Vulnerability Analysis

Jayson Waigwa - Security Analyst

Strathmore
UNIVERSITY

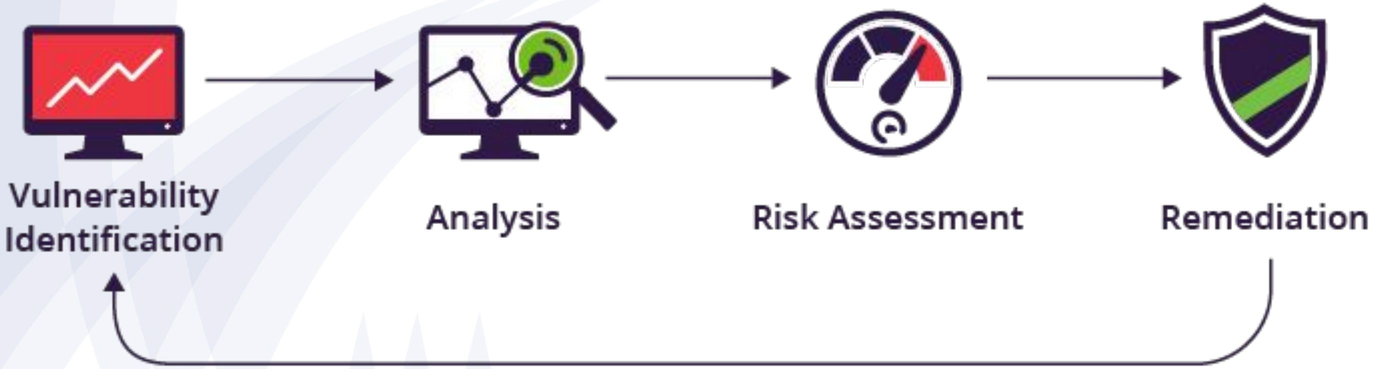
Outline

SESSION	CONTENT
1	Vulnerability Research, Vulnerability Assessment, and scoring System
2	Vulnerability Management Life Cycle (Assessment Phases)
3	Types of Vulnerabilities and Assessment Techniques
4	Different approaches of Vulnerability Assessment Solutions
5	Types of VA tools and criterias for selection
6	Generating and Analyzing VA reports.

Introduction

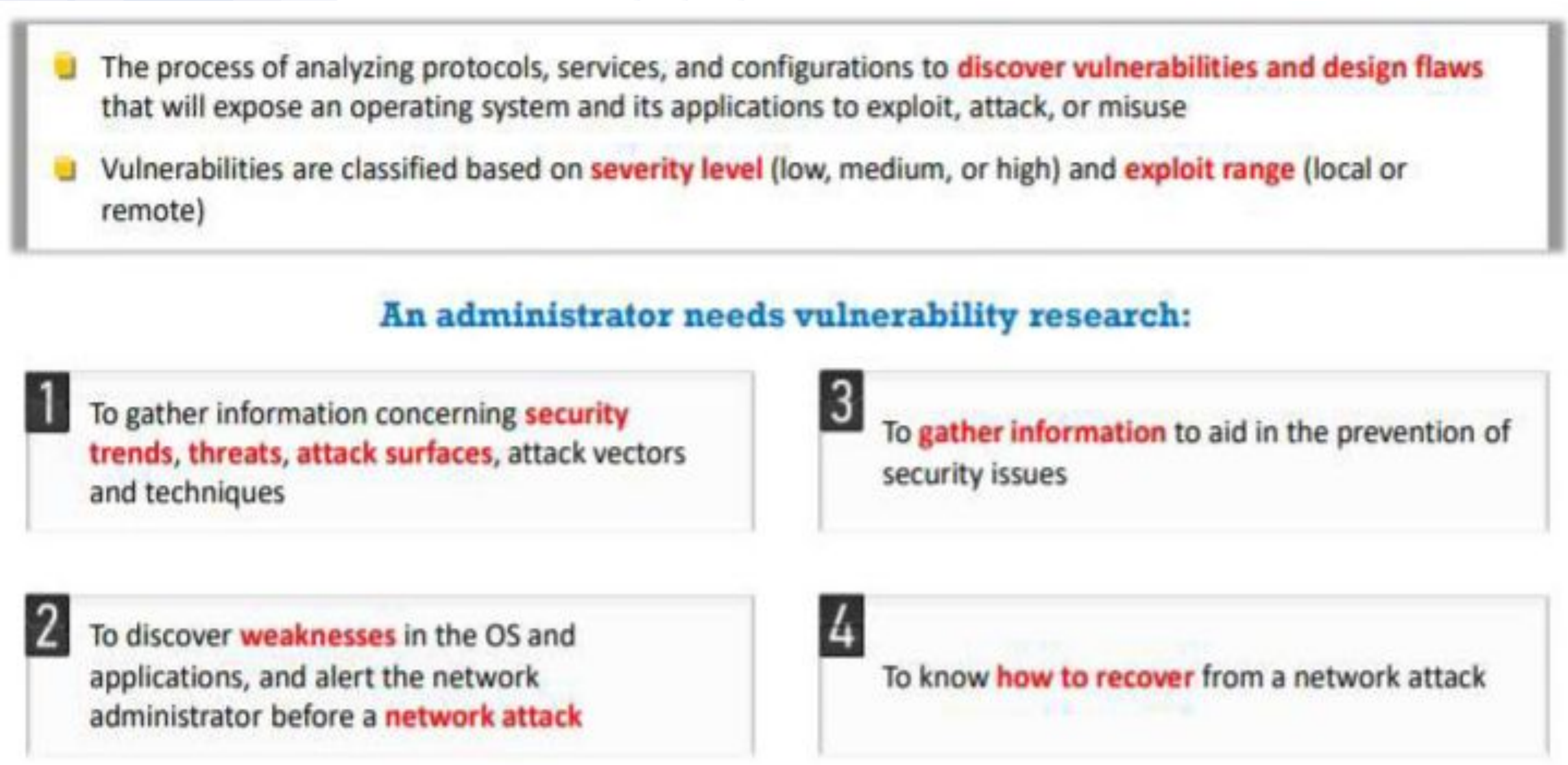
- In today’s world, organizations depend heavily on IT for protecting vital information.

Vulnerability Assessment



- There are 2 main causes for vulnerable systems:
  - Misconfiguration and
  - Poor programming practices.

Vulnerability Research



- The process of analyzing protocols, services, and configurations to **discover vulnerabilities and design flaws** that will expose an operating system and its applications to exploit, 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 concerning **security trends**, **threats**, **attack surfaces**, attack vectors and techniques

2 To discover **weaknesses** in the OS and applications, and alert the network administrator before a **network attack**

3 To **gather information** to aid in the prevention of security issues

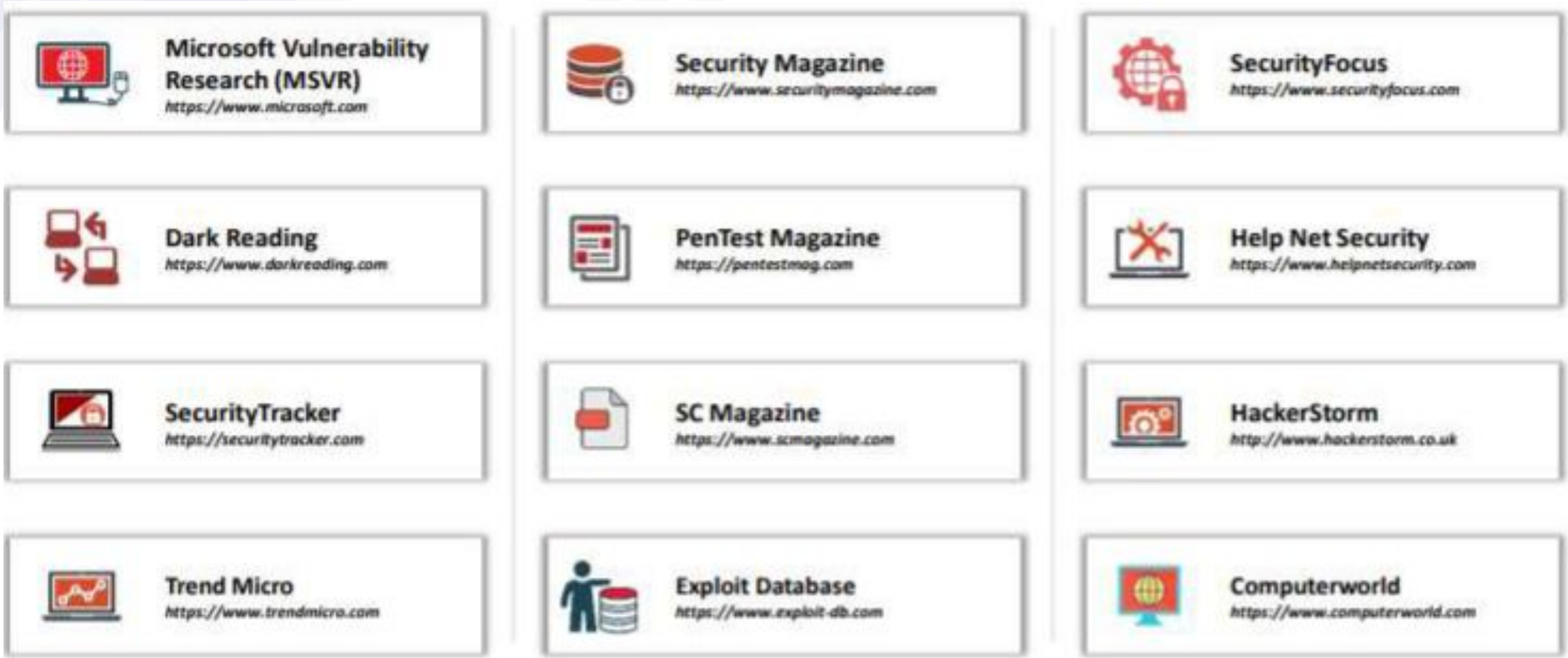
4 To know **how to recover** from a network attack

Why does an ethical hacker need to keep up with most recently discovered vulnerabilities and exploits?

cont’d

- Security experts and vulnerability scanners classify vulnerabilities by:
  - Severity level (Low, Medium and High)
  - Exploit range (Local or Remote)

Resources for VR



Microsoft Vulnerability Research (MSVR)
https://www.microsoft.com

Security Magazine
https://www.securitymagazine.com

SecurityFocus
https://www.securityfocus.com

Dark Reading
https://www.darkreading.com

PenTest Magazine
https://pentestmag.com

Help Net Security
https://www.helpnetsecurity.com

SecurityTracker
https://securitytracker.com

SC Magazine
https://www.scmagazine.com

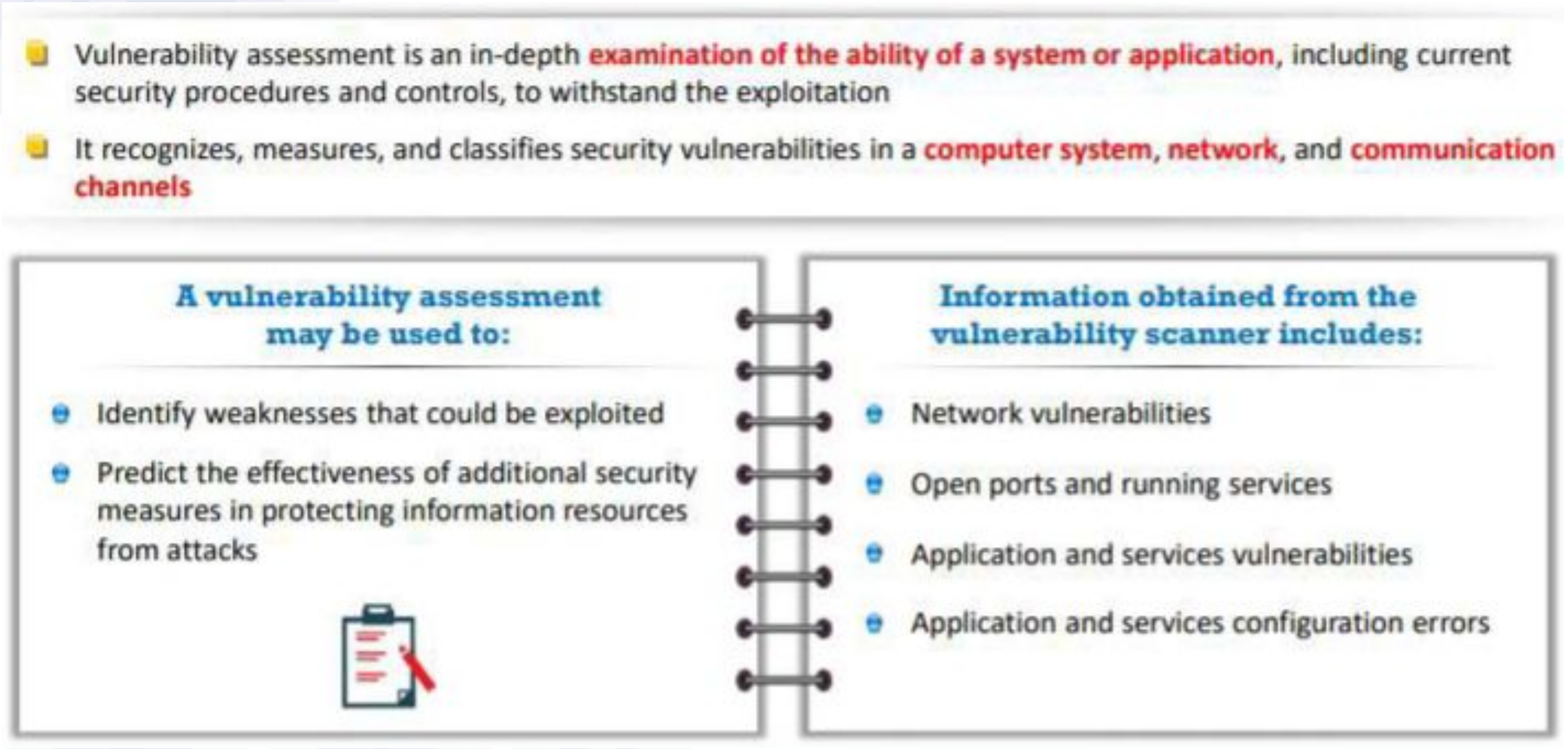
HackerStorm
http://www.hackerstorm.co.uk

Trend Micro
https://www.trendmicro.com

Exploit Database
https://www.exploit-db.com

Computerworld
https://www.computerworld.com

Vulnerability Assessment



- Vulnerability assessment is an in-depth **examination of the ability of a system or application**, including current security procedures and controls, to withstand the exploitation
- It recognizes, measures, and classifies security vulnerabilities in a **computer system**, **network**, and **communication channels**

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 attacks

Information obtained from the vulnerability scanner includes:

- Network vulnerabilities
- Open ports and running services
- Application and services vulnerabilities
- Application and services configuration errors

Types of Network Vulnerability Scanning

- Active Scanning
- Passive Scanning

What are some of the limitations of Vulnerability assessments?

Vulnerability Scoring Systems and DB

Strathmore UNIVERSITY

Common Vulnerability Scoring System (CVSS)

- CVSS provides an open framework **for communicating the characteristics and impacts** of IT vulnerabilities
- Its quantitative model ensures repeatable accurate measurement, while enabling users to view the **underlying vulnerability characteristics** used to **generate the scores**

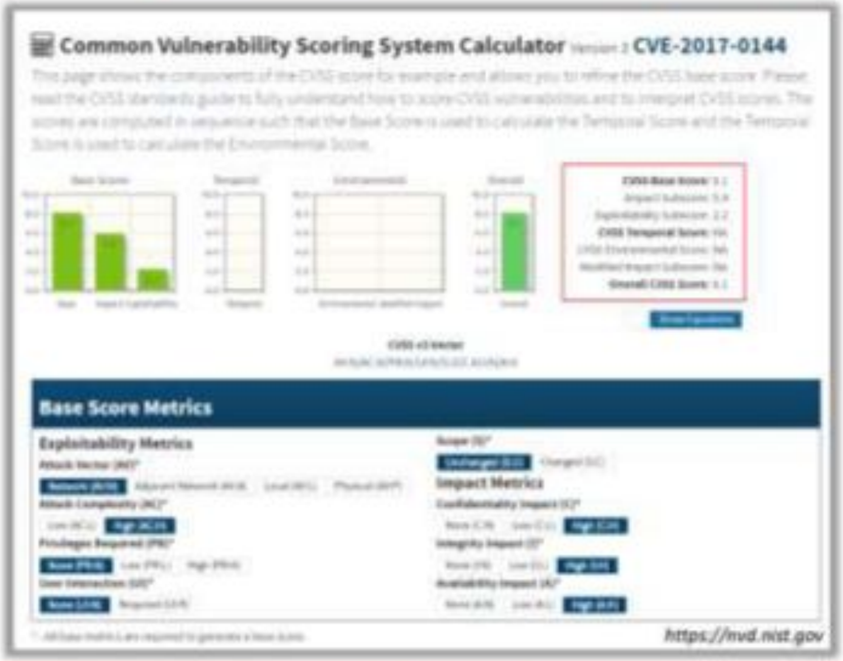
CVSS v3.0 Ratings

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

CVSS v2.0 Ratings

Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10

https://www.first.org



Common Vulnerability Scoring System Calculator Version 3 **CVE-2017-0144**

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

CVSS Base Score: [illegible]
Impact Subscore: [illegible]
Exploitability Subscore: [illegible]
CVSS Temporal Score: [illegible]
CVSS Environmental Score: [illegible]
Modified Impact Subscore: [illegible]
Overall CVSS Score: [illegible]

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*: Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)

Attack Complexity (AC)*: Low (AC:L) | High (AC:H)

Privileges Required (PR)*: None (PR:N) | Low (PR:L) | High (PR:H)

User Interaction (UI)*: None (UI:N) | Required (UI:R)

Scope (S)*: Unchanged (S:U) | Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*: None (C:N) | Low (C:L) | High (C:H)

Integrity Impact (I)*: None (I:N) | Low (I:L) | High (I:H)

Availability Impact (A)*: None (A:N) | Low (A:L) | High (A:H)

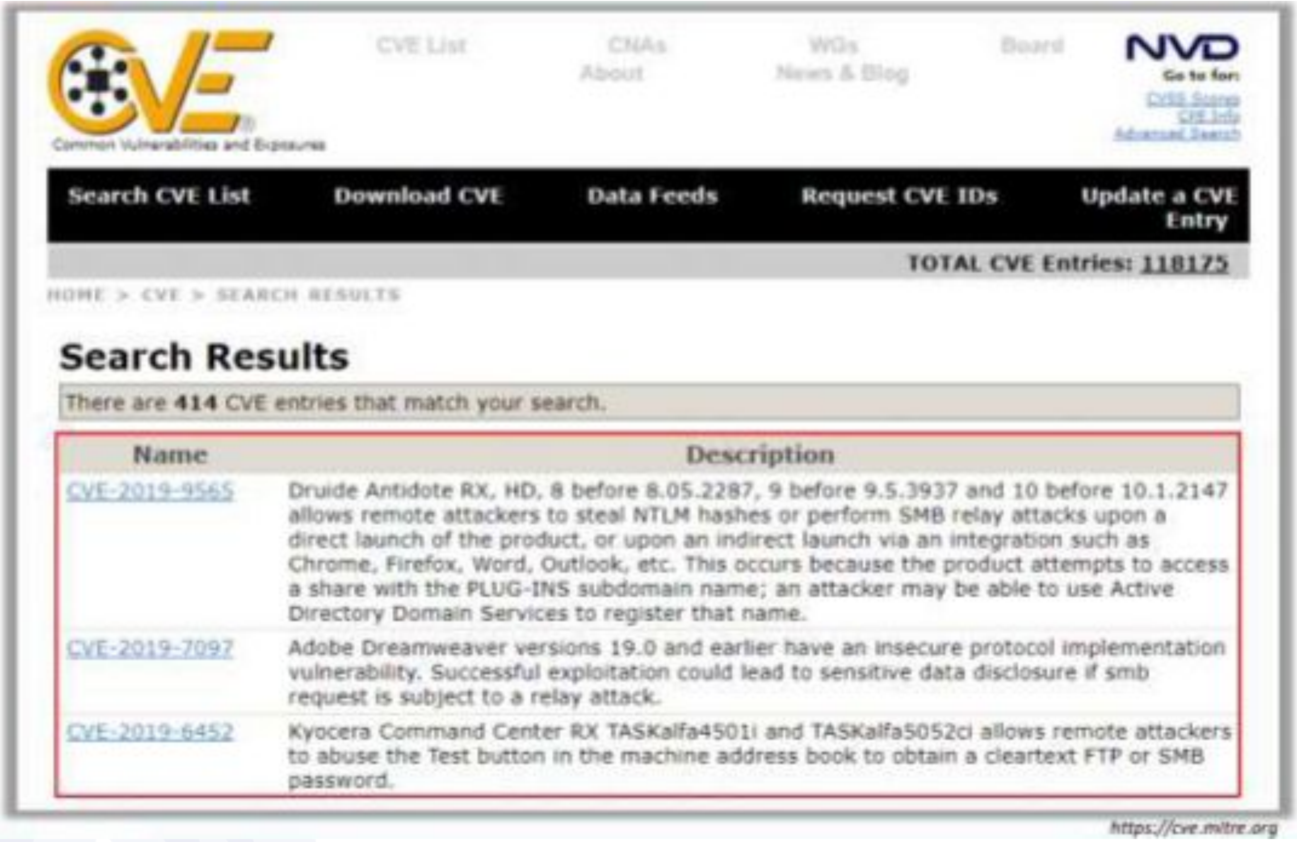
* - All base metrics are required to generate a base score.

https://nvd.nist.gov

cont'd CVE

Common Vulnerabilities and Exposures (CVE)

A publicly available and free-to-use **list or dictionary of standardized identifiers** for common software vulnerabilities and exposures



TOTAL CVE Entries: 118175

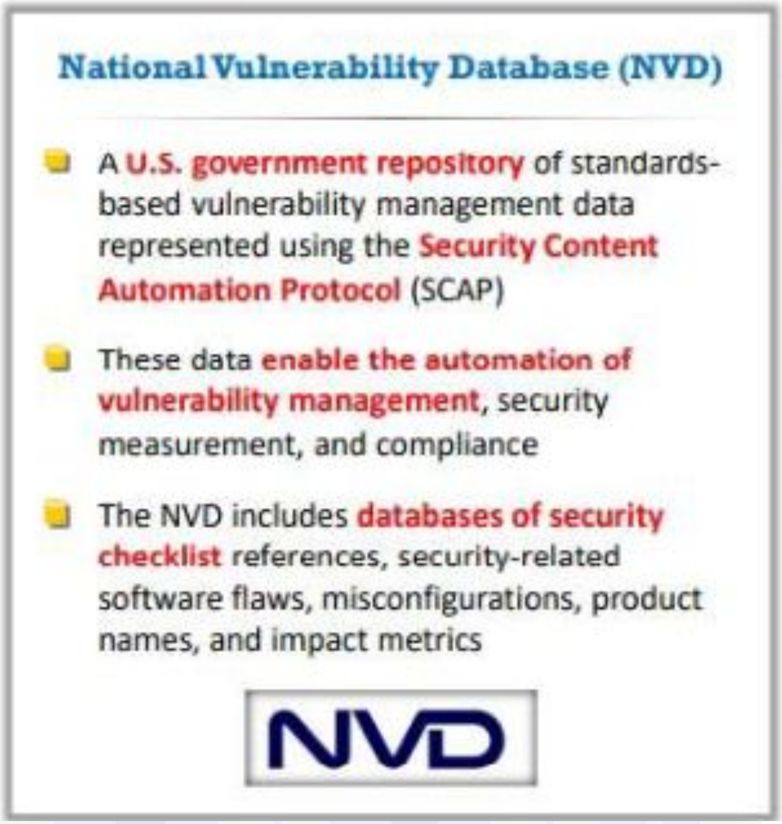
Search Results

There are **414** CVE entries that match your search.

Name	Description
CVE-2019-9565	Druide Antidote RX, HD, 8 before 8.05.2287, 9 before 9.5.3937 and 10 before 10.1.2147 allows remote attackers to steal NTLM hashes or perform SMB relay attacks upon a direct launch of the product, or upon an indirect launch via an integration such as Chrome, Firefox, Word, Outlook, etc. This occurs because the product attempts to access a share with the PLUG-INS subdomain name; an attacker may be able to use Active Directory Domain Services to register that name.
CVE-2019-7097	Adobe Dreamweaver versions 19.0 and earlier have an insecure protocol implementation vulnerability. Successful exploitation could lead to sensitive data disclosure if smb request is subject to a relay attack.
CVE-2019-6452	Kyocera Command Center RX TASKalfa4501i and TASKalfa5052ci allows remote attackers to abuse the Test button in the machine address book to obtain a cleartext FTP or SMB password.

https://cve.mitre.org

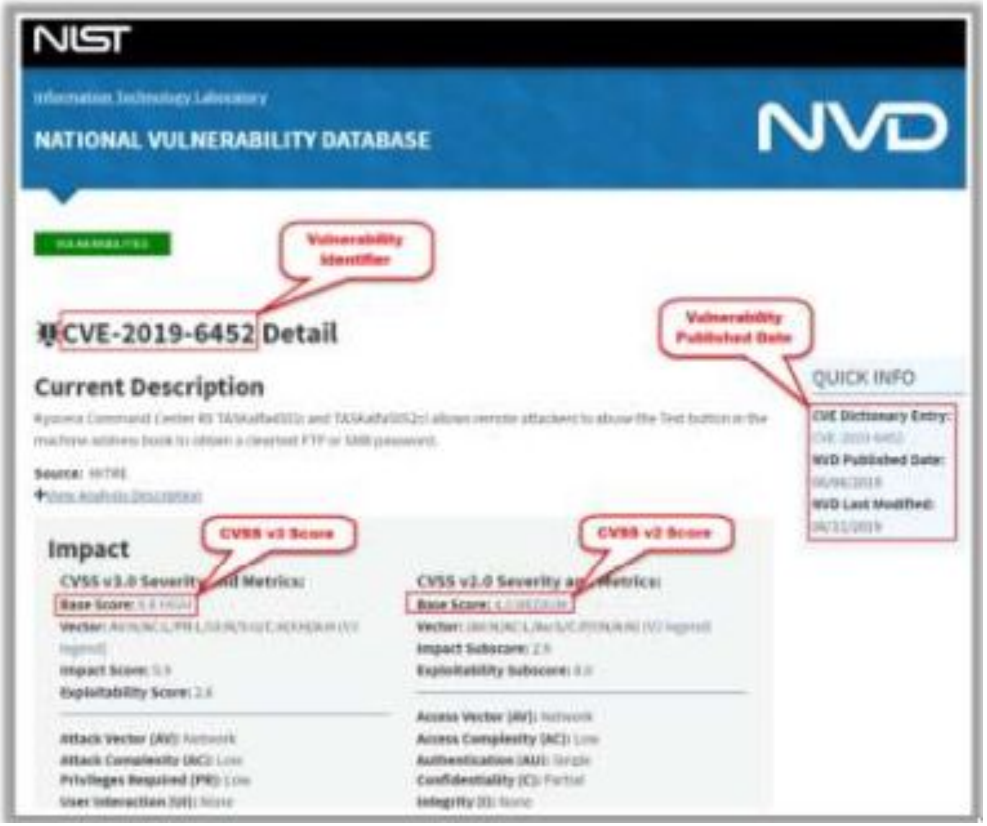
Cont’d NVD



National Vulnerability Database (NVD)

- A **U.S. government repository** of standards-based vulnerability management data represented using the **Security Content Automation Protocol** (SCAP)
- These data **enable the automation of vulnerability management**, security measurement, and compliance
- The NVD includes **databases of security checklist** references, security-related software flaws, misconfigurations, product names, and impact metrics

NVD



NIST

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NVD

VULNERABILITIES

CVE-2019-6452 Detail

Current Description

Kyocera Command Center RX TASKalfa4501i and TASKalfa5052ci allows remote attackers to abuse the Test button in the machine address book to obtain a cleartext FTP or SMB password.

Source: MITRE

+View Analysis Description

Impact

CVSS v3.0 Severity and Metrics:

Base Score: 8.8 HIGH

Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H (V3 legend)

Impact Score: 5.9

Exploitability Score: 2.8

Attack Vector (AV): Network

Attack Complexity (AC): Low

Privileges Required (PR): Low

User Interaction (UI): None

CVSS v2.0 Severity and Metrics:

Base Score: 4.0 MEDIUM

Vector: (AV:N/AC:L/Au:S/C:P/I:N/A:N) (V2 legend)

Impact Subscore: 2.9

Exploitability Subscore: 8.0

Access Vector (AV): Network

Access Complexity (AC): Low

Authentication (AU): Single

Confidentiality (C): Partial

Integrity (I): None

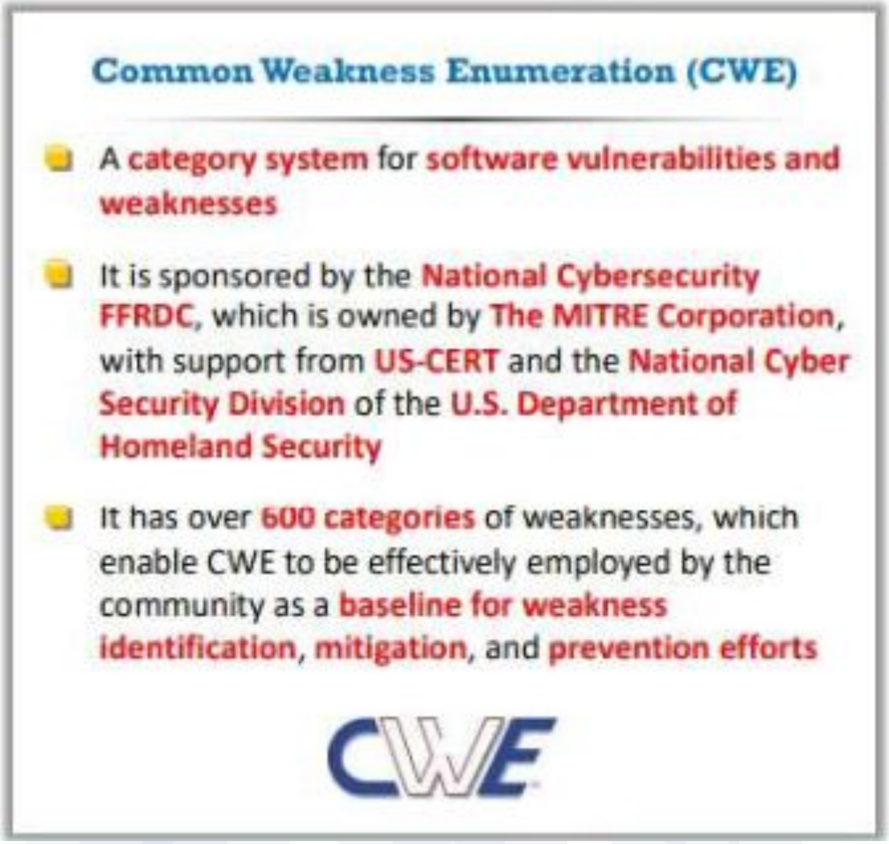
QUICK INFO

CVE Dictionary Entry:
CVE-2019-6452

NVD Published Date:
06/06/2019

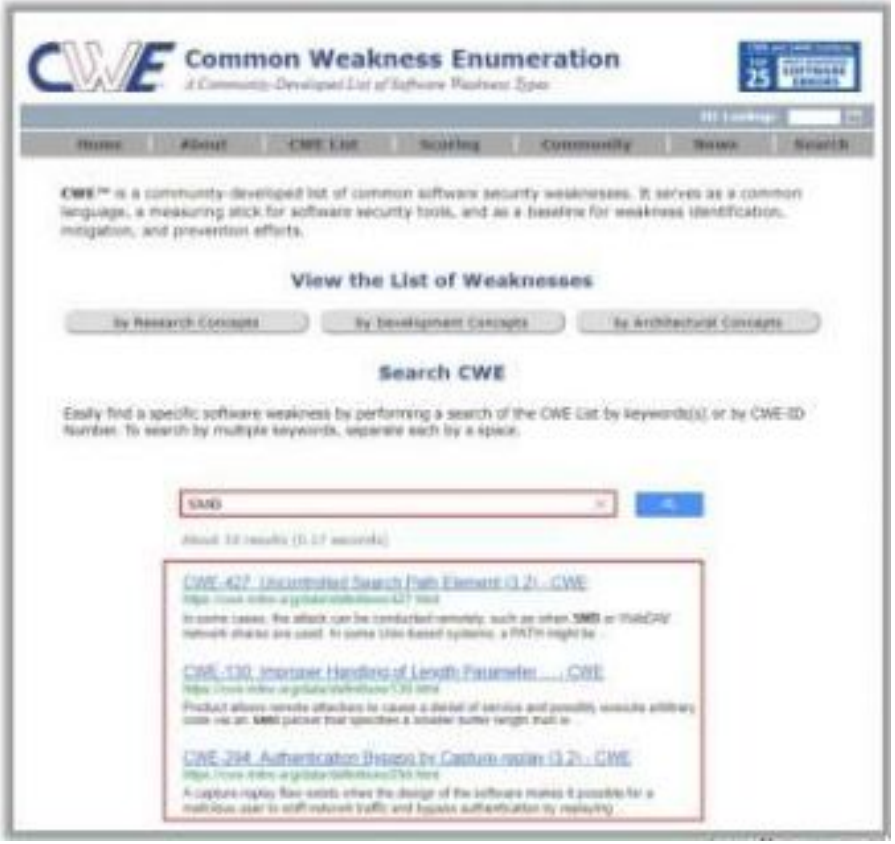
NVD Last Modified:
06/11/2019

Cont'd CWE



Common Weakness Enumeration (CWE)

- A **category system** for **software vulnerabilities and weaknesses**
- It is sponsored by the **National Cybersecurity FFRDC**, which is owned by **The MITRE Corporation**, with support from **US-CERT** and the **National Cyber Security Division** of the **U.S. Department of Homeland Security**
- It has over **600 categories** of weaknesses, which enable CWE to be effectively employed by the community as a **baseline for weakness identification**, **mitigation**, and **prevention efforts**


CWE
Common Weakness Enumeration
A Community-Developed List of Software Weakness Types
25
ID Lookup:
Home
About
CWE List
Scoring
Community
News
Search

CWE™ is a community-developed list of common software security weaknesses. It serves as a common language, a measuring stick for software security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.

View the List of Weaknesses

by Research Concepts
by Development Concepts
by Architectural Concepts

Search CWE

Easily find a specific software weakness by performing a search of the CWE List by keyword(s) or by CWE-ID Number. To search by multiple keywords, separate each by a space.

SMB

About 10 results (0.17 seconds)

CWE-427: Uncontrolled Search Path Element (3.2) - CWE
https://cwe.mitre.org/data/definitions/427.html
In some cases, the attack can be conducted remotely, such as when **SMB** or WebDAV network shares are used. In some Unix-based systems, a PATH might be ...

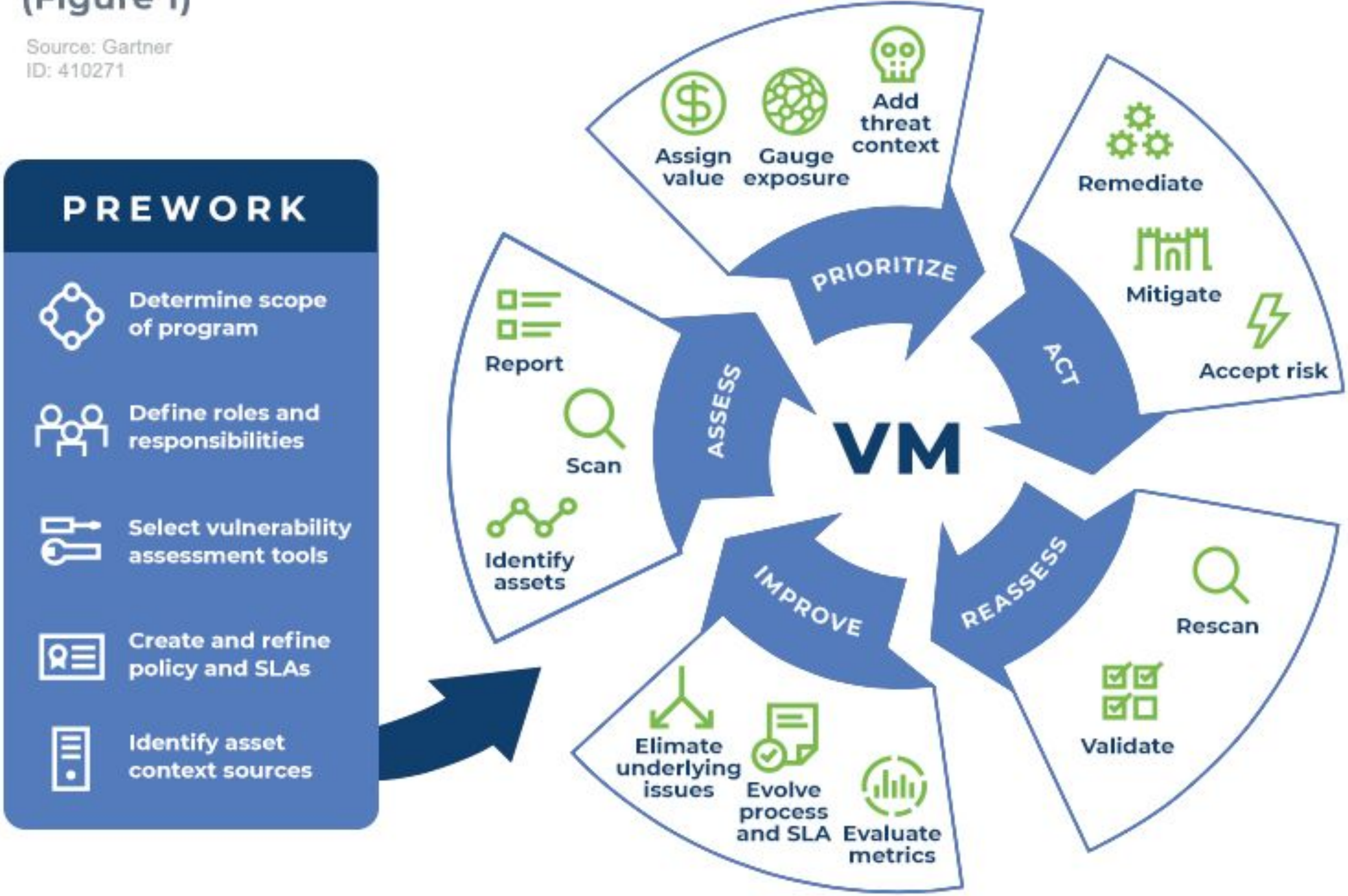
CWE-130: Improper Handling of Length Parameter ... - CWE
https://cwe.mitre.org/data/definitions/130.html
Product allows remote attackers to cause a denial of service and possibly execute arbitrary code via an **SMB** packet that specifies a smaller buffer length than is ...

CWE-294: Authentication Bypass by Capture-replay (3.2) - CWE
https://cwe.mitre.org/data/definitions/294.html
A capture-replay flaw exists when the design of the software makes it possible for a malicious user to sniff network traffic and bypass authentication by replaying ...

The Vulnerability Management Cycle

(Figure 1)

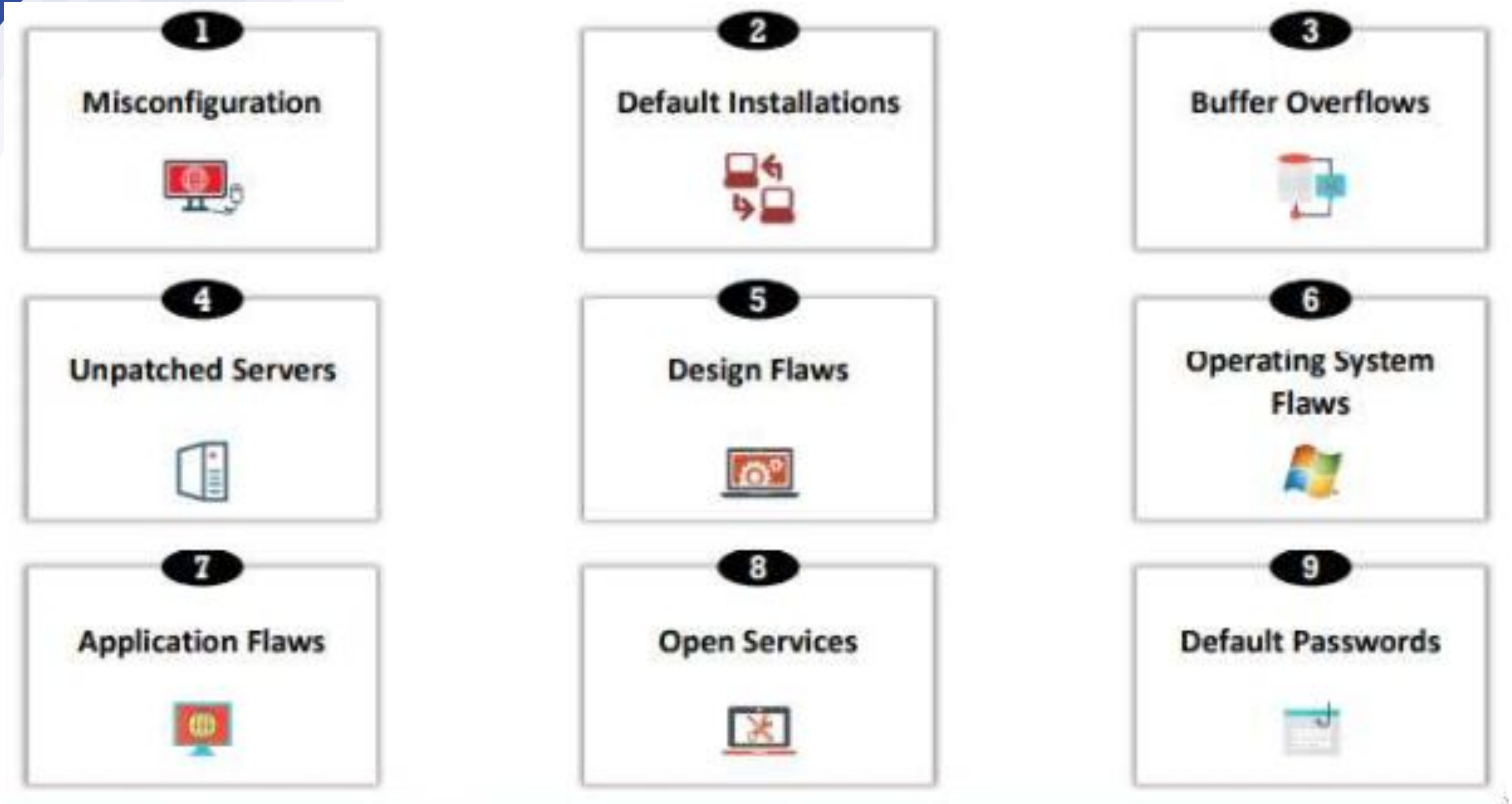
Source: Gartner
ID: 410271



PREWORK

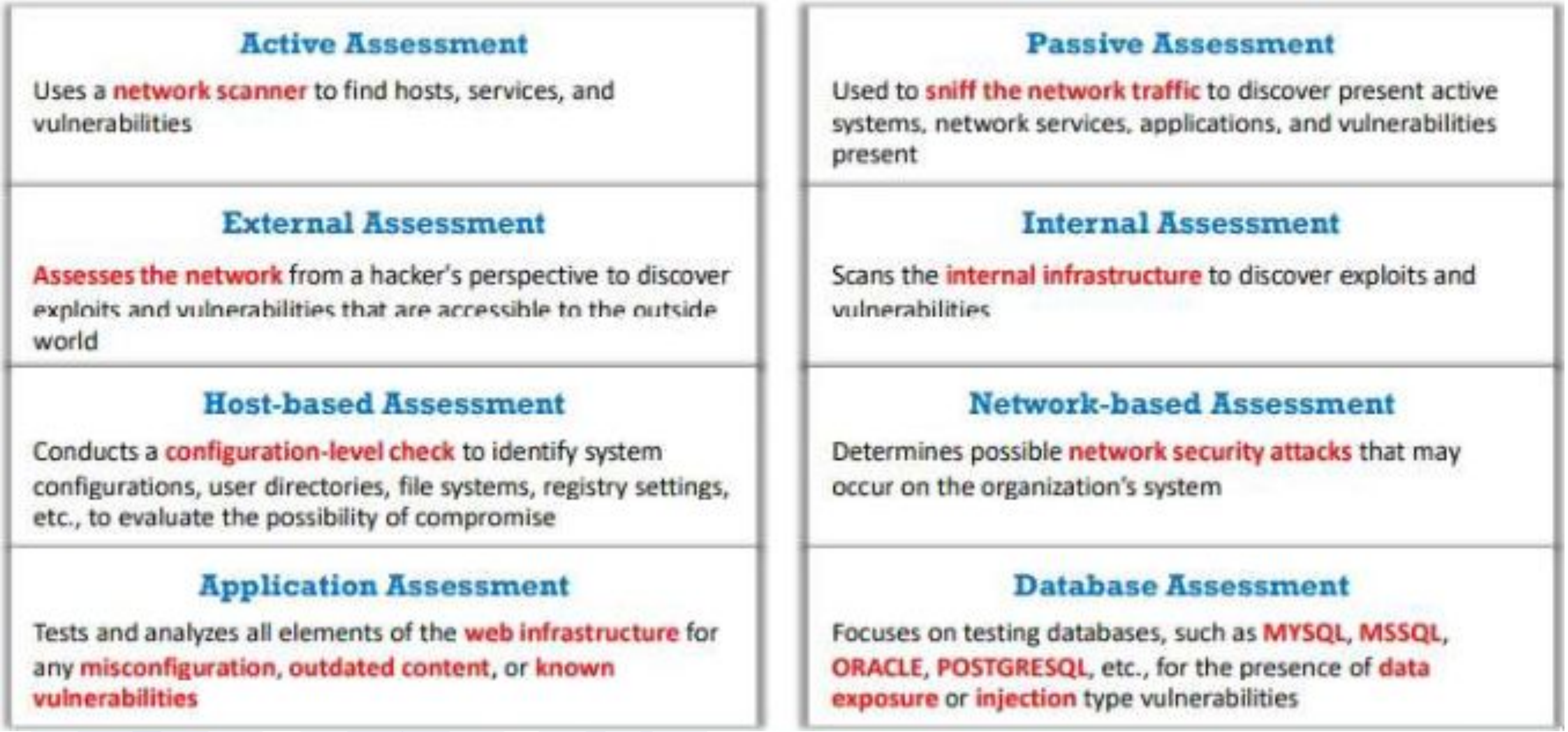
- Determine scope of program
- Define roles and responsibilities
- Select vulnerability assessment tools
- Create and refine policy and SLAs
- Identify asset context sources

Vulnerability Classification



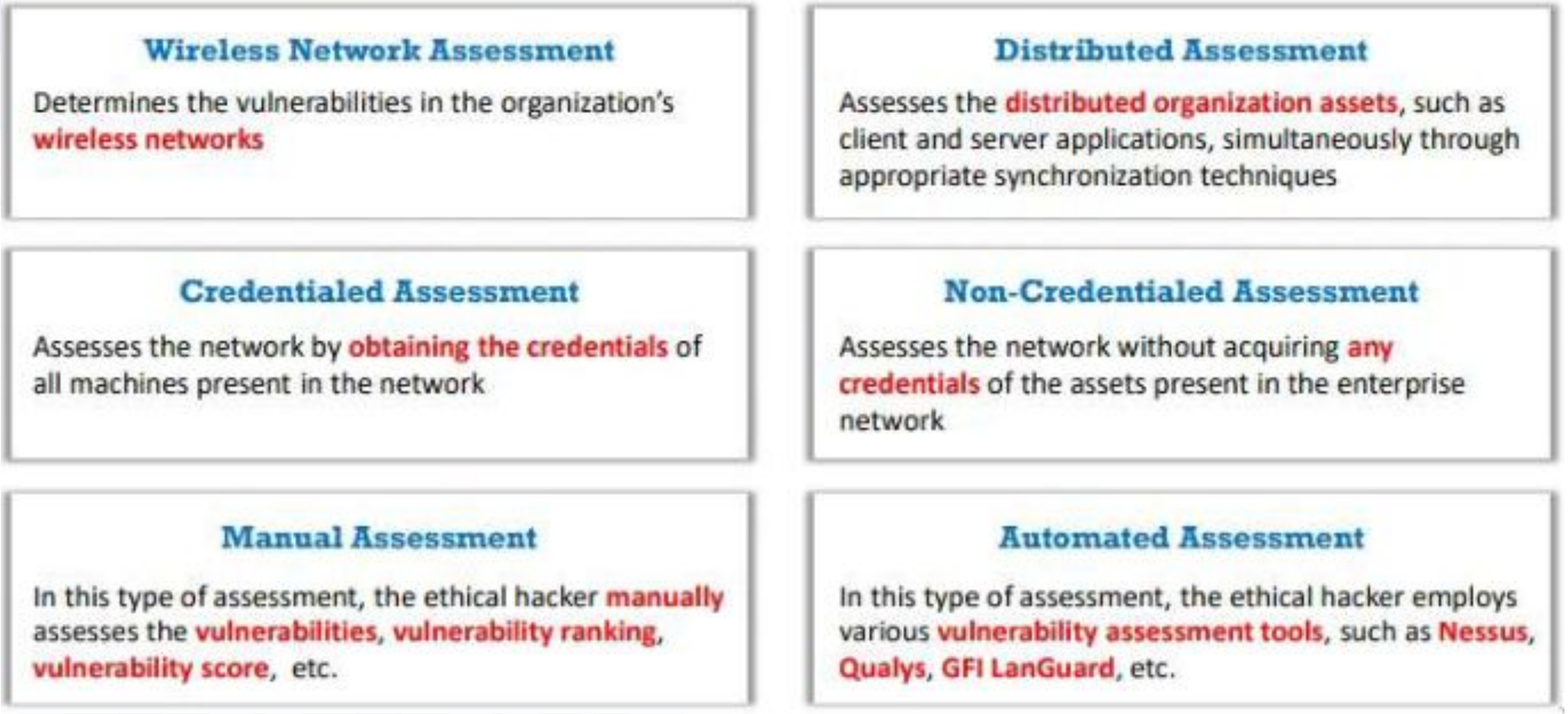
1. Misconfiguration
2. Default Installations
3. Buffer Overflows
4. Unpatched Servers
5. Design Flaws
6. Operating System Flaws
7. Application Flaws
8. Open Services
9. Default Passwords

Types of Vulnerability Assessment



Active Assessment Uses a **network scanner** to find hosts, services, and vulnerabilities	**Passive Assessment** Used to **sniff the network traffic** to discover present active systems, network services, applications, and vulnerabilities present
External Assessment **Assesses the network** from a hacker's perspective to discover exploits and vulnerabilities that are accessible to the outside world	**Internal Assessment** Scans the **internal infrastructure** to discover exploits and vulnerabilities
Host-based Assessment Conducts a **configuration-level check** to identify system configurations, user directories, file systems, registry settings, etc., to evaluate the possibility of compromise	**Network-based Assessment** Determines possible **network security attacks** that may occur on the organization's system
Application Assessment Tests and analyzes all elements of the **web infrastructure** for any **misconfiguration**, **outdated content**, or **known vulnerabilities**	**Database Assessment** Focuses on testing databases, such as **MYSQL**, **MSSQL**, **ORACLE**, **POSTGRESQL**, etc., for the presence of **data exposure** or **injection** type vulnerabilities

Cont’d



Wireless Network Assessment

Determines the vulnerabilities in the organization’s **wireless networks**

Distributed Assessment

Assesses the **distributed organization assets**, such as client and server applications, simultaneously through appropriate synchronization techniques

Credentialed Assessment

Assesses the network by **obtaining the credentials** of all machines present in the network

Non-Credentialed Assessment

Assesses the network without acquiring **any credentials** of the assets present in the enterprise network

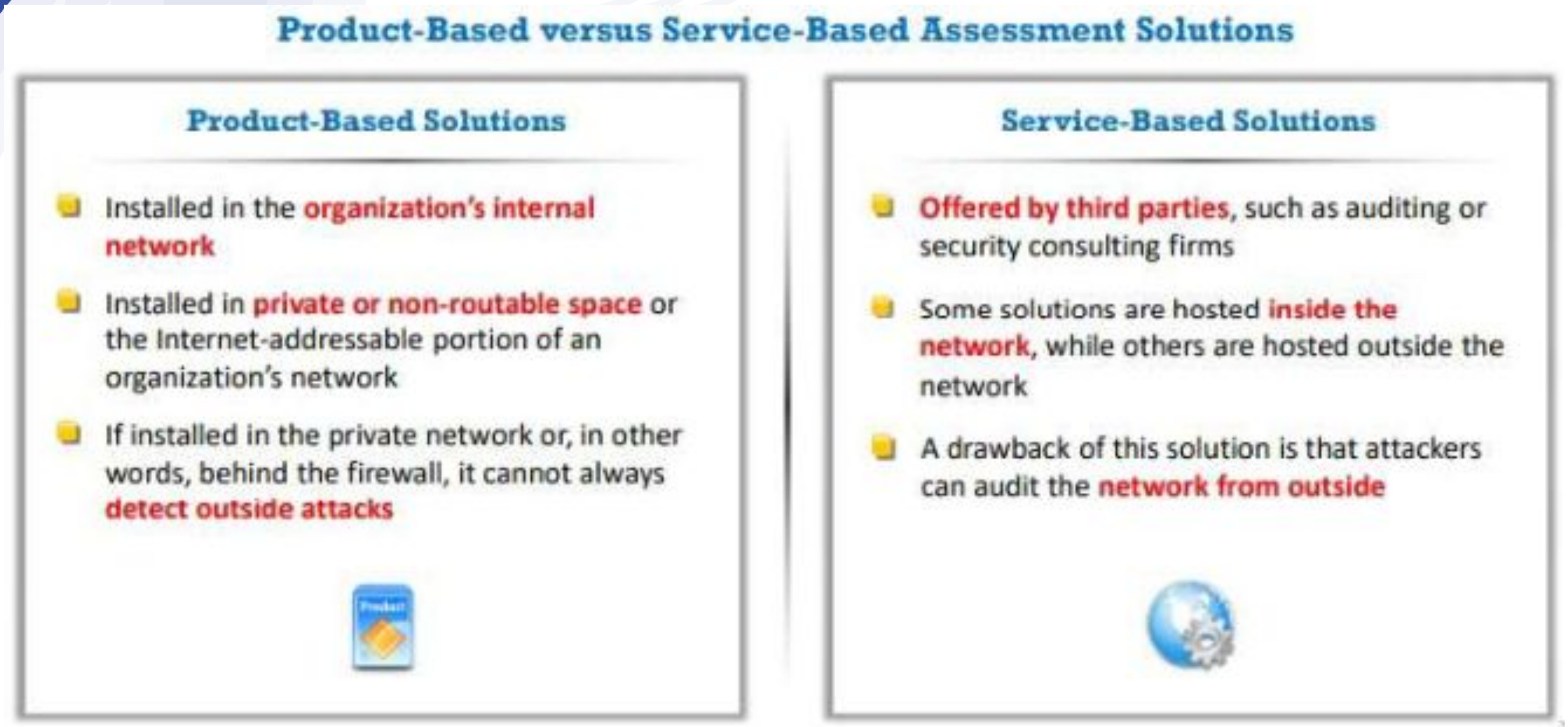
Manual Assessment

In this type of assessment, the ethical hacker **manually** assesses the **vulnerabilities**, **vulnerability ranking**, **vulnerability score**, etc.

Automated Assessment

In this type of assessment, the ethical hacker employs various **vulnerability assessment tools**, such as **Nessus**, **Qualys**, **GFI LanGuard**, etc.

Vulnerability Assessment Solutions



Product-Based versus Service-Based Assessment Solutions

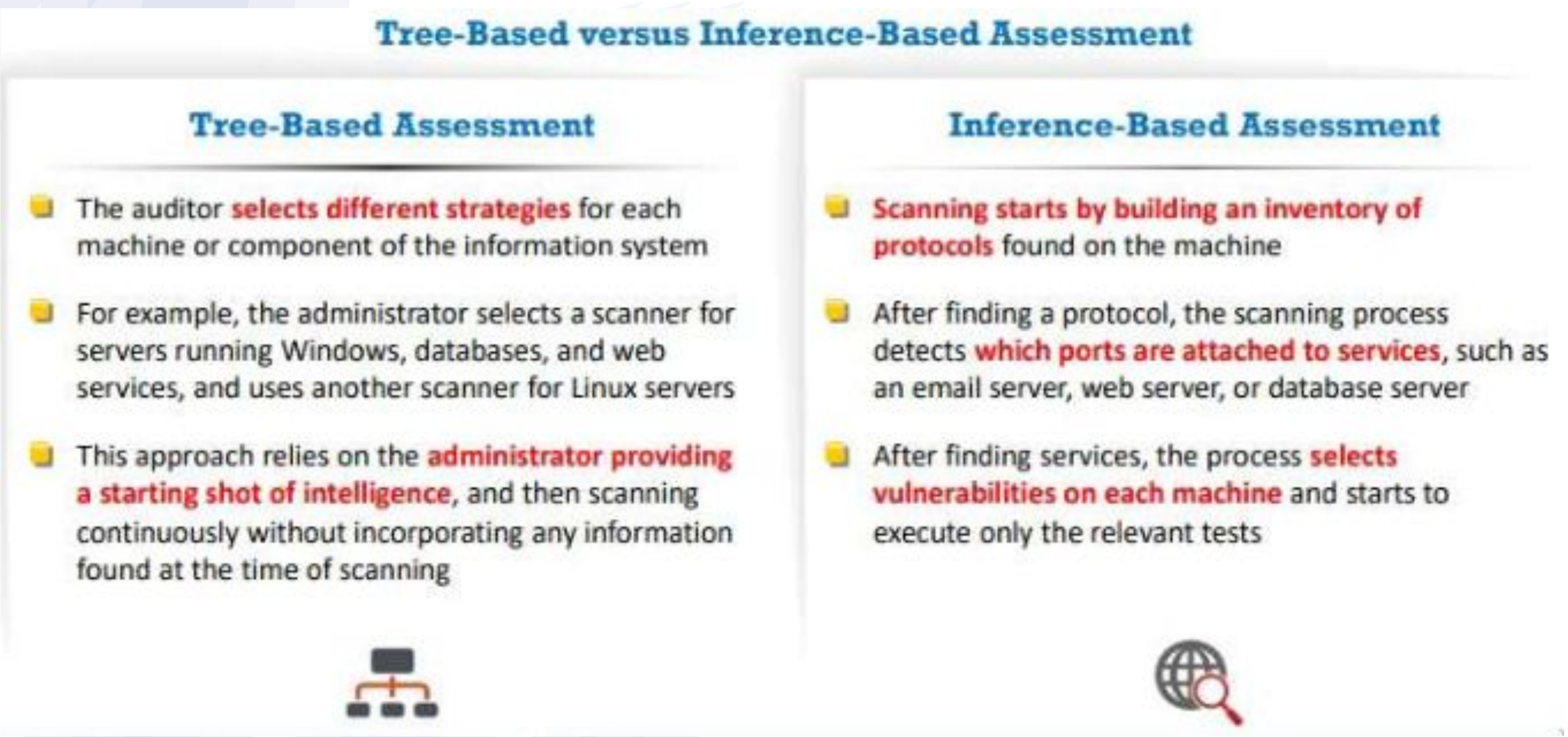
Product-Based Solutions

- Installed in the **organization's internal network**
- Installed in **private or non-routable space** or the Internet-addressable portion of an organization's network
- If installed in the private network or, in other words, behind the firewall, it cannot always **detect outside attacks**

Service-Based Solutions

- **Offered by third parties**, such as auditing or security consulting firms
- Some solutions are hosted **inside the network**, while others are hosted outside the network
- A drawback of this solution is that attackers can audit the **network from outside**

Cont’d



Tree-Based versus Inference-Based Assessment

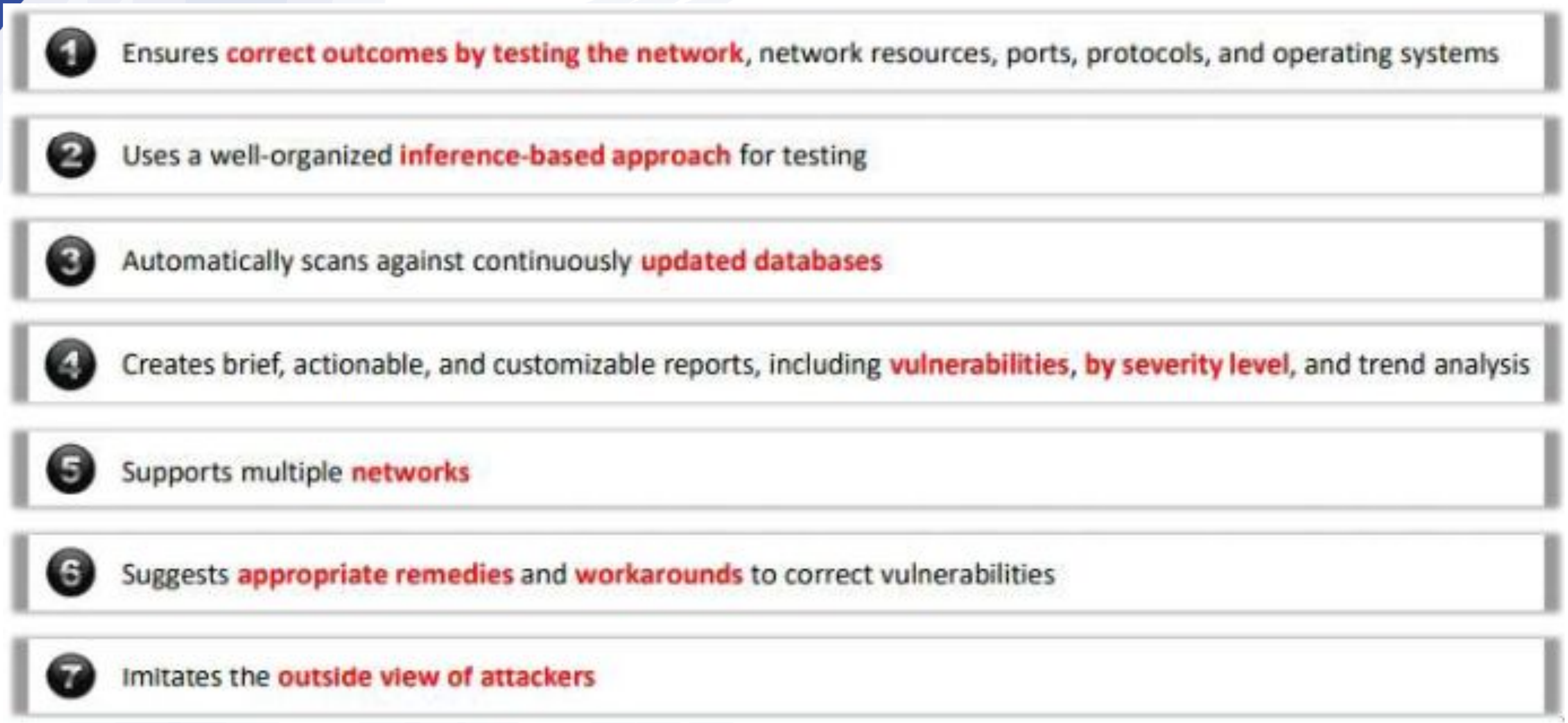
Tree-Based Assessment

- The auditor selects different strategies for each machine or component of the information system
- For example, the administrator selects a scanner for servers running Windows, databases, and web services, and uses another scanner for Linux servers
- This approach relies on the administrator providing a starting shot of intelligence, and then scanning continuously without incorporating any information found at the time of scanning

Inference-Based Assessment

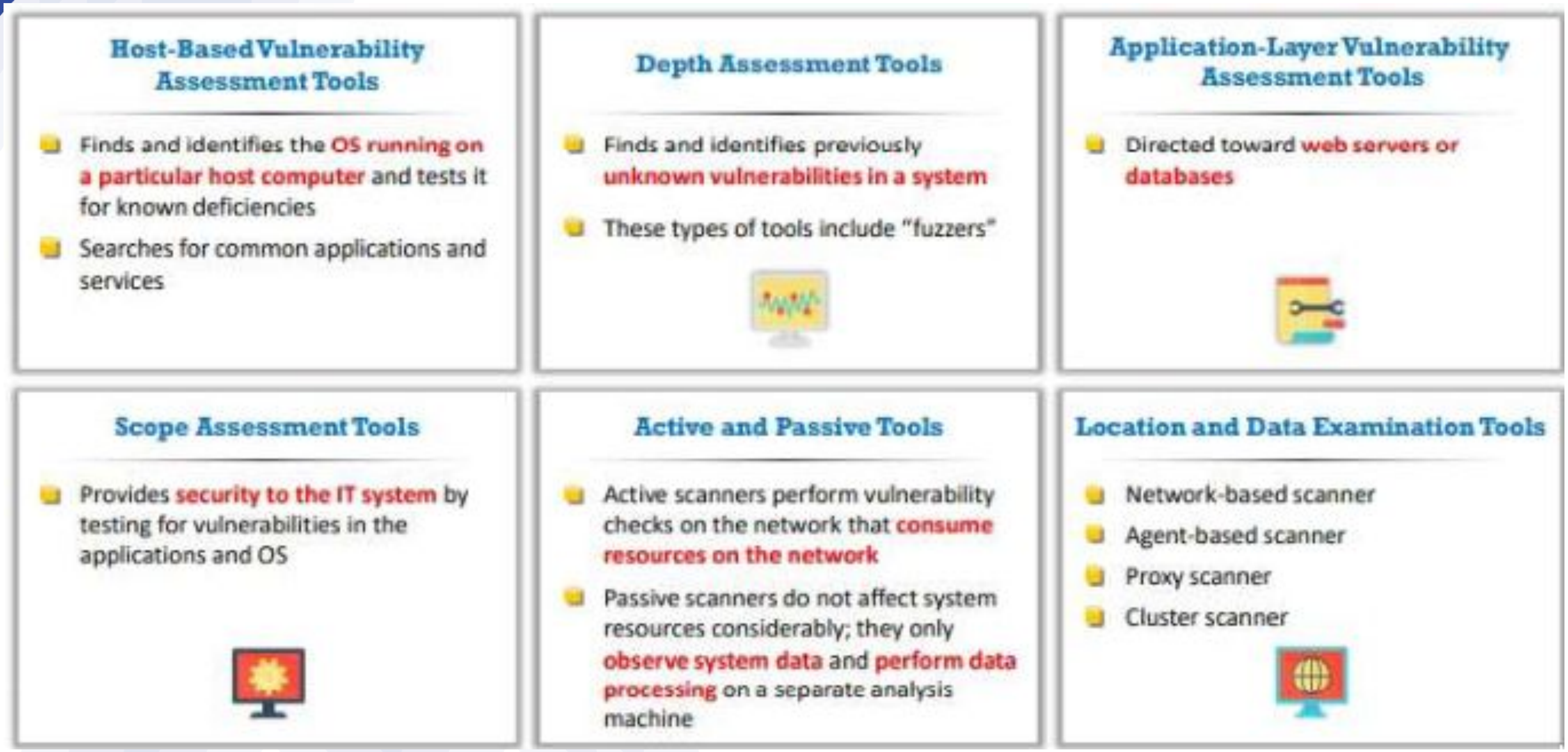
- Scanning starts by building an inventory of protocols found on the machine
- After finding a protocol, the scanning process detects which ports are attached to services, such as an email server, web server, or database server
- After finding services, the process selects vulnerabilities on each machine and starts to execute only the relevant tests

Characteristics of a good VA Solution



1. Ensures correct outcomes by testing the network, network resources, ports, protocols, and operating systems
2. Uses a well-organized inference-based approach for testing
3. Automatically scans against continuously updated databases
4. Creates brief, actionable, and customizable reports, including vulnerabilities, by severity level, and trend analysis
5. Supports multiple networks
6. Suggests appropriate remedies and workarounds to correct vulnerabilities
7. Imitates the outside view of attackers

Types of VA tools



Host-Based Vulnerability Assessment Tools

- Finds and identifies the **OS running on a particular host computer** and tests it for known deficiencies
- Searches for common applications and services

Depth Assessment Tools

- Finds and identifies previously **unknown vulnerabilities in a system**
- These types of tools include "fuzzers"

Application-Layer Vulnerability Assessment Tools

- Directed toward **web servers or databases**

Scope Assessment Tools

- Provides **security to the IT system** by testing for vulnerabilities in the applications and OS

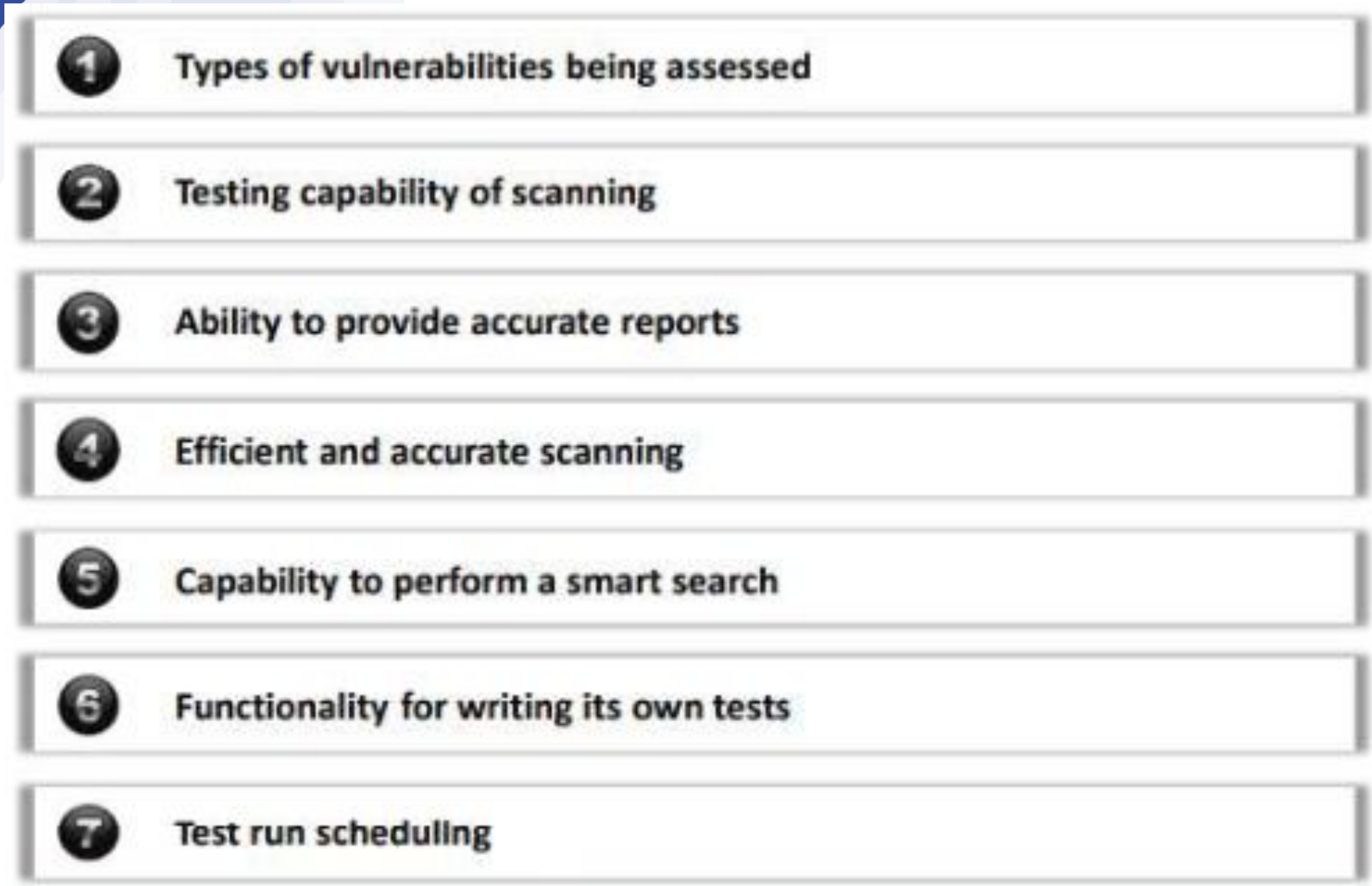
Active and Passive Tools

- Active scanners perform vulnerability checks on the network that **consume resources on the network**
- Passive scanners do not affect system resources considerably; they only **observe system data** and **perform data processing** on a separate analysis machine

Location and Data Examination Tools

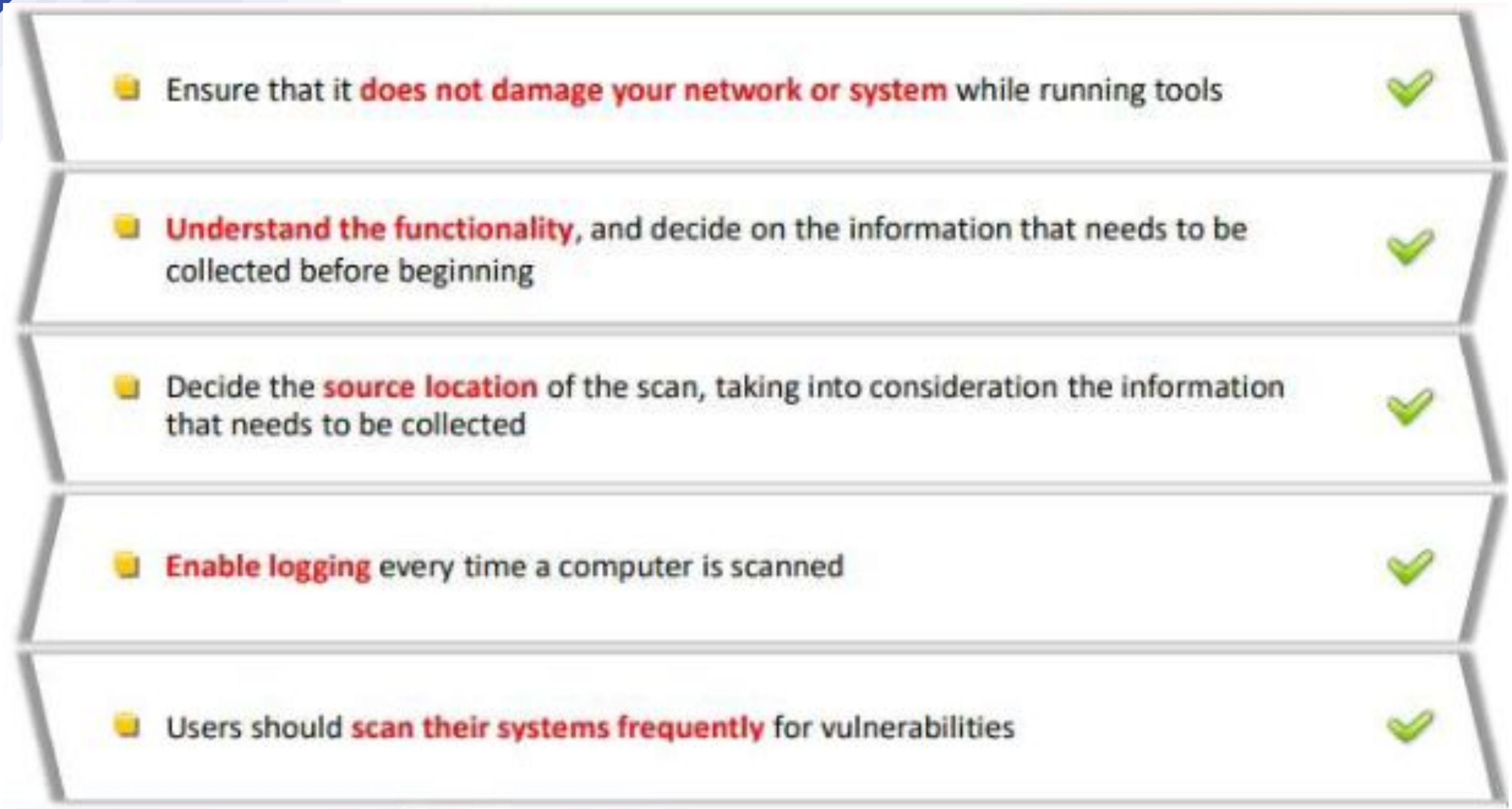
- Network-based scanner
- Agent-based scanner
- Proxy scanner
- Cluster scanner

What determines a good Vulnerability Assessment tool?



1. Types of vulnerabilities being assessed
2. Testing capability of scanning
3. Ability to provide accurate reports
4. Efficient and accurate scanning
5. Capability to perform a smart search
6. Functionality for writing its own tests
7. Test run scheduling

Best Practices for selecting a good VA tool



- Ensure that it **does not damage your network or system** while running tools ✓
- **Understand the functionality**, and decide on the information that needs to be collected before beginning ✓
- Decide the **source location** of the scan, taking into consideration the information that needs to be collected ✓
- **Enable logging** every time a computer is scanned ✓
- Users should **scan their systems frequently** for vulnerabilities ✓

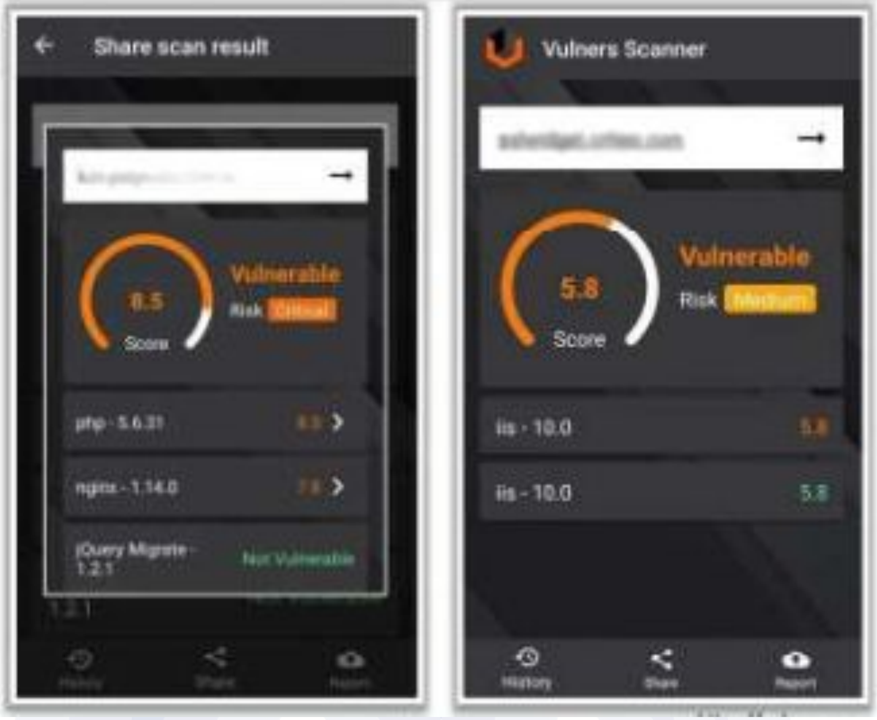
VA Tools

- OpenVAS by greenbone security
- Nikto
- GFI Languard
- Qualys
- Acunetix
- Nexpose
- Nessus

VA tools for Mobile

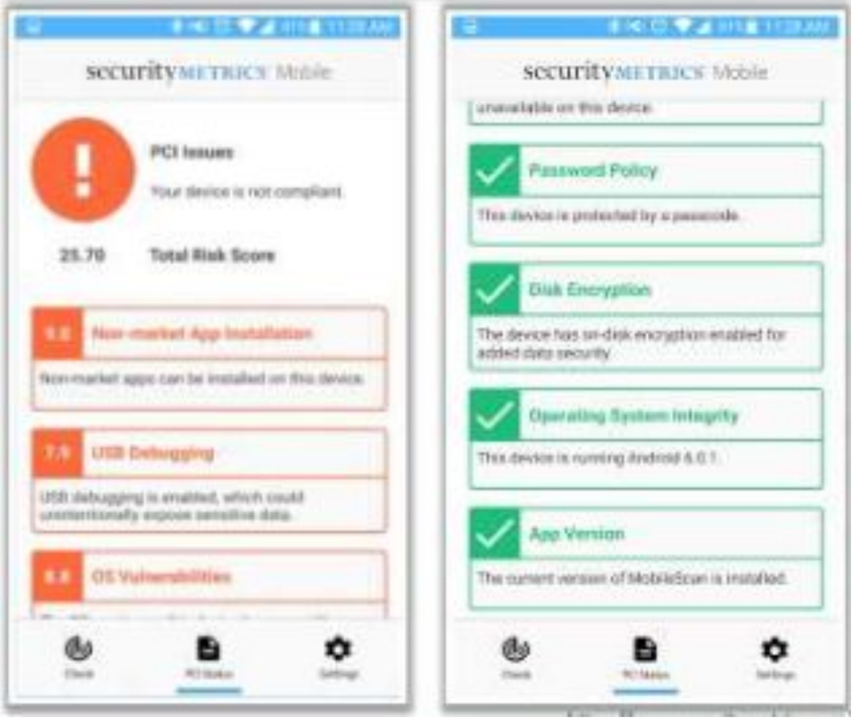
Vulners Scanner

An android app that **performs passive vulnerability detection** based on the fingerprint of the software version



Security Metrics Mobile

An android app that **complies with PCI SSC** guidelines to **generate a scan report**


securityMETRICS Mobile

PCI Issues

Your device is not compliant.

25.70 Total Risk Score

Non-market App Installation

Non-market apps can be installed on this device.

USB Debugging

USB debugging is enabled, which could unintentionally expose sensitive data.

OS Vulnerabilities

securityMETRICS Mobile

unavailable on this device.

Password Policy

This device is protected by a passcode.

Disk Encryption

The device has on-disk encryption enabled for added data security.

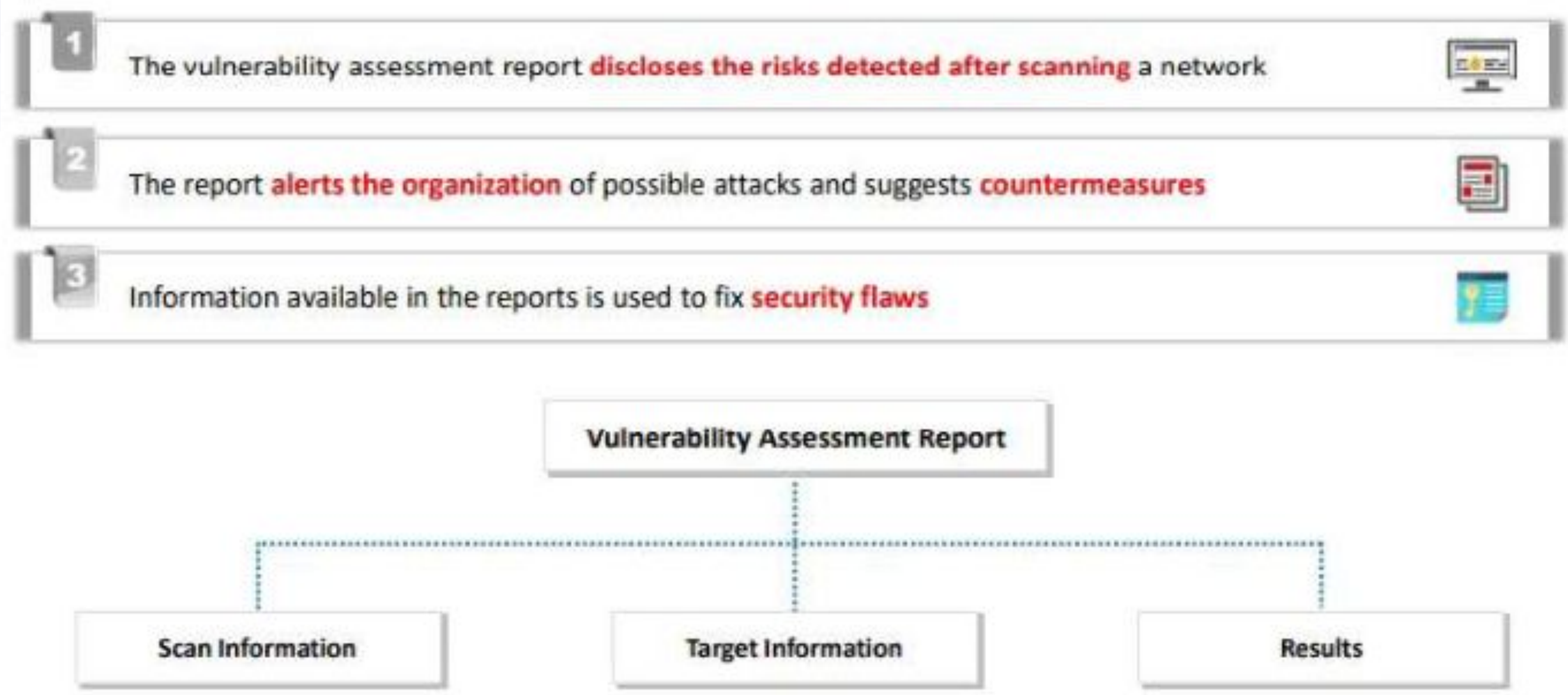
Operating System Integrity

This device is running Android 6.0.1.

App Version

The current version of MobileScan is installed.

Vulnerability Assessments Reports



1. The vulnerability assessment report **discloses the risks detected after scanning** a network

2. The report **alerts the organization** of possible attacks and suggests **countermeasures**

3. Information available in the reports is used to fix **security flaws**

Vulnerability Assessment Report

- **Scan Information**
- **Target Information**
- **Results**

Cont'd

The Vulnerability report must include but not limited to the following:

- Vulnerability's name and its mapped CVE ID.
- Date of discovery.
- CVE score.
- Description.
- Impact.
- Details of the affected system.
- PoC if possible.

Sample vulnerability report

[TAISOC SECURITY ADVISORY REPORT]

Strathmore UNIVERSITY

Thank you!

Any Questions?