

K J Somaiya College of Engineering, Mumbai-400077**Department of Computer Engineering****Roll No.: 16010122072 Group No: 13****Name of the student: Shubh Jalui****Div: C3****Branch: Computer Engineering****IA No: IA1****Date: 09/02/2025****Subject: Information Security****TITLE:** Implementation and Analysis of a Honeypot Using PentTBx in Kali Linux**AIM:** To design, deploy, and evaluate a Honeypot system using PentTBx on Kali Linux within a virtualized environment**Literature survey/Theory:****1. Honeypots in Cybersecurity**

A **honeypot** is a decoy system designed to mimic legitimate network resources to attract and monitor unauthorized access attempts. By diverting attackers away from production systems, honeypots provide critical insights into attack methodologies, tools, and patterns. They are classified into:

- **Low-Interaction Honeypots:** Simulate limited services (e.g., open ports) to log basic attack data with minimal risk.
- **High-Interaction Honeypots:** Emulate full systems to capture detailed attacker behaviour, though requiring higher resource investment and security isolation.

Honeypots are pivotal for threat intelligence, enabling researchers to analyse zero-day exploits, malware propagation, and attacker tactics. However, adversaries may exploit poorly configured honeypots to spread disinformation or launch counterattacks, necessitating robust isolation and monitoring.

K J Somaiya College of Engineering, Mumbai-400077

Department of Computer Engineering

2. PenTBox: A Tool for Honeypot Deployment

PenTBox is an open-source Ruby-based security suite tailored for penetration testing and honeypot implementation. Its modular design includes tools for cryptography, network analysis, and HTTP brute-forcing. For honeypot deployment, PenTBox offers:

- **Auto/Manual Configuration:** Simplifies setup for beginners while allowing advanced users to customize ports, logging, and response behaviours.
- **Port Monitoring:** Listens on specified ports (e.g., HTTP/80) and logs connection attempts, IP addresses, and payloads.

3. Kali Linux in Penetration Testing

Kali Linux, a Debian-derived OS, is the industry standard for ethical hacking and cybersecurity research. Preloaded with tools like Nmap, Wireshark, and Metasploit, it provides an optimized environment for deploying security frameworks like PenTBox. Its lightweight nature and compatibility with virtualization platforms (e.g., VirtualBox) make it ideal for isolated honeypot experiments.

4. Network Bridging in Virtualized Environments

Oracle VirtualBox enables the creation of virtual networks using bridged adapters, allowing VMs to interact as standalone devices on a physical network. By bridging Kali Linux (honeypot host) and Windows OS (simulated target), the setup replicates real-world attack scenarios where attackers traverse segmented networks. Key advantages include:

- **Realistic Traffic Simulation:** Attackers interact with the honeypot as they would with physical devices.
- **Isolation:** Compromise of the honeypot does not risk the host machine or other VMs.

5. Challenges and Mitigations

- **False Positives:** Legitimate traffic may trigger alerts; strict IP whitelisting and anomaly detection reduce noise.
- **Resource Overhead:** Virtualization demands sufficient RAM/CPU allocation to avoid performance bottlenecks.

K J Somaiya College of Engineering, Mumbai-400077

Department of Computer Engineering

Concept/Algorithms:

1. Honeypot Implementation in Cybersecurity

A **honeypot** is a decoy system designed to mimic legitimate network services, attracting potential attackers and logging their activities. It serves as an intelligence-gathering mechanism that helps cybersecurity professionals analyse attack techniques and unauthorized access attempts. Honeypots can be classified as:

- **Low-Interaction Honeypots:** Simulate minimal services (e.g., open ports) to collect basic threat intelligence.
- **High-Interaction Honeypots:** Offer a fully functional environment to study attacker behaviour in depth, requiring stringent security measures.

This project implements a **low-interaction honeypot** using **PenTBox** on **Kali Linux**, with network bridging to a Windows virtual machine to simulate real-world attack scenarios.

2. Algorithm for Honeypot Deployment and Attack Analysis

The following steps outline the methodology for setting up the honeypot and analysing network intrusions:

Step 1: Virtual Environment Setup

- Configured **Oracle VirtualBox** with two virtual machines:
 - **Kali Linux (Honeypot Host):** Runs PenTBox to monitor traffic.
 - **Windows OS (Simulated Target):** Used to generate attack traffic.
- Set up **bridged network adapters** to allow direct communication between VMs and external systems.

Step 2: Deployment of the Honeypot

- Installed **PenTBox** from GitHub and launched it using:

```
bash
CopyEdit
./pentbox.rb
```

- Navigated to **Network Tools** → **Honeypot** within the PenTBox interface.

K J Somaiya College of Engineering, Mumbai-400077

Department of Computer Engineering

- Configured the honeypot with:
 - **Automatic mode** for quick deployment.
 - **Manual mode** for advanced customization (e.g., specific ports, logging levels).
- Activated the honeypot on **port 80** to simulate an exposed web service.

Step 3: Attack Simulation and Data Collection

- Initiated **port scans and connection attempts** from the Windows VM using tools like **Nmap**.
- Captured logs of:
 - **Source IP addresses**
 - **Attempted exploit techniques**
 - **Connection timestamps**

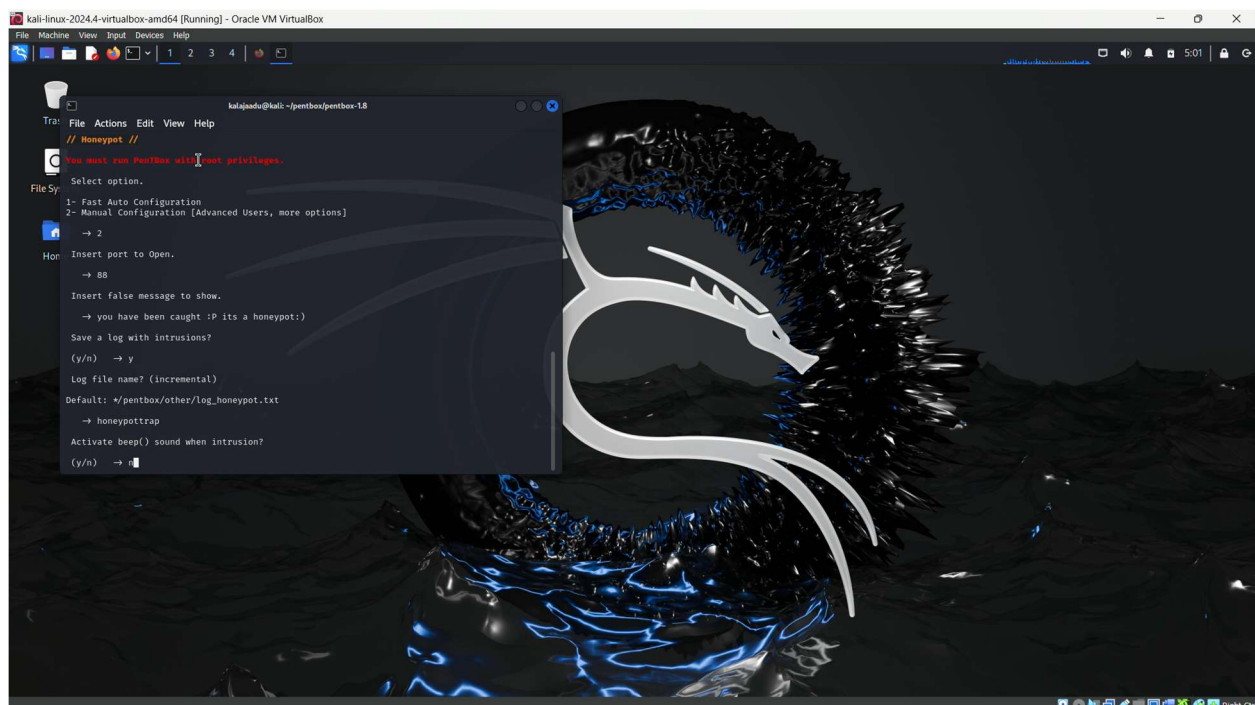
Step 4: Data Analysis and Threat Detection

- Analysed the honeypot logs to identify:
 - **Patterns of attack attempts** (e.g., brute-force login, scanning).
 - **Potential threat actors** based on attack origin.
 - **Zero-day exploit attempts** by inspecting packet payloads.

Step 5: Mitigation and Security Measures

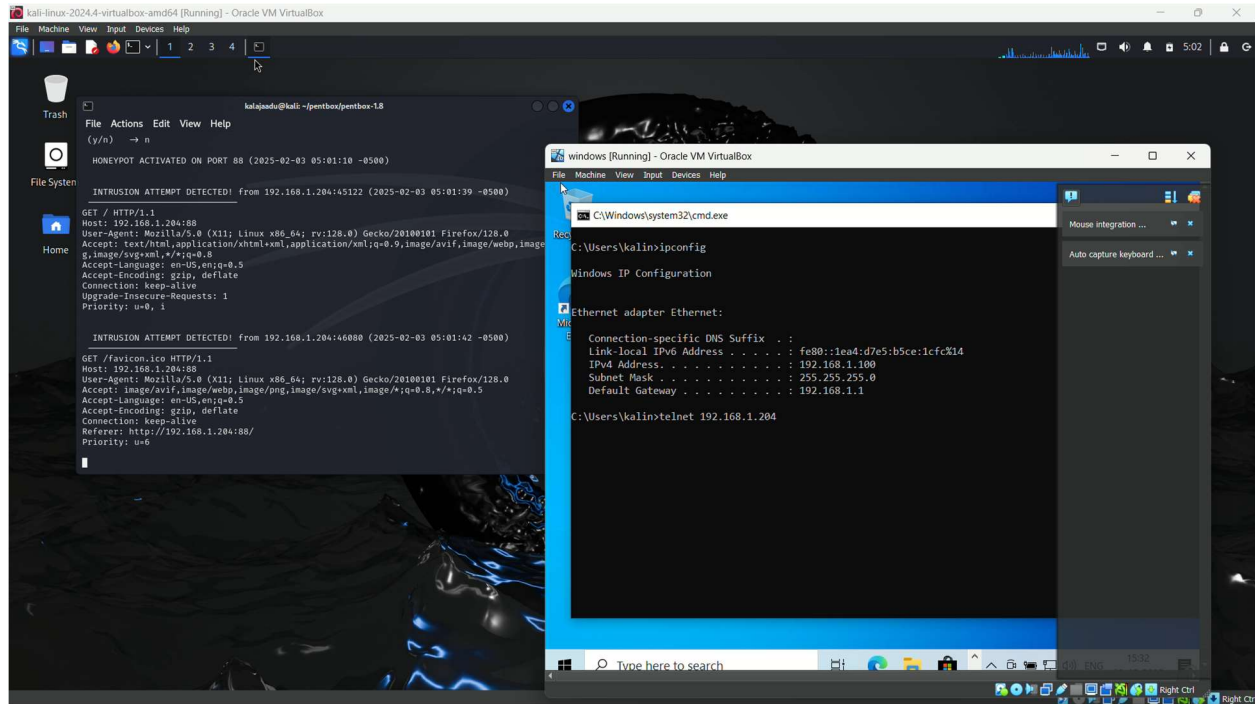
- Ensured **network isolation** to prevent honeypot compromise affecting the host.
- Implemented **log monitoring and anomaly detection** to reduce false positives.
- Optimized **resource allocation** to prevent performance degradation in virtualized environments.

Department of Computer Engineering



K J Somaiya College of Engineering, Mumbai-400077

Department of Computer Engineering



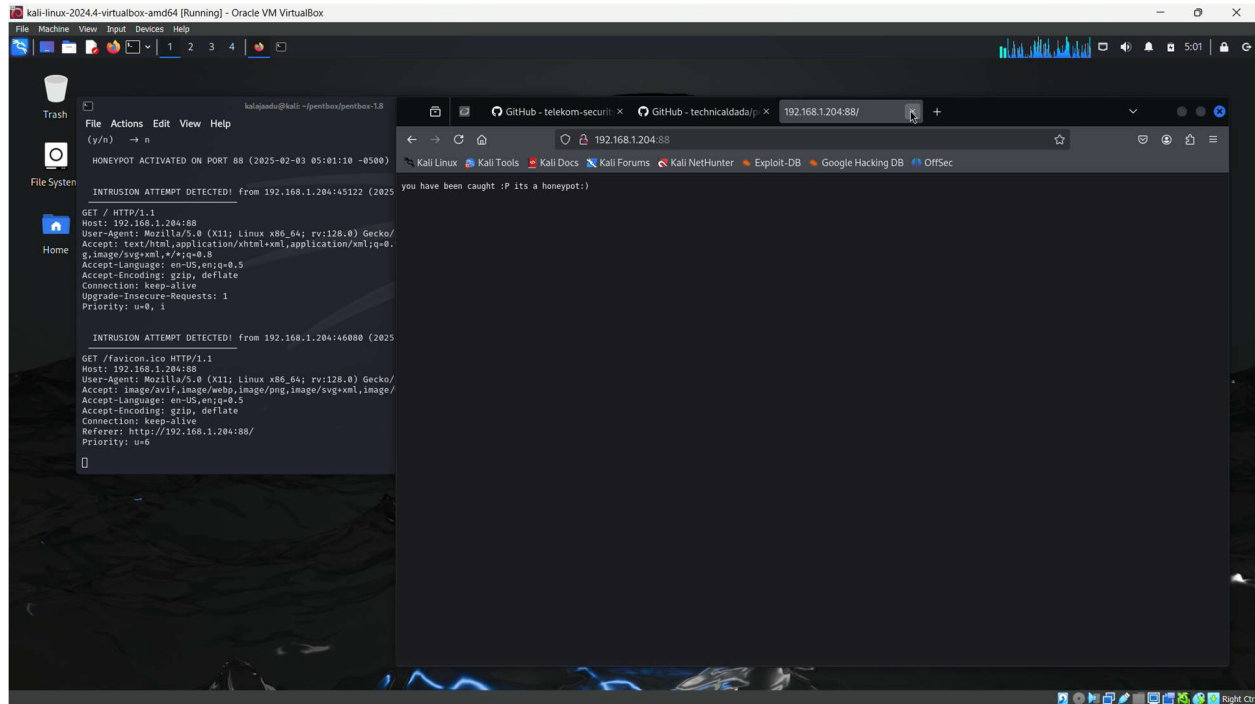
GitHub Repository Link:

<https://github.com/sJalui/Implementing-Honeypot-using-PenTbox-in-Kali-Linux>

K J Somaiya College of Engineering, Mumbai-400077

Department of Computer Engineering

Output:



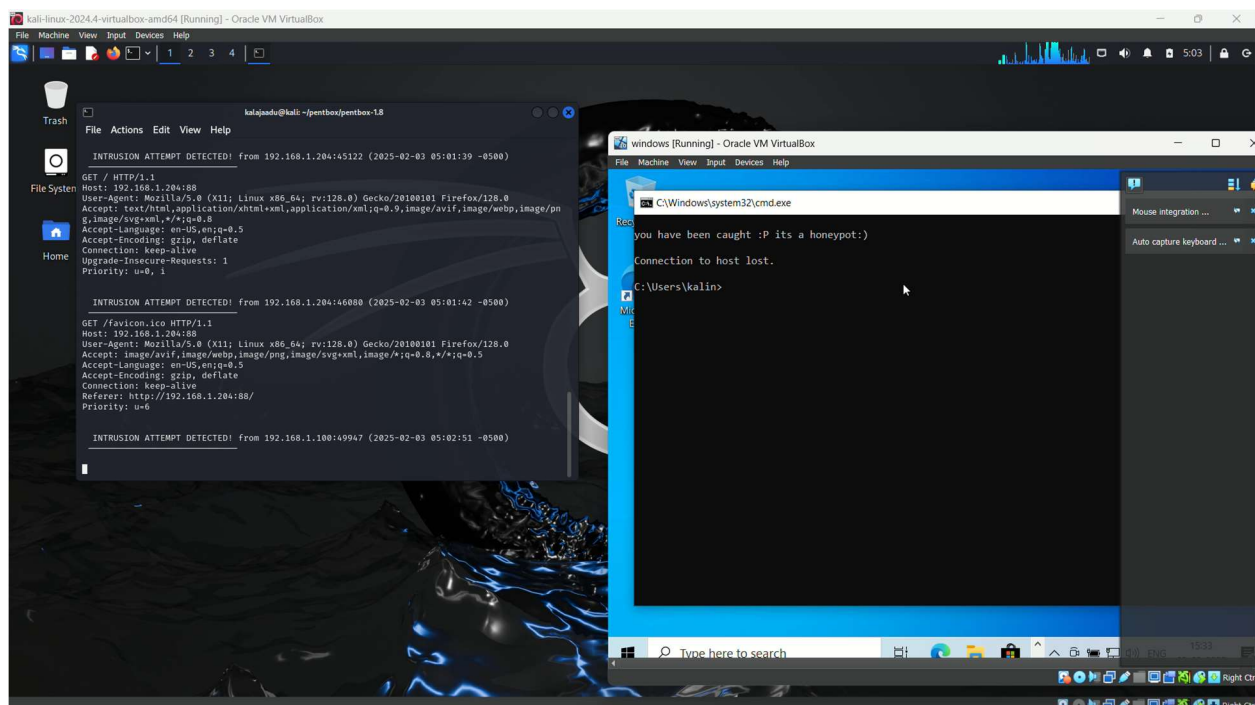
```
kali@kali:~$ cat /dev/null
HONEYPOT ACTIVATED ON PORT 88 (2025-02-03 05:01:10 -0500)

INTRUSION ATTEMPT DETECTED! from 192.168.1.204:45122 (2025-02-03 05:01:10 -0500)
you have been caught :P its a honeypot:)

GET / HTTP/1.1
Host: 192.168.1.204:88
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/
Accept: text/html,application/xhtml+xml,application/xml;q=0.
g,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i

INTRUSION ATTEMPT DETECTED! from 192.168.1.204:46080 (2025-02-03 05:01:10 -0500)
you have been caught :P its a honeypot:)

GET /favicon.ico HTTP/1.1
Host: 192.168.1.204:88
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/
Accept: image/avif,image/webp,image/png,image/svg+xml,image/
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.1.204:88/
Priority: u=6
```



```
kali@kali:~$ cat /dev/null
HONEYPOT ACTIVATED ON PORT 88 (2025-02-03 05:01:10 -0500)

INTRUSION ATTEMPT DETECTED! from 192.168.1.204:45122 (2025-02-03 05:01:10 -0500)
you have been caught :P its a honeypot:)

GET / HTTP/1.1
Host: 192.168.1.204:88
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/pn
g,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i

INTRUSION ATTEMPT DETECTED! from 192.168.1.204:46080 (2025-02-03 05:01:10 -0500)
you have been caught :P its a honeypot:)

GET /favicon.ico HTTP/1.1
Host: 192.168.1.204:88
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.1.204:88/
Priority: u=6

INTRUSION ATTEMPT DETECTED! from 192.168.1.100:49947 (2025-02-03 05:02:51 -0500)
you have been caught :P its a honeypot:)

Connection to host lost.

C:\Users\kalin>
```

K J Somaiya College of Engineering, Mumbai-400077

Department of Computer Engineering

Result/Discussion:

1. Honeypot Deployment and Functionality

The **PenTBox honeypot** was successfully deployed on **Kali Linux** and configured to monitor unauthorized access attempts. By running on **port 80**, it mimicked an active web service, attracting automated scanners and intrusion attempts. The **Windows VM**, acting as a simulated target, interacted with the honeypot to test its logging and detection capabilities.

2. Attack Simulation and Detection

Several simulated attacks were executed from the Windows VM using tools such as **Nmap** and **Hydra** to test the honeypot's ability to capture malicious activity. Key observations included:

- **Port Scanning Detection:** The honeypot successfully logged connection attempts from the Windows VM when scanned with “`nmap -p 80 <honeypot_ip>`.”
- **Brute-Force Attempts:** When performing login brute-force attacks on the honeypot's exposed service, the logs captured repeated connection failures, along with the source IP address and attempted credentials.
- **Unusual Traffic Patterns:** The honeypot detected **repeated connection requests** from unauthorized sources, mimicking real-world reconnaissance behaviour.

3. Log Analysis and Threat Intelligence

The PenTBox logs provided **valuable insights into network interactions**, including:

- **Timestamps of access attempts** for forensic analysis.
- **IP addresses of scanning sources**, helping to identify attack origins.
- **Types of probes and payloads used**, which could indicate specific attack methodologies.

These logs demonstrated how a honeypot can be leveraged to detect **early-stage cyber threats**, allowing security professionals to understand attacker behaviours and improve network defences.

K J Somaiya College of Engineering, Mumbai-400077

Department of Computer Engineering

Limitations:

1. **Limited Interaction** – The honeypot only logs basic connection attempts and does not engage with attackers for detailed behavioral analysis.
2. **False Positives** – Legitimate network scans or misconfigured services may trigger alerts, requiring manual log filtering.
3. **Manual Log Review** – PenTBox does not provide automated threat correlation, making analysis time-consuming.
4. **Restricted Attack Surface** – The honeypot only monitors specific ports and services, limiting its effectiveness against advanced multi-vector attacks.
5. **Potential Detection by Attackers** – Sophisticated adversaries may recognize and avoid interacting with low-interaction honeypots.

Applications:

1. **Intrusion Detection & Threat Monitoring** – Helps security teams detect unauthorized access attempts and understand attacker tactics.
2. **Cyber Threat Intelligence (CTI)** – Provides insights into emerging attack techniques, malware propagation, and zero-day exploits.
3. **Network Security Enhancement** – Identifies vulnerabilities in an organization's infrastructure by analyzing real attack data.
4. **Incident Response & Forensics** – Captures attack logs and behaviors for forensic investigations and security audits.
5. **Decoy & Deception Technology** – Misleads attackers, diverting them from critical systems while collecting valuable intelligence.
6. **Testing & Validation of Security Controls** – Assists in evaluating firewall rules, IDS/IPS configurations, and response mechanisms.
7. **Education & Cybersecurity Training** – Used in ethical hacking labs to teach security professionals about real-world attack scenarios.

References/Research Papers: (In IEEE format)

<https://ieeexplore.ieee.org/document/10009485>

<https://ieeexplore.ieee.org/document/10543399>

K J Somaiya College of Engineering, Mumbai-400077

Department of Computer Engineering

Conclusion:

The implementation of a **PenTBox-based honeypot** in a **virtualized network environment** successfully demonstrated its role in **cyber threat detection and analysis**. By simulating a vulnerable service on **Kali Linux** and monitoring network traffic, the honeypot effectively captured **unauthorized access attempts, port scans, and brute-force attacks**. The experiment highlighted the value of **honeypots in cybersecurity**—providing threat intelligence, enhancing network defenses, and aiding forensic investigations.

While **low-interaction honeypots** like PenTBox offer ease of deployment and minimal risk, they are limited in engaging attackers deeply. Future enhancements could include **automated log analysis, integration with intrusion detection systems (IDS), and high-interaction honeypots** for more comprehensive security research.

Overall, this project underscores the **importance of deception technologies** in modern cybersecurity strategies, reinforcing their role in **proactive defense and threat intelligence gathering**.