Module 05

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 Flow

1 Vulnerability Assessment Concepts

2 Vulnerability Assessment Solutions

3 Vulnerability Scoring Systems

4 Vulnerability Assessment Tools

5 Vulnerability Assessment Reports

Vulnerability Research

- 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

Vulnerability Classification

1. Misconfigurations
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

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

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

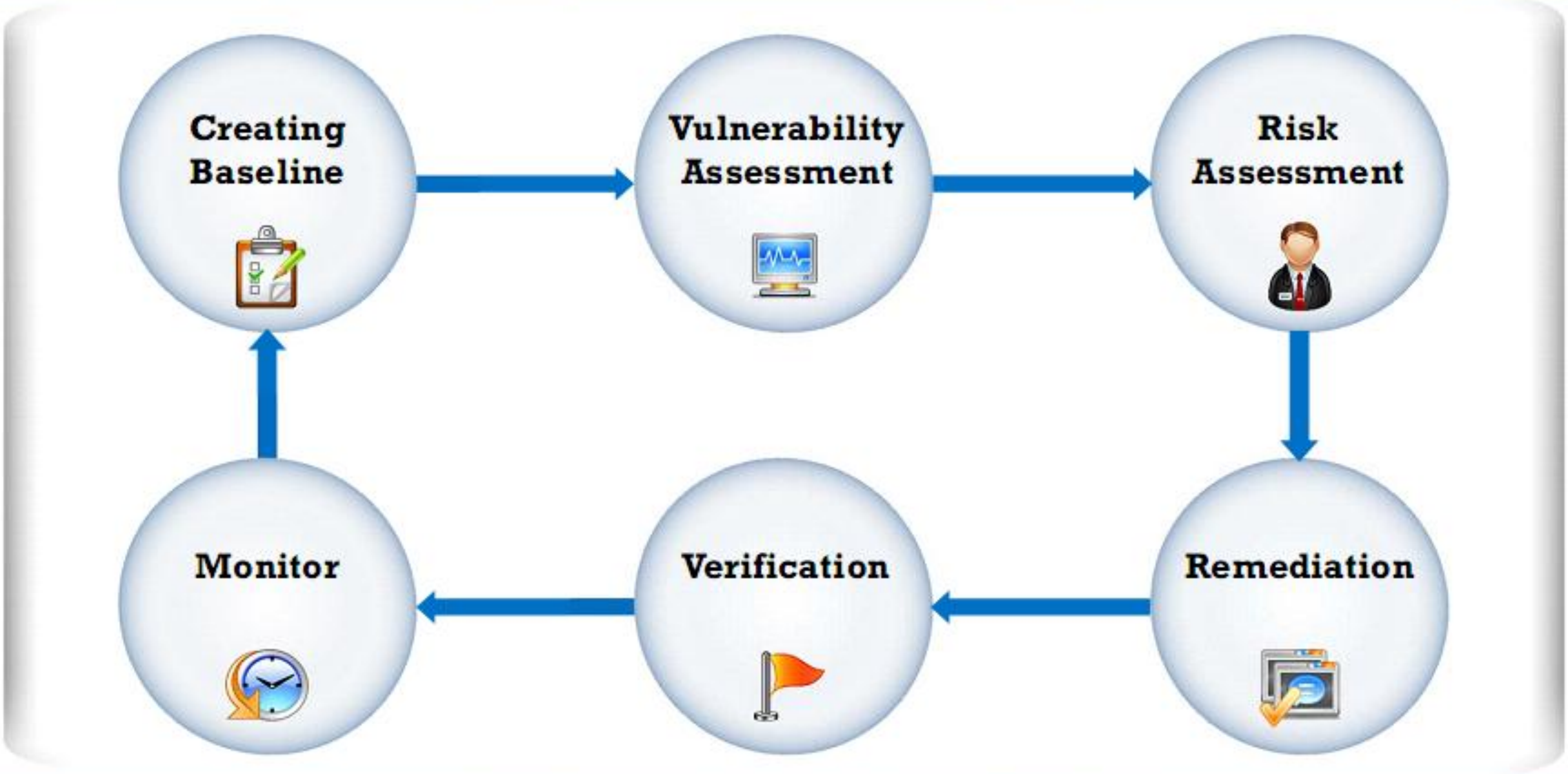
Application Assessments

Tests the web infrastructure for any misconfiguration and known vulnerabilities

Wireless Network Assessments

Determines the vulnerabilities in the organization's wireless networks

Vulnerability-Management Life Cycle



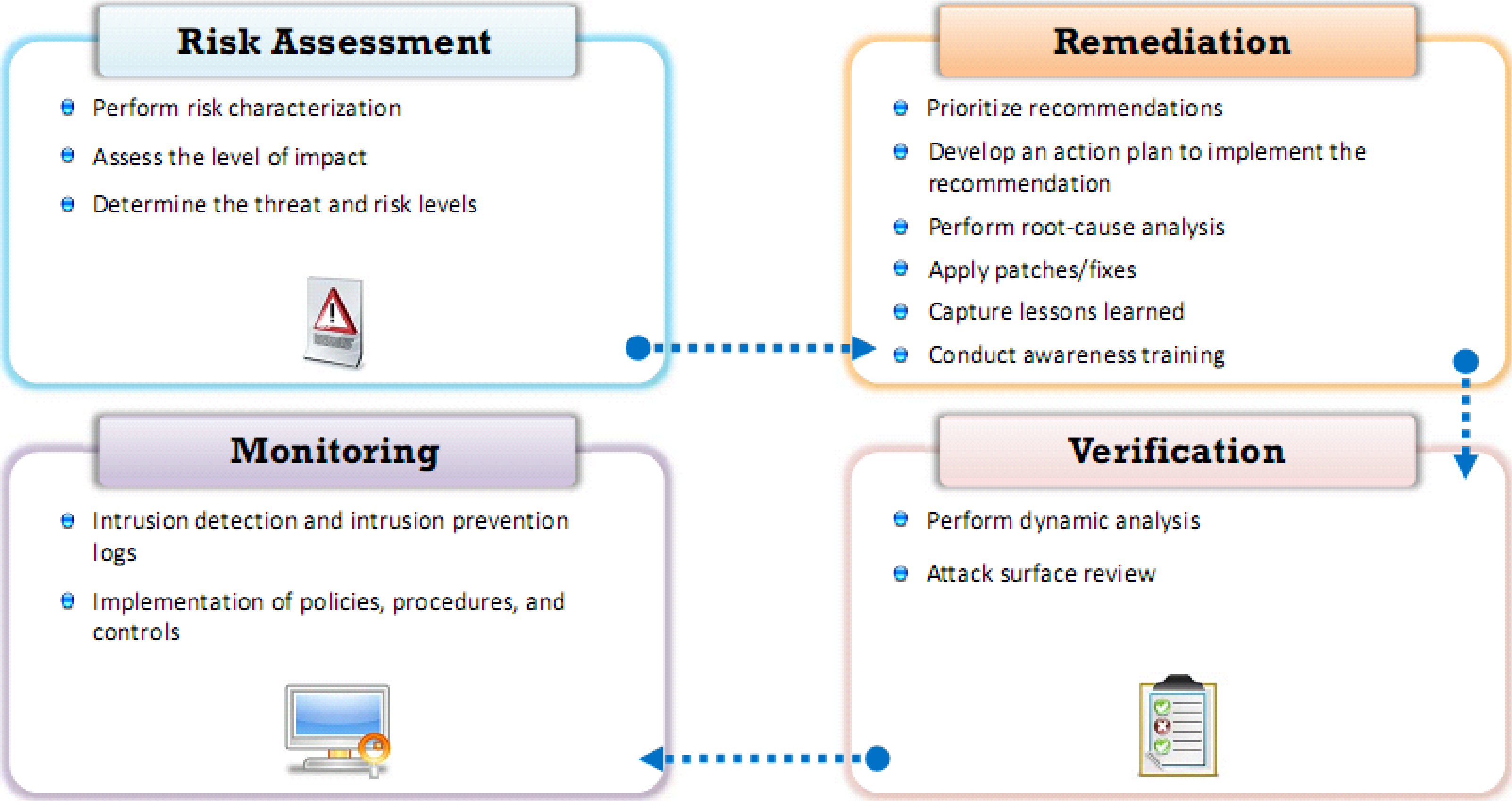
Pre-Assessment Phase: Creating a Baseline

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

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**

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

Module Flow

1 Vulnerability Assessment Concepts

2 Vulnerability Assessment Solutions

3 Vulnerability Scoring Systems

4 Vulnerability Assessment Tools

5 Vulnerability Assessment Reports

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**

Comparing Approaches to Vulnerability Assessment (Cont'd)

Tree-Based versus Inference-Based Assessment

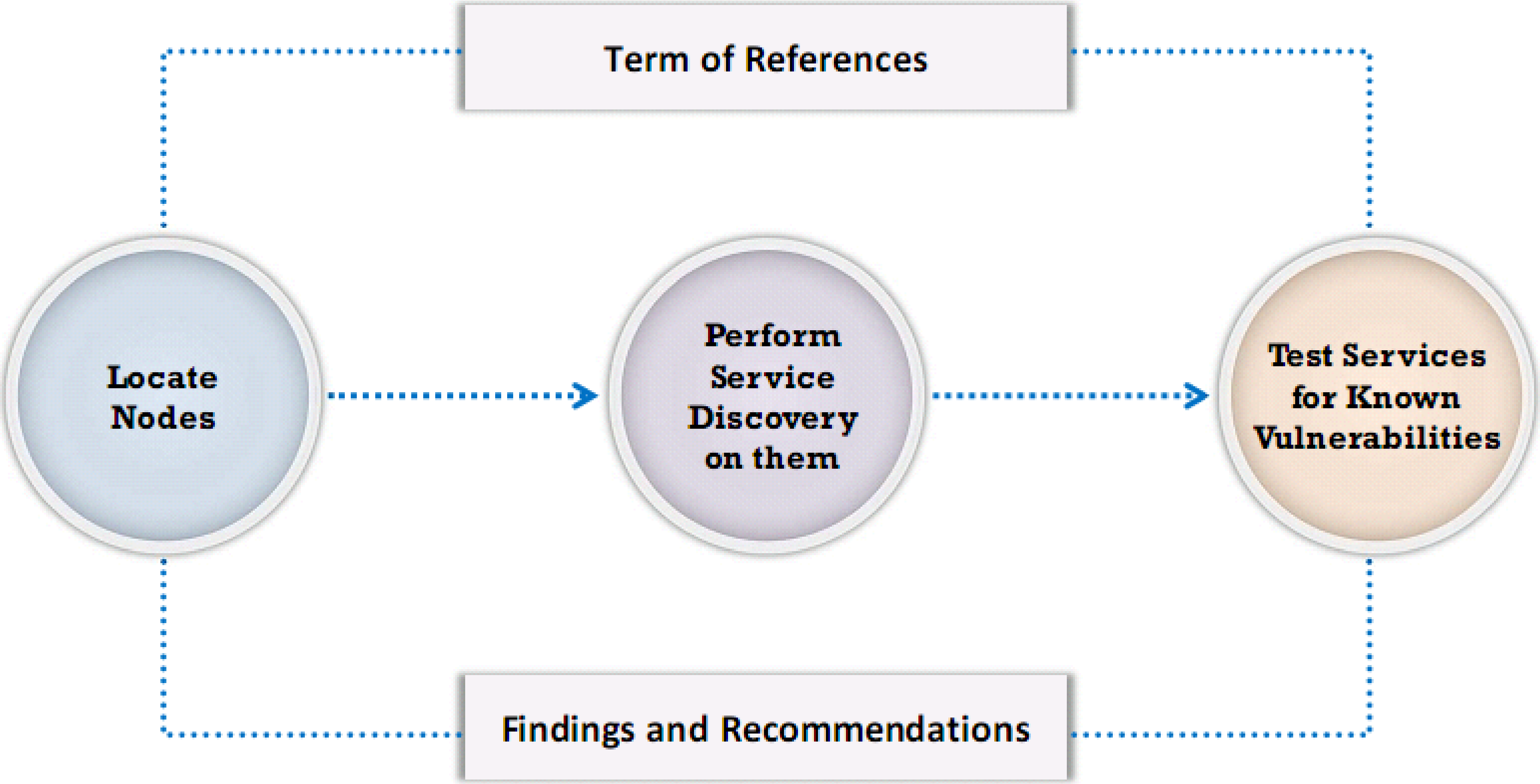
Tree-Based Assessment

- 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

Working of Vulnerability Scanning Solutions



Term of References

Locate Nodes

Perform Service Discovery on them

Test Services for Known Vulnerabilities

Findings and Recommendations

Types of Vulnerability Assessment Tools

Host-Based Vulnerability Assessment Tools

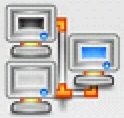
- A host-based vulnerability assessment tool finds and identifies the OS running on a particular host computer and tests it for known deficiencies
- Searches for common applications and services

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

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

Choosing a Vulnerability Assessment Tool

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

- Choose the tools that best **satisfy** the following requirements:
  - 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

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

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 ✓

Module Flow

1 Vulnerability Assessment Concepts

2 Vulnerability Assessment Solutions

3 Vulnerability Scoring Systems

4 Vulnerability Assessment Tools

5 Vulnerability Assessment Reports

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**

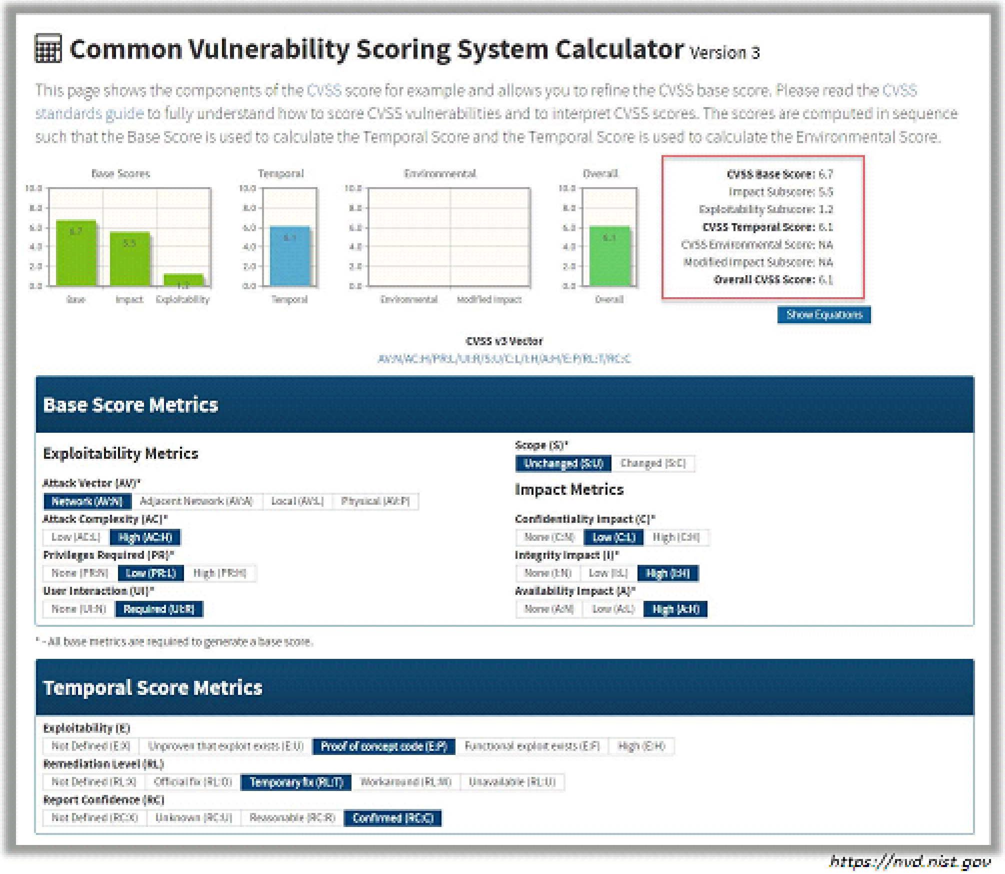
CVSS v3.0 Ratings

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

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: 6.7
Impact Subscore: 5.5
Exploitability Subscore: 1.2
CVSS Temporal Score: 6.1
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 6.1

CVSS v3 Vector
AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:H/A:H/E:P/RL:T/RC:C

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.

Temporal Score Metrics

Exploitability (E)
○ Not Defined (E:X) ○ Unproven that exploit exists (E:U) ● Proof of concept code (E:P) ○ Functional exploit exists (E:F) ○ High (E:H)

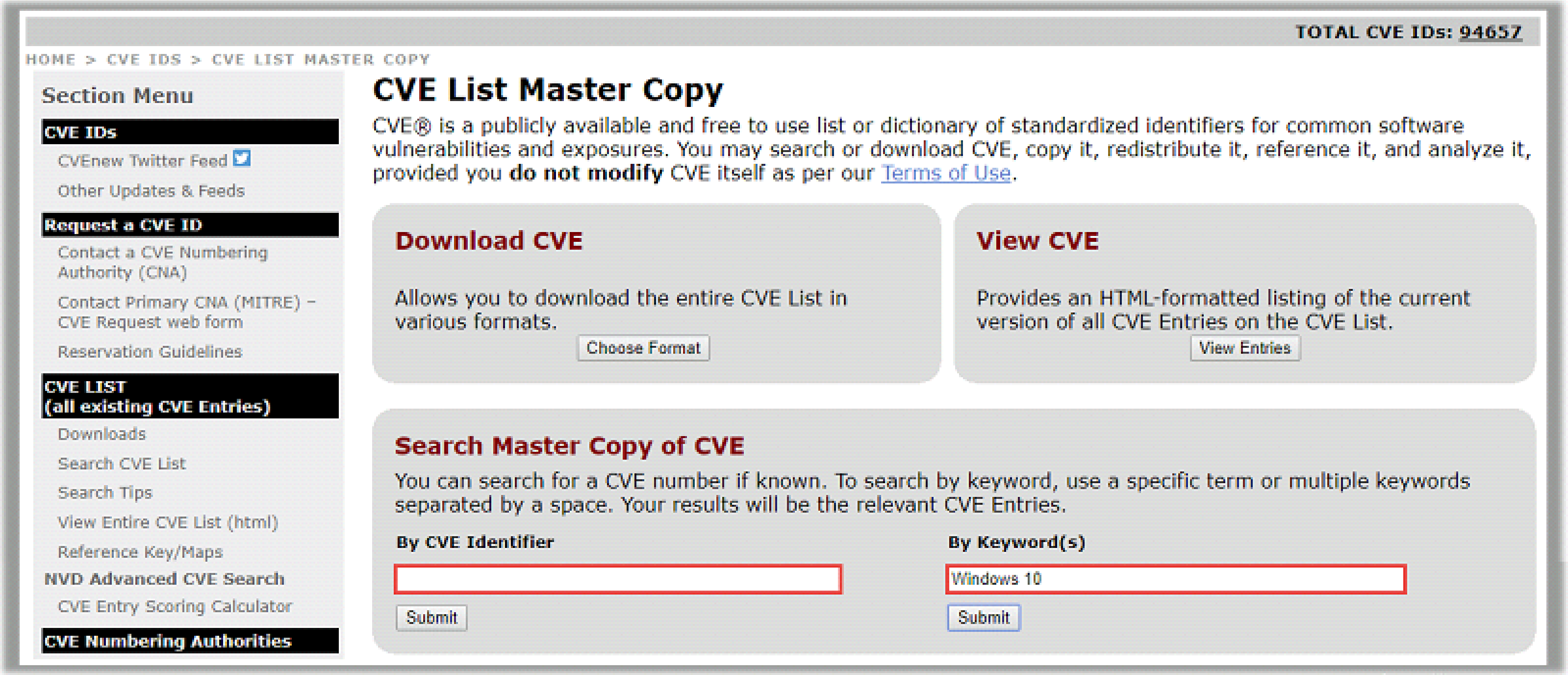
Remediation Level (RL)
○ Not Defined (RL:X) ○ Official fix (RL:O) ● Temporary fix (RL:T) ○ Workaround (RL:W) ○ Unavailable (RL:U)

Report Confidence (RC)
○ Not Defined (RC:X) ○ Unknown (RC:U) ○ Reasonable (RC:R) ● Confirmed (RC:C)

https://nvd.nist.gov

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

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.

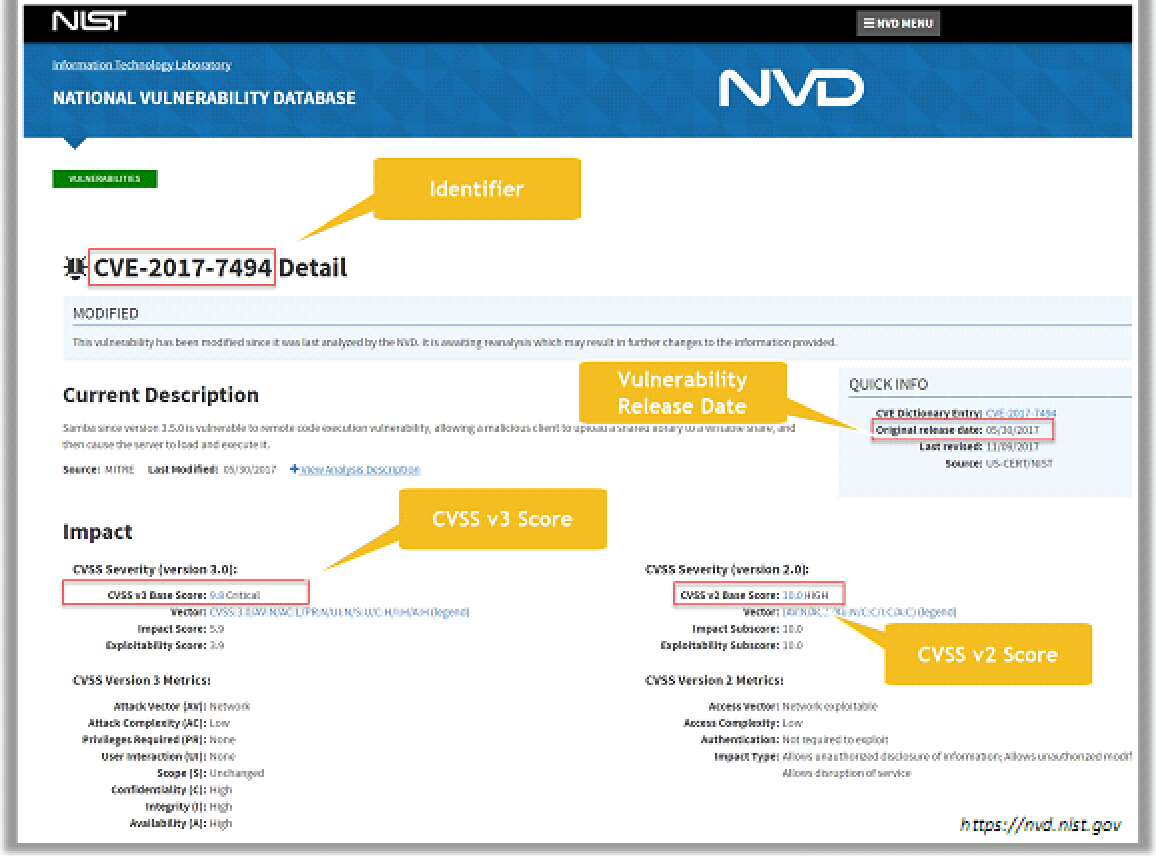
By CVE Identifier:

By Keyword(s): Windows 10

https://cve.mitre.org

National Vulnerability Database (NVD)

- 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


NIST
☰ NVD MENU
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE
NVD
VULNERABILITIES

Identifier

CVE-2017-7494 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

Samba since version 3.5.0 is vulnerable to remote code execution vulnerability, allowing a malicious client to upload a shared library to a writable share, and then cause the server to load and execute it.

Source: MITRE **Last Modified:** 05/30/2017 + View Analysis Description

Vulnerability Release Date

QUICK INFO

CVE Dictionary Entry: CVE-2017-7494
Original release date: 05/30/2017
Last revised: 11/09/2017
Source: US-CERT/NIST

CVSS v3 Score

Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score: 9.8 Critical
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (legend)
Impact Score: 5.9
Exploitability Score: 3.9

CVSS Version 3 Metrics:

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

CVSS Severity (version 2.0):

CVSS v2 Base Score: 10.0 HIGH
Vector: (AV:N/AC:L/Au:N/C:C/I:C/A:C) (legend)
Impact Subscore: 10.0
Exploitability Subscore: 10.0

CVSS v2 Score

CVSS Version 2 Metrics:

Access Vector: Network exploitable
Access Complexity: Low
Authentication: Not required to exploit
Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modif
Allows disruption of service

https://nvd.nist.gov

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

Module Flow

1 Vulnerability Assessment Concepts

2 Vulnerability Assessment Solutions

3 Vulnerability Scoring Systems

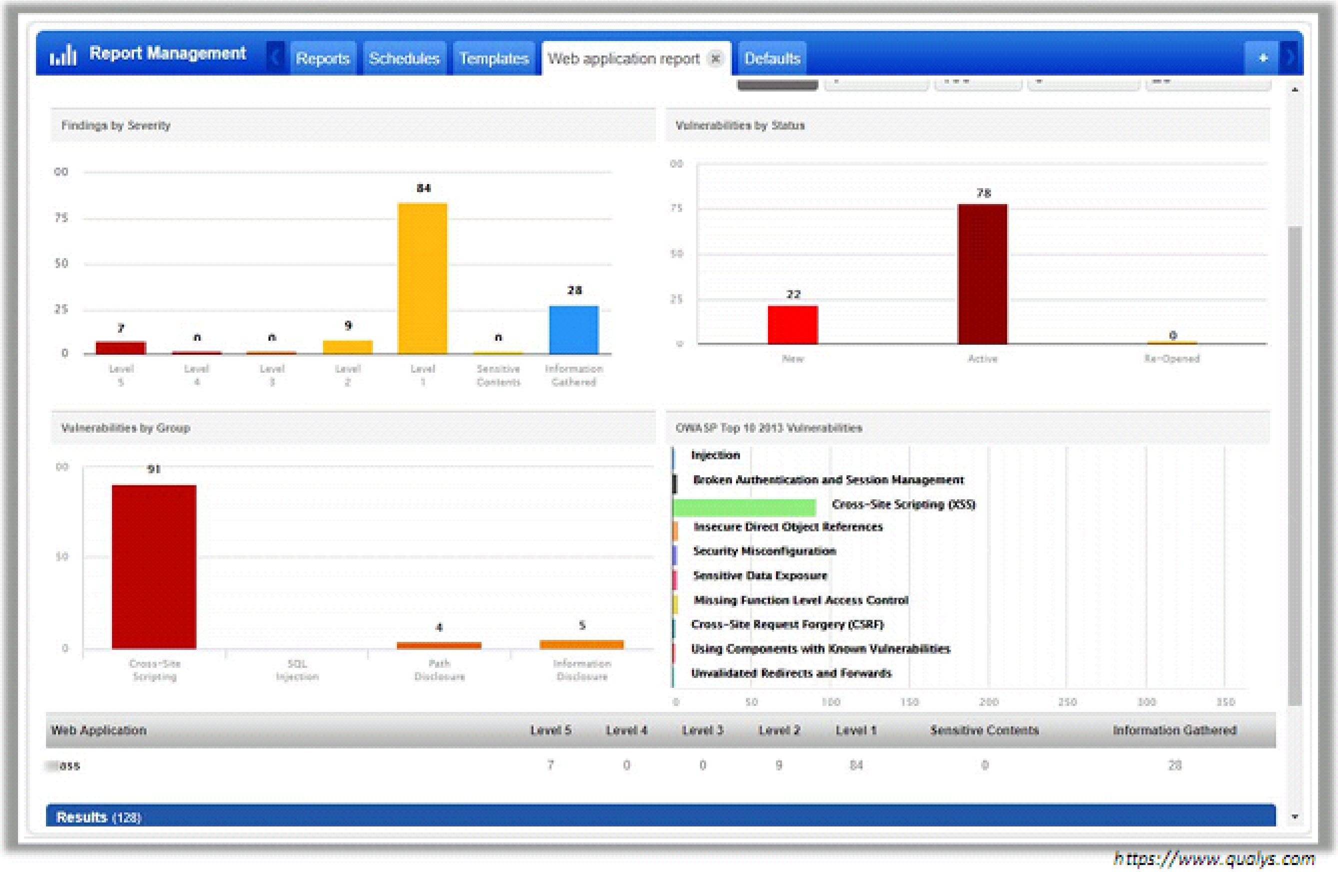
4 Vulnerability Assessment Tools

5 Vulnerability Assessment Reports

Qualys Vulnerability Management

- 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.



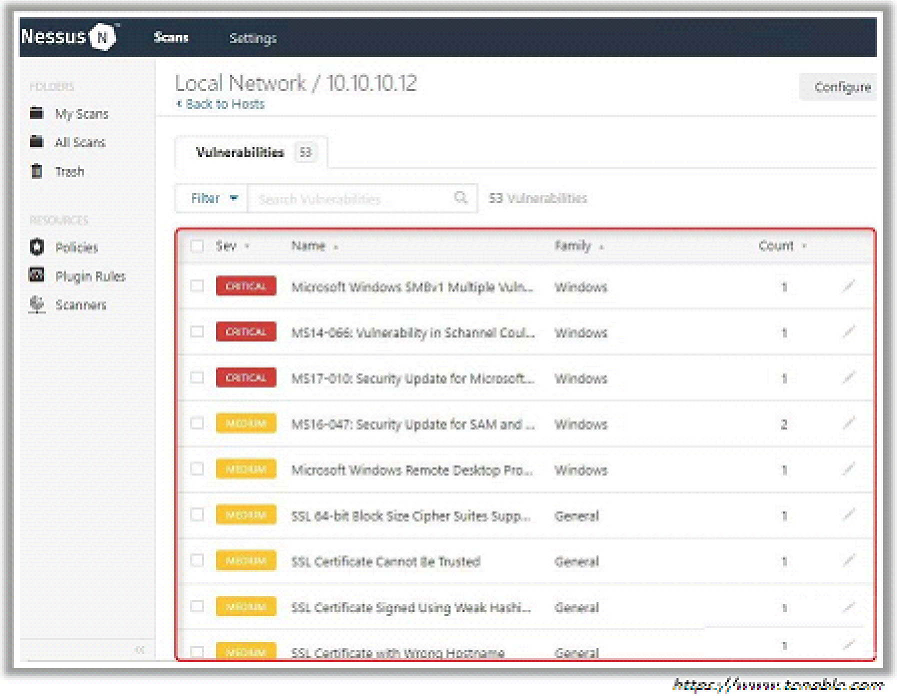
Web Application	Level 5	Level 4	Level 3	Level 2	Level 1	Sensitive Contents	Information Gathered
[redacted]ass	7	0	0	9	84	0	28

https://www.qualys.com

Vulnerability Assessment Tools: Nessus Professional and GFI LanGuard

Nessus Professional

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



Local Network / 10.10.10.12
‹ Back to Hosts

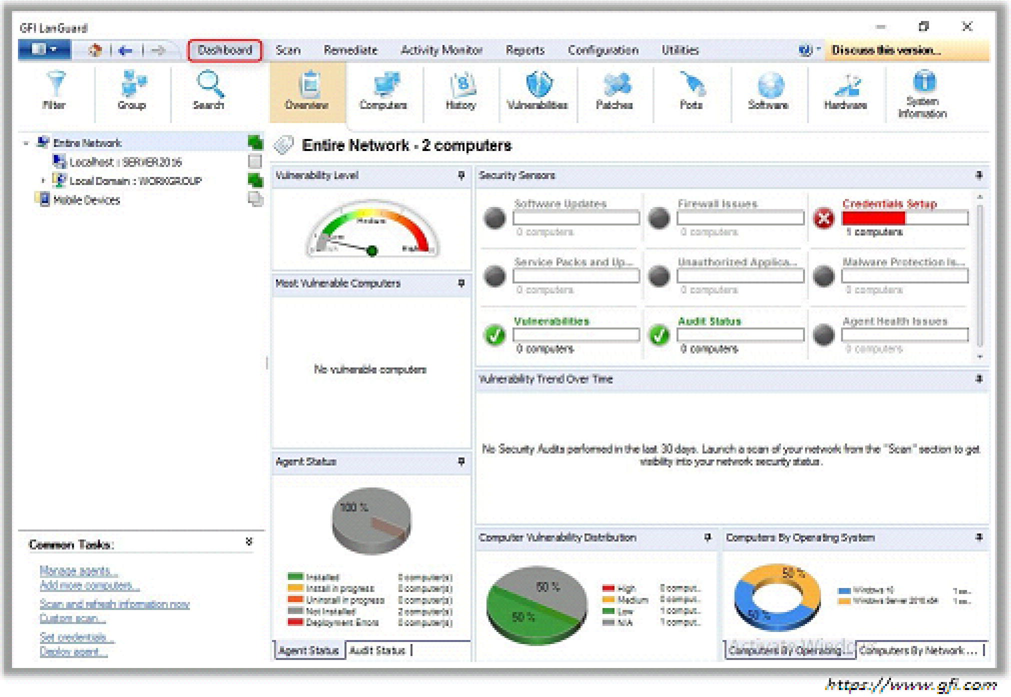
53 Vulnerabilities

Sev	Name	Family	Count
CRITICAL	Microsoft Windows SMBv1 Multiple Vuln...	Windows	1
CRITICAL	MS14-066: Vulnerability in Schannel Coul...	Windows	1
CRITICAL	MS17-010: Security Update for Microsoft...	Windows	1
MEDIUM	MS16-047: Security Update for SAM and ...	Windows	2
MEDIUM	Microsoft Windows Remote Desktop Pro...	Windows	1
MEDIUM	SSL 64-bit Block Size Cipher Suites Supp...	General	1
MEDIUM	SSL Certificate Cannot Be Trusted	General	1
MEDIUM	SSL Certificate Signed Using Weak Hashi...	General	1
MEDIUM	SSL Certificate with Wrong Hostname	General	1

https://www.tenable.com

GFI LanGuard

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



Entire Network - 2 computers

Sensor	Status
Software Updates	0 computers
Firewall Issues	0 computers
Credentials Setup	1 computers
Service Packs and Up...	0 computers
Unauthorized Applica...	0 computers
Malware Protection Is...	0 computers
Vulnerabilities	0 computers
Audit Status	0 computers
Agent Health Issues	0 computers

No vulnerable computers

No Security Audits performed in the last 30 days. Launch a scan of your network from the "Scan" section to get visibility into your network security status.

Installed	0 computer(s)
Install in progress	0 computer(s)
Uninstall in progress	0 computer(s)
Not Installed	2 computer(s)
Deployment Errors	0 computer(s)

High	0 comput...
Medium	0 comput...
Low	1 comput...
N/A	1 comput...

Common Tasks:

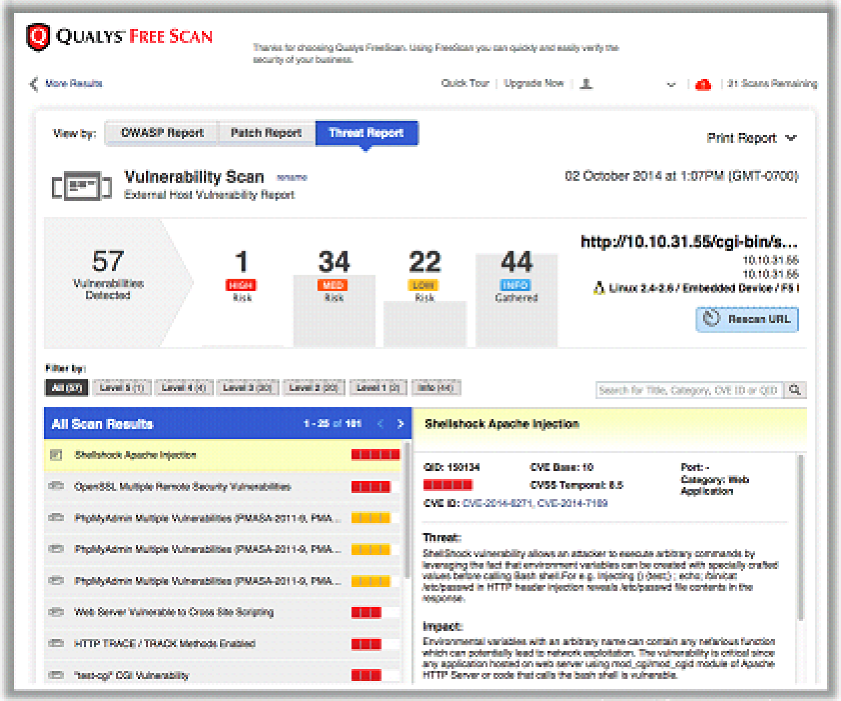
Manage agents...
Add more computers...
Scan and refresh information now
Custom scan...
Set credentials...
Deploy agent...

https://www.gfi.com

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



QUALYS FREE SCAN
Thanks for choosing Qualys FreeScan. Using FreeScan you can quickly and easily verify the security of your business.
More Results
Quick Tour | Upgrade Now | 21 Scans Remaining
View by: OWASP Report | Patch Report | Threat Report
Print Report
rename
Rescan URL
Filter by:
All (57) | Level 5 (1) | Level 4 (4) | Level 3 (30) | Level 2 (20) | Level 1 (2) | Info (44)
Search for Title, Category, CVE ID or QID

Vulnerability Scan
External Host Vulnerability Report
02 October 2014 at 1:07PM (GMT-0700)

57 Vulnerabilities Detected | 1 HIGH Risk | 34 MED Risk | 22 LOW Risk | 44 INFO Gathered

http://10.10.31.55/cgi-bin/s...
10.10.31.55
10.10.31.55
Linux 2.4-2.6 / Embedded Device / F5 I

All Scan Results 1 - 25 of 101

- Shellshock Apache Injection
- OpenSSL Multiple Remote Security Vulnerabilities
- PhpMyAdmin Multiple Vulnerabilities (PMASA-2011-9, PMA...
- PhpMyAdmin Multiple Vulnerabilities (PMASA-2011-9, PMA...
- PhpMyAdmin Multiple Vulnerabilities (PMASA-2011-9, PMA...
- Web Server Vulnerable to Cross Site Scripting
- HTTP TRACE / TRACK Methods Enabled
- "test-cgi" CGI Vulnerability

Shellshock Apache Injection

QID: 150134
CVE Base: 10
CVSS Temporal: 8.5
Port: -
Category: Web Application
CVE ID: CVE-2014-6271, CVE-2014-7169

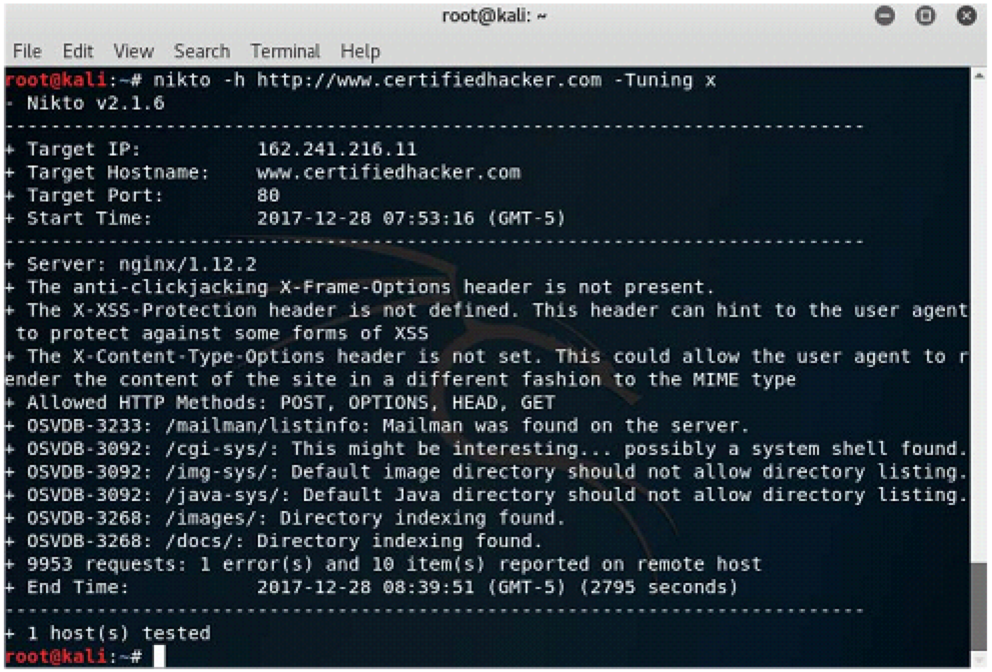
Threat:
ShellShock vulnerability allows an attacker to execute arbitrary commands by leveraging the fact that environment variables can be created with specially crafted values before calling Bash shell.For e.g. injecting () {test;} ; echo; /bin/cat /etc/passwd in HTTP header injection reveals /etc/passwd file contents in the response.

Impact:
Environmental variables with an arbitrary name can contain any nefarious function which can potentially lead to network exploitation. The vulnerability is critical since any application hosted on web server using mod_cgi/mod_cgid module of Apache HTTP Server or code that calls the bash shell is vulnerable.

https://freescan.qualys.com

Nikto

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



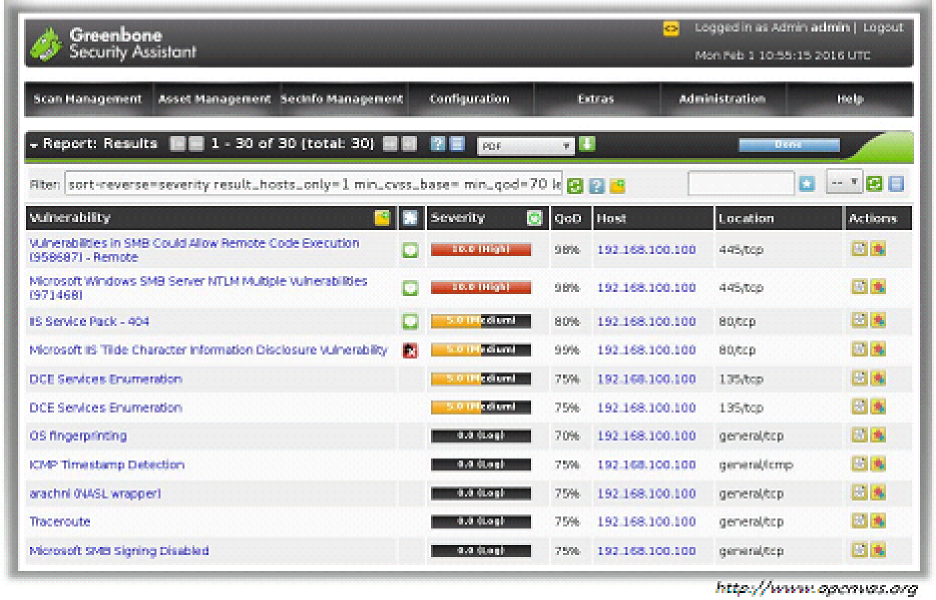
```
root@kali:~# nikto -h http://www.certifiedhacker.com -Tuning x
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          162.241.216.11
+ Target Hostname:    www.certifiedhacker.com
+ Target Port:        80
+ Start Time:         2017-12-28 07:53:16 (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

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**



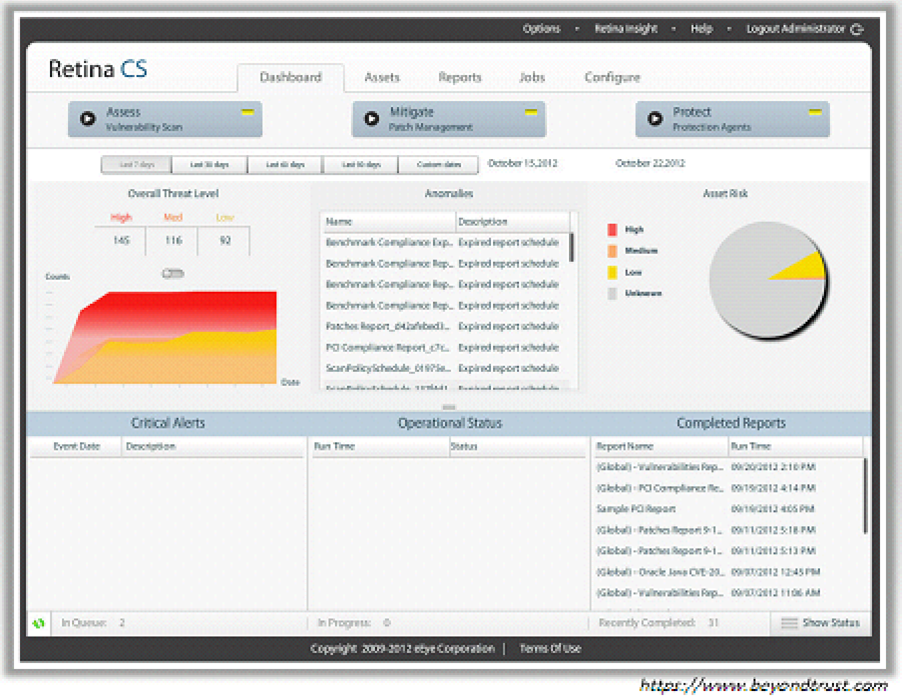
Filter: sort-reverse=severity result_hosts_only=1 min_cvss_base= min_qod=70 le

Vulnerability		Severity	QoD	Host	Location	Actions
Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote		10.0 (High)	98%	192.168.100.100	445/tcp	
Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)		10.0 (High)	98%	192.168.100.100	445/tcp	
IIS Service Pack - 404		5.0 (Medium)	80%	192.168.100.100	80/tcp	
Microsoft IIS Tilde Character Information Disclosure Vulnerability		5.0 (Medium)	99%	192.168.100.100	80/tcp	
DCE Services Enumeration		5.0 (Medium)	75%	192.168.100.100	135/tcp	
DCE Services Enumeration		5.0 (Medium)	75%	192.168.100.100	135/tcp	
OS fingerprinting		0.0 (Log)	70%	192.168.100.100	general/tcp	
ICMP Timestamp Detection		0.0 (Log)	75%	192.168.100.100	general/icmp	
arachni (NASL wrapper)		0.0 (Log)	75%	192.168.100.100	general/tcp	
Traceroute		0.0 (Log)	75%	192.168.100.100	general/tcp	
Microsoft SMB Signing Disabled		0.0 (Log)	75%	192.168.100.100	general/tcp	

http://www.openvas.org

Retina CS

- Retina CS is a vulnerability management software solution designed tc provide organizations with **context-aware vulnerability a:sessment** and **risk analysis**



High	Med	Low
145	116	92

Name	Description
Benchmark Compliance Exp...	Expired report schedule
Benchmark Compliance Rep...	Expired report schedule
Benchmark Compliance Rep...	Expired report schedule
Benchmark Compliance Rep...	Expired report schedule
Patches Report_d42afebed1...	Expired report schedule
PCI Compliance Report_c7c...	Expired report schedule
ScanPolicySchedule_01975e...	Expired report schedule

Event Date	Description

Run Time	Status

Report Name	Run Time
(Global) - Vulnerabilities Rep...	09/20/2012 2:10 PM
(Global) - PCI Compliance Re...	09/19/2012 4:14 PM
Sample PCI Report	09/19/2012 4:05 PM
(Global) - Patches Report 9-1...	09/11/2012 5:18 PM
(Global) - Patches Report 9-1...	09/11/2012 5:13 PM
(Global) - Oracle Java CVE-20...	09/07/2012 12:45 PM
(Global) - Vulnerabilities Rep...	09/07/2012 11:06 AM

In Queue: 2 In Progress: 0 Recently Completed: 31

Copyright 2009-2012 eEye Corporation | Terms Of Use

https://www.beyondtrust.com

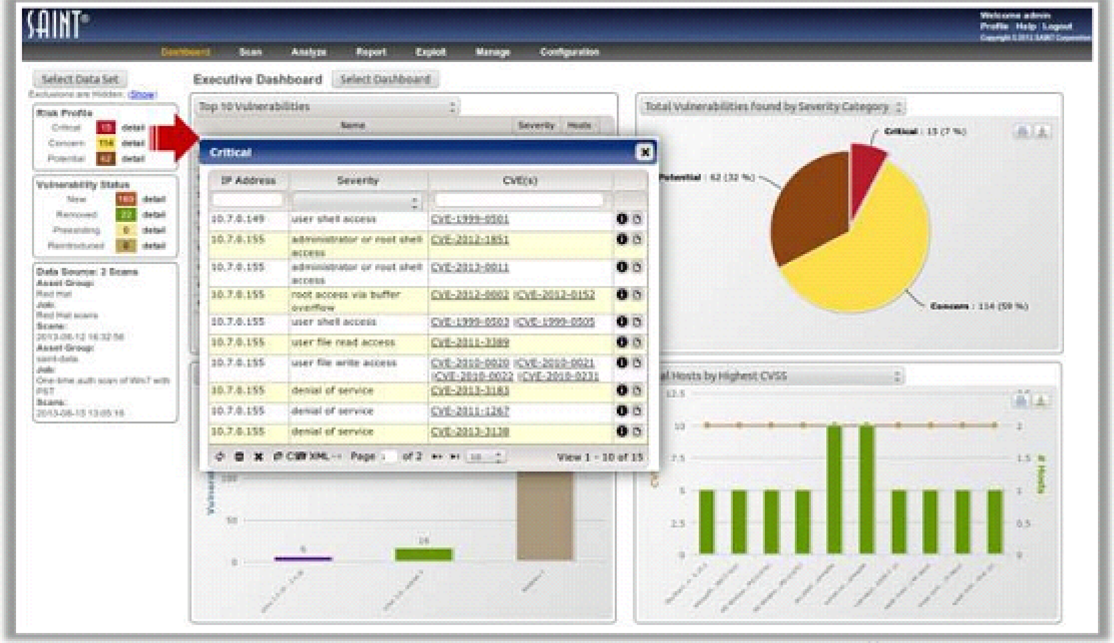
Vulnerability Assessment Tools: SAINT and Microsoft Baseline Security Analyzer (MBSA)

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.

Microsoft Baseline Security Analyzer (MBSA)

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

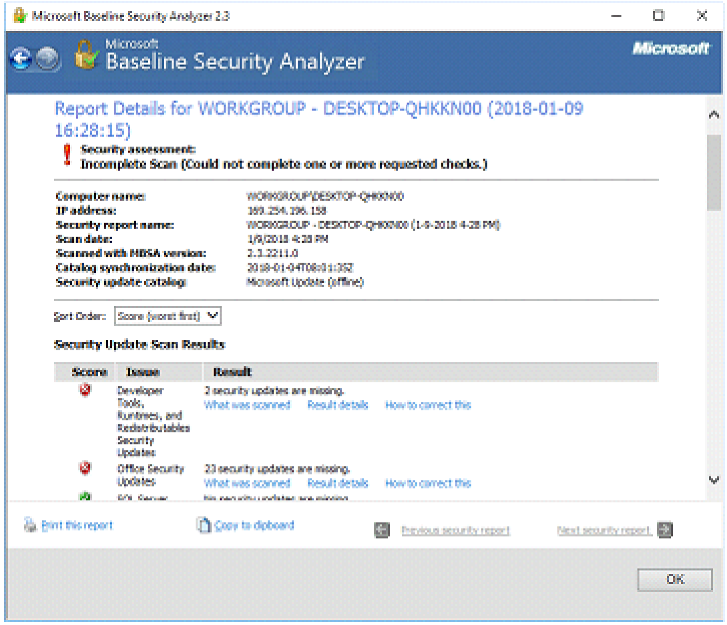


Critical

IP Address	Severity	CVE(s)
10.7.0.149	user shell access	CVE-1999-0501
10.7.0.155	administrator or root shell access	CVE-2012-1851
10.7.0.155	administrator or root shell access	CVE-2013-0011
10.7.0.155	root access via buffer overflow	CVE-2012-0002 |CVE-2012-0152
10.7.0.155	user shell access	CVE-1999-0503 |CVE-1999-0505
10.7.0.155	user file read access	CVE-2011-3389
10.7.0.155	user file write access	CVE-2010-0020 |CVE-2010-0021 |CVE-2010-0022 |CVE-2010-0231
10.7.0.155	denial of service	CVE-2013-3183
10.7.0.155	denial of service	CVE-2011-1267
10.7.0.155	denial of service	CVE-2013-3138

Page 1 of 2 View 1 - 10 of 15

http://www.saintcorporation.com



Report Details for WORKGROUP - DESKTOP-QHKKN00 (2018-01-09 16:28:15)

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

Computer name:	WORKGROUP\DESKTOP-QHKKN00
IP address:	169.254.196.158
Security report name:	WORKGROUP - DESKTOP-QHKKN00 (1-9-2018 4-28 PM)
Scan date:	1/9/2018 4:28 PM
Scanned with MBSA version:	2.3.2211.0
Catalog synchronization date:	2018-01-04T08:01:35Z
Security update catalog:	Microsoft Update (offline)

Sort Order: Score (worst first)

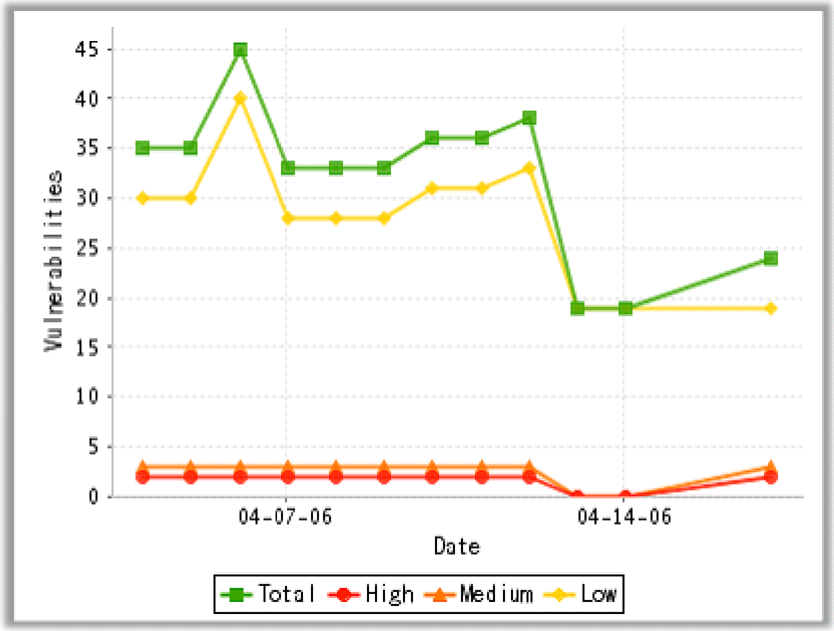
Security Update Scan Results

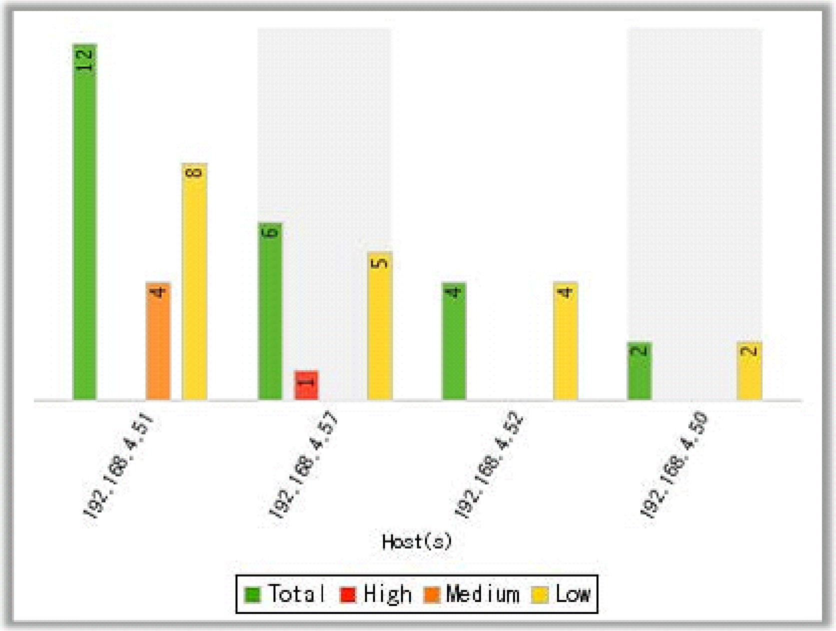
Score	Issue	Result
☒	Developer Tools, Runtimes, and Redistributables Security Updates	3 security updates are missing. What was scanned Result details How to correct this
☒	Office Security Updates	23 security updates are missing. What was scanned Result details How to correct this
✓	SQL Server	No security updates are missing.

https://www.microsoft.com

AVDS - Automated Vulnerability Detection System

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





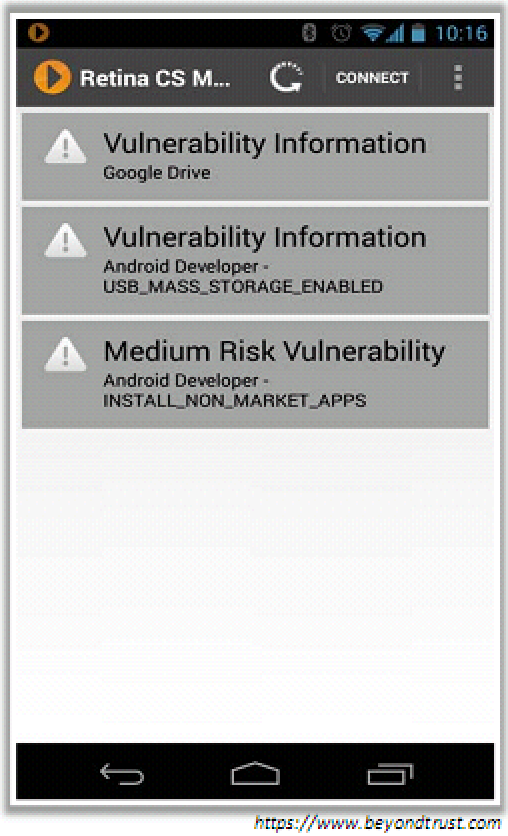
https://www.beyondsecurity.com

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



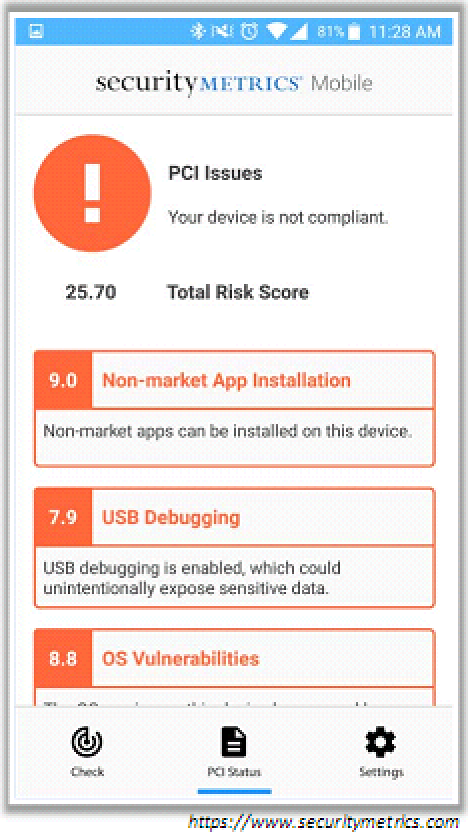
Vulnerability Information
Google Drive

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.

7.9 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*)

Module Flow

1 Vulnerability Assessment Concepts

2 Vulnerability Assessment Solutions

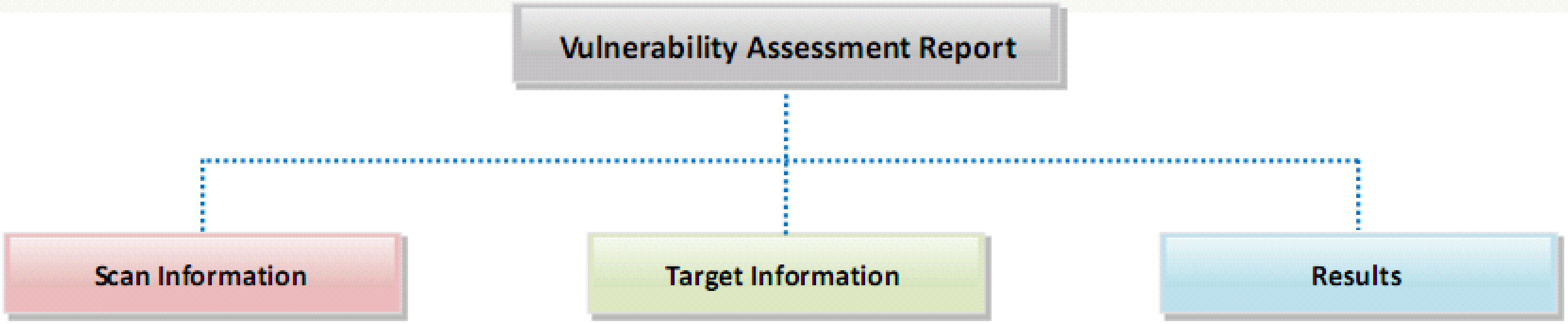
3 Vulnerability Scoring Systems

4 Vulnerability Assessment Tools

5 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



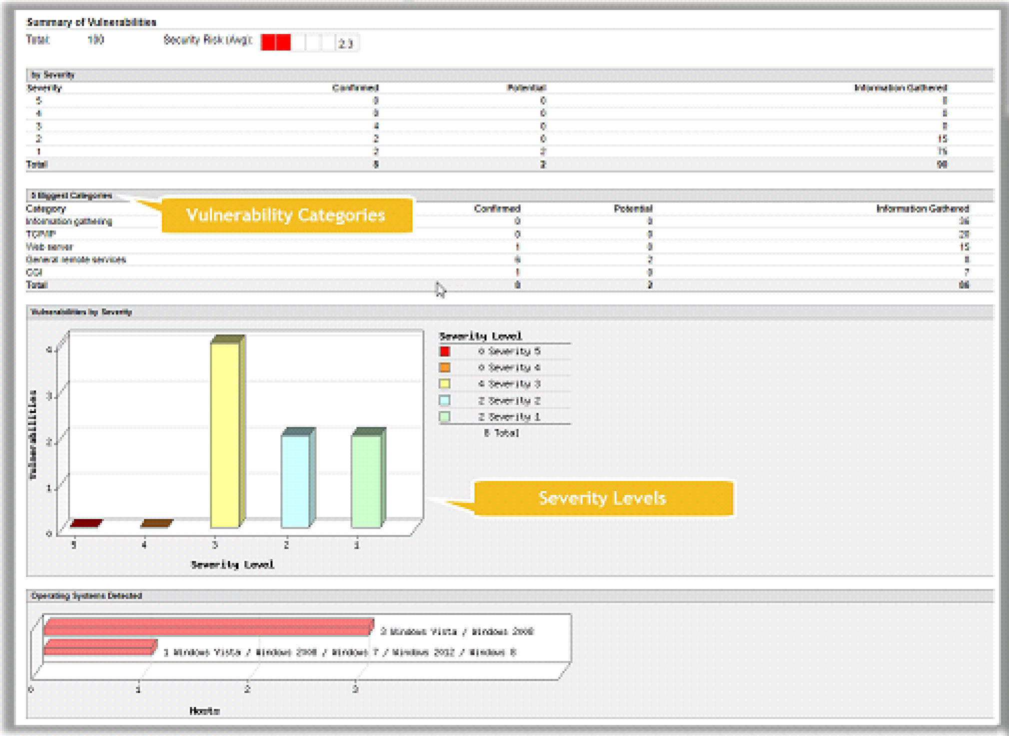
Vulnerability Assessment Report

Scan Information

Target Information

Results

Analyzing Vulnerability Scanning Report



Summary of Vulnerabilities

Total: 100 Security Risk (Avg): 2.3

by Severity			
Severity	Confirmed	Potential	Information Gathered
5	0	0	8
4	0	0	8
3	4	0	8
2	2	0	15
1	2	2	75
Total	8	2	98

5 Biggest Categories			
Category	Confirmed	Potential	Information Gathered
Information gathering	0	0	36
TCP/IP	0	0	28
Web server	1	0	15
General remote services	6	2	8
CGI	1	0	7
Total	8	2	66

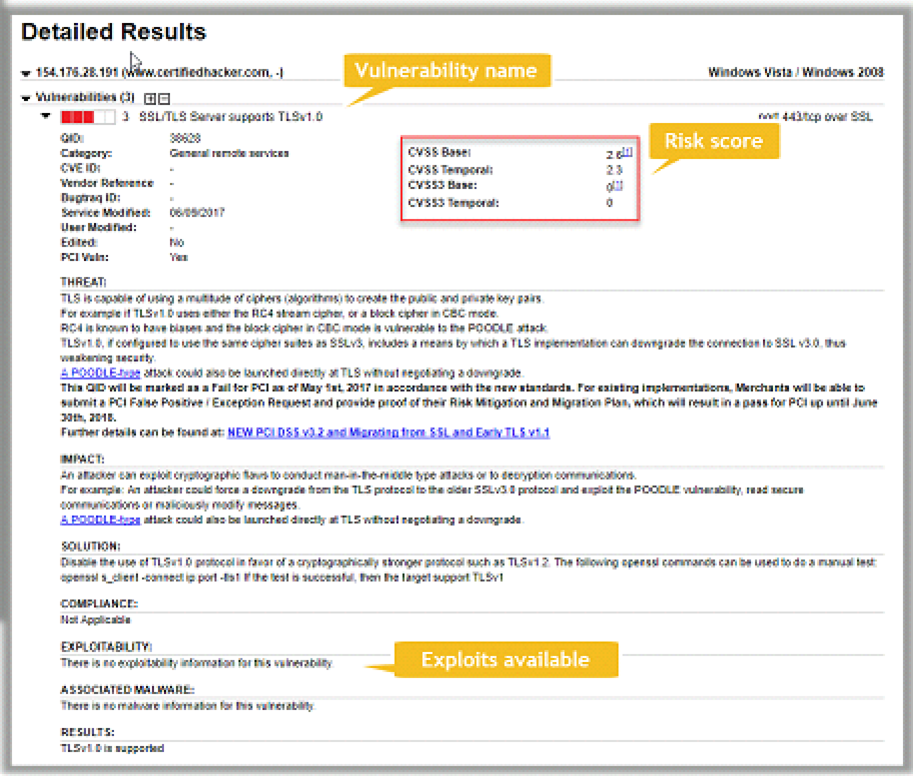
Vulnerability Categories

Vulnerabilities by Severity

Severity Levels

Operating Systems Detected

3 Windows Vista / Windows 2008
1 Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8
0
1
2
3
Hosts



Detailed Results

▾ 154.176.28.191 (www.certifiedhacker.com, -) Windows Vista / Windows 2008

Vulnerability name

▾ Vulnerabilities (3) ⊞⊟

▾ 3 SSL/TLS Server supports TLSv1.0 port 443/tcp over SSL

QID:	38628
Category:	General remote services
CVE ID:	-
Vendor Reference	-
Bugtraq ID:	-
Service Modified:	06/09/2017
User Modified:	-
Edited:	No
PCI Vuln:	Yes

CVSS Base:	2.6[1]
CVSS Temporal:	2.3
CVSS3 Base:	0[1]
CVSS3 Temporal:	0

Risk score

THREAT:

TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs.
For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.
TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.
A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.
This QID will be marked as a Fail for PCI as of May 1st, 2017 in accordance with the new standards. For existing implementations, Merchants will be able to submit a PCI False Positive / Exception Request and provide proof of their Risk Mitigation and Migration Plan, which will result in a pass for PCI up until June 30th, 2018.
Further details can be found at: NEW PCI DSS v3.2 and Migrating from SSL and Early TLS v1.1

IMPACT:

An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.
For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.
A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:

Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2. The following openssl commands can be used to do a manual test:
openssl s_client -connect ip:port -tls1 If the test is successful, then the target support TLSv1

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

Exploits available

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.0 is supported

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