Penetration testing is the process of attacking a system to determine its vulnerabilities before a perpetrator in order to eliminate them to secure the system. In penetration testing a virtual lab is built containing Kali linux for testing purposes and ensures that access is limited to the local network. By limiting access, we can use testing tools such as test scans and probes that would otherwise be considered illegal on the internet. Virtualization is not only a good way to create a lab but also allows us to deal with potentially dangerous tools. By using virtualization, the tester can take snapshots of the system which would be used to recover the system just in case of a malware infection. Virtualization comes in two different forms, one of which is the type 1 hypervisor also known as bare metal hypervisor and the type 2 hypervisor known as the hosted hypervisor. The type 1 hypervisor is installed directly onto the computer hardware. Examples of the type 1 hypervisor are microsoft’s hyper-v hypervisor and Vmware’s esxi hypervisor. Type 2 hypervisors are installed to a hosting operating system and include vmware and oracle’s virtualbox.

Kali linux is a linux distribution that was built for security work and includes over 300 security testing tools. It is the new name of a security testing suite that started out called backtrack and is the most used tool in penetration testing. It contains information gathering tools about a target by probing the target directly. These include, gathering dns information to profile a target system and identifying any ids to filter traffic. One of the information gathering tools on Kali is dmitry (Deep magic information gathering tool). Dmitry can be used to look up hosts, identify subdomains and scan the target for open ports. The first thing that dmitry provides, is the target’s IP address followed by the target’s subdomains and finally the registration information of the target. Dmitry can also be used for port scanning by using the -p and -b switches on one of the target servers. Another tool for information gathering is the DNSenum which is a DNS analysis tool that is used to enumerate information for a system, identify subdomains and provide the associated mail servers. The first thing we get from dnsenum is the host’s address which is followed by its associated name servers. By using the -s and -p switches, we can also get the subdomain information from the dns servers. Kali also contains vulnerability analysis tools used for vulnerability testing. One of the vulnerability analysis tools provided by Kali is nikto which is mainly used for web scanning. It is used to scan for vulnerabilities in the underlying webserver. Running nikto gives us the type of the webserver, the missing features, the version of the server and then the vulnerabilities based on the open source vulnerability database (OSVDB). Another and one of the most important tool for vulnerability scanning is the OpenVAS (The open Vulnerability Assessment System) tool, however, it doesn’t come pre-installed on Kali. The user has to manually install OpenVAS. OpenVAS is usually run through its web interface. An OpenVAS scan shows a number of vulnerabilities and their severity. By clicking on the report link, we get a full report of all alerts raised and their solutions where solutions exist. The solution shows a number of possible fixes to the alert. We also get links to individual vulnerabilities with their detailed reports, their severity and the host address. Clicking on individual alert links, takes you to the page containing the details of that alert. This page shows a summary of the report, the vulnerability detection result and the vulnerability detection method.

Since everyone has access and uses the internet, it is important to teach people about penetration testing and also provide them with tools to help them protect themselves against cyber-attacks. People have to be taught to think like perpetrators in order to know how to protect themselves. Kali linux is available for free and can be obtained by anyone on the internet. Kali is a great tool however, it is not as popular as other operating systems like windows, mac or other linux distributions. Most people rely heavily on antiviruses on their pcs but with the rapid evolution of cyber-attacks, the antiviruses can’t keep up with every attack. Recently Microsoft announced that they will be embedding a linux kernel in the upcoming windows 10 which is a great step towards protection against these attacks. With a linux kernel, windows users will be able to install tools like OpenVAS which are good at detecting and eliminating these attacks.

Kali is a great and one of the best tools at protecting oneself against cyber-attacks, however it is not as popular as other operating systems. One other tool that is available to people that don’t use Kali is wireshark. Wireshark formerly known as ethereal is an open source package analysis tool that is used for network packet analysis, network troubleshooting and network traffic analysis. Packet analysis is important in troubleshooting network congestion, create firewalls and intrusion detection. Packet analysis is mostly done by network administrators. It is a big topic to cover and takes a lot of time to master however, knowing the basics is enough to protect oneself against attacks and the tool that is most used for this is wireshark. If people are not comfortable using Kali, they should at least invest in learning some basic wireshark for protection. In addition to wireshark, there are some other packet analyzers like Cain and Abel which recovers passwords and can record voice over ip conversations, dSniff which monitors traffic like emails, passwords, etc. and Naruslnsight which monitors internet traffic. Although all these tools are great, the most used and recommended is wireshark

People need to be aware of cybersecurity issues and attacks. By raising awareness, people would be cautious about using the internet. Apart from raising awareness of cybersecurity, there needs to be free education and training about security. By providing free education, everyone would have access to the training material without any cost or barrier. People also need to be careful with what they post on social media as this is where attacks begin i.e. in the reconnaissance stage of an attack, the attacker usually uses information provided by social media or any other information that is publicly available. Penetration testing is a huge field that takes years to master but if people do learn about the two security tools (Kali linux and wireshark), the internet would be a secure place and everyone would know how to protect themselves against attacks. There would be less cyber criminals and people would feel safe while using the internet. For the people that need to specialize in security, there are courses like the CEH (Certified Ethical Hacker) by the EC-Council, CISM (Certified Information Security Manager), Comptia’s security+ and GSEC. I’m planning to learn some wireshark in the near future as I want to get CCIE certified in security. My family is ignorant about cybersecurity, but I try to remind them to visit secure websites to keep our network safe. They are not interested in learning either wireshark or Kali linux but once I get my CCIE in security, I will make sure that all their devices are secure.