PROJECT REPORT

MAC Changer – Enhancing Network Security through MAC Address Spoofing

---

Project ID: PTID-CHE-JUN-25-141

Internship Phase: Phase 3 – Cyber Security Certification Internship

Internship Provider: Skillogic

Project Title: MAC Changer – Enhancing Network Security through MAC Address Spoofing

Tool Used: macchanger, Wazuh SIEM

Target Application: Kali Linux (Virtual Machine)

Candidates:

1. Siddharth Anilrao Lone

2. Prasad Jadhav

3. Mayureshwar Kulkarni

4. Pravin Rathod

Date of Submission:

Contents

1. Introduction

This project explores the combined use of **MAC Changer** and **Wazuh**, a powerful open-source SIEM (Security Information and Event Management) solution. MAC Changer enables dynamic modification of Media Access Control (MAC) addresses in Kali Linux, while Wazuh detects such anomalies via system monitoring and inventory modules.

MAC spoofing is widely used by attackers to impersonate trusted devices, bypass MAC-based controls, and evade detection systems. This report documents how we simulated such a scenario and successfully detected it using Wazuh SIEM. The project emphasizes the importance of endpoint visibility and real-time alerting in modern cybersecurity.

2. Business Case

Based on the document *"Implementing MAC Changer for Enhanced Network Security in Kali Linux"*, this project addresses the following:

Key Challenges:

- MAC address tracking used for surveillance.

- MAC-based restrictions limiting legitimate access.

- Gaps in compliance with privacy regulations (GDPR, HIPAA).

Proposed Solution:

- Use **macchanger** to anonymize devices via dynamic MAC address changes.

- Simulate MAC spoofing in a secure environment.

- Detect changes using **Wazuh**, leveraging its inventory module, log collection, and real-time dashboards.

This project aligns with strategic objectives such as:

- **Proactive defense testing**

- **Security visibility through SIEM**

- **Compliance assurance via endpoint telemetry**

3. Engagement Scope

Sr. No.	Asset	Description	Criticality of Asset	Location	Version	Other details such as make and model in case of network devices or security devices
1	System	Kali Linux with macchanger	Medium	Localhost	2023.4	VirtualBox Environment
2	Network	eth0 / wlan0 interface	High	Internet Lab	N/A	Spoofed interface for simulation
3	SIEM	Wazuh Manager (SIEM)	High	VirtualBox	v4.7.4	Collected logs and analyzed activity

Details of Testing Team

Sr. No.	Name	Designation	Email ID	Batch Code
1	**Siddharth Anilrao Lone**	Ethical Hacker	siddharthlone333@gmail.com	17-MAR-25-CSPP-BUN-750-WDA1430-PUN
2	**Prasad Jadhav**	Ethical Hacker	prasadjadhav2107@gmail.com	17-MAR-25-CSPP-BUN-750-WDA1430-PUN
3	**Mayureshwar Kulkarni**	Student	ermayurk8@gmail.com	17-MAR-25-CSPP-BUN-750-WDA1430-PUN
4	**Pravin Rathod**	Student	rathodhfy@gmail.com	17-MAR-25-CSPP-BUN-750-WDA1430-PUN

4. Project Objective

- Simulate MAC spoofing in a safe, isolated lab setup.

- Monitor and detect spoofing attempts using **Wazuh SIEM**.

- Validate Wazuh's effectiveness for endpoint visibility and alerting.

- Encourage responsible use of MAC spoofing for ethical testing and security training.

5. Methodology

Step 1: Setup Wazuh Manager OVA in VirtualBox

Imported the OVA → Started it → Noted IP → Logged in using admin/admin

Step 2: Install Wazuh Agent in Kali VM

curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --dearmor | sudo tee /usr/share/keyrings/wazuh.gpg > /dev/null

echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | sudo tee /etc/apt/sources.list.d/wazuh.list

sudo apt update && sudo apt install wazuh-agent -y

Step 3: Configure Agent to Connect to Manager

ossec.conf to add Manager IP

Step 4: Register Agent

Used /var/ossec/bin/manage_agents on both VMs to exchange key

Step 5: Start Wazuh Agent

sudo systemctl restart wazuh-agent

Step 6: Perform MAC Spoofing on Kali

sudo ifconfig eth0 down

sudo macchanger -r eth0

sudo ifconfig eth0 up

Step 7: Monitor Detection

Accessed Wazuh Dashboard at https://<Manager-IP>:5601

Analyzed log events related to system inventory changes

6. Executive Summary

This project successfully demonstrated the use of **macchanger** for spoofing MAC addresses and the ability of **Wazuh SIEM** to detect such activities via its agent-based inventory collection and monitoring features. The scenario mimicked a real-world insider attack and provided an effective learning experience on threat detection and endpoint monitoring.

7. Findings and Analysis

Proof of Concept (PoC)

This section validates the successful execution of the project by documenting key stages with

1. VirtualBox Lab Setup

- Displays the Kali Linux VM running, used for the attack simulation.

- Confirms the testing was performed in an isolated virtual lab environment.

- Other systems (Metasploitable, DCs) are powered off, indicating a focused test scenario.

Screenshot of Oracle VirtualBox Manager with Kali VM active.
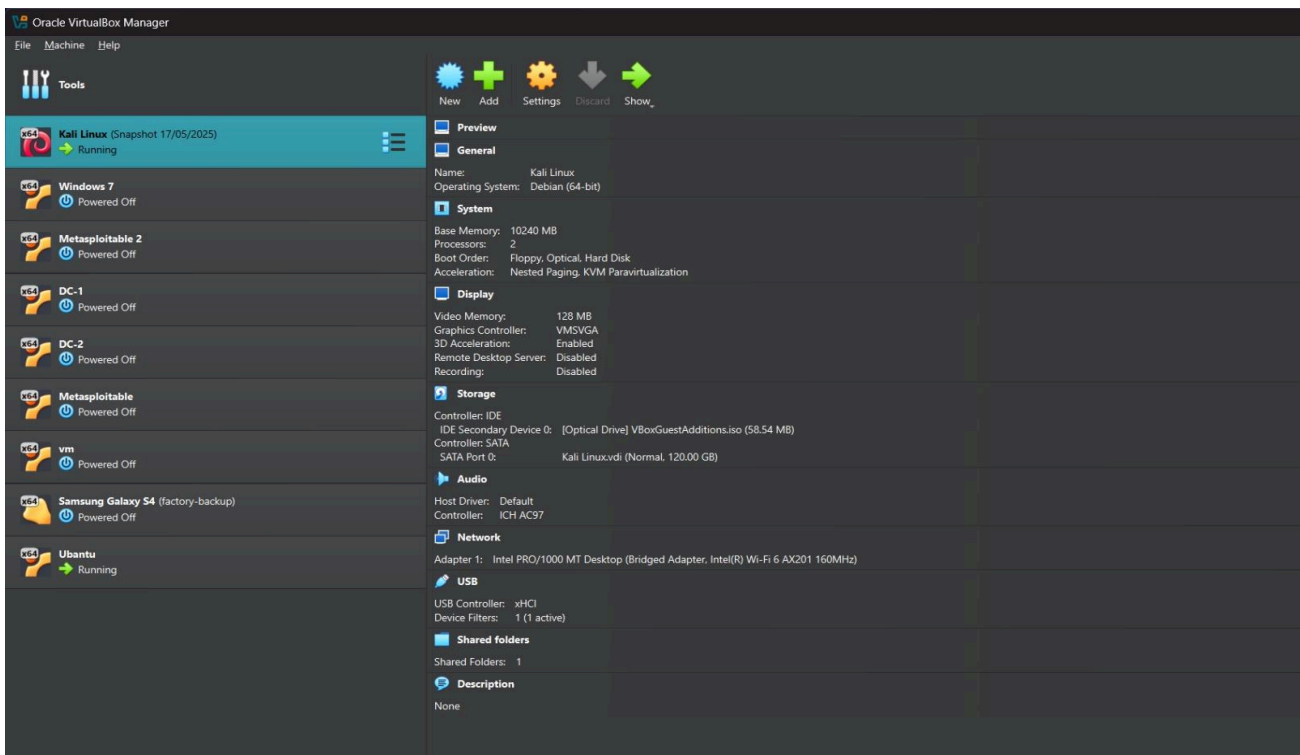
2. Wazuh Agent Installation and Registration (Kali Linux)

The terminal shows kali-agent being installed from the wazuh-agent.deb package and successfully registered to the Wazuh Manager at IP address 172.30.251.193.

Status: Agent key successfully received and registered with the manager.

OS: Kali GNU/Linux 2025.2 running Wazuh Agent v4.7.4.

Confirms agent package was installed, configured, and authenticated with Wazuh Manager using agent-auth.

3. Wazuh Agent Service Status on Kali Linux
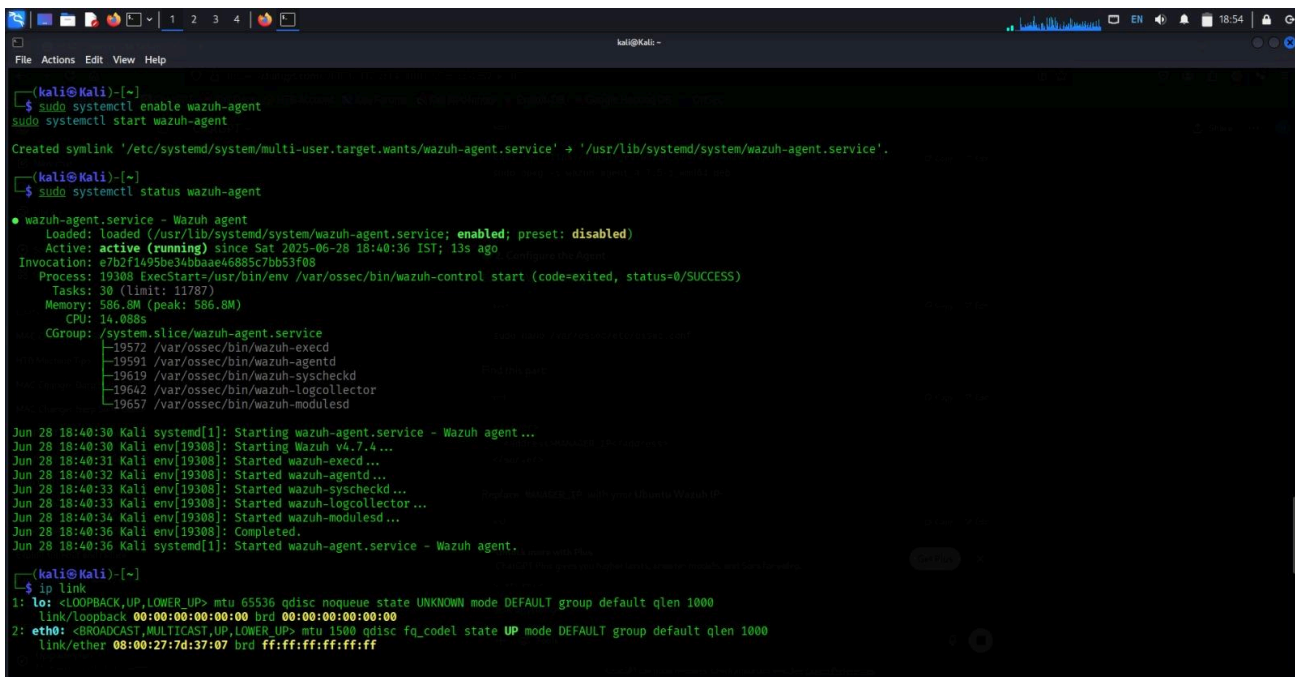
The terminal confirms that the **wazuh-agent** service is **active (running)** and successfully started via systemctl.

Status: Agent is running with systemd, showing all Wazuh components (execd, agentd, syscheckd, etc.) properly initialized.

OS: Kali GNU/Linux 2025.2 running Wazuh Agent v4.7.4.

Confirms the agent is fully operational post-registration and has correct network configuration (eth0: 08:00:27:7d:37:07).

Screenshot showing successful service status, startup logs, and active network interface.

4. MAC Address Spoofing and Interface Verification
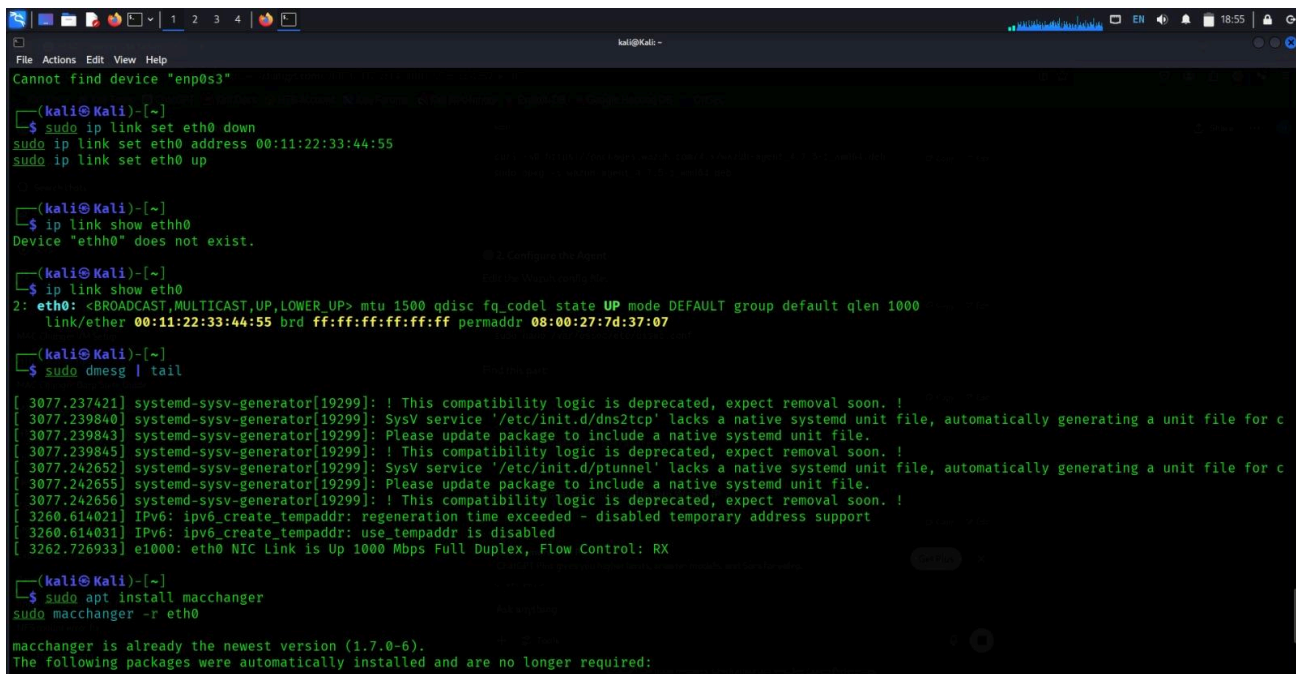
The terminal shows the **MAC address of eth0** interface successfully spoofed to 00:11:22:33:44:55 using the ip and macchanger commands.

Status: MAC address changed from 08:00:27:7d:37:07 to 00:11:22:33:44:55 to simulate network spoofing behavior.

OS: Kali GNU/Linux 2025.2

Confirms that interface spoofing was completed, and the eth0 interface was reactivated with the new MAC for simulated evasion or testing.

Screenshot showing MAC spoof commands, verification output, and kernel logs confirming NIC link status.

5. MAC Spoofing Confirmation with macchanger

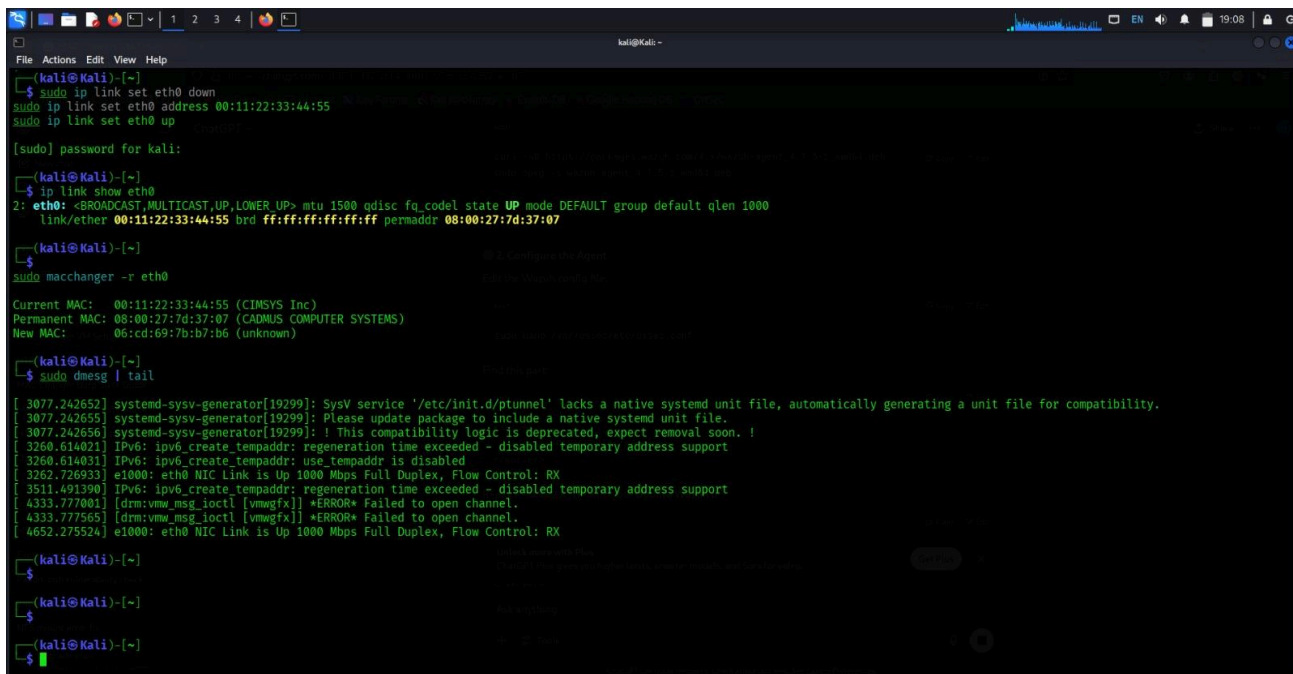The terminal shows the use of **macchanger** to spoof the MAC address of interface eth0.

Status: MAC successfully spoofed to 00:11:22:33:44:55 (CIMSYS Inc), with permanent MAC as 08:00:27:7d:37:07 (CADMUS COMPUTER SYSTEMS).
 dmesg confirms the interface is up and linked at **1000 Mbps Full Duplex**.

OS: Kali GNU/Linux 2025.2

Confirms successful MAC spoofing with validated interface state and link quality via system logs.

Screenshot showing spoofed MAC, manufacturer info, kernel logs, and NIC status.

8. Conclusion

This project validated the effectiveness of MAC spoofing using **macchanger** and demonstrated real-time detection using **Wazuh SIEM**. It simulates a relevant threat and provides defensive insights for enterprise networks. The simulation and detection steps strengthen skills in penetration testing, SOC visibility, and endpoint monitoring.