M.Saeed Mohiti Lab05 116236159

1. **What is Kali?**
   Kali or Kali Linux is a security-focused operating system that you can run off a CD or USB anywhere. It is an open-source project that is funded and maintained by Offensive Security, the provider of a world-class penetration testing services and information security training. Kali Linux contains a whole toolkit (at least 300 pre-installed tools) used for many information security tasks.

2. **What is Kali used for?**
   As previously mentioned, Kali Linux has a pre-installed tools for many tasks towards information security such as Penetration Testing, Security research, Computer Forensics, and Reverse Engineering, Web Applications, Sniffing and Spooling, Hardware Hacking, Reporting, and so much more. A lot of famous and popular tasks that could be done with Kali Linux includes cracking Wi-Fi passwords with brute force techniques, creating fake networks and routers to trick machines into logging into it, eavesdrop on network communications.

3. **What are a couple of the major networking tools available on Kali?**
   Ten major networking tools available on Kali which are considered to be the major ten tools, include a variety of tasks of cracking code, exploitation, web applications and network scanning. Burp Suite, one of the major ten tools, is used for web applications pentesting. Wireshark is another big tool that is used as a network protocol analyzer. Aircrack –ng is used for wireless cracking and can crack WPA Wi-Fi Passwords. Hydra is a similar one where it is uses for on-line brute forcing of passwords. Maltego, is used for Intelligence Gathering. John is used for offline Password cracking. Metasploit Framework and sqlmap are used for exploitation. Owasp-zap is used for finding vulnerabilities in web application. Finally nmap is used for network scanning.

4. **What are a couple of the major penetration / exploit tools available on Kali?**
   Two major exploitation tools that were mentioned previously above are Metasploit Framework and sqlmap. Sqlmap specifically is used for exploiting SQL injection vulnerabilities. It is a free open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. Metasploit is a tool for developing and executing exploit code against a remote target mention. It allows you to safely simulate attacks on your network to uncover security issues, verify defenses, test security controls, track mitigation efforts, manage phishing exposure, and audit web applications.

5. **What is nmap and what is it used for?**
   Nmap is one of the many tools in Kali Linux, and its main function is a network scanner. It is a free open source utility and a command line tool and is used to discover hosts and services of a computer network, essentially making a map of the network. That is accomplished by sending specially crafted packets to the target host(s) and then analyzes the responses. The functionality of nmap is fairly easy and straightforward like many other sophisticated security tools, however there are many command line switches that the mind can comprehend. However, there is a front-end GUI called Zenmap which makes nmap fairly easy to use.