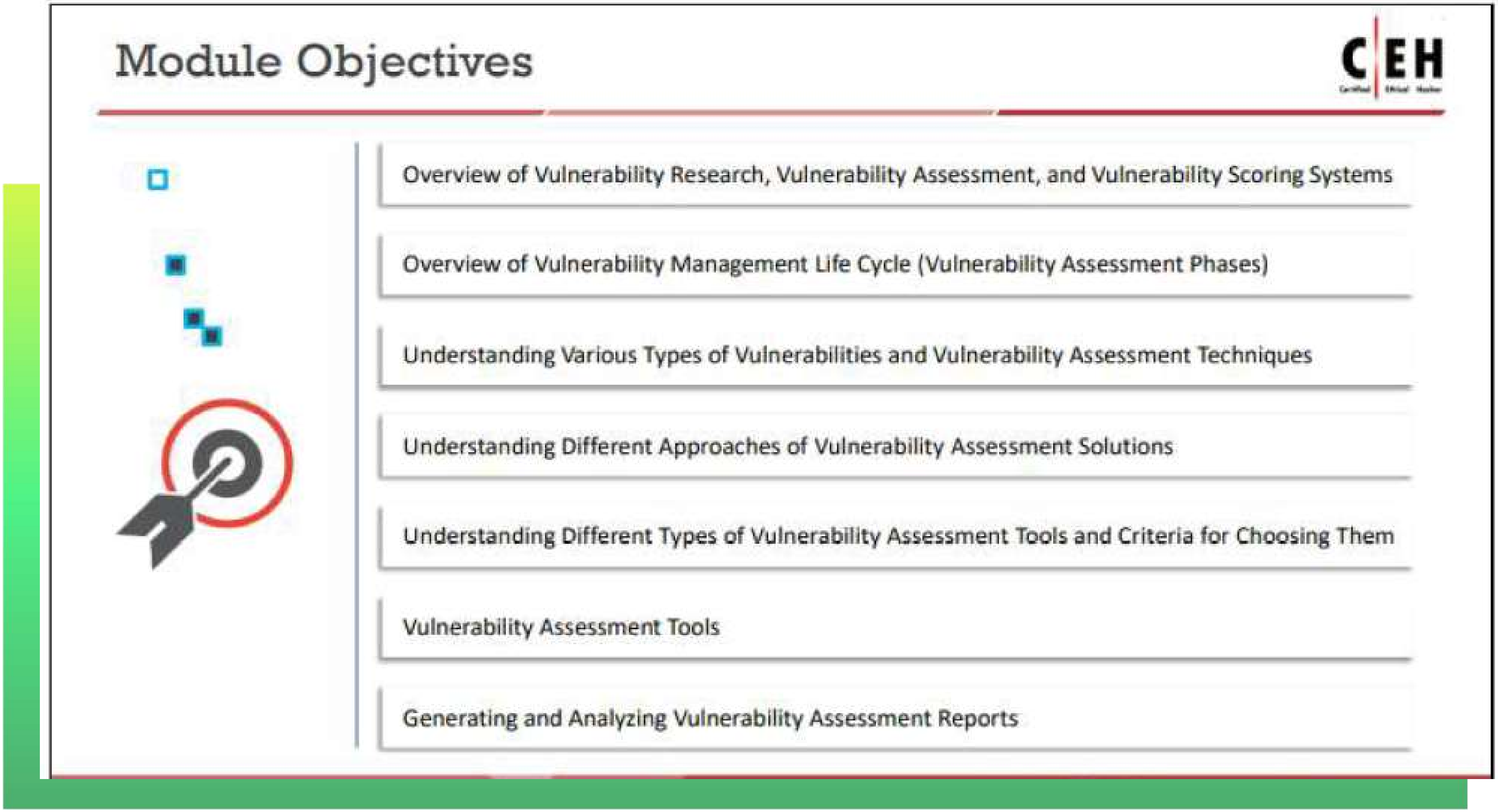
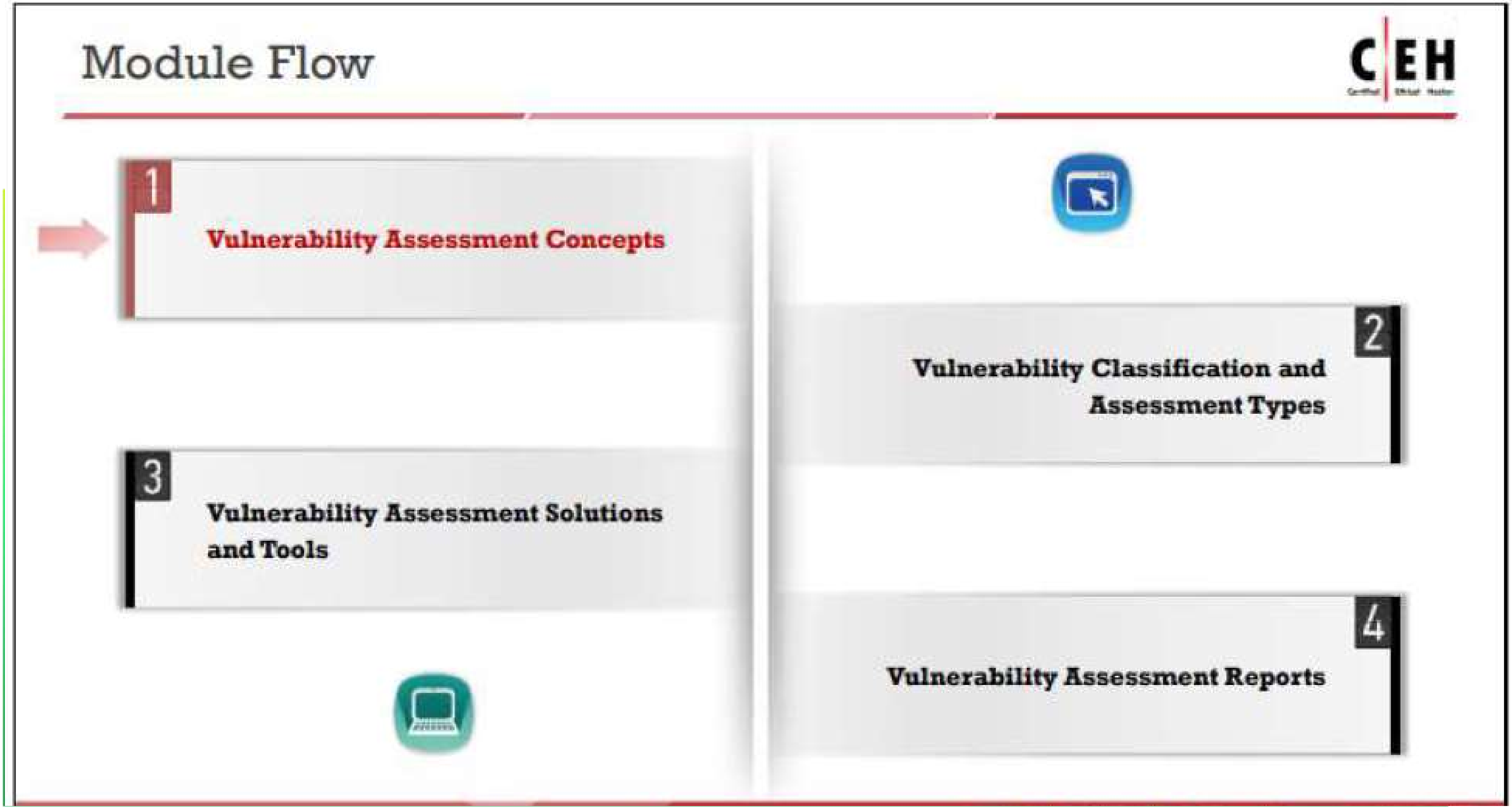
VULNERABILITY ANALYSIS



Module Objectives

C|EH
Certified Ethical Hacker

- Overview of Vulnerability Research, Vulnerability Assessment, and Vulnerability Scoring Systems
- Overview of Vulnerability Management Life Cycle (Vulnerability Assessment Phases)
- Understanding Various Types of Vulnerabilities and Vulnerability Assessment Techniques
- Understanding Different Approaches of Vulnerability Assessment Solutions
- Understanding Different Types of Vulnerability Assessment Tools and Criteria for Choosing Them
- Vulnerability Assessment Tools
- Generating and Analyzing Vulnerability Assessment Reports



Module Flow

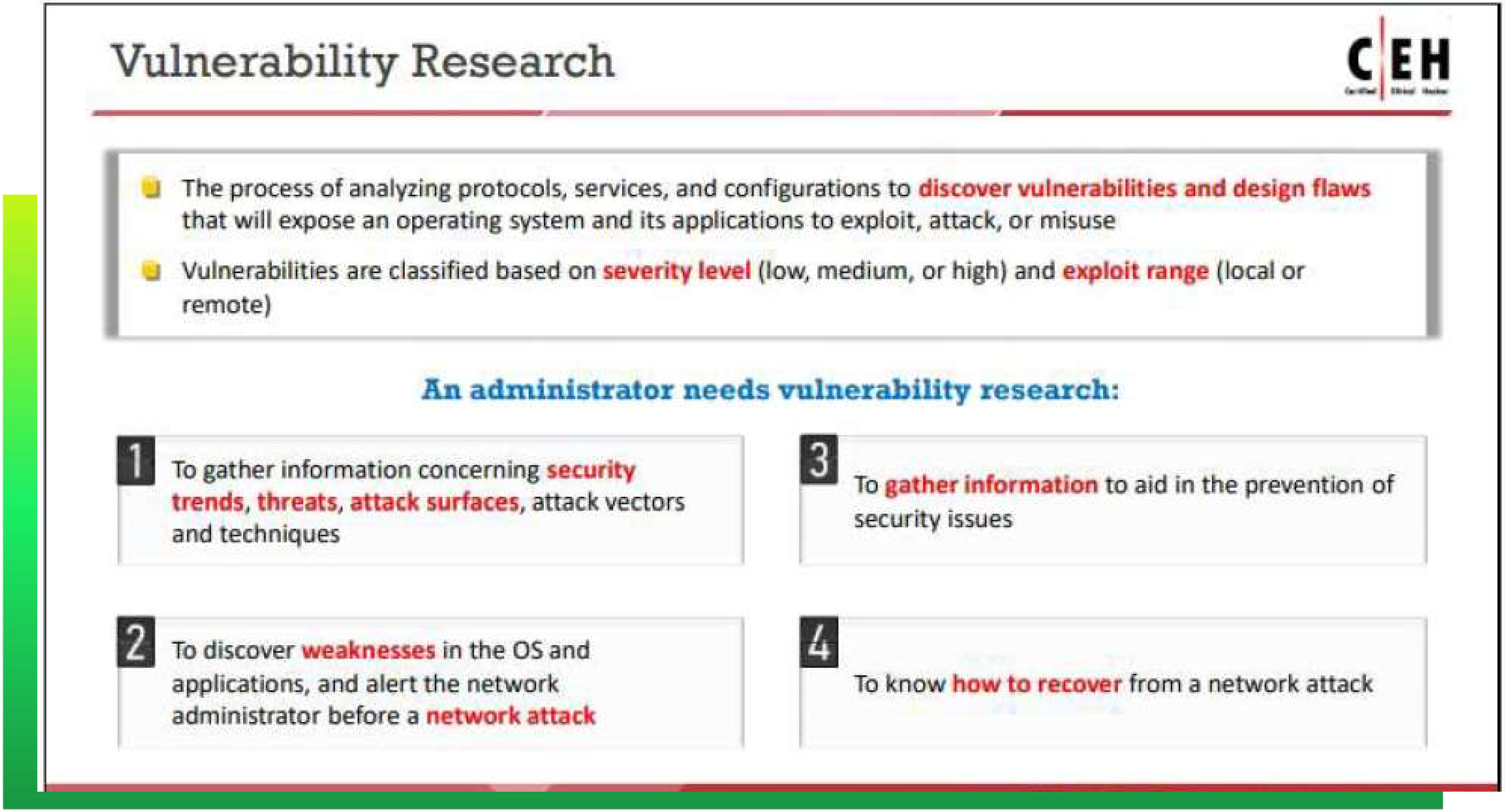
CEH

1 **Vulnerability Assessment Concepts**

2 **Vulnerability Classification and Assessment Types**

3 **Vulnerability Assessment Solutions and Tools**

4 **Vulnerability Assessment Reports**

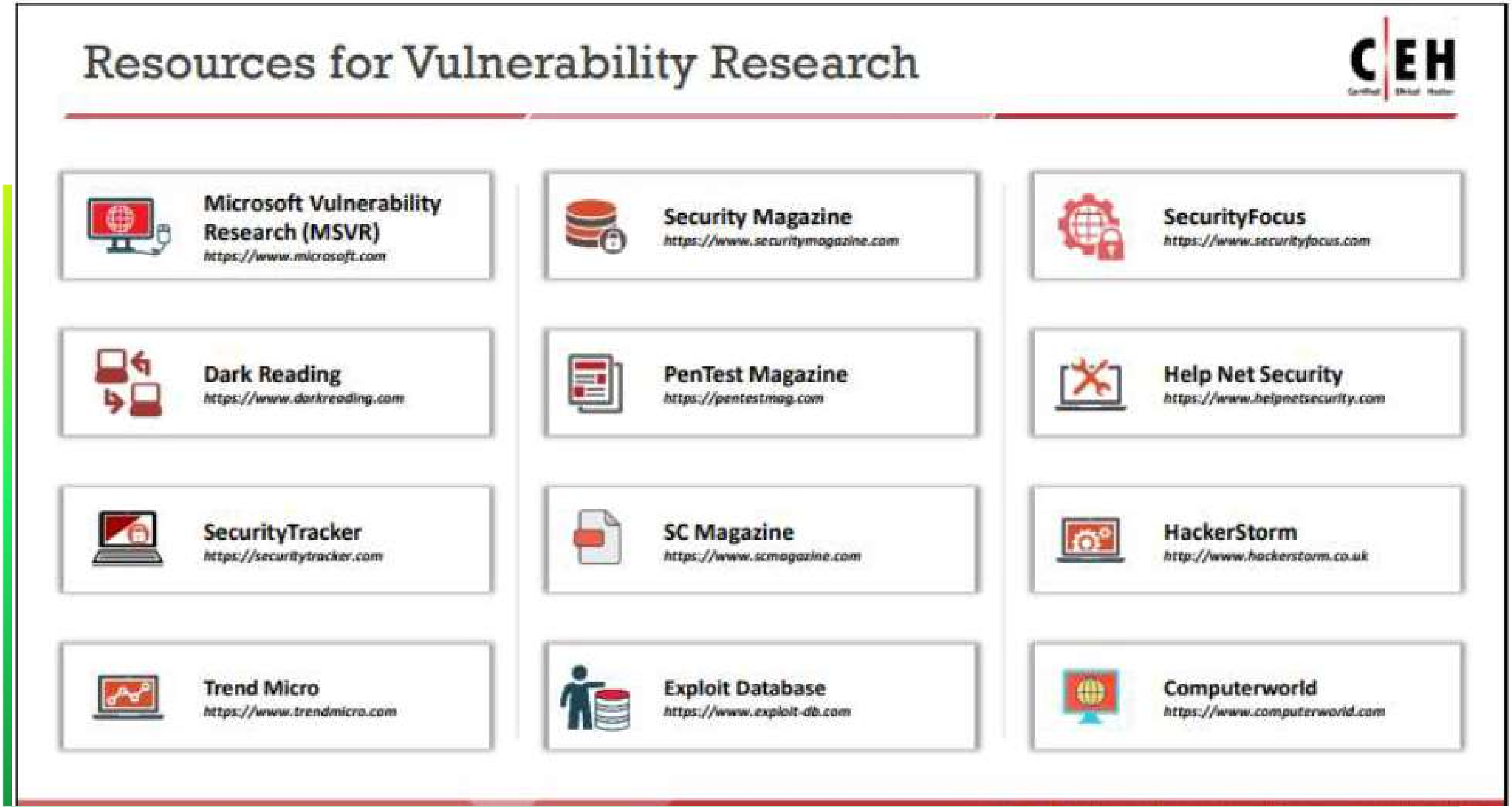


Vulnerability Research

- 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



Resources for Vulnerability Research

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

Dark Reading
https://www.darkreading.com

SecurityTracker
https://securitytracker.com

Trend Micro
https://www.trendmicro.com

Security Magazine
https://www.securitymagazine.com

PenTest Magazine
https://pentestmag.com

SC Magazine
https://www.scmagazine.com

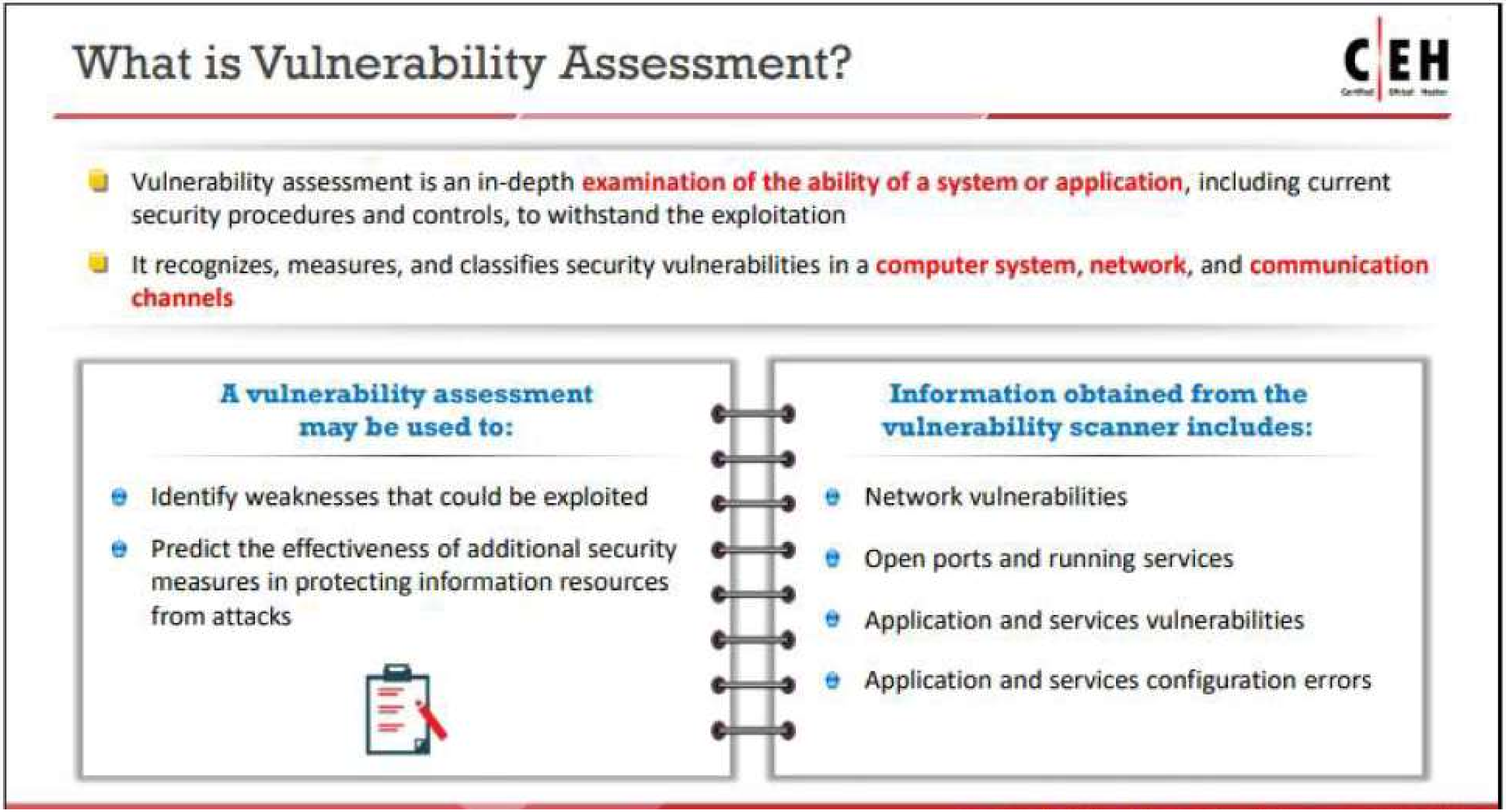
Exploit Database
https://www.exploit-db.com

SecurityFocus
https://www.securityfocus.com

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

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

Computerworld
https://www.computerworld.com



What is Vulnerability Assessment?

CEH

- 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

Vulnerability Scoring Systems and Databases

C|EH Certified Ethical Hacker

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**

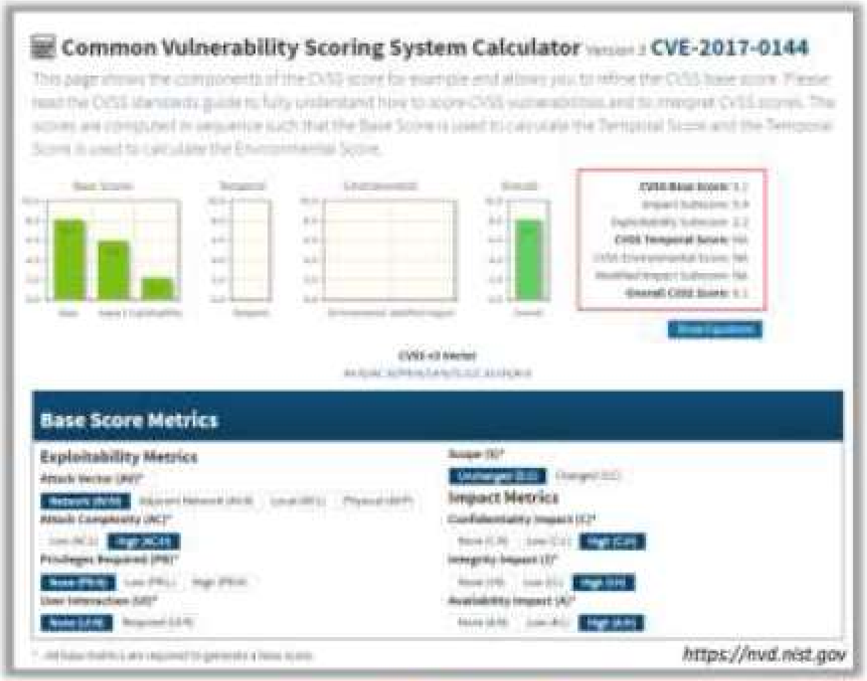
CVSS v3.0 Ratings

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: 8.1
Impact Subscore: 5.9
Exploitability Subscore: 2.2
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 8.1

CVSS v3 Vector
AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

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)

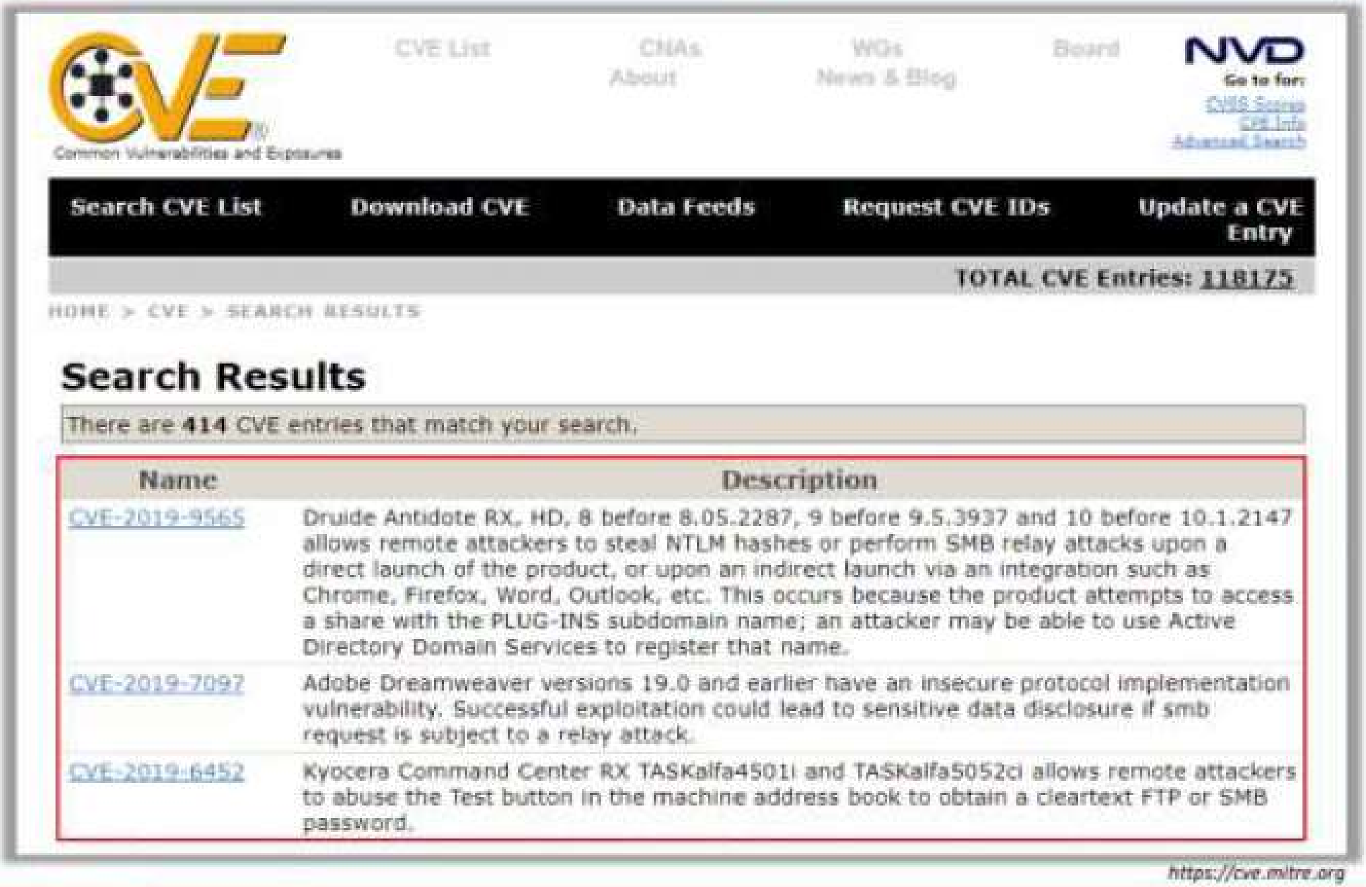
* - All base metrics are required to generate a base score.

https://nvd.nist.gov

Vulnerability Scoring Systems and Databases (Cont'd)

Common Vulnerabilities and Exposures (CVE)

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



Search Results

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

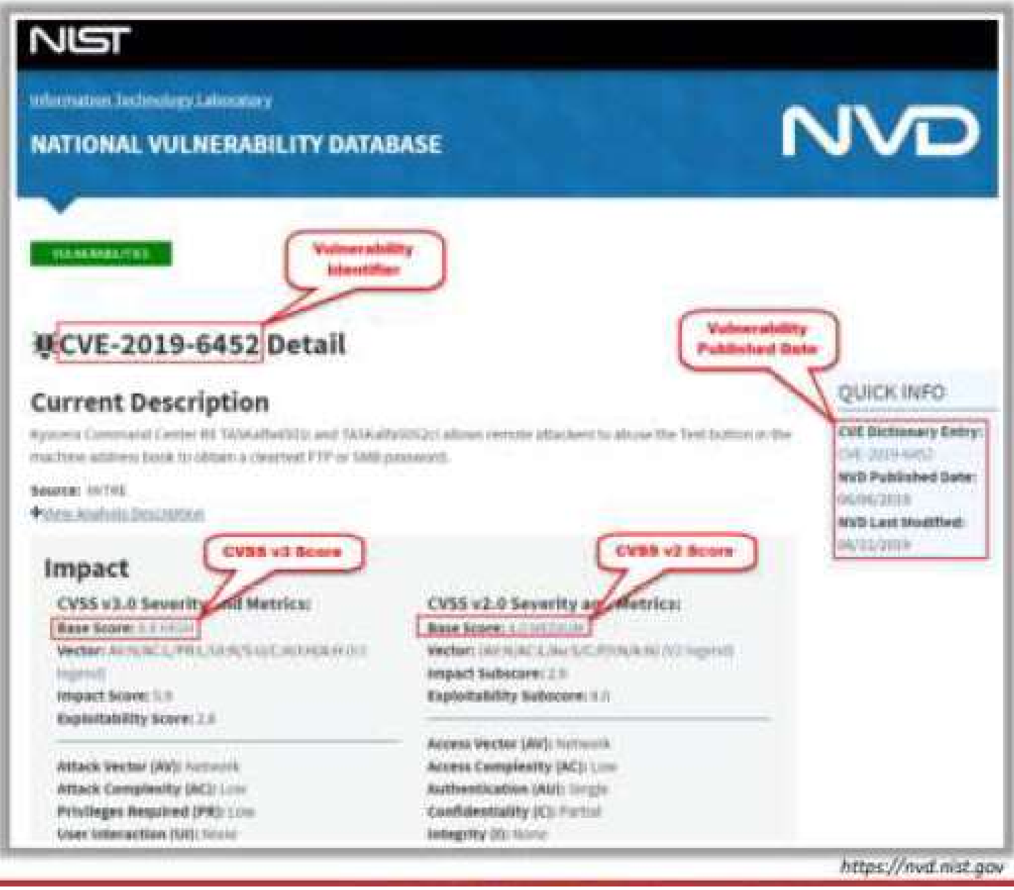
Name	Description
CVE-2019-9565	Druide Antidote RX, HD, 8 before 8.05.2287, 9 before 9.5.3937 and 10 before 10.1.2147 allows remote attackers to steal NTLM hashes or perform SMB relay attacks upon a direct launch of the product, or upon an indirect launch via an integration such as Chrome, Firefox, Word, 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

Vulnerability Scoring Systems and Databases (Cont'd)

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



NIST
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE
NVD
VULNERABILITIES
Vulnerability Identifier
Vulnerability Published Date
CVSS v3 Score
CVSS v2 Score

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

QUICK INFO

CVE Dictionary Entry: CVE-2019-6452

NVD Published Date: 06/06/2019

NVD Last Modified: 06/11/2019

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

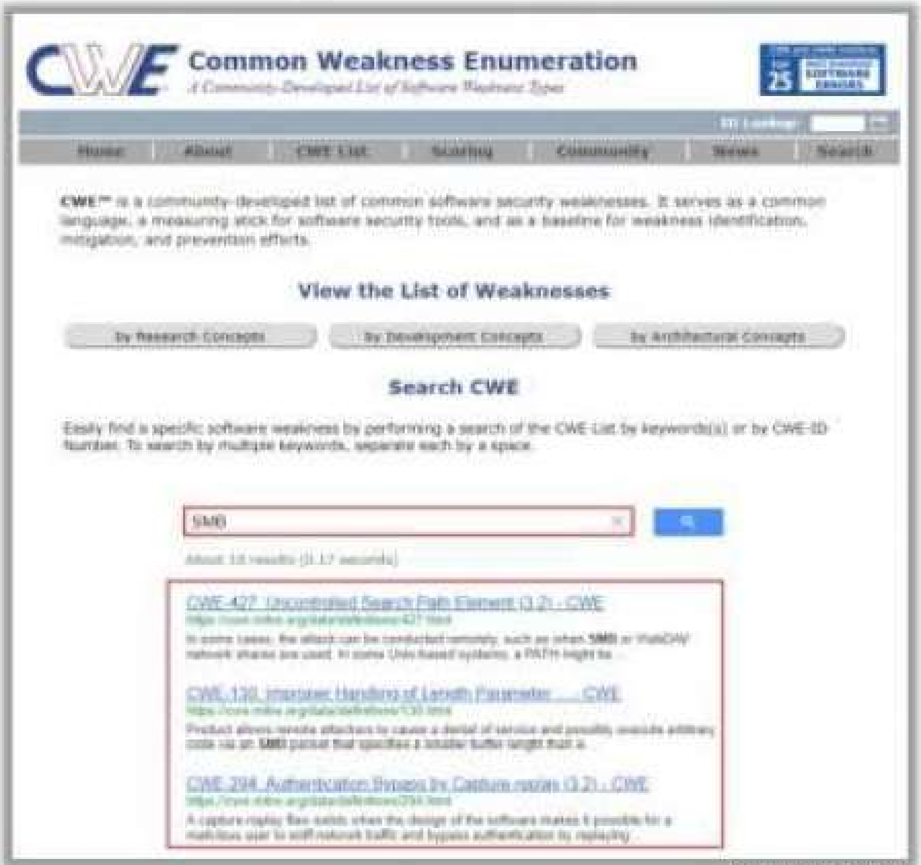
Integrity (I): None

https://nvd.nist.gov

Vulnerability Scoring Systems and Databases (Cont'd)

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**


Common Weakness Enumeration
A Community-Developed List of Software Weakness Types
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

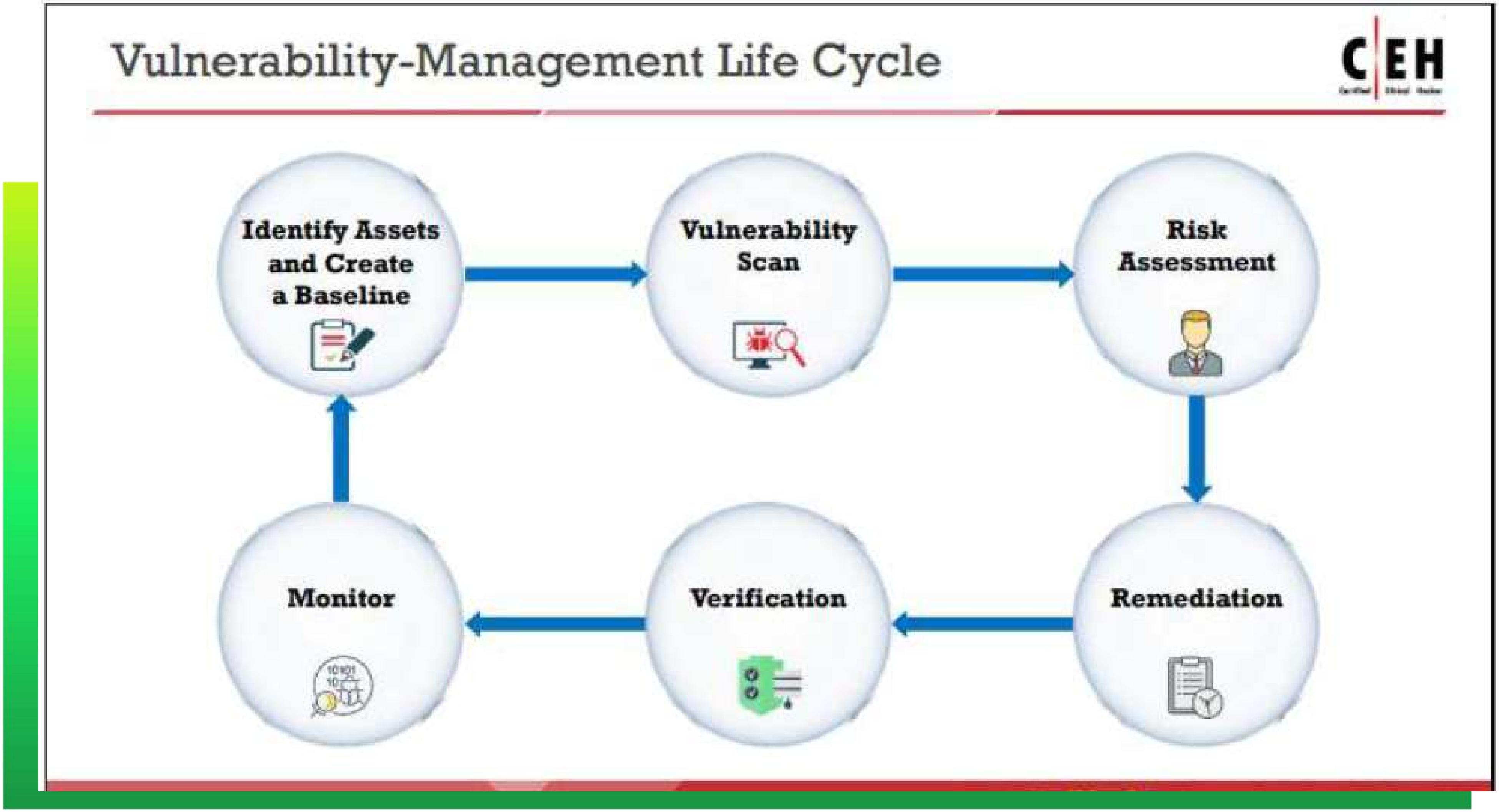
About 18 results (0.17 seconds)

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 a ...

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 ...

https://cwe.mitre.org



Vulnerability-Management Life Cycle

Identify Assets and Create a Baseline

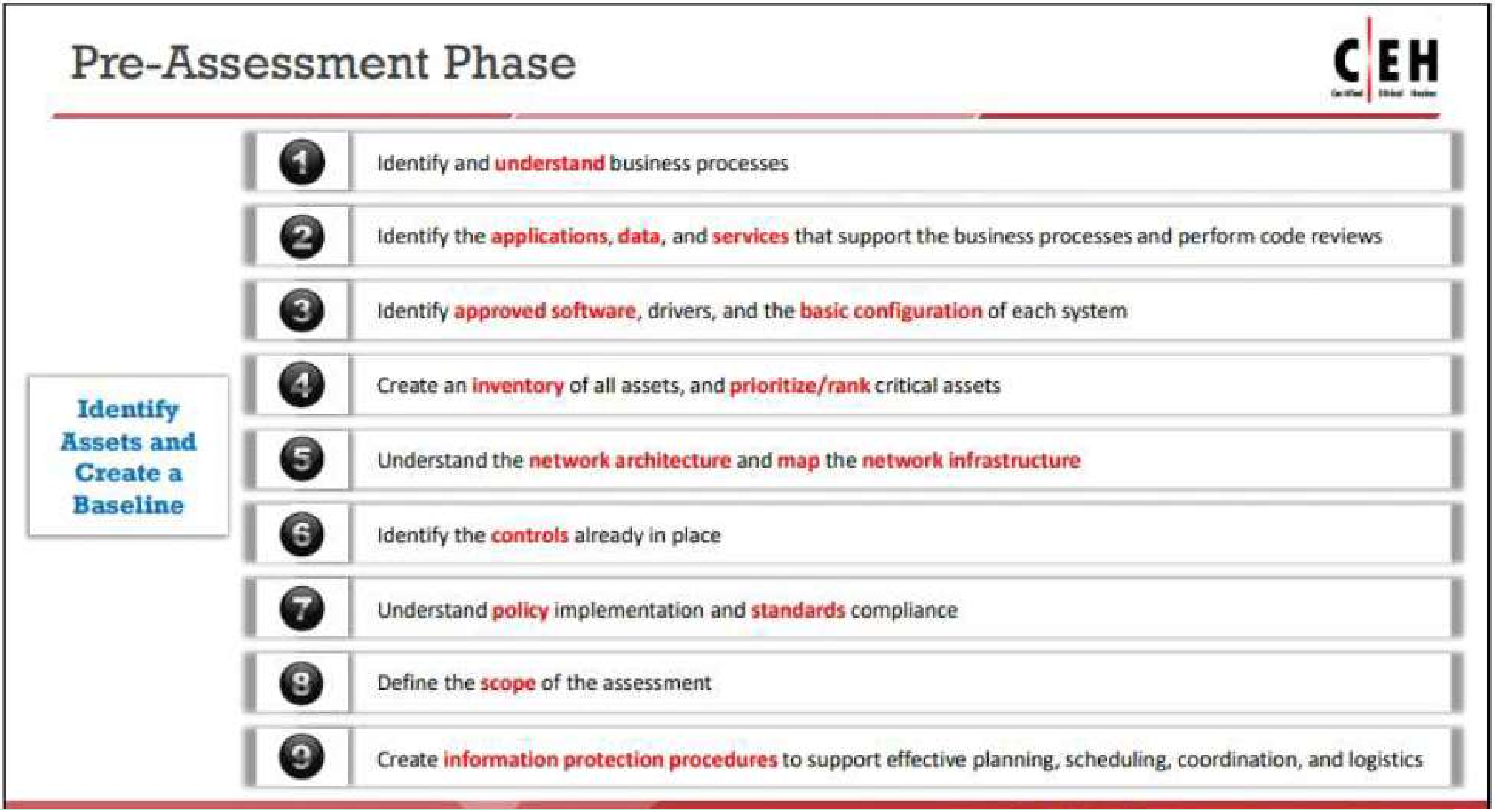
Vulnerability Scan

Risk Assessment

Remediation

Verification

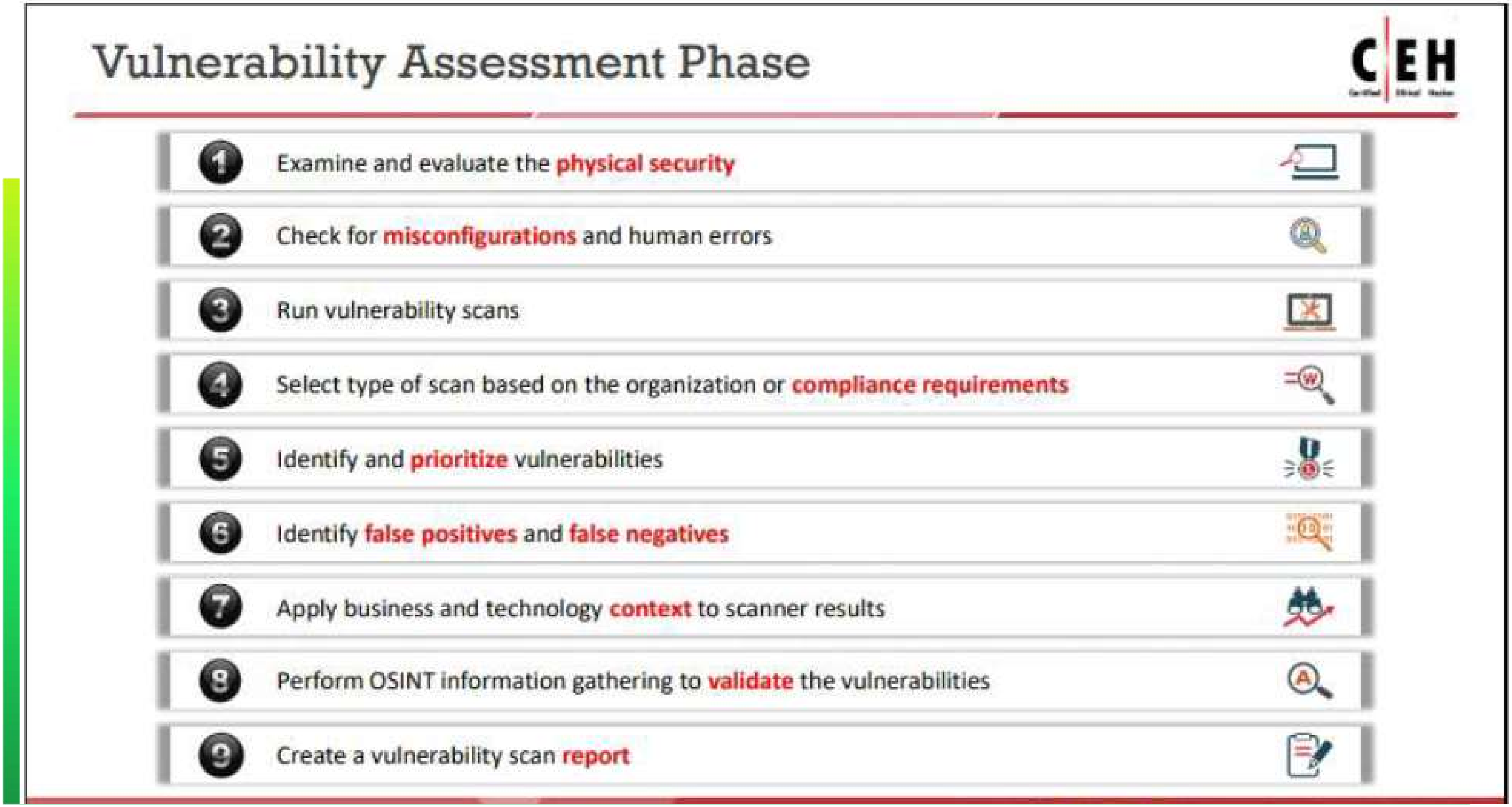
Monitor



Pre-Assessment Phase

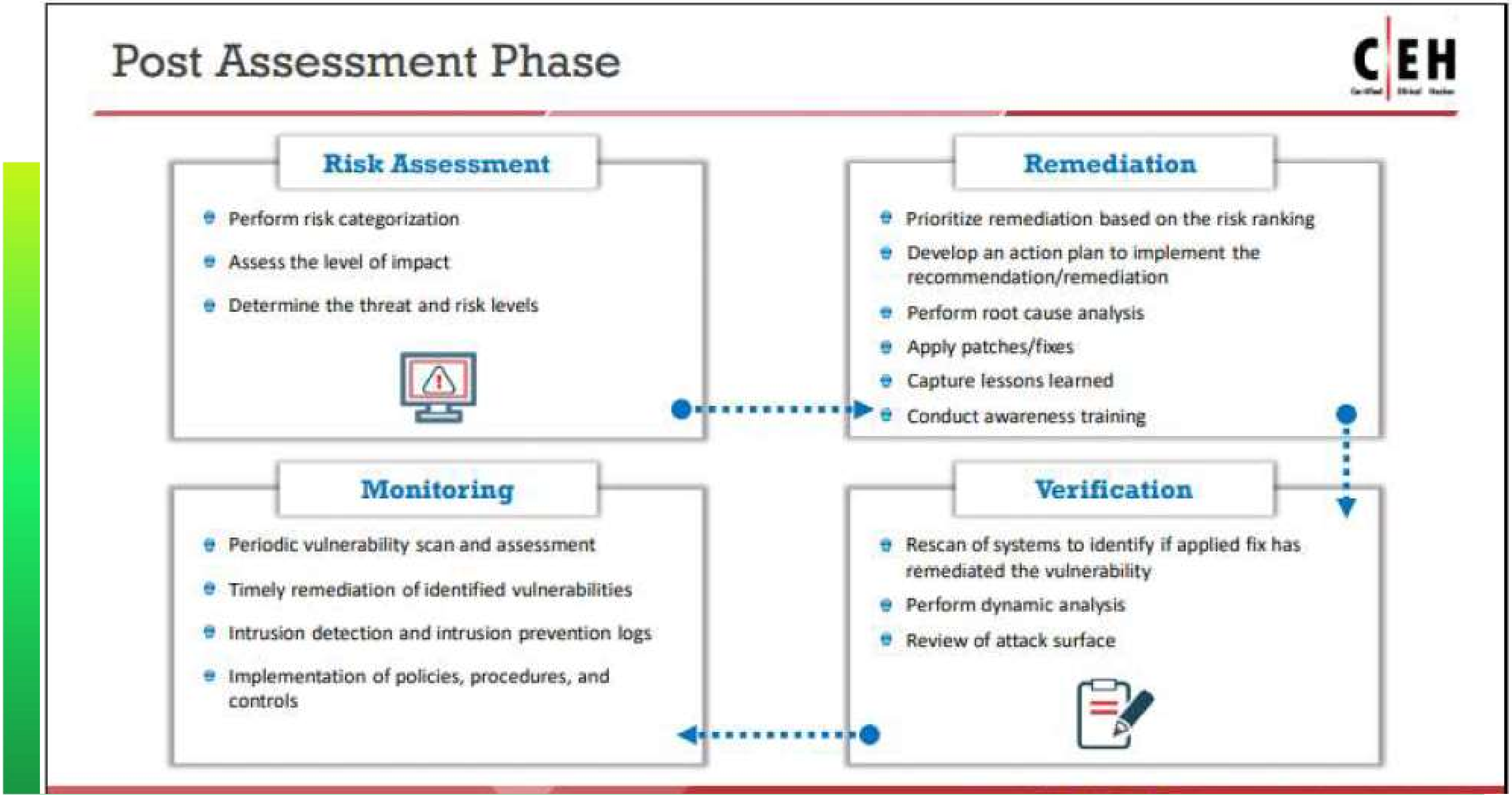
Identify Assets and Create a Baseline

1. Identify and **understand** business processes
2. Identify the **applications**, **data**, and **services** that support the business processes and perform code reviews
3. Identify **approved software**, drivers, and the **basic configuration** of each system
4. Create an **inventory** of all assets, and **prioritize/rank** critical assets
5. Understand the **network architecture** and **map** the **network infrastructure**
6. Identify the **controls** already in place
7. Understand **policy** implementation and **standards** compliance
8. Define the **scope** of the assessment
9. Create **information protection procedures** to support effective planning, scheduling, coordination, and logistics



Vulnerability Assessment Phase

1. Examine and evaluate the **physical security**
2. Check for **misconfigurations** and human errors
3. Run vulnerability scans
4. Select type of scan based on the organization or **compliance requirements**
5. Identify and **prioritize** vulnerabilities
6. Identify **false positives** and **false negatives**
7. Apply business and technology **context** to scanner results
8. Perform OSINT information gathering to **validate** the vulnerabilities
9. Create a vulnerability scan **report**



Post Assessment Phase

Risk Assessment

- Perform risk categorization
- Assess the level of impact
- Determine the threat and risk levels

Remediation

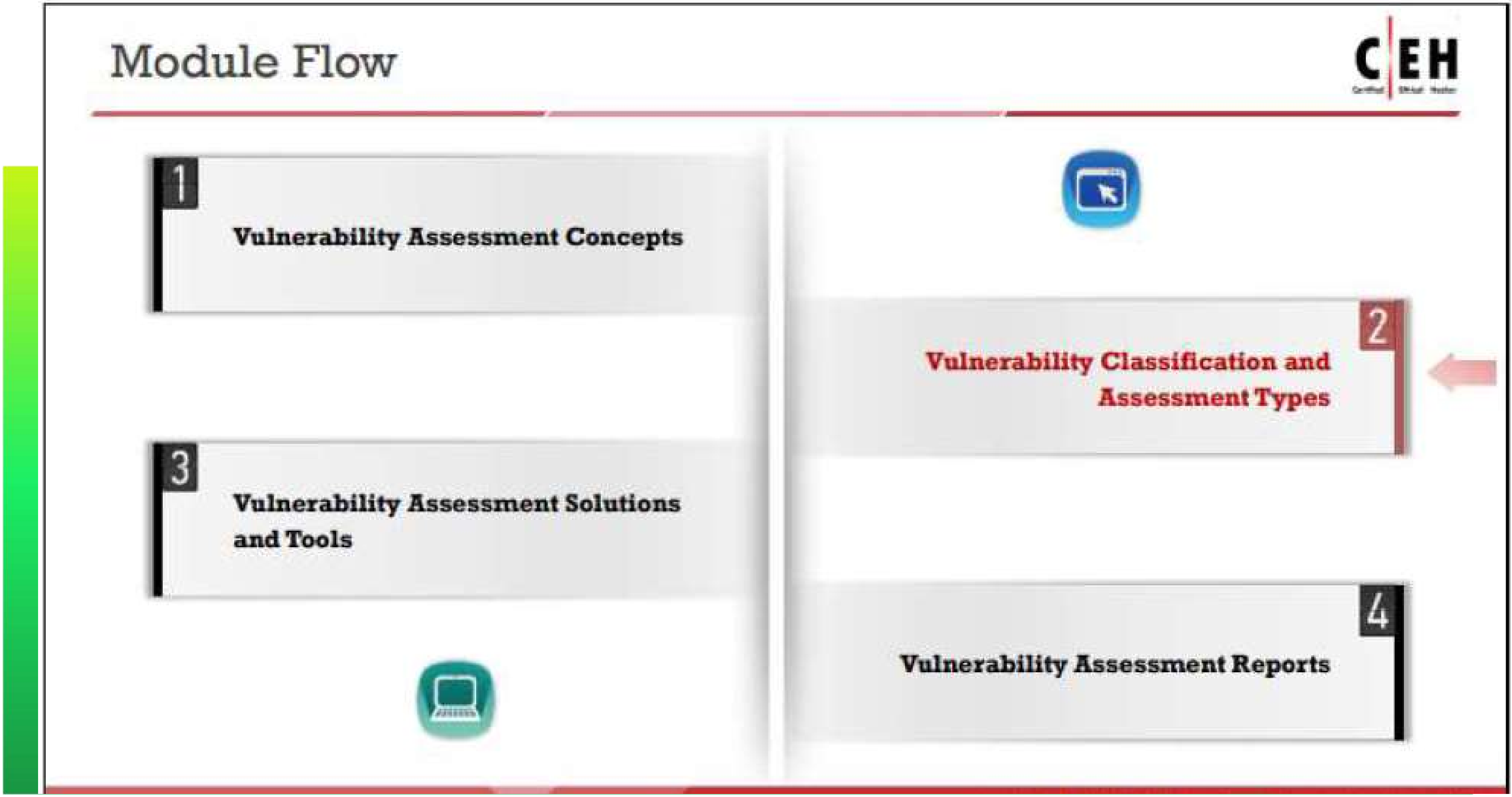
- Prioritize remediation based on the risk ranking
- Develop an action plan to implement the recommendation/remediation
- Perform root cause analysis
- Apply patches/fixes
- Capture lessons learned
- Conduct awareness training

Monitoring

- Periodic vulnerability scan and assessment
- Timely remediation of identified vulnerabilities
- Intrusion detection and intrusion prevention logs
- Implementation of policies, procedures, and controls

Verification

- Rescan of systems to identify if applied fix has remediated the vulnerability
- Perform dynamic analysis
- Review of attack surface



Module Flow

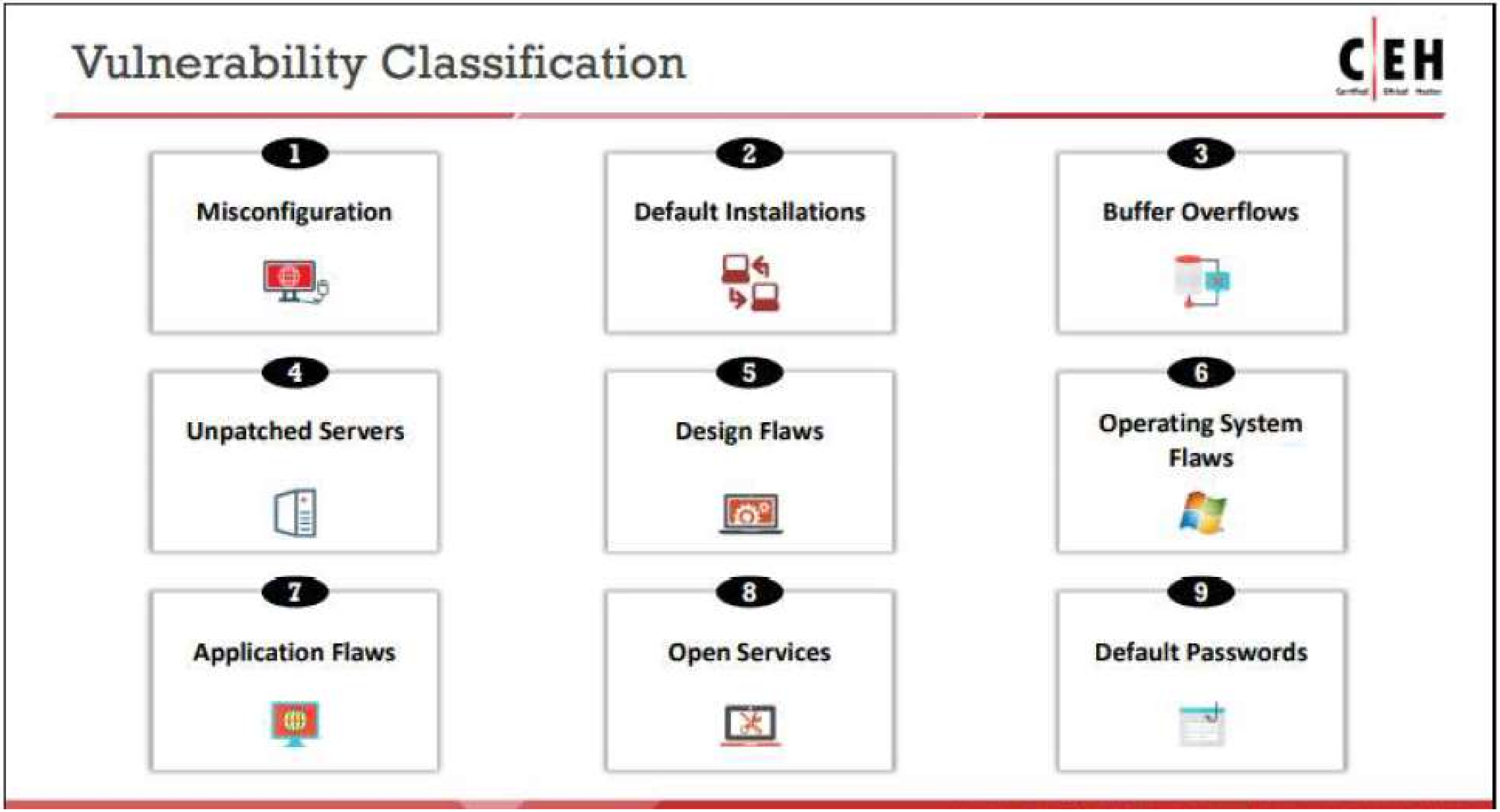
C|EH Certified Ethical Hacker

1 Vulnerability Assessment Concepts

2 Vulnerability Classification and Assessment Types

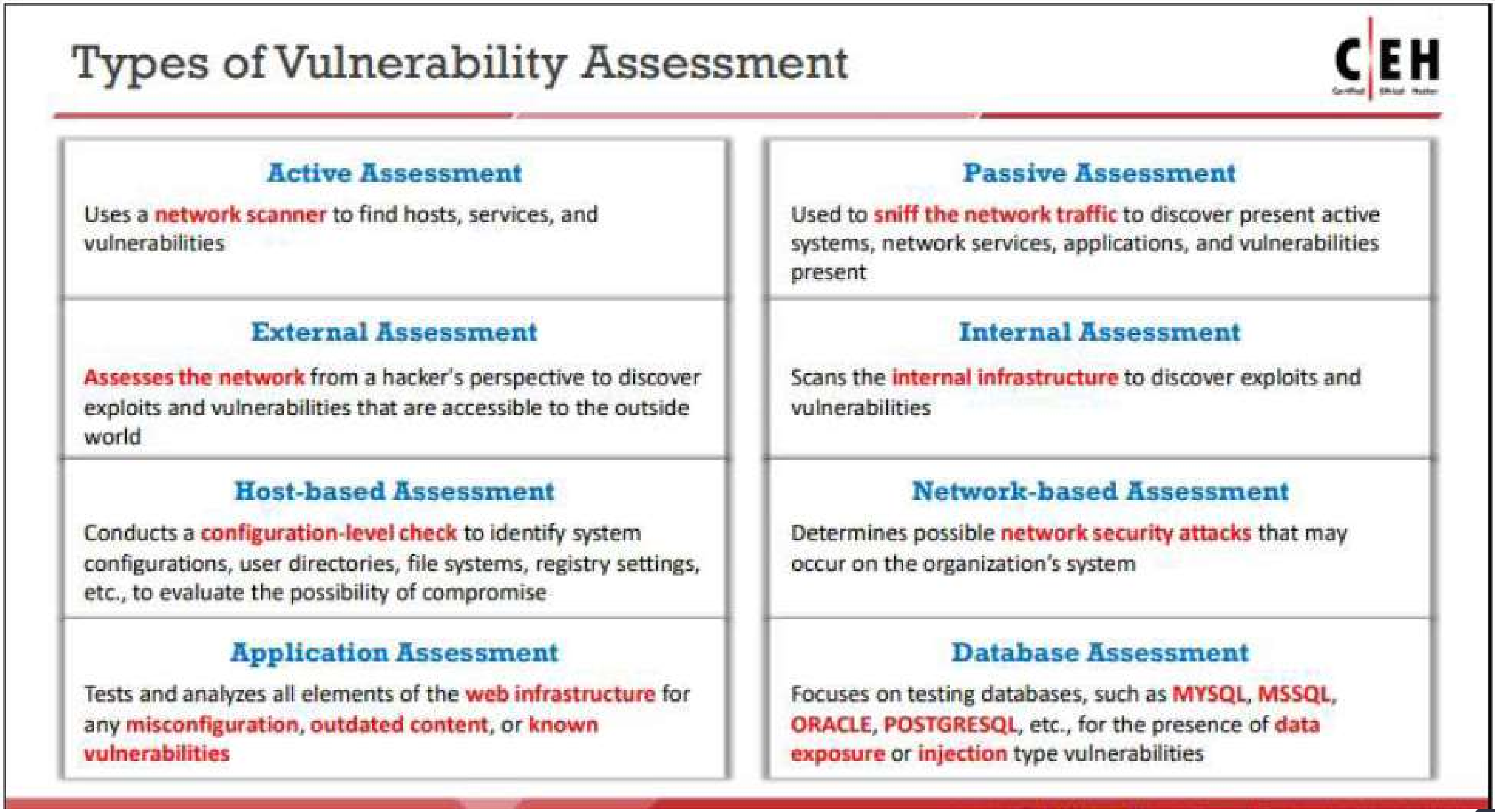
3 Vulnerability Assessment Solutions and Tools

4 Vulnerability Assessment Reports



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

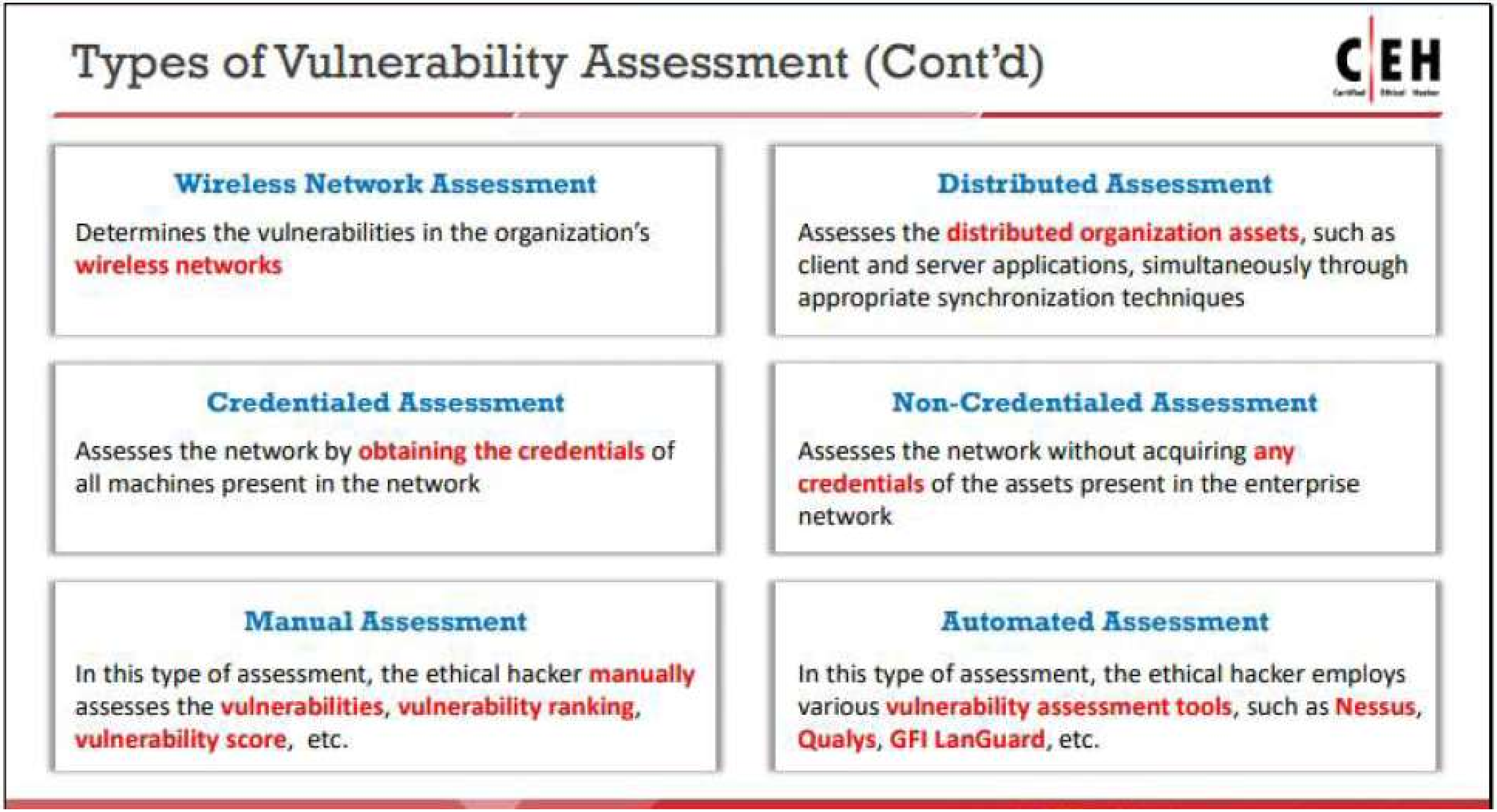
Determines possible **network security attacks** that may occur on the organization's system

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



Types of Vulnerability Assessment (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

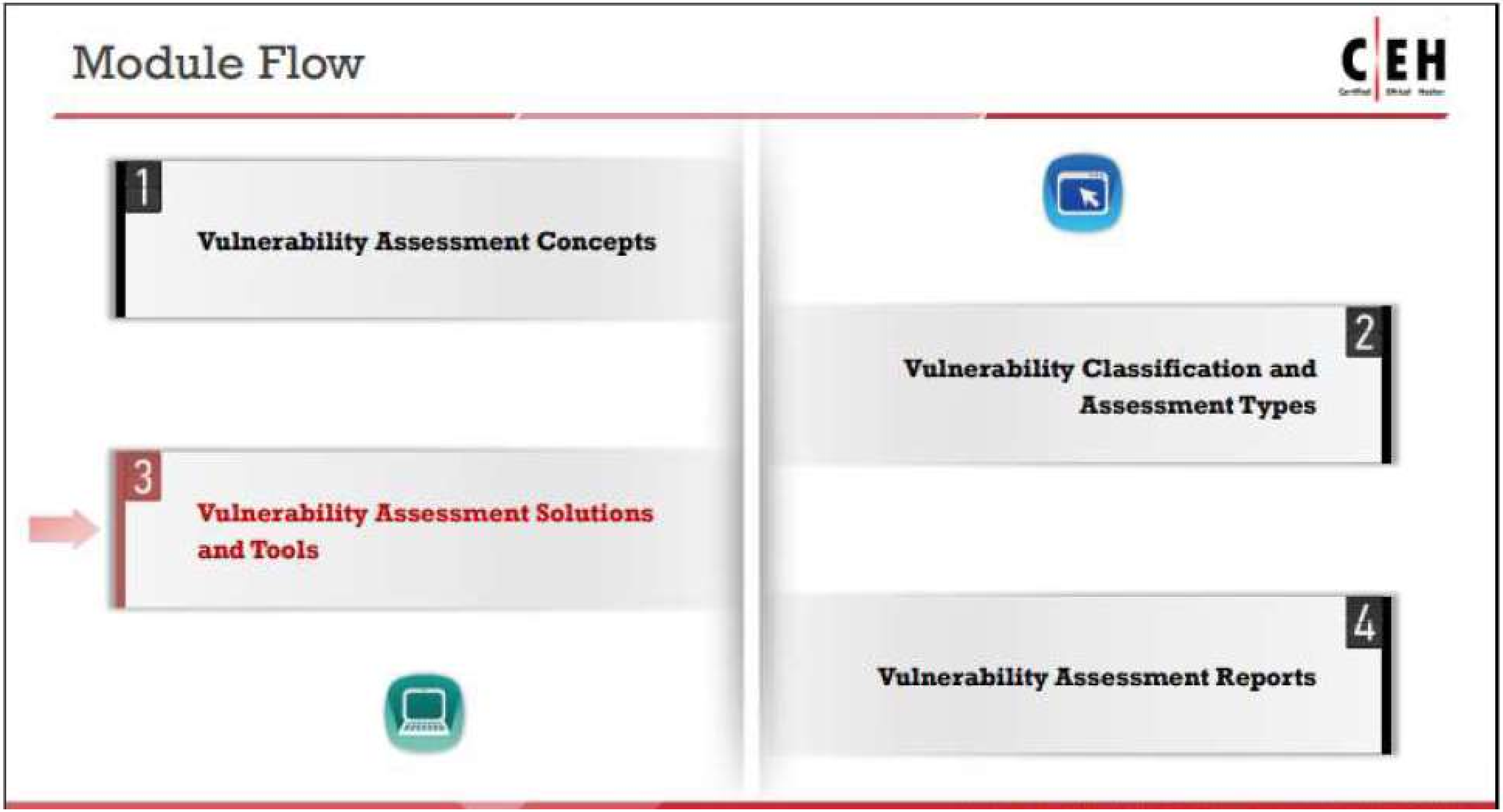
Assesses the network without acquiring **any credentials** of the assets present in the enterprise network

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.



Module Flow

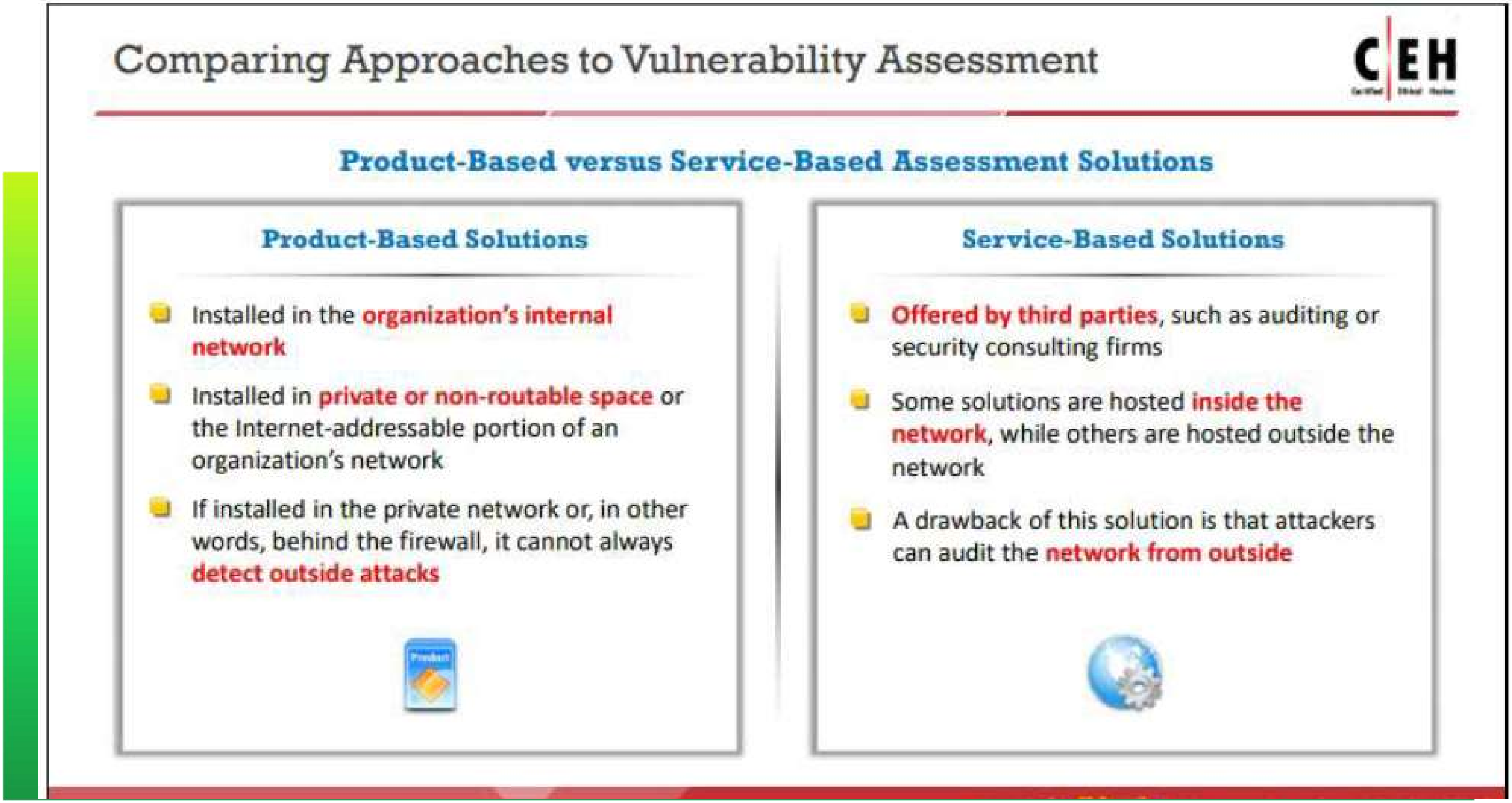
C|EH

1 Vulnerability Assessment Concepts

2 Vulnerability Classification and Assessment Types

3 Vulnerability Assessment Solutions and Tools

4 Vulnerability Assessment Reports



Comparing Approaches to Vulnerability Assessment

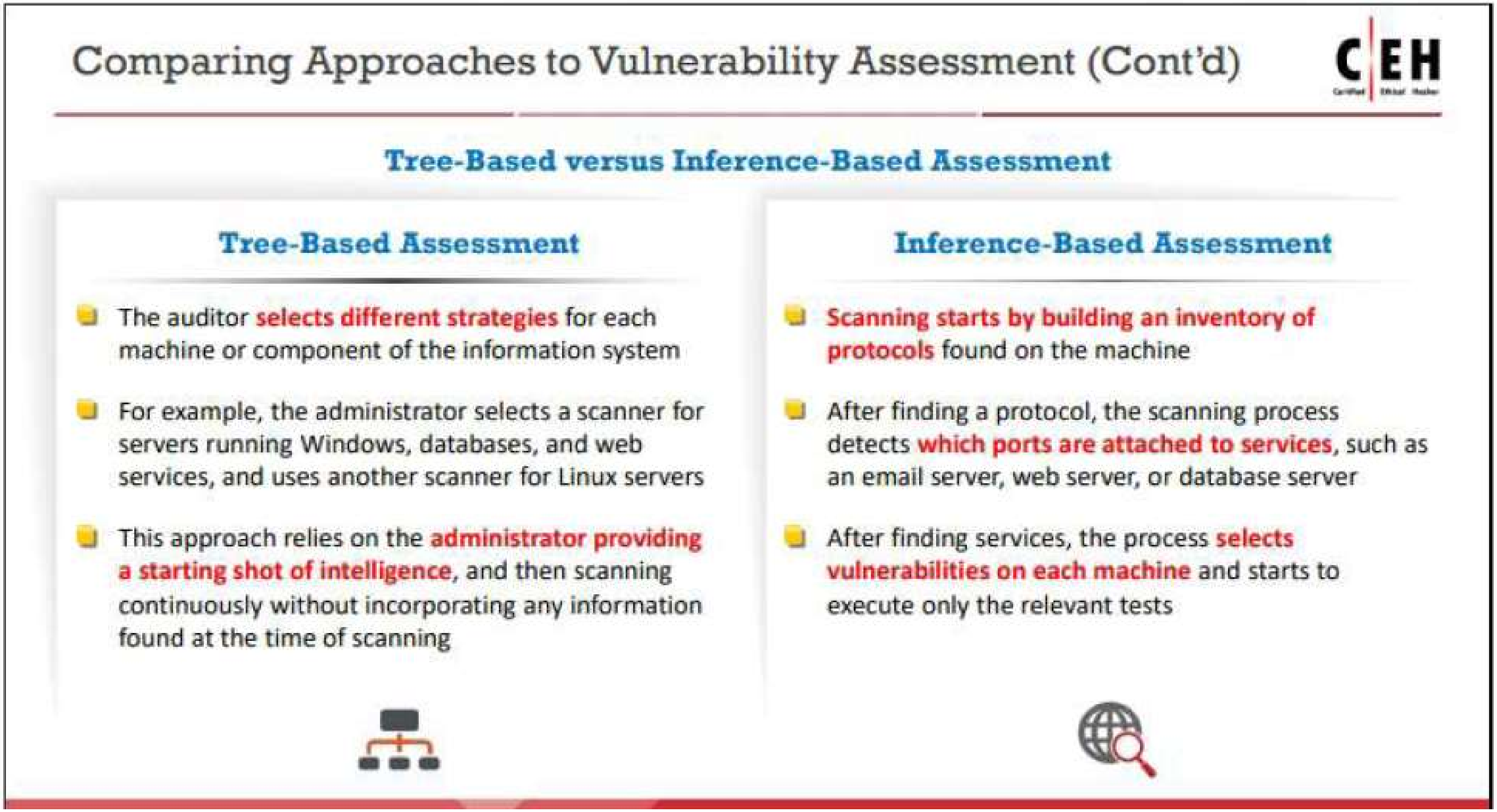
Product-Based versus Service-Based Assessment Solutions

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**



Comparing Approaches to Vulnerability Assessment (Cont'd)

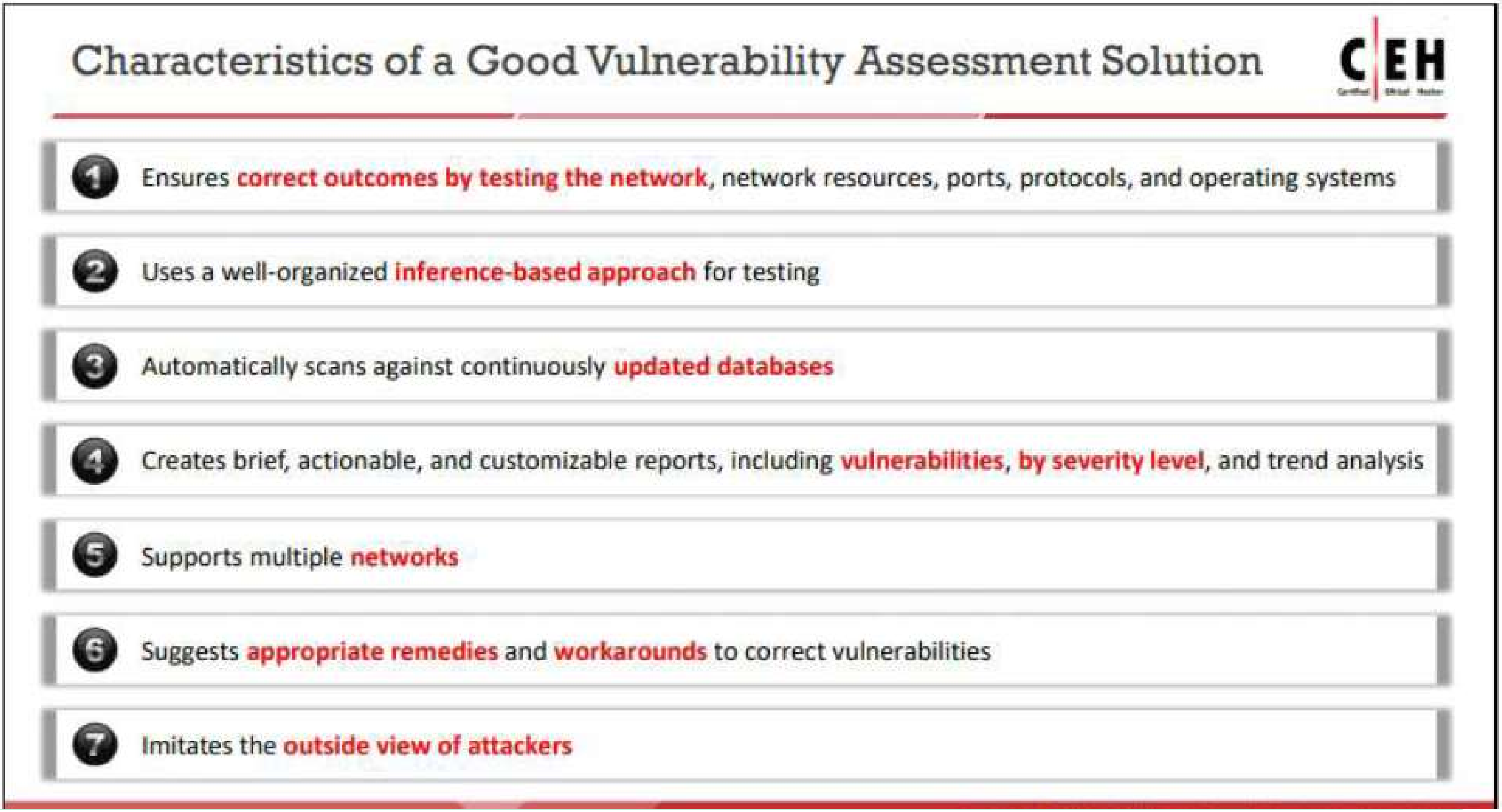
Tree-Based versus Inference-Based Assessment

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

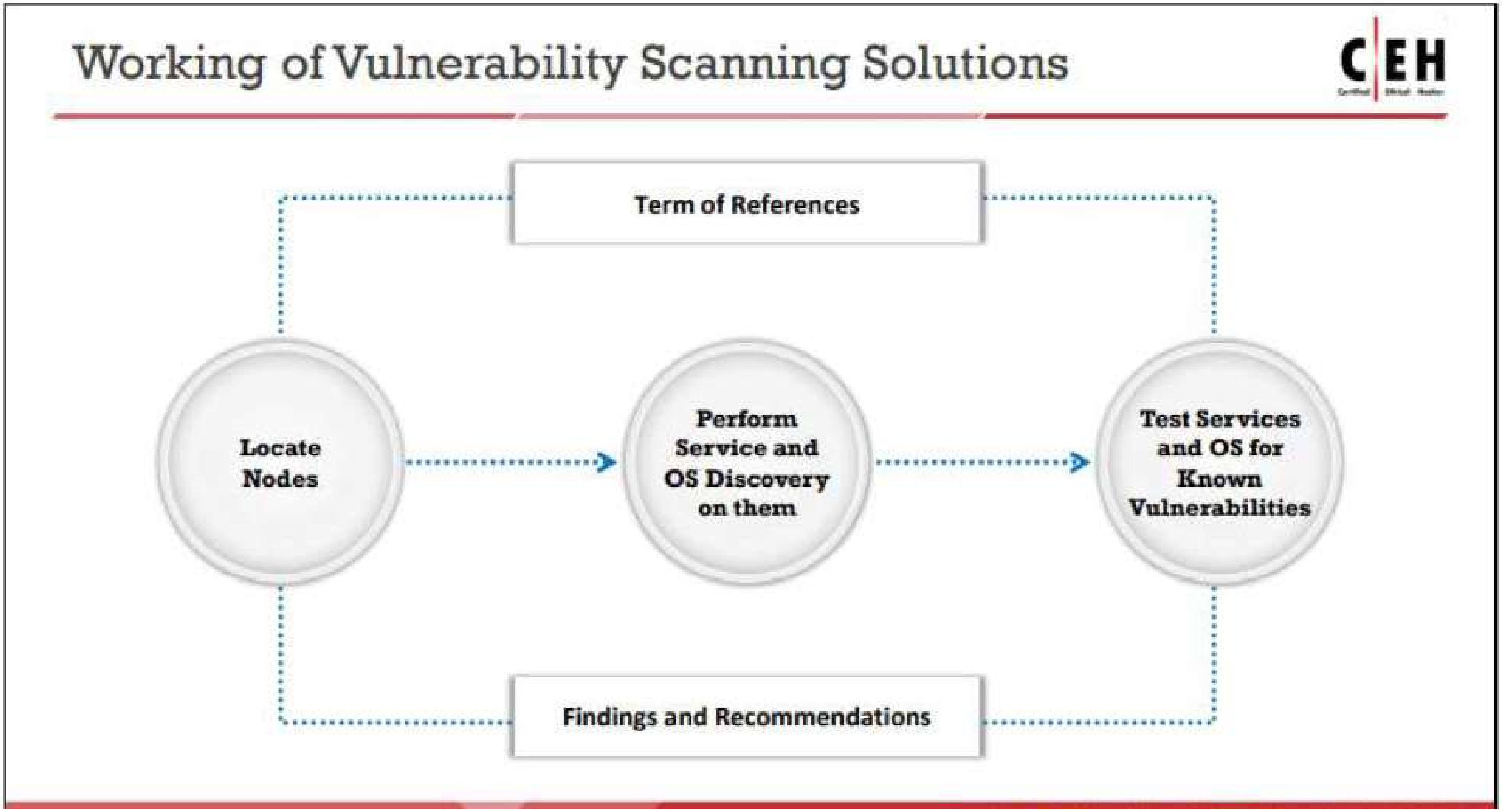
Inference-Based Assessment

- **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 Vulnerability Assessment 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**



Working of Vulnerability Scanning Solutions

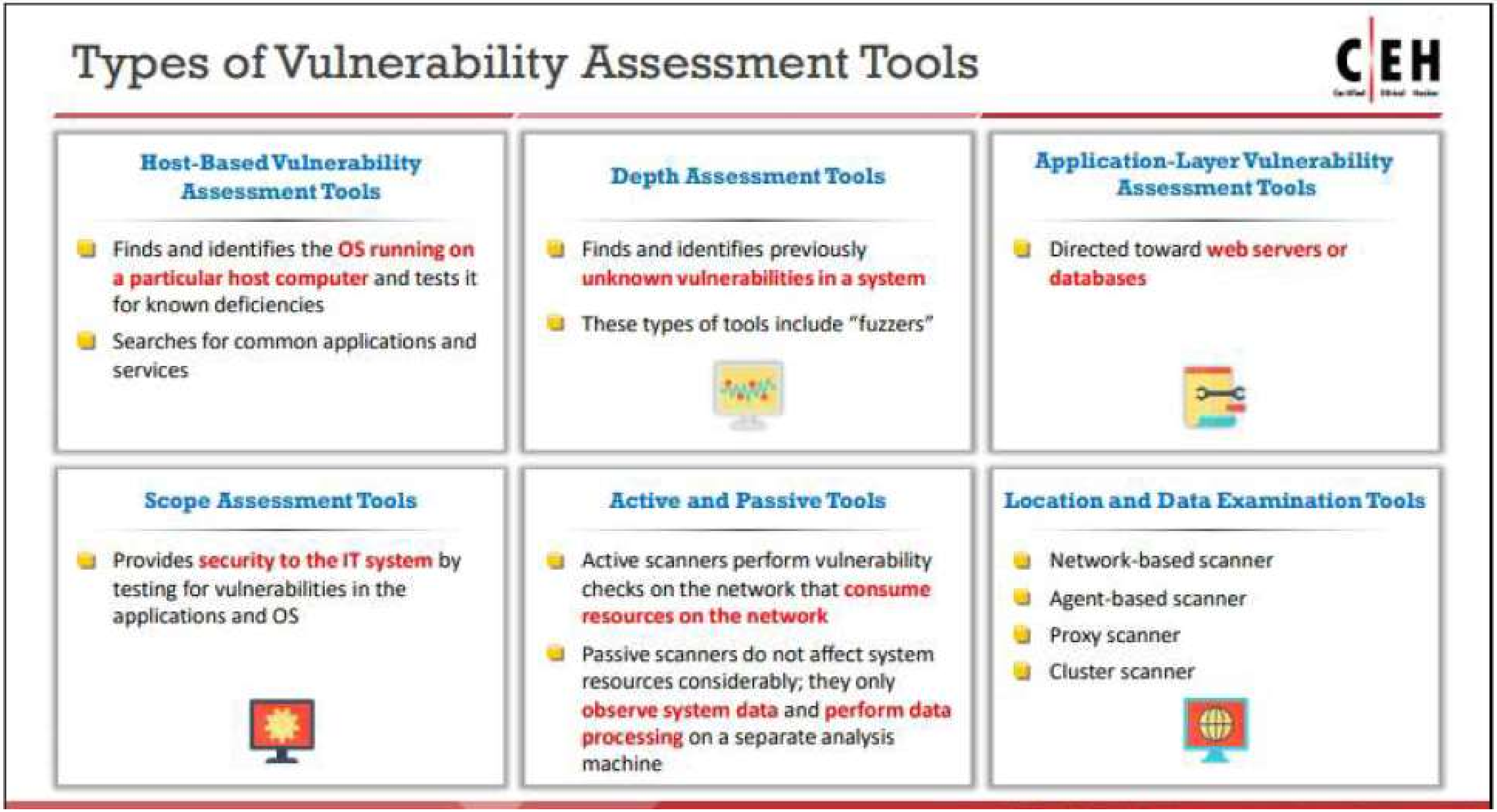
Term of References

Locate Nodes

Perform Service and OS Discovery on them

Test Services and OS for Known Vulnerabilities

Findings and Recommendations



Types of Vulnerability Assessment Tools

C|EH

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

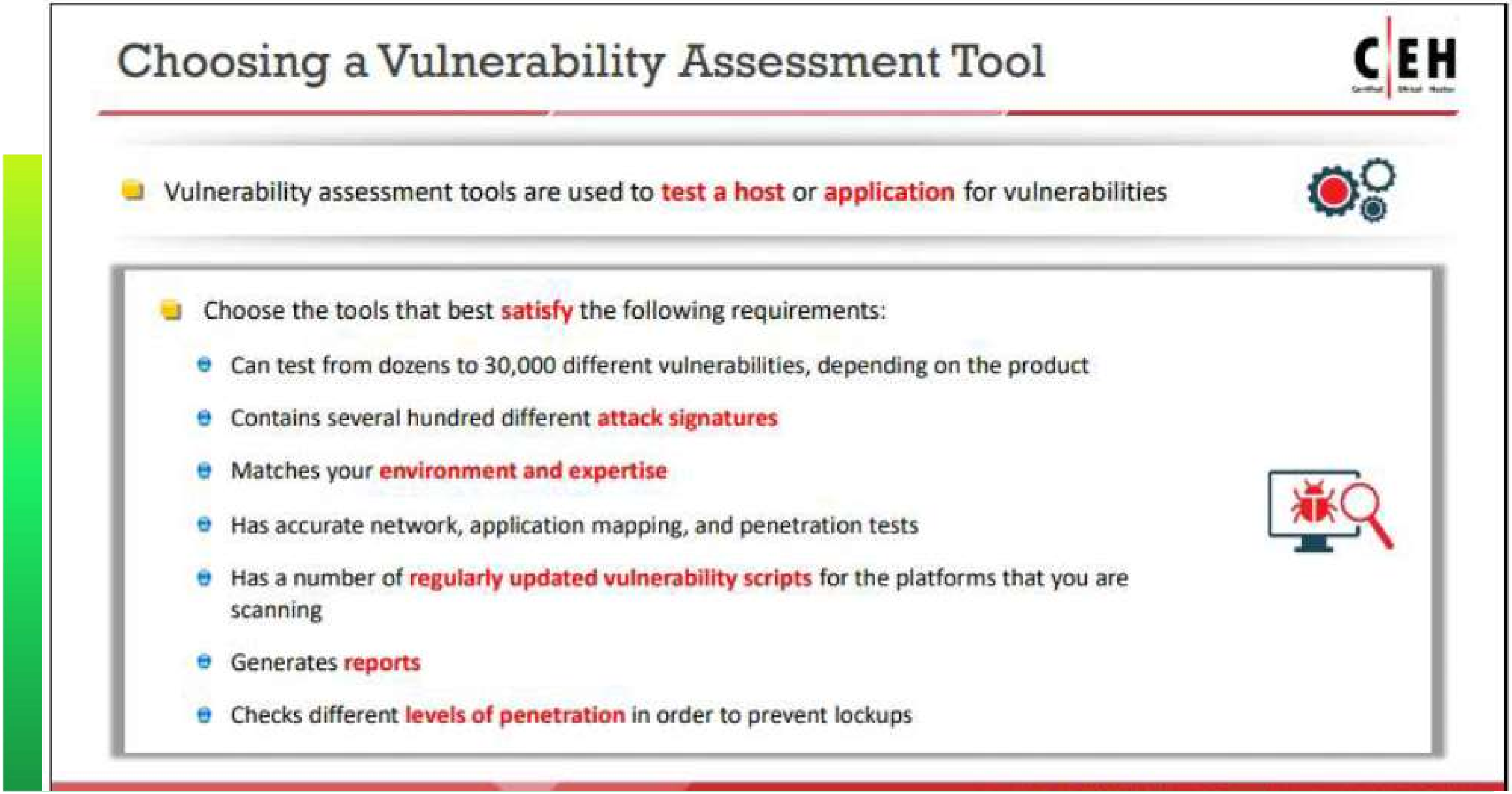
- Provides **security to the IT system** by testing for vulnerabilities in the applications and OS

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

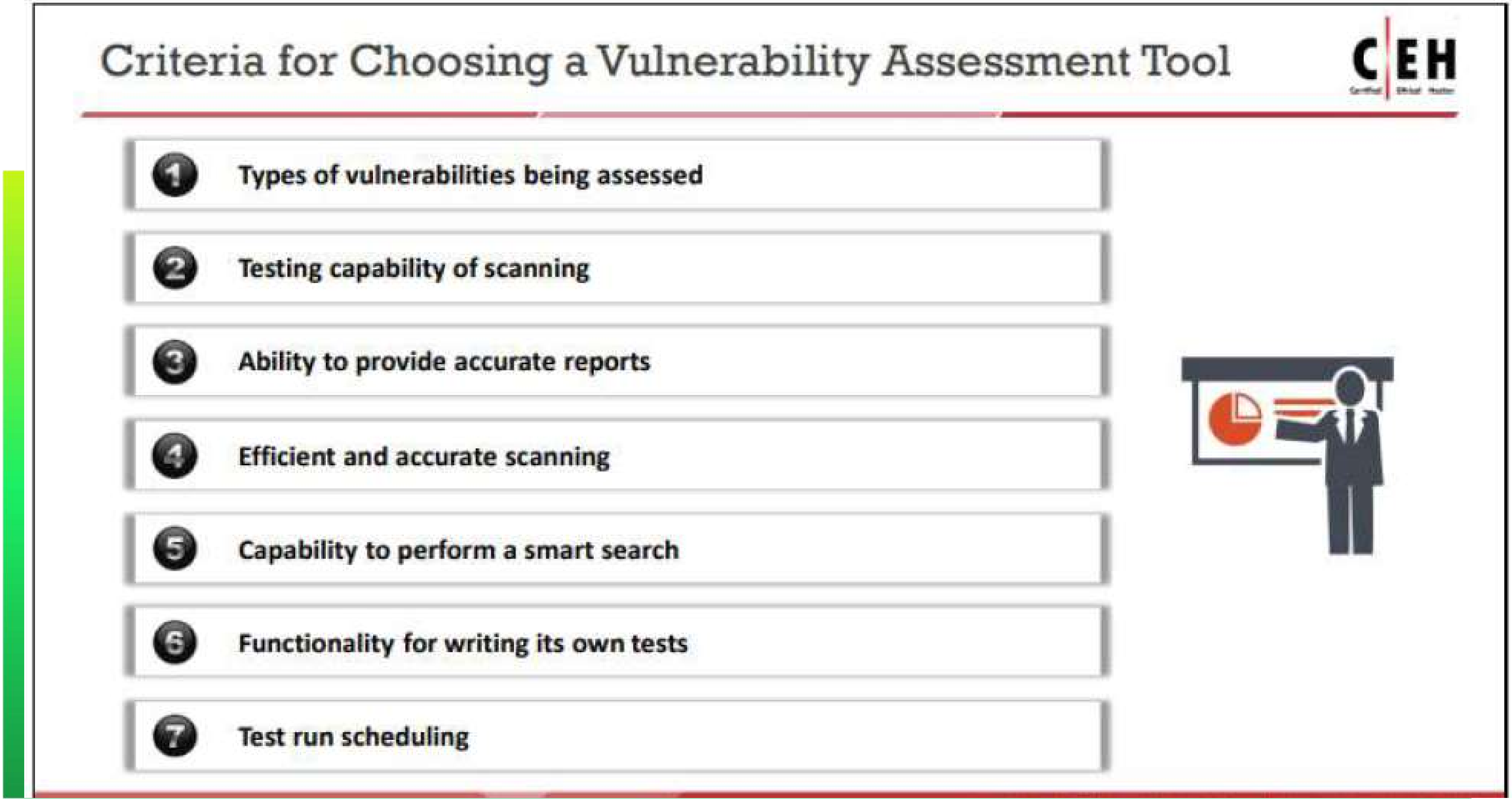
- Network-based scanner
- Agent-based scanner
- Proxy scanner
- Cluster scanner



Choosing a Vulnerability Assessment Tool

- Vulnerability assessment tools are used to **test a host** or **application** for vulnerabilities

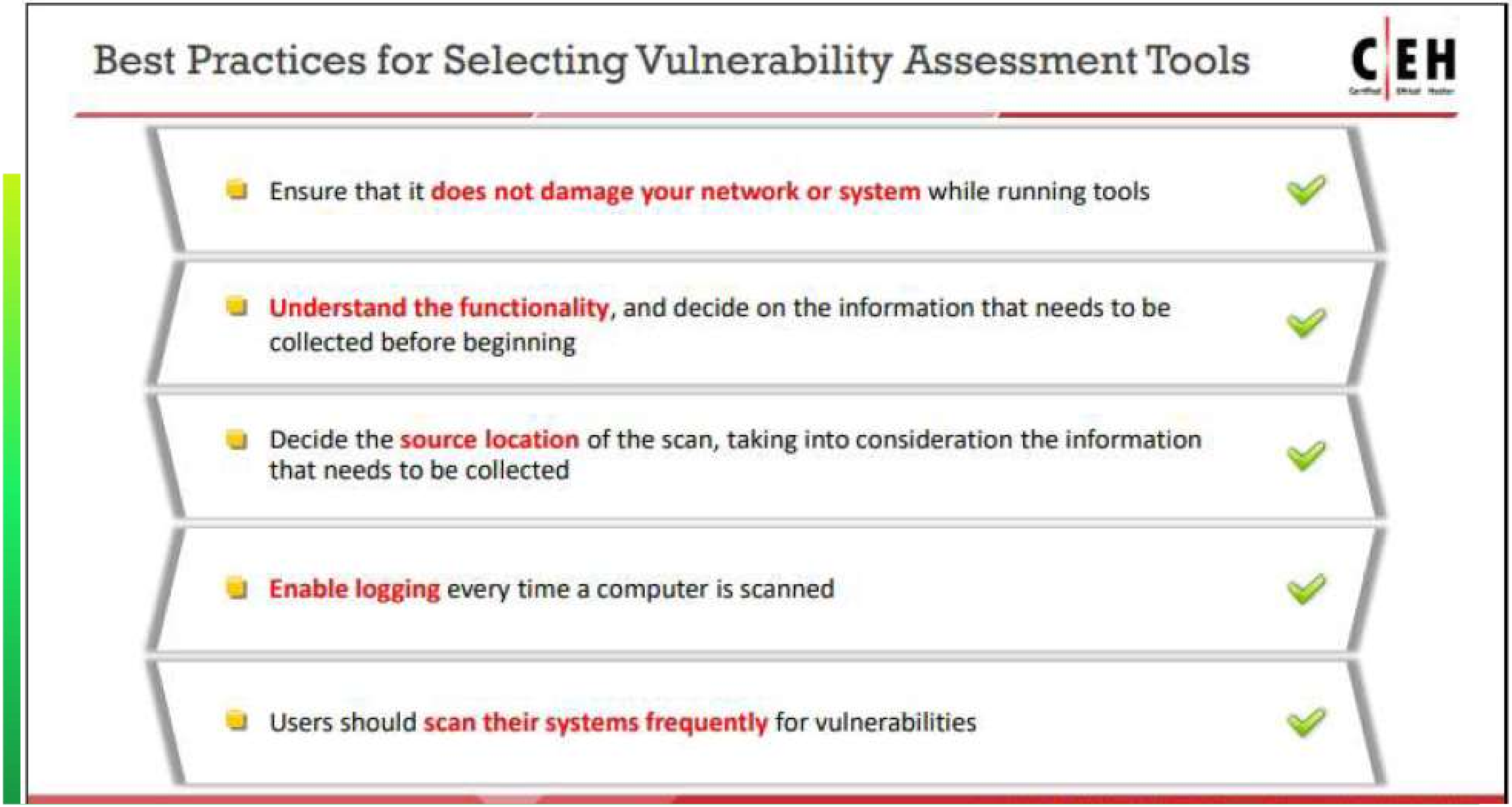
- Choose the tools that best **satisfy** the following requirements:
  - Can test from dozens to 30,000 different vulnerabilities, depending on the product
  - Contains several hundred different **attack signatures**
  - Matches your **environment and expertise**
  - Has accurate network, application mapping, and penetration tests
  - Has a number of **regularly updated vulnerability scripts** for the platforms that you are scanning
  - Generates **reports**
  - Checks different **levels of penetration** in order to prevent lockups



Criteria for Choosing a Vulnerability Assessment Tool

CEH

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

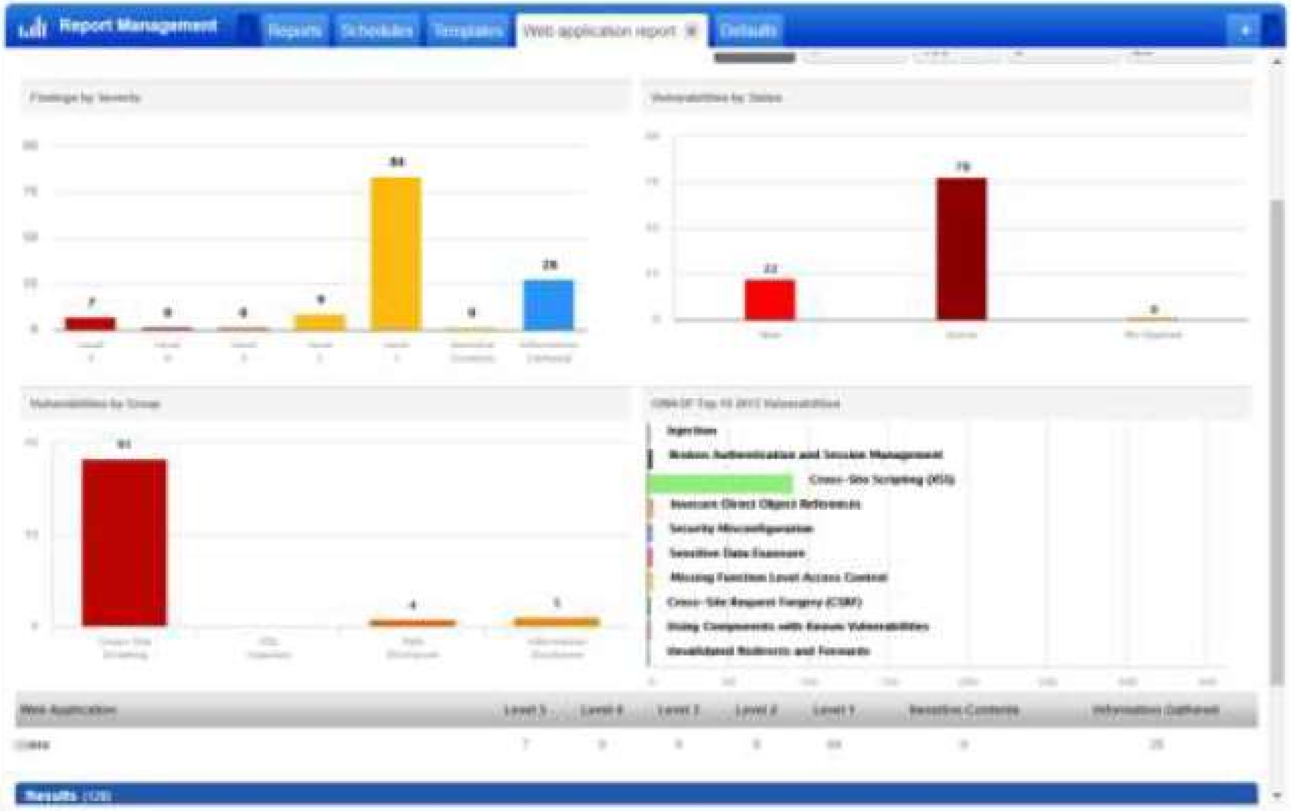


Best Practices for Selecting Vulnerability Assessment Tools

- 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

Vulnerability Assessment Tools: Qualys Vulnerability Management

- A cloud-based service that offers immediate global visibility into IT system areas that might be **vulnerable to the latest Internet threats** and how to protect them
- Aids in the continuous **identification of threats and monitoring of unexpected changes** in a network before they become breaches


Report Management
Reports
Schedules
Templates
Web application report
Details
Findings by Severity
Vulnerabilities by Status
7
0
4
9
84
0
28
22
78
New
Active
Vulnerabilities by Group
91
4
5
OWASP Top 10 2013 Vulnerabilities
Injection
Broken Authentication and Session Management
Cross-Site Scripting (XSS)
Insecure Direct Object References
Security Misconfiguration
Sensitive Data Exposure
Missing Function Level Access Control
Cross-Site Request Forgery (CSRF)
Using Components with Known Vulnerabilities
Unvalidated Redirects and Forwards
Results (128)

Web Application	Level 5	Level 4	Level 3	Level 2	Level 1	Sensitive Contents	Information Gathered
[illegible]	7	0	4	9	84	0	28

https://www.qualys.com

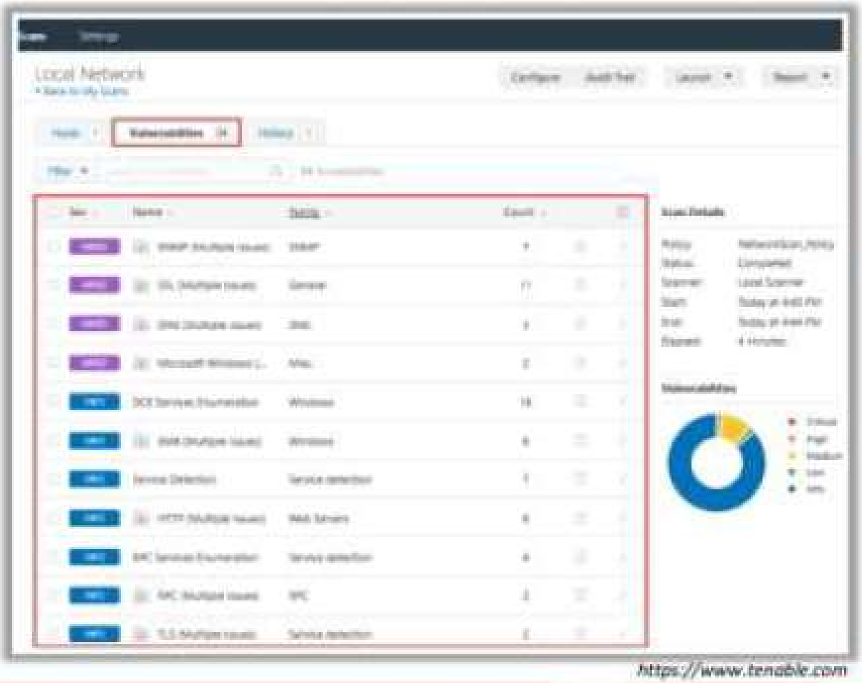
Vulnerability Assessment Tools: Nessus Professional and GFI LanGuard

Nessus Professional

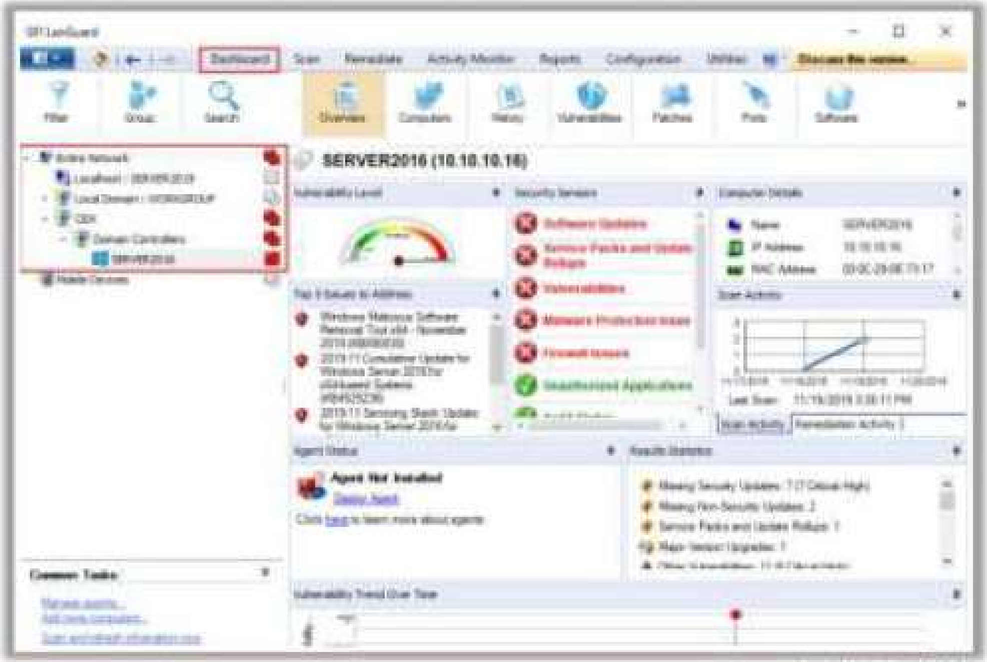
An assessment solution for **identifying the vulnerabilities, configuration issues,** and **malware**

GFI LanGuard

Scans, detects, assesses, and rectifies **security vulnerabilities** in a network and connected devices



https://www.tenable.com



https://www.gfi.com

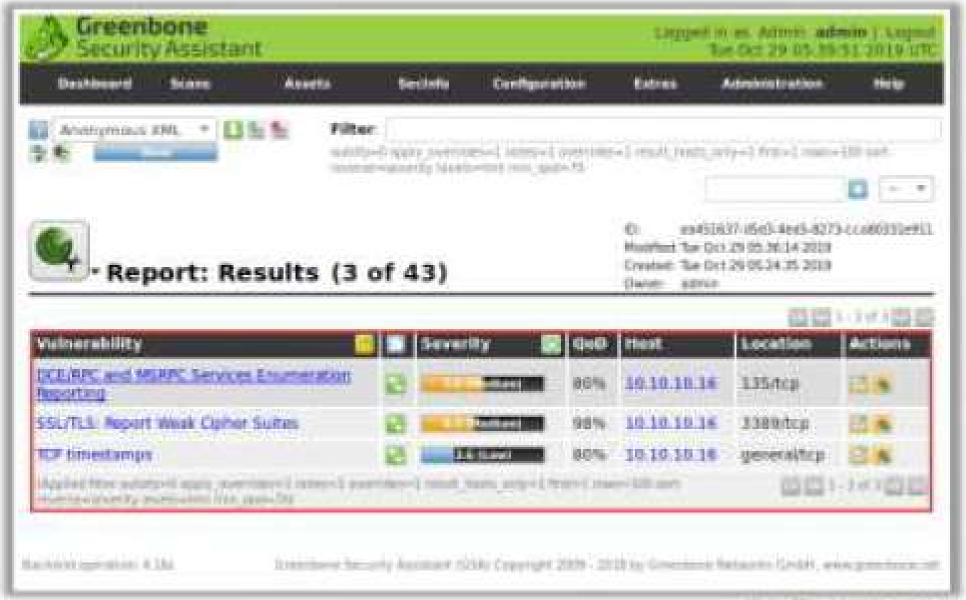
Vulnerability Assessment Tools: OpenVAS and Nikto

OpenVAS

A framework of several services and tools offering a comprehensive and powerful **vulnerability scanning** and **vulnerability management solution**

Nikto

A **web server assessment tool** that examines a web server to discover potential problems and security vulnerabilities

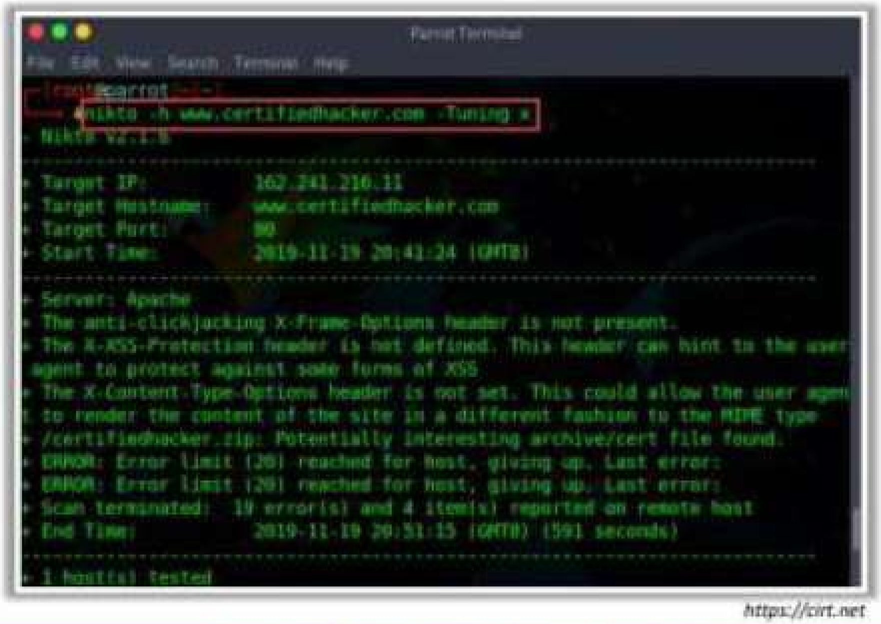


Report: Results (3 of 43)

ID: ea451637-i5e3-4ee3-8273-cca80331e#11
Modified: Tue Oct 29 05:36:14 2019
Created: Tue Oct 29 05:24:35 2019
Owner: admin

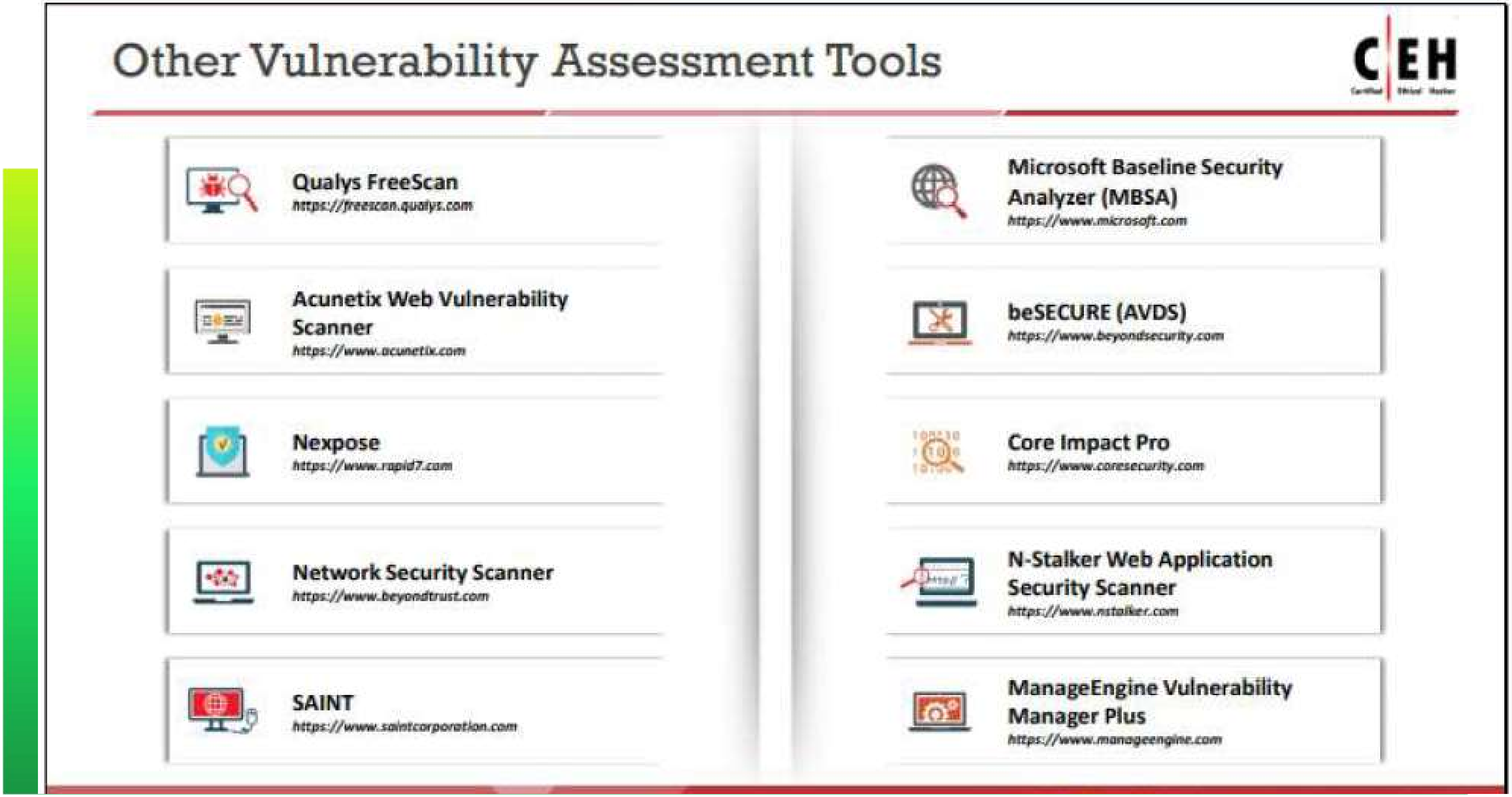
Vulnerability		Severity	QoD	Host	Location	Actions
DCE/RPC and MSRPC Services Enumeration Reporting		5.0 (Medium)	80%	10.10.10.16	135/tcp	
SSL/TLS: Report Weak Cipher Suites		4.3 (Medium)	98%	10.10.10.16	3389/tcp	
TCP timestamps		2.6 (Low)	80%	10.10.10.16	general/tcp	

http://www.openvas.org



```
┌─[root@parrot]─[~]
└──╼ #nikto -h www.certifiedhacker.com -Tuning x
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          162.241.216.11
+ Target Hostname:    www.certifiedhacker.com
+ Target Port:        80
+ Start Time:         2019-11-19 20:41:24 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user
agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agen
t to render the content of the site in a different fashion to the MIME type
+ /certifiedhacker.zip: Potentially interesting archive/cert file found.
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated:  19 error(s) and 4 item(s) reported on remote host
+ End Time:           2019-11-19 20:51:15 (GMT8) (591 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

https://cirt.net

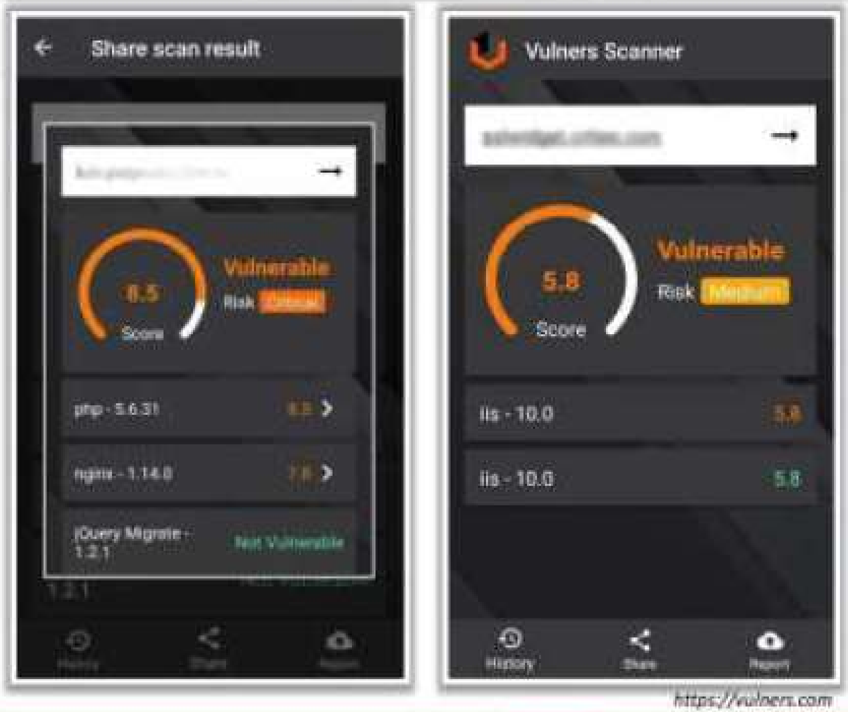


Other Vulnerability Assessment Tools

- Qualys FreeScan — https://freescan.qualys.com
- Acunetix Web Vulnerability Scanner — https://www.acunetix.com
- Nexpose — https://www.rapid7.com
- Network Security Scanner — https://www.beyondtrust.com
- SAINT — https://www.saintcorporation.com
- Microsoft Baseline Security Analyzer (MBSA) — https://www.microsoft.com
- beSECURE (AVDS) — https://www.beyondsecurity.com
- Core Impact Pro — https://www.coresecurity.com
- N-Stalker Web Application Security Scanner — https://www.nstalker.com
- ManageEngine Vulnerability Manager Plus — https://www.manageengine.com

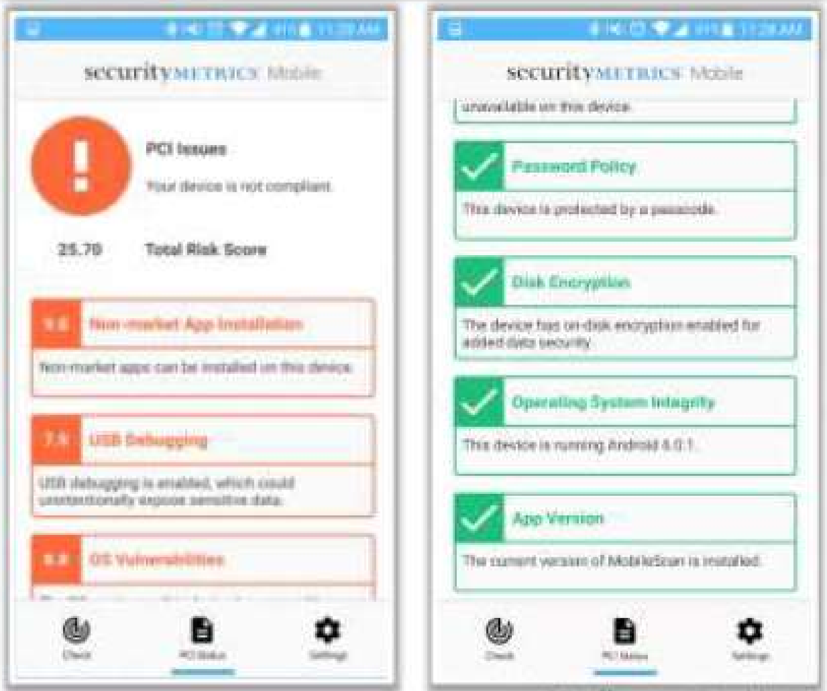
Vulnerability Assessment Tools for Mobile

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



https://vulners.com

Security Metrics Mobile | An android app that **complies with PCI SSC** guidelines to **generate a scan report**



Your device is not compliant.

Non-market apps can be installed on this device.

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

unavailable on this device.

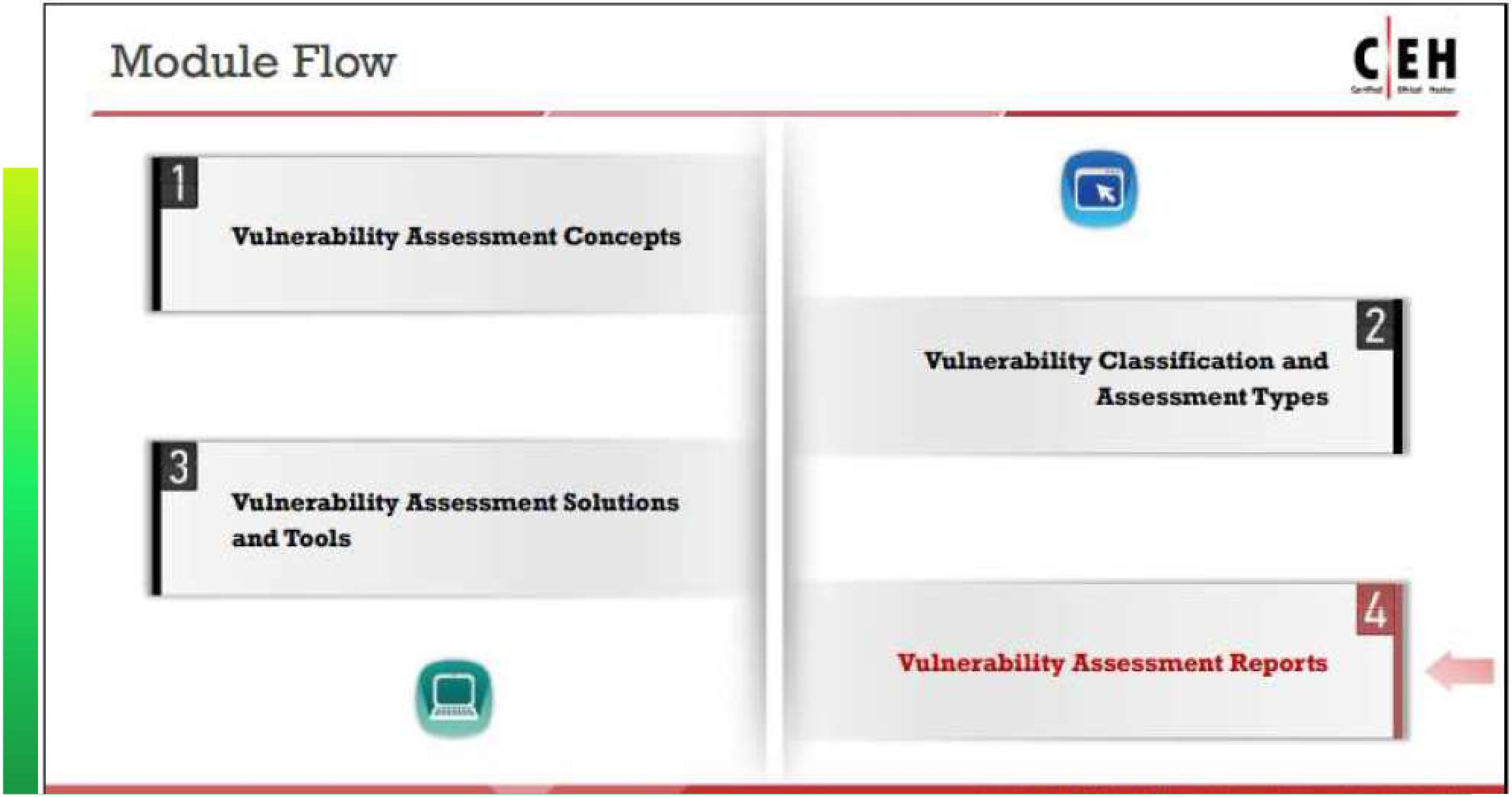
This device is protected by a passcode.

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

This device is running Android 6.0.1.

The current version of MobileScan is installed.

https://www.securitymetrics.com



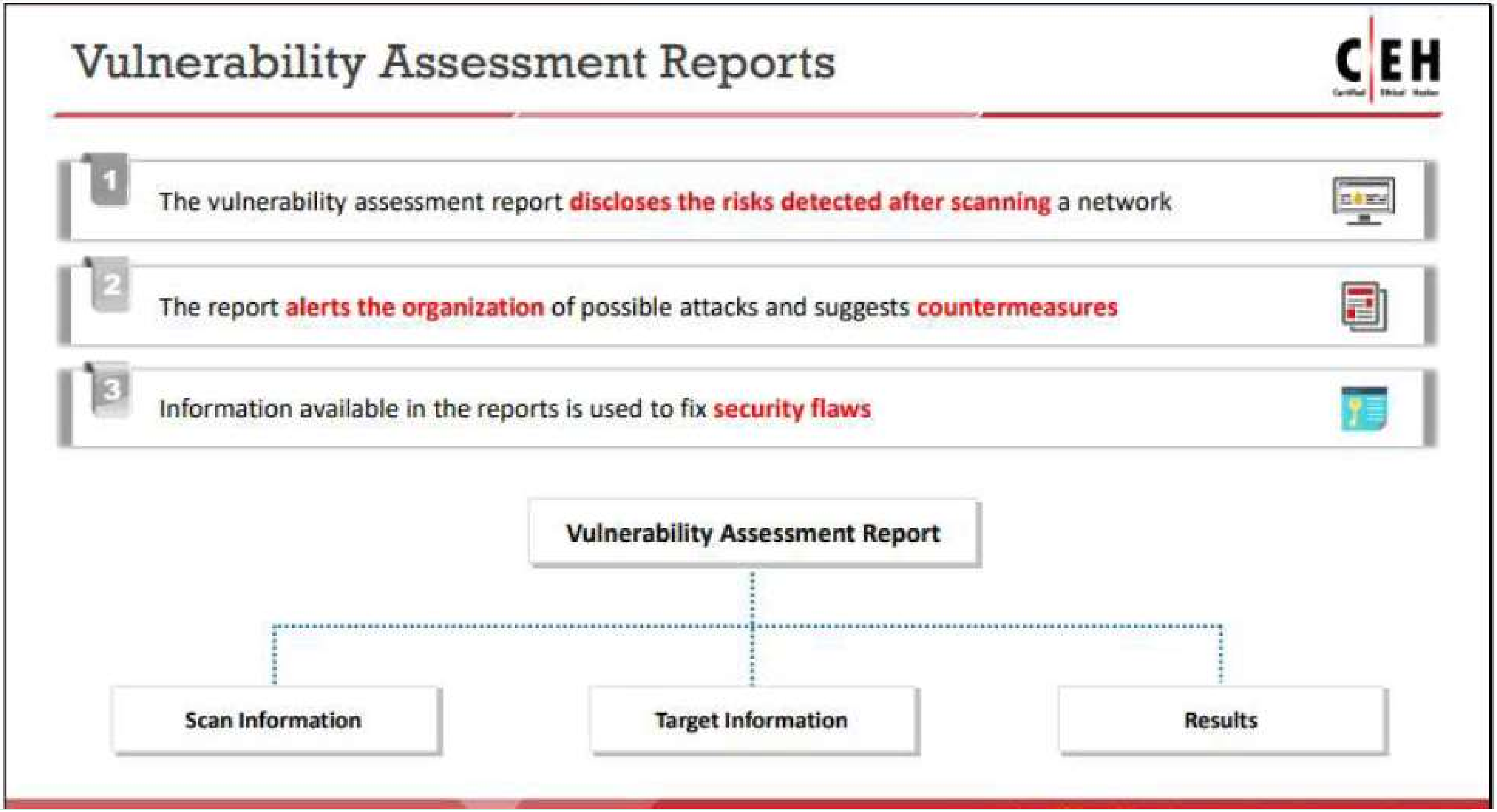
Module Flow

1 Vulnerability Assessment Concepts

2 Vulnerability Classification and Assessment Types

3 Vulnerability Assessment Solutions and Tools

4 Vulnerability Assessment Reports



Vulnerability Assessment 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**

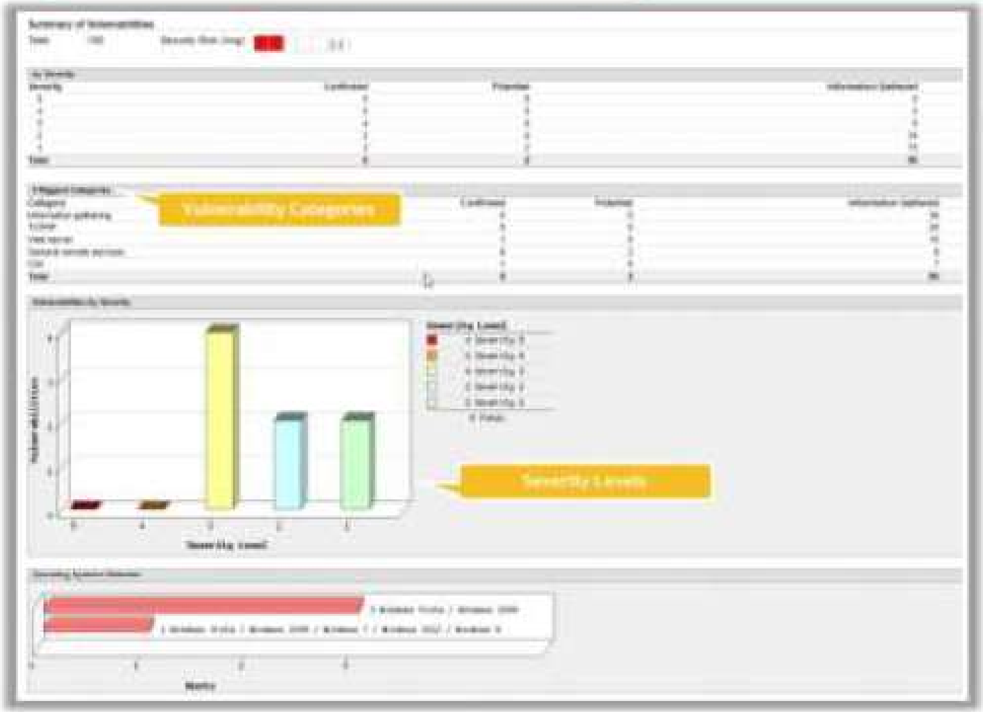
Vulnerability Assessment Report

Scan Information

Target Information

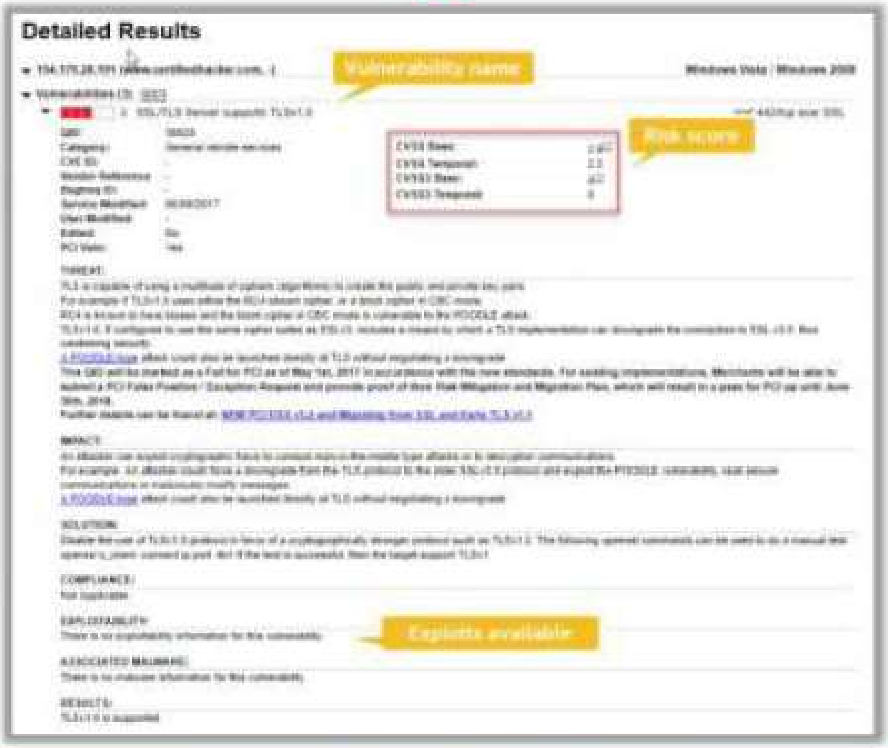
Results

Analyzing Vulnerability Scanning Report



Vulnerability Categories

Severity Levels



Detailed Results

www.certifiedhacker.com — Windows Vista / Windows 2008

SSL/TLS Server supports TLSv1.0

QID:
Category: General remote services
CVE ID:
Vendor Reference:
Bugtraq ID:
Service Modified:
User Modified:
Edited: No
PCI Vuln: Yes

CVSS Base
CVSS Temporal
CVSS3 Base
CVSS3 Temporal

THREAT:

IMPACT:

SOLUTION:

COMPLIANCE:

EXPLOITABILITY:

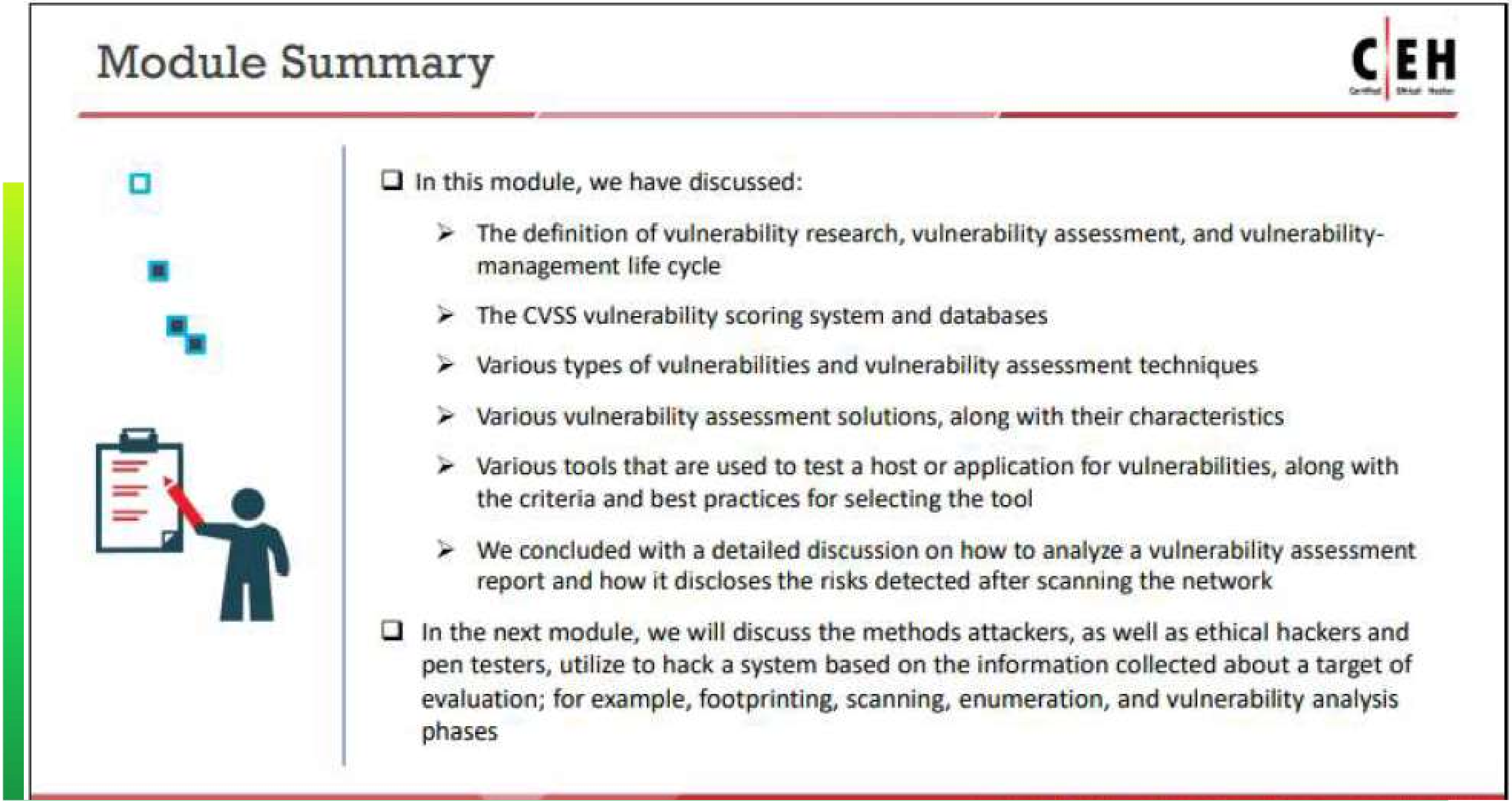
ASSOCIATED MALWARE:

RESULTS:

Vulnerability name

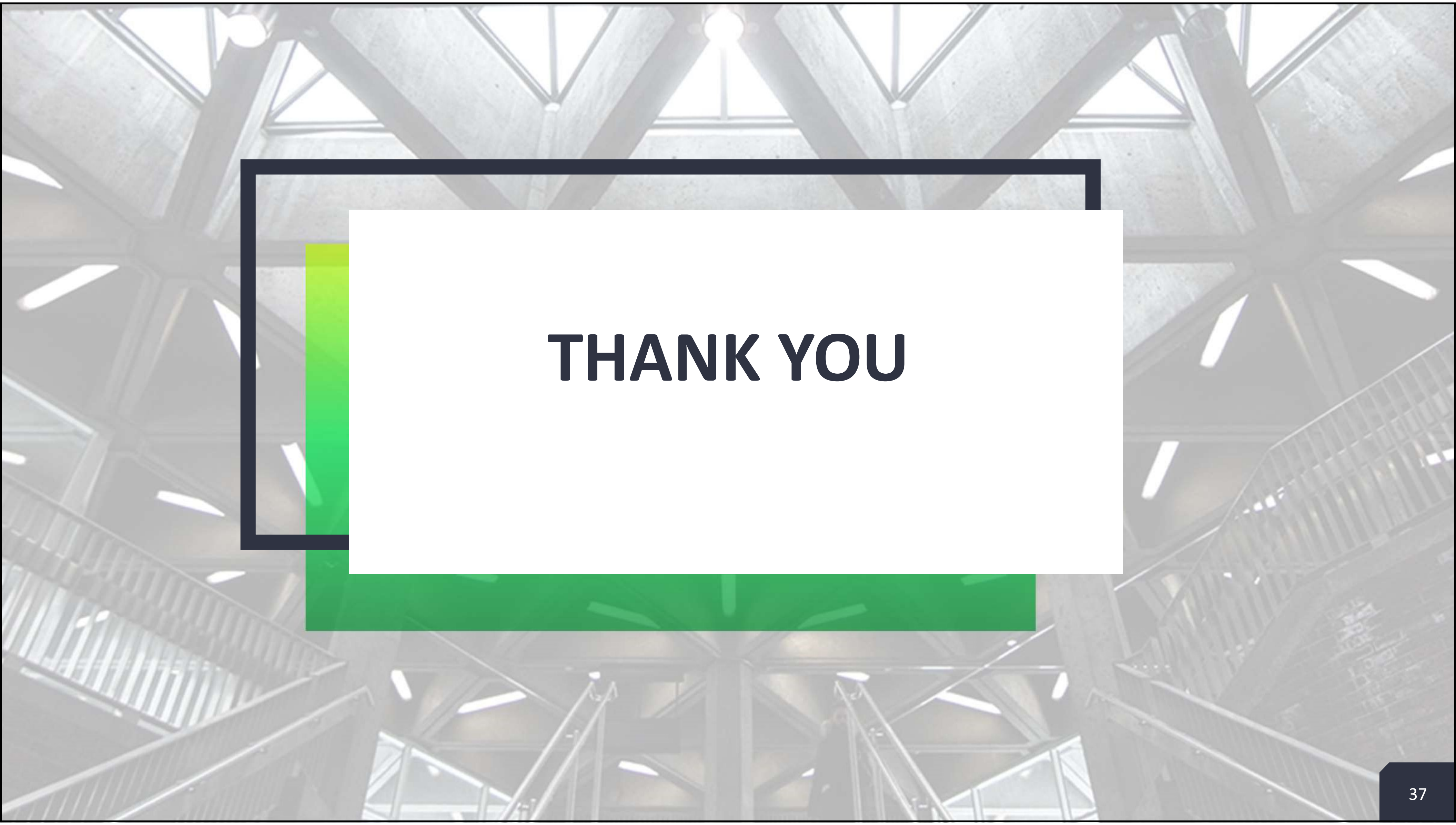
Risk score

Exploits available



Module Summary

- ❑ In this module, we have discussed:
  - ➢ The definition of vulnerability research, vulnerability assessment, and vulnerability-management life cycle
  - ➢ The CVSS vulnerability scoring system and databases
  - ➢ Various types of vulnerabilities and vulnerability assessment techniques
  - ➢ Various vulnerability assessment solutions, along with their characteristics
  - ➢ Various tools that are used to test a host or application for vulnerabilities, along with the criteria and best practices for selecting the tool
  - ➢ We concluded with a detailed discussion on how to analyze a vulnerability assessment report and how it discloses the risks detected after scanning the network
- ❑ In the next module, we will discuss the methods attackers, as well as ethical hackers and pen testers, utilize to hack a system based on the information collected about a target of evaluation; for example, footprinting, scanning, enumeration, and vulnerability analysis phases



THANK YOU