Hacking Roadmap: Beginner to Advanced

1. Prerequisites (Foundational Knowledge)

✅ **Computer Networking** – Learn TCP/IP, HTTP/HTTPS, DNS, and VPNs.
✅ **Linux Basics** – Master CLI, bash scripting, and common commands.
✅ **Programming** – Python (automation), Bash (scripting), C (memory exploits).
✅ **Operating Systems** – Windows, Linux (Kali, ParrotOS), Mac security.
✅ **Cybersecurity Fundamentals** – OWASP Top 10, CIA triad, encryption, hashing.

2. Beginner Level (Ethical Hacking Basics)

- 🔹 **Essential Tools:** Nmap, Wireshark, Metasploit, Burp Suite.
- 🔹 **Footprinting & Reconnaissance:** OSINT, Google Dorking, WHOIS lookup.
- 🔹 **Scanning & Enumeration:** Network scanning, vulnerability scanning.
- 🔹 **Exploitation Basics:** Understanding exploits, gaining initial access.

3. Intermediate Level (Pentesting & Exploits)

🛠️ **Web Application Hacking** – SQL Injection, XSS, CSRF, IDOR.
🔓 **Wireless Hacking** – WPA2 cracking, MITM attacks, Evil Twin.
🎭 **Social Engineering** – Phishing, pretexting, impersonation.
🔑 **Privilege Escalation** – Linux & Windows priv-esc techniques.
💾 **Reverse Engineering & Malware Analysis** – Debuggers, disassemblers.

4. Advanced Level (Specialization & Real-World Testing)

🕵️ **Bug Bounty Hunting** – Hunting for zero-days, fuzzing, writing PoCs.
🔗 **Active Directory Exploitation** – Kerberoasting, Pass-the-Hash, Lateral Movement.
🌐 **Cloud Security** – AWS, Azure, GCP pentesting.
🔒 **Red Teaming & Blue Teaming** – Offense & defense strategies.

5. Certifications & Career Path

🎓 **Certifications:** CEH, OSCP, PNPT, CISSP, eJPT.
💼 **Career Options:** Penetration Tester, Security Analyst, Red Team, SOC Analyst.