EC-Council

C|EH™
Certified Ethical Hacker

Module 05

Vulnerability Analysis

Module Flow

1. Vulnerability Assessment Concepts
2. Vulnerability Classification and Assessment Types
3. Vulnerability Assessment Solutions and Tools
4. Vulnerability Assessment Reports

Vulnerability Research

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

An administrator needs vulnerability research:

1. To gather information concerning security trends, threats, attack surfaces, attack vectors and techniques
2. To discover weaknesses in the OS and applications, and alert the network administrator before a network attack
3. To gather information to aid in the prevention of security issues
4. To know how to recover from a network attack

Resources for Vulnerability Research

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

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 scanner includes:

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

Vulnerability Scoring Systems and Databases

Common Vulnerability Scoring System (CVSS)

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

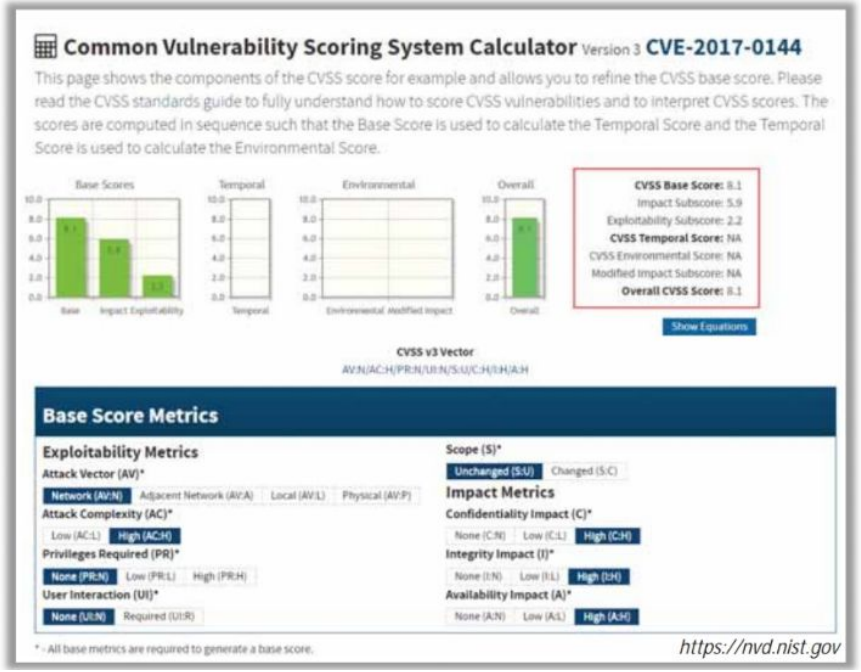
CVSS v3.0 Ratings

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

CVSS v2.0 Ratings

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

https://www.first.org

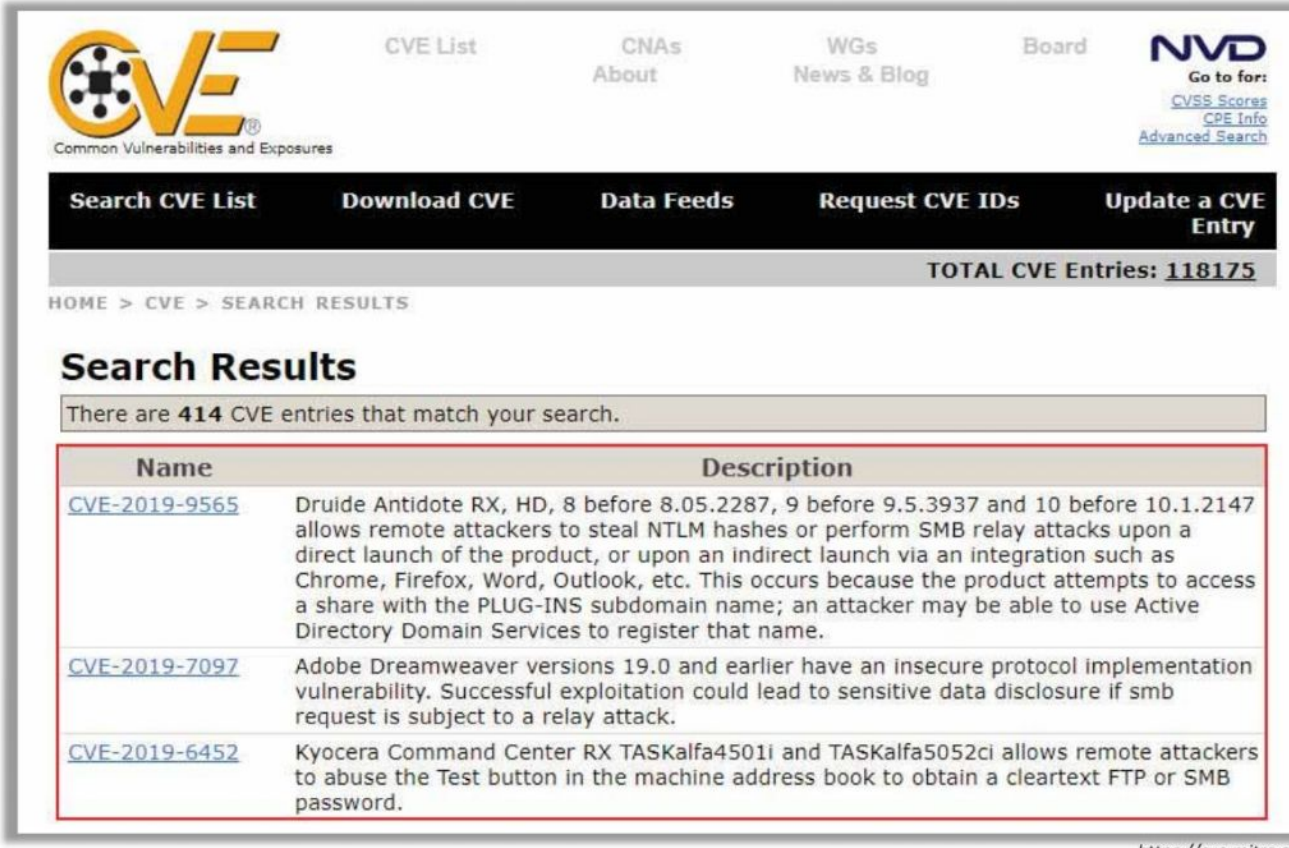


https://nvd.nist.gov

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

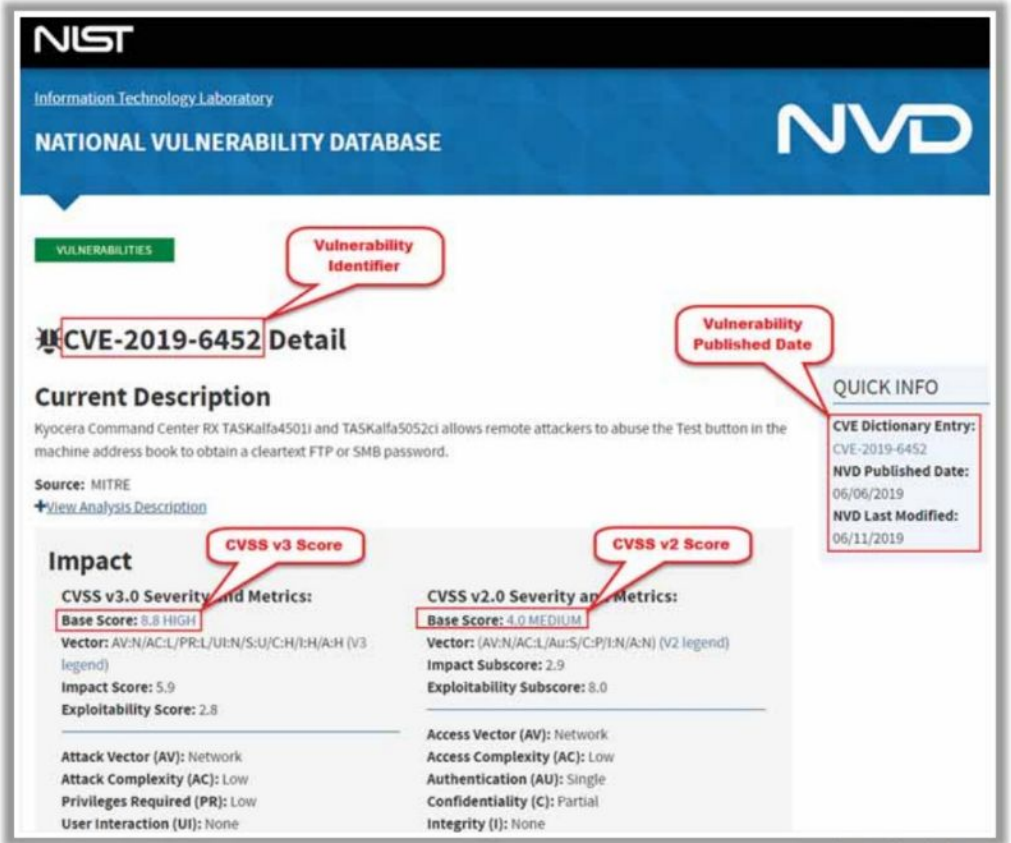


https://cve.mitro.org

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

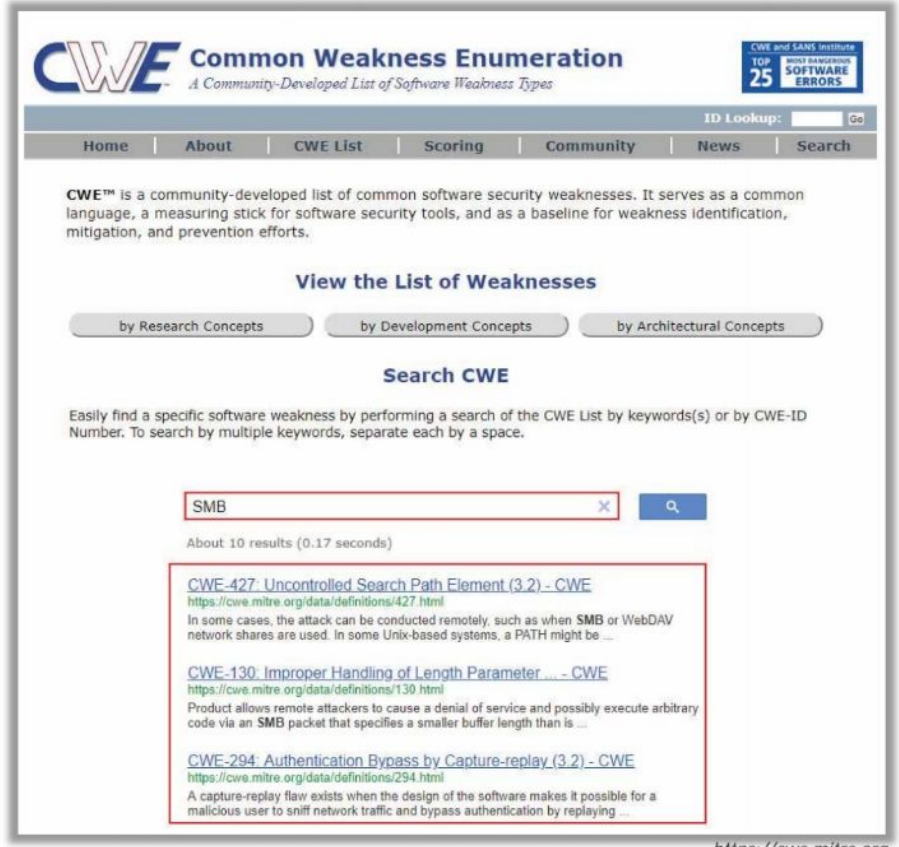


https://nvd.nist.gov

Vulnerability Scoring Systems and Databases (Cont'd)

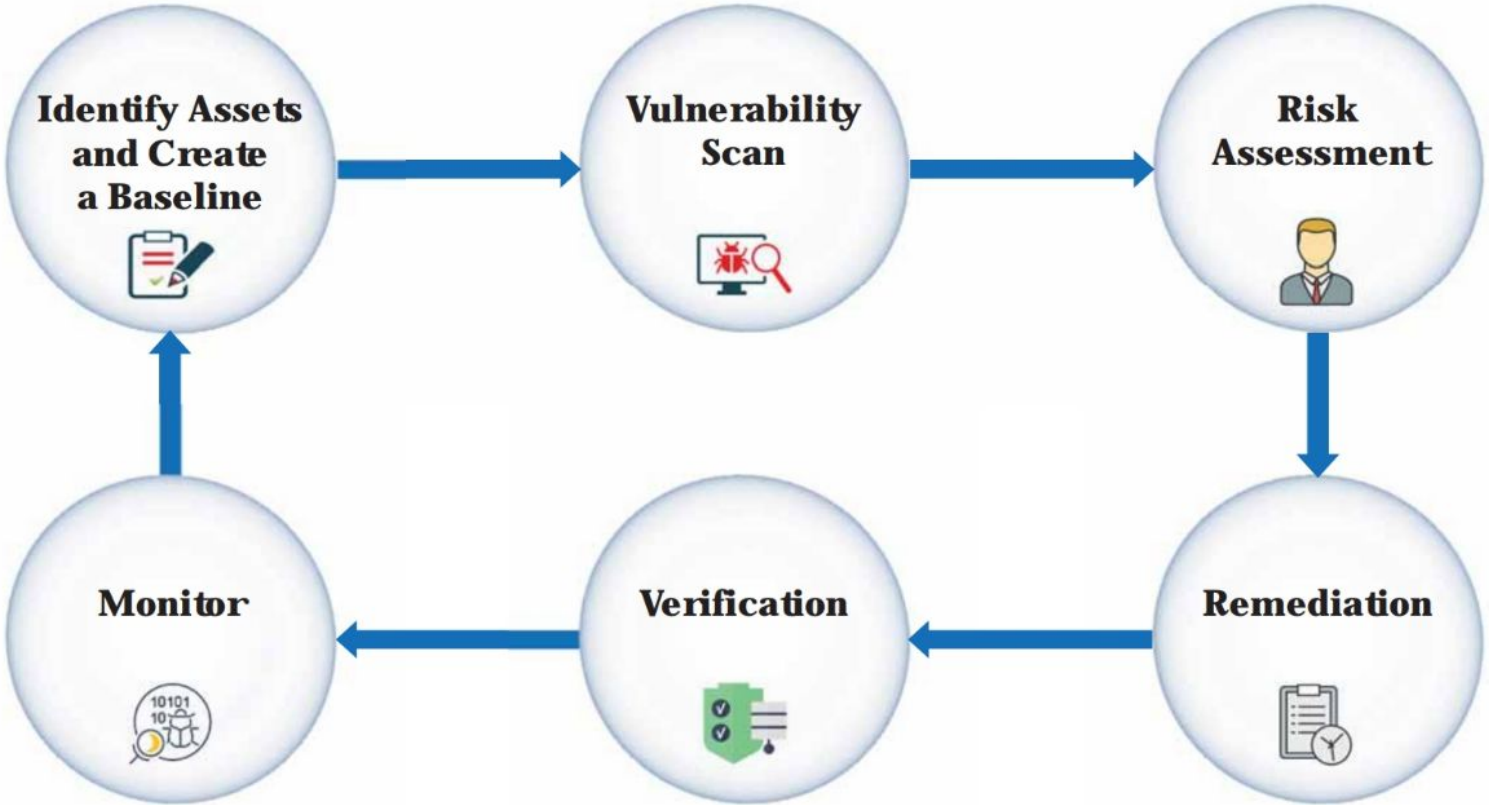
Common Weakness Enumeration (CWE)

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



https://cwe.mitre.org

Vulnerability-Management Life Cycle



Pre-Assessment Phase

Identify Assets and Create a Baseline

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

Vulnerability Assessment Phase

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

Post Assessment Phase

Risk Assessment

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

Remediation

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

Verification

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

Monitoring

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

Module Flow

1. Vulnerability Assessment Concepts

2. Vulnerability Classification and Assessment Types

3. Vulnerability Assessment Solutions and Tools

4. Vulnerability Assessment Reports

Vulnerability Classification

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

Types of Vulnerability Assessment

Active Assessment

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

Passive Assessment

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

External Assessment

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

Internal Assessment

Scans the internal infrastructure to discover exploits and vulnerabilities

Host-based Assessment

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

Network-based Assessment

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

Application Assessment

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

Database Assessment

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

Types of Vulnerability Assessment (Cont'd)

CEH Certified Ethical Hacker

Wireless Network Assessment

Determines the vulnerabilities in the organization's wireless networks

Distributed Assessment

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

Credentialed Assessment

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

Non-Credentialed Assessment

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

Manual Assessment

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

Automated Assessment

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

Module Flow

1. Vulnerability Assessment Concepts
2. Vulnerability Classification and Assessment Types
3. Vulnerability Assessment Solutions and Tools
4. Vulnerability Assessment Reports

Comparing Approaches to Vulnerability Assessment

Product-Based versus Service-Based Assessment Solutions

Product-Based Solutions

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

Service-Based Solutions

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

Comparing Approaches to Vulnerability Assessment (Cont'd)

Tree-Based versus Inference-Based Assessment

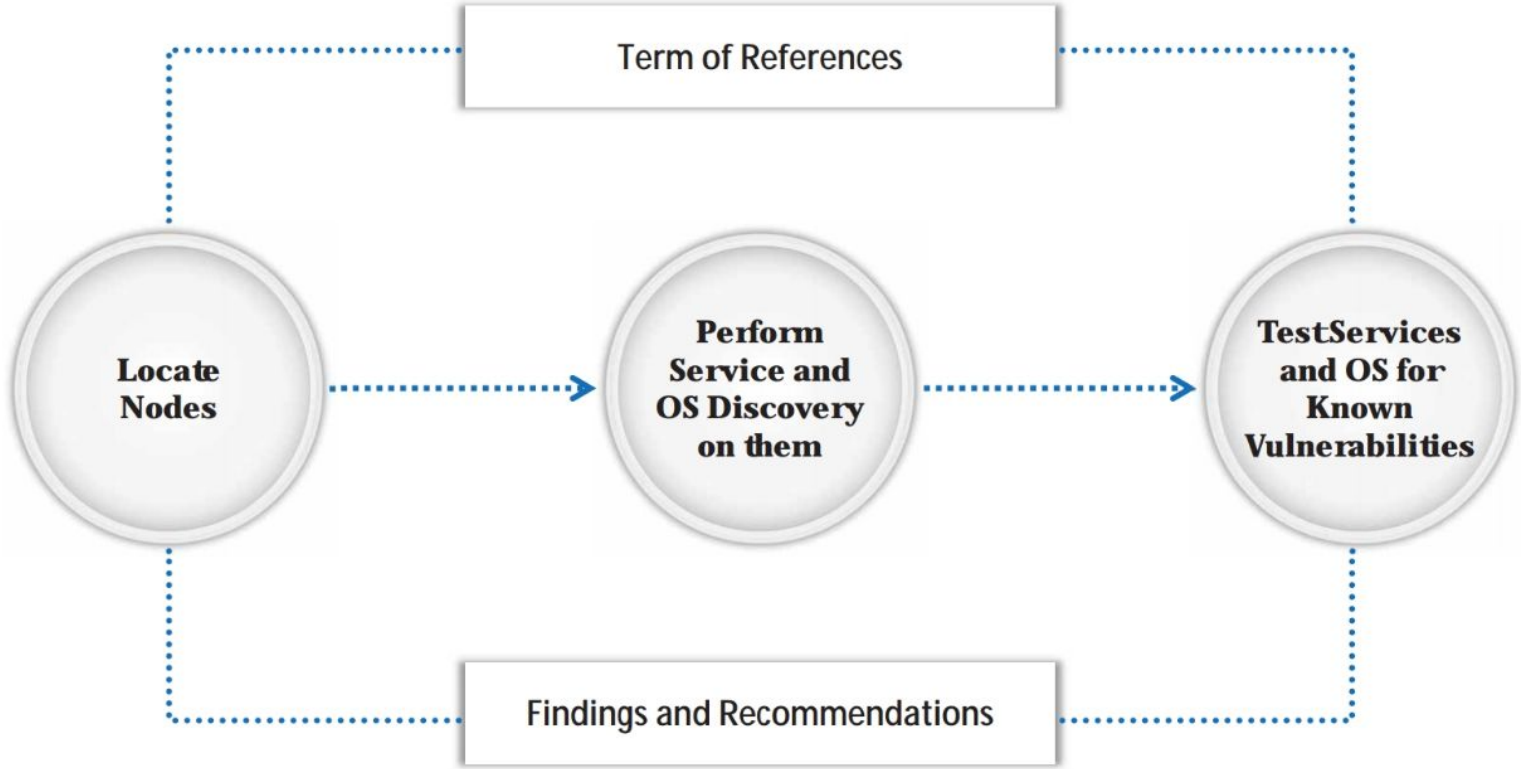
Tree-Based Assessment

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

Inference-Based Assessment

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

Working of Vulnerability Scanning Solutions



Types of Vulnerability Assessment Tools

CEH Certified Ethical Hacker

Host-Based Vulnerability Assessment Tools

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

Depth Assessment Tools

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

Application-Layer Vulnerability Assessment Tools

- Directed toward web servers or databases

Scope Assessment Tools

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

Active and Passive Tools

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

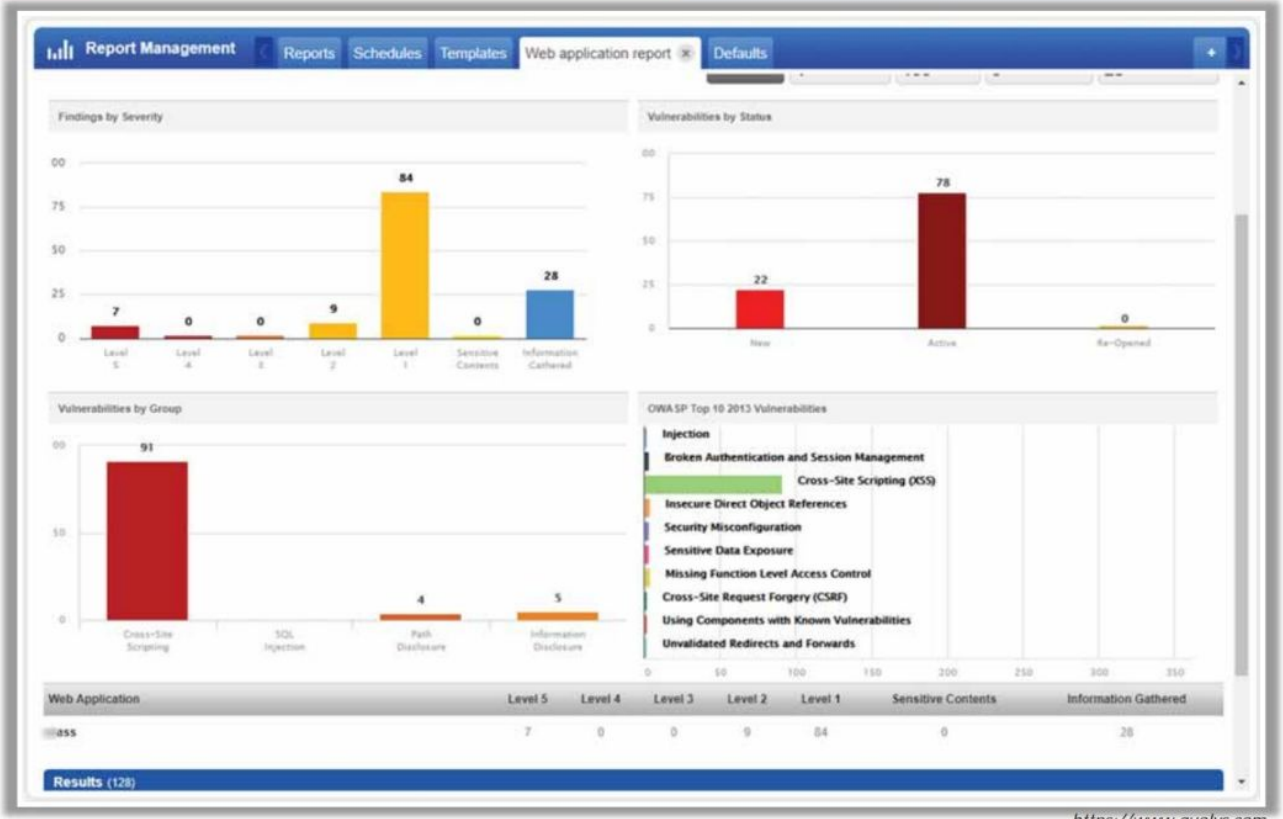
Location and Data Examination Tools

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

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

Qualys.

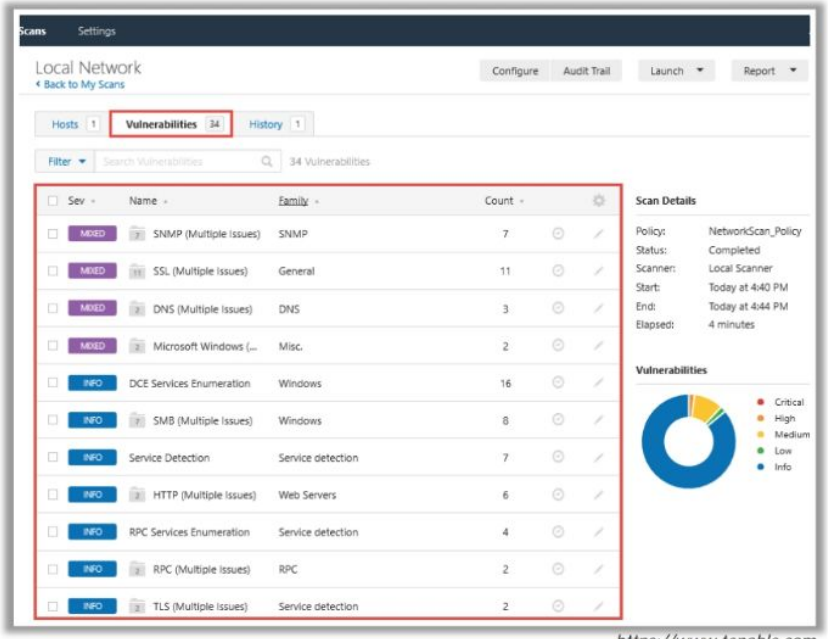


https://www.qualys.com

Vulnerability Assessment Tools: Nessus Professional and GFI LanGuard

Nessus Professional

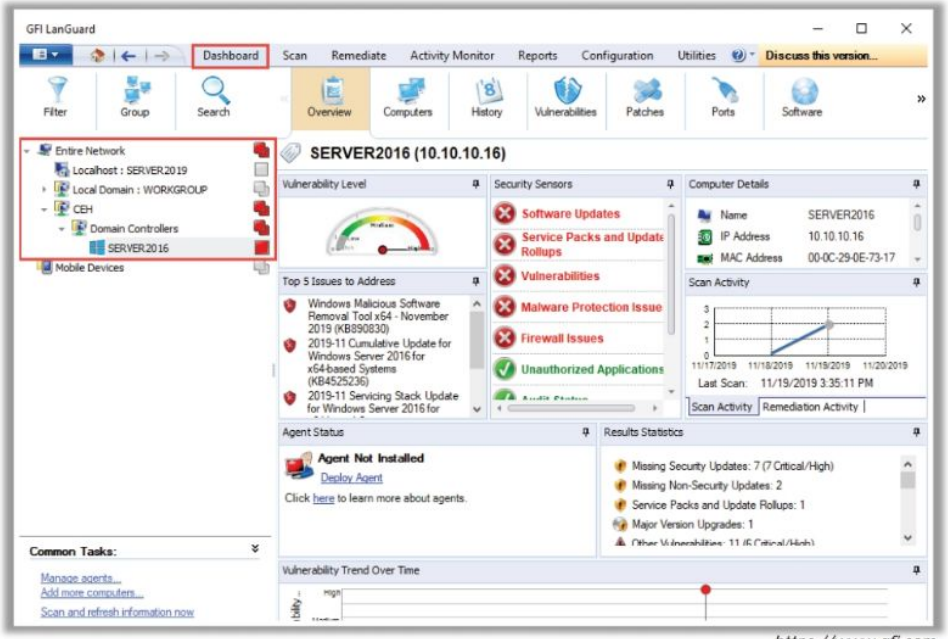
An assessment solution for identifying the vulnerabilities, configuration issues, and malware



https://www.tenable.com

GFI LanGuard

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



https://www.gfi.com

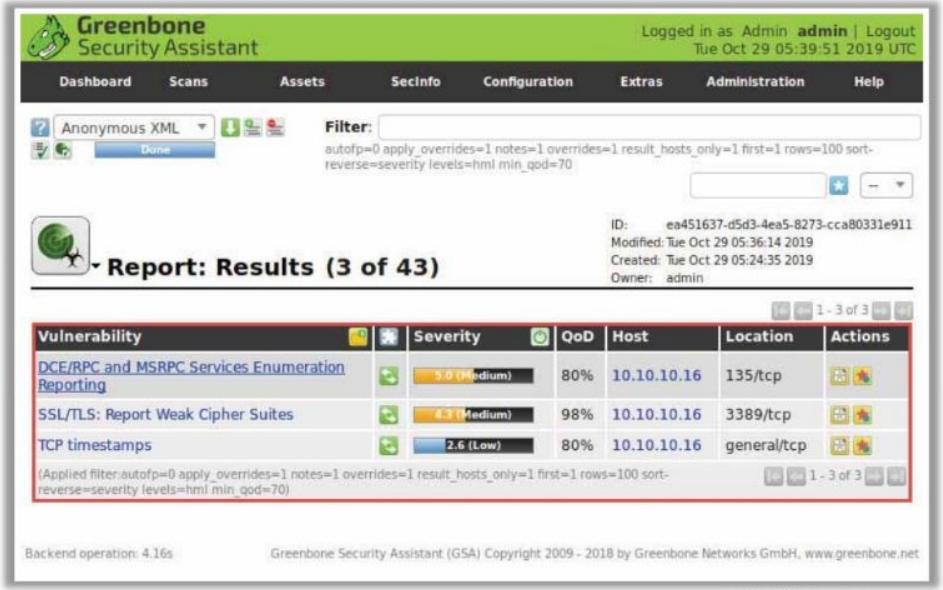
Vulnerability Assessment Tools: OpenVAS and Nikto

OpenVAS

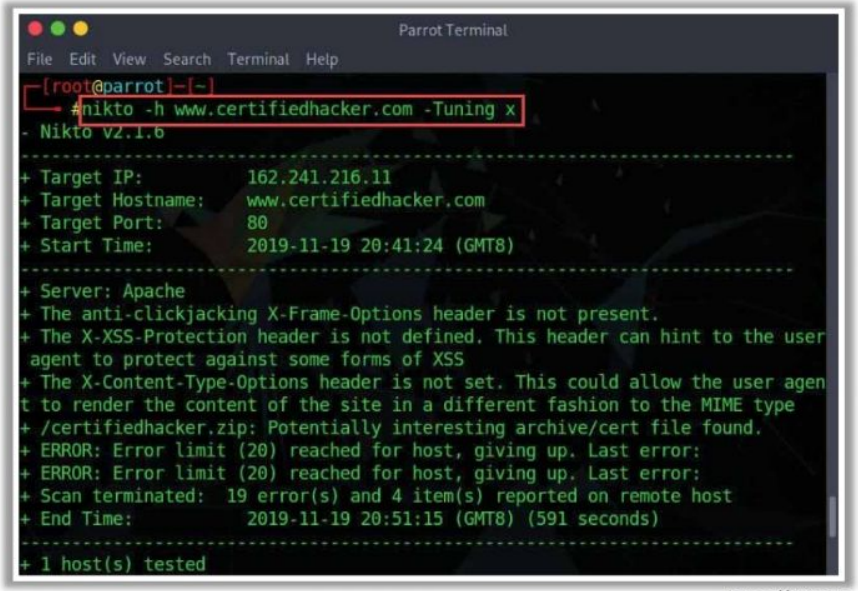
A framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution

Nikto

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



http://www.openvas.org



https://cirt.net

Other Vulnerability Assessment Tools

Qualys FreeScan
https://freescan.qualys.com

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

Nexpose
https://www.rapid7.com

Network Security Scanner
https://www.beyondtrust.com

SAINT
https://www.saintcorporation.com

Microsoft Baseline Security Analyzer (MBSA)
https://www.microsoft.com

beSECURE (AVDS)
https://www.beyondsecurity.com

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

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

ManageEngine Vulnerability Manager Plus
https://www.manageengine.com

Vulnerability Assessment Tools for Mobile

Vulners Scanner

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

https://vulners.com

Security Metrics Mobile

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

https://www.securitymetrics.com

Module Flow

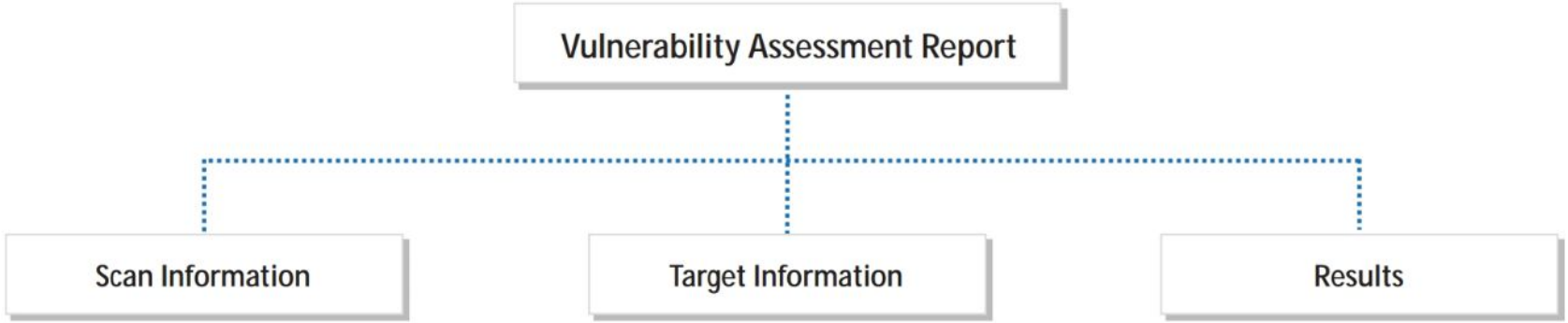
1. Vulnerability Assessment Concepts
2. Vulnerability Classification and Assessment Types
3. Vulnerability Assessment Solutions and Tools
4. Vulnerability Assessment Reports

Vulnerability Assessment Reports

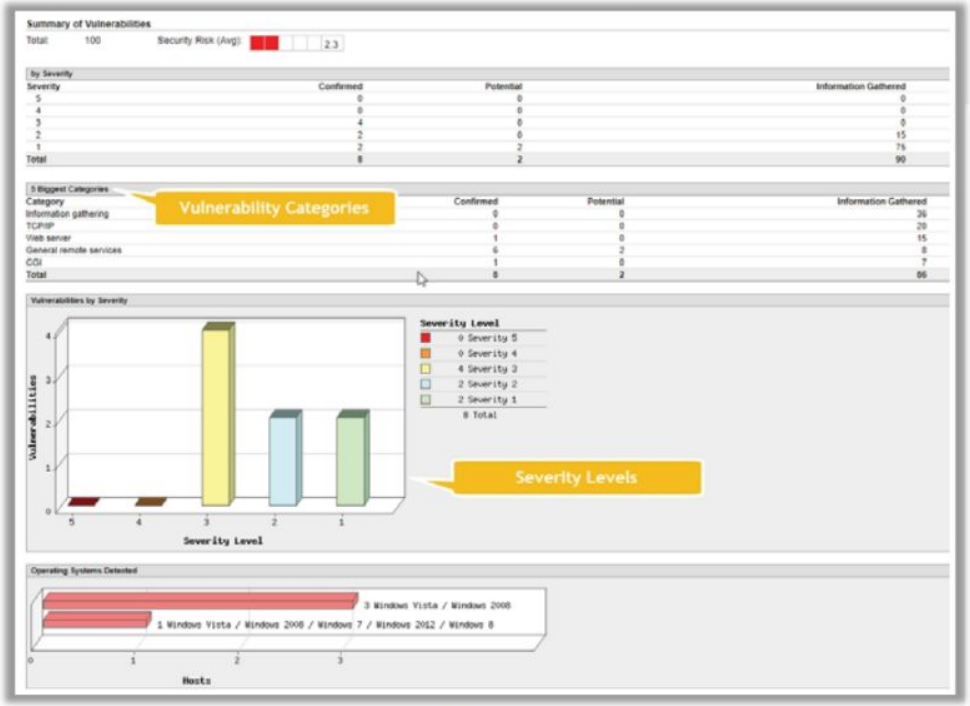
1. The vulnerability assessment report discloses the risks detected after scanning a network

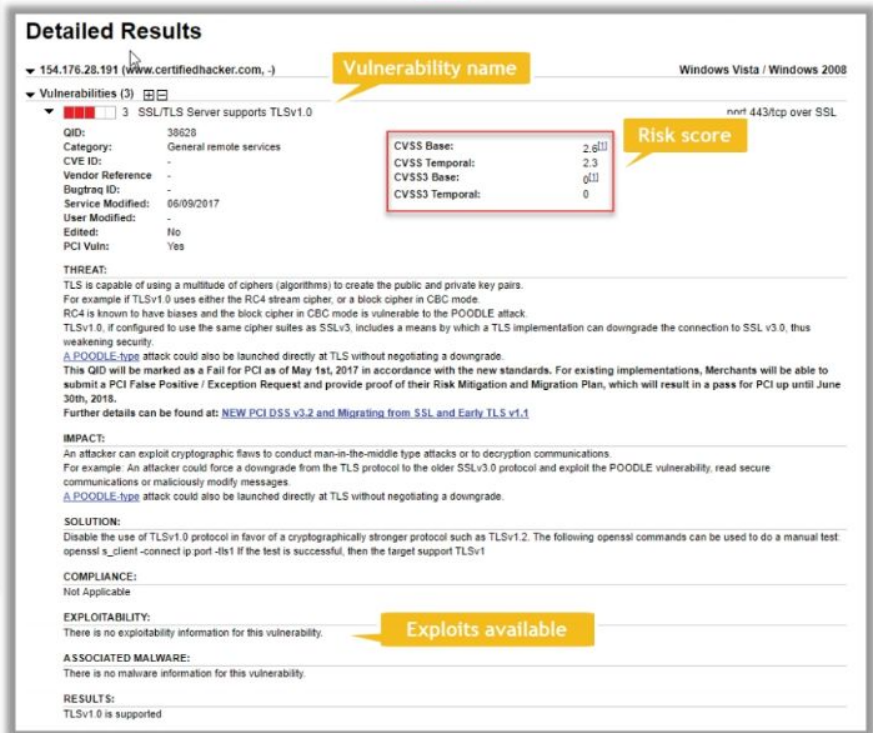
2. The report alerts the organization of possible attacks and suggests countermeasures

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



Analyzing Vulnerability Scanning Report





Module Summary

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