 

CEH based TEST

National Vocational and Technical Training Commission

1. A **nc -zv <target\_ip> <port\_range>** scan is performed to detect open ports on a system.
2. What is the primary purpose of vulnerability scanning?

The purpose of it is to protect the website from to exploit data and to make the website or software more protective

1. What is CVSS and what is the major difference between CVSS 2.0 and CVSS 3.0?

Common vulnerability scoring system (CVSS) is the ranking system of the vulnerabilities in the world and CVSS 2.0 is the uses a different vector string format and scoring algorithm and CVSS 3.0 have the hih vulnerability and high emphasia

1. Open sourse vulnerability scanner type of scanning involves the use of tools like Nessus and OpenVAS.
2. What is the first step in a vulnerability assessment?

It is planning and parameters

1. Define CVE and write about any CVE database that you know?

Common vulnerabilities exposure define as the vulnerabilities and the weakness of the website or software  CVE-2020-1938? CVE-2020-1938 is a file read/inclusion vulnerability in the AJP connector in Apache Tomcat. This is enabled by default with a default configuration port of 8009.

1. OpenVAS stands for Open Vulne ability Assessment System.
2. The process of identifying vulnerabilities without automated tools is known as

Passive vulnerability assessment.

1. Which automated scanner is known for its ability to detect a wide range of vulnerabilities with minimal configuration?

Openvass and nesses and Nmap are the mosted used tools \_

\_

1. Security Information and Event Management (SIEM) systems often aggregate log data from diverse sources, and advanced SIEM platforms leverage Correlation

Rules and Behavioral Analytic to identify sophisticated attack patterns.

1. The vulnerability scanning technique that involves sending crafted packets to

identify open ports is known What does CVSS stand for?

As port scanning

Common vulnerabilities scoring system

1. The database that maintains a list of known vulnerabilities is called a Vulnerability Database .
2. Describe the key features of the Common Vulnerability Scoring System (CVSS).

It involes the numeral stanrd and the impacts of the vulnerabilities and how harmful the viruses is

1. How does CVSS contribute to the prioritization of vulnerabilities?

It contributs to basic scoring and collrabaritions and the pirotirization in it and base tempermonal etc

1. OSVDB, vFeed and NVD.\_ databases are essential for keeping up-to-date with the latest vulnerabilities.

List three best practices for effective vulnerability management.

Asset Discovery.

Asset Prioritization and Assessment.

Reporting.

Remediation/Mitigation.

Verification.

1. How can a vulnerability database like CVE be integrated into an organization’s

vulnerability management program?

 **Automated Vulnerability Detection**

 **Patch Management**

 **Risk Assessment and Reporting**

 **Threat Intelligence Integration**

 **Compliance and Auditing**

 **Security Awareness and Training**

1. Defense in Depth involves layering multiple security controls throughout an

organization’s IT environment to ensure that if one layer fails, others remain intact .

1. Threat Intelligence Integration involves incorporating real-time information about current and emerging threads into an organization’s security operations to better anticipate and defend against potential attacks.
2. The Least Privilege Principle dictates that users and systems should have the

minimiun level of access necessary to perform their functions.

1. Explain the difference between automated and manual vulnerability scanning.

Automated vulnerabilities id uses to check quickly but the manual check slowly and depper

1. Nmap's Scripting Engine (NSE) is used for advanced vulnerability scanning.
2. How does the Nmap Scripting Engine (NSE) enhance the capabilities of Nmap?

1. \*\*Customizable Scanning\*\*

2. \*\*Flexibility\*\*

3. \*\*Enhanced Detection\*\*

4. \*\*Automation\*\*

5. \*\*Extended Functionality\*\*

1. Compare and contrast Nessus and OpenVAS as vulnerability scanners.

1. \*\*Overview\*\*

2. \*\*Licensing and Cost\*\*

3. \*\*Features\*\*

4. \*\*User Interface\*\*

5. \*\*Updates and Community\*\*

6. \*\*Performance and Scalability\*\*

7. \*\*Support\*\*

1. Explain the role of Ǫualys in vulnerability management.

Qualys provides automated vulnerability scanning, continuous monitoring, and risk assessment to identify and manage security weaknesses. and integration with other IT tools for comprehensive vulnerability management.

1. The openvas Top Ten list is a critical resource for web application security.
2. What is the OWASP Top Ten?
3. How can vulnerability assessments improve the security of web applications?

By making it more secure and the again and agin penetration testing

1. \*\*OWASP ZAP\*\*is a widely used vulnerability scanner for assessing web applications.
2. What is the focus of vulnerability analysis for mobile applications?

The focus of vulnerability analysis for mobile applications is to identify and address security weaknesses specific to mobile platforms, such as insecure data storage, weak authentication mechanisms, and vulnerabilities in app communication and code.

1. Mobile application vulnerabilities can often be linked to app code flaws.
2. What are the common techniques used in vulnerability analysis for network devices?

 **Port Scanning**

 **Network Mapping**

 **Vulnerability Scanning**

 **Configuration Analysis**

 **Penetration Testing**

 **Service Enumeration**

1. Why is it important to conduct vulnerability analysis on network devices?

Conducting vulnerability analysis on network devices is crucial to identify and address security weaknesses that could be exploited by attackers, thereby protecting the network infrastructure and ensuring the integrity, confidentiality, and availability of data and services.

1. In the Kill Chain Model, the Exploit phase may involve the use of zero-day vulnerabilities, which are unknown to the public and are often exploited through

Malware embedded , a technique involving embedded code in seemingly benign files.

1. Vulnerability analysis of network devices often focuses on openport,frimework , configurations, and firmware.
2. What are the typical steps involved in the reporting of vulnerabilities?

* **Typical steps in reporting vulnerabilities**:
* **Identification**
* **Assessment**
* **Documentation**
* **Notification**
* **Remediation Tracking**

1. Define SǪL injection and write an example of SǪL injection?

SQL injection is a security vulnerability that occurs when an attacker is able to insert or manipulate SQL queries in an application's input fields, allowing them to execute arbitrary SQL commands on the database.

1. How do exploitation frameworks assist in vulnerability analysis?

Exploitation frameworks assist in vulnerability analysis by providing tools and techniques to test and demonstrate the impact of vulnerabilities. They automate the process of exploiting known vulnerabilities, allowing security professionals to:

.

1. What is the primary function of OpenVAS?

Is to scan the vulnerabilites

1. Exploitation frameworks like metaploit are used to simulate attacks on discovered vulnerabilities.
2. Discuss the ethical considerations involved in vulnerability analysis.

Ethical considerations in vulnerability analysis include obtaining explicit permission, ensuring confidentiality, and minimizing impact. Responsible disclosure and adherence to legal and ethical standards are crucial to prevent harm and misuse.

Reporting and remediation are crucial in vulnerability management as they ensure that identified vulnerabilities are communicated clearly to stakeholders and addressed effectively, reducing the risk of exploitation and enhancing overall security.

1. Zero Trust Architecture operates on the principle of " \*\*Lateral movement\*\* refers to the techniques used by attackers to move across a network after initially compromising a system. It’s done to gain access to additional systems, escalate privileges, and achieve broader objectives, such as accessing sensitive data or furthering an attack’s impact. , always verify," meaning that every access request is subjected to strict verification regardless of its origin.
2. Case studies in vulnerability analysis often highlight \*\*Lessons learned\*\* from real- world scenarios.
3. Why are case studies important in learning about vulnerability analysis?

Case studies are important in learning about vulnerability analysis because they provide real-world examples of vulnerabilities, attacks, and their impacts. They offer insights into practical application, help identify best practices, and illustrate the consequences of security weaknesses, enhancing understanding and application of theoretical concepts.

1. How can case studies improve your approach to vulnerability analysis?

Case studies improve your approach to vulnerability analysis by providing practical insights into real-world vulnerabilities, attack methods, and remediation strategies. They help you understand the context of security issues, learn from past incidents, and apply proven solutions to enhance your own vulnerability assessment practices.

1. Describe a scenario where comprehensive vulnerability analysis would be critical.

A comprehensive vulnerability analysis would be critical during a major network upgrade for a financial institution. As the organization integrates new systems and applications, a thorough analysis ensures that any new vulnerabilities are identified and addressed before they can be exploited. This prevents potential breaches, protects sensitive financial data, and ensures compliance with regulatory standards.

1. Define lateral movement and why it's done?

\*\*Lateral movement\*\* refers to the techniques used by attackers to move across a network after initially compromising a system. It’s done to gain access to additional systems, escalate privileges, and achieve broader objectives, such as accessing sensitive data or furthering an attack’s impact.

1. During the practical on vulnerability analysis, students may use tools like

\*\*Nessus\*\*, \*\*Metasploit\*\*, \*\*OpenVAS\*\*, or \*\*Burp Suite\*\*to assess system security.

1. What is the purpose of practical exercises in a vulnerability analysis course?

The purpose of practical exercises in a vulnerability analysis course is to provide hands-on experience in identifying, analyzing, and addressing vulnerabilities. This practical experience helps learners apply theoretical concepts to real-world scenarios, develop problem-solving skills, and gain confidence in their ability to conduct effective vulnerability assessments.

1. Explain how a hands-on practical approach enhances understanding of vulnerability analysis.

A hands-on practical approach enhances understanding of vulnerability analysis by providing real-world experience in identifying, exploiting, and mitigating vulnerabilities. It allows individuals to apply theoretical knowledge to actual systems, improving their skills in detection, analysis, and remediation while also deepening their understanding of the practical challenges and nuances of cybersecurity.

1. What are the key components of a comprehensive vulnerability analysis report?
2. The key components of a comprehensive vulnerability analysis report include:

\*\*Executive Summary\*\*

\*\*Vulnerability Findings\*\*

\*\*Risk Assessment\*\*

\*\*Recommendations\*\*

\*\*Remediation Plan\*\*

\*\*Technical Details\*\*

\*\*Appendices\*\*

1. A well-conducted vulnerability analysis should lead to effective \*\*remediation\*\* of discovered vulnerabilities.
2. What is the goal of a practical vulnerability analysis session?

The goal of a practical vulnerability analysis session is to identify, assess, and prioritize security weaknesses in a system or network to improve its overall security posture and mitigate potential risks.

1. \*\*Ethical hacking\*\* hacking is the practice of exploiting vulnerabilities in systems to gain unauthorized access.
2. cracking tools are used to recover lost or stolen passwords.
3. Name two commonly used password-cracking techniques.

\*\*Brute Force Attack\*\*

\*\*Dictionary Attack\*\*