CYBERSECURITY MASTERY PROGRAM

A 4-Month Journey from Basic to Advanced Cybersecurity

Includes dedicated modules on Phishing, Social Engineering, Wi-Fi Security & a 1-Month Capstone Project

Duration	16 Weeks (4 Months)
Format	Theory + Hands-on Labs + Capstone Project
Level	Beginner → Intermediate → Advanced
Mode	Self-paced / Instructor-led (Adaptable)

Table of Contents

Program Overview

This 4-month program takes a learner from absolute basics of cybersecurity to advanced, hands-on offensive and defensive skills. Each month builds on the last: fundamentals first, then core network/system/web security, then applied offensive topics including **phishing**, **social engineering**, and **Wi-Fi (wireless) security**, and finally an entire month dedicated to a real-world **capstone project** that ties every skill together.

Learning Outcomes

- Understand core security principles: CIA triad, threat modeling, risk management, and compliance basics.

Month	Focus	Level
Month 1	Cybersecurity Foundations, Networking & OS Basics	Basic
Month 2	System, Network & Web Application Security	Intermediate
Month 3	Phishing, Social Engineering, Wi-Fi Security & Ethical Hacking	Advanced

Month 4	Capstone Project — Plan, Build, Test, Report, Present	Applied / Advanced

- Gain working knowledge of networking, operating systems (Linux/Windows), and cryptography.
- Identify and analyze common attack vectors: malware, phishing, social engineering, and wireless attacks.
- Perform basic penetration testing and vulnerability assessment using industry-standard tools.
- Design phishing-simulation and security-awareness exercises for organizations.
- Secure wireless networks and understand Wi-Fi attack/defense techniques (WPA2/WPA3, rogue APs, etc.).
- Plan, execute, document, and present a full end-to-end cybersecurity capstone project.

Program Structure at a Glance

MONTH 1

Week 1 — Introduction to Cybersecurity

- What is cybersecurity? CIA Triad (Confidentiality, Integrity, Availability)
- Types of hackers, cybercrime landscape, and common threat actors
- Security terminology: vulnerability, exploit, threat, risk
- Overview of cybersecurity career paths and certifications (CompTIA Security+, CEH, OSCP)

Hands-on Lab: Set up a personal cybersecurity lab (VirtualBox/VMware + Kali Linux + Windows VM).

Week 2 — Networking Fundamentals

- OSI & TCP/IP models, IP addressing, subnetting basics
- Common protocols: HTTP/HTTPS, DNS, FTP, SSH, SMTP
- Ports, firewalls, and how packets travel across a network
- Introduction to Wireshark for packet analysis

Hands-on Lab: Capture and analyze live traffic with Wireshark; identify protocols and suspicious packets.

Week 3 — Operating System & Linux Essentials

- Linux fundamentals: file system, permissions, users/groups
- Essential Linux commands for security professionals
- Windows security basics: Active Directory overview, user accounts, policie
- Introduction to Kali Linux and its toolset

Hands-on Lab: Navigate and harden a Linux VM; practice permission management and basic shell scripting.

Week 4 — Cryptography & Security Principles

- Symmetric vs asymmetric encryption, hashing, digital signatures
- SSL/TLS and how HTTPS secures the web
- Authentication, authorization & access control models (MFA, RBAC)
- Month 1 recap quiz and knowledge checkpoint

Hands-on Lab: Use OpenSSL to generate keys, encrypt files, and verify hashes (MD5/SHA256).

MONTH 2

Week 5 — Network Security

- Firewalls, IDS/IPS, VPNs, and network segmentation
- Common network attacks: MITM, ARP spoofing, DoS/DDoS
- Secure network architecture design principles

Hands-on Lab: Configure a basic firewall (iptables/pfSense) and simulate an ARP spoofing attack in a lab.

Week 6 — System & Endpoint Security

- Malware types: viruses, worms, trojans, ransomware, spyware
- Antivirus/EDR concepts, patch management, hardening checklists
- Introduction to malware analysis (static vs dynamic)

Hands-on Lab: Analyze a sample malware behavior report in a sandboxed environment (e.g., Any.Run/Cuckoo).

Week 7 — Web Application Security

- OWASP Top 10 overview: SQL Injection, XSS, CSRF, broken auth
- Web security testing basics with Burp Suite
- Secure coding principles and input validation

Hands-on Lab: Exploit and remediate vulnerabilities in OWASP Juice Shop / DVWA (legal practice environments).

Week 8 — Vulnerability Assessment & Risk Management

- Vulnerability scanning with Nessus/OpenVAS
- Risk assessment frameworks (NIST, ISO 27001 basics)
- Incident response lifecycle and security policies
- Month 2 recap and hands-on assessment

Hands-on Lab: Run a full vulnerability scan on a lab network and produce a basic risk report.

MONTH 3

Week 9 — Social Engineering

- Psychology of social engineering: pretexting, baiting, tailgating, quid pro quo
- Real-world case studies of social engineering attacks
- Building organizational security awareness and human-risk programs
- Legal and ethical boundaries of social engineering testing

Hands-on Lab: Design a social engineering awareness scenario/script and evaluate it against an ethics checklist.

Week 10 — Phishing: Attack & Defense

- Types of phishing: email phishing, spear phishing, whaling, smishing, vishing
- Anatomy of a phishing email: headers, spoofed domains, malicious links/attachments
- Building a phishing-simulation campaign (for authorized awareness training only)
- Anti-phishing defenses: SPF, DKIM, DMARC, email gateways, user training

Hands-on Lab: Set up a controlled, authorized phishing-awareness simulation using an open-source platform (e.g., GoPhish) inside your lab.

Week 11 — Wi-Fi & Wireless Security

- Wireless standards and encryption: WEP, WPA2, WPA3
- Common Wi-Fi attacks: rogue access points, evil twin, deauthentication, handshake capture
- Wireless auditing tools: Aircrack-ng suite, Wireshark for Wi-Fi
- Hardening a wireless network: strong encryption, segmentation, monitoring

Hands-on Lab: Audit a personal/lab Wi-Fi network's security posture and apply WPA3-level hardening recommendations.

Week 12 — Ethical Hacking & Penetration Testing Basics

- Penetration testing methodology: recon, scanning, exploitation, reporting
- Introduction to Metasploit Framework for authorized testing
- Combining phishing, social engineering & technical exploits in a red-team scenario
- Month 3 recap: capture-the-flag (CTF) style challenge

Hands-on Lab: Complete a beginner CTF room (e.g., TryHackMe/HackTheBox) covering recon-to-exploitation basics.

MONTH 4

The final month is dedicated entirely to a hands-on capstone project. Learners choose one project track (or an instructor-assigned one) and work through the full security lifecycle: planning, execution, documentation, and presentation — mirroring a real job deliverable.

Week 13 — Project Planning & Scoping

- Choose a project track (see options below) and define scope & rules of engagement
- Create a project plan, timeline, and required tool/lab setup
- Draft a threat model / attack plan for the chosen environment

Week 14 — Execution Phase 1

- Begin technical work: scanning, testing, or building (based on chosen track)
- Document findings continuously (screenshots, logs, evidence)
- Mid-project check-in and adjustment of scope if needed

Week 15 — Execution Phase 2 & Remediation

- Complete remaining technical work and validate results
- Propose remediation/mitigation steps for every finding
- Begin drafting the formal project report

Week 16 — Reporting, Review & Presentation

- Finalize a professional security report (executive summary + technical findings)
- Peer review / instructor review of the project
- Final presentation of the project and Q&A;
- Course wrap-up, feedback, and certificate of completion

Suggested Capstone Project Tracks (choose one)

Track	Description
Phishing Awareness Campaig	n Design, launch (in an authorized lab), and report on a full phishing-simulati including me
Wi-Fi Security Audit	Perform a complete wireless security audit of a lab network: identify weakn scenario
Small Business Security Asse	Simulate a full vulnerability assessment and social engineering risk revie small business.
Home/SOHO Network Defens	e BuildDesign and implement a secure home/small-office network: firewall rul ardening, mon

Capture-the-Flag Portfolio Pro	ectSolve and document a series of progressive CTF challenges spanning we *w*ireless se

Tools & Platforms Used Throughout the Course

Category	Tools / Platforms
Lab Environment	VirtualBox / VMware, Kali Linux, Windows VM
Network Analysis	Wireshark, Nmap
Web Security	Burp Suite, OWASP Juice Shop, DVWA
Vulnerability Scanning	Nessus, OpenVAS
Exploitation Framework	Metasploit Framework
Phishing Simulation	GoPhish (authorized/lab use only)
Wireless Security	Aircrack-ng suite, Wireshark
Practice Ranges	TryHackMe, HackTheBox (CTF platforms)
Cryptography	OpenSSL

Assessment, Certification & Career Paths

Learners are assessed through weekly labs, monthly checkpoint quizzes/CTF challenges, and the final capstone project (report + presentation). Upon successful completion, learners receive a Certificate of Completion and a portfolio-ready capstone project suitable for job applications or as a foundation to pursue industry certifications such as CompTIA Security+, CEH, or OSCP.

Ethics Note: All offensive techniques (phishing simulations, social engineering exercises, Wi-Fi attacks, exploitation) are taught strictly for use in authorized lab environments or with explicit written permission. Unauthorized use against real systems is illegal.