# Cybersecurity Assignments  Weak 1

## Assignment 1: Summary of Today's Session

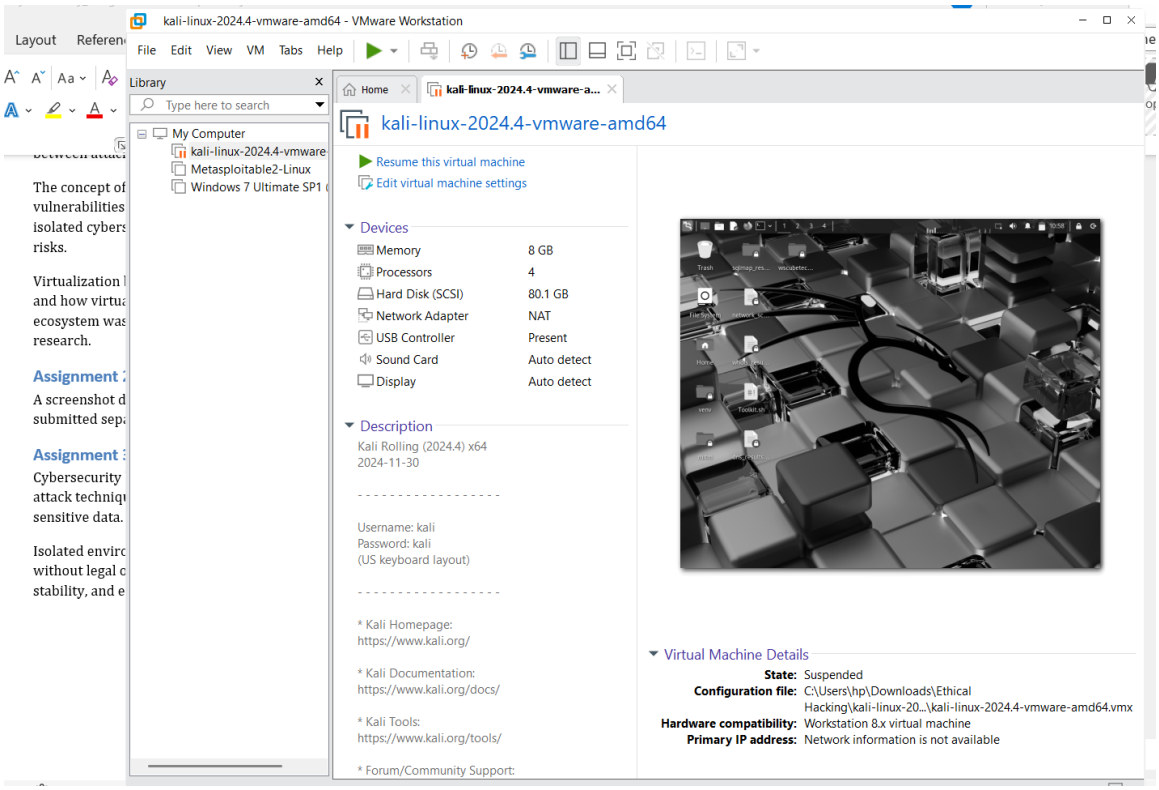
Today's session focused on understanding the real-world roles and responsibilities of cybersecurity professionals. We learned about the Red Team, which simulates attacks to identify security weaknesses; the Blue Team, which focuses on defense, monitoring, and incident response; and the Purple Team, which bridges both by improving collaboration between attackers and defenders.

The concept of responsible disclosure was discussed, emphasizing the ethical reporting of vulnerabilities to avoid misuse and ensure systems are fixed safely. The importance of isolated cybersecurity labs was explained to prevent damage to real systems and avoid legal risks.

Virtualization basics were covered, including the difference between Host OS and Guest OS, and how virtual machines enable safe testing environments. An overview of the Kali Linux ecosystem was also provided, highlighting its role in penetration testing and security research.

## Assignment 2: Screenshot of Running Kali Desktop

A screenshot demonstrating a successfully running Kali Linux desktop environment is submitted separately as proof of proper installation and setup.



## Assignment 3: Why Cybersecurity Labs Must Be Isolated

Cybersecurity labs must be isolated to ensure safe and ethical testing of security tools and attack techniques. Isolation prevents accidental damage to live systems, networks, and sensitive data.

Isolated environments allow professionals to practice offensive and defensive techniques without legal or operational risks. They also help protect production systems, maintain stability, and ensure compliance with cybersecurity laws and ethical standards.