Top 10 best pentest tools 2021

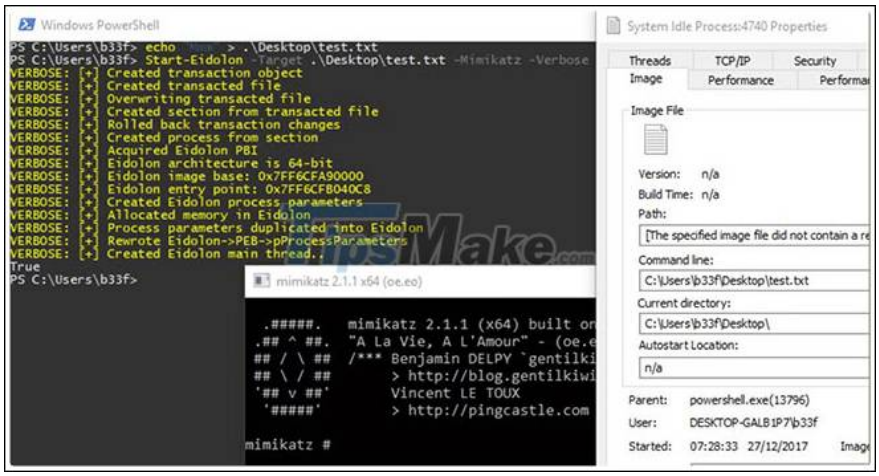
Penetration testing (pentest) has become an essential part of the security verification process. While it's nice to have so many penetration testing tools to choose from, with so many that perform similar functions, it can be difficult to choose which one gives you the best value.

In today's article, Tipsmake will join you to find out the top 10 best pentest tools available today.

1. Powershell-Suite

Powershell-Suite is a collection of PowerShell scripts that extract information about processes, processes, DLLs, and many other aspects of a Windows machine. By scripting specific tasks together, you can quickly navigate and test which systems on the network are vulnerable to exploitation.

1. Best used for purposes: Making automated tasks easy to spot vulnerable content on the network.
2. Supported Platforms: Windows



2. Zmap

Zmap is a lightweight network scanner capable of scanning everything from your home network to the entire Internet. This free network scanner is best used to gather basic details about the network. If you only have one IP range to use, use Zmap to get a quick overview of the network.

1. Best used for the purpose: Gathering information and classifying initial attack scenarios.
2. Platforms Supported: Zmap is supported on a variety of Linux and macOS platforms

3. Xray

Xray is an excellent network mapping tool that uses the OSINT framework. Xray uses word lists, DNS requests and any API keys to help identify open ports on the network from the outside.

1. Best used for: Pentest performers gain access to the network without help
2. Supported Platforms: Linux and Windows

4. SimplyEmail

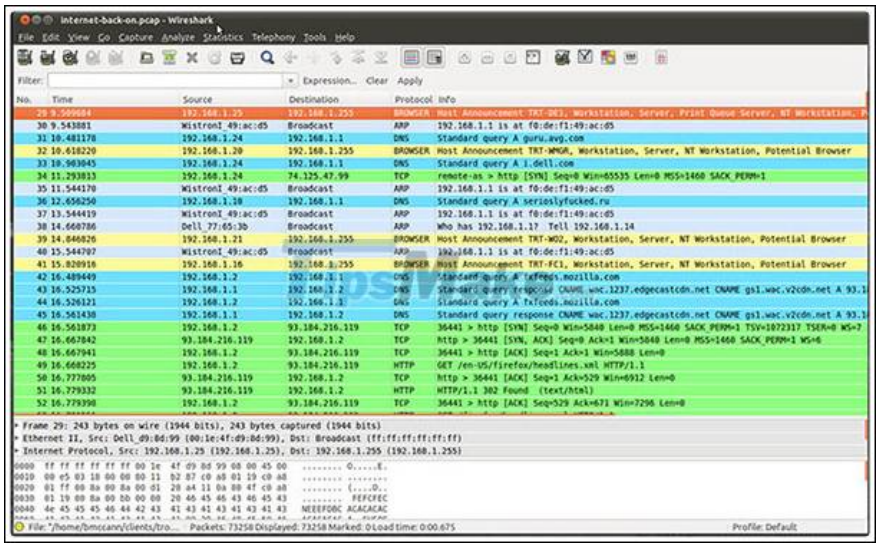
SimplyEmail is a tool used to help collect relevant information found on the Internet based on someone's email address. SimplyEmail works to search the Internet for any data that might help provide information about any email address.

1. Best used for: Pentesters looking to list accounts for enterprise-grade testing commitments.
2. Supported Platforms: Docker, Kali, Debian, Ubuntu, macOS

5. Wireshark

Wireshark is possibly the most widely used network protocol analysis tool worldwide. Network traffic collected via Wireshark can show which protocols and systems are active, which accounts are most active, and allow an attacker to intercept sensitive data. Refer to the article: Using Wireshark to analyze the data packets in the network for details.

1. Best used for: Network visibility at a deep level of communication.
2. Supported Platforms: Windows, Linux, macOS, Solaris



6. Hashcat

Hashcat is one of the fastest password recovery tools to date. By downloading the Suite version, you get access to the password recovery tool, word generator and password cracking element. Dictionary, Combination, Brute-

force, Rule-based, Toggle-case, and Hybrid password attacks are fully supported. Best of all, Hashcat has a great online community to help with bug fixes, WiKi site and tutorials.

1. Best used for: System recovery experts or pentester looking for the best password recovery tool for claiming ownership in their business.
2. Supported Platforms: Linux, Windows, and macOS

7. John the Ripper

John the Ripper is a password cracking tool. Its sole purpose is to find weak passwords on a certain system and reveal them. John the Ripper is a tool that can be used for both security purposes and for checking compliance with regulations. John is known for his ability to quickly reveal weak passwords in a short amount of time.

1. Best used for purposes: Cracking passwords for newbies
2. Supported Platforms: Windows, Unix, macOS, Windows

8. Hydra

Hydra is also a password cracking tool, but with a difference. Hydra is a single password application tool that supports multiple protocols and parallel connections at the same time. This feature allows penetration testers to try to crack multiple passwords on different systems at the same time without losing connection if unbreakable.

1. Best used for purposes: Cracking passwords for professionals
2. Supported Platforms: Linux, Windows, Solaris, macOS

9. Aircrack-ng

Aircrack-ng is an all-in-one wireless network security tool for penetration testing. Aircrack-ng has four main functions that make it stand out in the segment; It performs monitoring of network packets, attacks through packet infecting, WiFi capabilities testing, and finally password cracking.

1. Best used for: Command line users who prefer to create attacks or defenses.
2. Supported Platforms: Windows, OS X Solaris, Linux

10. Burp Suite

For the pentesting of web applications, Burp Suite is an essential tool. Burps UI is fully optimized for professionals working with built-in profiles, allowing configuration to be saved on a per-task basis.

1. Best used for: Professionals in charge of enterprise application security.
2. Supported Platforms: Windows, macOS, and Linux

Above are some of the best pentest tools in the present time that Tipsmake wants to introduce to readers. Hope you will find yourself a suitable option!

You finished reading the article "**Top 10 best pentest tools 2021**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
