100 days cybersecurity plan.

Days 1-10: Introduction to Cybersecurity

1. Familiarize yourself with the basics of cybersecurity, including common threats, attack vectors, and security principles.
2. Understand the importance of cybersecurity in protecting systems, networks, and data.
3. Learn about various cybersecurity roles and career paths.

Days 11-20: Networking Fundamentals

1. Gain a solid understanding of networking concepts, including TCP/IP, OSI model, IP addressing, and subnetting.
2. Learn about network protocols, such as HTTP, DNS, and SMTP.
3. Explore network security fundamentals, including firewalls, VPNs, and intrusion detection systems.

Days 21-30: Operating System Security

1. Study the security features and vulnerabilities of popular operating systems (e.g., Windows, Linux, macOS).
2. Learn about user access controls, privilege escalation, and securing system configurations.
3. Understand the importance of patching and updating operating systems to mitigate vulnerabilities.

Days 31-40: Web Application Security

1. Familiarize yourself with common web application vulnerabilities, such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF).
2. Learn about secure coding practices, input validation, and web application firewalls (WAFs).

3. Explore tools like Burp Suite and OWASP ZAP for web application security testing.

Days 41-50: Cryptography

1. Understand the principles of cryptography and encryption algorithms.
2. Learn about symmetric and asymmetric encryption, digital signatures, and hashing algorithms.
3. Explore cryptographic protocols like SSL/TLS and their role in securing data in transit.

Days 51-60: Security Assessments and Penetration Testing

1. Study the methodologies and techniques used in security assessments and penetration testing.
2. Learn how to perform vulnerability scanning, reconnaissance, and exploitation of common vulnerabilities.

3. Familiarize yourself with tools like Nmap, Metasploit, and Wireshark for penetration testing.

4. Days 61-70: Incident Response and Forensics

1. Gain an understanding of incident response procedures and the incident handling lifecycle.
2. Learn about evidence collection, preservation, and analysis in digital forensics.
3. Explore tools like EnCase, Autopsy, or The Sleuth Kit for digital forensics investigations.

Days 71-80: Network Security

1. Dive deeper into network security concepts, including secure network design, segmentation, and defense-in-depth strategies.
2. Learn about network intrusion detection and prevention systems (IDS/IPS) and security information and event management (SIEM) solutions.

3. Understand wireless network security principles and secure Wi-Fi configurations.

Days 81-90: Cloud Security

1. Study the security considerations and best practices for cloud computing environments (e.g., AWS, Azure, GCP).
2. Learn about securing cloud instances, network configurations, and access controls.
3. Understand container security and the challenges of securing containerized applications.

Days 91-100: Capstone Project and Practical Applications

1. Apply your knowledge by working on a cybersecurity project, such as setting up a secure network, conducting a penetration test, or creating a security incident response plan.
2. Continuously practice and stay updated on emerging threats, security trends, and new technologies.
3. Engage in cybersecurity communities, participate in Capture the Flag (CTF) competitions, or pursue relevant certifications like CompTIA Security+ or Certified Ethical Hacker (CEH).

Remember to adapt the plan to your learning pace and interests. Actively engage in hands-on exercises, practice ethical hacking responsibly, and stay informed about the latest cybersecurity news. Developing strong cybersecurity skills takes time and dedication,

1.

- edX: Offers cybersecurity courses and programs from renowned universities and organizations.

- Cybrary: Provides free and paid cybersecurity training, covering a broad range of topics.

2. Cybersecurity Blogs and Websites:

- KrebsOnSecurity: Brian Krebs' blog covering cybersecurity news, investigations, and insights.
- Schneier on Security: Bruce Schneier's blog offering analysis and commentary on various security topics.
- OWASP: Open Web Application Security Project provides resources, tools, and guidelines for web application security.
- SANS Institute: Offers a wealth of free resources, including whitepapers, webcasts, and newsletters.