Vulnerability Analysis

Def.

Attackers perform VA to identify security loopholes in the target's network, and end devices. The identified Vulnerabilities are used by attackers to further exploit the target network.

VA Researchers VA has an important role to play in an organization's security from different internal and external threats. To secure a network, an administrator needs to perform patch management, install proper antivirus software, check configuration, solve known issues in third-party applications, and troubleshoot hardware default configurations. All these activities together consitutue Vulnerability assessment.

In this section we will learn:

- Vulnerability Assessment Concepts
- Vulnerability Classification and Assessment Types
- Vulnerability Assessment Solutions and Tools
- Vulnerability Assessment Reports

Vulnerability Assessment Concepts:

There are two causes of vulnerable systems in a network:

1. Misconfiguration in software or Hardware
2. Poor Programming practices

Attackers leverage these vulnerabilities to perform different attacks on an organizational resource. We will be covering Vulnerability Assessment, Vulnerability scoring systems, Vulnerability databases, and the Vulnerability assessment life cycle.

Vulnerability Research

It is the process of analyzing protocols, services, and configurations to discover the vulnerabilities and design flaws that will expose an OS and its applications to exploit, attack, or misuse.

An administrator needs Vulnerability Research:

- To gather information about security trends, newly discovered threats, attack surfaces, attack vectors and techniques
- To find weaknessess in the OS and applications and alert the network administrator before a network attack
- To understand information that helps prevent security problems
- To know how to recover from a network attack

An ethicalhacker needs to keep up with the most recently discovered vulnerabilities and exploits to stay one step ahead of the attackers through vulnerability research which includes:

- Discovering the sytem design faults and weaknesses that might alllow attackers to compromise a system
- Stay updated about new products and technologies and reading news related to currnet exploits
- Checking underground hacking web sites (deep and Dark websites) for newly discovered vulnerabilities and exploits
- Checking newly released alerts regarding relevant innovations and product improverments for security systems

Security experts and vulnerability scanners classify vulnerabilities by:

- Severity level (low, medium, high)
- Exploit range (local or remote)

Resources for Vulnerability Research

The following are some of the online websites used to perform vulnerability research:

- Microsoft Vulnerability Researc (MSVR) (https://www.microsoft.com)
- Dark Readin (https://www.darkreading.com)
- SecurityTracker (https://securitytracker.com)
- Trend Micr (https://www.trendmicro.com)
- Security Magazin (https://www.securitymagazine.com)
- PenTest Magazin (https://pentestmag.com)
- SC Magazin (https://www.scmagazine.com)
- Exploit Databas (https://www.exploit-db.com)
- Security Focu (https://www.securityfocus.com)
- Help Net Securit (https://www.helpnetsecurity.com)
- HackerStor (http://www.hackerstorm.co.uk)
- Computerworl (https://www.computerworld.com)
- WindowsSecurit (http://www.windowsecurity.com)

- D'Cryp (https://www.d-crypt.com)

What is Vulnerability Assessment?

A vulnerability assessment is an in-depth examination of the ability of a system or application, including current security procedures and controls, to withstand exploitation. It scans networks for known security weaknesses, and recognizes, measures, and classifies security vulnerabilities in computer systems, networks, and communication channels. It identifies, quantifies, and ranks possible vulnerabilities to threats in a system. Additionally, it assists security professionals in securing the network by identifying security loopholes or vulnerabilities in the current security mechanism before attackers can exploit them.

A vulnerability assessment may be used to:

- Identify weaknesses that could be exploited
- Predict the effectiveness of additional security measures in protecting information resources from attack

Typically, vulnerability-scanning tools search network segments for IP-enabled devices and enumerate systems, operating systems, and applications to identify vulnerabilities resulting from vendor negligence, system or network administration activities, or day-to-day activities. Vulnerability-scanning software scans the computer against the Common Vulnerability and Exposures (CVE) index and security bulletins provided by the software vendor.

Vulnerability scanners are capable of identifying the following information:

- The OS version running on computers or devices
- IP and Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports that are listening
- Applications installed on computers
- Accounts with weak passwords
- Files and folders with weak permissions
- Default services and applications that might have to be uninstalled
- Errors in the security configuration of common applications
- Computers exposed to known or publicly reported vulnerabilities
- EOL/EOS software information
- Missing patches and hotfixes
- Weak network configurations and misconfigured or risky ports
- Help to verify the inventory of all devices on the network

There are two approaches to network vulnerability scanning:

- **Active Scanning**: The attacker interacts directly with the target network to find vulnerabilities. Active scanning helps in simulating an attack on the target network to uncover vulnerabilities that can be exploited by the attacker.

Example: An attacker sends probes and specially crafted requests to the target host in the network to identify vulnerabilities.

- **Passive Scanning**: The attacker tries to find vulnerabilities without directly interacting with the target network. The attacker identifies vulnerabilities via information exposed by systems during normal communications. Passive scanning identifies the active operating systems, applications, and ports throughout the target network, monitoring activity to determine its vulnerabilities. This approach provides information about weaknesses but does not provide a path for directly combating attacks.

Example: An attacker guesses the operating system information, applications, and application and service versions by observing the TCP connection setup and teardown.

Vulnerability-Management Life Cycle

The process helps identify remediate any potential security weaknesses before they can be exploited.

- **Identify Assets and Create a Baseline**

This phase identifies critical assets and prioritizes them to define the risk based on the criticality and value of eeach system. This created a good baseline for vulnerability management. This phase involves the gathering of information about the identified systems to understand the approved ports, software, drivers, and basic configuration each system in order to develop and maintain a system baseline.

- **Vulnerability Scan**

This phase is very crucial in vulnerability management. In this step, the security analyst performs the vulnerability scan on the network to identify the known vulnerabilities in the organization's infrastructure. Vulnerability scans can also be performed on applicable compliance templates to assess the organization's Infrastructure weaknesses against the respective compliance guidelines.

- **Risk Assessment**

In this phase, all serious uncertainties that are associated with the system are assessed and prioritized, and remediation is planned to permanently eliminate system flaws. The risk assessment summarizes the vulnerability and risk level identified for each of the selected assets. It determines whether the risk level for a particular asset is high, moderate, or low. Remediation is planned based on the determined risk level. For example, vulnerabilities ranked high-risk are targeted first to decrease the chances of exploitation that would adversely impact the organization.

- **Remediation**

Remediation is the process of applying fixes on vulnerable systems in order to reduce the impact and severity of vulnerabilities. This phase is initiated after the successful. implementation of the baseline and assessment steps.

- **Verification**

In this phase, the security team performs a re-scan of systems to assess if the required remediation is complete and whether the individual fixes have been applied to the impacted assets. This phase provides clear visibility into the firm and allows the security. team to check whether all the previous phases have been perfectly employed or not. Verification can be performed by using various means such as ticketing systems, scanners, and reports.

- **Monitor**

Organizations need to performed regular monitoring to maintain system security. They use tools such as IDS/IPS and firewalls. Continuous monitoring identifies potential threats and any new vulnerabilities that have evolved. As per security best practices, all phases of vulnerability management must be performed regularly.