|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Project Name | Problem Statement | Solution | Tools Used | Area of Cybersecurity | Difficulty Level |
| Email Phishing Detector  Advanced Email Phishing Detector | Phishing emails trick users into revealing sensitive data.  Phishing emails trick users into revealing sensitive data, leading to security breaches. | Use ML to detect phishing emails based on patterns.  Use AI and NLP to detect and flag phishing emails. | Python, TensorFlow  Python, NLTK, SpaCy | Social Engineering & Email Security  Social Engineering, Threat Detection | Easy  Medium |
| Secure Login System | Unauthorized access to accounts is a major threat. | Implement MFA using OTPs or biometrics for enhanced security. | Flask, Twilio API | Identity & Access Management | Easy |
| Basic Malware Analysis  Automated Malware Analysis System | Malware steals data and damages systems.  Manual malware detection is slow and inefficient. | Use a virtual environment to analyze and understand malware behavior.  Use automation for malware behavior and signature analysis. | VirtualBox, Wireshark  Cuckoo Sandbox, Python | Malware Analysis | Easy  Hard |
| Secure File Transfer Protocol | Unencrypted file transfers lead to data breaches. | Encrypt files before transmission using OpenSSL. | OpenSSL, Python | Data Security | Easy |
| Secure Chat Application | Online communications are vulnerable to interception. | Implement end-to-end encrypted chat. | JavaScript, WebRTC | Communication Security | Easy |
| Ransomware Detector System | Ransomware encrypts files and demands ransom, causing severe data loss and financial damage. | Create a system that detects ransomware based on file encryption patterns. | Python, TensorFlow | Malware Analysis, Threat Detection | Medium |
| Secure IoT Network | IoT devices have weak security, making them an easy target for hackers. | Build a secure IoT network with encryption and multi-factor authentication. | Arduino, MQTT | IoT Security | Medium |
| Web Application Firewall (WAF) | Web applications are vulnerable to attacks like XSS and SQL Injection. | Develop a WAF to block malicious traffic before it reaches web apps. | Python, Flask/Django | Web Security | Medium |
| SIEM System | Organizations need real-time alerts to track security threats across multiple sources. | Build a SIEM system to collect, analyze logs, and generate security alerts. | ELK Stack, Python | Security Monitoring, Threat Intelligence | Medium |
| Cloud Security System | Cloud environments are prone to security breaches, requiring strong protection mechanisms. | Build a cloud security system with encryption, access control, and vulnerability scanning. | AWS/Google Cloud, Terraform | Cloud Security | Medium |
| AI-Based Threat Detection | Traditional tools cannot keep up with evolving cyber threats. | Use AI/ML for real-time anomaly detection. | Python, TensorFlow | Threat Intelligence, AI Security | Hard |
| Blockchain-Based Identity Management | Identity theft and breaches are rising due to centralized systems. | Use blockchain and cryptography for secure identity verification. | Ethereum, Solidity | Identity & Access Management | Hard |
| Advanced Penetration Testing Framework | Existing pentest tools lack flexibility for different systems. | Develop a customizable pentesting framework. | Python/Ruby, Metasploit | Ethical Hacking, Red Teaming | Hard |
| Digital Forensics Investigation Toolkit | Current forensic tools struggle with large datasets. | Build an automated forensic toolkit for digital investigations. | Kali Linux, Autopsy | Digital Forensics | Hard |
| Cyber Attack-Wise AI Chatbot | AI-driven chatbots are vulnerable to phishing and manipulation. | Secure chatbot using NLP, encryption, and MFA. | Python, TensorFlow | AI Security, Social Engineering Defense | Hard |
| Real-Time Threat Intelligence Platform | Traditional security tools fail to provide real-time insights. | Aggregate and analyze threat data for proactive monitoring. | ELK Stack, Python | Threat Intelligence | Hard |
| Secure Cloud Storage Solution | Cloud storage is vulnerable to unauthorized access. | Encrypt data at rest and in transit with strict access controls. | AWS/Google Cloud, OpenSSL | Cloud Security | Hard |
| Automated Malware Analysis System | Manual malware detection is slow and inefficient. | Use automation for malware behavior and signature analysis. | Cuckoo Sandbox, Python | Malware Analysis | Hard |
| Compliance and Risk Management Dashboard | Manual compliance tracking is error-prone. | Automate security compliance monitoring and risk assessment. | Power BI/Tableau, Python | Compliance, Risk Management | Hard |