

HANDS-ON ACTIVITY 1: CONDUCTING A STRUCTURED PENETRATION TEST IN YOUR EXISTING LAB

Task 1: Logging Into the Virtual Machines

1. Log in to your **personal laptop hosting your virtual machine**. Familiarize yourself with the networking setup, available virtual machines, and installed software tools.
2. Determine the IP configuration of your **personal laptop** by following these steps:
 - Open the Command Prompt.
 - Type the following command and press Enter: `ipconfig`
 - Review the output and locate the following information:

a. Local IPv4 Address of your personal laptop:

(Look for “IPv4 Address” under your active network adapter.)

Write it here:

b. Default Gateway IPv4 Address:

(Look for “Default Gateway” under the same network adapter section.)

Write it here:

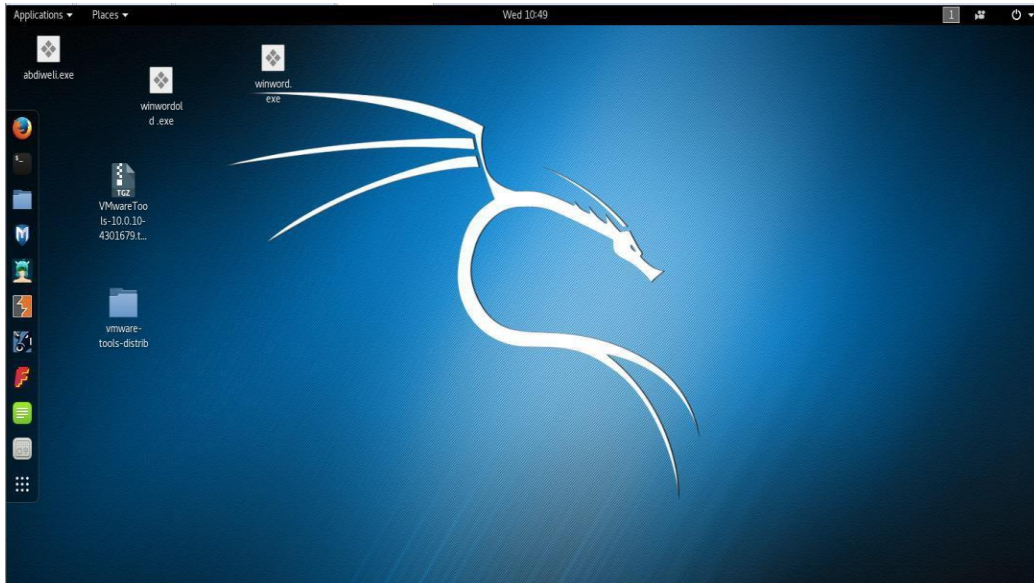
This will allow you to identify both your laptop’s local IP address and its default gateway.

Task 2: Introduction to Kali Linux

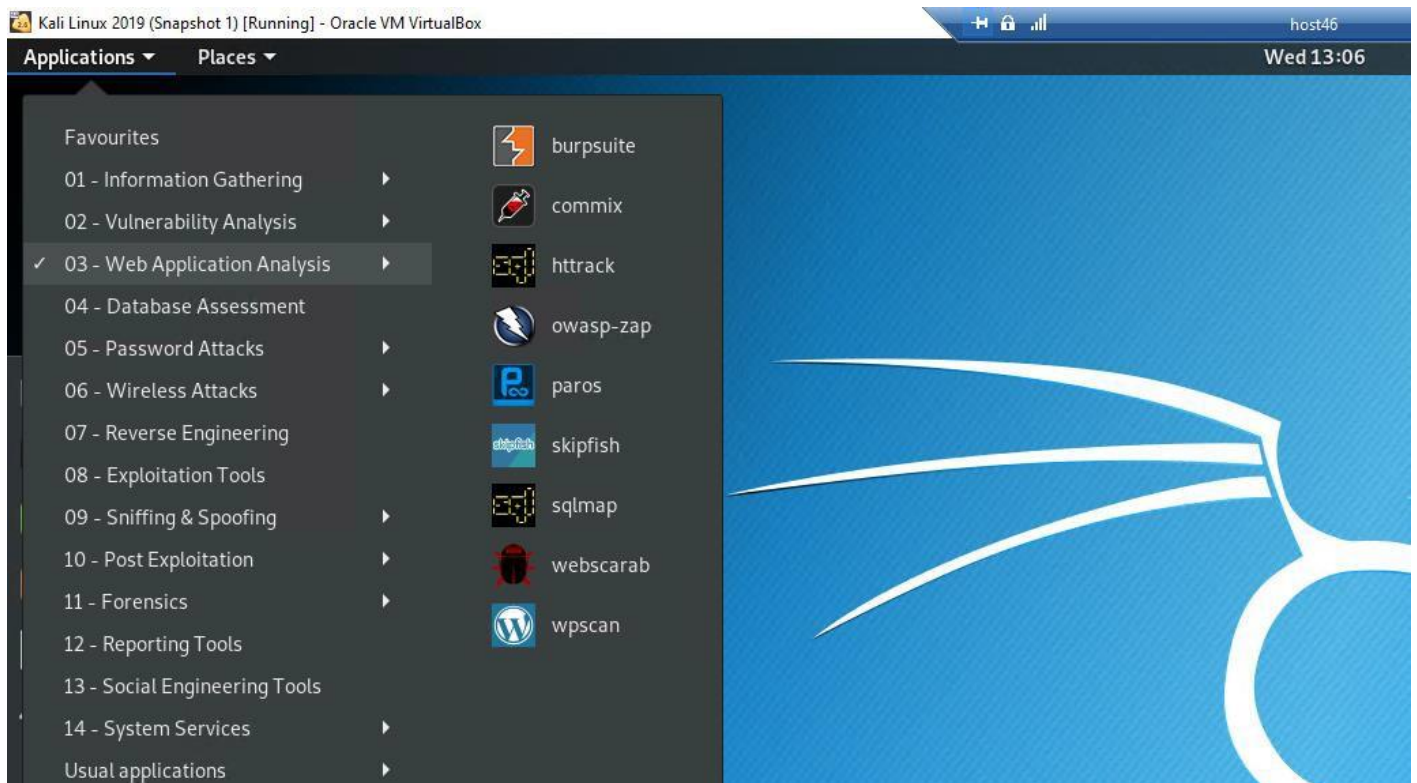
Kali Linux is a Debian based Linux distribution designed for advanced penetration testing and security auditing. It includes hundreds of specialized tools used for various information security tasks such as penetration testing, security research, digital forensics, and reverse engineering.

Kali Linux is developed, funded, and maintained by Offensive Security, a well-known information security training organization. It was officially released on March 13, 2013 as a complete rebuild of BackTrack Linux, fully aligned with Debian development standards.

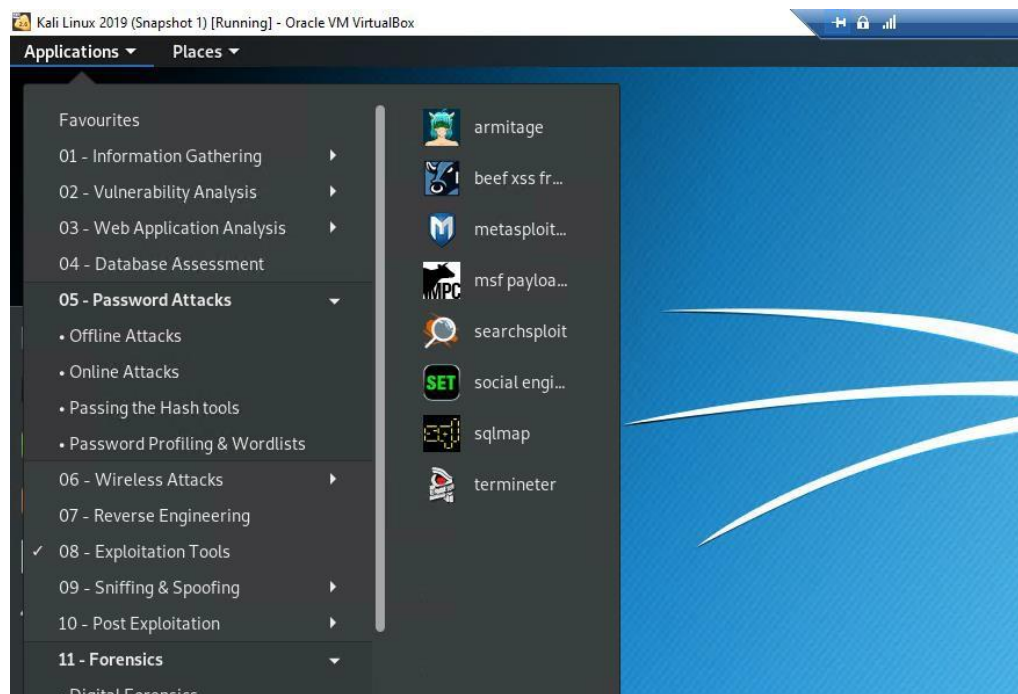
1. Kali Linux Login Credential: **Username:** `root` **Password:** `osboxes.org`
2. The Graphical User Interface (GUI) should look like this after a successful login.



3. **How to view available tools:** Navigate to the **Applications** drop-down menu in the top left corner of the desktop.



4. How to open the Kali Linux Terminal (the command prompt): **Navigate to "Application | Favorites | Terminal" using the drop-down menu.**



5. A penetration tester must collect information during the penetration test. Assessments are typically time and resource constrained. As a result, it is critical to identify and concentrate on the most vulnerable points. Even the best tools are rendered ineffective if they are not used correctly and at the appropriate time. That is why experienced testers devote a significant amount of time to data collection.

Task 3: Understanding TCP Ports

Transmission Control Protocol, commonly known as TCP, uses two 16 bit fields within each packet to store the source and destination port numbers. These port numbers are logical identifiers rather than physical components. They define specific communication endpoints and indicate which service is active on a device.

A TCP port identifies a particular application or service running on a system. For example, web traffic using the Hypertext Transfer Protocol typically communicates through port 80 by default. When a client sends a request to a server, the destination port specifies the intended service, while the source port helps manage the return communication.

Understanding ports is essential for network security. Each active service on a server listens on a specific port. The more services that are running, the more open ports exist, and each open port can present a potential entry point for an attacker. Limiting unnecessary services reduces the number of open ports and strengthens overall security.

Securing a system with many open ports is similar to protecting a house with numerous open doorways. The fewer open entry points available, the easier it is to maintain a secure environment.

1. Start your **Windows virtual machine**.
2. Open a **Command Prompt** window.
3. To check for open ports on the system, use the `netstat` command.
4. At the Command Prompt, type the following and press Enter: `netstat`
5. If no active ports are displayed, type the following command and press Enter: `netstat -a`. This command displays all active connections and listening ports on your system, including both TCP and UDP ports.
6. After reviewing the results, close the Command Prompt window and any other open windows.

```
Command Prompt - netstat
Microsoft Windows [Version 10.0.19045.2486]
(c) Microsoft Corporation. All rights reserved.

C:\Users\DIPODU.ITSECURITY>netstat

Active Connections

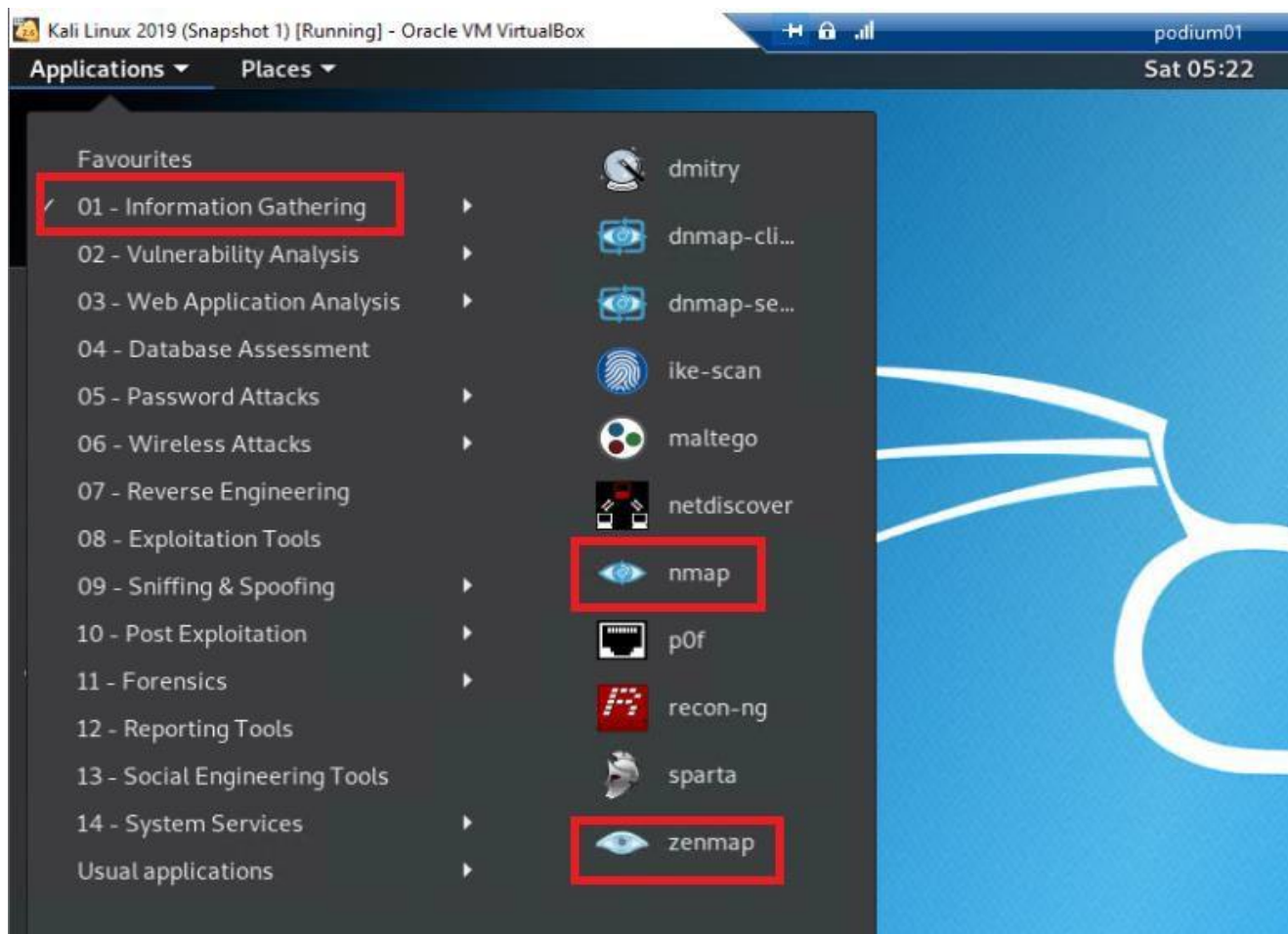
Proto Local Address           Foreign Address         State
TCP    10.72.2.55:7680         UFED-Lic-Srv:56213     TIME_WAIT
TCP    10.72.2.55:7680         UFED-Lic-Srv:56218     TIME_WAIT
TCP    10.72.2.55:7680         UFED-Lic-Srv:56219     TIME_WAIT
TCP    10.72.2.55:7680         UFED-Lic-Srv:56222     TIME_WAIT
TCP    10.72.2.55:7680         UFED-Lic-Srv:56223     TIME_WAIT
TCP    10.72.2.55:7680         Tech01:55992           TIME_WAIT
TCP    10.72.2.55:7680         Tech01:55999           TIME_WAIT
TCP    10.72.2.55:7680         Tech01:56003           TIME_WAIT
TCP    10.72.2.55:7680         T720B-W019023:49850    TIME_WAIT
TCP    10.72.2.55:56618        itsecdc01:microsoft-ds ESTABLISHED
TCP    10.72.2.55:56800        lhr48s27-in-f14:https  TIME_WAIT
TCP    10.72.2.55:56951        lhr48s28-in-f3:https   ESTABLISHED
```

Task 4: Information Gathering

A penetration tester relies heavily on the information gathered during the penetration test. As a result, identifying the points most likely to be vulnerable is critical. Nmap and Zenmap are useful tools for gathering information during the ethical hacking phase of Kali Linux. Nmap and Zenmap are essentially the same tool, but Nmap uses the command line and Zenmap has a graphical user interface.

Nmap uses raw IP packets in novel ways to determine which hosts are running on the network, which ports are open or closed, what services (version and name) those hosts provide, what operating systems (and OS versions) they are running, what type of packet filters or firewalls are in use, and other features.

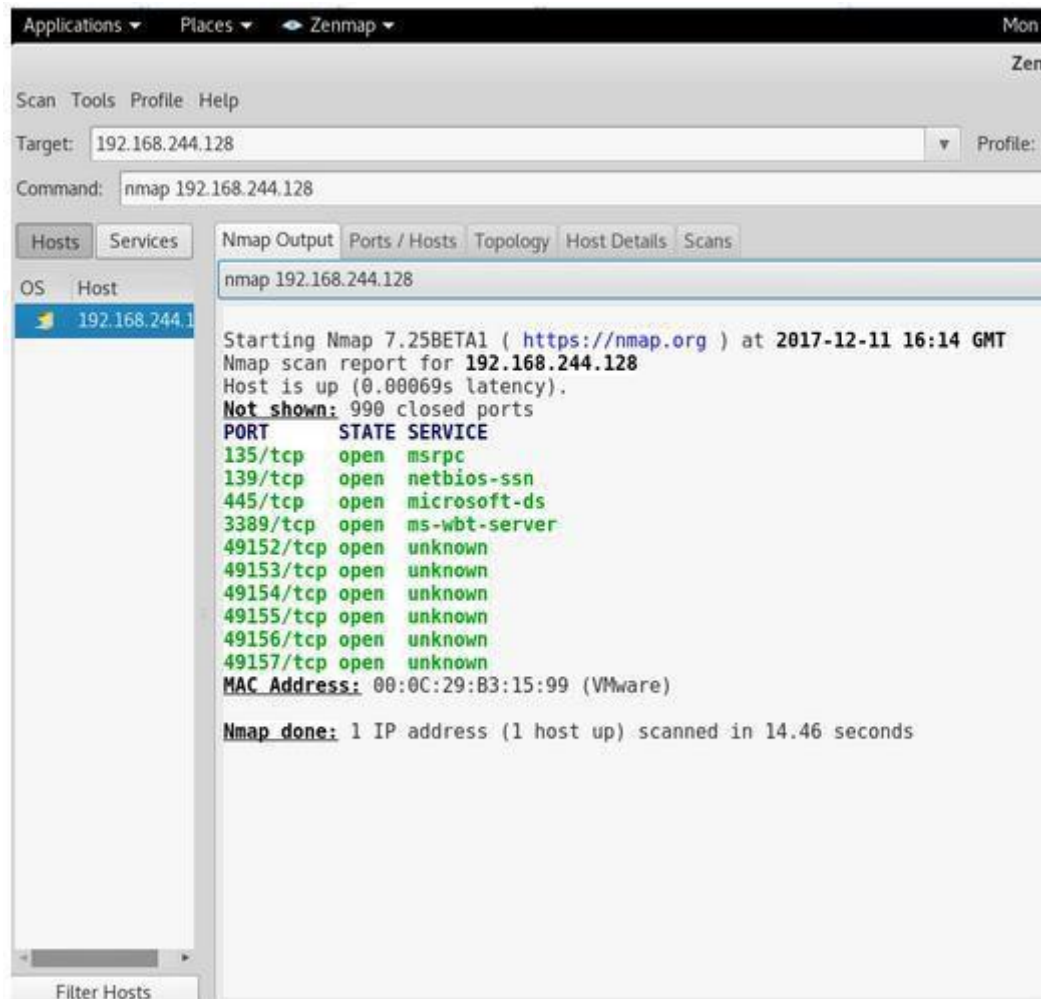
How to open the information gathering tool, open Kali Linux: in the drop-down menu go to **Application | Information Gathering | Zenmap or Application | Favorites | Terminal | type zenmap or Nmap** (case-sensitive)



Task 5 – Gathering information from single host using Zenmap

1. Open Terminal **Application** | **Favourites** | **Terminal** | type **zenmap**

- Step 1: Enter the target **IP address** (the target is the host about which you are gathering information; use the work you did last week to determine the host IP address you wish to target).
- Step 2: Select a scanning profile | **Regular scan**
- Step 3: press the **scan button**.
- The result of the scan will be displayed once the host scan is complete. The **Nmap Output** tab displays the raw output of the host scan, as it will also appear on the open terminal (command prompt).



2. Find and record the following information about a scanned host computer:

- Open TCP ports
- Windows host details
- Host status
- Host IP address
- Host Mac address
- Operating system
- Ports used
- OS classes
- Services
- Topology

Interactive answer pages added below

Use the fillable worksheets on the following pages to record IP addresses, netstat findings, Zenmap or Nmap scan results, Windows 11 scan results, reflections, evidence, and confirmation.

Interactive Worksheet - Activity 2

Complete these fields as you work through the lab. Save a copy of the PDF when finished.

Student Details and Lab Setup

Student name:

Date:

Course / group:

Host-only network / subnet:

Task 1: Logging Into the Virtual Machines

Record the IP details from your personal laptop after running ipconfig.

Laptop local IPv4 address:

Default gateway IPv4 address:

I recorded my laptop IP address and default gateway.

I confirmed the virtual machines are available before continuing.

Task 2: Kali Linux Introduction

I logged into Kali Linux successfully.

I found the Applications menu and reviewed the available tool categories.

I opened the Kali Linux terminal.

Task 3: Understanding TCP Ports

Use this section to summarize what you saw after running netstat or netstat -a on Windows.

In your own words, what is a TCP port?

Why can many open ports increase security risk?

Windows netstat sample findings

Protocol	Local address	Foreign address	State	Notes

Interactive Worksheet - Nmap / Zenmap Scan Results

Use this page to record the results from Task 4 and Task 5. Record only what you actually find in your scan.

Task 4: Information Gathering Setup

I opened Zenmap or Nmap from Kali Linux.

Scan command or profile used:

Network or target range used:

Task 5: Single Host Scan Details

Target name	Target IP address	Host status	Operating system
Metasploitable			
Windows 11			

Metasploitable scan results

Port	State	Service	Version / details	Observation

Windows 11 scan results

Port	State	Service	Version / details	Observation

Interactive Worksheet - Analysis and Confirmation

Compare the Two Systems

Which system exposed more services?

Which system appeared more secure or hardened?

Why might Windows 11 show fewer open ports?

What did you learn from comparing the two systems?

Risk and Recommendation Notes

Choose 2 or 3 findings and suggest a safe recommendation for each.

Finding	Why it matters	Recommended fix

Evidence and Student Confirmation

I saved screenshots or notes as evidence for academic use only.

I did not test real websites, public IP addresses, school systems, or personal devices.

I avoided destructive activity such as brute force, data modification, backdoors, or denial of service.

Student signature / name:

Date:

Reminder: This activity is for a controlled lab only. Testing outside the approved environment is not allowed without clear permission.