# KALI LINUX ™

In this section, we're going to cover a Linux distribution that's widely used in security and discuss KALI LINUX™.
KALI LINUX™ is a trademark of Offensive Security and is Debian derived.
This open-source distro was made specifically with penetration testing and digital forensics in mind.
There are many tools pre-installed into KALI LINUX™.
It's important to note that KALI LINUX™ should be used on a virtual machine.
This prevents damage to your system in the event its tools are used improperly.
An additional benefit is that using a virtual machine gives you the ability to revert to a previous state.

As security professionals advance in their careers, some specialize in penetration testing.
A penetration test is a simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes.
KALI LINUX™ has numerous tools that are useful during penetration testing.
Let's look at a few examples.

To begin, Metasploit can be used to look for and exploit vulnerabilities on machines.
Burp Suite is another tool that helps to test for weaknesses in web applications.
And finally, John the Ripper is a tool used to guess passwords.
As a security analyst, your work might involve digital forensics.
Digital forensics is the process of collecting and analyzing data to determine what has happened after an attack.
For example, you might take an investigative look at data related to network activity.
KALI LINUX™ is also a useful distribution for security professionals who are involved in digital forensic work.
It has a large number of tools that can be used for this. As one example, tcpdump is a command-line packet analyzer. It's used to capture network traffic.
Another tool commonly used in the security profession is Wireshark.
It has a graphical user interface that can be used to analyze live and captured network traffic.
And as a final example, Autopsy is a forensic tool used to analyze hard drives and smartphones.
These are just a few tools included with KALI LINUX™.
This distribution has many tools used to conduct pen testing and digital forensics.

We've explored how KALI LINUX™ is an important distribution that's widely used in security, but there are other distributions that security professionals use as well.
Next we'll explore a few more distributions.

quick note from the student.. the course says to use it on a VM, however you can use it as your own flavor of Linux for your desktop. its not recommended unless you know what you are doing or willing to wipe the machine :p

---

Revision #1
Created 5 July 2023 09:44:35 by naruzkurai
Updated 5 July 2023 09:46:23 by naruzkurai