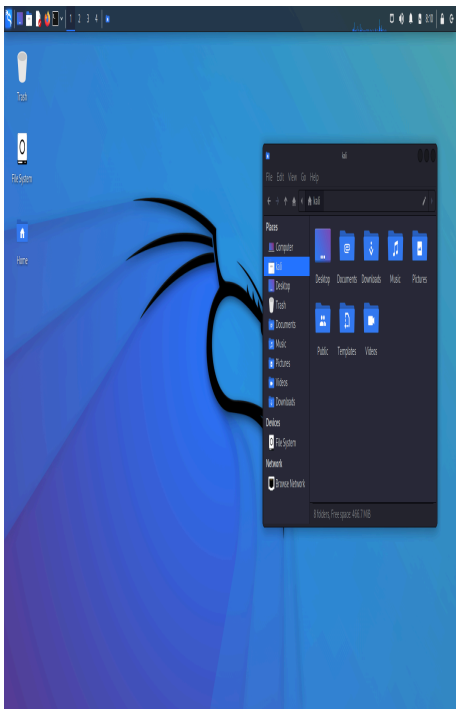
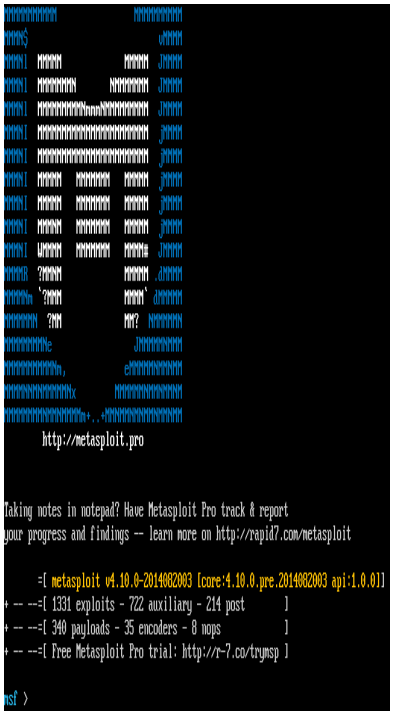
Kali Linux, Metasploit, and Splunk Tutorial





This cyber-security tutorial will help you understand how Kali Linux, Metasploit, and Splunk, fit into the Computer Science, Information Technology, and Cyber-Security industry.

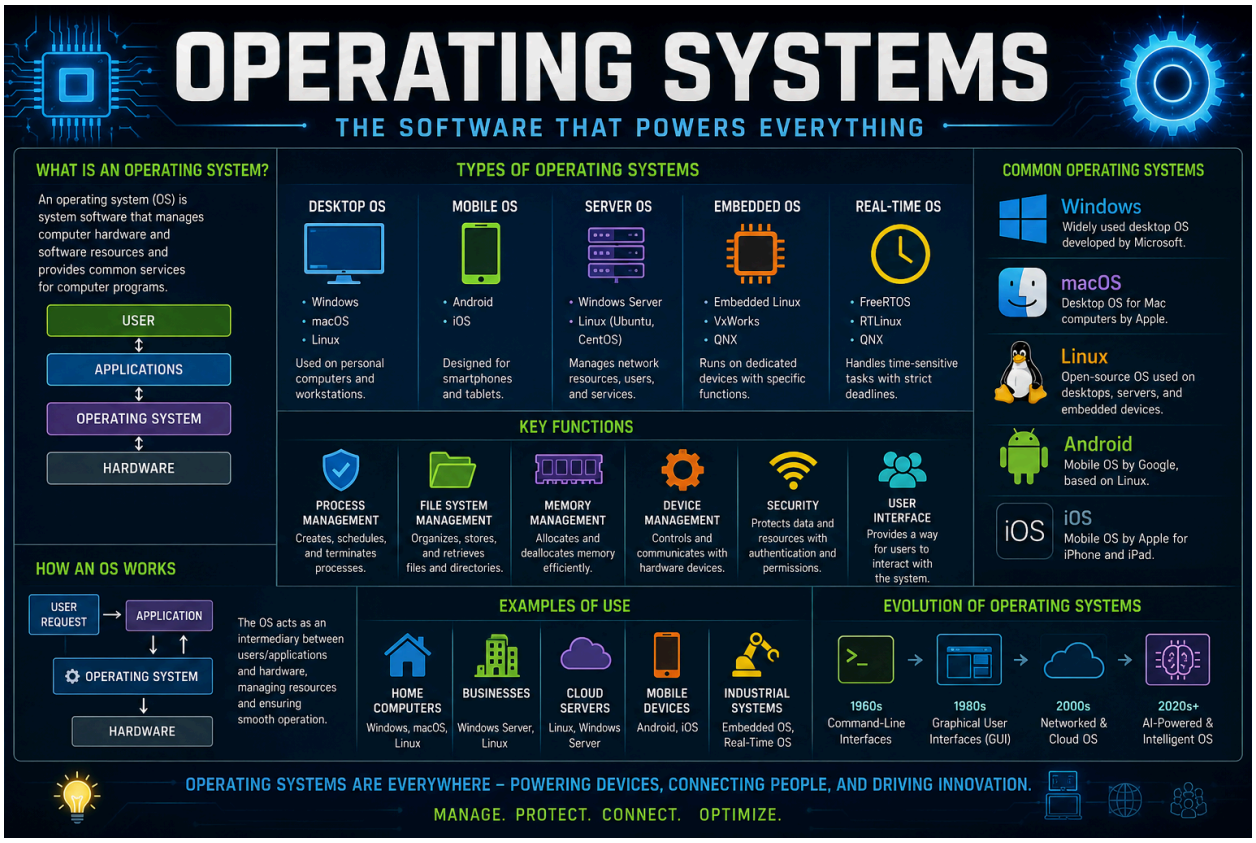
Cybersecurity has two main teams of professionals:

Offensive security

(Red Team): involves penetration tests, and testing systems by trying to destroy them and

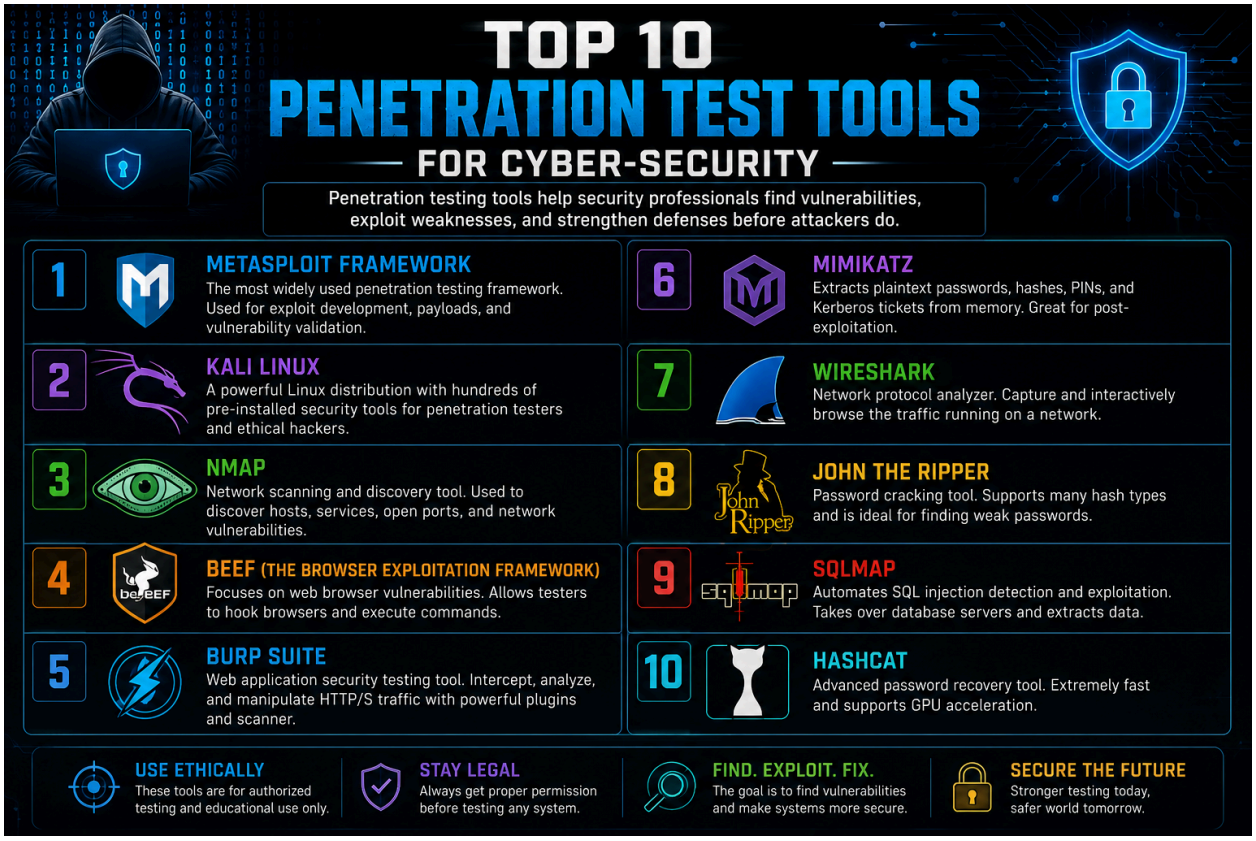
Defensive security

(Blue Team): monitors information infrastructures to detect and stop threats.



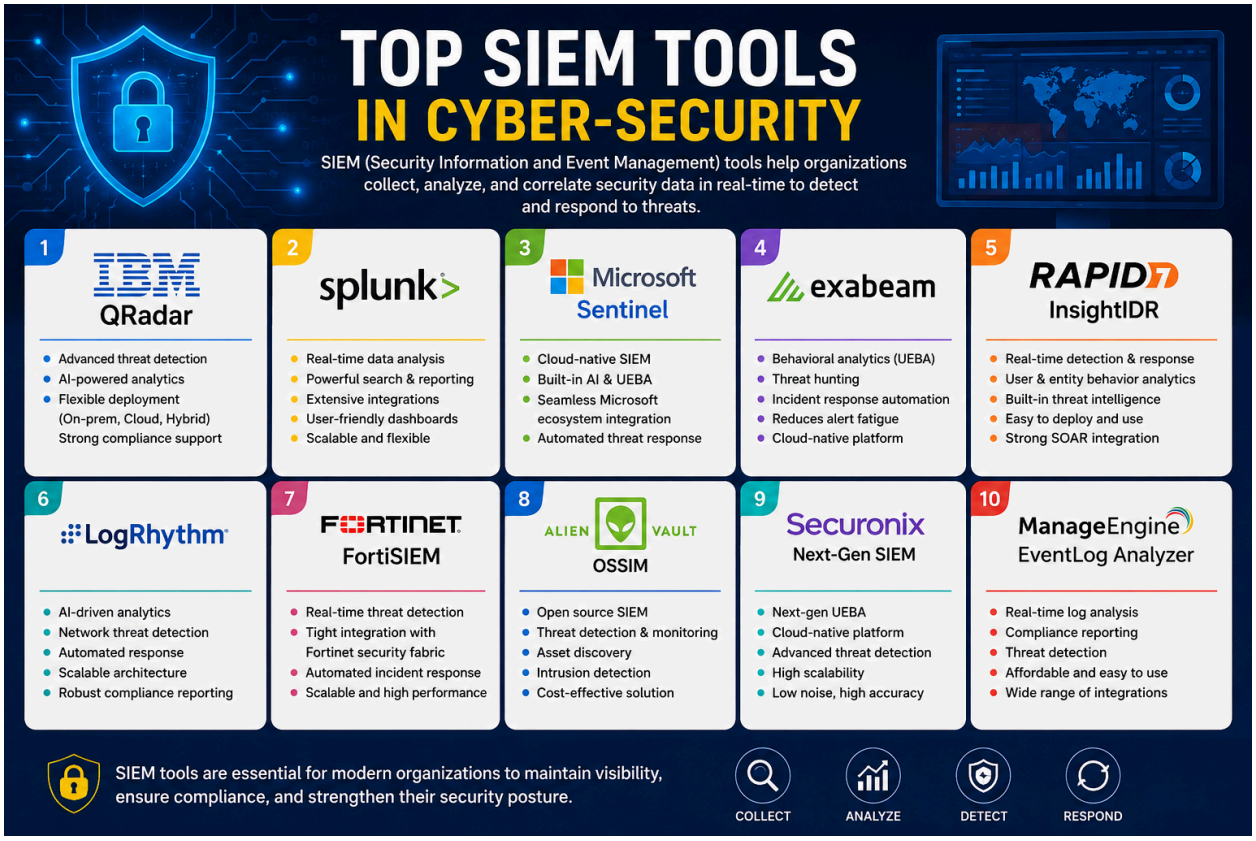
Kali Linux:

Kali is a no cost, cyber security operating system, built on Linux foundations that focuses on cyber-security offensive and defensive procedures. Kali is very different from windows or Max OS, Kali specializes in cyber-security and is pre-packaged with hundreds of cybersecurity industry tools used to audit networks, assess wireless security, and scan for software glitches, bugs, and malware.



Offensive Tool:

Metasploit: This tool is an automation framework that exists inside Kali Linux. Metasploit has a huge database of software glitches or vulnerabilities and exploits like malicious scripts that permits cyber-security professionals to safely assess if a target computer can be illegally accessed or broken into.

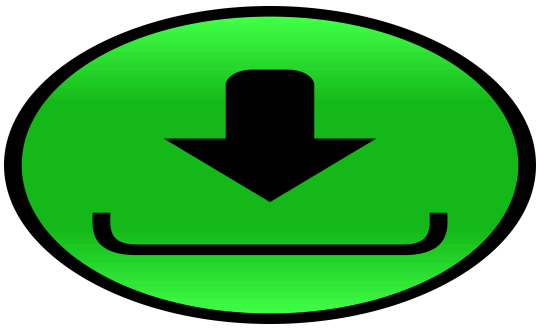


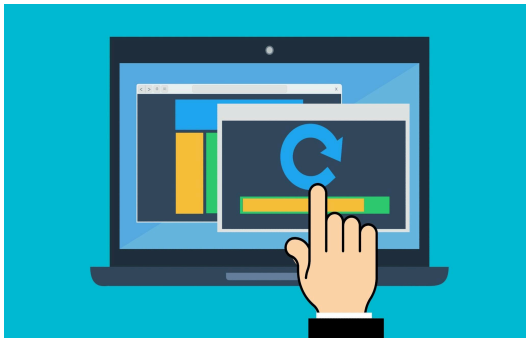
Defensive Tool:

Splunk:

Splunk is a data analytics and monitoring platform that acts like a digital security surveillance camera for a company's information technology infrastructure, it collects background files from all computers, servers, and the fire wall. This tool helps cyber-security defense teams to parse through millions of data areas of a network to find network exploiters in real time.

How to Download and Configure these Cyber-security Tools Safely:





The healthiest industry standard or best practices for setting up these cyber-security tools is to learn these tools at home within an isolated virtual machine environment. Implementing these tools inside a virtual machine (VM) makes sure that your assets and computers remain completely hazard free and not put in danger by your testing in this tutorial.

Step 1: Installation of the virtual environment

To operate virtually on computers inside your current operating system, you will need hypervisor software. A free hypervisor software is “virtual box”.

1. Login to your computer and go to the website virtualbox.org
2. Download the installer package that matches your current operating system. For example Windows, Linux, Chrome, and Mac OS.
3. Run the installer for Virtual Box and complete the default prompt to set up configuration.

Step 2: Download and Activate Kali Linux (includes Metasploit in the OS download)

Metasploit comes pre-installed inside Kali Linux.

1. Go to official website kali.org and click on “Get Kali”
2. Select the option to use “virtual machines.”

3. Download the pre-built image, specifically for “Virtual Box” (this will cause the download of a “.7z” or “.ova” file).
4. Open Virtual Box, click on “File Z import Appliance”, select the downloaded Kali file, and click import.
5. Once the file is imported, next you need to click the green “start” arrow. The default login username is “kali” named after the operating system and the password is also “kali”. In order to open and implement Metasploit inside the Kali Linux Operating system you need to open a terminal window and type the following command “sudo msfconsole.”

Step 3: Downloading and installing Splunk

To exercise detecting network activities, you need to install Splunk on a different test virtual machine or you can use Splunk on your main computer to analyze your lab data.

1. Go to the Splunk website Splunk.com
2. Click free Splunk or Sign up to create a free Splunk account.
3. Move through the products webpage and download Splunk Enterprise (Use the free trial version for your operating system such as Windows “.msi” or Linux “.deb”)
4. Run the Splunk installation tool, it will ask you to create an administrator “username” and “password” for your Splunk dashboard.
5. When Splunk is installed, open your web browser and go to the web address: http://localhost:8000 to login and view the defense dashboard.

References

Oracle. (n.w.). *Oracle VM VirtualBox*. VirtualBox. virtualbox.org

OffSec. (n.d.). *Download official Kali Linux images*. Kali Linux Documentation. kali.org

OffSec. (n.d.). *Get Kali Linux: Virtual machines*. Kali Linux. kali.org

Rapid7. (n.d.). *Metasploit framework overview*. Rapid7 Documentation. rapid7.com

Rapid7. (n.d.). *Metasploit framework getting started guide*. Rapid7 Documentation. rapid7.com

Splunk. (n.d.). *Splunk Enterprise documentation*. Splunk Help. splunk.com

Splunk. (2020, November 3). *Introducing Splunk Attack Range v1.4 with Caldera and Kali Linux integration*. Splunk Blog. splunk.com

Stark, J. (2023, March 15). *What is Splunk? A guide to the data platform*. Splunk Blog. splunk.com