Detailed roadmap tailored to various cybersecurity domains commonly found in the industry, each of which can be pursued by a fresher and Entry Level candidates. Each roadmap includes:

- Overview

- Skills required

- Certifications to aim

- Tools to master

- Learning resources

- Job roles relevant to the domain

- Typical roadmap (with timeline)

1. Network Security

Overview

Network security involves protecting the integrity, confidentiality, and accessibility of computer networks and data using both hardware and software technologies.

Skills Required

- Understanding of network architecture
- Knowledge of firewalls, IDS/IPS
- Knowledge of protocols (TCP/IP, DNS, HTTP/S)
- Network monitoring tools

Certifications

- CompTIA Network+
- CompTIA Security+
- Cisco CCNA Security

- Certified Ethical Hacker (CEH)

Tools to Learn

- Wireshark (for packet analysis)
- Nmap (for port scanning)
- Snort (IDS/IPS)
- Cisco Firepower
- pf Sense

Learning Resources

- Cisco Networking Academy
- Pluralsight or Udemy courses
- TryHackMe’s Network Fundamentals path

Job Roles

- Network Security Engineer
- Firewall Administrator
- SOC Analyst

Roadmap (3–6 months)

Time	**Goal**
Month 1	Learn Networking Basics (TCP/IP, OSI model)
Month 2	Install and configure firewalls (e.g., pfSense)
Month 3	Practice Wireshark and Nmap
Month 4	Take CompTIA Network+/Security+
Month 5–6	Build a home lab project on network traffic analysis and firewall rule creation

2. Penetration Testing / Ethical Hacking

Overview

Penetration testing (or ethical hacking) simulates cyberattacks on systems to find vulnerabilities that hackers could exploit.

Skills Required

- Strong understanding of OS (Linux / Windows)
- Python/Bash scripting
- Knowledge of web & network apps
- Basic understanding of exploits and payloads

Certifications

- CEH (Certified Ethical Hacker)
- OSCP (Offensive Security Certified Professional)
- GPEN (GIAC Penetration Tester)
- eJPT (eLearnSecurity Junior PenTest)

Tools to Learn

- Kali Linux
- Metasploit
- Burp Suite
- Nmap
- SQL map
- Nessus

Learning Resources

- Hack The Box, TryHackMe, PentesterLab
- Books: Web Penetration Testing with Kali Linux, The Hacker Playbook
- Cybrary or TCM Security courses

Job Roles

- Penetration Tester
- Ethical Hacker
- Security Consultant

Roadmap (4–8 months)

Time	Goal
Month 1–2	Learn Linux and Python scripting
Month 3	Begin TryHackMe or Hack The Box easy labs
Month 4	Learn web app assessment (OWASP Top 10)
Month 5	Practice active recon, vulnerability scanning
Month 6	Attempt CEH or eJPT prep
Month 7–8	Complete 2–3 real lab write-ups (document them on GitHub)

3. SOC (Security Operations Center) Analyst

Overview

SOC Analysts monitor and analyze security incidents using various tools and respond to threats in real time.

Skills Required

- Log analysis
- Knowledge of SIEM tools
- Incident response

- Threat hunting basics

Certifications

- CompTIA Security+

- CEH

- GIAC GSEC

- CompTIA CySA+ (Cybersecurity Analyst)

Tools to Learn

- Splunk

- ELK Stack (Elasticsearch, Logstash, Kibana)

- Microsoft Sentinel/SIEM

- Osquery

- Wireshark

Learning Resources

- Cybrary SOC Analyst Learning Path

- Pluralsight – SOC Core Skills

- Free Splunk courses

Job Roles

- SOC Analyst Level 1/2

- Incident Responder

- Threat Hunter

Roadmap (3–6 months)

Time	Goal
Month 1	Learn basics of OS (Windows/Linux)
Month 2	Practice with Splunk or ELK Stack in labs
Month 3	Analyze logs using SIEM tools
Month 4	Learn basics of incident response
Month 5	Take CompTIA CySA+ certification
Month 6	Apply to entry-level SOC Analyst positions

4. Cloud Security

Overview

Cloud security protects data, applications, and infrastructure in cloud environments like AWS, Azure, or GCP.

Skills Required

- Understanding of cloud platforms (AWS/Azure/GCP)
- IAM Policies
- Data Encryption
- Compliance (GDPR, HIPAA)

Certifications

- AWS Certified Security – Specialty
- Microsoft Certified: Azure Security Engineer
- Google Professional Cloud Security Engineer
- CCSP (Certified Cloud Security Professional)

Tools to Learn

- AWS IAM, CloudTrail, GuardDuty
- Azure Security Center
- GCP IAM, VPC
- Cloud Custodian

Learning Resources

- A Cloud Guru, Coursera cloud security courses
- Hands-on Labs: Qwiklabs, AWS labs

Job Roles

- Cloud Security Engineer
- Cloud Security Architect
- Cloud Compliance Analyst

Roadmap (3–6 months)

Time	Goal
Month 1	Learn AWS basics
Month 2	Understand cloud security concepts
Month 3	Implement basic IAM policies and security groups
Month 4	Learn compliance (GDPR, HIPAA)
Month 5	Work with native cloud security tools
Month 6	Pursue AWS Certified Security Specialty or Azure equivalent

5. Digital Forensics & Incident Response (DFIR)

Overview

DFIR involves investigating and analyzing security breaches to understand the root cause and extent of compromise.

Skills Required

- Knowledge of investigation tools
- Understanding of logs and evidence collection
- Disk and memory analysis

Certifications

- GCFA (GIAC Certified Forensic Analyst)
- GCIH (GIAC Certified Incident Handler)
- CHFI (Computer Hacking Forensics Investigator)

Tools to Learn

- Autopsy
- Sleuth Kit
- Volatility (memory analysis)
- FTK Imager
- Wireshark

Learning Resources

- SANS DFIR courses
- Books: Digital Evidence and Computer Crime

Job Roles

- Forensics Investigator
- Incident Response Analyst
- Threat Hunter

Roadmap (4–8 months)

Time	Goal
Month 1–2	Learn basics of OS and filesystems
Month 3	Use tools like Autopsy and FTK Imager
Month 4	Understand network forensics with Wireshark
Month 5	Learn memory analysis with Volatility
Month 6–7	Take CHFI or GCFA certification prep
Month 8	Practice with real-world case write-ups

6. Application Security (AppSec)

Overview

AppSec involves securing applications via code reviews, security testing, and integrating security into the development lifecycle.

Skills Required

- Understanding of web apps
- Knowledge of OWASP Top 10
- Familiarity with DevOps/CI/CD

Certifications

- CSSLP (Certified Secure Software Lifecycle Professional)
- SSCP (Systems Security Certified Practitioner)

- Burp Suite Certified Practitioner

Tools to Learn

- Burp Suite
- OWASP ZAP
- SonarQube
- SAST/DAST tools

Learning Resources

- PortSwigger Web Security Academy
- OWASP Guides
- GitHub for secure coding practices

Job Roles

- Application Security Engineer
- Security Developer
- DevSecOps Engineer

Roadmap (3–6 months)

Time	Goal
Month 1	Understand web app basics (HTML, JS, etc.)
Month 2	Learn OWASP Top 10
Month 3	Practice with tools like Burp Suite and OWASP ZAP
Month 4	Perform basic code reviews and write secure code
Month 5	Understand integration into CI/CD pipelines
Month 6	Take Burp Suite certification or CSSLP

7. Governance, Risk & Compliance (GRC)

Overview

GRC ensures systems align with regulatory standards and manage cyber risks across the organization.

Skills Required

- Risk assessment
- ISO 27001/2, NIST
- Policy development
- Auditing

Certifications

- CISA (Certified Information Systems Auditor)
- CISM (Certified Information Security Manager)
- CRISC (Certified in Risk and Information Systems Control)

Tools to Learn

- RSA Archer
- LogicGate
- SAP GRC
- MS Excel (for risk analysis)

Learning Resources

- ISACA official guides
- LinkedIn Learning (CISA / CISM courses)
- NIST Frameworks

Job Roles

- Compliance Analyst
- Risk Manager
- Information Security Officer

Roadmap (3–6 months)

Time	Goal
Month 1–2	Learn frameworks like NIST, ISO 27001
Month 3	Understand risk assessment and business impact analysis
Month 4	Practice creating policies
Month 5	Work with GRC platforms
Month 6	Take CISA/CISM prep and apply to related jobs

Jaleel