Ahnaf Sayed **18-36920-1**

Network Security Report

1.Exploration report on Kali Linux.

Answer: Kali Linux is an open-source Debian based Linux distribution that is used towards various kind of information security tasks, penetration testing, security research, computer forensics and reverse engineering. Kali Linux was developed by Mati Aharoni and Devon Kearns of Offensive Security by rewriting of BackTrack, a previous information testing Linux distribution based on Knoppix. Kali Linux imports most of packages from the Debian repositories. Kali is used by hackers for ethical hacking because it's a free operating system and it has tools over 600 for penetration testing and security analytics. By exploring Kali Linux I have found various kinds of tools that is used for Information Gathering, Vulnerability Analysis, Web Application Analysis, Database Assessment, Password Attacks, Wireless Attacks, Reverse Engineering, Exploration Tools, Sniffing and Spoofing, Post Exploitation, Forensics, Reporting Tools, Social Engineering Tools etc. Some penetration testing programs like Armitage -a graphical cyber-attack management tool, Nmap – a port scanner, Wireshark – a packet analyzer tool, Metasploit framework – a penetration testing framework, John the Ripper -a password cracker tool, sqlmap -an automatic SQL injection and database takeover tool, Maltego- an intelligence and forensics application, Owasp-ZAP -another web application testing tool, Aircrack-ng -a software suite that is used for penetration testing wireless LANs. Kali Linux also has Root Terminal Emulator, Powershell. Many professionals use Kali Linux like security administrators, network administrators, network architects, pen testers, chief information security officers, white hat hackers, black hat hackers.

2.What is penetration testing?

Answer: Penetration testing is a kind of cybersecurity technique that organizations use to identify, test, and highlight vulnerabilities in their security posture. It is mainly used for security testing that covers vulnerabilities, threats and risks that an attacker could exploit in software applications, networks or web applications. The main purpose of penetration testing is to identify and test all possible security outcome in vulnerabilities that are present in the software application. Penetration testing is also known as pen testing and it is a kind of ethical hacking. There are three kinds of penetration testing; first one is black box testing, second one is white box penetration testing and last one is grey box penetration testing. For penetration testing main important tools are Nmap, Nessus and Pass the Hash.

3.What are different operating system and tools we use for penetration testing?

Answer: For penetration test or ethical hacking there are many operating system that organizations used to check the vulnerability, threats and risks of their software applications, networks or web applications. There are operating systems like Kali Linux, BackBox, Parrot Security Operating System, DEFT Linux, Network Security Toolkit, BlackArch Linux, Cybrog Hawk Linux, GnackTrack, NodeZero, Fedora Security Lab, Dracos Linux, Samurai Web Testing Framework, Demon Linux etc. For penetration testing tools like Powershell, Zmap, Xray, SimplyEmail, Wireshark, Hashcat, John the Ripper, Hydra, Aircrack-ng is used.