المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

AL KHABEER
معهد الخبير التربوي للتدريب

أمن المعلومات

Kali liunx

Course Outlines

✓ As **the course title states**, the focus of this course is to explore the skills of using kali Linux distribution for cybersecurity specialist.

In this course, you will do the following:

- Understand the need for cybersecurity.
- Understand virtual environments and virtual machines.
- Explore and understand the fundamentals of Kali Linux.
- How to setup your pen testing Lab using virtual systems.
- How to setup your portable pen testing Lab using Raspberry Pi.
- Explore different tools for system security testing on Kali.
- Understand of the basics of ethical hacking and penetration testing.

Attention !

THE CONTENTS OF THIS PRESENTATION FOR EDUCATION PURPOSE ONLY

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

AL KHABEER
معهد الخبير التربوي للتدريب

More Learn, More Power

The Real Experience = Hands On and Troubleshooting

No System is 100 % secure

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

AL KHABEER
معهد الخبير التربوي للتدريب

Introduction to Kali Linux

Kali Linux

- ✓ **Kali Linux** is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing.
- ✓ **Kali Linux** contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Digital Forensics and Reverse Engineering.
- ✓ **Kali Linux** is developed, funded and maintained by Offensive Security, a leading information security training company.

✓ Kali Linux is one of the best open-source security packages of an ethical hacker, containing a set of tools divided by categories.

✓ Kali Linux can be installed in a machine as an Operating System.

✓ Kali Linux was released on the 13th March 2013 as a complete, top-to-bottom rebuild of BackTrack Linux, adhering completely to Debian development standards.

✓ Kali Linux can run on a wide variety of hardware, is compatible with numerous wireless and USB devices, and also has support for ARM devices

✓ Kali Linux include several tools, for example, and not limited to:

- Metasploit for network penetration testing,
- Nmap for port and vulnerability scanning,
- Wireshark for monitoring network traffic,
- Aircrack-Ng for testing the security of wireless networks.

Customized Linux Distribution For Cybersecurity, Why?

- A **custom security distribution of Linux** can be created for security purpose with just the tools needed for testing.

  ✓Packet Capture (Wireshark)

  ✓Malware Analysis Tools

  ✓Intrusion Detection Systems (IDSs)

  ✓Firewalls

  ✓Penetration testing tools

Linux Operating System

- ## Understanding Linux
  - **Linux** is open source, fast, reliable and small and requires very little hardware resources to run.
  - **Linux** is part of several platforms; from wristwatches to supercomputers.
  - **Linux** distributions include the Linux kernel, plus a number of customized tools and software packages.
  - Debian, Red Hat, Ubuntu and Slackware are just a few examples of Linux distributions.
  - **Raspbian** is a Linux distribution based on Debian and created specifically for the Raspberry Pi.
- ## Accessing the Linux Shell
  - The Linux operating system can be divided into kernel and shell.
  - The shell is a command interpreter.
  - The shell is text based and also called CLI (command line interface

Linux Operating System (Cont.)

- **Accessing the CLI**
  - The CLI can be accessed directly through a shell in non-graphical systems.
  - A terminal emulator application can be used to access the CLI in graphical environments.
  - Popular terminal emulators on Linux are **Terminator**, **eterm**, **xterm**, **console**, and **gnome-terminal**.
- **Basic Linux Commands**
  - Linux commands are programs created to perform a specific task.
  - To invoke a command via shell, simply type its name.
  - **grep**, **ifconfig**, **iwconfig**, **passwd** and **pwd** are a few basic Linux commands.
  - Commands can be piped together, using the output of one as the input of the other.

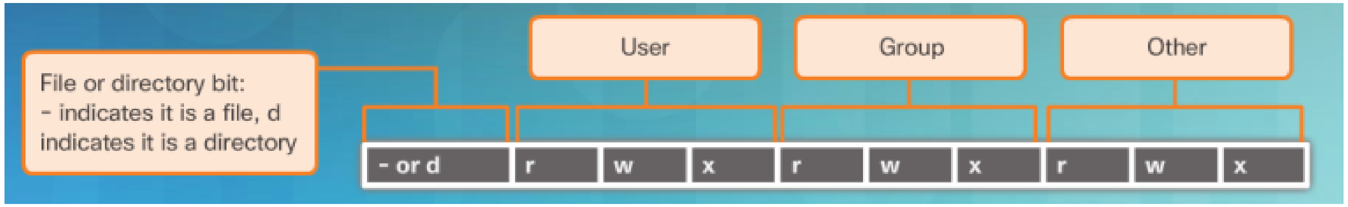
Linux Operating System (Cont.)

Process Managing Commands

- In Linux, a process is any task or command being executed by the system.
- PIDs are unique numbers assigned to processes for identification.
- **ps** and **kill** are commands used to manage processes.

File Permissions

- In Linux, most everything is treated as a file.
- File Permissions provide a mechanism to define permissions to files.
- Possible permissions rights are **Read**, **Write**, and **Execute** and can be defined for the user who owns the file, the group, and other system users.
- The root user can override file permissions.



File or directory bit:
– indicates it is a file, d indicates it is a directory

Working with Text Files

- There are many text editors available in Linux.
- Some text editors are for the CLI only, like vi, vim, and nano.
- Other text editors, like gedit, are GUI-based.
- CLI text editors allow system management remotely, such as via SSH.

Importance of Text Files in Linux

- In Linux, everything is treated as a file, this includes the memory, the disks, the monitor, the files, and the directories.
- The operating system as well as most programs are configured by editing the configuration files which are text files.
- Editing system or application configuration files requires super user (root) privileges. This can be accomplished with the sudo command.

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

الخبير
AL KHABEER
معهد الخبير التربوي للتدريب

Basic of hacking concept for Penetration Testing

What is Cybersecurity?

✓ Protection of networked system and data from unauthorized use or harm.

Levels of Cybersecurity

❑ **Personal level**

✓ You need to safeguard your identity, your data, and your computing devices.

❑ **Corporate level**

✓ It is everyone’s responsibility to protect the organization’s reputation, data, and customers.

❑ **State level**

✓ National security, and the safety and well-being of the citizens are at stake.

Proactive and Reactive Security

There are two basic methods of dealing with security breaches:

- ❑ **Reactive Method** is **passive**; when a breach occurs, you respond to it, doing damage control at the same time **you track down how the intruder or attacker got in and cut off** that means of access so **it will not happen again**.

- ❑ **Proactive Method** is **active**; instead of waiting for the hackers to show you where you are vulnerable, **you put on your own hacker hat in relation to your own network** and **set out to find the vulnerabilities yourself**, before **anyone else discovers and exploits them**.

✓ **The best security strategy** employs both **reactive** and **proactive** mechanisms. **IDS**, for example, are **reactive in that they detect suspicious network activity so that you can respond to it appropriately.**

Attacks and Cybercrimes

✓ Cybercrimes is a term used to describe the criminal activity in which computers or networks are a tool, a target or a place of criminal activity.

✓ Cybercrime is defined as any illegal act involving a computer, its system, or its applications.

✓ Cybercrime Types:

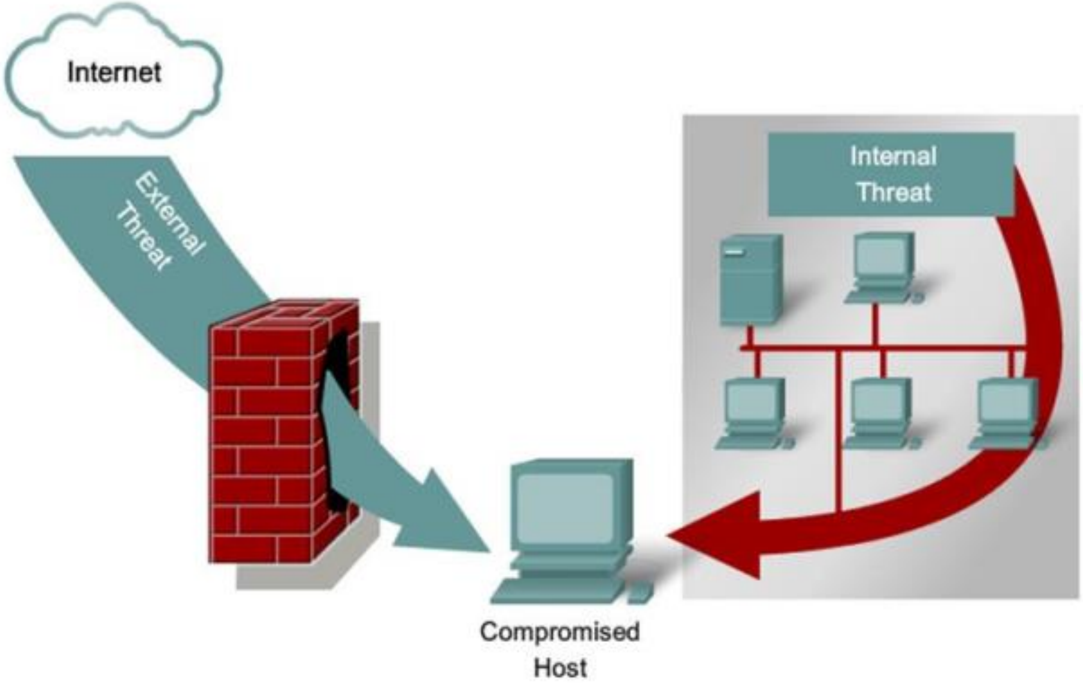
- ✓ Crime against a computer system
- ✓ Computer as a tool to commit the crime

Modes of Attacks

Cybercrimes can be classified based on the line of attack

1. Internal Attacks

2. External Attacks



Software Requirements for Testing Lab

- ✓ **Virtualization Software:** VMware Workstation/Oracle VirtualBox
- ✓ Kali Linux Virtual Machine (VM)
- ✓ Metasploitable VM (**optional**)
- ✓ Windows XP VM