C|EH™

Certified Ethical Hacker

Module 05

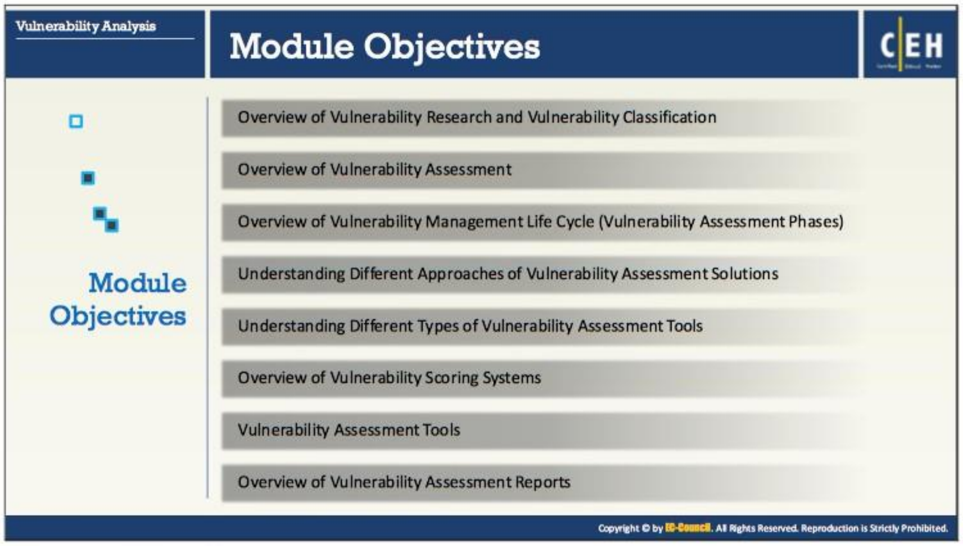
Vulnerability Analysis

C|EH™
Certified Ethical Hacker

Module 05

Vulnerability Analysis

This page is intentionally left blank.



Vulnerability Analysis

Module Objectives

Module Objectives

- Overview of Vulnerability Research and Vulnerability Classification
- Overview of Vulnerability Assessment
- Overview of Vulnerability Management Life Cycle (Vulnerability Assessment Phases)
- Understanding Different Approaches of Vulnerability Assessment Solutions
- Understanding Different Types of Vulnerability Assessment Tools
- Overview of Vulnerability Scoring Systems
- Vulnerability Assessment Tools
- Overview of Vulnerability Assessment Reports

Module Objectives

In today's world, organizations depend heavily on information technology. It is necessary for them to protect their vital information. This information addresses areas of finance, research and development, personnel, legality, and security. Vulnerability assessments scan networks for known security weaknesses.

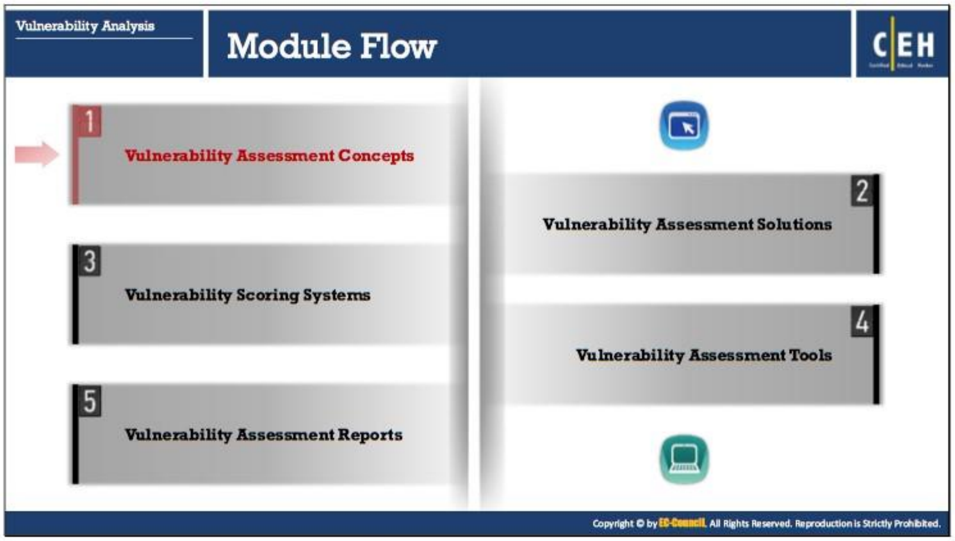
Attackers perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems. The identified vulnerabilities are used by the attackers to perform further exploitation on that target network.

On the other hand, vulnerability assessment plays a major role in providing security to any organization's resources and infrastructure from various internal and external threats. To secure a network, an administrator needs to perform patch management, install proper antivirus software, check configurations, solve known issues in third party applications, and troubleshoot hardware with default configurations. All these activities together constitute vulnerability assessment.

This module starts with an introduction to vulnerability assessment concepts. This module also discusses the vulnerability management life cycle and various approaches and tools used to perform the vulnerability assessment. This module will focus your awareness on tools and techniques used by the attackers to perform vulnerability analysis. The module ends with an overview of vulnerability assessment report, which helps an ethical hacker in taking necessary steps to fix the identified vulnerabilities.

At the end of this module, you will be able to:

- Understand vulnerability research and vulnerability classification
- Describe vulnerability assessment
- Describe about vulnerability management life cycle (vulnerability assessment phases)
- Understand different approaches of vulnerability assessment solutions
- Describe different characteristics of good vulnerability assessment solutions
- Explain different types of vulnerability assessment tools
- Choose an appropriate vulnerability assessment tools
- Understand vulnerability scoring systems
- Use various vulnerability assessment tools
- Generate vulnerability assessment reports



Vulnerability Analysis

Module Flow

1 Vulnerability Assessment Concepts

2 Vulnerability Assessment Solutions

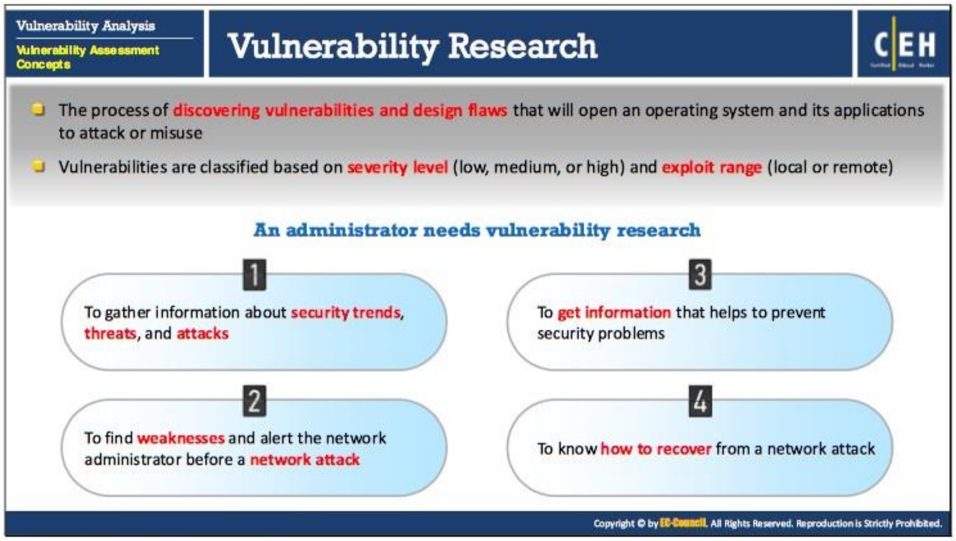
3 Vulnerability Scoring Systems

4 Vulnerability Assessment Tools

5 Vulnerability Assessment Reports

Vulnerability Assessment Concepts

In a network there are generally two main causes for systems being vulnerable, software or hardware misconfiguration and poor programming practices. Attackers exploit these vulnerabilities to perform various types of attacks on organizational resources. This section gives an overview on vulnerability assessment, classification, types of vulnerability assessments and vulnerability assessment phases.



Vulnerability Analysis
Vulnerability Assessment Concepts

Vulnerability Research

CEH

- 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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Research

Vulnerability research is the process of discovering vulnerabilities and design flaws that will open an operating system and its applications to attack or misuse.

An administrator needs vulnerability research:

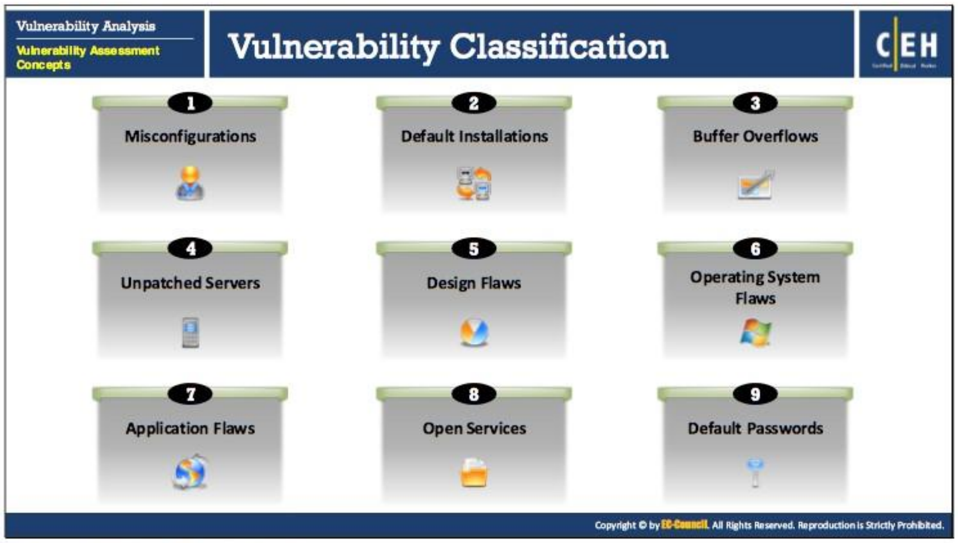
- To gather information about security trends, threats, and attacks
- To find weaknesses, and alert the network administrator before a network attack
- To get information that helps prevent the security problems
- To know how to recover from a network attack

An ethical hacker needs to keep up with the most recently discovered vulnerabilities and exploits in order 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 in order to find news related to current exploits
- Checking underground hacking web sites for new vulnerabilities and exploits
- Checking newly released alerts regarding relevant innovations and product improvements for security systems

Security experts and vulnerability scanners classify vulnerabilities by:

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



Vulnerability Analysis

Vulnerability Assessment Concepts

Vulnerability Classification

Vulnerability Classification

Vulnerabilities present in a system or network are classified into the following categories:

- **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:

  - An application running with debug enabled
  - Outdated software running on the system
  - Running unnecessary services on a machine
  - Using misconfigured SSL certificates and default certificates
  - Improperly authenticated external systems
  - Disabling security settings and features

  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 security. In some cases, infected devices may not contain any valuable information but 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**

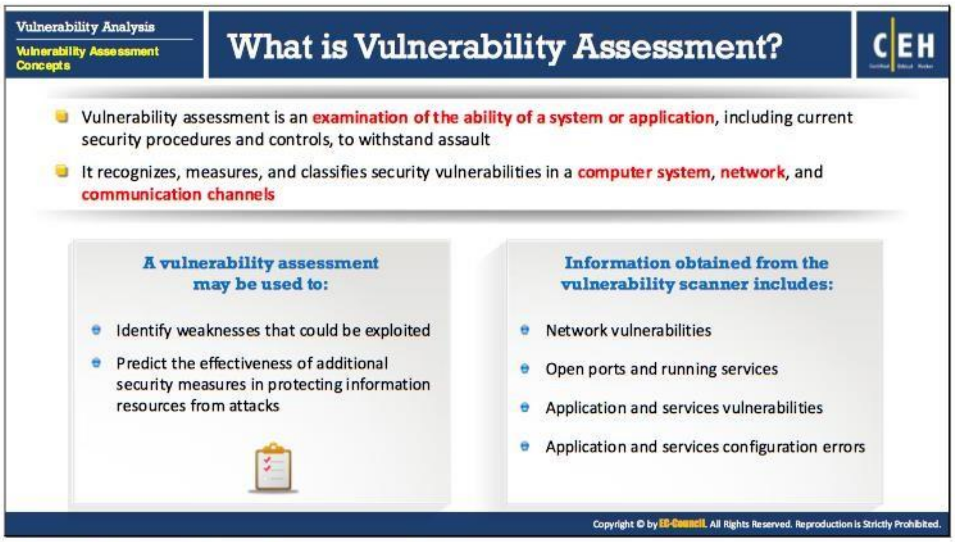
  Application flaws are vulnerabilities in applications that are exploited by the attackers. Applications should be secured using validation and authorization of the user. Applications pose security threats such as data tampering and unauthorized access to configuration stores. If the applications are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



Vulnerability Analysis
Vulnerability Assessment Concepts

What is Vulnerability Assessment?

- Vulnerability assessment is an **examination of the ability of a system or application**, including current security procedures and controls, to withstand assault
- 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

What is Vulnerability Assessment?

Vulnerability assessment is an examination of the ability of a system or application, including current security procedures and controls, to withstand assault. Vulnerability assessment scans networks for known security weaknesses. It recognizes, measures, and classifies security vulnerabilities in a computer system, network, and communication channels. It also assists security professionals in securing the network by determining security loopholes or vulnerabilities in the current security mechanism before the bad guys can exploit them.

A vulnerability assessment may be used to:

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

Typically, vulnerability-scanning tools search network segments for IP-enabled devices and enumerate systems, operating systems, and applications. Vulnerability-scanning software scans the computer against the Common Vulnerability and Exposures (CVE) index and security bulletins provided by the software vendor.

Vulnerability scanners are capable of identifying the following information:

- The OS version running on computers or devices
- IP and Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports that are listening
- Applications installed on computers
- Accounts with weak passwords

- Files and folders with weak permissions
- Default services and applications that might have to be uninstalled
- Mistakes in the security configuration of common applications
- Computers exposed to known or publicly reported vulnerabilities

There are two approaches to network vulnerability scanning:

- **Active Scanning**: The attacker interacts directly with the target network to find vulnerabilities.

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

- **Passive Scanning**: The attacker tries to find vulnerabilities without directly interacting with the target network. The attacker identifies vulnerabilities via information exposed by systems in their normal communications.

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

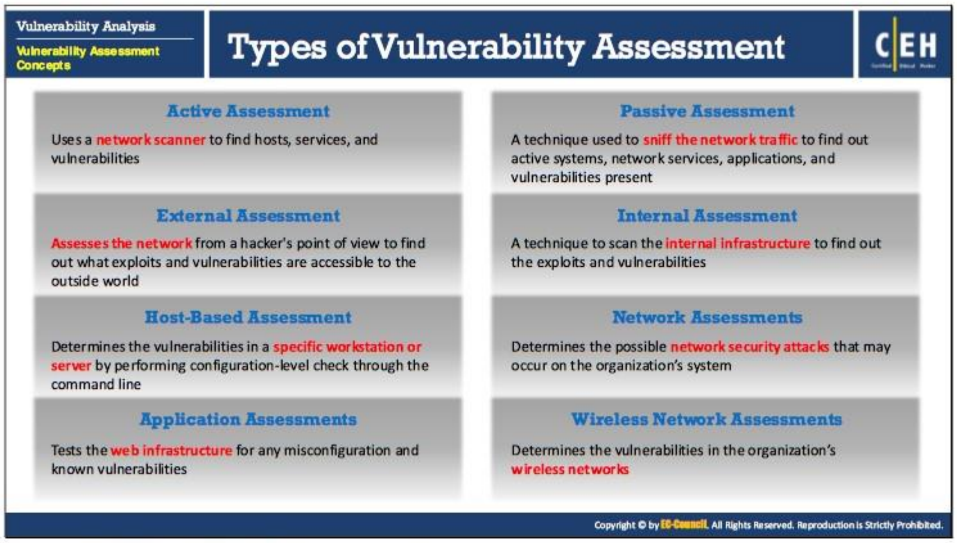
Attackers scan for vulnerabilities using tools such as Nessus, GFI LanGuard, and OpenVAS. Vulnerability scanning enables an attacker to identify network vulnerabilities, open ports and running services, application and services configuration errors, and application and services vulnerabilities.

Limitations of Vulnerability Assessment

The following are some of the limitations of vulnerability assessments:

- Vulnerability-scanning software is limited in its ability to detect vulnerabilities at a given point in time.
- Vulnerability-scanning software must be updated when new vulnerabilities are discovered or improvements are made to the software being used.
- Software is only as effective as the maintenance performed on it by the software vendor and by the administrator who uses it.
- It does not measure the strength of security controls.
- Vulnerability-scanning software itself is not immune to software engineering flaws that might lead to missing serious vulnerabilities.

The methodology used might have an impact on the result of the test. For example, vulnerability-scanning software that runs under the security context of the domain administrator will yield different results than if it were run under the security context of an authenticated user or a non-authenticated user. Similarly, diverse vulnerability-scanning software packages assess security differently and have unique features. This can influence the result of the assessment.



Vulnerability Analysis
Vulnerability Assessment Concepts

Types of Vulnerability Assessment

Active Assessment

Uses a network scanner to find hosts, services, and vulnerabilities

Passive Assessment

A technique used to sniff the network traffic to find out active systems, network services, applications, and vulnerabilities present

External Assessment

Assesses the network from a hacker's point of view to find out what exploits and vulnerabilities are accessible to the outside world

Internal Assessment

A technique to scan the internal infrastructure to find out the exploits and vulnerabilities

Host-Based Assessment

Determines the vulnerabilities in a specific workstation or server by performing configuration-level check through the command line

Network Assessments

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

Application Assessments

Tests the web infrastructure for any misconfiguration and known vulnerabilities

Wireless Network Assessments

Determines the vulnerabilities in the organization's wireless networks

Types of Vulnerability Assessment

Given below are the different types of vulnerability assessments:

- **Active Assessment**

  Active assessments are a type of vulnerability assessment that uses network scanners to scan the network to identify the hosts, services, and vulnerabilities present in that network. Active network scanners have the capability to reduce the intrusiveness of the checks they perform.

- **Passive Assessment**

  Passive assessments sniff the traffic present on the network to identify the active systems, network services, applications, and vulnerabilities. Passive assessments also provide a list of the users who are currently using the network.

- **External Assessment**

  External assessment assesses the network from a hacker's point of view to find out what exploits and vulnerabilities are accessible to the outside world. These types of assessments use external devices such as firewalls, routers, and servers. An external assessment estimates the threat of network security attacks external to the organization. It determines how secure the external network and firewall are.

  The following are some of the possible steps in performing an external assessment:

  - Determine the set of rules for firewall and router configurations for the external network.
  - Check whether external server devices and network devices are mapped.

- Identify open ports and related services on the external network.
- Examine patch levels on the server and external network devices.
- Review detection systems such as IDS, firewalls, and application-layer protection systems.
- Get information on DNS zones.
- Scan the external network through a variety of proprietary tools available on the Internet.
- Examine Web applications such as e-commerce and shopping cart software for vulnerabilities.

- **Internal Assessment**

  An internal assessment involves scrutinizing the internal network to find exploits and vulnerabilities. The following are some of the possible steps in performing an internal assessment:

  - Specify the open ports and related services on network devices, servers, and systems.
  - Check for router configurations and firewall rule sets.
  - List the internal vulnerabilities of the operating system and server.
  - Scan for Trojans that may be present in the internal environment.
  - Check the patch levels on the organization's internal network devices, servers, and systems.
  - Check for the existence of malware, spyware, and virus activity and document them.
  - Evaluate the physical security.
  - Identify and review the remote management process and events.
  - Assess the file-sharing mechanisms (for example, NFS and SMB/CIFS shares).
  - Examine the antivirus implementation and events.

- **Host-based Assessment**

  Host-based assessments are a type of security check that involves carrying out a configuration-level check through the command line. These assessments check the security of a particular network or server. Host-based scanners assess systems to identify vulnerabilities such as incorrect registry and file permissions, as well as software configuration errors. Host-based assessment can use many commercial and open-source scanning tools.

- **Network Assessments**

  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. A typical network assessment conducts the following tests on a network:

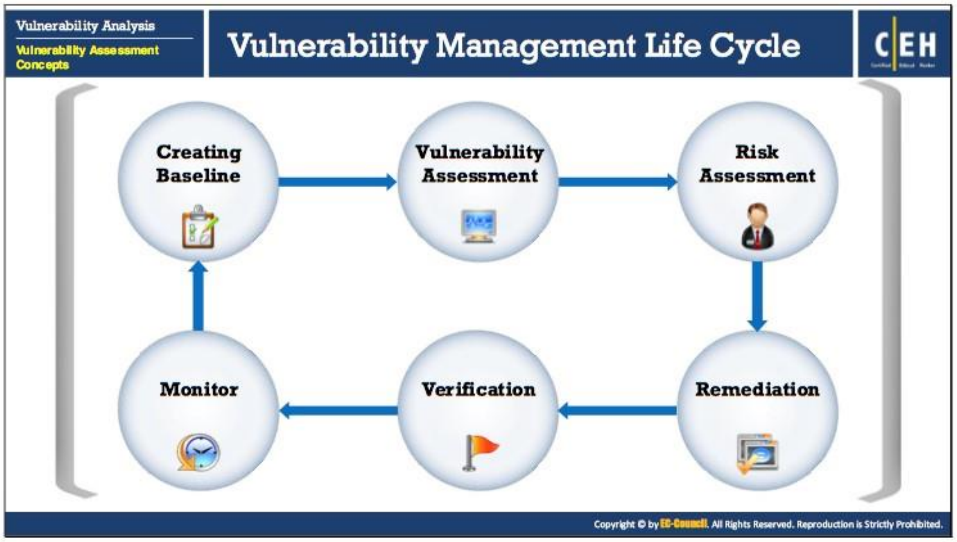
- Checks the network topologies for inappropriate firewall configuration
- Examines the router filtering rules
- Identifies inappropriately configured database servers
- Tests individual services and protocols such as HTTP, SNMP, and FTP
- Reviews HTML source code for unnecessary information
- Performs bounds checking on variables

- **Application Assessments**

  An application assessment focuses on transactional Web applications, traditional client-server applications, and hybrid systems. It analyzes all elements of an application infrastructure, including deployment and communication within the client and server. This type of assessment tests the web server infrastructure for any misconfiguration, outdated content, and known vulnerabilities. Security professionals use both commercial and open-source tools to perform such assessments.

- **Wireless Network Assessments**

  Wireless network assessment determines the vulnerabilities in an organization's wireless networks. In the past, wireless networks used weak and defective data encryption mechanisms. Now, wireless network standards have evolved, but many networks still use the weak and outdated security mechanisms, and are open for attack. Wireless network assessments try to attack wireless authentication mechanisms and get unauthorized access. This type of assessment tests wireless networks and identifies rogue wireless networks that may exist within an organization's perimeter. These assessments audit client-specified sites with a wireless network. They sniff wireless network traffic and try to crack encryption keys. Auditors test other network access once they get access to the wireless network.



Vulnerability Analysis
Vulnerability Assessment Concepts

Vulnerability Management Life Cycle

Creating Baseline → Vulnerability Assessment → Risk Assessment → Remediation → Verification → Monitor → Creating Baseline

Vulnerability Management Life Cycle

Vulnerability management life cycle is an important process that helps in finding and remediating security weaknesses before they are exploited. This includes defining the risk posture and policies for an organization, creating a complete asset list of systems, scanning and assessing the environment for vulnerabilities and exposures, and taking action to mitigate the vulnerabilities that are found. The implementation of a vulnerability management lifecycle makes the insecure computing environments more resilient to attacks.

Vulnerability management should be implemented in every organization as it evaluates and controls the risks and vulnerabilities in the system. The management process continuously examines the IT environments for vulnerabilities and risks associated with the system.

Organizations should maintain a proper vulnerability management program for ensuring the overall information security. The vulnerability management provides best results if it is implemented in a sequence of well-organized phases.

The phases involved in vulnerability management are:

- **Creating Baseline**

  In this phase, critical assets are identified and prioritized to create a good baseline for the vulnerability management.

- **Vulnerability Assessment**

  This is a very crucial phase in vulnerability management. In this step, the security analyst identifies the known vulnerabilities in the organization infrastructure.

- **Risk Assessment**

  In this phase, all the serious uncertainties that are associated with the system are assessed, fixed, and permanently eliminated for ensuring a flaw free system. Risk assessment summarizes the vulnerability and risk level identified for each of the selected asset. It determines the risk level for a particular asset, whether it is high, moderate or low.

- **Remediation**

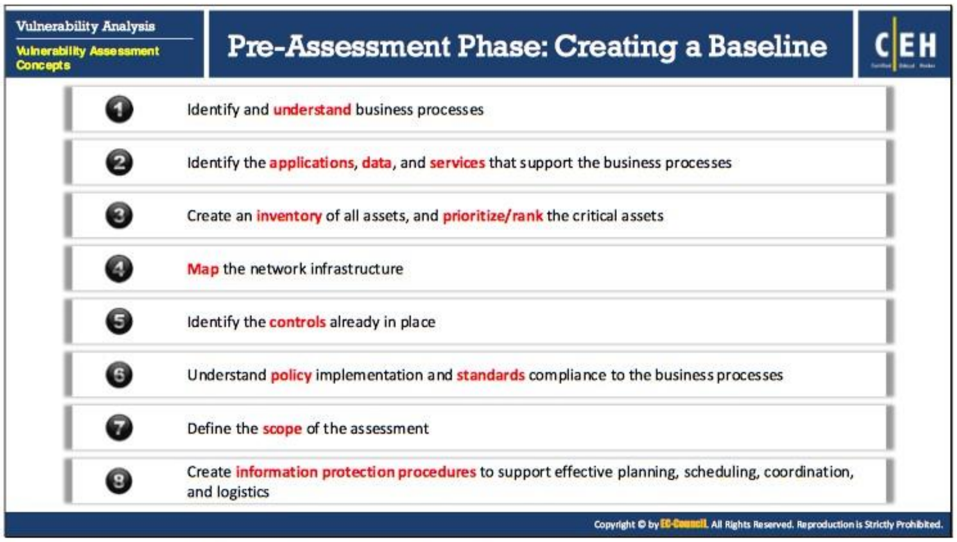
  Remediation is the process of reducing the severity of vulnerabilities. This phase is initiated after the successful implementation of the baseline and assessment steps.

- **Verification**

  This phase provides a clear visibility into the firm and allows the security team to check whether all the previous phases are perfectly employed or not. Verification can be performed by using various means such as ticking systems, scanners, reports, etc.

- **Monitor**

  Regular monitoring needs to be performed for maintaining the system security using tools such as IDS/IPS, firewalls, etc. Continuous monitoring identifies potential threats and any new vulnerabilities that have evolved.



Vulnerability Analysis

Vulnerability Assessment Concepts

Pre-Assessment Phase: Creating a Baseline

1. Identify and understand business processes
2. Identify the applications, data, and services that support the business processes
3. Create an inventory of all assets, and prioritize/rank the critical assets
4. Map the network infrastructure
5. Identify the controls already in place
6. Understand policy implementation and standards compliance to the business processes
7. Define the scope of the assessment
8. Create information protection procedures to support effective planning, scheduling, coordination, and logistics

Pre-Assessment Phase: Creating a Baseline

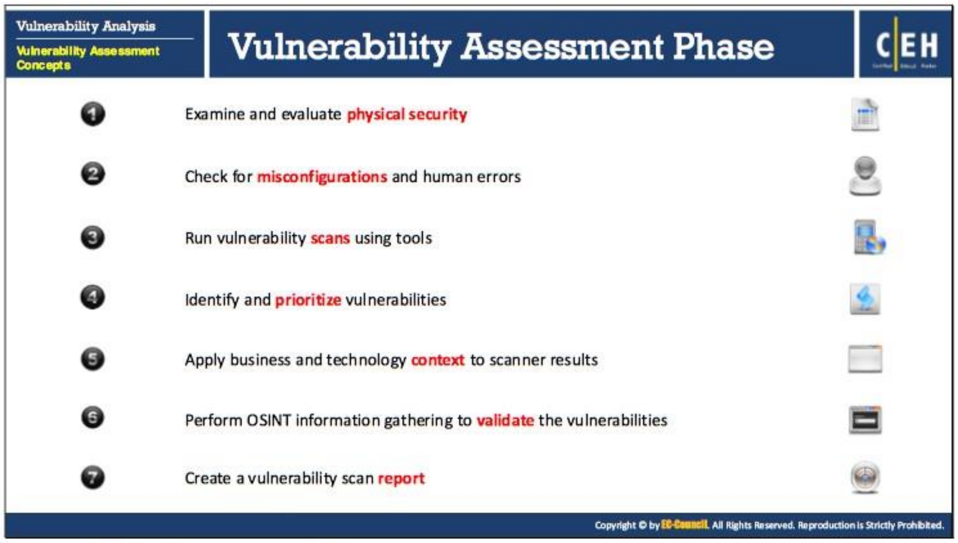
Pre-assessment phase refers to the preparatory phase, which includes defining policies and standards, defining the scope of assessment, designing appropriate information protection procedure, and identifying and prioritizing the critical assets to create a good baseline for the vulnerability management.

Steps involved in creating a baseline:

1. Identify and understand business processes
2. Identify the applications, data, and services that support the business processes
3. Create an inventory of all assets, and prioritize/rank the critical assets
4. Map the network infrastructure
5. Identify the controls already in place
6. Understand policy implementation and standards compliance to the business processes
7. Define the scope of the assessment
8. Create information protection procedures to support effective planning, scheduling, coordination, and logistics

Classify the identified assets, according to the business needs. Classification helps in identifying the high business risks in an organization. Prioritize the rated assets based on the impact of their failure and on the reliability of those assets in the business. Prioritization helps:

- Evaluating and deciding a solution for the consequence of the assets failing
- Examining the risk tolerance level
- Organizing the methods for prioritizing the assets



Vulnerability Analysis
Vulnerability Assessment Concepts

Vulnerability Assessment Phase

1. Examine and evaluate **physical security**
2. Check for **misconfigurations** and human errors
3. Run vulnerability **scans** using tools
4. Identify and **prioritize** vulnerabilities
5. Apply business and technology **context** to scanner results
6. Perform OSINT information gathering to **validate** the vulnerabilities
7. Create a vulnerability scan **report**

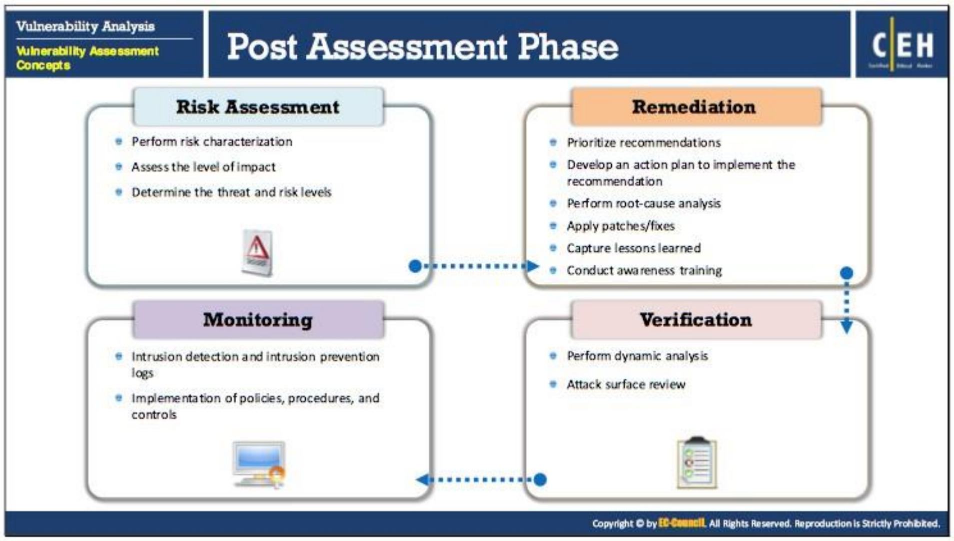
Vulnerability Assessment Phase

Vulnerability assessment phase refers to identifying vulnerabilities in the organization infrastructure including the operating system, web applications, web server, etc. It helps identify the category and criticality of the vulnerability in an organization and minimizes the levels of risk. The ultimate goal of vulnerability scanning includes scanning, examining, evaluating and reporting the vulnerabilities in the organization information system.

The assessment phase involves examining the architecture of the network, evaluating the threats to the environment, performing penetration testing, examining and evaluating physical security, analyzing physical assets, assessing operational security, observing policies and procedures, and assessing the infrastructure's interdependencies.

Steps involved in assessment phase:

1. Examine and evaluate physical security
2. Check for misconfigurations and human errors
3. Run vulnerability scans using tools
4. Identify and prioritize vulnerabilities
5. Apply business and technology context to scanner results
6. Perform OSINT information gathering to validate the vulnerabilities
7. Create a vulnerability scan report



Vulnerability Analysis
Vulnerability Assessment Concepts

Post Assessment Phase

Risk Assessment

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

Remediation

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

Verification

- Perform dynamic analysis
- Attack surface review

Monitoring

- Intrusion detection and intrusion prevention logs
- Implementation of policies, procedures, and controls

Post Assessment Phase

Post assessment phase is also known as the recommendation phase, which is performed after the risk assessment. Post-assessment is based on the risk assessment. Risk characterization is categorized by the key criteria, which helps to prioritize the list of recommendations.

The tasks performed in post assessment phase include:

- Making a priority list for assessment recommendations
- Developing an action plan to implement the proposed recommendation
- Capturing lessons learned to improve the complete process in the future
- Conducting training for the employees

Post assessment includes risk assessment, remediation, verification, and monitoring.

- **Risk Assessment**

  In the risk assessment phase, risks are identified, characterized, and classified along with the techniques used to control or reduce the impact of the risks. It is an important step to identify the security weaknesses in the IT architecture of an organization.

  The tasks performed in the risk assessment phase include:

  - Perform risk characterization
  - Assess the level of impact
  - Determine the threat and risk level

- **Remediation**

  Remediation refers to the steps that are taken to mitigate the found vulnerabilities such as evaluating vulnerabilities, locating risks, and designing responses for the vulnerabilities, etc. It is important for remediation process to be specific, measurable, attainable, relevant and time-bound.

  The tasks performed in the remediation phase include:

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

- **Verification**

  The verification phase helps the security analysts to verify whether all the previous phases are perfectly employed or not. This phase includes the verification of remedies that were taken for the mitigation of risks.

  The tasks performed in the verification phase include:

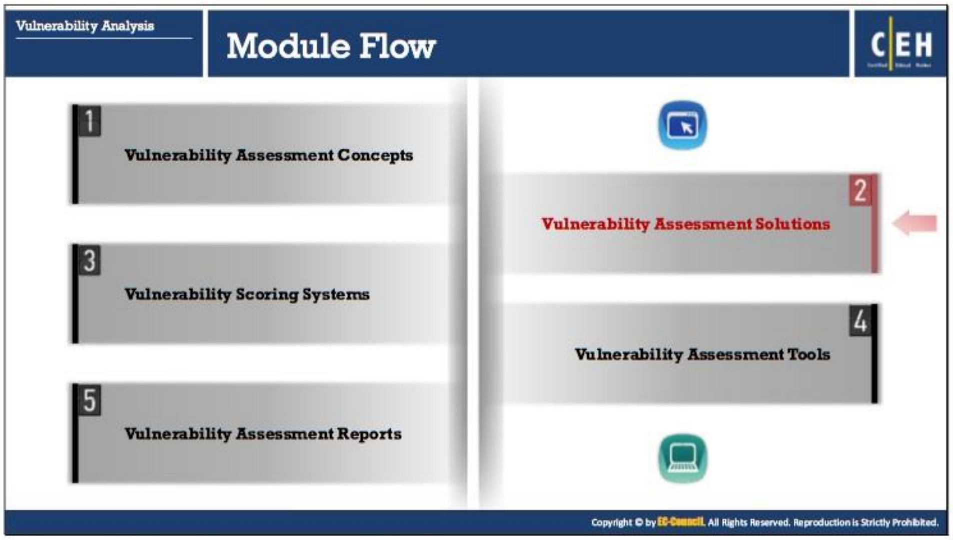
  - Perform dynamic analysis
  - Attack surface review

- **Monitoring**

  In this phase, incident monitoring is performed using tools such as IDS/IPS, SIEM, firewalls, etc. This phase implements continuous security monitoring to thwart ever evolving threats.

  The tasks performed in the monitoring phase include:

  - Monitoring intrusion detection and intrusion prevention logs
  - Implementation of policies, procedures, and controls



Vulnerability Analysis

Module Flow

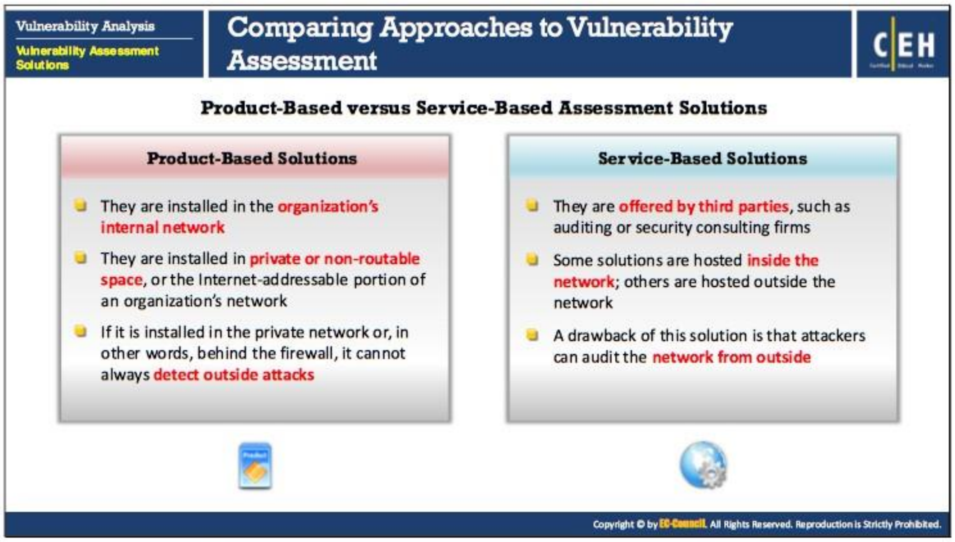
1
Vulnerability Assessment Concepts
2
Vulnerability Assessment Solutions
3
Vulnerability Scoring Systems
4
Vulnerability Assessment Tools
5
Vulnerability Assessment Reports

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Assessment Solutions

Vulnerability assessment solution is an important tool for information security management as it identifies all the security weaknesses before an attacker can exploit them. There are different approaches and solutions available to perform vulnerability assessment. Selecting an appropriate assessment approach plays a major role to mitigate the threats an organization is facing.

This section outlines various approaches and solutions used to perform vulnerability assessment.



Vulnerability Analysis
Vulnerability Assessment Solutions

Comparing Approaches to Vulnerability Assessment

Product-Based versus Service-Based Assessment Solutions

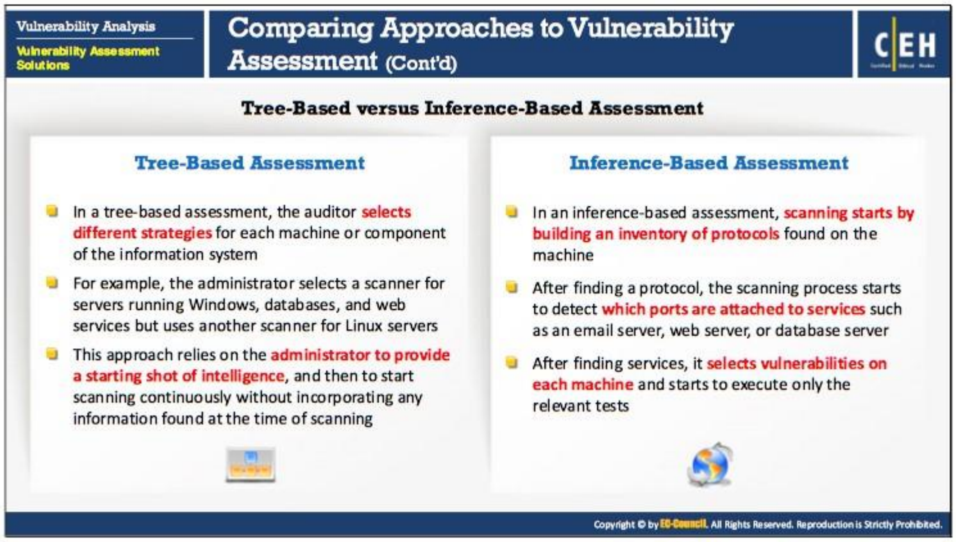
Product-Based Solutions

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

Service-Based Solutions

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Vulnerability Analysis
Vulnerability Assessment Solutions

Comparing Approaches to Vulnerability Assessment (Cont'd)

Tree-Based versus Inference-Based Assessment

Tree-Based Assessment

- In a 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 but uses another scanner for Linux servers
- This approach relies on the **administrator to provide a starting shot of intelligence**, and then to start scanning continuously without incorporating any information found at the time of scanning

Inference-Based Assessment

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Comparing Approaches to Vulnerability Assessment

There are four types of vulnerability assessment solutions: product-based solutions, service-based solutions, tree-based assessment, and inference-based assessment.

- **Product-Based Solutions**

  Product-based solutions are installed in the organization's internal network. They are installed in a private or non-routable space, or the Internet-addressable portion of an organization's network. If they are installed in the private network or, in other words, behind the firewall, they cannot always detect outside attacks.

- **Service-Based Solutions**

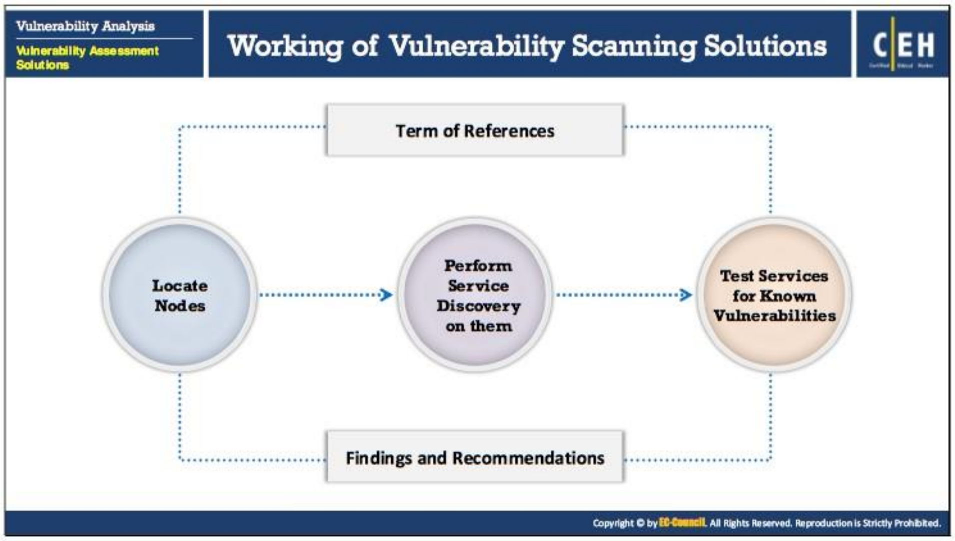
  Service-based solutions are offered by third parties, such as auditing or security consulting firms. Some solutions are hosted inside the network; others are hosted outside the network. A drawback of this solution is that attackers can audit the network from outside.

- **Tree-Based Assessment**

  In a 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 but uses another scanner for Linux servers. This approach relies on the administrator to provide a starting shot of intelligence, and then to start scanning continuously without incorporating any information found at the time of scanning.

- **Inference-Based Assessment**

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



Vulnerability Analysis
Vulnerability Assessment Solutions

Working of Vulnerability Scanning Solutions

Term of References

Locate Nodes

Perform Service Discovery on them

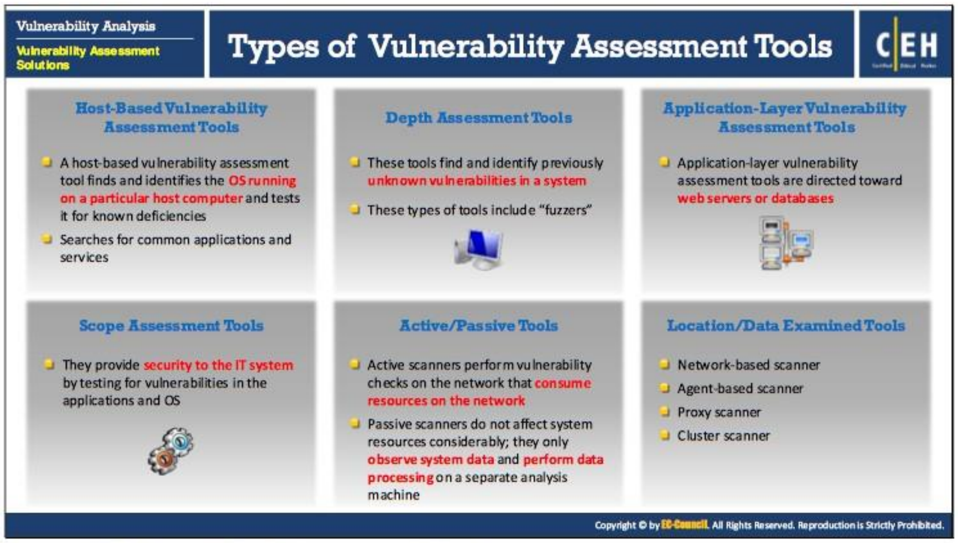
Test Services for Known Vulnerabilities

Findings and Recommendations

Working of Vulnerability Scanning Solutions

Any organization needs to handle and process large volumes of data in order to carry out business. These large volumes of data contain the information of that particular organization for which access is denied to the unauthorized users. Attackers try to find certain vulnerabilities that they can exploit and use those to gain access to the critical data for illegal purposes. Vulnerability analysis performs a study on the risk-prone areas of the organizational network. This analysis is done using various tools. The vulnerability analysis reports on the vulnerabilities present in the network. Vulnerability scanning solutions perform vulnerability penetration tests on the organizational network in three steps:

- **Locating nodes**: The first step in vulnerability scanning is to locate live hosts in the target network using various scanning techniques.
- **Performing service discovery on them**: After detecting live hosts in the target network, the next step is to enumerate open ports and services on the target systems.
- **Testing those services for known vulnerabilities**: Finally, after identifying open services, these services are tested for known vulnerabilities.



Vulnerability Analysis

Vulnerability Assessment Solutions

Types of Vulnerability Assessment Tools

C|EH

Host-Based Vulnerability Assessment Tools

- A host-based vulnerability assessment tool 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

- These tools find and identify previously unknown vulnerabilities in a system
- These types of tools include "fuzzers"

Application-Layer Vulnerability Assessment Tools

- Application-layer vulnerability assessment tools are directed toward web servers or databases

Scope Assessment Tools

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

Active/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/Data Examined Tools

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

Types of Vulnerability Assessment Tools

There are six types of vulnerability assessment tools: host-based vulnerability assessment tools, application-layer vulnerability assessment tools, depth assessment tools, scope assessment tools, active/passive tools, and location/data-examined tools.

- **Host-Based Vulnerability Assessment Tools**

  The host-based scanning tools are apt for servers that run various applications such as the web, critical files, databases, directories, and remote accesses. These host-based scanners are able to detect high levels of vulnerabilities and provide the required information of the fixes (patches). A host-based vulnerability assessment tool finds and identifies the OS running on a particular host computer and tests it for known deficiencies. It also searches for common applications and services.

- **Depth Assessment Tools**

  Depth assessment tools are used to find and identify previously unknown vulnerabilities in a system. Generally, these tools are used to identify vulnerabilities to an unstable degree of depth. Such types of tools include fuzzers that give arbitrary input to a system's interface. Many of these tools use a set of vulnerability signatures for testing that the product is resistant to a known vulnerability or not.

- **Application-Layer Vulnerability Assessment Tools**

  Application-layer vulnerability assessment tools are designed to serve the needs of all kinds of operating system types and applications. Various resources pose a variety of security threats and are identified by the tools designed for that purpose. Observing system vulnerabilities through the Internet using an external router, firewall, and web server, is called external vulnerability assessment. These vulnerabilities could be external

DoS/DDoS threats, network data interception, etc. The assessment for vulnerabilities is performed and the resources that are vulnerable are noted. The network vulnerability information is updated regularly into the tools. Application-layer vulnerability assessment tools are directed towards web servers or databases.

- **Scope Assessment Tools**

  Scope assessment tools provides assessment of the security by testing vulnerabilities in the applications and operating system. These tools provide a standard control and a reporting interface that allows the user to select a suitable scan. These tools generate a standard report of the information found. Some assessment tools are designed to test a specific application or its type for vulnerability.

- **Active/Passive Tools**

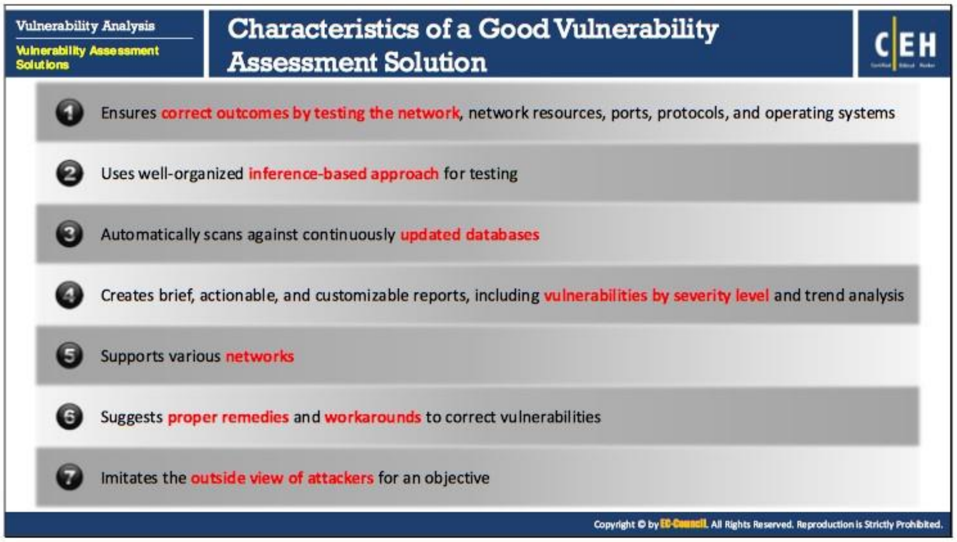
  Active scanners perform vulnerability checks on the network that consume resources on the network. The main advantage of the active scanner is that the system administrator or IT manager has good control of the timing and the degree of vulnerability scans. This scanner cannot be used for critical operating systems because it uses system resources that affect the processing of other tasks.

  Passive scanners are those that do not affect system resources considerably, as they only observe system data and perform data processing on a separate analysis machine. A passive scanner first receives system data that provides complete information on processes that are running and then assesses that data against the set of rules.

- **Location/Data Examined Tools**

  Listed below are some of the location/data examined tools:

  - **Network-Based Scanner:** Network-based scanners are those that interact only with the real machine where they reside and give the report to the same machine after scanning.
  - **Agent-Based Scanner:** Agent-based scanners reside on a single machine but have the ability to scan a number of machines on the same network.
  - **Proxy Scanner:** Proxy scanners are the network-based scanners that have the ability to scan networks from any machine in the network.
  - **Cluster scanner:** Cluster scanners are similar to proxy scanners but have the ability to perform two or more scans on different machines simultaneously in the network.



Vulnerability Analysis
Vulnerability Assessment Solutions

Characteristics of a Good Vulnerability Assessment Solution

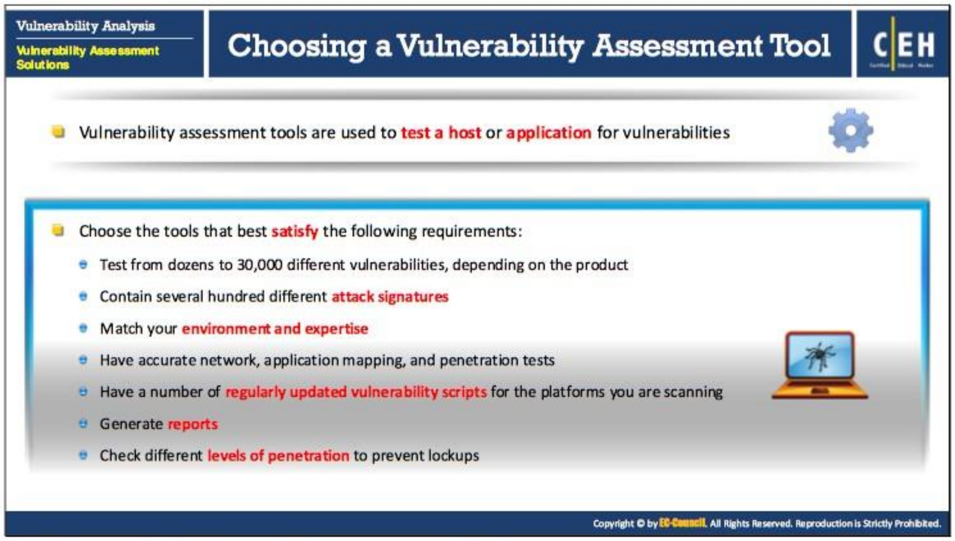
1. Ensures correct outcomes by testing the network, network resources, ports, protocols, and operating systems
2. Uses well-organized inference-based approach for testing
3. Automatically scans against continuously updated databases
4. Creates brief, actionable, and customizable reports, including vulnerabilities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

Characteristics of a Good Vulnerability Assessment Solution

Organizations need to select a proper and suitable vulnerability assessment solution to detect, assess, and protect their critical IT assets from various internal and external threats.

The characteristics of a good vulnerability assessment solution are as follows:

- Ensures correct outcomes by testing the network, network resources, ports, protocols, and operating systems
- Uses well-organized inference-based approach for testing
- Automatic scan against constantly updated databases
- Creates brief, actionable, customizable reports, including reports of vulnerabilities by severity level and trend analysis
- Supports various networks
- Suggests proper remedies and workarounds to correct vulnerabilities
- Imitates the outside view of attackers for an objective



Vulnerability Analysis
Vulnerability Assessment Solutions

Choosing a Vulnerability Assessment Tool

C|EH

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

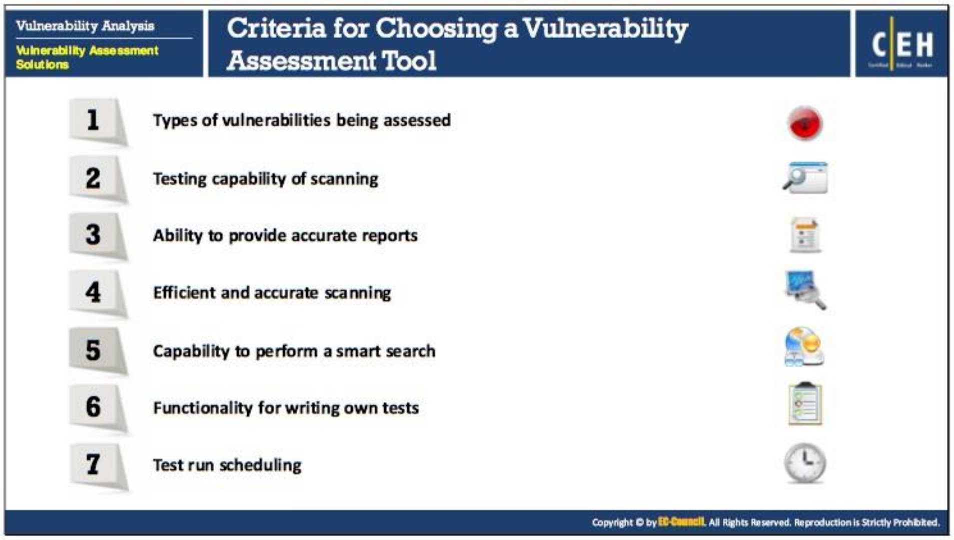
- Choose the tools that best **satisfy** the following requirements:
  - Test from dozens to 30,000 different vulnerabilities, depending on the product
  - Contain several hundred different **attack signatures**
  - Match your **environment and expertise**
  - Have accurate network, application mapping, and penetration tests
  - Have a number of **regularly updated vulnerability scripts** for the platforms you are scanning
  - Generate **reports**
  - Check different **levels of penetration** to prevent lockups

Choosing a Vulnerability Assessment Tool

Vendor-designed vulnerability assessment tools can be used to test a host or application for vulnerabilities. There are several vulnerability assessment tools available that include port scanners, vulnerability scanners, and OS vulnerability assessment scanners. Organizations have to choose the right tools based on their test requirements.

Choose the tools that best satisfy the following requirements:

- Tools must be capable of testing dozens to 30,000 different vulnerabilities, depending on the product
- The selected tool should have a sound database of vulnerabilities and attack signatures that are updated frequently
- Pick a tool that matches your environment and expertise
- Verify that the vulnerability assessment tool you chose has accurate network mapping, application mapping, and penetration tests. Not all the tools can find the protocols running and analyze the network's performance.
- Ensure that the tool has a number of regularly updated vulnerability scripts for the platforms you are scanning
- Make sure the patches are applied, failing which might lead to false positives
- Find out how many reports you get, what information they contain, and whether you can export the reports
- Check whether the tool has different levels of penetration to stop lockups
- Maintenance cost of the tools can be utilized by effectively using the tools



Vulnerability Analysis
Vulnerability Assessment Solutions

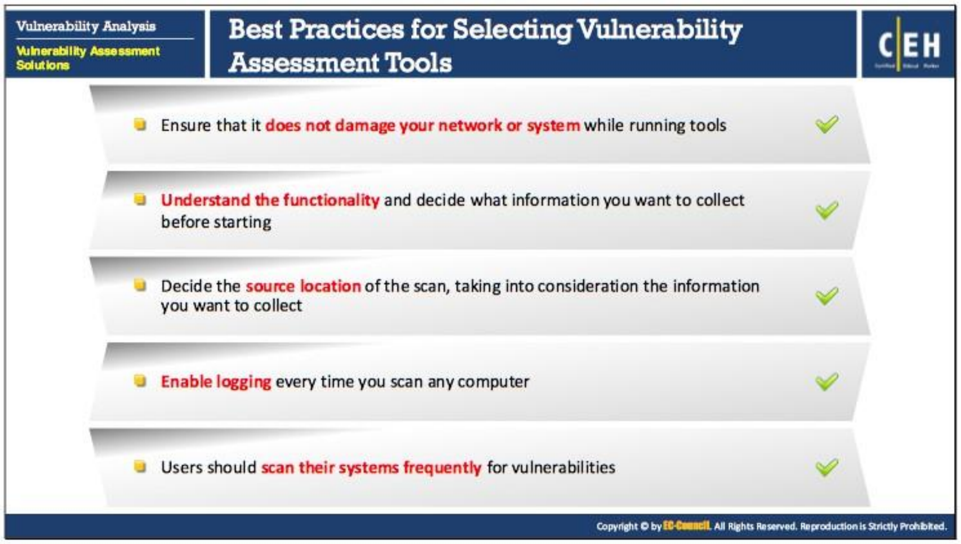
Criteria for Choosing a Vulnerability Assessment Tool

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 own tests
7. Test run scheduling

Criteria for Choosing a Vulnerability Assessment Tool

The criteria to be followed at the time of choosing or purchasing any vulnerability assessment tool are as follows:

- **Types of vulnerabilities being assessed:** The most important information at the time of evaluating any tool is to find out how many types of vulnerabilities it will discover.
- **Testing capability of scanning:** The vulnerability assessment tool must have the capacity to execute the entire selected test and must scan all the systems selected for scanning.
- **Ability to provide accurate reports:** Ability to prepare an accurate report is essential. Vulnerability reports should be short, clear, and should provide an easy method to mitigate the discovered vulnerability.
- **Efficient and accurate scanning:** There are two aspects of performance. The first one is how much time it takes for a single host and what resources they require. The second one is the loss of services at the time of scanning. It is important to ensure how accurate they are and what accurate results they give.
- **Capability to perform smart search:** How clever they are at the time of scanning is also a key factor in judging any vulnerability assessment tool.
- **Functionality for writing own tests:** When a signature is not present for a recently found vulnerability, it is helpful if the vulnerability scanning tool allows user-developed tests to be used.
- **Test run scheduling:** It is important to be able to do test run scheduling as it allows users to perform scanning when traffic on the network is light.



Vulnerability Analysis

Vulnerability Assessment Solutions

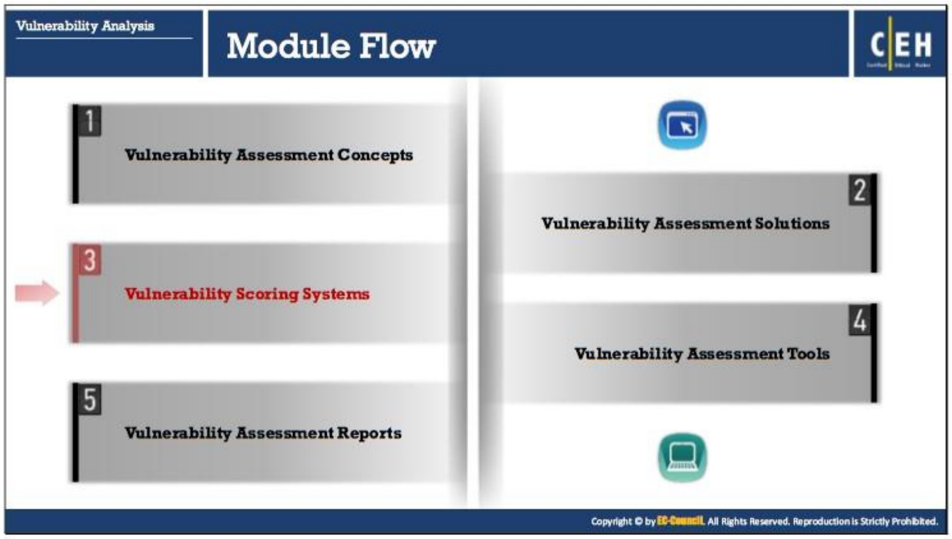
Best Practices for Selecting Vulnerability Assessment Tools

- Ensure that it **does not damage your network or system** while running tools ✓
- **Understand the functionality** and decide what information you want to collect before starting ✓
- Decide the **source location** of the scan, taking into consideration the information you want to collect ✓
- **Enable logging** every time you scan any computer ✓
- Users should **scan their systems frequently** for vulnerabilities ✓

Best Practices for Selecting Vulnerability Assessment Tools

Some of the best practices that can be adopted for selecting vulnerability assessment tools are as follows:

- Vulnerability assessment tools are used to secure and protect the organization's system or network. Ensure that they do not damage your network or system while running.
- Before using any vulnerability assessment tools, it is important to understand their function and to decide what information you want to collect before starting
- Security mechanisms are somewhat different for accessing from within the network and from outside the network; so first decide the source of location for the scan based on what information you want to collect.
- At the time of scanning, enable the loggings every time you scan on every computer and ensure that all outcomes and methodologies are annotated
- Users should scan their systems frequently for vulnerabilities and regularly monitor them for vulnerabilities and exploits



Vulnerability Analysis

Module Flow

1 Vulnerability Assessment Concepts

2 Vulnerability Assessment Solutions

3 Vulnerability Scoring Systems

4 Vulnerability Assessment Tools

5 Vulnerability Assessment Reports

Vulnerability Scoring System

Vulnerability scoring systems and vulnerability databases are used by security analysts to rank information system vulnerabilities, and to provide a composite score of the overall severity and risk associated with identified vulnerabilities. Vulnerability databases collect and maintain information about various vulnerabilities present in the information systems.

This section discusses Common Vulnerability Scoring System (CVSS), and vulnerability databases like Common Vulnerabilities and Exposures (CVE), and National Vulnerability Database (NVD).

Vulnerability Analysis
Vulnerability Scoring Systems

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 see the **underlying vulnerability characteristics** that were 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

Base Score Metrics

Exploitability Metrics

Impact Metrics

Temporal Score Metrics

https://nvd.nist.gov

Common Vulnerability Scoring System (CVSS)

Source: *https://www.first.org*, *https://nvd.nist.gov*

CVSS is a published standard that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Its quantitative model ensures repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability impact scores. Two common uses of CVSS are prioritization of vulnerability remediation activities and in calculating the severity of vulnerabilities discovered on one's systems. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.

CVSS provides a way to capture the principal characteristics of a vulnerability, and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

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.

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

TABLE 5.1: CVSS v3.0 ratings

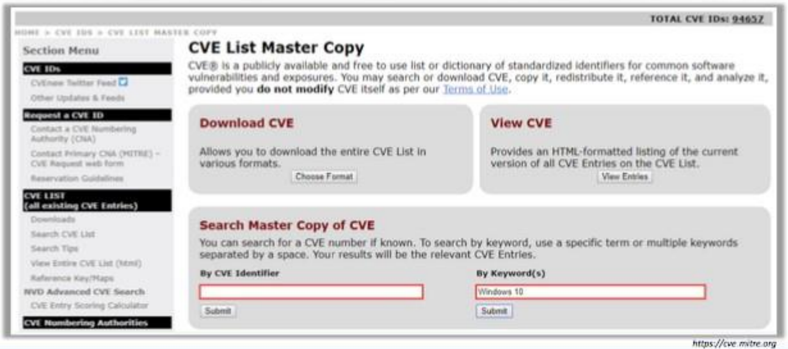
Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10

TABLE 5.2: CVSS v2.0 ratings

Vulnerability Analysis
Vulnerability Scoring Systems

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


TOTAL CVE IDs: 94657
HOME > CVE IDS > CVE LIST MASTER COPY
Section Menu
CVE IDs
CVEnew Twitter Feed
Other Updates & Feeds
Request a CVE ID
Contact a CVE Numbering Authority (CNA)
Contact Primary CNA (MITRE) – CVE Request web form
Reservation Guidelines
CVE LIST (all existing CVE Entries)
Downloads
Search CVE List
Search Tips
View Entire CVE List (html)
Reference Key/Maps
NVD Advanced CVE Search
CVE Entry Scoring Calculator
CVE Numbering Authorities
Choose Format
View Entries
Submit
Submit

CVE List Master Copy

CVE® is a publicly available and free to use list or dictionary of standardized identifiers for common software vulnerabilities and exposures. You may search or download CVE, copy it, redistribute it, reference it, and analyze it, provided you **do not modify** CVE itself as per our Terms of Use.

Download CVE

Allows you to download the entire CVE List in various formats.

View CVE

Provides an HTML-formatted listing of the current version of all CVE Entries on the CVE List.

Search Master Copy of CVE

You can search for a CVE number if known. To search by keyword, use a specific term or multiple keywords separated by a space. Your results will be the relevant CVE Entries.

By CVE Identifier:

By Keyword(s): Windows 10

https://cve.mitre.org

Common Vulnerabilities and Exposures (CVE)

Source: *https://cve.mitre.org*

CVE® is a publicly available and free to use list or dictionary of standardized identifiers for common software vulnerabilities and exposures. Use of CVE Identifiers, or "CVE IDs," which are assigned by CVE Numbering Authorities (CNAs) from around the world, ensures confidence among parties when used to discuss or share information about a unique software or firmware vulnerability, provides a baseline for tool evaluation, and enables data exchange for cyber security automation. CVE IDs also provide a baseline for evaluating the coverage of tools and services so that users can determine which tools are most effective and appropriate for their organization's needs. In short, products and services compatible with CVE provide better coverage, easier interoperability, and enhanced security.

What CVE is:

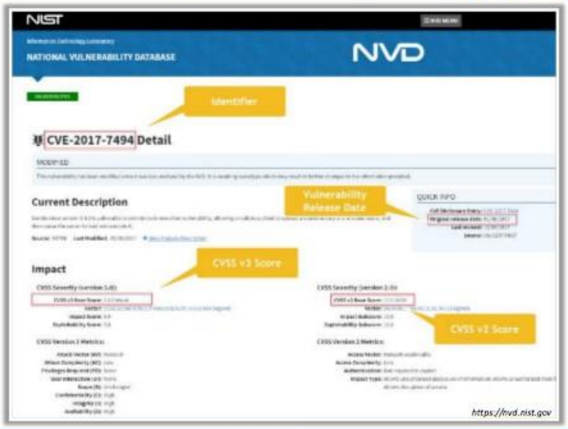
- One identifier for one vulnerability or exposure
- One standardized description for each vulnerability or exposure
- A dictionary rather than a database
- How disparate databases and tools can "speak" the same language
- The way to interoperability and better security coverage
- A basis for evaluation among services, tools, and databases
- Free for public to download and use
- Industry-endorsed via the CVE Numbering Authorities, CVE Board, and numerous products and services that include CVE

Vulnerability Analysis
Vulnerability Scoring Systems

National Vulnerability Database (NVD)

C|EH

- The NVD is the **U.S. government repository** of standards based vulnerability management data represented using the **Security Content Automation Protocol** (SCAP)
- This data **enables 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



National Vulnerability Database (NVD)

Source: *https://nvd.nist.gov*

The NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables 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.

The NVD performs analysis on CVEs that have been published to the CVE Dictionary. NVD staff are tasked with analysis of CVEs by aggregating data points from the description, references supplied and any supplemental data that can be found publicly at the time. This analysis results in association impact metrics (Common Vulnerability Scoring System - CVSS), vulnerability types (Common Weakness Enumeration - CWE), and applicability statements (Common Platform Enumeration - CPE), as well as other pertinent metadata. The NVD does not actively perform vulnerability testing, relying on vendors, third party security researchers and vulnerability coordinators to provide information that is then used to assign these attributes.

Vulnerability Analysis
Vulnerability Scoring Systems

Resources for Vulnerability Research

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

Security Magazine
https://www.securitymagazine.com

SecurityFocus
https://www.securityfocus.com

Help Net Security
https://www.net-security.org

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

SC Magazine
https://www.scmagazine.com

Computerworld
https://www.computerworld.com

WindowsSecurity
http://www.windowsecurity.com

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

CVE Details
https://www.cvedetails.com

Security Tracker
https://securitytracker.com

Vulnerability Lab
https://www.vulnerability-lab.com

D'Crypt
https://www.d-crypt.com

Trend Micro
https://www.trendmicro.com

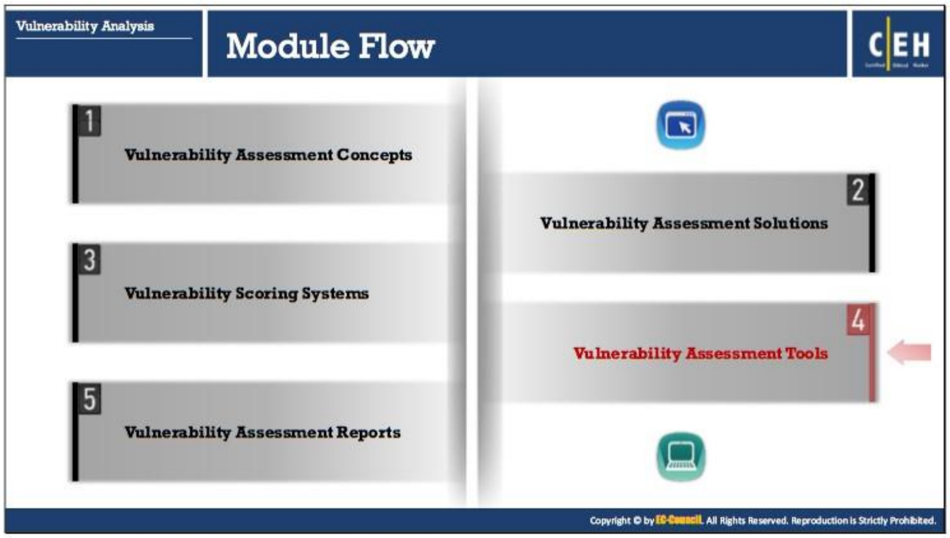
Rapid7
https://www.rapid7.com

Resources for Vulnerability Research

Due to a growing severity of cyber-attacks, vulnerability research has become the need of the hour as it helps to mitigate the chances of attacks. Vulnerability research provides awareness on advanced techniques to identify flaws or loopholes in the software that can be exploited by attackers.

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

- Microsoft Vulnerability Research (MSVR) (*https://technet.microsoft.com*)
- Security Magazine (*https://www.securitymagazine.com*)
- SecurityFocus (*https://www.securityfocus.com*)
- Help Net Security (*https://www.net-security.org*)
- HackerStorm (*http://www.hackerstorm.co.uk*)
- SC Magazine (*https://www.scmagazine.com*)
- Computerworld (*https://www.computerworld.com*)
- WindowsSecurity (*http://www.windowsecurity.com*)
- Exploit Database (*https://www.exploit-db.com*)
- CVE Details (*https://www.cvedetails.com*)
- Security Tracker (*https://securitytracker.com*)
- Vulnerability Lab (*https://www.vulnerability-lab.com*)
- D'Crypt (*https://www.d-crypt.com*)
- Trend Micro (*https://www.trendmicro.com*)
- Rapid7 (*https://www.rapid7.com*)
- Dark Reading (*https://www.darkreading.com*)



Vulnerability Analysis

Module Flow

1 Vulnerability Assessment Concepts

2 Vulnerability Assessment Solutions

3 Vulnerability Scoring Systems

4 Vulnerability Assessment Tools

5 Vulnerability Assessment Reports

Vulnerability Assessment Tools

An attacker performs vulnerability scanning in order to identify security loopholes in the target network that he/she can exploit to launch attacks. Security analysts can use vulnerability assessment tools to identify weaknesses present in the organization's security posture and remediate the identified vulnerabilities before an attacker exploits.

Network vulnerability scanners help in analyzing and identifying vulnerabilities in the target network or network resources by means of vulnerability assessment and network auditing. These tools also assist in overcoming weaknesses in the network by suggesting various remediation techniques.

This section describes vulnerability scanning using various vulnerability assessment tools.

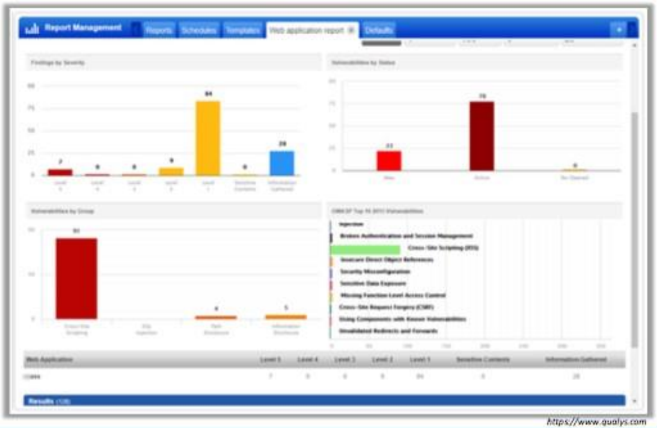
Vulnerability Analysis
Vulnerability Assessment Tools

Qualys Vulnerability Management

C|EH

- Qualys VM is a cloud-based service that gives you immediate global visibility into where your IT systems might be **vulnerable to the latest Internet threats** and how to protect them
- It helps you to continuously **identify threats and monitor unexpected changes** in your network before they turn into breaches

Qualys.


Report Management
Reports
Schedules
Templates
Web application report
Defaults
Findings by Severity
84
28
Vulnerabilities by Status
78
Vulnerabilities by Group
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
Web Application
Level 5
Level 4
Level 3
Level 2
Level 1
Sensitive Contents
Information Gathered
Results

https://www.qualys.com

Qualys Vulnerability Management

Source: *https://www.qualys.com*

Qualys VM is a cloud-based service that gives you immediate, global visibility into where your IT systems might be vulnerable to the latest Internet threats and how to protect them. It helps you to continuously identify threats and monitor unexpected changes in your network before they turn into breaches.

Features:

- **Agent-based detection**

  It also works with the Qualys Cloud Agents, extending its network coverage to assets that cannot be scanned.

- **Constant monitoring and alerts**

  When VM is paired with Continuous Monitoring (CM), InfoSec teams are proactively alerted about potential threats so problems can be tackled before turning into breaches.

- **Comprehensive coverage and visibility**

  It continuously scans and identifies vulnerabilities, protecting your IT assets on premises, in the cloud and mobile endpoints. Its executive dashboard displays an overview of your security posture and access to remediation details. VM generates custom, role-based reports for multiple stakeholders, including automatic security documentation for compliance auditors.

- **VM for the perimeter-less world**

  As enterprises adopt cloud computing, mobility, and other disruptive technologies for digital transformation, Qualys VM offers next-generation vulnerability management for these hybrid IT environments whose traditional boundaries have been blurred.

- **Discover forgotten devices and organize your host assets**

  With Qualys, you can quickly determine what is actually running in the different parts of your network—from your perimeter and corporate network to virtualized machines and cloud services. Uncover unexpected access points, web servers and other devices that can leave your network open to attack.

- **Scan for vulnerabilities everywhere, accurately and efficiently**

  Scan systems anywhere from the same console: your perimeter, your internal network, and cloud environments.

- **Identify and prioritize risks**

  Using Qualys, you can identify the highest business risks using trend analysis, Zero-Day and Patch impact predictions.

- **Remediate vulnerabilities**

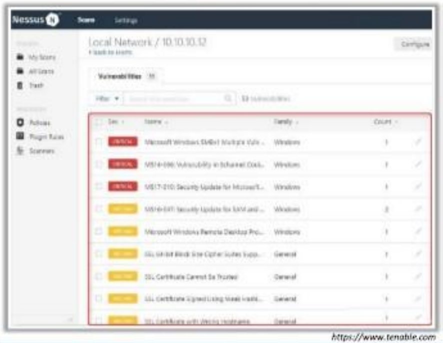
  Qualys' ability to track vulnerability data across hosts and time lets you use reports interactively to better understand the security of your network.

Vulnerability Analysis
Vulnerability Assessment Tools

Vulnerability Assessment Tools: Nessus Professional and GFI LanGuard

Nessus Professional

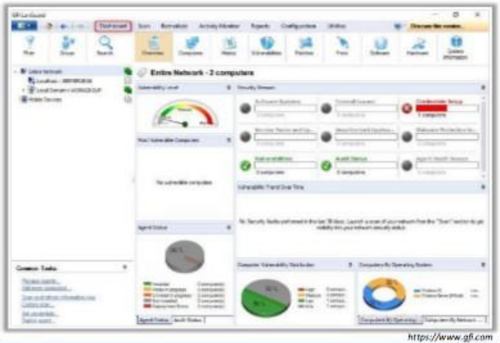
- Nessus Professional is an assessment solution for **identifying the vulnerabilities**, **configuration issues**, and **malware**



https://www.tenable.com

GFI LanGuard

- GFI LanGuard scans, detects, assesses and rectifies **security vulnerabilities** in your network and connected devices



https://www.gfi.com

Nessus Professional

Source: *https://www.tenable.com*

Nessus Professional is an assessment solution for identifying vulnerabilities, configuration issues, and malware that attackers use to penetrate networks. It performs vulnerability, configuration, and compliance assessment. It supports various technologies such as operating systems, network devices, hypervisors, databases, tablets/phones, web servers and critical infrastructure.

Nessus is the vulnerability scanning platform for auditors and security analysts. Users can schedule scans across multiple scanners, use wizards to easily and quickly create policies, schedule scans and send results via email.

Features:

- High-speed asset discovery
- Vulnerability assessment
- Malware/Botnet detection
- Configuration and compliance auditing
- Scanning and auditing of virtualized and cloud platforms

GFI LanGuard

Source: *https://www.gfi.com*

GFI LanGuard scans, detects, assesses and rectifies security vulnerabilities in your network and connected devices. It scans the network and ports to detect, assess, and correct security vulnerabilities, with minimal administrative effort. It scans your operating systems, virtual environments and installed applications through vulnerability check databases. It enables you to analyze the state of your network security, identify risks and address how to take action before it is compromised.

Features:

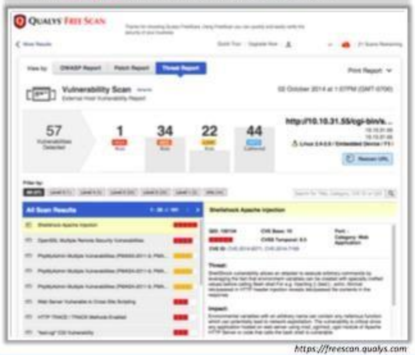
- Patch management for operating systems and third-party applications
- Vulnerability assessment
- Web reporting console
- Track latest vulnerabilities and missing updates
- Integration with security applications
- Network device vulnerability checks
- Network and software auditing
- Support for virtual environments

Vulnerability Analysis
Vulnerability Assessment Tools

Vulnerability Assessment Tools: Qualys FreeScan and Nikto

Qualys FreeScan

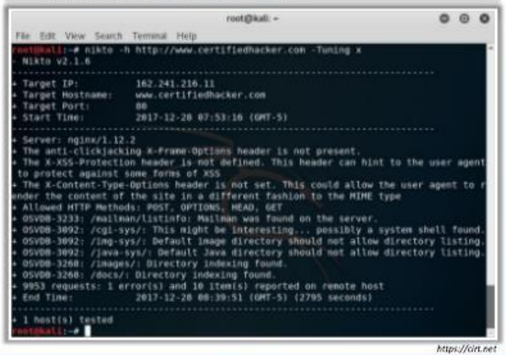
- Qualys FreeScan service **scans your network, servers, desktops** and **web apps** for security threats and vulnerabilities



https://freescan.qualys.com

Nikto

- Nikto is a **web server assessment tool** which examines a web server to find potential problems and security vulnerabilities



```
root@kali:~# nikto -h http://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:         2017-12-28 07:53:16 (GMT-5)
---------------------------------------------------------------------------
+ Server: nginx/1.12.2
+ 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 agent to r
ender the content of the site in a different fashion to the MIME type
+ Allowed HTTP Methods: POST, OPTIONS, HEAD, GET
+ OSVDB-3233: /mailman/listinfo: Mailman was found on the server.
+ OSVDB-3092: /cgi-sys/: This might be interesting... possibly a system shell found.
+ OSVDB-3092: /img-sys/: Default image directory should not allow directory listing.
+ OSVDB-3092: /java-sys/: Default Java directory should not allow directory listing.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /docs/: Directory indexing found.
+ 9953 requests: 1 error(s) and 10 item(s) reported on remote host
+ End Time:           2017-12-28 08:39:51 (GMT-5) (2795 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali:~# 
```

https://cirt.net

Qualys FreeScan

Source: *https://freescan.qualys.com*

Qualys FreeScan service enables you to safely and accurately scan your network, servers, desktops and web apps for security threats and vulnerabilities. It is a free vulnerability scanner and network security tool for business networks. FreeScan is limited to ten (10) unique security scans of Internet accessible assets. It provides a detailed report that can be used to correct and fix security threats proactively.

Features:

- Scans computers and apps on the Internet or in the network
- Detects security vulnerabilities and the patches needed to fix them
- Enables viewing of interactive scan reports by threat or by patch
- Tests websites and apps for OWASP Top Risks and malware
- Tests computers against SCAP security benchmarks

Nikto

Source: *https://cirt.net*

Nikto is an Open Source (GPL) web server scanner that performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software.

Features:

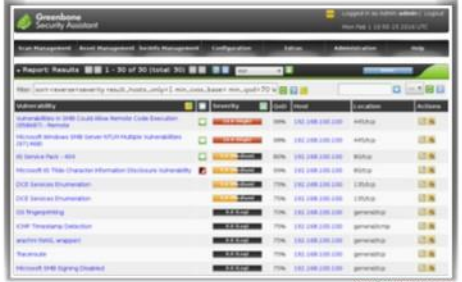
- SSL Support (Unix with OpenSSL or maybe Windows with ActiveState's Perl/NetSSL)
- Full HTTP proxy support
- Checks for outdated server components
- Saves reports in plain text, XML, HTML, NBE or CSV
- Template engine to easily customize reports
- Scans multiple ports on a server, or multiple servers via input file
- LibWhisker's IDS encoding techniques
- Identifies installed software via headers, favicons and files
- Host authentication with Basic and NTLM
- Subdomain guessing
- Apache and cgiwrap username enumeration
- Scan tuning to include or exclude entire classes of vulnerability checks
- Guesses credentials for authorization realms (including many default id/pw combos)

Vulnerability Analysis
Vulnerability Assessment Tools

Vulnerability Assessment Tools: OpenVAS and Retina CS

OpenVAS

- OpenVAS is a framework of several services and tools offering a comprehensive and powerful **vulnerability scanning** and **vulnerability management solution**



http://www.openvas.org

Retina CS

- Retina CS is a vulnerability management software solution designed to provide organizations with **context-aware vulnerability assessment** and **risk analysis**

https://www.beyondtrust.com

OpenVAS

Source: *http://www.openvas.org*

OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. The framework is part of Greenbone Networks' commercial vulnerability management solution from which developments are contributed to the Open Source community since 2009.

The actual security scanner is accompanied with a regularly updated feed of Network Vulnerability Tests (NVTs), over 50,000 in total.

Retina CS

Source: *https://www.beyondtrust.com*

Retina CS is a vulnerability management software solution designed to provide organizations with context-aware vulnerability assessment and risk analysis. Retina's result-oriented architecture works with users to proactively identify security exposures, analyze business impact, and plan and conduct remediation across disparate and heterogeneous infrastructure. Retina CS Enterprise Vulnerability Management software enables you to:

- Discover network, web, mobile, cloud, virtual and IoT infrastructure
- Profile asset configuration and risk potential
- Pinpoint vulnerabilities, malware and attacks
- Analyze threat potential and return on remediation
- Remediate vulnerabilities via integrated patch management (optional)
- Report on vulnerabilities, compliance, benchmarks, etc.
- Protect endpoints against client-side attacks

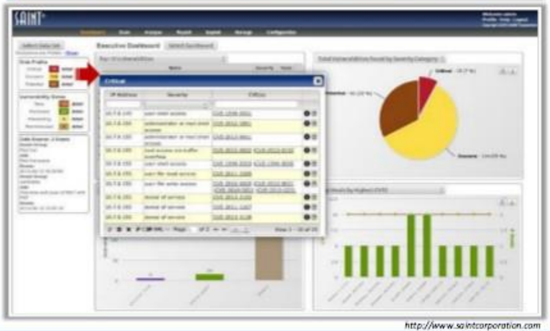
Vulnerability Analysis
Vulnerability Assessment Tools

Vulnerability Assessment Tools: SAINT and Microsoft Baseline Security Analyzer (MBSA)

C|EH

SAINT

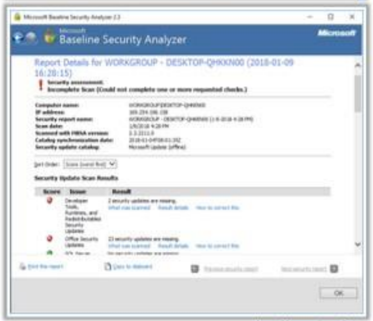
SAINT's **vulnerability management capabilities** identify operating system and software vulnerabilities and patch deficiencies, web applications vulnerabilities and risk exposures, state of anti-virus installations, configuration assessments, etc.



http://www.saintcorporation.com

Microsoft Baseline Security Analyzer (MBSA)

MBSA lets administrators **scan local and remote systems** for missing security updates as well as common security misconfigurations



Microsoft Baseline Security Analyzer

Report Details for WORKGROUP - DESKTOP-QHKKN00 (2018-01-09 16:20:15)

Security assessment:
Incomplete Scan (Could not complete one or more requested checks.)

Computer name:
IP address:
Security report name:
Scan date:
Scanned with MBSA version:
Catalog synchronization date:
Security update catalog:

Security Update Scan Results

Score	Issue	Result
	Developer Tools, Runtimes, and Redistributables Security Updates	2 security updates are missing.
	Office Security Updates	23 security updates are missing.

https://www.microsoft.com

SAINT

Source: *http://www.saintcorporation.com*

As a vulnerability assessment solution, SAINT's security research and development efforts focus on investigation, triage, prioritization and coverage of vulnerabilities of the highest severity. It performs risk analysis, and remediation and continuous monitoring. SAINT provides a robust set of capabilities to discover assets across the enterprise, and create asset tags based on your specific needs – to enable assessments and remediation activities that are directed at the highest priority assets and exposures. SAINT's vulnerability management capabilities identify operating system and software vulnerabilities and patch deficiencies, Microsoft Patch Tuesday assessments, web applications vulnerabilities and risk exposures, state of anti-virus installations, configuration assessments based on industry-standard best-practices, exposure of sensitive content, etc.

Microsoft Baseline Security Analyzer (MBSA)

Source: *https://www.microsoft.com*

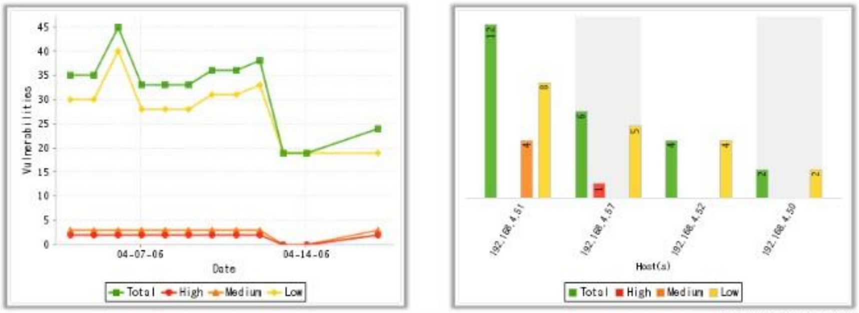
Microsoft Baseline Security Analyzer (MBSA) is a tool designed for IT professionals and helps small- and medium-sized businesses to determine their security state in accordance with Microsoft security recommendations. It lets administrators scan local and remote systems for missing security updates as well as common security misconfigurations. MBSA includes a graphical and command line interface that can perform local or remote scans of Microsoft Windows systems. To assess missing security updates, MBSA will only scan for missing security updates, update rollups and service packs available from Microsoft Update.

Vulnerability Analysis
Vulnerability Assessment Tools

AVDS - Automated Vulnerability Detection System

C|EH

- AVDS tests every node according to its characteristics and records system responses to reveal **security issues** in equipment, operating systems, and applications



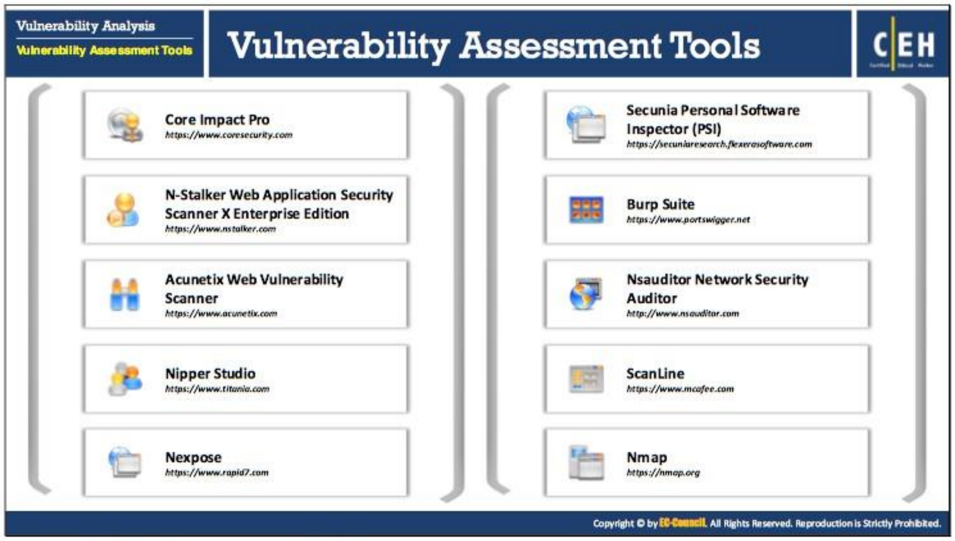
https://www.beyondsecurity.com

AVDS - Automated Vulnerability Detection System

Source: *https://www.beyondsecurity.com*

AVDS is a network vulnerability assessment appliance for networks of 50 to 200,000 nodes. It performs an in-depth inspection for security weaknesses that can replace exhaustive penetration testing. With each scan, it will automatically find new equipment and services and add them to the inspection schedule. AVDS then tests every node based on its characteristics and records the system's responses to reveal security issues in equipment, operating systems and applications. You set the IP range to investigate and in a matter of hours and with no network down time or interruption of services our vulnerability assessment tool will generate detailed reports specifying network security weaknesses.

AVDS conducts automated vulnerability assessment scans daily, weekly or monthly, or on ad-hoc basis. It records results and generates vulnerability trends for your entire WAN, a LAN or a single IP address. With three levels of reporting, each business unit can receive a report on its own network and local results can be combined into a company-wide picture.



Vulnerability Analysis
Vulnerability Assessment Tools

Vulnerability Assessment Tools

CEH

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

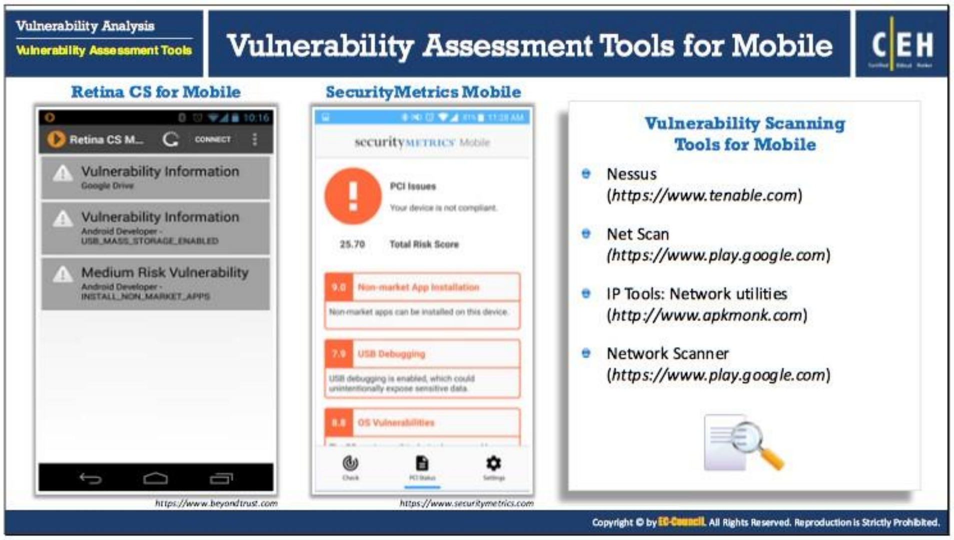
ScanLine
https://www.mcafee.com

Nmap
https://nmap.org

Vulnerability Assessment Tools

Listed below are some of the 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*)



Vulnerability Assessment Tools for Mobile

Retina CS for Mobile

Vulnerability Information
Google Drive

Vulnerability Information
Android Developer -
USB_MASS_STORAGE_ENABLED

Medium Risk Vulnerability
Android Developer -
INSTALL_NON_MARKET_APPS

https://www.beyondtrust.com

SecurityMetrics Mobile

PCI Issues
Your device is not compliant.

25.70 Total Risk Score

9.0 Non-market App Installation
Non-market apps can be installed on this device.

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

8.8 OS Vulnerabilities

https://www.securitymetrics.com

Vulnerability Scanning Tools for Mobile

- Nessus (*https://www.tenable.com*)
- Net Scan (*https://www.play.google.com*)
- IP Tools: Network utilities (*http://www.apkmonk.com*)
- Network Scanner (*https://www.play.google.com*)

Vulnerability Assessment Tools for Mobile

- **Retina CS for Mobile**

  Source: *https://www.beyondtrust.com*

  Retina CS for Mobile is the industry's innovative approach to security, policy, and health management for mobile devices. It provides comprehensive vulnerability management for mobile devices, smart phones, and tablets. It integrates mobile device assessment and vulnerability management for proactively discovering, prioritizing, and fixing smartphone security weaknesses.

  Features:

  - Reduce risk across BlackBerry, Android, and ActiveSync-managed mobile devices
  - Access reports locally via the mobile app and alongside enterprise vulnerability data in the BeyondInsight console
  - Ease compliance via in-depth mobile vulnerability management audit trails
  - Reveal vulnerability profiles of mobile devices accessing the network
  - Streamline remediation through severity-based mobile threat prioritization
  - Audit mobile device hardware, applications, and configurations
  - Rely on automatic vulnerability audit updates from BeyondSaaS

- **SecurityMetrics Mobile**

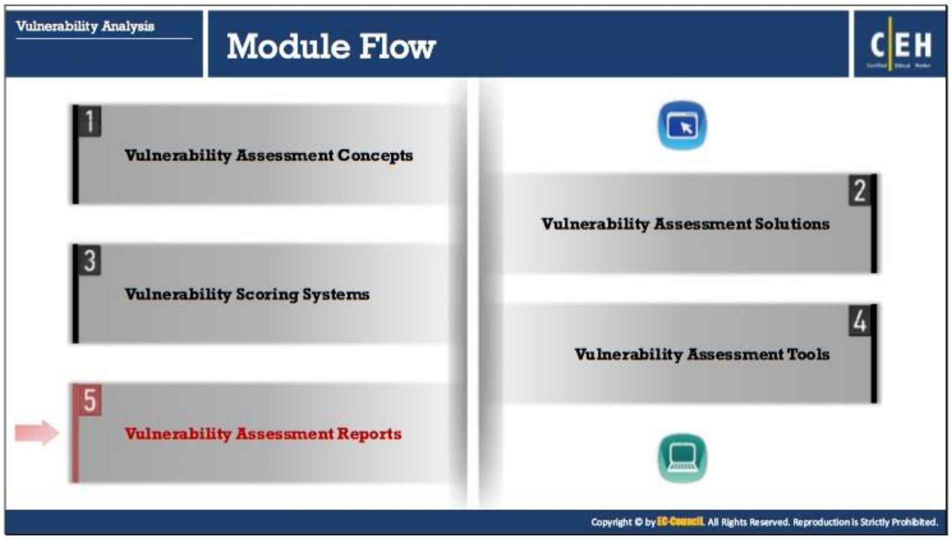
  Source: *https://www.securitymetrics.com*

  SecurityMetrics Mobile is a mobile defense tool that helps to identify mobile device vulnerabilities to protect the customer's sensitive data. It helps to avoid threats that originate from mobile malware, device theft, Wi-Fi network connectivity, data entry, personal and business use, unwarranted app privileges, data and device storage, account data access, Bluetooth, Infrared (IR), Near-field communication (NFC), and SIM and SD cards.

  SecurityMetrics MobileScan complies with PCI SSC (Payment Card Industry Security Standards Council) guidelines to prevent mobile data theft. On completion of a scan, the report generated comprises of a total risk score, summarization of discovered vulnerabilities, and recommendations on how to resolve threats.

Listed below are some of the vulnerability scanning tools for mobile devices:

- Nessus (*https://www.tenable.com*)
- Net Scan (*https://www.play.google.com*)
- IP Tools: Network utilities (*http://www.apkmonk.com*)
- Network Scanner (*https://www.play.google.com*)



Vulnerability Analysis

Module Flow

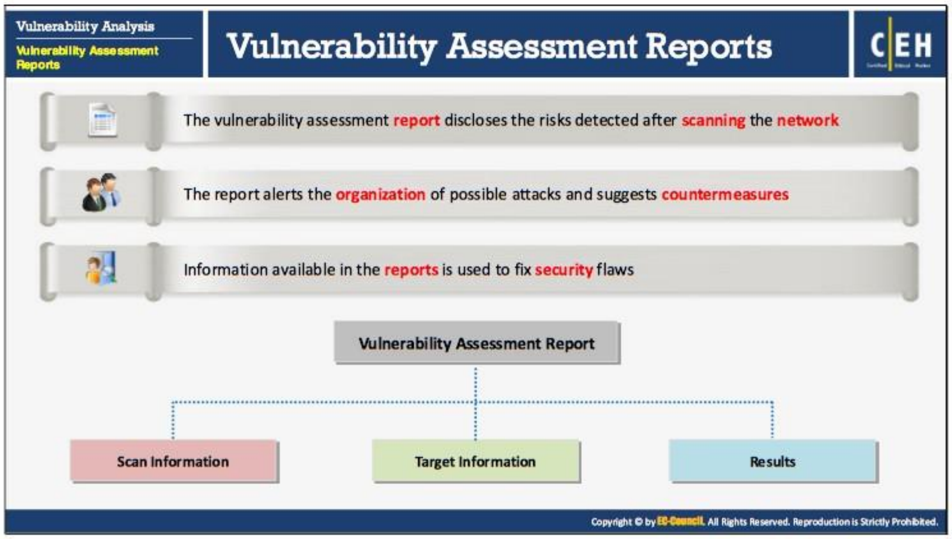
1 Vulnerability Assessment Concepts

2 Vulnerability Assessment Solutions

3 Vulnerability Scoring Systems

4 Vulnerability Assessment Tools

5 Vulnerability Assessment Reports



Vulnerability Analysis
Vulnerability Assessment Reports

Vulnerability Assessment Reports

- The vulnerability assessment report discloses the risks detected after scanning the network
- The report alerts the organization of possible attacks and suggests countermeasures
- Information available in the reports is used to fix security flaws

Vulnerability Assessment Report

Scan Information

Target Information

Results

Vulnerability Assessment Reports

In the vulnerability assessment process, once all the phases are completed, the security team will review the results and process the information to prepare the final report. In this phase, the security team will try to disclose any identified vulnerabilities, document any variations and findings and include all these in the final report along with remediation steps to mitigate the identified risks.

The vulnerability assessment report discloses the risks that are detected after scanning the network. Tools such as Nessus, GFI LanGuard, and Qualys Vulnerability Management are used for vulnerability assessment. These tools provide a comprehensive assessment report in a specified format. The report alerts the organization to possible attacks and suggests countermeasures.

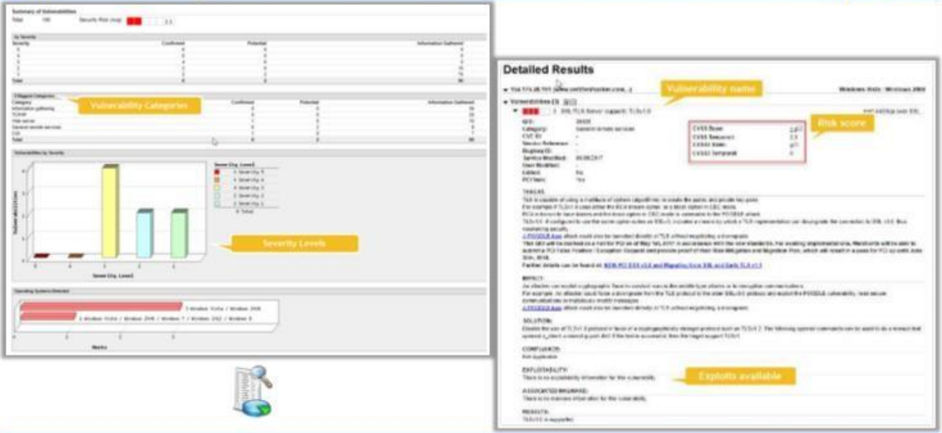
The report provides details of all the possible vulnerabilities with regard to the company's security policies. The vulnerabilities are categorized based on severity into three levels: High, Medium, and Low risks.

High-risk vulnerabilities are those with the possibility of allowing unauthorized access into the network. These vulnerabilities need to be rectified immediately, before the network is compromised. The report describes different kinds of attacks that are possible given the organization's set of operating systems, network components, and protocols.

Vulnerability Analysis

Vulnerability Assessment Reports

Analyzing Vulnerability Scanning Report



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Vulnerability Scanning Report

A vulnerability assessment report will provide detailed information on the vulnerabilities that are found in the computing environment. The report will help organizations to identify the security posture found in the computing systems (such as web servers, firewalls, routers, email, and file services) and provide solutions to reduce failures in the computing system.

The assessment report helps organizations to take mitigation steps to proactively avoid the risks by identifying, tracking and eliminating the security vulnerabilities.

Vulnerability reports cover the following elements:

- **Scan information**: This part of the report provides information such as the name of the scanning tool, its version, and the network ports that have to be scanned.
- **Target information**: This part of the report contains information about the target system's name and address.
- **Results**: This section provides a complete scanning report. It contains subtopics such as target, services, vulnerability, classification, and assessment.
- **Target**: This subtopic includes each host's detailed information. It contains the following information:
  - **<Node>**: Contains the name and address of the host
  - **<OS>**: Shows the operating system type
  - **<Date>**: Gives the data of the test
- **Services**: The subtopic defines the network services by their names and ports.

- **Classification**: This subtopic allows the system administrator to obtain additional information about the scanning such as origin of the scan.
- **Assessment**: This class provides information regarding the scanner's assessment of the vulnerability.

Vulnerability assessment reports are classified into two types:

- Security Vulnerability Report
- Security Vulnerability Summary

Security Vulnerability Report

This is a combined report for all the scanned devices and servers in the organization's network.

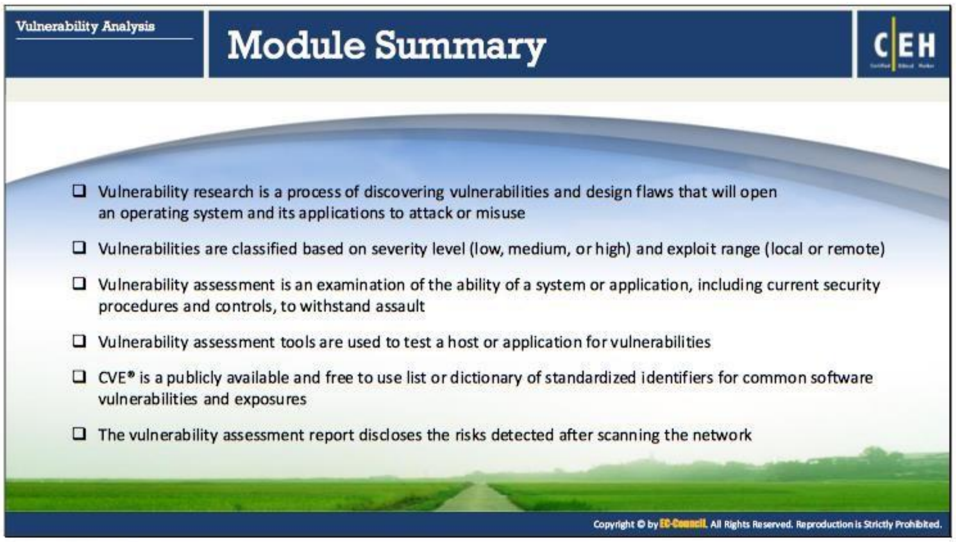
The security vulnerability report includes the following details:

- Newly found vulnerability
- Open port and detected services
- Suggestion for remediation
- Links to patches

Security Vulnerability Summary

This report is produced for every device or server after scanning. It gives the summary of the scan result that includes the following elements:

- Current security flaws
- Categories of vulnerabilities
- New security vulnerabilities detected
- Severity of vulnerabilities
- Resolved vulnerabilities



Vulnerability Analysis

Module Summary

- □ Vulnerability research is a 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)
- □ Vulnerability assessment is an examination of the ability of a system or application, including current security procedures and controls, to withstand assault
- □ Vulnerability assessment tools are used to test a host or application for vulnerabilities
- □ CVE® is a publicly available and free to use list or dictionary of standardized identifiers for common software vulnerabilities and exposures
- □ The vulnerability assessment report discloses the risks detected after scanning the network

Module Summary

This module familiarized you with various topics related to vulnerability assessment, such as its concepts, types, solutions, tools and criteria for proper tool selection, vulnerability scoring systems, and vulnerability assessment reports.

In the next module, we will see how attackers as well as ethical hackers and pen testers attempt system hacking based on the information collected about a target of evaluation from footprinting, scanning, enumeration, and vulnerability analysis phases.