**The Complete Cybersecurity Encyclopedia: 200+ Class Ultimate Mastery Program**

**Phase 1: Digital Literacy Foundation**

1. Computer Hardware Deep Dive (CPU, RAM, Storage Architectures)
2. Operating System Internals (Windows, Linux, macOS)
3. Filesystems Explained (NTFS, EXT4, APFS, ZFS)
4. Memory Management Fundamentals
5. Process and Thread Architecture
6. Interrupts and System Calls
7. Device Drivers and Kernel Modules
8. BIOS/UEFI Firmware Security
9. Hardware Security Modules (HSM, TPM)
10. Virtualization Technologies (Type 1/2 Hypervisors)
11. Containerization vs Virtualization
12. Cloud Computing Models (IaaS, PaaS, SaaS)
13. Binary and Hexadecimal Mastery
14. Data Representation (Big/Little Endian)
15. Character Encoding (Unicode, ASCII)
16. Boolean Algebra for Security
17. Regular Expressions for Security Pros
18. Data Structures for Hackers
19. Algorithms in Cybersecurity
20. Computational Complexity Basics
21. Networking Hardware (Routers, Switches, Firewalls)
22. Wireless Technologies (WiFi 6, 5G, Bluetooth)
23. IoT Device Architectures
24. Embedded Systems Security
25. Industrial Control Systems Overview
26. Automotive Systems Security
27. Aerospace Cybersecurity Basics
28. Medical Device Security
29. Satellite Communication Security
30. Quantum Computing Primer

**Phase 2: Networking Mastery**

1. Physical Layer Exploits (Cable Tapping, Signal Jamming)
2. Data Link Layer Attacks (MAC Flooding, VLAN Hopping)
3. Network Layer Warfare (IP Spoofing, ICMP Attacks)
4. Transport Layer Exploits (TCP Sequence Prediction)
5. Session Layer Manipulation (Session Hijacking)
6. Presentation Layer Attacks (Encoding/Encryption Flaws)
7. Application Layer Assaults (HTTP Smuggling)
8. DNS Deep Dive (All Record Types)
9. Advanced DHCP Exploitation
10. BGP Hijacking Techniques
11. MPLS Security Considerations
12. VoIP Vulnerabilities (SIP, RTP)
13. VPN Protocols Analysis (IPSec, OpenVPN, WireGuard)
14. TLS 1.3 Internals and Attacks
15. QUIC Protocol Security
16. WebSockets Security Analysis
17. gRPC Security Considerations
18. API Gateway Security
19. CDN Security Challenges
20. Load Balancer Security
21. Proxy Server Vulnerabilities
22. Mail Server Security (SMTP, IMAP, POP3)
23. Database Protocol Security
24. Industrial Protocols (Modbus, DNP3)
25. SCADA Protocol Analysis
26. Automotive Protocols (CAN Bus)
27. Aviation Protocols (ARINC, AFDX)
28. Maritime Communication Security
29. Satellite Protocols Security
30. RFID/NFC Security Deep Dive
31. Bluetooth Low Energy Hacking
32. Zigbee/Z-Wave Security
33. 5G Network Security
34. WiFi 6 Security Analysis
35. Rogue Device Detection
36. Network Forensic Artifacts
37. Full Packet Capture Analysis
38. NetFlow/SFlow Analysis
39. Network Behavior Analysis
40. Advanced Threat Hunting

**Phase 3: Web Security**

1. HTTP/1.1 vs HTTP/2 vs HTTP/3 Security
2. Browser Security Mechanisms
3. Same-Origin Policy Deep Dive
4. CORS Implementation Flaws
5. CSP Bypass Techniques
6. Web Cryptography API Security
7. Advanced SQL Injection
8. NoSQL Injection Techniques
9. GraphQL Injection
10. Server-Side Template Injection
11. Server-Side Request Forgery
12. Server-Side JavaScript Injection
13. Web Cache Poisoning
14. HTTP Request Smuggling
15. WebSocket Hijacking
16. DOM-Based Vulnerabilities
17. Prototype Pollution Attacks
18. WebAssembly Security
19. JWT Implementation Flaws
20. OAuth/OIDC Security Issues
21. SAML Security Considerations
22. Web Application Firewall Bypasses
23. API Security Testing
24. Microservices Security
25. Serverless Security
26. Web3 Security (Smart Contracts)
27. NFT Security Considerations
28. DeFi Security Analysis
29. Blockchain Node Security
30. Cryptocurrency Wallet Security

**Phase 4: System Exploitation**

1. Windows Kernel Architecture
2. Linux Kernel Internals
3. macOS Darwin Kernel
4. Android Security Model
5. iOS Security Architecture
6. Hypervisor Security (VMware, Hyper-V, KVM)
7. Container Breakout Techniques
8. Cloud Instance Escapes
9. Process Injection Techniques
10. Memory Corruption Fundamentals
11. Stack-Based Buffer Overflows
12. Heap Exploitation Techniques
13. Use-After-Free Exploits
14. Race Condition Vulnerabilities
15. Format String Exploits
16. Integer Overflow/Underflow
17. Type Confusion Vulnerabilities
18. Logic Bugs in Software
19. Windows Privilege Escalation
20. Linux Privilege Escalation
21. macOS Privilege Escalation
22. Active Directory Exploitation
23. LDAP Injection Attacks
24. Kerberos Attacks (Golden/Silver Tickets)
25. NTLM Relay Attacks
26. Pass-the-Hash Techniques
27. Token Impersonation Attacks
28. Windows Registry Attacks
29. Linux SUID/SGID Exploitation
30. macOS Authorization Bypass
31. Firmware-Level Attacks
32. Bootloader Vulnerabilities
33. Secure Boot Bypasses
34. TPM Exploitation Techniques
35. Virtualization-Based Attacks

**Phase 6: Defensive Basics**

**Core Security Principles**

1. CIA Triad Deep Dive (Confidentiality, Integrity, Availability)
2. Defense-in-Depth Strategy (Layered Security Controls)
3. Least Privilege & Zero Trust Models
4. Security Policies & Procedures (ISO 27001, NIST CSF)
5. Risk Management Fundamentals (Identification, Assessment, Mitigation)

**Endpoint Protection**

1. Antivirus vs. EDR vs. XDR (How They Work)
2. Host-Based Firewalls (Windows Firewall, iptables)
3. Patch Management (WSUS, Linux Repositories)
4. Application Whitelisting/Blacklisting\*\*
5. \*\*USB Device Control\*\* (Blocking Malicious Peripherals)
6. #### \*\*Module 3: Network Defense\*\*
7. \*\*Network Segmentation\*\* (VLANs, Subnets)
8. \*\*Firewall Configuration\*\* (pfSense, Cisco ACLs)
9. \*\*IDS/IPS Systems\*\* (Snort, Suricata Rule Basics)
10. \*\*VPN Security\*\* (WireGuard, IPsec Best Practices)
11. \*\*Wi-Fi Protection\*\* (WPA3, Rogue AP Detection)
12. #### \*\*Module 4: Authentication Security\*\*
13. \*\*Password Policies\*\* (Complexity, Rotation, Hashes)
14. \*\*Multi-Factor Authentication\*\* (TOTP, FIDO2, Push)
15. \*\*Single Sign-On (SSO) Security\*\*
16. \*\*Active Directory Hardening\*\*
17. \*\*Privileged Access Management (PAM)\*\*
18. #### \*\*Module 5: Monitoring & Response\*\*
19. \*\*Log Management\*\* (SIEM Overview - Splunk, ELK)
20. \*\*Windows Event Log Analysis\*\* (Critical IDs to Monitor)
21. \*\*Linux Auditd Framework\*\* (System Call Monitoring)
22. \*\*Incident Response Steps\*\* (Preparation to Recovery)
23. \*\*Backup Strategies\*\* (3-2-1 Rule, Immutable Backups)
24. #### \*\*Module 6: Web & Email Protection\*\*
25. \*\*Web Application Firewalls\*\* (ModSecurity, Cloudflare)
26. \*\*Secure Email Gateways\*\* (DMARC, DKIM, SPF)
27. \*\*Browser Security Controls\*\* (CSP, SRI, HTTPS)
28. \*\*Cloud Security Basics\*\* (Shared Responsibility Model)
29. \*\*Security Awareness Training\*\* (Phishing Simulations)

**Phase 6: Offensive Cyber Attack**

**Network Attacks**

1. Network Reconnaissance (Nmap, Masscan, Zmap)
2. ARP Spoofing/Poisoning (MITM Attacks)
3. DNS Cache Poisoning (Pharming Attacks)
4. DHCP Starvation & Rogue Server Attacks
5. BGP Hijacking (Internet Route Manipulation)
6. VPN Exploitation (IPSec, OpenVPN, WireGuard)
7. SSL/TLS Stripping (Downgrade Attacks)
8. VoIP Hacking (SIPVicious, RTP Injection)

**Password & Authentication Attacks**

1. Brute Force Attacks (Hydra, Medusa)
2. Dictionary & Rainbow Table Attacks (Hashcat, John)
3. Pass-the-Hash (PtH) Attacks
4. Kerberos Exploits (Golden/Silver Ticket Attacks)
5. NTLM Relay Attacks (Responder, Impacket)
6. OAuth & JWT Exploitation (Token Hijacking)
7. Biometric Bypass (Fingerprint Spoofing)

**Web Application Attacks**

1. SQL Injection (SQLi) – Manual & Automated
2. Cross-Site Scripting (XSS) – Stored, Reflected, DOM
3. CSRF & SSRF Exploitation
4. XML External Entity (XXE) Injection
5. API Abuse (GraphQL, REST, SOAP)
6. Web Cache Poisoning & Deception
7. HTTP Request Smuggling (CL.TE, TE.CL)
8. WebSocket Hijacking
9. OAuth & SAML Exploits

**Social Engineering & Phishing**

1. Advanced Phishing (GoPhish, SEToolkit)
2. Clone Websites & Evil Twin Attacks
3. Vishing (Voice Phishing) & Smishing (SMS)
4. Malicious QR Codes & Physical Attacks
5. Deepfake Phishing (AI-Generated Audio/Video)

**Malware & Exploitation**

1. Trojan Development (Python, C, PowerShell)
2. Ransomware Development (Encryption, Exfiltration)
3. Fileless Malware (Memory-Resident Attacks)
4. Polymorphic Malware (AV Evasion)
5. Rootkit Development (Kernel-Level Persistence)
6. USB Drop Attacks (BadUSB, Rubber Ducky)

**Wireless & IoT Attacks**

1. Wi-Fi Cracking (WPA3, WPS Attacks)
2. Bluetooth Hacking (BLE Exploits)
3. RFID/NFC Cloning & Spoofing
4. Zigbee/Z-Wave Hacking (Smart Home Attacks)
5. Drone Hijacking (GPS Spoofing)

**Cloud & Container Attacks**

1. AWS/Azure/GCP Exploitation (Misconfigurations)
2. Kubernetes Privilege Escalation
3. Container Breakouts (Docker, Podman)
4. Serverless Function Abuse (Lambda, Cloud Functions)

**Advanced Attacks**

1. Zero-Day Exploitation (Fuzzing, Reverse Engineering)
2. SCADA/ICS Attacks (Modbus, DNP3 Exploits)
3. Automotive Hacking (CAN Bus Injection)
4. Satellite Communication Hacks
5. AI-Powered Attacks (GPT-Phishing, Worm Generation)

Quantum Computing Attacks (Future Threats)

**Phase 7: Advanced Defense**

1. Security Operations Center Architecture
2. Threat Intelligence Platforms
3. Security Information Event Management
4. Extended Detection and Response
5. Network Detection and Response
6. Endpoint Detection and Response
7. Cloud Detection and Response
8. Deception Technology
9. Threat Hunting Methodologies
10. Malware Analysis Sandboxes
11. Static Analysis Techniques
12. Dynamic Analysis Methods
13. Reverse Engineering Fundamentals
14. IDA Pro Advanced Usage
15. Ghidra Scripting
16. Binary Ninja Techniques
17. Windows Forensic Analysis
18. Linux Forensic Analysis
19. Memory Forensic Analysis
20. Network Forensic Analysis
21. Mobile Device Forensics
22. Cloud Forensics
23. IoT Device Forensics
24. Automotive Forensics
25. Industrial System Forensics
26. Threat Actor Attribution
27. Cyber Kill Chain Analysis
28. MITRE ATT&CK Framework
29. Diamond Model of Analysis
30. Cyber Threat Intelligence

**Phase 7: Emerging Technologies**

1. AI Security Risks
2. Machine Learning Model Attacks
3. AI-Powered Defense Systems
4. Quantum Cryptography
5. Post-Quantum Algorithms
6. Homomorphic Encryption
7. Secure Multi-Party Computation
8. Zero-Knowledge Proofs
9. Blockchain Security
10. Smart Contract Auditing
11. Decentralized Identity Security
12. 6G Security Preview
13. Space Network Security
14. Drone Security Systems
15. Autonomous Vehicle Security
16. Robotics Security
17. Brain-Computer Interface Security
18. Nanotechnology Security
19. Biomedical Device Security
20. Smart City Security
21. Critical Infrastructure Protection
22. Cyber Warfare Strategies
23. Nation-State Threat Analysis
24. Cyber Arms Control
25. Future of Cybersecurity

**Phase 8: Professional Mastery**

1. Security Consulting Business
2. Managed Security Services
3. Product Security Engineering
4. Security Architecture Design
5. Compliance Frameworks
6. Risk Management Methodologies
7. Security Awareness Training
8. Incident Response Planning
9. Disaster Recovery Planning
10. Business Continuity Planning
11. Security Metrics and Reporting
12. Executive Communication
13. Technical Writing for Security
14. Public Speaking for Security Pros
15. Security Certification Paths
16. Building a Personal Brand
17. Security Research Methodologies
18. Responsible Disclosure
19. Bug Bounty Strategies
20. Career Growth Planning