Task 2

For the following explain how the security testing tools work and see if your can describe real life uses for these:

* NMap

NMap is a free and open-source security scanner. It is used to discover hosts and services on a computer network.

* OpenVAS

OpenVAS is a software framework of several services and tools offering vulnerability scanning and vulnerability management.

* Burp Suite

Burp or Burp Suite is a graphical tool for testing Web application security. The tool is written in Java and developed by PortSwigger Web Security.

* BeEF

BeEF is short for The Browser Exploitation Framework. It is a penetration testing tool that focuses on the web browser. BeEF will hook one or more web browsers and use them as beachheads for launching directed command modules and further attacks against the system from within the browser context.

* Metasploit

The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.

* OpenSSH

OpenSSH is a suite os secure networking utilities based on the Secure Shell protocol, which provides a secure channel over an unsecured network in a client-server architecture.

* Wireshark

Wireshark is a free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development and education.

* Kali Linux

Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing.

* Nagios

Nagios now known as Nagios Core, is a free and open source computer software application that monitors systems, networks and infrastructure.