



Best Project Ideas



Informative 299+ Computer Security Project Ideas 2025-26

JULY 20, 2025 | JOHN DEAR



In today's connected world, protecting information and systems from attacks is more important than ever.

Whether you're a beginner dipping your toes into security or an experienced student looking for a challenge, working on hands-on projects is one of the best ways to learn.

This article will guide you through the essentials of computer security, show you how to pick the perfect topic, explain why these projects matter, and provide a list of inspiring project ideas across different skill levels. Let's get started!

Also Read: [281+ Easy Color Wheel Project Ideas For Students](#)

Table of Contents



What Is Computer Security?

Computer security—also known as cybersecurity—is the practice of safeguarding computers, networks, programs, and data from unauthorized access, damage, or theft. Key goals include:

- **Confidentiality:** Ensuring that sensitive information is seen only by those with permission.
- **Integrity:** Making sure that data remains accurate and unaltered except by authorized actions.
- **Availability:** Guaranteeing that systems and data are accessible when needed.

Common threats include malware (viruses, worms), phishing attacks, denial-of-service (DoS) attacks, and insider threats. By studying computer security, you learn how attackers operate and how to design defenses that keep systems safe.

How Do I Choose a Project Topic?

Selecting the right topic sets you up for success. Follow these steps:

1. Assess Your Skill Level

- **Beginner:** Focus on fundamental concepts like encryption, network scanning, or simple vulnerability assessments.
- **Intermediate:** Tackle live capture-the-flag challenges, build intrusion detection tools, or simulate attacks in controlled environments.

- **Advanced:** Work on machine-learning based threat detection, secure protocol design, or develop honeypots and automated pentesting frameworks.

2. Identify Your Interests

- Do you prefer coding (Python, Java)?
- Are you intrigued by networking or web application security?
- Would you like to explore hardware security or IoT devices?

3. Consider Resources

- **Tools:** Wireshark, Metasploit, Nmap, Burp Suite, or open-source libraries.
- **Environments:** Virtual machines (e.g., VirtualBox), cloud sandboxes, or Raspberry Pi setups.
- **Mentorship and Documentation:** Availability of tutorials, community forums, or faculty guidance.

4. Define Clear Objectives

- What problem will your project solve?
- What outcomes or deliverables will you produce (reports, code, demos)?
- What learning goals do you have?

5. Scope & Timeline

- Keep projects manageable: define MVP (minimum viable product) first, then extend if time allows.
- Align with academic deadlines or competition timelines.

By following these steps, you'll land on a project that's challenging yet achievable—and, most importantly, fun!

Informative 299+ Computer Security Project Ideas 2025-26

Network Security

1. **Intrusion Detection with Machine Learning:** Build an IDS using supervised learning to flag anomalous network traffic patterns.
2. **Software-Defined Networking Firewall:** Implement a dynamic firewall on an SDN controller to block threats in real time.

3. **Encrypted Network Traffic Analyzer:** Create a tool that inspects metadata of encrypted flows to detect potential attacks without decrypting content.
4. **IoT Device Scanner:** Develop a scanner that fingerprints and monitors IoT devices on a network for unauthorized changes.
5. **Botnet Detection System:** Design a honeypot-based botnet detector that alerts when infected machines try to propagate.
6. **Secure VLAN Configuration Tool:** Build a script to automate VLAN setup with secure ACLs and logging.
7. **Network Honeynet Deployment:** Deploy a honeynet to trap attackers and analyze their tactics.
8. **Wi-Fi Rogue AP Detector:** Create a system to detect and alert when rogue access points appear.
9. **Automated Port-Scan Monitor:** Implement a service that detects port scanning and temporarily blocks the scanner's IP.
10. **Deep Packet Inspection Engine:** Build a DPI tool to classify traffic and block malicious payloads.
11. **Zero-Trust Network Proof-of-Concept:** Set up a micro-segmented network enforcing least-privilege access.
12. **VPN Vulnerability Scanner:** Develop a scanner that tests common VPN configurations for known flaws.
13. **TLS Certificate Transparency Monitor:** Create a service checking CT logs to detect unauthorized certificate issuance.
14. **SDN Threat Visualization Dashboard:** Build a dashboard showing live threats in an SDN environment.
15. **Network Behavior Baseline Tool:** Design software that learns normal traffic and flags deviations.
16. **Automated IPS Rule Generator:** Use ML to translate IDS alerts into effective IPS blocking rules.
17. **Anomaly Detection for SCADA Networks:** Create a system to spot irregularities in industrial control communications.
18. **Encrypted DNS Abuse Detector:** Build a monitor for DNS over HTTPS/TLS misuse.
19. **Wireless Sensor Network Security Framework:** Develop lightweight encryption and authentication for WSNs.

20. **Network Segmentation Advisor:** Design a tool that suggests optimal segmentation based on traffic analysis.
21. **Passive Traffic Auditor:** Implement a passive tap to audit all network flows for policy compliance.
22. **Network Forensics Toolkit:** Build scripts to capture, index, and search packet captures for investigations.
23. **Secure BGP Route Validation:** Create a POC for RPKI-backed BGP announcement validation.
24. **High-Availability Firewall Cluster:** Deploy two firewalls in active-standby with secure state synchronization.
25. **Latency-Aware IDS:** Research how detection accuracy is affected by packet delays.
26. **Network Access Control with RADIUS:** Implement NAC enforcing endpoint posture checks via RADIUS.
27. **Encrypted Traffic Fingerprinting:** Use ML to identify applications within encrypted streams.
28. **SDN-Based DDoS Mitigator:** Develop a module that reroutes or drops traffic based on volume thresholds.
29. **Port-Knocking Authentication:** Build a port-knocking daemon to stealth-open services only after a secret sequence.
30. **IoT Botnet Honeypot:** Deploy simulated vulnerable IoT devices to study modern botnet behaviors.

Web Application Security

31. **Automated SQLi Scanner:** Develop a crawler that finds and tests SQL injection points in web apps.
32. **XSS Attack Visualization:** Create a tool illustrating how stored XSS propagates through pages.
33. **Content Security Policy Auditor:** Build software that suggests optimal CSP headers for a given site.
34. **API Fuzz Testing Framework:** Implement a fuzzer targeting REST and GraphQL endpoints.

35. **CSRF Exploit Demo App:** Create a demo web app vulnerable to CSRF, then patch it and compare.
36. **OAuth Misconfiguration Detector:** Build a scanner that finds weak OAuth2 setups.
37. **Web Shell Detection:** Develop a system to identify malicious PHP or ASP web shells.
38. **Open Redirect Examiner:** Build a tool to discover and exploit open redirect parameters.
39. **Automated Dependency Vulnerability Checker:** Integrate SCA to flag outdated or vulnerable libraries.
40. **Rate Limiting Bypass Tester:** Research techniques to bypass rate limits on login forms.
41. **Secure Cookie Auditor:** Create a script to test cookie flags (Secure, HttpOnly, SameSite).
42. **JWT Attack Simulator:** Build a suite to test JWT secret weaknesses and replay attacks.
43. **Server-Side Template Injection Finder:** Implement a scanner to locate SSTI in web templates.
44. **Directory Traversal Scanner:** Develop a crawler that tests for path traversal vulnerabilities.
45. **Clickjacking Proof-of-Concept:** Build a demo page that uses iframes to overlay a malicious layer.
46. **GraphQL Schema Vulnerability Analyzer:** Create a tool to find overly permissive GraphQL queries.
47. **Subdomain Takeover Detector:** Automate checks for DNS/CNAME records pointing to unclaimed services.
48. **HTML5 Local Storage Security Review:** Research risks of storing sensitive data in browser storage.
49. **Automated TLS Downgrade Tester:** Build a client that attempts downgrade attacks against HTTPS servers.
50. **Web Application Firewall Bypass Tool:** Implement payloads that evade common WAF rules.
51. **Directory Listing Scanner:** Detect publicly exposed directories and generate reports.

52. **Password Strength Meter Enhancer:** Integrate zxcvbn and test effectiveness against real-world guesses.
53. **Sensitive Data Exposure Auditor:** Crawl pages to find accidental leaks of keys or PII.
54. **Web Cache Poisoning Demonstrator:** Show how crafted requests can poison intermediate caches.
55. **WebSocket Security Tester:** Evaluate authentication and message integrity in WebSocket apps.
56. **Content Injection Scanner:** Automate checks for injection points in user-editable pages.
57. **HTTP2 Attack Stress-Tester:** Research hp2 vulnerabilities like stream multiplexing abuse.
58. **Subresource Integrity Checker:** Build a tool to validate SRI hashes for external scripts.
59. **Automated Security Headers Tester:** Scan sites for missing headers (HSTS, X-Frame, etc.).
60. **Secure File Upload Module:** Implement and test sandboxing for user-uploaded files.

Mobile Security

61. **Android Static Code Analyzer:** Build a tool that flags insecure API usage in APKs.
62. **iOS Jailbreak Detection Library:** Implement runtime checks to detect device compromise.
63. **Mobile App SSL Pinning Demo:** Create an app with pinning and test bypass techniques.
64. **In-App Purchase Fraud Detector:** Research patterns of tampered purchase receipts.
65. **Secure Local Storage Module:** Build an encrypted storage wrapper for sensitive data.
66. **Bluetooth LE Sniffer App:** Capture and analyze BLE packets to find weaknesses.

67. **QR Code Phishing App:** Demonstrate how malicious QR codes can lead to drive-by downloads.
68. **Dynamic Taint Analysis on Android:** Use Frida to track sensitive data flows at runtime.
69. **Mobile Malware Sandbox:** Deploy an emulated environment to safely analyze APK behavior.
70. **SMS Phishing Detector:** Build NLP routines to flag malicious SMS content.
71. **App Permission Visualizer:** Create a UI showing how apps over-request permissions.
72. **Mobile Keylogger Proof-of-Concept:** Show how accessibility services can capture keystrokes.
73. **Secure Biometric Authentication Module:** Integrate and test Android's BiometricPrompt API.
74. **Network Traffic Proxy for Mobile:** Develop a transparent proxy to inspect app traffic.
75. **Tapjacking Vulnerability Demo:** Implement UI overlays to steal touch events.
76. **Android Intent Hijacking Scanner:** Detect apps that mishandle implicit intents.
77. **Mobile Blockchain Wallet Audit:** Analyze a mobile wallet's key management.
78. **Encrypted Backup Tool:** Build an app that securely backs up and restores data.
79. **Location Spoofing Detector:** Research techniques apps use to detect fake GPS.
80. **Kernel Exploit PoC on Android:** Demonstrate privilege escalation via a known CVE.
81. **Mobile Ad Library Privacy Review:** Scan common SDKs for data collection practices.
82. **Automated Mobile App Fuzzer:** Generate random inputs for mobile UI elements.
83. **Secure WebView Integration:** Show proper configuration to prevent JS injection.
84. **Mobile OAuth Flow Tester:** Build scripts to test redirect URIs and token leaks.
85. **Insecure Data in Logs Detector:** Crawl app logs for sensitive information.

86. **Certificate Transparency in Mobile Apps:** Validate CT compliance in TLS connections.
87. **App Store Malware Scanner:** Scrape app stores to flag potentially malicious apps.
88. **Automated Reverse Engineering Pipeline:** Use apktool and jadx to streamline analysis.
89. **Secure OTA Update Mechanism:** Implement signed update checks for a mobile app.
90. **Push Notification Abuse Detector:** Research ways attackers can craft malicious notifications.

IoT & Embedded Systems Security

91. **Firmware Integrity Verifier:** Build a tool that checks firmware images against signed hashes.
92. **Embedded Device UART Sniffer:** Capture bootloader output to find insecure debug messages.
93. **RFID Cloning Detector:** Research anti-cloning techniques for access cards.
94. **IoT Botnet Traffic Analyzer:** Simulate and analyze Mirai-style traffic patterns.
95. **Secure Bootloader for ARM Chips:** Implement chain of trust on a development board.
96. **Wireless Sensor Data Encryption:** Design lightweight crypto for resource-constrained nodes.
97. **Smart Home Protocol Auditor:** Test Zigbee/Z-Wave devices for weak authentication.
98. **Bluetooth Classic Pairing Attack Demo:** Show vulnerabilities in SSP protocols.
99. **CAN Bus Security Module:** Build an intrusion detector for automotive CAN traffic.
100. **IoT Device Honeypot:** Emulate common devices to lure and log attackers.
101. **Physical Unclonable Function POC:** Use silicon variations for device identity.
102. **Firmware Decompilation Toolkit:** Automate extraction and analysis of binary firmware.

103. **Radio Frequency Jamming Detector:** Create a monitor for detecting jamming events.
104. **Smart Meter Privacy Auditor:** Analyze data leaks from smart energy meters.
105. **IoT Over-the-Air Update Security:** Implement HTTPS and signature checks on updates.
106. **Embedded Heap Overflow Exploit:** Demonstrate buffer overflow on a simple IoT OS.
107. **Secure Boot Chain Validation:** Verify each boot stage with public-key signatures.
108. **Wireless Keyless Entry Hack:** Research replay attacks on car key fobs.
109. **IoT Certificate Management Tool:** Automate issuance and rotation for device certs.
110. **Side-Channel Analysis on Crypto Chips:** Measure power traces to extract keys.
111. **LoRaWAN Security Assessment:** Test uplink/downlink encryption and key reuse.
112. **Machine Vision Camera Exploit:** Demonstrate insecure RTSP streams on IP cams.
113. **Smart Lightbulb Penetration Test:** Reverse engineer firmware for backdoors.
114. **Embedded Secure Element Integration:** Add a TPM or SE to a microcontroller project.
115. **Drone Communication Sniffer:** Capture and decode drone control signals.
116. **Secure MQTT Broker:** Build TLS-only broker with client cert authentication.
117. **Over-The-Air OTA Integrity Monitor:** Detect tampering in wireless updates.
118. **IoT Key Provisioning System:** Develop a secure initial key injection process.
119. **RTOS Memory Protection Analysis:** Test MPU setups on FreeRTOS or Zephyr.
120. **Wireless Charging Attack Demo:** Research how inductive chargers can leak data.

Cloud Security

121. **Automated Cloud Misconfiguration Scanner:** Detect open S3 buckets or public IAM roles.

122. **Serverless Function Security Auditor:** Scan AWS Lambda functions for insecure code.
123. **Container Escape POC:** Demonstrate breaking out of a Docker container to host.
124. **Kubernetes RBAC Analyzer:** Build a tool to flag over-permissive cluster roles.
125. **Cloud SIEM Dashboard:** Aggregate logs from multiple cloud services for threat hunting.
126. **IAM Policy Least-Privilege Advisor:** Suggest refined policies based on real usage.
127. **Container Image Vulnerability Scanner:** Integrate Trivy/Clair into CI pipeline.
128. **Cloud Key Management Demo:** Use AWS KMS or GCP KMS to encrypt application data.
129. **Serverless Denial-of-Wallet Mitigator:** Implement limits to prevent runaway billing.
130. **Cloud Forensics Toolkit:** Automate snapshot, log, and metadata collection from VMs.
131. **Multi-Cloud Identity Federation:** Configure trust between Azure AD and AWS IAM.
132. **Encryption-at-Rest Auditor:** Verify that all storage volumes use CMEK/CSEK.
133. **Cloud Network Segmentation POC:** Use VPCs and subnets to enforce zero-trust.
134. **Infrastructure as Code Security Checker:** Lint Terraform/ARM templates for best practices.
135. **Cloud Native WAF:** Deploy and test a WAF service on a Kubernetes ingress.
136. **API Gateway Threat Simulator:** Generate malicious calls to AWS API Gateway.
137. **Cloud Data Leak Detection:** Monitor accidental data exfiltration via logs.
138. **Live VM Memory Analysis:** Snapshot a cloud VM's RAM for malware hunting.
139. **Cloud Secret Scanner:** Crawl code repos for hard-coded API keys destined for the cloud.
140. **Automated Patching Pipeline:** Orchestrate patch rollout to VMs with minimal downtime.
141. **Cloud Honeytrap Deployment:** Spin up decoy services in multiple regions.
142. **Immutable Infrastructure Demo:** Prove how replacing nodes reduces drift and vulnerabilities.

- 143. **Cloud Spoofing Attack Simulator:** Test SSRF and metadata API abuse.
- 144. **Secure CI/CD Pipeline:** Integrate static analysis, vulnerability scanning, and signing.
- 145. **Cloud Access Monitoring:** Alert on unusual API calls or console logins.
- 146. **Container Runtime Security Module:** Hook into containerd to block unsafe syscalls.
- 147. **Cloud Network Traffic Encryption:** Force TLS between all microservices.
- 148. **Multi-Tenant Isolation Test:** Show how noisy neighbors can be prevented.
- 149. **Cloud Patch Compliance Dashboard:** Visualize which resources are out of date.
- 150. **Serverless Function ALT Test:** Fuzz function triggers (S3, SNS, API) for misconfigurations.

Cryptography & Encryption

- 151. **Hybrid Encryption Chat App:** Implement end-to-end encryption combining RSA and AES.
- 152. **Quantum-Safe Encryption Demo:** Use lattice-based crypto to secure messages.
- 153. **Homomorphic Encryption Calculator:** Allow arithmetic on encrypted data without decryption.
- 154. **Secure Multi-Party Computation POC:** Compute sum of private inputs without revealing them.
- 155. **Blockchain-Based Key Exchange:** Use a lightweight ledger to exchange ephemeral keys.
- 156. **Password Manager Prototype:** Build a cross-platform manager with encrypted vaults.
- 157. **ChaCha20 vs AES Benchmark:** Compare performance of both ciphers on embedded boards.
- 158. **Digital Signature Service:** Provide RSA/ECDSA signing and verification APIs.
- 159. **Secure Hash Algorithm Comparison:** Test SHA-2 vs SHA-3 collision resistance.
- 160. **Elliptic Curve Crypto Library:** Implement basic EC key agreement and signatures.
- 161. **Steganography Tool:** Hide encrypted messages within images or audio.

162. **Shamir's Secret Sharing Demo:** Split a secret into n shares with threshold k .
163. **TLS Handshake Visualizer:** Illustrate each step and cryptographic exchange.
164. **Random Number Generator Auditor:** Test entropy sources for bias or weakness.
165. **Side-Channel Resistant AES Implementation:** Add masking to thwart power analysis.
166. **Paillier Encryption Demo:** Showcase additive homomorphic properties in a web app.
167. **Post-Quantum Key Exchange Benchmark:** Compare Kyber or NTRU speeds.
168. **Certificate Authority Simulator:** Issue and revoke certificates in a POC PKI.
169. **Secure Voting System Prototype:** Use crypto to ensure ballot privacy and integrity.
170. **Crypto Wallet Key Recovery Tool:** Implement mnemonic seed generation and validation.
171. **Threshold ECDSA Signing:** Distribute ECDSA signing across multiple parties.
172. **Encrypted Email Plugin:** Integrate PGP encryption into a desktop client.
173. **Macaroons and Attenuation Tokens:** Demo fine-grained authorization with caveats.
174. **Attribute-Based Encryption System:** Encrypt data so only holders of attributes can decrypt.
175. **Quantum Key Distribution Simulator:** Model BB84 protocol exchanges in software.
176. **Secure Random Beacon Service:** Broadcast unpredictable values for time-stamping.
177. **Elliptic Curve Digital Cash POC:** Create unlinkable e-cash tokens with blind signatures.
178. **Verifiable Delay Function Demo:** Use VDFs to time-lock encrypted data.
179. **Crypto-Agility Framework:** Build a toolkit to switch crypto algorithms on the fly.
180. **Encrypted Search Engine:** Enable keyword search over encrypted documents.

Malware Analysis & Reverse Engineering

181. **Automated Malware Sandbox:** Build an isolated VM farm that runs and logs samples.
182. **PE Header Analyzer:** Parse Windows executables and flag suspicious sections.
183. **Heap Exploitation Tutorial:** Craft a controlled buffer overflow in a test program.
184. **Ransomware Behavior Monitor:** Simulate and detect file-encryption patterns.
185. **Obfuscation Technique Comparison:** Test packers like UPX, Themida, and how to unpack.
186. **Linux Rootkit POC:** Demonstrate stealth techniques in a kernel module.
187. **API Hooking Detector:** Build a tool that spots inline hooks in userland processes.
188. **Malware Code Similarity Clustering:** Use fuzzy hashing to group related samples.
189. **Android Native Library Analyzer:** Reverse engineer .so files for suspicious calls.
190. **Phishing Kit Fingerprinter:** Extract unique markers to identify kit families.
191. **Dynamic API Tracer:** Use Frida to log all Windows API calls of a process.
192. **Malicious Office Macro Sandbox:** Automate doc execution and monitor VBScripts.
193. **IoT Malware Emulator:** Reproduce Mirai on a local network to study propagation.
194. **YARA Rule Generator:** Train a model to create YARA signatures from samples.
195. **Steganographic Malware Detector:** Spot executables hiding payloads in images.
196. **DLL-Side Loading Scanner:** Find Windows apps vulnerable to DLL hijacking.
197. **Firmware Backdoor Finder:** Reverse embedded firmware to locate hardcoded credentials.
198. **Machine Learning for Malware Classification:** Train models on static and dynamic features.
199. **API Call Sequence Visualization:** Graph the control flow of disassembled code.
200. **Virustotal API Integration:** Automate bulk submission and report aggregation.
201. **Memory-Only Malware Demo:** Load shellcode directly into memory without files.

- 202. **Rootkit Signature Scanner:** Develop a tool that checks kernel structures for hooks.
- 203. **Encrypted Payload Extractor:** Bypass custom packers to dump decrypted code.
- 204. **Dynamic Link-Time Instrumentation:** Use Intel PIN or DynamoRIO for malware tracing.
- 205. **Macro-less Office Exploit POC:** Leverage OLE or DDE to run code without macros.
- 206. **IoT Botnet Command-and-Control Analysis:** Reverse engineer C&C protocols.
- 207. **Code Obfuscator and Deobfuscator Pair:** Build simple JS obfuscator and corresponding undo tool.
- 208. **Sandbox Escape Experiment:** Demonstrate techniques to break out of Cuckoo or FireEye.
- 209. **Polymorphic Shellcode Generator:** Create shellcode that mutates each build.
- 210. **Malicious PDF Analyzer:** Parse and detect embedded JavaScript exploits.

Ethical Hacking & Penetration Testing

- 211. **Automated Bug-Bounty Recon:** Script OSINT to gather target info for pentests.
- 212. **Wi-Fi WPA3 Cracking POC:** Research weaknesses and attempt handshake capture.
- 213. **Bluetooth LE Pentest Toolkit:** Automate scanning and pairing attacks.
- 214. **Automated Subdomain Enumerator:** Combine bruteforce and certificate transparency data.
- 215. **Privilege Escalation Exploit Demo:** Chain local vulnerabilities on Linux.
- 216. **SSH Brute-Force Detector:** Build a real-time guard to block repeated attempts.
- 217. **Wireless Deauth Attack Tool:** Implement a deauth frame flooder using SDR.
- 218. **RFID Access Bypass:** Emulate valid tags to gain unauthorized entry.
- 219. **Active Directory Attack Simulator:** Demonstrate Kerberoasting and DCSync techniques.
- 220. **USB Rubber Ducky Payloads:** Develop custom keystroke injection scripts.

- 221. **Web-Based VPN Exploit POC:** Test known CVEs against popular VPN appliances.
- 222. **Cross-Platform Backdoor:** Build a stealthy reverse shell in Go.
- 223. **Physical Security Assessment:** Create tools to test badge readers and locks.
- 224. **Password Spraying Automation:** Script low-and-slow attempts against corporate endpoints.
- 225. **Cloud Pivoting Demonstrator:** Show how to move from SaaS to IaaS environments.
- 226. **Social Engineering Toolkit Extension:** Write new modules for phishing campaigns.
- 227. **Firmware Jailbreak Exploit:** Exploit a consumer router to install custom firmware.
- 228. **Satellite Link Penetration Test:** Investigate vulnerabilities in small-sat comms.
- 229. **Active TLS MITM Proxy:** Build a tool that transparently intercepts HTTPS.
- 230. **IoT Device Brute-Force Script:** Automate login attempts against common credentials.
- 231. **API Parameter Fuzzing Tool:** Generate and test random or boundary values.
- 232. **Automated Exploit Chaining:** Create a pipeline that sequences multiple CVEs.
- 233. **Windows Lateral Movement Demo:** Use WMIC/PSEXEC to spread inside a LAN.
- 234. **Pentest Reporting Generator:** Compile findings into a professional PDF report.
- 235. **Mobile App Pentest Framework:** Integrate dynamic and static tools in one suite.
- 236. **Air-Gap Jump Experiment:** Demonstrate data exfiltration via optical or acoustic channels.
- 237. **Java Deserialization Attack Demo:** Craft gadgets to exploit insecure deserialization.
- 238. **Cloud API Abuse Checker:** Test misconfigured IAM and API endpoints.
- 239. **DNS Tunneling Pentest Tool:** Exfiltrate data via crafted DNS queries.
- 240. **Bluetooth Mesh Attack Simulator:** Research potential man-in-the-middle in mesh nets.


Digital Forensics

241. **Disk Image Carving Tool:** Recover deleted files from raw disk images.
242. **Memory Dump Analyzer:** Extract process and network artifacts from RAM captures.
243. **Browser Artifact Parser:** Aggregate history, cookies, and cache for investigations.
244. **File System Timeline Generator:** Build timeline of file events from MFT or inodes.
245. **Registry Change Monitor:** Detect and log Windows registry modifications in real time.
246. **Email Header Analyzer:** Parse headers to trace phishing origins.
247. **Mobile Forensics Suite:** Automate data extraction from Android/iOS backups.
248. **Log Correlation Dashboard:** Merge logs from multiple sources for multi-host incidents.
249. **Cloud Forensics Coordinator:** Script AWS/GCP API calls to gather forensic data.
250. **Encrypted Volume Breaker:** Research weaknesses in LUKS or BitLocker headers.
251. **USB Device History Extractor:** List all USB devices ever connected to a system.
252. **Network Evidence Collector:** Automate pcap capture and indexing by timestamp.
253. **Live Forensics Toolkit:** Develop scripts for safe triage on running systems.
254. **Malware Artifact Extractor:** Identify persistence mechanisms in the registry or crontab.
255. **Cross-Drive Correlator:** Link artifacts across multiple disk images for complex cases.
256. **MAC Address Timeline Visualizer:** Show device movement based on Wi-Fi associations.
257. **Encrypted Chat Recovery:** Recover messages from local app caches.
258. **Forensic Watermark Detector:** Identify steganographic watermarks in media files.
259. **Registry Hive Parser:** Build your own tool to interpret registry hives.
260. **Browser Sync Artifact Extractor:** Analyze synced data from cloud-backed browsers.
261. **Log File Anomaly Detector:** Use ML to flag unusual patterns in system logs.

- 262. **Video Metadata Forensics:** Extract GPS and timestamp info from recorded footage.
- 263. **Database Forensics Engine:** Recover deleted rows and audit transaction logs.
- 264. **Cloud Snapshot Integrity Checker:** Verify VM snapshots against tampering.
- 265. **File Carving with Deep Learning:** Use a neural net to improve file recovery accuracy.
- 266. **Network Flow Reconstruction:** Reassemble sessions from NetFlow records.
- 267. **Automated Incident Response Playbook:** Trigger scripts based on alert types.
- 268. **Encrypted Slack Export Analyzer:** Decrypt and parse archived channel history.
- 269. **Timeline Correlation with OSINT:** Enrich local events with publicly available data.
- 270. **Malware Persistence Path Finder:** Trace registry, service, and scheduled task entries.

AI & Machine Learning Security

- 271. **Adversarial Example Generator:** Craft inputs that mislead image-classification models.
- 272. **Model Poisoning Defense:** Research techniques to detect poisoned training data.
- 273. **Privacy-Preserving ML Demo:** Implement federated learning on distributed datasets.
- 274. **Explainable AI Auditor:** Build a tool that highlights why a model made certain decisions.
- 275. **Deepfake Detector:** Train a CNN to spot forged videos and audio.
- 276. **ML-Based IDS Comparison:** Evaluate different classifiers for network anomaly detection.
- 277. **Model Watermarking POC:** Embed secret signatures in neural network weights.
- 278. **Feature-Space Anomaly Detection:** Use autoencoders to detect out-of-distribution samples.
- 279. **Secure Model Serving API:** Add authentication, rate limiting, and encryption.

280. **Data Drift Monitor:** Alert when incoming data distribution shifts beyond thresholds.
281. **ML Hyperparameter Attack Study:** Show how attackers can infer model hyperparameters.
282. **GAN-Based Malware Generator:** Use GANs to create novel malware and test defenses.
283. **Explainable XSS Classifier:** Build an NLP model to classify and explain XSS payloads.
284. **Robustness Testing Framework:** Automate perturbation tests on vision models.
285. **Machine Vision Spoofing Demo:** Show how printed images can fool object detectors.
286. **Privacy Risk Estimator:** Estimate membership inference risks on a given model.
287. **Steganographic ML Channel:** Hide data within network traffic detected by ML.
288. **Meta-Learning Attack Simulator:** Explore how few-shot learning can be exploited.
289. **Secure Feature Extraction Library:** Harden common feature pipelines against poisoning.
290. **ML-Backed Phishing Detector:** Train a model on email features to flag phishing.
291. **Differential Privacy Integration:** Add DP guarantees to a simple regression model.
292. **Automated Threat Intelligence Classifier:** Use NLP to categorize threat feeds.
293. **SSL/TLS Fingerprint ML Scanner:** Train on handshake metadata to identify malicious servers.
294. **AI-Driven Patch Prioritization:** Predict which vulnerabilities are most likely to be exploited.
295. **Federated Malware Detection:** Share ML model updates, not raw data, across endpoints.
296. **Secure Model Update Protocol:** Design a protocol ensuring integrity of model snapshots.
297. **Explainable Phishing SMS Detector:** Combine NLP and attention maps for  security.

298. **Model Stealing Attack POC:** Demonstrate replication of an API-served model via queries.
299. **Adversarial Training Pipeline:** Automate generation and inclusion of adversarial samples.
300. **Graph-Based Anomaly Detector:** Use GNNs to spot irregularities in network topology.

Why Computer Security Project Ideas Matter

1. Hands-On Learning

- Theory only goes so far—practical projects let you apply concepts, troubleshoot real issues, and gain confidence.

2. Portfolio Building

- Completed projects showcase your skills to employers and academic programs.

3. Problem-Solving Skills

- Security projects force you to think like an attacker and a defender, improving critical thinking and creativity.

4. Staying Current

- Cybersecurity is ever-evolving. Projects on modern topics (e.g., cloud security, machine learning threats) keep you ahead of the curve.

5. Positive Impact

- Your work can help secure open-source tools or small organizations that lack dedicated security teams, making a real difference.

Also Read: [25+ Top Algorithm Project Ideas For Final Year Students](#)

Tips for a Successful Project

- **Document Everything:** Maintain clear README, design notes, and usage guides.
- **Version Control:** Use Git for code and report history.
- **Peer Review:** Share your work with classmates or online communities for feedback.

- **Testing Environment:** Always test security projects in isolated VMs to avoid accidental harm.
- **Ethical Considerations:** Obtain permission before scanning or testing live systems.

Conclusion

Computer security projects aren't just assignments—they're opportunities to make the digital world safer, strengthen your skills, and showcase your talent to future employers.

Whether you start with a simple encryption tool or tackle an advanced machine-learning detector, each project brings you one step closer to becoming a cyber defender. Choose a topic that excites you, plan carefully, and dive in with curiosity and caution. Happy securing!

 [Blog](#)



JOHN DEAR

I am a creative professional with over 5 years of experience in coming up with project ideas. I'm great at brainstorming, doing market research, and analyzing what's possible to develop innovative and impactful projects. I also excel in collaborating with teams, managing project timelines, and ensuring that every idea turns into a successful outcome. Let's work together to make your next project a success!



291+ Simple Design Thinking Project Ideas For Engineering Students

Best Project Ideas

Are you ready to make your big ideas happen? Let's connect and discuss how we can bring your vision to life. Together, we can create amazing results and turn your dreams into reality.

Top Pages

[Terms And Conditions](#)

[Disclaimer](#)

[Privacy Policy](#)

Follow Us

© 2024 [Best Project Ideas](#)