



Ethical Hacking Essentials (EHE)

1 Master of Science in Cybersecurity



Dr. Kamal Alieyan

Everyone Smart University

Faculty of IT – 2022/2023

Module 03

Information Security Threats and Vulnerability Assessment



Module Objectives

- 1 Understanding the Threat and Threat Sources
- 2 Understanding Malware and Components of Malware
- 3 Overview of Common Techniques Attackers use to Distribute Malware on the Web
- 4 Overview of Different Types of Malware and Malware Countermeasures
- 5 Understanding Vulnerability and Vulnerability Classification
- 6 Understanding Vulnerability Assessment and Types of Vulnerability Assessment
- 7 Overview of Vulnerability Scoring Systems and Vulnerability Management Life Cycle
- 8 Understanding Vulnerability Assessment Tools and Vulnerability Exploitation

Module Flow



1

**Define Threat and
Threat Sources**



2

**Define Malware
and its Types**



3

**Define
Vulnerabilities**



4

**Define Vulnerability
Assessment**





What is Vulnerability?

- ❑ Refers to the existence of **weakness** in an asset that can be exploited by threat agents



Common Reasons behind the Existence of Vulnerability

- 1 Hardware or software misconfiguration
- 2 Insecure or poor design of the network and application
- 3 Inherent technology weaknesses
- 4 Careless approach of end users

1

Misconfiguration



2

Default Installations



3

Buffer Overflows



4

Unpatched Servers



5

Design Flaws



6

Operating System
Flaws



Vulnerability Classification

7

Application Flaws



8

Open Services



9

Default Passwords



10

Zero-day/Legacy
Platform vulnerabilities



Examples of Network Security Vulnerabilities

Technological Vulnerabilities	Description
TCP/IP protocol vulnerabilities	☐ HTTP, FTP, ICMP, SNMP, SMTP are inherently insecure
Operating System vulnerabilities	☐ An OS can be vulnerable because: ▪ It is inherently insecure ▪ It is not patched with the latest updates
Network Device Vulnerabilities	☐ Various network devices such as routers, firewall, and switches can be vulnerable due to: ▪ Lack of password protection ▪ Lack of authentication ▪ Insecure routing protocols ▪ Firewall vulnerabilities



Examples of Network Security Vulnerabilities (Cont'd)



Configuration Vulnerabilities	Description
User account vulnerabilities	Originating from the insecure transmission of user account details such as usernames and passwords, over the network
System account vulnerabilities	Originating from setting of weak passwords for system accounts
Internet service misconfiguration	Misconfiguring internet services can pose serious security risks. For example, enabling JavaScript and misconfiguring IIS, Apache, FTP, and Terminal services, can create security vulnerabilities in the network
Default password and settings	Leaving the network devices/products with their default passwords and settings
Network device misconfiguration	Misconfiguring the network device

Examples of Network Security Vulnerabilities (Cont'd)

Security Policy Vulnerabilities	Description
Unwritten Policy	Unwritten security policies are difficult to implement and enforce
Lack of Continuity	Lack of continuity in implementing and enforcing the security policy
Politics	Politics may cause challenges for implementation of a consistent security policy
Lack of awareness	Lack of awareness of the security policy

Impact of Vulnerabilities

1

Information disclosure

2

Unauthorized access

3

Identity theft

4

Reputational damage

5

Financial loss

6

Legal consequences

7

Data modification



Module Flow



1
**Define Threat and
Threat Sources**



2
**Define Malware
and its Types**



3
**Define
Vulnerabilities**



4
**Define Vulnerability
Assessment**



Vulnerability Research

- ❑ The process of analyzing protocols, services, and configurations to **discover vulnerabilities and design flaws** that will expose an operating system and its applications to exploit, attack, or misuse

- ❑ Vulnerabilities are classified based on **severity level** (low, medium, or high) and **exploit range** (local or remote)



An administrator needs vulnerability research:

1

To gather information concerning **security trends, threats, attack surfaces**, attack vectors and techniques

2

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

3

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

4

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

Resources for Vulnerability Research



Microsoft Vulnerability Research (MSVR)

<https://www.microsoft.com>



Security Magazine

<https://www.securitymagazine.com>



SecurityFocus

<https://www.securityfocus.com>



Dark Reading

<https://www.darkreading.com>



PenTest Magazine

<https://pentestmag.com>



Help Net Security

<https://www.helpnetsecurity.com>



SecurityTracker

<https://securitytracker.com>



SC Magazine

<https://www.scmagazine.com>



HackerStorm

<http://www.hackerstorm.co.uk>



Trend Micro

<https://www.trendmicro.com>



Exploit Database

<https://www.exploit-db.com>



Computerworld

<https://www.computerworld.com>

What is Vulnerability Assessment?



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

A vulnerability assessment may be used to:

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

Information Obtained from the Vulnerability Scanning



OS version running on computers or devices



Open ports and running services



Application and services vulnerabilities



Application and services configuration errors



Accounts with weak passwords



Missing patches and hotfixes

Vulnerability Scanning Approaches

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 to identify vulnerabilities



Passive Scanning

- ☐ The attacker tries to find vulnerabilities **without directly interacting** with the target network
- ☐ **Example:** An attacker guesses the operating system information, applications, and application and service versions by observing the TCP connection setup and teardown

Vulnerability Scoring Systems and Databases

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

Common Vulnerability Scoring System (CVSS)

CVSS v3.0 Ratings

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

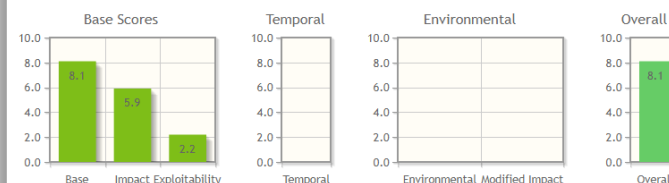
CVSS v2.0 Ratings

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

<https://www.first.org>

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

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



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

Show Equations

CVSS v3 Vector

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

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N) Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L) High (AC:H)

Privileges Required (PR)*

None (PR:N) Low (PR:L) High (PR:H)

User Interaction (UI)*

None (UI:N) Required (UI:R)

Scope (S)*

Unchanged (S:U) Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N) Low (C:L) High (C:H)

Integrity Impact (I)*

None (I:N) Low (I:L) High (I:H)

Availability Impact (A)*

None (A:N) Low (A:L) High (A:H)

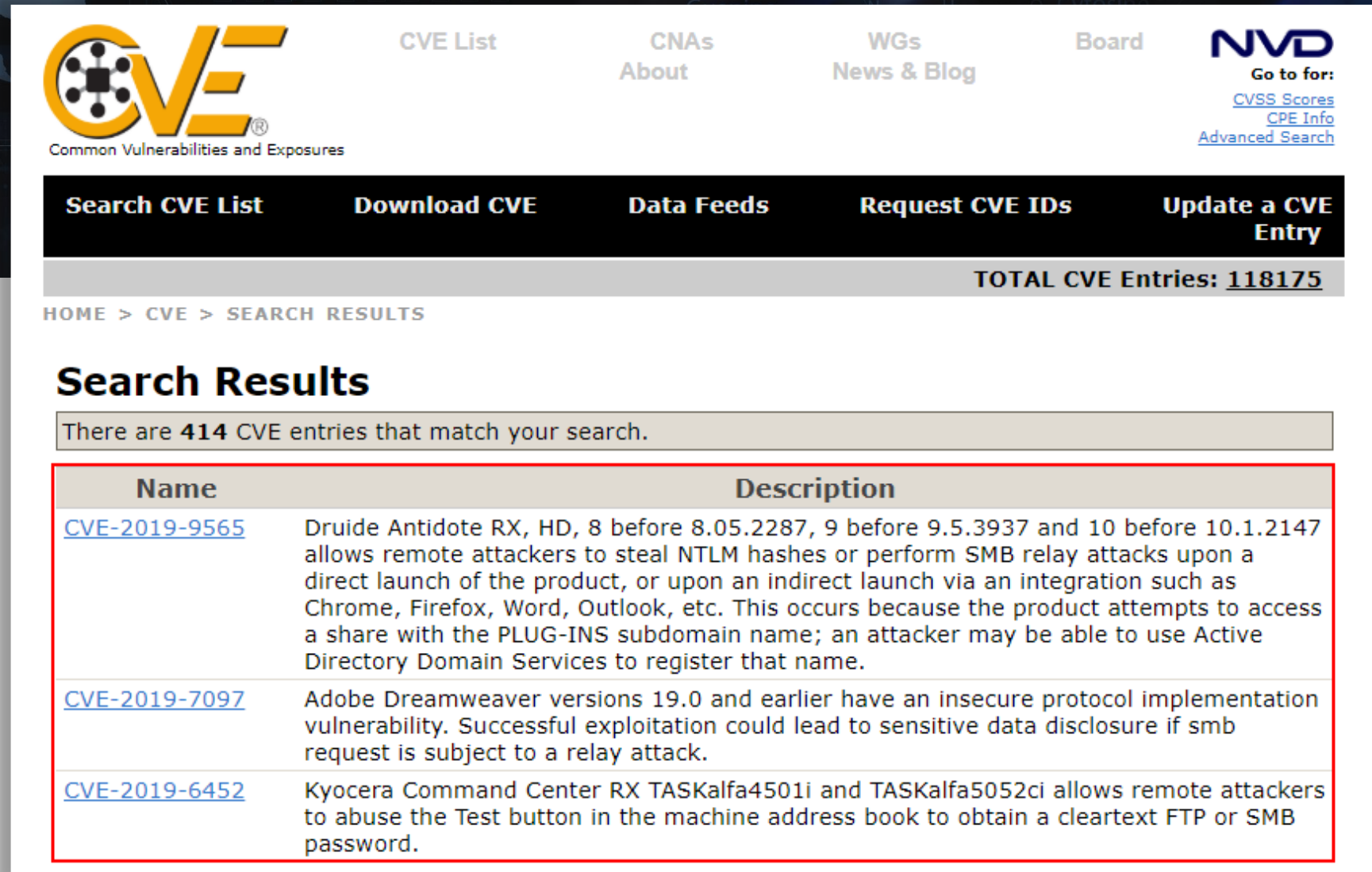
* - All base metrics are required to generate a base score.

<https://nvd.nist.gov>

Vulnerability Scoring Systems and Databases (Cont'd)

Common Vulnerabilities and Exposures (CVE)

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



The screenshot displays the CVE website interface. At the top, there is a navigation bar with links for 'CVE List', 'CNAs About', 'WGs News & Blog', and 'Board'. The CVE logo is prominently displayed on the left, with the text 'Common Vulnerabilities and Exposures' below it. On the right, there are links for 'NVD', 'Go to for: CVSS Scores', 'CPE Info', and 'Advanced Search'. Below the navigation bar, a black bar contains links for 'Search CVE List', 'Download CVE', 'Data Feeds', 'Request CVE IDs', and 'Update a CVE Entry'. A grey bar below this indicates 'TOTAL CVE Entries: 118175'. The main content area shows the breadcrumb 'HOME > CVE > SEARCH RESULTS' and the heading 'Search Results'. A message states 'There are 414 CVE entries that match your search.' Below this, a table lists three CVE entries:

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

<https://cve.mitre.org>

Vulnerability Scoring Systems and Databases (Cont'd)

National Vulnerability Database (NVD)

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

NIST
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE

VULNERABILITIES

CVE-2019-6452 Detail

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

Source: MITRE
[View Analysis Description](#)

Impact
CVSS v3.0 Severity and Metrics:
Base Score: 8.8 HIGH
Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H (V3 legend)
Impact Score: 5.9
Exploitability Score: 2.8

CVSS v3 Score

CVSS v2.0 Severity and Metrics:
Base Score: 4.0 MEDIUM
Vector: (AV:N/AC:L/Au:S/C:P/I:N/A:N) (V2 legend)
Impact Subscore: 2.9
Exploitability Subscore: 8.0

CVSS v2 Score

QUICK INFO
CVE Dictionary Entry: CVE-2019-6452
NVD Published Date: 06/06/2019
NVD Last Modified: 06/11/2019

Vulnerability Identifier

Vulnerability Published Date

<https://nvd.nist.gov>

Vulnerability Scoring Systems and Databases (Cont'd)



The screenshot shows the homepage of the Common Weakness Enumeration (CWE) website. The header includes the CWE logo, the title 'Common Weakness Enumeration', and the subtitle 'A Community-Developed List of Software Weakness Types'. A navigation bar contains links for Home, About, CWE List, Scoring, Community, News, and Search. A search bar is located in the top right corner. Below the navigation bar, a paragraph describes CWE as a community-developed list of common software security weaknesses. A button labeled 'View the List of Weaknesses' is present, with three sub-buttons: 'by Research Concepts', 'by Development Concepts', and 'by Architectural Concepts'. A 'Search CWE' section follows, with instructions on how to search. A search box contains the text 'SMB', and a magnifying glass icon is to its right. Below the search box, it says 'About 10 results (0.17 seconds)'. A red box highlights the first three search results: 'CWE-427: Uncontrolled Search Path Element (3.2) - CWE', 'CWE-130: Improper Handling of Length Parameter - CWE', and 'CWE-294: Authentication Bypass by Capture-replay (3.2) - CWE'. Each result includes a URL and a brief description. The URL 'https://cwe.mitre.org' is visible at the bottom right of the screenshot.

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

CWE and SANS Institute
TOP 25 MOST DANGEROUS SOFTWARE ERRORS

ID Lookup: Go

Home | About | CWE List | Scoring | Community | News | Search

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

View the List of Weaknesses

by Research Concepts | by Development Concepts | by Architectural Concepts

Search CWE

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

About 10 results (0.17 seconds)

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

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

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

<https://cwe.mitre.org>

Common Weakness Enumeration (CWE)



A **category system** for **software vulnerabilities and weaknesses**



It is sponsored by the **National Cybersecurity FFRDC**, which is owned by **The MITRE Corporation**, with support from **US-CERT** and the **National Cyber Security Division** of the **U.S. Department of Homeland Security**



It has over **600 categories** of weaknesses, which enable CWE to be effectively employed by the community as a **baseline for weakness identification, mitigation, and prevention efforts**

Types of Vulnerability Assessment



Active Assessment



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

External Assessment



Assesses the network from a hacker's perspective to discover exploits and vulnerabilities that are accessible to the outside world

Host-based Assessment



Conducts a **configuration-level check** to identify system configurations, user directories, file systems, registry settings, etc., to evaluate the possibility of compromise

Application Assessment



Tests and analyzes all elements of the **web infrastructure** for any **misconfiguration**, **outdated content**, or **known vulnerabilities**

Types of Vulnerability Assessment (Cont'd)

Used to **sniff the network traffic** to discover present active systems, network services, applications, and vulnerabilities present



Passive Assessment

Scans the **internal infrastructure** to discover exploits and vulnerabilities



Internal Assessment

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



Network-based Assessment

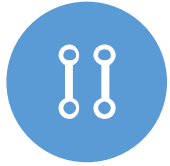
Focuses on testing databases, such as **MYSQL, MSSQL, ORACLE, POSTGRESQL**, etc., for the presence of **data exposure** or **injection** type vulnerabilities



Database Assessment



Types of Vulnerability Assessment (Cont'd)



Wireless Network Assessment

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



Distributed Assessment

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



Credentialed Assessment

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



Non-Credentialed Assessment

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



Manual Assessment

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



Automated Assessment

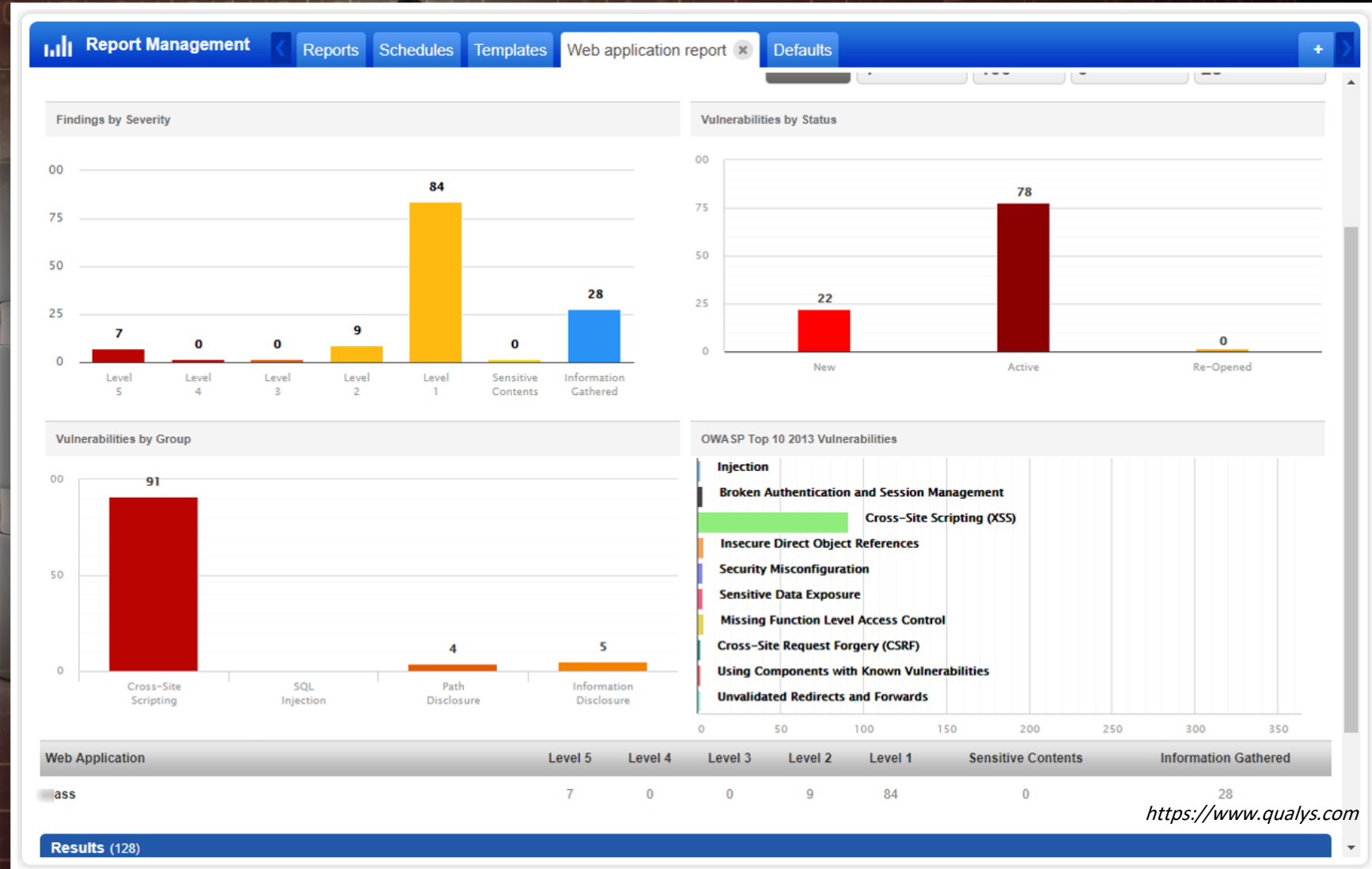
In this type of assessment, the ethical hacker employs various **vulnerability assessment tools**, such as **Nessus**, **Qualys**, **GFI LanGuard**, etc.

Vulnerability-Management Life Cycle



Vulnerability Assessment Tools: Qualys Vulnerability Management

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



Vulnerability Assessment Tools: OpenVAS and GFI LanGuard

OpenVAS

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

The screenshot shows the OpenVAS Greenbone Security Assistant (GSA) interface. The top navigation bar includes Dashboard, Scans, Assets, SecInfo, Configuration, Extras, Administration, and Help. The main content area displays a report titled "Report: Results (3 of 43)". The report shows a table of vulnerabilities with columns for Vulnerability, Severity, QoD, Host, Location, and Actions. The vulnerabilities listed are DCE/RPC and MSRPC Services Enumeration Reporting (Severity: 5.0 Medium), SSL/TLS: Report Weak Cipher Suites (Severity: 4.3 Medium), and TCP timestamps (Severity: 2.6 Low). The interface also shows a filter section and a sidebar with a tree view of the network structure.

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

<https://www.openvas.org>

GFI LanGuard

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

The screenshot shows the GFI LanGuard interface. The top navigation bar includes Dashboard, Scan, Remediate, Activity Monitor, Reports, Configuration, Utilities, and Discuss this version... The main content area displays a dashboard for "SERVER2016 (10.10.10.16)". The dashboard includes a Vulnerability Level gauge, a list of Top 5 Issues to Address (Windows Malicious Software Removal Tool x64 - November 2019, 2019-11 Cumulative Update for Windows Server 2016 for x64-based Systems, 2019-11 Servicing Stack Update for Windows Server 2016), a Security Sensors section (Software Updates, Service Packs and Update Rollups, Vulnerabilities, Malware Protection Issue, Firewall Issues, Unauthorized Applications, Audit Status), and a Computer Details section (Name: SERVER2016, IP Address: 10.10.10.16, MAC Address: 00-0C-29-0E-73-17). The interface also shows a Scan Activity graph and a Results Statistics section (Missing Security Updates: 7 (7 Critical/High), Missing Non-Security Updates: 2, Service Packs and Update Rollups: 1, Major Version Upgrades: 1, Other Vulnerabilities: 11 (6 Critical/High)).

<https://www.gfi.com>

Other Vulnerability Assessment Tools

Nessus Professional

<https://www.tenable.com>



Nikto

<https://cirt.net>



Qualys FreeScan

<https://freescan.qualys.com>



Acunetix Web Vulnerability Scanner

<https://www.acunetix.com>



Nexpose

<https://www.rapid7.com>



Network Security Scanner

<https://www.beyondtrust.com>



SAINT Security Suite

<https://www.carson-saint.com>



beSECURE (AVDS)

<https://www.beyondsecurity.com>



Core Impact

<https://www.coresecurity.com>



N-Stalker Web Application Security Scanner

<https://www.nstalker.com>



Vulnerability Exploitation

- ❑ Vulnerability exploitation involves the execution of multiple complex, interrelated steps to **gain access to a remote system**
- ❑ The steps involved are as follows:

01 Identify the vulnerability

02 Determine the risk associated with the vulnerability

03 Determine the capability of the vulnerability

04 Develop the exploit

05 Select the method for delivering – local or remote

06 Generate and deliver the payload

07 Gain remote access

Module Summary



- 01 — This module has discussed threat and threat sources
- 02 — It also discussed in detail on malware and its types
- 03 — This module gave an overview of malware countermeasures
- 04 — This module also discussed in detail on vulnerabilities and classification of vulnerabilities
- 05 — Finally, this module ended with a detailed discussion of vulnerability assessment concepts such as vulnerability research, vulnerability scoring systems and databases, vulnerability management life cycle, and vulnerability exploitation
- 06 — In the next module, we will discuss in detail on various password cacking techniques and countermeasures