**Healthcare IT Cybersecurity Project**

**📌 Project Overview**

This project focuses on securing Electronic Health Records (EHRs) by implementing cybersecurity measures such as vulnerability assessments, network traffic monitoring, and endpoint protection. The project includes security testing using tools like Kali Linux, Nmap, Wireshark, ClamAV, and Splunk.

**🎯 Objectives**

* Identify vulnerabilities in healthcare IT systems
* Monitor network traffic for suspicious activity
* Implement endpoint protection for securing EHR data
* Automate security assessments and log analysis

**🛠 Tools & Technologies**

* **Kali Linux** – Security testing and penetration testing
* **Nmap** – Vulnerability scanning
* **Wireshark** – Network traffic analysis
* **ClamAV** – Antivirus and endpoint protection
* **Splunk** – Log monitoring and alerting

**🚀 Implementation Steps**

1. **Set up Virtual Machines** (Windows & Kali Linux)
2. **Perform a network scan** with Nmap to identify vulnerabilities
3. **Monitor network traffic** with Wireshark
4. **Set up endpoint protection** with ClamAV
5. **Configure log monitoring and alerts** using Splunk

**📂 Project Files**

* **Security Scripts** (.py, .sh) – Automated security scans & monitoring scripts
* **Reports** (.pdf, .docx) – Findings, risk assessments, and recommendations

**📢 Contributors**

* **Nikhil Reddy Chitkula** – Health Informatics & Cybersecurity Enthusiast

**📌 License**

This project is open-source under the MIT License.