🚀 Guide2Code - Cybersecurity Roadmap 🔐

🔰 Beginner Level - Cybersecurity Foundations

Required Programming Languages:

- **Python** 🐍
- **Bash** 💻
- **SQL** 💾

Required Skills:

- **Understanding Cybersecurity Basics** 🔐
- **Networking Fundamentals** 🌐
- **Operating Systems Security** 💻
- **Threats & Vulnerabilities** ⚠️
- **Basic Cryptography** 🔑

Learn the Fundamentals:

- **Cybersecurity Concepts**: Learn about confidentiality, integrity, availability (CIA), and how cybersecurity fits into organizations.
- **Networking Basics**: Understand the OSI model, IP addressing, DNS, HTTP, and TCP/IP protocols.
- **Operating System Security**: Learn the security mechanisms of Windows, Linux, and macOS (e.g., permissions, user accounts, firewalls).
- **Types of Cybersecurity Threats**: Understand malware, phishing, DoS/DDoS, ransomware, and social engineering attacks.
- **Cryptography Basics**: Learn encryption, hashing, and key management.

Beginner Projects 🚀:

1. **Setting Up a Firewall**: Set up a basic firewall to block unauthorized access to a local network.
2. **Create a Simple Encryption Program**: Implement basic encryption and decryption using Python's cryptography library.
3. **Network Packet Sniffing**: Use Wireshark or tcpdump to capture and analyze network packets.

4. **Secure a Web Application**: Identify and fix basic vulnerabilities like XSS (Cross-Site Scripting) or SQL Injection in a test web app.
5. **Build a Password Strength Checker**: Create a tool to check the strength of a password based on common patterns.

🔄 Intermediate Level - Expanding Cybersecurity Skills

Required Programming Languages:

- **Python (Advanced)** 🐍
- **Bash/Shell Scripting** 💻
- **PowerShell** 💻

Required Skills:

- **Penetration Testing** 🕵️
- **Security Auditing** 🔍
- **Incident Response & Management** ⚡
- **Network Security** 🌐
- **Security Policies & Compliance** 📜

Expanding Your Knowledge:

- **Penetration Testing**: Learn ethical hacking techniques, how to test systems for vulnerabilities, and how to exploit them safely.
- **Incident Response**: Understand how to detect, respond, and recover from security breaches, and how to analyze security incidents.
- **Network Security**: Study firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and VPNs.
- **Security Auditing**: Learn how to audit and assess the security of systems and networks.
- **Security Policies & Compliance**: Understand security frameworks like NIST, GDPR, HIPAA, and how to enforce policies.

Intermediate Projects 🔄:

1. **Penetration Testing on a Web App**: Use tools like Kali Linux, Burp Suite, or OWASP ZAP to perform ethical hacking on a vulnerable web app.

2. **Set Up an IDS/IPS**: Configure Snort or Suricata to monitor and prevent suspicious network activity.
3. **Incident Response Playbook**: Create an incident response plan for handling a security breach.
4. **Network Security Configuration**: Set up a VPN and configure a network firewall for a small organization.
5. **Security Audit of a System**: Perform a security audit on a server or application to identify potential vulnerabilities.

🔝 Advanced Level - Mastering Cybersecurity

Required Programming Languages:

- **Python (Advanced)** 🐍
- **C/C++** 💻
- **Assembly** 🔍 (Optional for reverse engineering)

Required Skills:

- **Advanced Penetration Testing** 🕵️
- **Malware Analysis & Reverse Engineering** 🧪
- **Advanced Cryptography** 🔑
- **Security Architecture & Design** 🏛️
- **Threat Intelligence & Forensics** 🕵️

Deep Dive Into Advanced Topics:

- **Advanced Penetration Testing**: Learn advanced exploitation techniques, reverse engineering, and how to bypass security mechanisms.
- **Malware Analysis**: Study techniques to analyze and dissect malware using tools like IDA Pro or Ghidra.
- **Advanced Cryptography**: Study more advanced cryptographic concepts such as elliptic curve cryptography, PKI, and digital signatures.
- **Security Architecture & Design**: Learn to design secure systems, networks, and infrastructures from the ground up.
- **Threat Intelligence**: Understand threat intelligence frameworks and how to use them to anticipate and counter cyber threats.

- **Digital Forensics**: Learn how to collect, analyze, and preserve evidence in cybersecurity investigations.

Advanced Projects 🌟:

1. **Advanced Penetration Testing**: Perform a thorough penetration test on a network, from reconnaissance to exploitation, using advanced tools and techniques.
2. **Malware Reverse Engineering**: Analyze malware in a controlled lab environment to understand its behavior and write signatures for detection.
3. **Build a Secure System Architecture**: Design a secure infrastructure for an organization with layered defenses and secure protocols.
4. **Forensics Analysis on a Compromised System**: Conduct a forensic investigation of a compromised system to identify attack vectors and gather evidence.
5. **Threat Intelligence Dashboard**: Build a dashboard to monitor and analyze real-time threat intelligence data using tools like STIX or TAXII.

Thank You for Visiting Guide2Code!

"Stay ahead of the attackers and secure the digital world!"