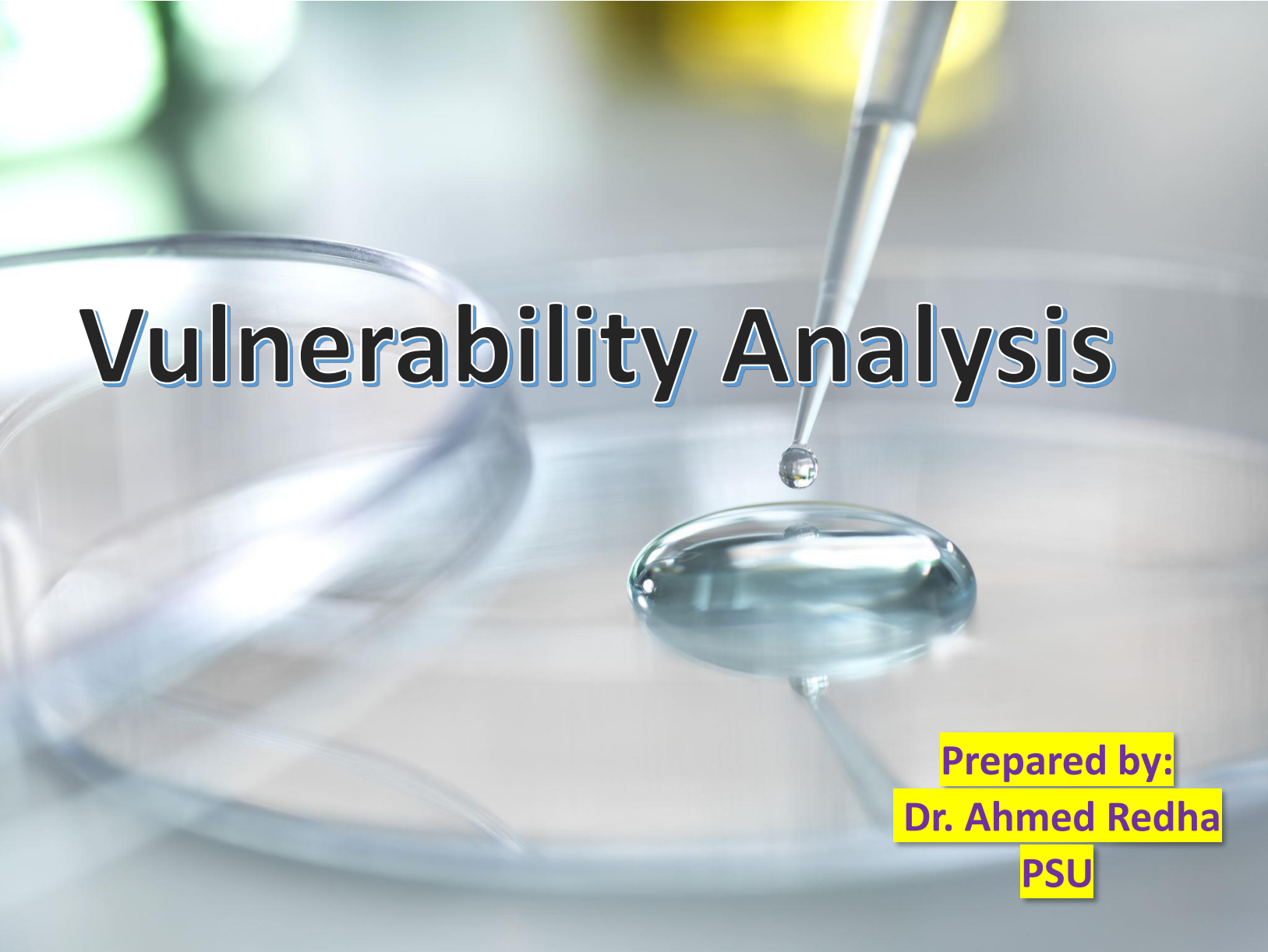


Vulnerability Analysis

Prepared by:
Dr. Ahmed Redha
PSU

INTRODUCTION

Vulnerability assessment is an integral component of a good security program. In fact, a well-functioning vulnerability management system, including testing and remediation, is often cited by industry standards and regulatory bodies as an essential requirement for security and mandatory for compliance

Traditionally, cyber security professionals are trained to consider vulnerabilities from a technical perspective, such as flaws identified in software platforms or configuration issues that can be leveraged by an attacker to gain access.

Although, given the definition previously, vulnerabilities encompass weaknesses of all types (including, for example, those found within physical environments and governance structures)

What Is a Vulnerability Assessment?

The US National Institute of Standards and Technology (NIST) defines a vulnerability as:

"**a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source**."

Thus, a vulnerability is a weakness that can be exploited by adversaries to advance their goals.

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

- ✓Discovering system design faults and weaknesses that might allow attackers to compromise a system.
- ✓Being informed about new products and technologies to find news related to current exploits.
- ✓Checking underground hacking web sites for new vulnerabilities and exploit.
- ✓Checking newly released alerts regarding relevant innovations and product improvements for security systems.

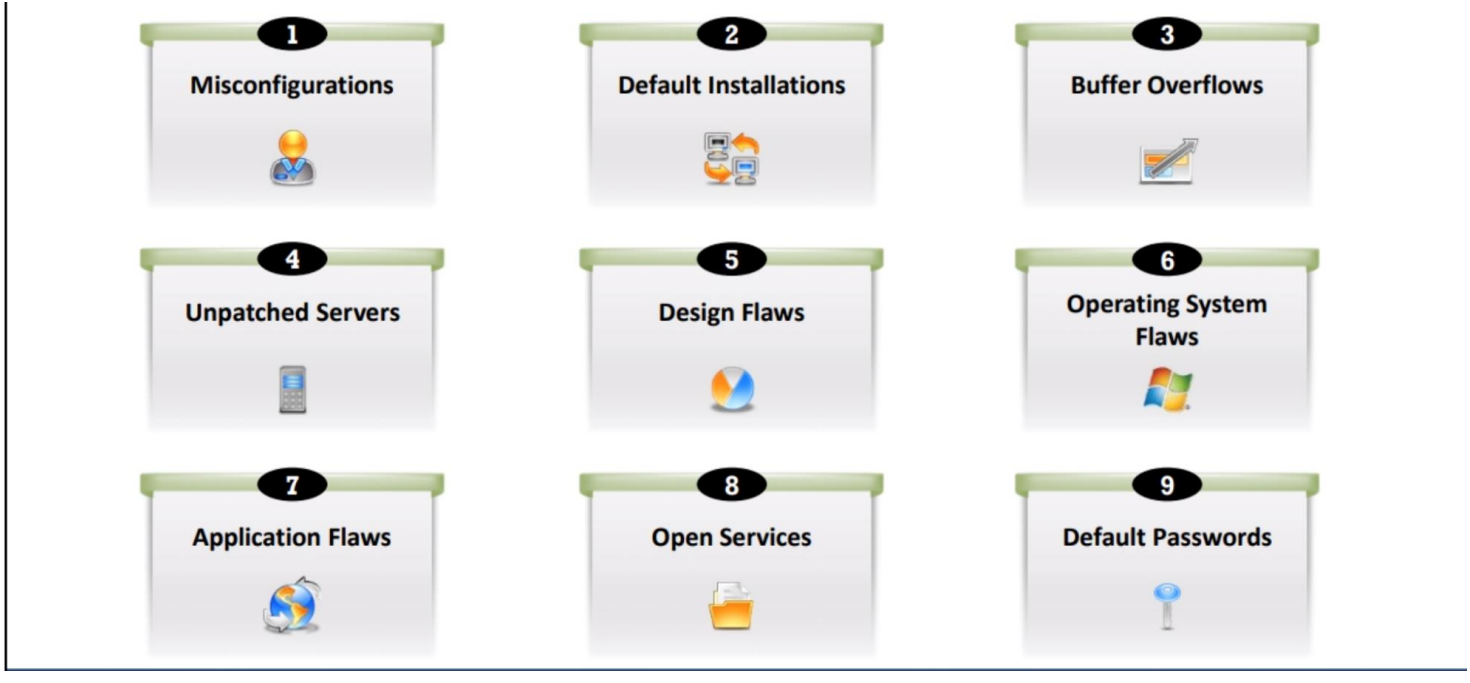
Vulnerability Research

- The process of **discovering vulnerabilities and design flaws** that will open an operating system and its applications to attack or misuse
- Vulnerabilities are classified based on **severity level** (low, medium, or high) and **exploit range** (local or remote)

An administrator needs vulnerability research

1. To gather information about **security trends**, **threats**, and **attacks**
2. To find **weaknesses** and alert the network administrator before a **network attack**
3. To **get information** that helps to prevent security problems
4. To know **how to recover** from a network attack

Vulnerability Classification



Misconfiguration

- Misconfiguration is the most common vulnerability that is mainly caused by human error, which allows attackers to gain unauthorized access to the system. This may happen intentionally or unintentionally affecting web servers, application platform, database and network.

A system can be misconfigured in so many ways such as Disabling security settings and features, Improperly authenticated external systems, Running unnecessary services on a machine etc..

Attackers can easily detect these misconfigurations using scanning tools and then exploit the backend systems. It is important for the administrators to change default configuration of devices and optimize the security of the devices.

Default Installations

- Default installations are usually kept user friendly especially when the device is being used for the first time, as the primary concern is usability of the device rather than the device's they are connected to networks or systems that have confidential information that would result in a data breach.
- Not changing the default settings while deploying the software or hardware allows the attacker to guess the settings in order to break into the systems.

Buffer Overflows

Buffer overflows are common software vulnerabilities that happen due to coding errors allowing attackers to get access to the target system. In a buffer overflow attack, attackers undermine the functioning of programs and try to take the control of the system by writing content beyond the allocated size of the buffer. Insufficient bounds checking in the program is the root cause because of which the buffer is not able to handle data beyond its limit, causing the flow of data to adjacent memory locations and overwriting their data values. Systems often crash or become unstable or show erratic program behavior, when buffer overflow occurs.

Unpatched Servers

- Servers are an essential component of the infrastructure of any organization. There are several cases where organizations run unpatched and misconfigured servers compromising the security and integrity of the data in the system. Hackers look out for these vulnerabilities in the servers and exploit them.
- As these unpatched servers are a hub for the attackers, they serve as an entry point into the network.
- This can lead to exposure of private data, financial loss, discontinuation of operations, etc.
- Updating software regularly and maintaining systems properly by patching and fixing bugs can help in mitigating vulnerabilities caused due to unpatched servers.

Design Flaws

Vulnerabilities that are caused due to design flaws are universal to all operating devices and systems.

Design vulnerabilities such as incorrect encryption or poor validation of data, refer to logical flaws in the functionality of the system that is exploited by the attackers to bypass the detection mechanism and acquire access to a secure system.

Operating System

Flaws Due to vulnerabilities in the operating systems, applications such as Trojans, worms, and viruses pose threats. These attacks are performed by using malicious code, script or unwanted software, which result in loss of sensitive information and loss of control on computer operations. Timely patching of OS, installing minimum software applications and use of applications with firewall capabilities are essential steps that an administrator needs take to protect OS from any attack.

Application Flaws

Application flaws are vulnerabilities in applications that are exploited by the attackers. Applications should be secured using validation and authorization of the user. Applications pose security threats such as data tampering and unauthorized access to configuration stores.

If the applications are not secured, sensitive information may be lost or corrupted. Hence, it is important for developers to understand the anatomy of common security vulnerabilities and develop highly secure applications by providing proper user validation and authorization.

Open Services

Open ports and services may lead to loss of data, DoS attacks and allow attackers to perform further attacks on other connected devices. Administrators need to continuously check for unnecessary or insecure ports and services to reduce the risk on the network.

Default Passwords

- Manufacturers provide default passwords to the users to access the device during initial set-up and users need to change the passwords for future use. However, users forget to update the passwords and continue using the default passwords making devices and systems vulnerable to various attacks such as brute-force, dictionary attack, etc.
- Attackers exploit this vulnerability to obtain access to the system. Passwords should be kept secret; failing to protect the confidentiality of a password allows the system to be compromised with ease.

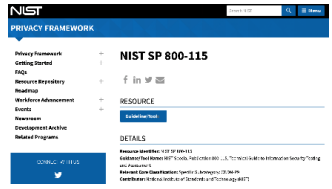
As a practical matter, it is impossible to remove every technical vulnerability from a given environment. There are several reasons for this.

- **Some vulnerabilities are latent** until they are discovered and publicly disclosed; these are typically referred to as zero days, referring to the fact that there are zero days since public disclosure.
- **Other vulnerabilities might persist due to challenges associated with patching certain devices**, including those that support legacy applications or that are directly managed by external vendors.
- Still other vulnerabilities **might be cost prohibitive** to address for other reasons.

- This in turn means that any given environment will have multiple latent vulnerabilities at any given time.
- A vulnerability assessment is the process of identifying and analyzing those security vulnerabilities that might exist in the enterprise.
- Discovery, testing, analysis and reporting of systems and vulnerabilities.
- Manual techniques can also be used to identify technical, physical and governance-based vulnerabilities.

- Vulnerability assessments are not exploitative by nature (compared to, for example, ethical hacking or penetration tests).
- In conducting a vulnerability assessment, practitioners (or the tools they employ) will not typically exploit vulnerabilities they find. Instead, a vulnerability assessment serves an altogether different purpose: it allows an enterprise to focus on reconnaissance and discover weaknesses in its environment.
- To accomplish that goal, a suspected vulnerability does not typically need to be exploited to identify its existence and apply a fix.

Types of Vulnerability Assessments



NIST Special Publication 800-115, **"Technical Guide to Information Security Testing and Assessment"** is a practical guide to techniques for information security testing and assessment. The standard discusses the following four vulnerability assessment activities:

1. Network-based scans
2. Host-based scans(i.e., system-configuration reviews)
3. Wireless scans
4. Application scans (included within penetration testing)

1- Network-Based Scans

- Network assessments determine the possible network security attacks that may occur on an organization's system. These assessments evaluate the organization's system for vulnerabilities such as missing patches, unnecessary services, weak authentication, and weak encryption.
- Network assessment professionals use firewall and network scanners such as Nessus. These scanners **find open ports**, **recognize the services** running on those ports, and **find vulnerabilities** associated with these services. These assessments help organizations determine how vulnerable systems are to Internet and intranet attacks, and how an attacker can gain access to important information.

2- Host-Based Scans

- Network-based scans may sometimes miss weaknesses that can be exploited only by a user who is logged onto the system (i.e., local exploits) because they may only have the capability or be configured only to look for “remotely exploitable” vulnerabilities (i.e., those that are accessible from somewhere else on the network).
- Host- based scans, by contrast, are executed from the target computer or are remotely controlled with authenticated account access to the target computer. These scans can provide greater visibility into a system’s configuration settings and patch details, while covering ports and services that are also visible to network-based scans. For this reason, host-based scans are more comprehensive than network-based scans; however, that breadth typically increases their overhead and makes them harder to set up and operate.

2- Host-Based Scans Scope (Cont…)

Component	What It Checks
Operating System	Patch level, version, kernel parameters, system configuration files.
Installed Software	Versions of applications (e.g., browsers, Java, Adobe), missing updates.
User Accounts	Password policies, privileged accounts, unused accounts, weak passwords.
File System	File permissions, sensitive files, log files, integrity of system files.
Running Processes	Malicious software, unnecessary services, memory usage.
Network Configuration	Local firewall settings, open sockets, routing tables.
Registry (Windows)	Security-related keys and values.

Component	What It Checks
Operating System	Patch level, version, kernel parameters, system configuration files.
Installed Software	Versions of applications (e.g., browsers, Java, Adobe), missing updates.
User Accounts	Password policies, privileged accounts, unused accounts, weak passwords.
File System	File permissions, sensitive files, log files, integrity of system files.
Running Processes	Malicious software, unnecessary services, memory usage.
Network Configuration	Local firewall settings, open sockets, routing tables.
Registry (Windows)	Security-related keys and values.

3- Wireless Network Scans

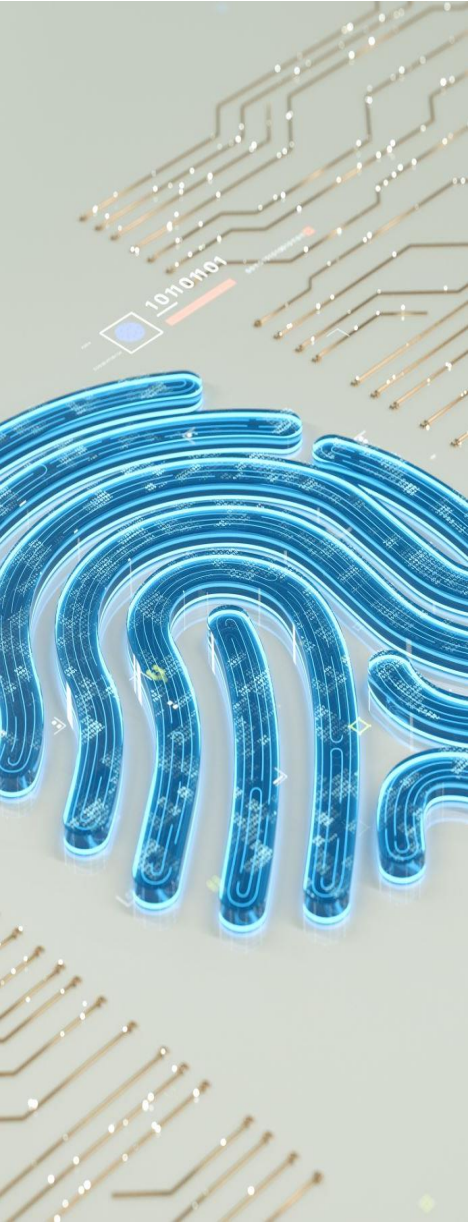
- Wireless scans of an enterprise's Wi-Fi networks focus on points of attack in wireless network infrastructure. One aspect of wireless network testing is validating that an enterprise's networks are securely configured. Although any benefit of disabling SSID broadcast to "hide" a network has long since passed, scanning validates that strong encryption is enabled and default settings are changed.
- Another purpose of wireless testing is to identify rogue access points, which pose as legitimate wireless networks of either an enterprise or a hotspot, such as a local coffee shop, to trick victims into joining an attacker's network.

Host-Based vs. Network-Based Scans

Feature	Host-Based Scan	Network-Based Scan
Perspective	**Internal** (on the host itself)	**External** (from the network)
Access Required	**High** (Admin/root credentials)	**None** or limited (network access)
Visibility	**Deep** (files, configs, users, processes)	**Shallow** (ports, services, OS guess)
Accuracy	**Very High** (exact info on patches, settings)	**Lower** (often infers information)
Impact	Can consume system resources (CPU, RAM)	Minimal impact on target host
Best For	**Compliance, precise hardening**	**Discovery, perimeter testing**

4- Application Scans

- Application scans typically focus on websites to discover and enumerate software vulnerabilities and misconfigurations.
- Many network vulnerability scanning tools also include web application security tests.
- Application security testing can be risky because scanning software may make changes to databases or delete content during testing, so enterprises should either restrict testing to nonproduction environments or exercise caution in scanning production environments.



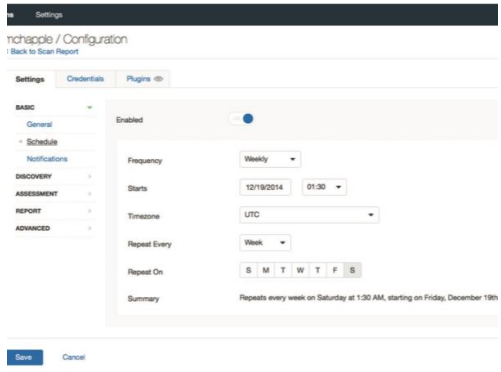
Identifying Scan Targets

Once an organization decides to conduct vulnerability scanning and determines which, if any, regulatory requirements apply to its scans, it moves on to the more detailed phases of the planning process. The next step is to identify the systems that will be covered by the vulnerability scans. Some organizations choose to cover all systems in their scanning process, whereas others scan systems differently (or not at all) depending on the answers to questions such as these:

- What is the *data classification* of the information stored, processed, or transmitted by the system?
- Is the system exposed to the Internet or other public or semipublic networks?
- What services are offered by the system?
- Is the system a production, test, or development system?
- Identifying Vulnerability Management Requirements

Organizations also use automated techniques to identify the systems that may be covered by a scan. Cybersecurity professionals use scanning tools to conduct *discovery scans* that search the network for connected systems, whether they were previously known or unknown, and build an *asset inventory*.

Determining Scan Frequency



Cybersecurity professionals depend on automation to help them perform their duties in an efficient, effective manner.

Vulnerability scanning tools allow the automated scheduling of scans to take the burden off administrators

What are vulnerability scanners and how do they work?

- Vulnerability scanners scan computers, networks, or applications looking for potential weaknesses that could be used by attackers to compromise the target. The way a vulnerability scanner works is that it probes the system by sending specific data to the target host/network, and based on its analysis of the response (fingerprint) received from the target, it can determine many things such as the following:
- Open ports
- Services
- Operating System
- Vulnerabilities

Pros and Cons of a Vulnerability Scanner

- The main advantage of any vulnerability scanner is **task automation;** it can automate many tasks such as reconnaissance, port scanning, service, and version detection. This can make your work faster and more effective than doing everything manually.
- On the other hand, there are some disadvantages of using a vulnerability scanner. One of the main disadvantages is that the vulnerability scanners are very loud by nature and can be easily detected since we are sending lots of traffic over the network.
- The other problem with a vulnerability scanner is that it can produce lots of false positives, meaning that it will report vulnerabilities in the target that may not exist in reality. However, it will also report a lot of false negatives, meaning that the scanner would miss or not report the vulnerabilities that actually exist.

Regulatory Environment

Many organizations find themselves bound by laws and regulations that govern the ways they store, process, and transmit information. This is especially true when the organization handles sensitive personal information or information belonging to government agencies.

Payment Card Industry Data Security Standard (PCI DSS)

orgs.
They should comply with this standard

PCI DSS prescribes specific security controls for merchants who handle credit card transactions and service providers who assist merchants with these transactions.

This standard includes what are arguably the most specific requirements for vulnerability scanning of any standard.

PCI DSS prescribes many of the details of vulnerability scans:

- ✓Organizations must run both internal and external vulnerability scans
- ✓Organizations must run scans on at least a quarterly basis (every few months) and "after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades)"
- ✓Internal scans must be conducted by qualified personnel
- ✓Organizations must remediate any high-risk vulnerabilities and repeat scans to confirm that they are resolved until they receive a "clean" scan report
- ✓External scans must be conducted by an Approved Scanning Vendor (ASV) authorized by PCI SSC.

- Vulnerability scanning for PCI DSS compliance is a thriving and competitive industry, and many security consulting firms specialize in these scans.
- Many organizations choose to conduct their own scans first to assure themselves that they will achieve a passing result before requesting an official scan from an Approved Scanning Vendor (ASV)

(*https://east.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors*)

.

How to Perform Vulnerability analysis?

There are many ways to perform vulnerability analysis, from manually searching through exploit database to fully automatic testing with tools like Open-Vas and Nessus vulnerability scanner.

Vulnerability scanning with automated tools is a very aggressive way of vulnerability scanning as it takes a lot of requests and traffic to complete this kind of scans. In some cases, the great deal of traffic might crash (DOS) target hosts and services, so it is advised to be careful when using these kind of tools.

Beware to only use these vulnerability scans on hosts which you have permission to scan. When you are using automated tools for vulnerability scanning it is always wise to use multiple tools to rule out false positives. Therefor it is important to also master the manual ways of vulnerability analysis and do not become too reliant on automated scanners

Many of the services contain known vulnerabilities which can be exploited. The following step is to find out which services are vulnerable and collect information about how they can be exploited. There are several sources which can be used to determine if a service is vulnerable or not.

The most popular and knows sources are:

1. exploit-db from Offensive Security and the Open Source Vulnerability Database (OSVDB).
2. searchsploit, an offline exploit database included with Kali Linux.

Common Vulnerability Scoring System

Common Vulnerability Scoring System Version 3.1 Calculator

Hover over metric group names, metric names and metric values for a summary of the information in the official CVSS v3.1 Specification Document. The Specification is available in the list of links on the left, along with a User Guide providing additional scoring guidance, an Examples document of scored vulnerabilities, and notes on using this calculator (including its design and an XML representation for CVSS v3.1).

Base Score

Select values for all base metrics to generate score

Attack Vector (AV)

Network (N) | Adjacent (A) | Local (L) | Physical (P)

Attack Complexity (AC)

Low (L) | High (H)

Privileges Required (PR)

None (N) | Low (L) | High (H)

User Interaction (UI)

Scope (S)

Unchanged (U) | Changed (C)

Confidentiality (C)

None (N) | Low (L) | High (H)

Integrity (I)

None (N) | Low (L) | High (H)

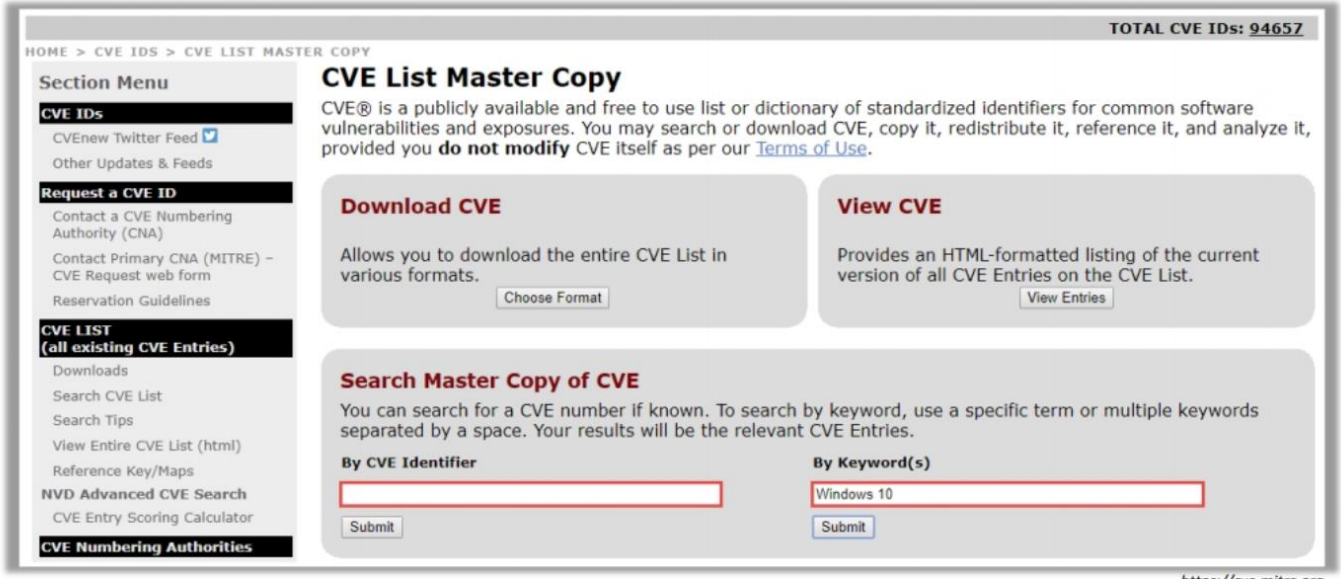
Availability (A)

CVSS assessment consists of three metrics for measuring vulnerabilities:

- **Base Metrics**: It represents the inherent qualities of a vulnerability
- **Temporal Metrics:** It represents the features that keep on changing during the lifetime of a vulnerability.
- **Environmental Metrics:** It represents the vulnerabilities that are based on a particular environment or implementation.
- Each metrics sets a score from 1-10, 10 being the most severe.
- CVSS score is calculated and generated by a vector string, which represents the numerical score for each group in the form of a block of a text.
- CVSS calculator is developed to rank the security vulnerabilities and provide the user with overall severity and risk related to the vulnerability

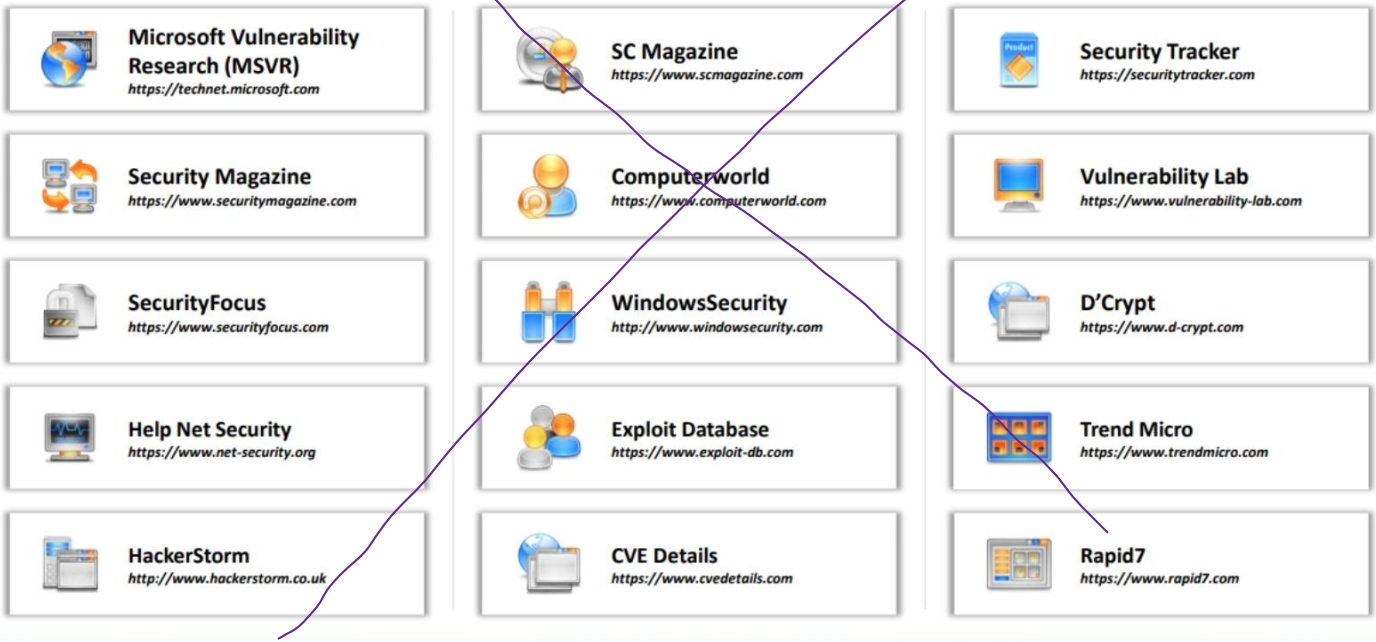
Common Vulnerabilities and Exposures (CVE)

- CVE® is a publicly available and free to use **list or dictionary of standardized identifiers** for common software vulnerabilities and exposures



https://nvd.nist.gov/vuln

Resources for Vulnerability Research



Vulnerability Assessment Tools

Core Impact Pro
https://www.coresecurity.com

N-Stalker Web Application Security Scanner X Enterprise Edition
https://www.nstalker.com

Acunetix Web Vulnerability Scanner
https://www.acunetix.com

Nipper Studio
https://www.titania.com

Nexpose
https://www.rapid7.com

Secunia Personal Software Inspector (PSI)
https://secuniaresearch.flexerasoftware.com

Burp Suite
https://www.portswigger.net

Nsauditor Network Security Auditor
http://www.nsauditor.com

ScanLine
https://www.mcafee.com

Nmap
https://nmap.org