Unit 3

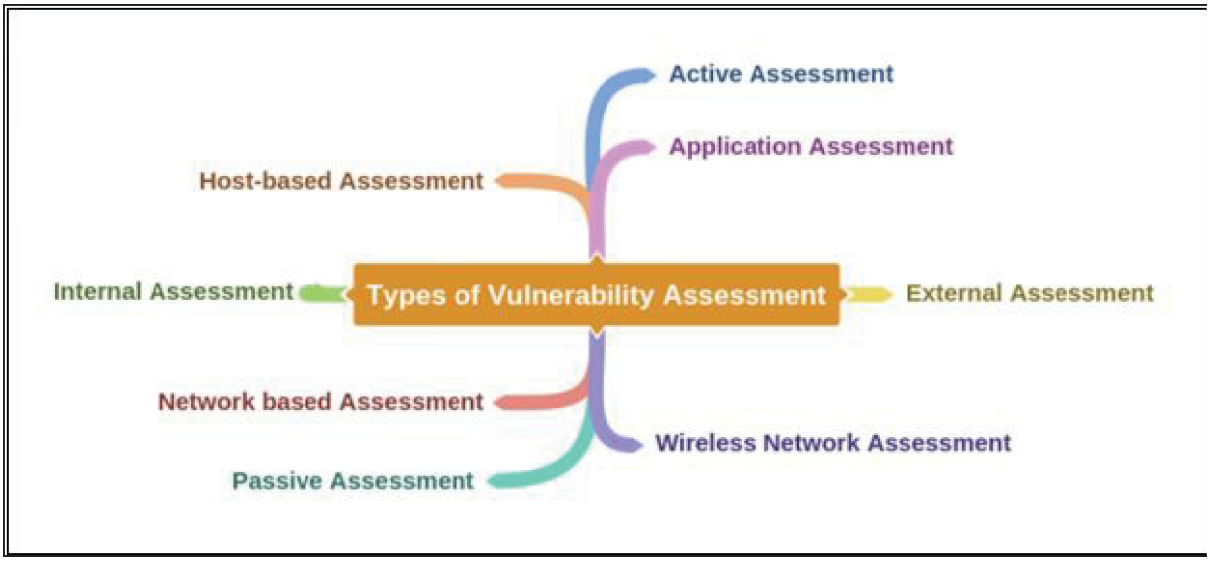
1. What is Vulnerability Assessment? Explain the types of Vulnerability Assessment with diagram?

Vulnerability Assessment

Vulnerability Assessment can be defined as a process of examination, discovery, and identification of system and applications security measures and weaknesses. Systems and applications are examined for security measures to identify the effectiveness of deployed security layer to withstand attacks and misuses. Vulnerability assessment also helps to recognize the vulnerabilities that could be exploited, need of additional security layers, and information's that can be revealed using scanners.

Types of Vulnerability Assessments

- **Active Assessments:** Active Assessment is the process of Vulnerability Assessment which includes actively sending requests to the live network and examining the responses. In short, it is the process of assessment which requires probing the target host.
- **Passive Assessments**: Passive Assessment is the process of Vulnerability Assessment which usually includes packet sniffing to discover vulnerabilities, running services, open ports and other information. However, it is the process of assessment without interfering the target host.
- **External Assessment:** Another type in which Vulnerability assessment can be categorized is an External assessment. It the process of assessment with hacking's perspective to find out vulnerabilities to exploit them from outside.
- **Internal Assessment:** This is another technique to find vulnerabilities. Internal assessment includes discovering vulnerabilities by scanning internal network and infrastructure.



2. Explain phases of Vulnerability Assessment life cycle?

Vulnerability Assessment life cycle includes the following phases:

Creating Baseline

Creating Baseline is a pre-assessment phase of the vulnerability assessment life-cycle in which pentester or network administrator who is performing assessment identifies the nature of the corporate network, the applications, and services. He creates an inventory of all resources and assets which helps to manage, prioritize the assessment. furthermore, he also maps the infrastructure, learns about the security controls, policies, and standards followed by the organization. In the end, baseline helps to plan the process effectively, schedule the tasks, and manage them with respect to priority.

Vulnerability Assessment

Vulnerability Assessment phase is focused on assessment of the target. The assessment process includes examination and inspection of security measures such as physical security as well as security policies and controls. In this phase, the target is evaluated for misconfigurations, default configurations,faults, and other vulnerabilities either by probing each component individually or using assessment tools. Once scanning is complete, findings are ranked in terms of their priorities. At the end of this phase, vulnerability assessment report shows all detected vulnerabilities, their scope, and priorities.

Figure 2. Vulnerability Assessment Lifecycle

Risk Assessment

Risk Assessment includes scoping these identified vulnerabilities and their impact on the corporate network or on an organization.

Remediation

Remediation phase includes remedial actions for these detected vulnerabilities. High priority vulnerabilities are addressed first because they can cause a huge impact.

Verification

Verification phase ensures that all vulnerabilities in an environment are eliminated.

Monitor

Monitoring phase includes monitoring the network traffic and system behaviors for any further intrusion

3. Explain CVSS and CVE? Name any 4 Vulnerability scanning tools.

Common Vulnerability Scoring Systems (CVSS)

The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

Security	Base Score Rating
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

Table 5-01 CVSSv5 SForing

To learn more about CVSS-SIG, go to website https://www.first.org.

Common Vulnerabilities and Exposure (CVE)

Common Vulnerabilities and Exposure (CVE) is another platform where you can find the information about vulnerabilities. CVE maintain the list of known vulnerabilities including an identification number and description of known cybersecurity vulnerabilities.

U.S. National Vulnerability Database (NVD) was launched by National Institute of Standards and Technology (NIST), The CVE List feeds NVD, which then builds upon the information included in CVE Entries to provide enhanced information for each entry such as fix information, severity scores, and impact ratings. As part of its enhanced information, NVD also provides advanced searching features such as by OS; by vendor name, product name, and/or version number; and by vulnerability type, severity, related exploit range and impact.

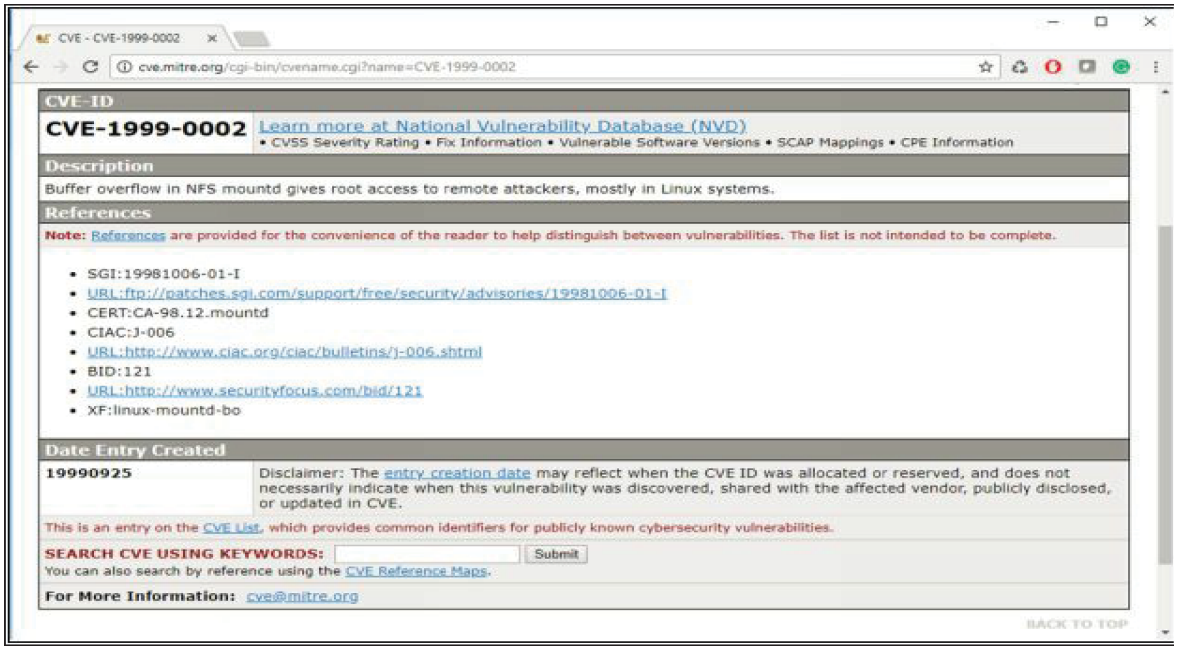


Figure3:CommonVulnerabilityandExposures(CVE)

Vulnerability Scanning

In this era of modern technology and advancement, finding vulnerabilities in an existing environment is becoming easy using different tools. Various tools, automated as well as manual tools, are available to help you in finding vulnerabilities. Vulnerability Scanners are automated utilities which are specially developed to detect vulnerabilities, weakness, problems, and holes in an operating system, network, software, and applications. These scanning tools perform deep inspection of scripts, open ports, banners, running services, configuration errors, and other areas.

These vulnerability scanning tools include: -

- Nessus
- OpenVAS
- Retina
- Nexpose
- GFI LanGuard
- Qualys FreeScan

4. **Explain any 3 popular penetration testing tools.**

Popular penetration testing tools

- The Metasploit Project is an open source project owned by the security company Rapid7, which licenses full-featured versions of the Metasploit software. It collects popular penetration testing tools that can be used on servers, online-based applications and networks. Metasploit can be used to uncover security issues, to verify vulnerability mitigations and to manage security processes.
- Nmap, short for "network mapper," is a port scanner that scans systems and networks for vulnerabilities linked to open ports. Nmap is directed to the IP address or addresses on which the system or network to be scanned is located and then tests those systems for open ports; in addition, Nmap can be used to monitor host or service uptime and map network attack surfaces.
- Wireshark is a tool for profiling network traffic and for analyzing network packets. Wireshark enables organizations to see the smaller details of the network activities taking place in their networks. This penetration tool is a network analyzer/network sniffer/network protocol analyzer that assesses vulnerabilities in network traffic in real time. Wireshark is often used to scrutinize the details of network traffic at various levels.
- John the Ripper incorporates different password crackers into one package, automatically identifies different types of password hashes and determines a customizable cracker. Pen testers typically use the tool to launch attacks to find password weaknesses in systems or databases.

5. **Explain any 6 Pentesting strategies.**

- **Targeted testing** is performed by the organization's IT team and the penetration testing team working together. It's sometimes referred to as a "lights turned on" approach because everyone can see the test being carried out.
- **External testing** targets a company's externally visible servers or devices including domain name servers, email servers, web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can get in once they've gained access.
- **Internal testing** mimics an inside attack behind the firewall by an authorized user with standard access privileges. This kind of test is useful for estimating how much damage a disgruntled employee could cause.
- **Blind testing** simulates the actions and procedures of a real attacker by severely limiting the information given to the person or team performing the test beforehand. Typically, the pen testers may only be given the name of the company. Because this type of test can require a considerable amount of time for reconnaissance, it can be expensive.
- **Double-blind testing** takes the blind test and carries it a step further. In this type of pen test, only one or two people within the organization might be aware a test is being conducted. Double-blind tests can be useful for testing an organization's security monitoring and incident identification as well as its response procedures.

- **Black box testing** is basically the same as blind testing, but the tester receives no information before the test takes place. Rather, the pen testers must find their own way into the system.
- **White box testing** provides the penetration testers information about the target network before they start their work. This information can include such details as IP addresses, network infrastructure schematics and the protocols used plus the source code.
- Pen Testing as a Service **(PTaaS)** provides information technology (IT) professionals with the resources they need to conduct and act upon point-in-time and continuous penetration tests.

6. Explain any 6 critical elements of Vulnerability Assessment Technical Report.

Every vulnerability scanning and assessment report should cover the following elements

Element	Description
Scan Information -	It carries information like the name of the scanning tool, its version, and the network ports to be scanned.
Target Information -	Under this section, the report carries details on the targeted system – its name and address.
Results -	This is the part where a reader would find the complete scanning report.
Target -	This sub-section of 'Results' comes with the detailed information of all the involved hosts, which includes – • This element contains the name and address of the host. • This will give the details of the operating system and its type. • It will show the date of the test.

Services -	The subtopic covers the names and ports of the network services.
Classification -	With this element, the system administrator can find out the additional details about scanning, like the origin of the scan.
Assessment -	The part covers the information on the scanner's vulnerability assessment.

7. Write the best practices order of activities for patch management? Name any 4 system hardening activities.

Best Practices – Order of Activities:

- Asset management identifies your attack surface
- Regular assessments keep up with emerging threats
- Patch management process tracks trending vulnerabilities over time
- Patches are implemented in a calculated and organized way

There are several types of system hardening activities, including:

- Application hardening
- Operating system hardening
- Server hardening
- Database hardening
- Network hardening

8. What are the benefits of system hardening and sandboxing?

Benefits of Systems Hardening

Systems hardening recovers continuous effort, but the diligence will pay off in substantive ways across your organization via:

- **Enhanced system functionality:** Since fewer programs and less functionality means there is less risk of operational issues, misconfigurations, incompatibilities, and compromise.

- **Significantly improved security:** A reduced attack surface translates into a lower risk of data breaches, unauthorized access, systems hacking, or malware.
  Simplified compliance and auditability: Fewer programs and accounts coupled with a less complex environment means auditing the environment will usually be more transparent and straightforward

The Benefits of Sandboxing

Using a sandbox has a number of advantages:

- **Does not risk your host devices or operating systems.** The main advantage of sandboxing is that it prevents your host devices and operating systems from being exposed to potential threats.
- **Evaluate potentially malicious software for threats.** If you're working with new vendors or untrusted software sources, you can test new software for threats before implementing it.
- **Test software changes before they go live.** If you're developing new code, you can use sandboxing to evaluate it for potential vulnerabilities before it goes live.
- **Quarantine zero-day threats.** With sandboxing, you can quarantine and eliminate zero-day threats.
- **Complement other security strategies.** Sandboxing functions as a complementary strategy to your other security products and policies, providing you with even more protection.