**Kali Linux**

**What is kali Linux?**

Kali Linux is a free and open-source operating system specifically designed for penetration testing and security professionals. It is based on the Debian Linux distribution and includes a wide range of tools for various purposes, including:

* Network scanning and enumeration
* Vulnerability assessment
* Exploit development
* Forensics
* Web application security testing

**Kali Linux Tools**

1. **Nmap**

Nmap (Network Mapper) is a free and open-source utility for network discovery and security auditing. It allows you to scan networks to identify the hosts that are available, the services they are offering, the operating systems they are running, and the firewall rules that are in place. Nmap uses raw IP packets to determine the available hosts on a network, the services they are offering, and the operating systems they are running. It can also scan for open ports and can be used to discover vulnerabilities in a network.

* Ping the host with ping command to get the IP address

ping hostname

* Open the terminal and enter the following command there:

Nmap -sV ipaddress

1. **Burp Suite**

Burp Suite consists of multiple tools that work together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities. One of the most popular web application security testing software.

1. **Wireshark**

Wireshark is a free and open-source network protocol analyzer. It is used for network troubleshooting, analysis, software and communication protocol development, and education. These packets may have information like the source IP and the destination IP, the protocol used, the data, and some headers. The packets generally have an extension of “.pcap” which could be read using the Wireshark tool.

1. **Metasploit Framework**

The Metasploit Framework is a distribution specifically designed for penetration testing and security professionals. It is available from the Applications menu or from the command line by typing "msfconsole".

* Exploit testing: to identify and confirm the existence of vulnerabilities in a system or application.
* Payload development: to create custom payloads for use in exploit development.
* Exploit development: to develop new exploits for previously unknown vulnerabilities.

1. **Aircrack-ng**

For cracking wireless networks, as well as other tools for wireless network troubleshooting and analysis.

The tools included in Aircrack-ng are:

* Aircrack: a tool for cracking WEP and WPA-PSK keys.
* Aireplay-ng: a tool for generating traffic and attacking wireless networks.
* Airodump-ng: a tool for capturing and analyzing wireless traffic.
* Airbase-ng: a tool for creating fake wireless access points.

Also, Aircrack-ng can be used for a variety of purposes, including:

* Wireless network security assessments: to identify vulnerabilities in wireless networks and to test the effectiveness of security measures.
* Wireless network penetration testing: to exploit vulnerabilities in wireless networks and gain unauthorized access.
* Wireless network troubleshooting: to diagnose and fix problems with wireless networks.

1. **John the Ripper**

John the Ripper is designed to be fast and effective, and it can crack a wide range of password hash types. It can be used to test the strength of passwords and to recover lost or forgotten passwords.

John the Ripper has a number of different modes of operation, including:

* Single crack mode: to crack a single password.
* Wordlist mode: to try a list of words as passwords.
* Incremental mode: to try a set of predefined character sets and lengths, incrementing the length and complexity of the password at each step.

John the Ripper is a powerful tool that is widely used by security professionals and enthusiasts for a variety of purposes, including:

* Password testing: to test the strength of passwords and to identify weak passwords.
* Password recovery: to recover lost or forgotten passwords.
* Security assessments: to identify vulnerabilities in password security practices.

1. **Sqlmap**

SQL injection is a type of vulnerability that allows an attacker to execute arbitrary SQL commands on a database. sqlmap automates the process of detecting and exploiting SQL injection vulnerabilities, making it easier for security professionals to identify and exploit these vulnerabilities.

sqlmap has a number of features, including:

* Support for a wide range of databases, including MySQL, Oracle, and Microsoft SQL Server.
* The ability to enumerate the users, password hashes, and privileges of a database.
* The ability to execute arbitrary commands on the operating system via the database.
* The ability to dump the entire contents of a database.

sqlmap is a powerful tool that is widely used by security professionals and enthusiasts for a variety of purposes, including:

* Testing the security of web applications: to identify and exploit SQL injection vulnerabilities.
* Penetrtion testing: to gain unauthorized access to databases and sensitive information.
* Security assessments: to identify vulnerabilities in the security practices of organizations.

1. **Autopsy**

Autopsy is a graphical tool that runs on Windows, Linux, and MacOS. It includes a number of modules for analyzing different types of evidence, including:

* File system analysis: to examine the files and directories on a hard drive.
* Network analysis: to examine network traffic and artifacts.
* Email analysis: to examine email messages and attachments.
* Web analysis: to examine the contents of web browsers and cache.

Autopsy is an important tool for law enforcement agencies and digital forensics professionals, and it is widely used in criminal investigations and other legal proceedings.

1. **Social Engineering Toolkit**

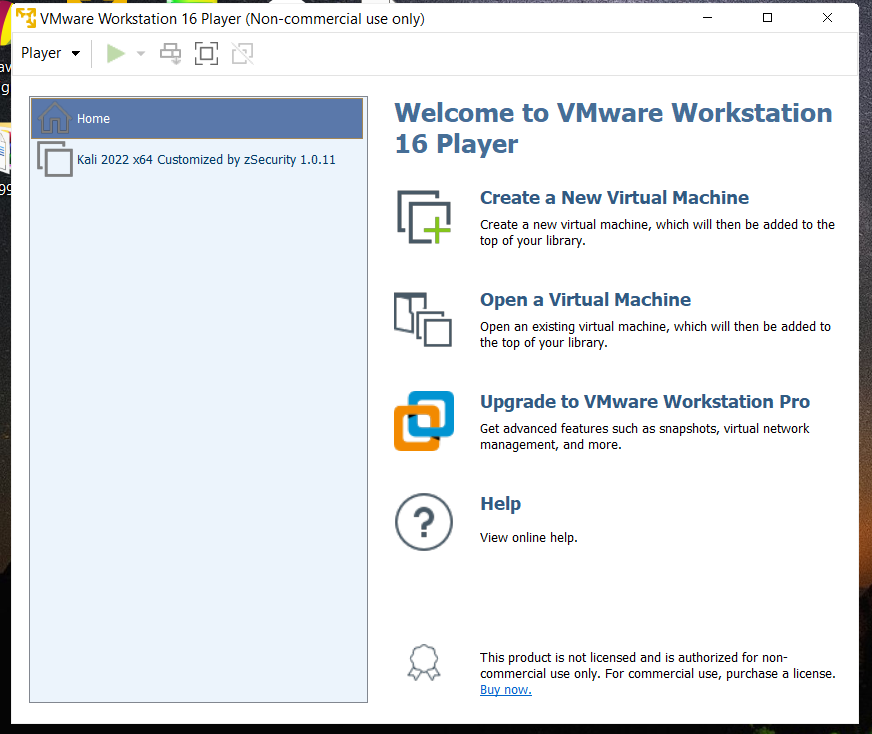
Social engineering attacks are a type of attack that rely on human interaction to trick people into disclosing sensitive information or performing actions that they wouldn't normally do. SET is designed to help security professionals test the defenses of an organization against social engineering attacks.

SET has a number of features, including:

* A number of pre-built attack scenarios that can be easily customized and launched.
* The ability to create custom attack scenarios.
* The ability to generate malicious payloads, such as malicious PDF files or executables.
* The ability to simulate phishing attacks.

SET is a powerful tool that is widely used by security professionals and enthusiasts for a variety of purposes, including:

* Testing the security of organizations: to identify and exploit vulnerabilities in their defenses against social engineering attacks.
* Security awareness training: to educate employees about the risks of social engineering attacks and how to protect themselves.



This is my VMware workstation I download then I install Kali Linux to my system but somehow it’s not working properly. I got some errors about starting to run kali files or something I cant figure out.