3 Months Roadmap to learn Cybersecurity (if you have a technical background)

Month 1: Foundations and Basics

Week 1: Introduction to Cybersecurity

- **Goal**: Understand basic cybersecurity concepts, the threat landscape, and the role of a cybersecurity professional.
- **Activities:**
- **Study**: Learn about the CIA Triad (Confidentiality, Integrity, Availability), types of threats (malware, phishing, etc.), and basic cybersecurity terminology.
- **Courses**: Enroll in an introductory cybersecurity course on platforms like Coursera or Udemy.
- **Reading**: Read a beginner's guide to cybersecurity (e.g., "Cybersecurity Essentials" by Charles Brooks).

Week 2: Networking Fundamentals

- **Goal**: Gain a solid understanding of networking, which is crucial for cybersecurity.
- **Activities**:
- **Study**: Learn about TCP/IP, DNS, DHCP, subnets, and routing.
- **Practical**: Set up a home lab to practice networking basics using tools like Cisco Packet Tracer.
- **Courses**: Take a networking fundamentals course (e.g., CompTIA Network+ on Udemy).

Week 3: Operating Systems Basics

- **Goal**: Understand the basics of operating systems, particularly Linux and Windows, as they are essential for cybersecurity tasks.
- **Activities**:
- **Study**: Learn about the Linux file system, basic commands, and Windows command line (CMD) and PowerShell.
- **Practical**: Install a Linux distribution (e.g., Ubuntu) in a virtual machine (VM) and practice using the command line.
- **Courses**: Follow a Linux and Windows fundamentals course on platforms like LinkedIn Learning.

Week 4: Basic Security Concepts and Tools

- **Goal**: Familiarize yourself with basic cybersecurity tools and concepts.
- **Activities**:
- **Study**: Learn about firewalls, antivirus software, VPNs, and encryption basics.
- **Practical**: Set up and configure a firewall, use basic encryption tools, and explore VPN setup.
- **Tools**: Get hands-on with tools like Wireshark (for network analysis) and simple encryption tools like OpenSSL.

Month 2: Intermediate Cybersecurity Skills

Week 5: Introduction to Ethical Hacking

- **Goal**: Start learning about ethical hacking and penetration testing.
- **Activities**:
- **Study**: Understand the principles of ethical hacking, legal aspects, and the penetration testing process.
- **Courses**: Begin an introductory ethical hacking course (e.g., “Intro to Ethical Hacking” on Udemy or EC-Council’s CEH course).
- **Practical**: Set up a lab environment using tools like VirtualBox and Kali Linux.

Week 6: Vulnerability Assessment and Basic Exploitation

- **Goal**: Learn how to identify and exploit basic vulnerabilities.
- **Activities**:
- **Study**: Learn about common vulnerabilities (e.g., SQL injection, XSS, buffer overflow).
- **Practical**: Use tools like Nmap for network scanning, and practice basic exploitation techniques on vulnerable machines (e.g., OWASP Juice Shop).
- **Courses**: Follow tutorials on specific tools like Nmap, Metasploit, and Burp Suite.

Week 7: Web Application Security

- **Goal**: Understand the basics of securing web applications.
- **Activities**:
- **Study**: Learn about the OWASP Top 10, the most common security risks to web applications.

- **Practical**: Use Burp Suite to test web application security; try SQL injection and XSS attacks in a controlled lab environment.
- **Courses**: Take a course or follow online tutorials on web application security (e.g., “Web Application Security for Beginners” on Udemy).

Week 8: Security Operations and Incident Response

- **Goal**: Get a basic understanding of security operations and incident response.
- **Activities**:
- **Study**: Learn about security monitoring, log analysis, and incident response processes.
- **Practical**: Set up a basic SIEM tool (e.g., Splunk Free) and practice analyzing logs for security incidents.
- **Tools**: Get familiar with log analysis tools and basic scripting for automation.

Month 3: Advanced Concepts and Practical Experience

Week 9: Advanced Ethical Hacking Techniques

- **Goal**: Dive deeper into more complex ethical hacking techniques.
- **Activities:**
- **Study**: Learn about advanced exploitation techniques, privilege escalation, and post-exploitation.

- **Practical**: Use tools like Metasploit for advanced penetration testing tasks, and explore CTF challenges on platforms like TryHackMe or Hack The Box.

- **Courses**: Continue with advanced ethical hacking tutorials.

Week 10: Cryptography and Network Security

- **Goal**: Understand cryptographic principles and enhance your network security skills.

- **Activities**:

- **Study**: Learn about encryption algorithms, hashing, and PKI. Study VPNs, IDS/IPS, and advanced firewall configurations.

- **Practical**: Implement basic encryption with OpenSSL, configure a VPN, and set up an IDS like Snort.

  - **Courses**: Take an intermediate course on cryptography and network security.

Week 11: Cybersecurity

Certifications Preparation

- **Goal**: Prepare for an entry-level certification to validate your skills.

- **Activities**:

  - **Study**: Review all material learned and focus on certification-specific content (e.g., CompTIA Security+ or CEH).

  - **Practice Exams**: Take practice exams to gauge your readiness.

  - **Resources**: Use official certification guides and study materials.

Week 12: Real-World Practice and Final Review

- **Goal**: Consolidate your knowledge and apply it to real-world scenarios.

- **Activities**:

  - **Practical**: Engage in Capture The Flag (CTF) challenges, contribute to open-source security projects, or participate in bug bounty programs.

  - **Review:** Revisit all topics covered, identify any weak areas, and reinforce your knowledge.

  - **Certification Exam**: If ready, schedule and take your certification exam.

Post-3 Months: Continuous Learning

- **Ongoing**: Cybersecurity is a field that requires continuous learning. Keep practicing, stay updated with the latest trends, and consider pursuing more advanced certifications as you progress.

Free courses to master Cybersecurity

1**. Cybrary - Introduction to IT & Cybersecurity**

[Cybrary - Introduction to IT & Cybersecurity](https://www.cybrary.it/course/introduction-to-it-and-cybersecurity/)

2. **Open Security Training - Introduction to x86 Architecture**

[Open Security Training - Intro to x86](http://opensecuritytraining.info/IntroX86.html)

3. **Coursera - IBM Cybersecurity Analyst Professional Certificate**

[Coursera - IBM Cybersecurity Analyst](https://www.coursera.org/professional-certificates/ibm-cybersecurity-analyst)

4. **Cisco Networking Academy - Introduction to Cybersecurity**

[Cisco Networking Academy - Introduction to Cybersecurity](https://www.netacad.com/courses/security/introduction-cybersecurity)

5. **Coursera - Google IT Support Professional Certificate**

[Coursera - Google IT Support](https://www.coursera.org/professional-certificates/google-it-support)

6. edX - Introduction to Cybersecurity

[edX - Introduction to Cybersecurity](https://www.edx.org/course/introduction-to-cybersecurity-2)

7. FutureLearn - Introduction to Cyber Security

[FutureLearn - Introduction to Cyber Security](https://www.futurelearn.com/courses/introduction-to-cyber-security)

8. Alison - Fundamentals of Cybersecurity

[Alison - Fundamentals of Cybersecurity](https://alison.com/course/fundamentals-of-cybersecurity)

9. **Udemy - Free Cybersecurity Courses**

[Udemy - Search for Free Cybersecurity Courses](https://www.udemy.com/)

10. Federal Virtual Training Environment (FedVTE)

[FedVTE - Cybersecurity Courses](https://fedvte.usalearning.gov/)