Unit VIII: Vulnerability Analysis and Penetration Testing

Submitted By

Dr. P. Vijayakumar

Associate Professor, School of Electronics Engineering,

Vellore Institute of Technology, Chennai

Roadmap

- Vulnerability Assessment
- Vulnerability Classification
- Types of Vulnerability Assessment
- Vulnerability Analysis Tools
- Reasons for conducting PenTests
- Penetration testing stages

Vulnerability analysis

- Vulnerability analysis, also known as vulnerability assessment, is a process that **defines, identifies, and classifies the security holes (vulnerabilities) in a computer, network**, or communications infrastructure.

- In addition, vulnerability analysis can forecast the effectiveness of **proposed countermeasures and evaluate** their actual effectiveness after they are put into use.

What Is Vulnerability Assessment?

- A key component of the vulnerability assessment is properly defining the ratings for **impact of loss and vulnerability**.

- The deliverable for the assessment is, most importantly, a **prioritized list of discovered vulnerabilities** (and often how to remediate).

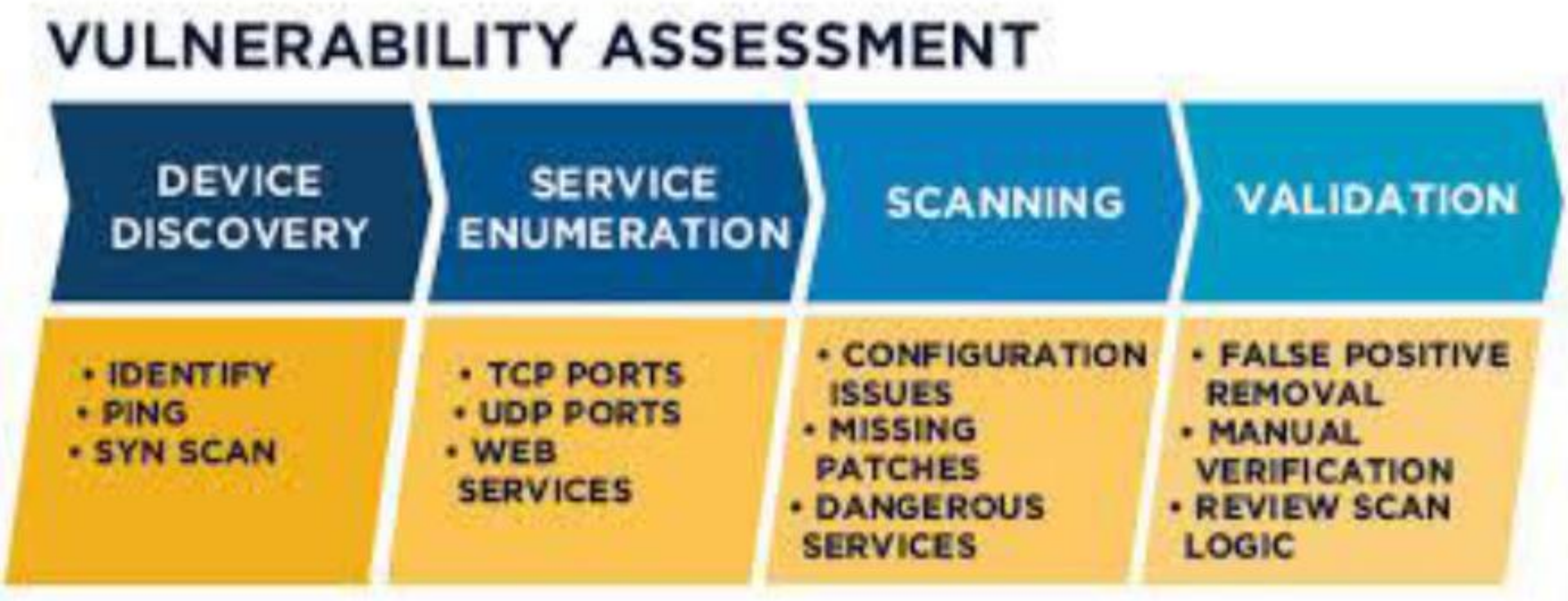
- The findings are classified into categories of **high, medium, and low risk**.

What Is Vulnerability Assessment?

- A vulnerability assessment system, will look at the network and **pinpoint the weaknesses** that need to be fixed/patched – before they ever get breached.

- With ever growing new vulnerabilities being **announced each week**, a company’s network is only as secure as its latest vulnerability assessment.

- An ongoing vulnerability assessment process, in **combination with proper remediation**, will help ensure that the network is fortified to withstand the latest attacks.



VULNERABILITY ASSESSMENT

DEVICE DISCOVERY	SERVICE ENUMERATION	SCANNING	VALIDATION
• IDENTIFY • PING • SYN SCAN	• TCP PORTS • UDP PORTS • WEB SERVICES	• CONFIGURATION ISSUES • MISSING PATCHES • DANGEROUS SERVICES	• FALSE POSITIVE REMOVAL • MANUAL VERIFICATION • REVIEW SCAN LOGIC

Why to carry out Vulnerability Assessment?

- Vulnerability assessment is important because it is a powerful **proactive process for securing an enterprise network**.

- With vulnerability assessment potential security holes are fixed before they **become problematic**, allowing companies to fend off attacks before they occur.

- **Virtually all attacks come from already known vulnerabilities.**

Vulnerability Classification

- The following are categories of vulnerabilities commonly recognised.

1. Misconfigurations
2. Default installations
3. Buffer overflows
4. Unpatched servers
5. Default passwords
6. Open services
7. Application flaws
8. Open system flaws
9. Design flaws

Misconfigurations

- Security misconfiguration is simply, **incorrectly assembled** safeguards for a web application.

- These misconfigurations typically occur when holes are left in the security framework of an application by **systems administrators, DBAs or developers**.

- They can occur at **any level of the application stack**, including the platform, web server, application server, database, framework, and custom code.

Misconfigurations

- These security misconfigurations can lead **an attacker right into the system and result in a partially or totally** compromised system.

- Attackers find these misconfigurations through unauthorized access to **default accounts, unused web pages, unpatched flaws, unprotected files and directories**, and more.

- If a system is compromised through faulty security configurations, **data can be stolen or modified slowly over time and can be time-consuming and costly to recover**.

Default installations

- Most **server applications** included in a default installation are solid, thoroughly tested pieces of software.

- Having been in use in production environments for many years, their **code has been thoroughly refined and many bugs** that have been found are fixed.

- However, there is no perfect software and there is always room for further refinement.

- Moreover, **newer software is often not as rigorously tested** because of its recent arrival to production environments or because it may not be as popular as other server software.

Default installations

- Developers and system administrators often **find exploitable bugs in server applications and publish the information on bug tracking** and security related websites such as the Bugtraq mailing list (http://www.securityfocus.com) or the Computer Emergency Response Team (CERT) website (http://www.cert.org).

Buffer overflows

- A buffer overflow occurs **when a program or process tries to store more data in a buffer** (temporary data storage area) than it was intended to hold.

- Since buffers are created to contain a finite amount of data**, the extra information** - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them.

- Although it may occur accidentally through **programming error, buffer overflow** is an increasingly common type of security attack on data integrity.

- In buffer overflow attacks, the extra data may contain codes designed to **trigger specific actions**, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information.

Unpatched servers

- According to Wikipedia, **a patch is a piece of software designed to update a computer program** or its supporting data, to fix or improve it.

- This includes fixing security vulnerabilities and other bugs, with such patches usually called bug fixes , and improving the usability or performance.

- Although meant to fix problems, **poorly designed patches** can sometimes introduce new problems.

- Server applications which languish **unpatched by developers or administrators who fail to patch their systems** leave this as one of the most exploited vulnerabilities.

Default passwords

- Another common error is to **leave the default passwords** or keys in services that have such authentication methods built into them.

- For example, some databases leave default administration passwords under the assumption that the system administrator will change this immediately upon configuration.

- Even an inexperienced cracker can use the widely-known default password to gain administrative privileges to the database.

Types of Vulnerability Assessment

- **Active Assessment: Scans the network** using any **network scanner** to find hosts, services and vulnerabilities.

- **Passive Assessment:** This is a technique that **sniffs the network traffic** to find out active systems, network services, applications and vulnerabilities present.

- **Host based Assessment:** This is a sort of security check carried out through a **configuration level test through command line.**

- **Internal Assessment:** This is a technique to **scan the internal infrastructure** to find out the exploit and vulnerabilities.

Types of Vulnerability Assessment

- **External Assessment:** This is used to assess the network from a hacker point of view to find out what exploits and vulnerabilities are available to the **outside world**.

- **Application Assessment:** This tests the **web server infrastructure** for any misconfiguration, **outdated content** and **known vulnerabilities**.

- **Network Assessment:** This determines the possible network security attacks that may occur on the organization system.

- **Wireless network Assessment:** This determines and tracks all the wireless network prevalent at the client side.

How to Conduct a Vulnerability Assessment

- The method for performing the VA will include reviewing appropriate policies and procedure relating to the systems being assessed, interviewing system administrators, and security scanning.

- Vulnerability analysis consists of several steps:

STEP 1. Defining and classifying network or system resources

STEP 2. Assigning relative levels of importance to the resources

STEP 3. Identifying potential threats to each resource

STEP 4. Developing a strategy to deal with the most serious potential problems first

STEP 5. Defining and implementing ways to minimize the consequences if an attack occurs.

The following tasks are involved in conducting a VA

- Use vulnerability assessment tools
- Check for misconfigured web servers, mail servers, firewalls, etc.
- Search the web for more postings about the company’s vulnerabilities
- Search at underground websites for more postings about the company’s vulnerabilities

The VA is done in three phases:

Pre-assessment phase

- Describes the scope of the Assessment
- Creates proper information protection procedures such as effective planning, scheduling, coordination and logistics
- Identifies and ranks the critical assets

Assessment phase

- Examines the network architecture
- Evaluates the threat environment
- Carries out penetration testing
- Examines and evaluates physical security
- Performs a physical asset analysis
- Observes policies and procedures
- Conducts and impact analysis
- Performs a risk characterization

Post Assessment phase

- Prioritizing assessment recommendations
- Providing action plan development to implement the proposed recommendation
- Capturing lessons that are learned to improve the complete process in the future
- Conducting training

Vulnerability Analysis phase

- This phase refers to identifying areas where vulnerability exists.

- This entails performing vulnerability analysis and listing of areas that need testing and penetration.

- Vulnerability penetration capabilities can be broken down into three steps:
  - Locating nodes
  - Performing service discoveries on them
  - Testing those services for known security holes

- Now that auditors have identified and verified the vulnerabilities, they must perform in-depth analysis of all the assembled data.

- The goal here is to identify systemic causes, and then they formulate plans to remedy each cause.

- These plans are the basis of the strategic recommendations that they bring before the business’ executives. Once the auditors have completed their assessment, the IT department or the consultants work alongside the executives to fix those problem areas.

- Once the business rectifies vulnerabilities, they can direct their attention to upgrading or transitioning the network.

Vulnerability Analysis Tools

- Types of tools available for vulnerability assessment are classified as follows:

Host based VA tools

- These find and identify the OS running on a particular host computer and tests it for known deficiencies. These search for common application and services.

Application-layer VA tools

- These are directed towards web servers or databases

Scope assessment tools

- They provide security to the IT system by testing for vulnerabilities in the application and OS

Depth assessment tools

- These tools find and identify previously unknown vulnerabilities in a system, and include ‘Fuzzers’.

Vulnerability Analysis Tools

- A Fuzzer is a program that attempts to discover security vulnerabilities by sending random input to an application.
- If the program contains a vulnerability that can leads to an exception, crash or server error (in the case of web apps), it can be determined that a vulnerability has been discovered.
- Fuzzers are often termed Fault Injectors for this reason, they generate faults and send them to an application.

- **Active/passive tools**

Active scanners perform vulnerability checks on the network that consumes resources on the network.

Passive scanners do not materially affect system resources, these only observe system data and performs data processing in a separate analysis machine.

While new vulnerabilities are discovered every day and new tools are required to tackle these, a list of available tools are listed below:

1. Qualys Vulnerability Scanner
2. Cycorp CycSecure Scanner
3. eEye Retina Network Security Scanner
4. Foundstone Professional Scanner
5. GFI LANguard Network Security Scanner
6. ISS Network Scanner
7. Saint Vulnerability Scanner
8. Symantec NetRecon Scanner
9. Shadow Security Scanner
10. Microsoft Baseline Security Analyzer
11. SPIKE Proxy
12. Foundstone’s ScanLine
13. Cerebrus Internet Scanner

Some of the free scanners available on the internet include:

Nmap

Nmap is a utility for network discovery and/or security auditing. It can be used to scan large networks or single hosts quickly and accurately, determining which hosts are available, what services each host is running and the operating system that is being used.

- **Nessus**

Nessus is a remote security scanner. This software can audit a given network and determine if there are any weaknesses present that may allow attackers to penetrate the defences. It launches predefined exploits, and reports on the degree of success each exploit had.

Some of the free scanners available on the internet include:

- **Whisker**

Whisker is a CGI web scanner. It scans for known vulnerabilities found in web servers, giving the URL that triggered the event as well, it can determine the type of web server being run. It is easy to update and has many useful features.

- **Enum**

Enum is a console-based Win32 information enumeration utility. Using null sessions, Enum can retrieve user lists, machine lists, share lists, name lists, group and member lists, password and LSA policy information. Enum is also capable of a rudimentary brute force dictionary attack on individual accounts.

Fire walk

- Fire walking is a technique that employs traceroute-like techniques to analyse IP packet responses to determine gateway ACL filters and map networks.

- It can also be used to determine the filter rules in place on a packet forwarding device.

Penetration Testing

Reasons for conducting PenTests:

- Identify the threats facing an organization's s information assets
- Reduce an organization's IT security costs and provide a better Return on IT Security Investment (ROSI) by identifying and resolving vulnerabilities and weaknesses
- Provide an organization with assurance - a thorough and comprehensive assessment of organizational assessment of organizational security covering policy
- Gain and maintain certification to an industry regulation (BS7799, HIPAA etc.)
- Adopt best practice by conforming to legal and industry regulations

Penetration Testing

- It focuses on high severity vulnerabilities and emphasizes application-level security issues to development security issues to development teams and management

- For testing and validating the efficiency of security protections and controls

- For enabling vulnerability perspectives to the organization internally and externally

- Providing indisputable information usable by audit team's gathering data for regulatory compliance

Penetration Testing

- Providing comprehensive approach of preparation steps that can be taken to prevent upcoming exploitation

- Evaluating the efficiency of network security devices such as firewalls, routers, and web servers

- For changing or upgrading existing infrastructure of software, hardware, or network design

What should be tested?

- An organization should conduct a risk assessment operation before the penetration testing that will help to identify the main threats, such as:

- Communications failure, e-commerce failure, and loss of confidential information.
- Public facing systems; websites, email gateways, and remote access platforms.
- Mail, DNS, firewalls, passwords, FTP, IIS, and web servers.

Testing should be performed d be performed on all hardware and software components of a network security system.

Penetration testing stages

- According to one classification, there are three stages in penetration testing
  - Pre-attack
  - Attack Phase
  - Post-attack phase

- Penetration (or external assessment) testing usually starts with three pre-test phases:

- Foot printing
- Scanning
- Enumerating

Together, the three pre-test phases are called reconnaissance.

Pre-attack phase

This process seeks to gather as much information about the target network as possible, following these seven steps:

- STEP 1. Gather initial information
- STEP 2. Determine the network range
- STEP 3. Identify active machines
- STEP 4. Discover open ports and access points
- STEP 5. Fingerprint the operating system
- STEP 6. Uncover services on ports
- STEP 7. Map the network

The goal of reconnaissance is primarily to discover the following information:

- IP addresses of hosts on a target network

- Accessible User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) ports on target systems

- Operating systems on target systems

- Malicious hackers also value reconnaissance as the first step in an effective attack.

- Keep in mind that the penetration test process is more organic than these steps would indicate.

- These pre-test phases entail the process of discovery, and although the process is commonly executed in this order, a good tester knows how to improvise and head in a different direction, depending upon the information found.

- There are two different reconnaissance methods to discover information on the hosts in your target network:

- Passive reconnaissance
- Active reconnaissance

a. **Passive Host Reconnaissance**

- Passive reconnaissance gathers data from open source information. Open source means that the information is freely available to the public. Looking at open source information is entirely legal.
- A company can do little to protect against the release of this information, but later sections of this chapter explore some of the options available. Following are examples of open source information:

Passive Host Reconnaissance

- A company website
- Electronic Data Gathering, Analysis, and Retrieval (EDGAR) filings (for publicly traded

  companies)
- Network News Transfer Protocol (NNTP) USENET Newsgroups
- User group meetings
- Business partners
- Dumpster diving
- Social engineering

b. Active reconnaissance

- Active reconnaissance, in contrast, involves using technology in a manner that the target might detect. This could be by doing DNS zone transfers and lookups, ping sweeps, traceroutes, port scans, or operating system fingerprinting. Some of the tools that are useful in active host reconnaissance include the following:

- NSLookup/Whois/Dig lookups
- SamSpade
- Visual Route/Cheops
- Pinger/WS_Ping_Pro

The three stages of reconnaissance are:

- **Footprinting**
  - Footprinting is the active blueprinting of the security profile of an organization.

  - It involves gathering information about your customer's network to create a unique profile of the organization's networks and systems.

  - It's an important way for an attacker to gain information about an organization passively, that is, without the organization's knowledge.

Footprinting

- Footprinting employs the first two steps of reconnaissance, gathering the initial target information and determining the network range of the target.

- Common tools/resources used in the footprinting phase are:

  - Whois
  - SmartWhois
  - NsLookup
  - Sam Spade

Footprinting may also require manual research, such as studying the company's Web page for useful information, for example:

- Company contact names, phone numbers and email addresses
- Company locations and branches
- Other companies with which the target company partners or deals
- News, such as mergers or acquisitions
- Links to other company-related sites
- Company privacy policies, which may help identify the types of security mechanisms in place
- Other resources that may have information about the target company are:
- The Capital Market database if the company is publicly traded
- Job boards, either internal to the company or external sites
- Disgruntled employee blogs and Web sites
- Trade press

Scanning

- The next four information-gathering steps -- identifying active machines, discovering open ports and access points, fingerprinting the operating system, and uncovering services on ports – are considered part of the scanning phase.

- The goal here is to discover open ports and applications by performing external or internal network scanning, pinging machines, determining network ranges and port scanning individual systems.

Some common tools used in the scanning phase are:

- NMap
- Ping
- Traceroute
- Superscan
- Netcat
- NeoTrace
- Visual Route

Enumerating

- In enumeration, a tester tries to identify valid user accounts or poorly-protected resource shares using active connections to systems and directed queries.

- The type of information sought by testers during the enumeration phase can be users and groups, network resources and shares, and applications.

The techniques used for enumeration include:

- Obtaining Active Directory information and identifying vulnerable user accounts
- Discovering NetBIOS name enumeration with NBTscan
- Using snmputil for SNMP enumeration
- Employing Windows DNS queries
- Establishing null sessions and connections

Attack Phase

- The next phase is the attack phase, where if an attack is successful, the vulnerability is verified and safeguards are identified to mitigate the associated security exposure.

- In many cases, exploits that are executed do not grant the maximum level of potential access to an attacker.

- They may instead result in the tester’s learning more about the targeted network and its potential vulnerabilities, or induce a change in the state of the targeted network’s security.

- Some exploits enable testers to escalate their privileges on the system or network to gain access to additional resources.

Attack Phase

- If this occurs, additional analysis and testing are required to determine the true level of risk for the network, such as identifying the types of information that can be gleaned, changed, or removed from the system.

- In the event an attack on a specific vulnerability proves impossible, the tester should attempt to exploit another discovered vulnerability.

Attack Phase

- If testers are able to exploit a vulnerability, they can install more tools on the target system or network to facilitate the testing process.

- These tools are used to gain access to additional systems or resources on the network, and obtain access to information about the network or organization.

- Testing and analysis on multiple systems should be conducted during a penetration test to determine the level of access an adversary could gain.