# Project Abstract

This project, conducted as part of the Egypt Digital Pioneers Initiative, involved a simulated red team operation targeting a legacy Linux server within a mid-sized tech company. The objective was to perform a comprehensive security assessment to identify existing vulnerabilities, evaluate the company’s current defenses—including the effectiveness of their Security Operations Center (SOC)—and recommend actionable improvements.  
  
The engagement simulated real-world attack scenarios across several phases: reconnaissance using Nmap and WhatWeb; brute force attacks on a WordPress login; exploitation of a vulnerable plugin to gain a reverse shell; MD5 hash cracking to escalate privileges; and achieving root access via an SUID binary. The red team successfully retrieved three sensitive keys and sanitized logs to avoid detection.  
  
The final report outlined critical vulnerabilities and gaps in monitoring and response, providing clear recommendations such as hardening WordPress, storing passwords securely using bcrypt, applying directory access controls, and enforcing strict privilege management. This project highlights how red teaming can uncover significant weaknesses, assess SOC performance, and guide organizations toward more robust cybersecurity postures.