Complete Ethical Hacking & Penetration Testing Master Syllabus

Phase 1: Foundations (0-100 Level)

1. Cybersecurity Fundamentals

CIA Triad vs DIE Model (Distributed, Immutable, Ephemeral)

Security vs Privacy vs Anonymity frameworks

Threat actors: Script Kiddies -> APTs -> Nation-State

2. Legal & Compliance

Computer Fraud and Abuse Act (CFAA) case studies

GDPR Article 32 technical requirements

HIPAA Security Rule penetration testing exceptions

3. Lab Architecture

Proxmox vs ESXi for nested virtualization

Docker-based vulnerable apps (Damn Vulnerable Docker)

Cloud lab alternatives: HTB Academy, PentesterLab Pro

Phase 2: Reconnaissance (100-200 Level)

4. Advanced OSINT

Satellite imagery analysis (Google Earth Engine)

Facial recognition OSINT (PimEyes, Clearview AI)

Vehicle recognition for physical penetration testing

5. Network Discovery

IPv6 scanning with thc-ipv6

SCADA protocol fingerprinting (Modbus, DNP3)

Passive DNS mapping with Farsight DNSDB

6. Vulnerability Assessment

Credentialed scanning with Nessus TNS

API scanning with Postman + OWASP ZAP

Container scanning: Trivy vs Grype vs Clair

Phase 3: Initial Access (200-300 Level)

7. Web App Exploitation

GraphQL batching attacks

WebSocket hijacking with ws-harness

DOM Clobbering to XSS chains

8. Binary Exploitation

ROP chain development with ROPgadget

Heap Feng Shui in modern glibc

Linux kernel UAF exploitation

9. Cloud Initial Access

Azure AD internal tenant enumeration

GCP organization policy bypasses

AWS Lambda persistence via layers

Phase 4: Post-Exploitation (300-400 Level)

10. Windows Domain Dominance

DCSync attack variations

ADCS relay attacks with PetitPotam

Certificate template exploitation

11. Linux Privilege Escalation

eBPF-based privilege escalation

Kernel module rootkits (DKOM)

Systemd timer backdoors

12. C2 Framework Mastery

Cobalt Strike Malleable C2 profiles

Mythic agent development in Go

DNS-over-HTTPS C2 channels

Phase 5: Advanced Red Teaming (400-500 Level)

13. Physical Security

RFID cloning with Proxmark3 Easy

Thermal camera attacks (keypad heat residue)

Ultrasonic keyboard eavesdropping

14. Wireless Advanced

WPA3 Dragonblood attacks

Bluetooth mesh network exploitation

5G IMSI catcher development

15. ICS/SCADA Offense

Modbus TCP command injection

Siemens S7 PLC stop commands

HMI vulnerability exploitation

Phase 6: Emerging Threats (500-600 Level)

16. AI Security

LLM prompt injection attacks

Model stealing via API side channels

Adversarial ML against EDR systems

17. Quantum Hacking

Shor's algorithm practical implementation

Post-quantum cryptanalysis

Quantum network sniffing techniques

18. Space Systems Security

Satellite command injection

GPS spoofing with HackRF + LTE

Cubesat security testing

Phase 7: Elite Tradecraft (600-700 Level)

19. Counter-Forensics

NTFS alternate data streams

Linux kernel memory anti-forensics

Secure element chip glitching

20. Advanced Evasion

Process Doppelgänging 2.0

Thread stack spoofing

Hardware-assisted stealth (Intel CET)

21. Zero-Click Exploits

iMessage zero-day chains

MMS exploit development

Bluetooth zero-click RCE

Phase 8: Specialized Targets (700-800 Level)

22. Automotive Hacking

CAN bus injection with CANtact

Tesla infotainment exploits

EV charging station attacks

23. Medical Devices

Insulin pump radio attacks

DICOM protocol manipulation

MRI machine security testing

24. Aviation Systems

ADS-B spoofing

ACARS protocol exploitation

FMS (Flight Management System) hacking

Phase 9: Offensive R&D (800-900 Level)

25. Exploit Development

ARM64 ROP chains

Windows 11 kernel exploit mitigation bypasses

Hypervisor escape techniques

26. Malware Engineering

Polymorphic engine development

UEFI rootkit creation

GPT-4 assisted malware coding

27. Custom Hardware

FPGA-based packet injection

Raspberry Pi Pico BadUSB devices

Hardware implants (Drop Bears)

Phase 10: The Ultimate Challenge (900-1000 Level)

28. Full-Spectrum Exercises

48-hour red team engagements

Purple team threat emulation

Black box critical infrastructure tests

29. Anti-Anti-Hacking

EDR behavioral bypass techniques

AI-powered anomaly detection evasion

Hardware-assisted debugging prevention

30. The Final Exam

72-hour CTF against corporate networks

Zero-day development under time pressure

Nation-state level attack simulation

Appendix: The Complete 100+ Topic Breakdown

[Full topic list as provided in syllabus]

Tool Encyclopedia (100+ Tools)

Recon - SpiderFoot, OSINT Framework, Maltego

Scanning - Naabu, RustScan, Masscan

Exploitation - Metasploit, PwnTools, ROPgadget

PrivEsc - PEASS-ng, GTFOBins, WinPEAS

C2 - Sliver, Havoc, Mythic

Cloud - Pacu, Cloudsplaining, ScoutSuite

Mobile - MobSF, Objection, Frida

Hardware - ChipWhisperer, JTAGulator, Bus Pirate

Forensics - Volatility 3, Rekall, LiME

AI - Adversarial Robustness Toolkit, Counterfit