

Forum:[Hack Forums](#)

Thread: [Vulnerability Scanners](#)

Mr.Nobody - April 12, 2020, 11:26 pm

1. Comodo HackerProof

Comodo's HackerProof is considered to be a revolutionary vulnerability scanning and trust building tool that enables overcoming the security concerns of your visitors. Following are a few key benefits you can obtain from HackerProof:

- Reduce cart abandonment
- Daily vulnerability scanning
- PCI scanning tools included
- Drive-by attack prevention
- Build valuable trust with visitors
- Convert more visitors into buyers

Besides the above-mentioned benefits, HackerProof also provides the visual indicator needed by your customers to feel safe transacting with you. It helps decrease shopping cart abandonment, enhance conversion rates, and drive your overall revenue up. Finally, it includes patent-pending scanning technology, SiteInspector, which is capable of eliminating drive-by attacks, thus providing a new level of security for all those who proudly display the HackerProof logo.

2. OpenVAS

This is an open source tool serving as a central service that provides vulnerability assessment tools for both vulnerability scanning and vulnerability management. OpenVAS supports different operating systems

The scan engine of OpenVAS is constantly updated with the Network Vulnerability Tests

OpenVAS scanner is a complete vulnerability assessment tool identifying issues related to security in the servers and other devices of the network

OpenVAS services are free of cost and are usually licensed under GNU General Public License (GPL)

3. Nexpose Community

Developed by Rapid7, Nexpose vulnerability scanner is an open source tool used for scanning the vulnerabilities and carrying out a wide range of network checks. Nexpose can be incorporated into a Metasploit framework

It takes into account the age of the vulnerability like which malware kit is employed in it, what advantages are used by it etc. and fixes the issue based on its priority

It is capable of automatically detecting and scanning the new devices and evaluating the vulnerabilities when they access the network

It monitors the exposure of vulnerabilities in real-time, familiarizing itself to latest hazards with new data

Most of the vulnerability scanners usually categorize the risks employing a medium or high or low scale.

4. Nikto

Nikto is a greatly admired and open source web scanner employed for assessing the probable issues and vulnerabilities.

It is also used for verifying whether the server versions are outdated, and also checks for any particular problem that affects the functioning of the server

Nikto is used to perform a variety of tests on web servers in order to scan different items like a few hazardous files or programs

It is not considered as a quiet tool and is used to test a web server in the least possible time

It is used for scanning different protocols like HTTPS, HTTPd, HTTP etc. This tool allows scanning multiple ports of a specific server.

5. Tripwire IP360

Developed by Tripwire Inc, Tripwire IP360 is considered to be a leading vulnerability assessment solution that is employed by different agencies and enterprises in order to manage their security risks.

It uses a wide-ranging view of networks to spot all the vulnerabilities, configurations, applications, network hosts etc.

It uses the open standards to help in the integration of risk management and vulnerability into multiple processes of the business.

6. Wireshark

Wireshark is an extensively used network protocol analyzer considered to be the most powerful tool in the security practitioners toolkit.

Wireshark is used across different streams like government agencies, enterprises, educational institutions etc.. to look into the networks at a microscopic level

It captures the issues online and executes the analysis offline

It runs on different platforms like Linux, macOS, Windows, Solaris etc.

7. Aircrack

Aircrack, also known as Aircrack-NG, is a set of tools employed for assessing the WiFi network security.

Aircrack tools are also used in network auditing

It supports multiple OS like Linux, OS X, Solaris, NetBSD, Windows etc.

It focuses on different areas of WiFi Security like monitoring the packets and data, testing the drivers and cards, replaying attacks, cracking etc.

With Aircrack, it is possible to retrieve the lost keys by capturing the data packets.

8. Nessus Professional

Nessus tool is a branded and patented vulnerability scanner created by Tenable Network Security.

It prevents the networks from the penetrations made by hackers by assessing the vulnerabilities at the earliest

It can scan the vulnerabilities which permit remote hacking of sensitive data from a system

It supports an extensive range of OS, DBs, applications and several other devices among cloud infrastructure, virtual and physical networks

It has been installed and used by millions of users all over the world for vulnerability assessment, configuration issues etc.

9. Retina CS Community

Retina CS is an open source and web-based console that has helped the vulnerability management to be both simplified and centralized.

With its feasible features like compliance reporting, patching and configuration compliance, Retina CS provides an assessment of cross-platform vulnerability

Retina CS help save the time, cost and effort for managing the network security

It is included with automated vulnerability assessment for DBs, web applications, workstations, and servers

Being an open source application, Retina CS presents complete support for virtual environments like vCenter integration, virtual app scanning etc.

10. Microsoft Baseline Security Analyzer (MBSA)

MBSA is a free Microsoft tool ideal for securing a Windows computer based on the specifications or guidelines set by Microsoft.

MBSA allows enhancing their security process by examining a group of computers for any misconfiguration, missing updates, and any security patches etc.

It can only scan for security updates, service packs and update rollups putting aside the Critical and Optional updates

It is used by medium-sized and small-sized organizations for managing the security of their networks

After scanning a system, MBSA will present a few solutions or suggestions related to fixing of the vulnerabilities

Chameleon - April 13, 2020, 12:07 am

Wow super informal, thank you for spending the time on this!

Bastille - April 13, 2020, 12:43 am

Some references I didn't know, I'll save this thread to check it later

Not really an hacking tutorial though.

Dotexe - April 14, 2020, 10:33 pm

How is that considered as a hacking tutorial ? At least you are good in one thing, copy and pasting. Fairly certain if i ask how does one operate in a different way you won't be able to answer me