairman, **Sri G. M. Mohan Kumar,** of **G. Pullaiah College of Engineering and Technology**, Kurnool, Andhra Pradesh for their good blessings. I owe indebtedness to our Principal **Dr. C. Srinivasa Rao, M.E., Ph.D. G. Pullaiah College of Engineering and Technology**, Kurnool for providing us the required facilities. I Would like to express our deep sense of gratitude and our sincere thanks to HOD

Dr. T. TIRUPAL M. Tech., Ph.D. Department of Electronics and Communication Engineering, G. Pullaiah College of Engineering and Technology, Kurnool for providing the necessary facilities and encouragement towards the project work.

I thank our project supervisor, **Dr. T. TIRUPAL M. Tech., Ph.D.**. for his guidance, valuable suggestions and support in the completion of the project.

ABSTRACT

Network vulnerability assessment includes scanning for, detecting, and analyzing security vulnerabilities within a corporate network infrastructure and aims to ensure its resilience to common cybersecurity threats. It is required to carry out vulnerability assessment of the network to comply with the majority of regulatory standards (HIPAA, PCI DSS, etc.). Usually, assessment is followed by penetration testing to exploit identified vulnerabilities and define the most probable attack scenarios.

What is Network Vulnerability?

From the security point of view of a hardware system like PC or a network, vulnerability is a flaw in the system which can be oppressed by a third party like a hacker for pursuing unauthorized activities within the system and the network.Sometimes vulnerability is also known as the attack surface as it provisions the attacker the base with which it can exploit the system.It can also be referred to as the flaw in the design, implementation, construction, operation, and maintenance of a network or system which will affect or ravage the overall security policies and management of the network.Often people get confused with vulnerability and security risk. But, both are different as the risk involved is the chances of an attack on any network by various means to exploit the vulnerability.

Network Vulnerability Assessment

It is the process that will assist you to explore, analyze and evaluate the security concerns in your computer and the network system. The same is applicable to an organization as well.The assessment will survey the loopholes and vulnerabilities in your network design or the running system that will leave the scope for the hacker to enter from it and access your system. Hence, it will generate awareness regarding possible network threats.

Content

CHAPTER 1

INTRODUCTION TO NETWORK VULNERABILITIES

A network vulnerabilities assessment project is an essential activity for organizations to identify and address potential weaknesses and security flaws within their computer networks. This process involves conducting a systematic review of the network infrastructure, applications, and systems to discover vulnerabilities that could be exploited by malicious actors.

As time passes, the world is becoming more connected due to internet and new networking technology. Due to open nature of Internet, security of network has hold attention. With the development of new technologies, organization is now moving its business functions to public network, and thus a huge amount of personal, commercial and organization's infor- mation are available on networking infrastructures worldwide. Thus a set of precautions are taken to ensure the data cannot be compromised or inaccessible to unauthorized person. Network access in unauthorized by an outside hacker or a disgruntled employee can intentionally harm or destruct exclusive information which adversely influences organization benefit, and upset the proficiency to contend in business. In this manner, Network security is happening to incredible essentialness due to intellectual property that could be gained through the web with some effort. Network security measures includes scanning and vulnerability analysis along with penetration testing.

In today's interconnected world, networks play a vital role in almost every aspect of our lives. From personal communication to business transactions, the reliance on computer networks has become undeniable. However, this increased connectivity also exposes these networks to various threats, making them vulnerable to potential attacks from malicious actors. Network Vulnerability Assessment (NVA) is a crucial process that aims to identify and analyze these weaknesses within a network infrastructure, ensuring that proactive measures can be taken to fortify against potential security breaches.

As technology evolves rapidly, so do the techniques used by hackers and cybercriminals. Their ability to exploit vulnerabilities in networks has become more sophisticated and alarming, causing substantial financial losses, data breaches, and damage to an organization's reputation. In response to this escalating threat landscape, businesses and institutions are recognizing the need for robust security measures to protect their sensitive information and maintain the confidentiality, integrity, and availability of their critical systems.

Network scanning : It is fundamental for gathering information about the real state of computer systems or networks. It is a system for identification of active hosts on a network either with the end goal of security assessment of network. Vulnerability Assessment is a systematic analysis of security status of Information systems. Both techniques are the most comprehensive service for auditing, penetration testing, reporting and patching forany organization’s network.

Vulnerability Scanning: Vulnerability scanning is the process of identifying security weaknesses and flaws in systems and software running on them. This is an integral component of a vulnerability management program, which has one overarching goal – to protect the organization from breaches and the exposure of sensitive data.

Vulnerability scanners are employed to automatically scan the network and identify known security weaknesses in the discovered assets. These scanners compare the system's configuration and software versions against known vulnerabilities in their respective databases. The results of this scan provide security professionals with a prioritized list of vulnerabilities that require immediate attention.

What is Network Security Assessment?

A network security assessment is an essential component of any solid business security plan. This type of audit is used to identify vulnerabilities that could compromise an organization's network security. These vulnerabilities are generally grouped into three main categories: external, internal and social.

Penetration Testing: A pen test, short for penetration test, is a type of cyber-attack that is simulated on a computer network or system to check for potential vulnerabilities that could be exploited by hackers. Pen testing often involves the attempted breaching of individual applications to determine if specific security gaps exist that cybercriminals could leverage to gain access to a system, steal confidential information or corrupt essential business files. Insights gathered from a pen test can be used to enhance IT security policies. Penetration testing generally consists of five main stages. The first stage of the process is the planning phase, in which test goals are defined and intelligence is collected. Next, scanning tools are used to help businesses understand how a target can respond to possible intrusions. Cyber attacks are then staged to uncover the target's vulnerabilities.

IT AUDITS: An IT audit is a comprehensive evaluation of an organization's information technology infrastructure, operations and policies. A business may choose to conduct an IT audit to determine if company data and assets are protected and if IT controls align with business goals.

The primary goal of an IT audit is to establish if information-related processes and controls are working properly. This process involves evaluating the systems in place responsible for securing business data, determining the risks to a business's assets and ensuring that information management processes comply with all relevant IT policies, laws and standards.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction to Vulnerability Assessment

2.1.1 Definition of Network Vulnerability Assessment (NVA):

Connections with different networks, for example, open internet give helpful channels through which attacker can bargain internal end-systems. Moreover, inner network clients can deliberately or unknowingly undermine the network and its end-systems through their movements. If there is possibility that one of the internal device on the network is compromised, it can turn into a risk to whatever is left of the network. Thus the internet as well as intranet provide convenient channels through which attacker (external/internal) can

compromise end-systems So, Network security plays an essential role in an organization.

Vulnerability assessment:

Vulnerability assessment return information concerning potential security chances that permit IT staff to view the network the way a potential hacker may, unmistakably seeing the potential roads denial of service attacks or gaining information through packet sniffing. Vulnerability scanners often prioritize the weaknesses they discover, assigning different values to represent the potential damage a hacker could cause within a network by exploiting a specific weakness. This allows network administrators to prioritize repair

work by indicating which nodes present the greatest security risks.

Here following concepts of vulnerability assessment is discussed:

- Where vulnerability can be found i.e. area of vulnerabilities?
- What are the type of vulnerabilities found?
- How this vulnerability is categorized i.e. vulnerability domains?
- Types of tools to perform vulnerability assessment
- Limitations of vulnerability assessment

2.1.2 Areas of vulnerabilities: At the point when evaluating an organization's or platform's risk, there are area ranges of vulnerability . These area are described here. Security mechanisms are the methods and technologies that might be conveyed inside every area to accomplish the security policy objectives. The security polices will control the level of protection and security mechanisms implemented within each area.

Access Control: Access control is the procedure by which users are recognized and allowed privileges to information, resources and systems.[4] Controlling how privileges are conceded and how resources are accessed is discriminating to ensuring private and confidential information from unauthorized users. The access control mechanism ought to record and timestamp all communications and transactions with the goal that they might be examined for security breaches and misuse.

Application and Data Protection: It includes tending to security concerns connected with the operating system, the application programs and the data. The objective is to empower better application and data availability, decrease exposure to data loss and to keep up integrity of the applications and data information.

Platforms Protection: Platform protection is revolved around tending to physical attacks on the client hardware. The dangers incorporate hardware tampering, theft, or destruction, and data tampering, disclosure, or destruction.

Network Protection: Selected area for this dissertation : Network-based protection is implemented to address both attacks attempted across a network as well as attacks against the networking protocols. Network-based protection is executed to address both attacks attempted over a network and attacks againthe networking protocols. Network-based attacks attempt to compromise a system through flaws in the internet protocol standard. These attacks are ordinarily used to get access to systems, applications and data. These attacks can additionally be utilized to cause a ”denial of service” failure that might avert users for accessing network assets. The network attack is typically the entrance point for the following level of attack on the client and/or network.

2.2 Types of Network Assessment:

1. Vulnerability Assessment:

This type of assessment focuses on identifying and quantifying vulnerabilities within the network infrastructure. Vulnerability scanners, such as Nessus, are commonly used to perform automated scans and detect potential security weaknesses.

2. Penetration Testing (Pen Testing):

Penetration testing, also known as ethical hacking, involves authorized simulated attacks to assess the network's resilience against real-world threats. Penetration testers attempt to exploit vulnerabilities to understand their potential impact.

3. Compliance Assessment:

This assessment ensures that the network adheres to industry-specific regulations and standards. It validates that security policies and controls are in place to protect sensitive data and user privacy.

Network assessment is a fundamental aspect of cybersecurity, providing organizations with valuable insights into their network's security and performance. By conducting regular and comprehensive assessments, organizations can proactively identify vulnerabilities, mitigate risks, and enhance their ability to withstand cyber threats. The knowledge gained from network assessment empowers organizations to make informed decisions and implement effective security measures to safeguard their networks and data in an ever-evolving threat landscape.

2.2.1 Factors to Consider For a Network Vulnerability Assessment

There are many factors to consider when conducting a network vulnerability assessment, but some of the most important aspects include:

- Identifying all network systems and devices in your network infrastructure
- Determining how these systems and devices are interconnected
- Analyzing system configurations and installed software for known vulnerabilities
- Scanning for open ports and services that could be exploited
- Testing for weak passwords or other authentication issues

CHAPTER 3

PROPOSED METHOD

3.1 Proposed Method for Network Security Assessment using Nessus

with Nessus, you can gain full visibility into your network by conducting a vulnerability assessment.

1.Nessus Configuration and Setup:

The initial phase of our approach involves the setup and configuration of Nessus, a powerful network security assessment tool. We will begin by installing the latest version of Nessus on the system. Following the installation, we will carefully configure scan policies to customize the assessment according to our network's needs. Additionally, we will ensure proper authentication credentials for enabling credential-based scanning, enhancing the accuracy of vulnerability identification.

2: Network Discovery:

In this crucial step, Nessus will undertake a comprehensive network discovery process to identify all active hosts and devices connected to the network. This exhaustive scan will provide a detailed overview of the network's topology, revealing the various components and their interconnections. By mapping out the network infrastructure, this step forms the essential groundwork for the subsequent vulnerability scanning phase.

3. Vulnerability Scanning:

The proposed approach involves employing the advanced features of Nessus to conduct a comprehensive and efficient assessment of network security. Utilizing Nessus' robust vulnerability scanning capabilities, the system will identify and evaluate potential security risks, including outdated software versions, misconfiguration ,weak passwords and known vulnerabilities.

4. Compliance Checks:

In addition to vulnerability scanning, Nessus will perform compliance checks against industry standards and regulatory requirements. This will help evaluate the network's compliance with standards like PCI DSS, CIS benchmarks, and other relevant security guidelines.

5. Severity Assessment and Prioritization:

Nessus will assign severity levels to the identified vulnerabilities based on their potential impact and exploitability. The proposed method will prioritize the vulnerabilities based on their severity, allowing organizations to focus on addressing the most critical issues first.

6. Mitigation Strategies:

The proposed method will provide detailed mitigation strategies for each identified vulnerability. These strategies will guide IT teams and administrators on how to remediate the vulnerabilities effectively.

7. Continuous Monitoring:

To ensure ongoing security, Nessus will be used for continuous monitoring of the network. Scheduled scans will detect new vulnerabilities and changes in the network environment over time.

8. Reporting:

The final step of the proposed method involves generating detailed reports. The Nessus reports will provide a comprehensive overview of the assessment results, including a summary of vulnerabilities, compliance status, severity rankings, and recommended actions for remediation.

The proposed method aims to utilize the powerful capabilities of Nessus to perform a thorough and efficient network security assessment. By leveraging Nessus' extensive vulnerability scanning and reporting capabilities, organizations can proactively identify and address potential security risks, thus enhancing the overall security posture of their networks.

3.1.2 Vulnerability Scanning Tools and Techniques

Automated Vulnerability Scanning Tools:

Nessus: A widely-used commercial vulnerability scanner that can discover and assess vulnerabilities in networks, systems, and applications.

OpenVAS: An open-source vulnerability scanner that is a free alternative to Nessus.

Qualys: A cloud-based vulnerability management tool that offers scanning and reporting capabilities.

Nexpose: A vulnerability management solution provided by Rapid7 that can identify vulnerabilities across various assets.

Network Scanning:

Port Scanning: Identifying open ports on a system to assess potential attack vectors.

Network Discovery: Identifying devices, hosts, and services on a network to understand its structure.

Web Application Scanning:

OWASP ZAP (Zed Attack Proxy): An open-source web application scanner used to find vulnerabilities in web applications.

Burp Suite: A widely-used web vulnerability scanner with both free and commercial versions.

Credential Testing:

Password Cracking: Attempting to crack passwords using techniques like brute force, dictionary attacks, or rainbow tables.

Password Strength Assessment: Evaluating the strength of passwords used in the system.

Patch Management and Software Updates:

Keeping software, operating systems, and applications up-to-date helps to address known vulnerabilities by installing the latest security patches.

Manual Code Review and Analysis:

Manual inspection of application code and configurations to identify potential security issues that automated tools might miss.

Penetration Testing:

More comprehensive than vulnerability scanning, penetration testing involves simulating real-world attacks to identify and exploit vulnerabilities. It can provide a deeper understanding of a system's security posture.

Compliance and Security Standards Review:

Ensuring that systems meet industry standards and compliance requirements (e.g., PCI DSS, HIPAA, ISO 27001).

Asset Management:

Keeping track of all assets in a network, including hardware, software, and cloud resources.

Continuous Monitoring:

Implementing a continuous monitoring program to identify and respond to new vulnerabilities as they arise.

It's important to note that vulnerability scanning is just one part of a comprehensive cybersecurity strategy. Organizations should also focus on regular risk assessments, security awareness training, strong access controls, and incident response planning to ensure a robust security posture. Additionally, always obtain proper authorization before conducting any vulnerability scanning or penetration testing to avoid legal issues.

CHAPTER 4

EXPERIMENTAL RESULTS

VULNERABILITIES BY HOST

0-CRITICAL

1-HIGH

3-MEDIUM

1-LOW

39-INFO

Host Information:

IP: 65.61.137.117

OS: Linux Kernel 2.6

Vulnerabilities:

35450 - DNS Server Spoofed Request Amplification DDoS

Synopsis:

The remote DNS server could be used in a distributed denial of service attack.

Description:

The remote DNS server answers to any request. It is possible to query the name servers (NS) of the root zone ('.') and get an answer that is bigger than the original request. By spoofing the source IP address, a remote attacker can leverage this 'amplification' to launch a denial of service attack against a third-party host using the remote DNS server.

See Also:

https://isc.sans.edu/diary/DNS+queries+for+/5713

Solution:

Restrict access to your DNS server from public network or reconfigure it to reject such queries.

Risk Factor:

Medium

CVSS v3.0 Base score:

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

VPR Score:

3.6

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References:

CVE CVE-2006-0987

Plugin Information:

Published: 2009/01/22, Modified: 2020/08/21

Plugin Output:

udp/53/dns

The DNS query was 17 bytes long, the answer is 429 bytes long.

Synopis:

The remote name server allows recursive queries to be performed by the host running nessused.

Description:

It is possible to query the remote name server for third-party names. If this is your internal nameserver, then the attack vector may be limited to employees or guest access if allowed. If you are probing a remote nameserver, then it allows anyone to use it to resolve third party names (such as www.nessus.org). This allows attackers to perform cache poisoning attacks against this nameserver. If the host allows these recursive queries via UDP, then the host can be used to 'bounce' Denial of Service attacks against another network or system.

See Also:

http://www.nessus.org/u?c4dcf24a

Solution:

Restrict recursive queries to the hosts that should use this nameserver (such as those of the LAN connected to it). If you are using bind 8, you can do this by using the instruction 'allow-recursion' in the 'options' section of your named.conf. If you are using bind 9, you can define a grouping of internal addresses using the 'acl' command. Then, within the options block, you can explicitly state: 'allow-recursion { hosts_defined_in_acl }' If you are using another name server, consult its documentation

Risk Factor:

Medium

VPR Score:

4.2

CVSS v2.0 Base Score:

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score:

3.7 (CVSS2#E:U/RL:OF/RC:C)

References:

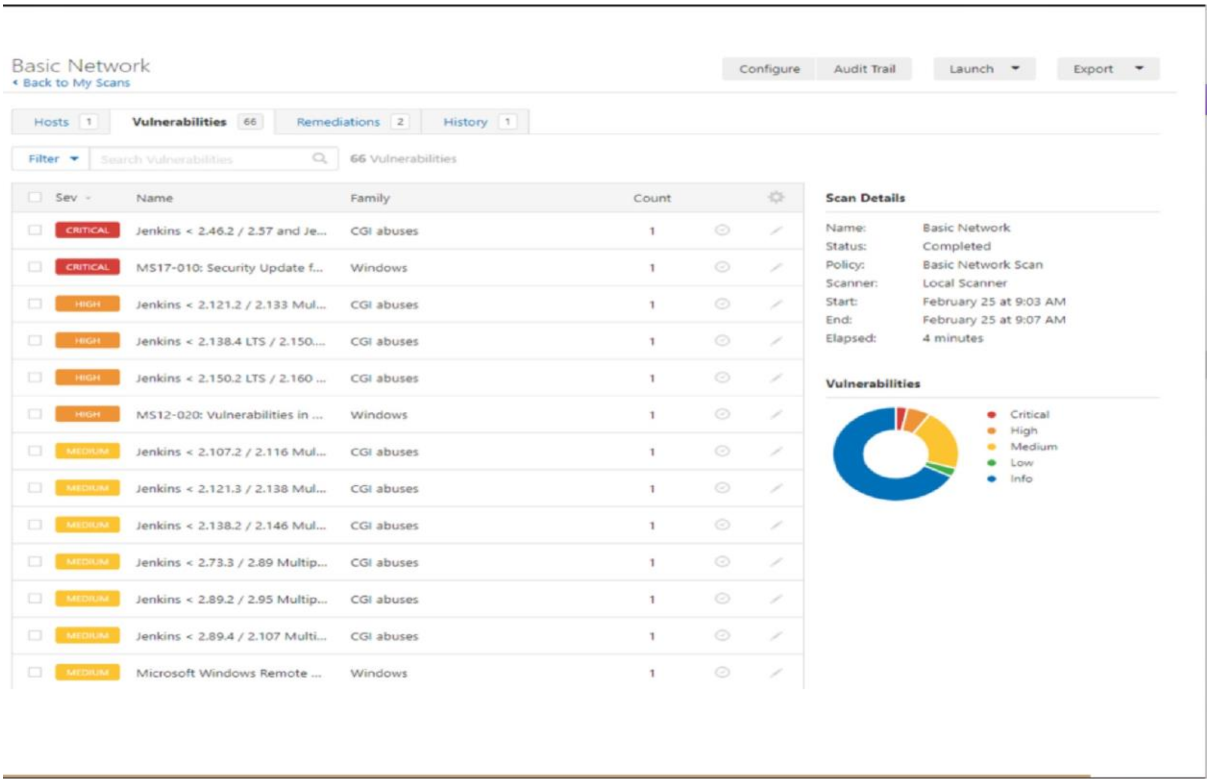
BID	136
BID	678
CVE	CVE-1999-0024
XREF	CERT-CC;CA-1977-22

Plugin Informtion:

Published: 2000/10/27, Modified: 2018/06/27

Plugin output:

udp/53/dns



☐	Sev	Name	Family	Count
☐	CRITICAL	Jenkins < 2.46.2 / 2.57 and Je...	CGI abuses	1
☐	CRITICAL	MS17-010: Security Update f...	Windows	1
☐	HIGH	Jenkins < 2.121.2 / 2.133 Mul...	CGI abuses	1
☐	HIGH	Jenkins < 2.138.4 LTS / 2.150....	CGI abuses	1
☐	HIGH	Jenkins < 2.150.2 LTS / 2.160 ...	CGI abuses	1
☐	HIGH	MS12-020: Vulnerabilities in ...	Windows	1
☐	MEDIUM	Jenkins < 2.107.2 / 2.116 Mul...	CGI abuses	1
☐	MEDIUM	Jenkins < 2.121.3 / 2.138 Mul...	CGI abuses	1
☐	MEDIUM	Jenkins < 2.138.2 / 2.146 Mul...	CGI abuses	1
☐	MEDIUM	Jenkins < 2.73.3 / 2.89 Multip...	CGI abuses	1
☐	MEDIUM	Jenkins < 2.89.2 / 2.95 Multip...	CGI abuses	1
☐	MEDIUM	Jenkins < 2.89.4 / 2.107 Multi...	CGI abuses	1
☐	MEDIUM	Microsoft Windows Remote ...	Windows	1

Scan Details

Name:	Basic Network
Status:	Completed
Policy:	Basic Network Scan
Scanner:	Local Scanner
Start:	February 25 at 9:03 AM
End:	February 25 at 9:07 AM
Elapsed:	4 minutes

Vulnerabilities

CHAPTER 5
APPLICATIONS/ADVANTAGES

Network vulnerability assessments have various applications across different sectors and industries. Some of the key applications include:

Enterprise Networks: Vulnerability assessments are commonly used in large organizations to evaluate the security posture of their internal networks. This helps identify and remediate vulnerabilities in servers, workstations, network devices, and other critical assets.

Cloud Infrastructure: As more businesses adopt cloud services, vulnerability assessments are crucial for evaluating the security of cloud-based environments, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) platforms.

Web Applications: Vulnerability assessments are widely used to evaluate the security of web applications, including e-commerce platforms, online banking portals, and other web-based services. This helps identify common web application vulnerabilities like SQL injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF).

Mobile Applications: Mobile app vulnerability assessments are performed to identify security flaws in mobile applications, ensuring that sensitive data and user interactions are adequately protected.

Industrial Control Systems (ICS) and SCADA Networks: Vulnerability assessments are essential for critical infrastructure sectors like energy, water, and transportation, where ICS and SCADA networks control essential operations. Identifying vulnerabilities in these systems is crucial for preventing potential cyber-attacks that can lead to severe consequences.

Healthcare Systems: The healthcare sector handles sensitive patient data and relies on networked medical devices. Vulnerability assessments are crucial to ensure the security and privacy of patient information and to prevent potential disruptions to medical services.

Financial Institutions: Banks, financial institutions, and payment processors are prime targets for cyber-attacks. Regular vulnerability assessments help protect financial networks, transactions, and customer data.

Government and Public Sector: Government agencies and public sector organizations often handle sensitive and classified information. Vulnerability assessments help protect their networks and data from threats and unauthorized access.

Education Institutions: Universities and schools have extensive networks with numerous connected devices. Vulnerability assessments can help maintain the security and privacy of educational institutions' digital infrastructure.

Small and Medium-sized Enterprises (SMEs): Vulnerability assessments are valuable for SMEs, which might not have extensive IT resources or dedicated cybersecurity teams, helping them address security gaps within their networks.

Third-Party Vendor Assessments: Organizations often conduct vulnerability assessments on third-party vendors and partners to ensure that their networks and systems meet security standards, as weaknesses in these external networks can potentially impact the organization's security.

Overall, vulnerability assessments play a critical role in enhancing network security and are an integral part of an organization's efforts to protect against cyber threats and maintain a robust cybersecurity posture.

Some Advantages of Network Vulnerability Assessment:

Risk Identification: NVA helps to identify potential security risks and vulnerabilities in the network. By discovering weaknesses before attackers do, organizations can take preventive measures to mitigate the risks and strengthen their security defenses.

Preventing Data Breaches: By identifying vulnerabilities in the network, NVA helps in preventing potential data breaches and unauthorized access to sensitive information. Addressing these vulnerabilities promptly reduces the chances of data loss or theft.

Proactive Security Approach: NVA enables a proactive security approach by regularly scanning and assessing the network. This ensures that security measures are continually updated and strengthened to counter new threats.

Compliance and Regulations: Many industries have specific compliance requirements that organizations must meet. Conducting regular network vulnerability assessments can help organizations demonstrate compliance with industry regulations and standards.

Reduced Downtime: Vulnerabilities in a network can lead to system crashes, service interruptions, or other operational issues. By identifying and resolving these vulnerabilities in advance, organizations can reduce unplanned downtime and associated costs.

Cost-Effectiveness: Network vulnerability assessments can be a cost-effective way to improve security compared to dealing with the aftermath of a successful cyber-attack or data breach, which can be significantly more expensive.

Enhanced Customer Trust: Customers and clients trust organizations that demonstrate a commitment to security. Conducting regular NVA and addressing vulnerabilities can enhance the trust of customers and stakeholders.

Insight into Security Posture: NVA provides valuable insights into the overall security posture of the network. It helps organizations understand their weak points and allows them to prioritize security efforts and investments accordingly.

Timely Patch Management: NVA highlights the importance of keeping software and systems up to date. By identifying unpatched or outdated software, organizations can ensure timely patch management, reducing the attack surface.

Threat Mitigation: Identifying vulnerabilities enables organizations to take proactive steps to mitigate potential threats. It allows security teams to stay ahead of attackers and significantly lowers the chances of successful cyber-attacks.

While NVA offers numerous benefits, it's essential to remember that it is just one aspect of a comprehensive cybersecurity strategy. To ensure robust protection, organizations should combine NVA with other security measures such as penetration testing, security awareness training, and regular security audits.

CHAPTER 6

CONCLUSIONS & FUTURE SCOPE

We also came to know more about vulnerability assessment and vulnerability scanning process. The assessment process will help in gathering data regarding the possible vulnerabilities in the organization.We explored the benefits and challenges faced by the scanning process and through this process, we can find out the vulnerabilities that are present in the hardware and software of the networking system or organization. The scanning process is conducted at various levels.Finally, from the vulnerability management process, we have explored more about assessment, scanning, evaluation, reporting and treating of the vulnerability issues.

Every day, vulnerabilities are found in commonly used software products. A network scanner developed in this project is an application which is used to scan the network and report any identified vulnerabilities.It is a web-based GUI which deals with two important aspect of network security:- network scanning and vulnerability assessment. Network scanning includes identification of alive hosts in the network, which operating systems is installed on them, and what services are running on them.

Throughout the vulnerability check a database of vulnerability signatures is contrasted with the data acquired from a network scan output to produce a list of vulnerabilities that are presumably present in the network. What’s more to check whether the vulnerability might be abused or not,and on the off chance that it can what are conceivable systems, testing is carried out. It performs functions of both NMAP and OpenVAS. It gives an administrator web-based GUI developed in PHP thus fulfilling portability and open-source requirement of project.The scanning can be done manually or a schedule can be fixed by administrator. The results are shown in different formats for better understanding of management authorities.This project was an excellent primer when implementing network security, but it was not without its challenges.

Future projects have great potential for growth and expansion. One possible expansion is optimizing OpenVAS scanner to deal with time-wait condition on target's machine which sometimes slows down the operation on machine or in severe case crashes the machine.

Another possible expansion of NMAP is to introduce more NSE scripts for vulnerability scanning. One more possible expansion is to integrate SNORT also with Network Scanner.

Time is of the essence when it comes to security testing and vulnerability management. The more actionable the vulnerability assessment report the better your chances of timely mitigation of the risk. Make sure you read a sample vulnerability scan report before engaging a vulnerability assessment company.

In conclusion, Network Vulnerability Assessments (NVA) is how you determine whether your network is secure against malicious attacks. It involves identifying possible weaknesses in your network and then taking steps to fix them. The goal of any Vulnerability is to ensure that no single point of failure exists on your network. You can conduct an Network Vulnerability using many different approaches, and each process has its strengths and weaknesses. Therefore, it's important to choose the right method based on your needs. In conclusion, network security vulnerabilities pose significant challenges and risks in the field of cybersecurity. As technology advances and networks become more interconnected, the potential attack surface for cyber threats widens. Addressing and mitigating network security vulnerabilities is crucial to maintaining the confidentiality, integrity, and availability of digital assets and sensitive information.