Hping3

hping3 is a network tool able to send custom ICMP/UDP/TCP packets and to display target replies. What can you do with hping3? Using hping3, you can test firewall rules, perform (spoofed) port scanning, test network performance using different protocols, fingerprint remote operating systems, audit TCP/IP stacks, etc

Nmap

Nmap ("Network Mapper") is a free and open source utility for network discovery, host discovery, ports scanning, and security auditing and it even supports web app scan. vulnerability and version detection

Zphisher

Zphisher is a powerful open-source tool Phishing Tool. It became very popular nowadays that is used to do phishing attacks on Target. Zphisher is used in Phishing attacks. Zphisher tool is a very lightweight, simple and easy tool. Zphisher is written in bash language. It can create phishing pages for famous websites like facebook, etc

Nessus

Nessus is a open-source vulnerability 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. It is developed by Tenable inc. It can run over 1200 checks on a given computer.

Wireshark

Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network. Wireshark is the most often-used packet sniffer in the world.

- Network administrators use it to troubleshoot network problems.
- Network security engineers use it to examine security problems.
- QA engineers use it to verify network applications.
- Developers use it to debug protocol implementations.

Burpsuite

Graphical tool for performing security testing of web applications. It supports the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities. It is written in Java. It is developed by PortSwigger Security. It is available in both free and professional editions.

Low Orbit Ion

Low Orbit Ion Cannon (LOIC) is a widely available, open-source application developed by Praetox Technologies used for network stress testing, as well as denial of service (DoS) and distributed denial of service (DDoS) attacks.

What is the difference between low orbit ion cannon and high orbit ion cannon?

HOIC was designed to improve upon several LOIC application flaws, including: Detection – HOIC uses booster scripts that let perpetrators scatter attack traffic and hide their geolocation. This differs from LOIC, which isn't capable of obfuscating attacker IP addresses.

Autopsy

Autopsy® is a digital forensics platform and graphical interface. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can even use it to recover photos from your camera's memory card. It is an easy to use, GUI-based program that allows you to efficiently analyze hard drives and smart phones. It has a plug-in architecture that allows you to find add-on modules or develop custom modules in Java or Python

Zenmap

Zenmap is a graphical user interface for Nmap. It is a free and open-source software that helps you get up and running with Nmap. In addition to providing visual network mappings, Zenmap also allows you to save and search your scans for future use.

Disk Digger

DiskDigger® is a tool that undeletes and recovers lost files from your hard drive, memory cards, USB flash drives — you name it! Whether you accidentally deleted some documents or photos from your computer, reformatted your camera's memory card, or want to see what files are lurking on an old USB drive.

Windows event viewer

Windows program that lets the users and administrators view the event logs on local or remote systems. It useful for troubleshooting and evidence gathering.

Quick stego

QuickStego is a lightweight encryption tool designed specifically to conceal a message in pictures with the goal that only other users of QuickStego can recover and read the hidden secret words.

md5 hash

This MD5 hash generator is useful for encoding passwords, credit cards numbers and other sensitive date into MySQL, Postgress or other databases.

keylogger

it do the action of recording the keys struck on a keyboard, typically covertly, so that a person using the keyboard is unaware that their actions are being monitored. Data can then be retrieved by the person operating the logging program. Spyrix keylogger software.

Metasploit

The Metasploit framework is a very powerful tool which can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers. Because it's an open-source framework, it can be easily customized and used with most operating systems

EnCase

It is traditionally used in forensics to recover evidence from seized hard drives. It allows the investigator to conduct in-depth analysis of user files to collect evidence such as documents, pictures, internet history and Windows Registry information. The company also offers EnCase training and certification.

maltego

Maltego is software used for open-source intelligence and forensics. Maltego focuses on providing a library of transforms for discovery of data from open sources, and visualizing that information in a graph format, suitable for link analysis and data mining

MBSA

The Microsoft Baseline Security Analyzer (MBSA) is a software tool that helps determine the security of your Windows computer based on Microsoft's security recommendations.