Introduction to Vulnerability Analysis / Assessment

- Vulnerability Analysis / Assessment can be defined as a process of examination, discovery, and identification of system and applications security measures and weaknesses.

- Systems and applications are tested for security measures to identify the effectiveness of security layer to set about to attacks and misuses.

- Vulnerability assessment also helps to acknowledge the vulnerabilities that would be exploited, need of additional security layers, and information's which will be revealed using scanners.

Types of Vulnerability Assessments

There are 4 types of vulnerability Assessments in Cyber Security and Penetration testing.
Below are brief explanation about each assessments:

- Active Assessment
- Passive Assessment
- External Assessment
- Internal Assessment

Types of Vulnerability Assessments

Active Assessment: Active Assessment is a process of Vulnerability Assessment which has actively sending requests to the live network and examining the responses. In short, it's the method of assessment which needs examine the target host.

Passive Assessment: Passive Assessment is a process of Vulnerability Assessment which usually includes packet sniffing to get vulnerabilities, running services, open ports and other information. However, it's the method of assessment without interfering the target host.

External Assessment: Another type of Vulnerability assessment are often categorized is an External assessment. It the method of assessment with hacking's perspective to seek out out vulnerabilities to take advantage of them from outside.

Internal Assessment: This is another technique to seek out vulnerabilities. Internal assessment includes discovering vulnerabilities through scanning internal network and infrastructure

Vulnerability Assessment Life Cycle

Vulnerability Assessment life cycle includes below phases

1. Creating Baseline
2. Vulnerability Assessments
3. Risk Assessments
4. Remediation
5. Verification
6. Monitor

Vulnerability Assessment Life Cycle

Creating Baseline :

Creating Baseline could be a pre-assessment phase of the vulnerability assessment life- cycle during which pentester and network administrators who is performing assessment identifies the company network, the applications, and services. He creates a listing of all resources & assets which helps to manage and prioritize the assessment. further, he also maps the infrastructure, learns about the safety controls, policies, and standards followed by the organization within the end, baseline helps to plan the method effectively, schedule the tasks, and manage them with regard to priority.

Vulnerability Assessment Life Cycle

Vulnerability Assessment:

Vulnerability Assessment phase is concentrated on assessment of the target. The testing process includes examination and inspection of security measures like physical security also as security policies and controls. during this phase, the target is evaluated for misconfigurations, default configurations, faults, and other vulnerabilities either by examine each component individually or using assessment tools. Once scanning completes, findings are ranked in terms of their priorities. At final of this phase, vulnerability assessment report shows all detected vulnerabilities, their scope, and priorities.

Vulnerability Assessment Life Cycle

Risk Assessment:

Risk Assessment which includes scoping certain identified vulnerabilities and their impact on the company network or on a company. .

Remediation:

Remediation phase includes solutions for these detected vulnerabilities on High priority vulnerabilities are addressed first because they will cause an enormous impact.

Verification:

Verification phase ensures that each one vulnerability are eliminated in resource.

Monitor:

Monitoring phase will include monitor the traffic in networka and system behaviour

Criteria for Choosing a Vulnerability Assessment Tool

Vulnerability assessment is crucial process as they scan for potential vulnerabilities that might be exploited. Anyone who cares about their Enterprise Security wouldn't compromise on not having a cutting-edge vulnerability scanner.

Below are the some consider elements to choose Best Vulnerability Tools

1. Simplified usage
2. Automation
3. Scanning Technologies
4. On-Demand Solutions
5. Reporting
6. Pricing
7. Support

Introduction of Vulnerability Scoring Systems

Common Vulnerability Scoring Systems (CVSS)

The Common Vulnerability scoring system (CVSS) provides the way to capture the principal characteristics of vulnerability and provides a numerical score reflecting its severity, that can be explained into a qualitative information to assist 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

Introduction of Vulnerability Scoring Systems

Common Vulnerabilities’ and Exposure (CVE)

Common Vulnerabilities and Exposure (CVE) is platform where you'll find the data about vulnerabilities. CVE maintain the records of known vulnerabilities including an positive identification number and outline of known cybersecurity vulnerabilities. list

Introduction of Vulnerability Scoring Systems

National Vulnerability Database (NVD)

U.S. National Vulnerability Database (NVD) was launched by National Institute of Standards and Technology (NIST), The CVE List which then builds upon the data included in CVE Entries to produce enhanced information for every entry like fix information, severity scores, and impact ratings. As a part of its enhanced information, NVD also provides advanced searching features like by OS by vendor name, product name, and by vulnerability type, severity, related exploit range, and impact.

Vulnerability Assessments Reports

A vulnerability assessment report offers detailed information on existing vulnerabilities. With the assistance of this report, companies can assess their security posture and find appropriate solutions to eliminate the vulnerabilities.

With complex underlying concepts, the report must be basic in nature. It should be understandable to technical also as non-technical stakeholders. Every modern company needs a talented , ethical hacker who can identify the vulnerabilities, offer valuable solutions, and write an in depth vulnerability assessment report.

Analyzing Vulnerability Scanning Report

First of all, let’s attempt to understand who should be involved in analyzing results. the right answer is: various teams and departments should be involved during this process.

Security professional because the report contains technical security issues and describes the foremost common hacking techniques to take advantage of the problems , a talented security professional should be involved.

Network or supervisor If the report contains results for network or OS vulnerability scan, the outcomes should be explained with the IT operational department to prove them and eliminate false positives.

Web developers This team are going to be quite useful during web application analysis. Have a talk with them before starting the scan to know an application’s functionality and technologies to form sure you don’t miss any critical requirements during the vulnerability scan.

Senior management it's absolutely critical to possess senior management support and deliver the results to them, as they're going to be liable for allocating a budget to repair the problems .

Legal and regulatory If a scope includes any systems which hold customer or employees personal data, have your legal or regulatory department review the problems .

Analyzing Vulnerability Scanning Report

First look at the report

Scope confirm all the required URLs and IP addresses were covered within the report. a couple of things can fail .

Scanning errors When analyzing the report, you would possibly see that ports were open during the initial scan, but after a couple of minutes they've been closed.

Plugins / signature version it's always recommended to use the newest plugins during the scanning. If plugins are quite one or fortnight old, critical vulnerabilities could be missed.

Date and time If analyzing a report performed by a 3rd party company or maybe by developers/network admin/test team, the date of the report is critical When scanning preproduction environments

Analyzing Vulnerability Scanning Report

First look at the report

False positives

All reports contain false positives. even though a vendor of the vulnerability scanner tells that their product doesn’t produce false positives, it's not exactly correct. Indeed vulnerability is also on the online site, but the severity should be always questioned.

Some common false positives are listed below:

- Outdated software
- Brute force attacks
- Changed admin credentials or paths

Analyzing Vulnerability Scanning Report

First look at the report

False negatives

False negatives are the vulnerabilities which weren't discovered by the scanner, but present on the important site. the safety analyst should remember when false negatives can happen and confirm they're discovered by manual testing.

Some common false positives are listed below:

- Out-of-Band Authentication
- Business login flaws
- Restricted pages and lack of privileges