



Romel Cabiling ▾



Home

Home > My courses > Network Attacks: Detection, Analysis & Counter... > 03 Internal Vulnerability Scanning > Lesson Proper for Week 3

Lesson Proper for Week 3

INTERNAL VULNERABILITY SCAN

Internal Vulnerability Scans

Specifically examines an organization's security profile from the perspective of an insider or someone who has access to systems and networks behind the organization's external security perimeter.

An internal vulnerability scan is carried out from inside an enterprise network. These scans allow you to harden and protect applications and systems that are not covered by external scans.

An internal vulnerability scan can detect issues such as: –

Vulnerabilities that can be exploited by an adversary who has penetrated the perimeter defences

Threat posed by malware that has made it to inside the network

Identify “**insider threats**” posed by disgruntled employees or contractors

INTERNAL VULNERABILITY SCANNING TOOLS

1. Microsoft Baseline Security Analyzer(MBA)

It is a standalone security and vulnerability scanner designed to provide a streamlined method for identifying common security misconfigurations and missing security updates.



How MBSA works

1. The MBSA can scan one or more computers by domain, IP address range or other grouping.
2. The MBSA provides a detailed report and instructions on how to help turn your system into a more secure working environment.
3. The MBSA provides dynamic assessment of missing security updates.

System Requirements:

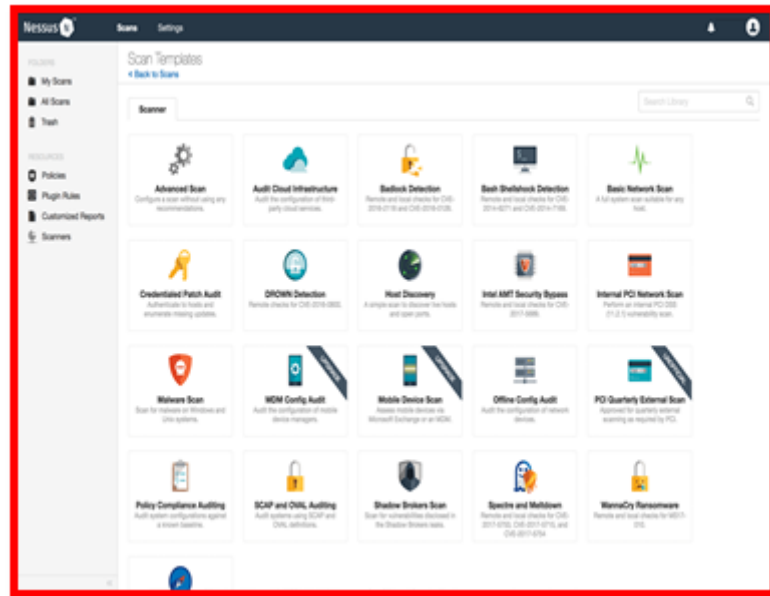
Before installing MBSA, make sure that your computer meets the following minimum requirements:

- In order to perform a scan you MUST have administrator privileges.
- Software:
 - § The latest Windows Update Agent (WUA) client. MBSA automatically updates computers that need an updated WUA client if 'Configure computers for Microsoft Update and scanning prerequisites' is selected.
 - § IIS (Internet Information Services) 5.0, 5.1 or 6.0 (required for IIS vulnerability checks).
 - § SQL Server 2000 or MSDE 2.0 (required for SQL vulnerability checks).
 - § Windows Server 2008 R2, Windows 7, Server 2003, Server 2008, Vista, XP or Windows 2000 and will need administrator privileges sufficient to scan the target computers.

2. Nessus

A remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network.

A tool that checks computers to find vulnerabilities that hackers COULD exploit.



Nessus can scan these vulnerabilities and exposures:

- Vulnerabilities that could allow unauthorized control or access to sensitive data on a system
- Misconfiguration (e.g. open mail relay)
- Denials of service (Dos) vulnerabilities
- Default passwords, a few common passwords, and blank/absent passwords on some system accounts
- Software flaws, missing patches, malware and misconfiguration errors across a wide range of operating systems, devices and applications are dealt with by Nessus.

The Nessus server is currently available for:

- Unix
- Linux
- FreeBSD

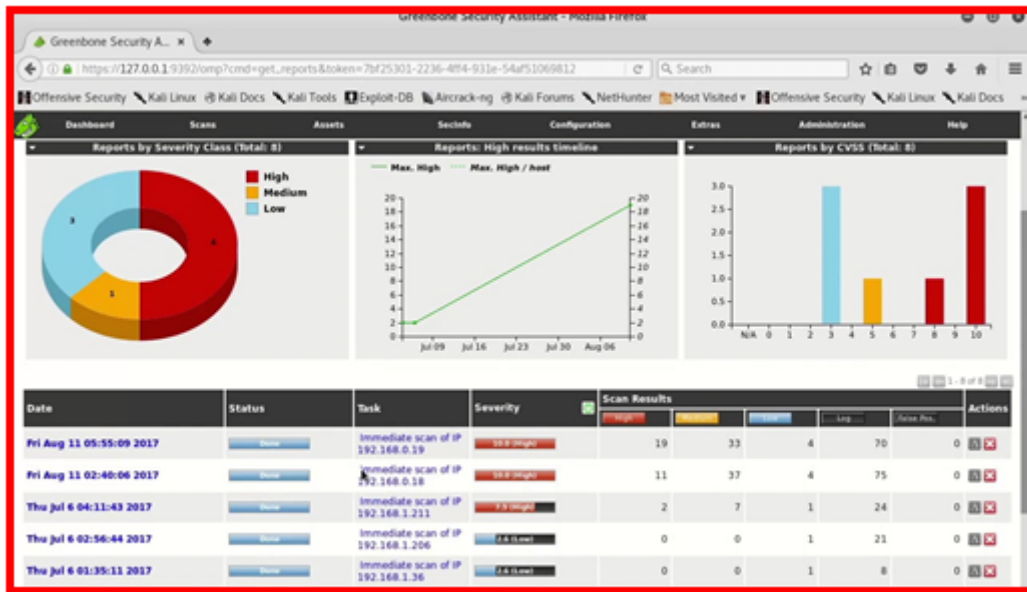
Also, the client is available for:

- Unix-based operating systems
- Windows-based operating systems

3. OpenVAS

The Open Vulnerability Assessment System, known more commonly as OpenVAS, is a suite of tools that work together to run tests against client computers using a database of known exploits and weaknesses.

A comprehensive vulnerability assessment system that can detect security issues in all manner of servers and network devices.



Brief History:

- o The scanner is developed and maintained by Greenbone Networks since 2009.
- o In 2008, two further companies became active, Secpod from India and Security Space from Canada. Both of them had a focus on contributing vulnerability tests, and teamed up with Greenbone to start producing a reliable and up-to-date feed of vulnerability tests.
- o The OpenVAS scanner was carefully improved, and quickly lost compatibility with its ancestor. All the Open Source works were published under the brand "OpenVAS". The first "Greenbone Security Manager" appliance products entered the market in the spring of 2010.
- o In the years 2010 to 2016, the commercial product was systematically improved and extended
- o In March 2017, the so-called OpenVAS framework reached version 9
- o In 2019 the branding separation was completed. OpenVAS now represents the actual vulnerability scanner as it did originally. The framework where OpenVAS is embedded is the Greenbone Vulnerability Management.

Pros of OpenVAS

- OpenVAS is a free open-source vulnerability assessment tool that is maintained by Greenbone Networks.
- Common vulnerabilities and exposure (CVE) coverage of around 26,000
- Popular and useful among SME's

- Built to be an all-in-one scanner
- The scan engine of OpenVAS is updated on a regular basis
- Greenbone provides thorough tutorials for the usage of this tool

Cons of OpenVAS

- Covers fewer CVEs as compared to Nessus
- Less operating system supportability
- Does not offer policy management

◀ Preliminary Activity for Week 3

Jump to...



Analysis, Application, and Exploration for Week 3 ▶



Navigation

Home



Dashboard

Site pages

My courses

Capstone Project 1

Network Attacks: Detection, Analysis & Counter...

Participants

General


01 The Home Router

02 External Vulnerability Scanning - Shodan, Qual...


03 Internal Vulnerability Scanning

 Preliminary Activity for Week 3

 **Lesson Proper for Week 3**

 Analysis, Application, and Exploration for Week 3

 Generalization for Week 3

 Evaluation for Week 3

 Assignment for Week 3

04 Open Source Custom Router Firmware

Ojt/Practicum 1

Social And Professional Issues

System Integration And Architecture 2

Courses

Fair Warning

NOTICE: Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for ***free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission.***

PROSECUTION: Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.

COURSE OF ACTION: Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.

Activities

 Assignments

 Forums

 Quizzes

 Resources