CYBERSECURITY ANALYST ROADMAP

VAISHALI SHISHODIA

Beginner Level

1. Learn the Basics of Cybersecurity

Understanding Cybersecurity Fundamentals

- **CIA Triad:** Understanding **Confidentiality (C)** (data is accessible only to authorized individuals), **Integrity (I)** (ensuring data is accurate and unaltered), and **Availability (A)** (ensuring data is available when needed). These are the three core principles of cybersecurity.
- **Security Governance & Compliance:** Learn about major security policies and compliance frameworks such as **ISO 27001 (Information Security Management System), NIST (National Institute of Standards and Technology), GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability Act), and PCI-DSS (Payment Card Industry Data Security Standard).** These frameworks guide organizations in protecting sensitive data.
- **Types of Cyber Threats:** Study various attack methods such as **Malware (Viruses, Worms, Trojans, Ransomware), Phishing (Email, Smishing, Vishing), Social Engineering (Pretexting, Baiting), Denial-of-Service (DoS, DDoS), Man-in-the-Middle (MITM), SQL Injection, Cross-Site Scripting (XSS), and Zero-Day Vulnerabilities.**
- **Network Security Basics:** Understanding how **firewalls, intrusion detection and prevention systems (IDS/IPS), Virtual Private Networks (VPNs), Proxies, Secure Email Gateways, and Endpoint Detection and Response (EDR) solutions** protect networks from attacks.

2. Learn Basic Networking

- **Networking Models:** Learn the **OSI Model (7 layers - Physical, Data Link, Network, Transport, Session, Presentation, Application)** and **TCP/IP Model** (4 layers - Network Access, Internet, Transport, Application).
- **IP Addressing & Subnetting:** Learn about **IPv4 (e.g., 192.168.1.1) and IPv6 (e.g., 2001:db8::ff00:42:8329)**, subnet masks, and CIDR notation.
- **Ports & Protocols:** Study commonly used ports and protocols such as **TCP/UDP ports (HTTP - 80, HTTPS - 443, DNS - 53, SSH - 22, SMTP - 25, SNMP - 161, RDP - 3389).**
- **Packet Analysis with Wireshark:** Learn how to capture and analyze network traffic using **Wireshark** to identify suspicious activity, detect potential intrusions, and troubleshoot network issues.

3. Learn Operating Systems (Windows & Linux)

- **Windows:** Learn about **Windows Event Logs (Security, Application, System), User Account Management, Active Directory, Group Policies, Registry Editing, PowerShell Scripting.**
- **Linux:** Master basic Linux commands such as **ls, cd, chmod, sudo, grep, find, awk, sed**, user management, permissions, log files, and cron jobs.

- **Kali Linux & Security Tools:** Set up Kali Linux and explore penetration testing tools like **Nmap, Metasploit, John the Ripper, Nikto, Hydra, Burp Suite, SQLmap.**

4. Learn Common Cybersecurity Tools

- **Security Information and Event Management (SIEM):** Introduction to tools like **Splunk, ELK Stack (Elasticsearch, Logstash, Kibana), IBM QRadar, ArcSight** for real-time security monitoring.
- **Firewall Management:** Learn how to configure and analyze firewall rules using **pfSense, Palo Alto Networks, Cisco ASA.**
- **Endpoint Security Solutions:** Gain hands-on experience with **Microsoft Defender ATP, CrowdStrike Falcon, SentinelOne.**
- **Threat Intelligence & Malware Analysis:** Understand how to analyze suspicious files and domains using **VirusTotal, Any.Run, Hybrid Analysis, YARA Rules, MITRE ATT&CK Framework.**

5. Hands-on Practice

- **Set up a Home Lab:** Install **VirtualBox/VMware, Kali Linux, Windows Server, SIEM Tools** to simulate cybersecurity scenarios.
- **Network Traffic Analysis:** Use **Wireshark, TCPDump, Sysmon** to analyze network behavior and detect anomalies.
- **Capture The Flag (CTF) Challenges:** Platforms like **TryHackMe, HackTheBox, CyberDefenders** provide real-world cybersecurity challenges.

6. Certifications (Optional)

- **CompTIA Security+ (SY0-601)** - Beginner-friendly certification covering security fundamentals.
- **Microsoft SC-900 (Security, Compliance, and Identity Fundamentals)** - Cloud security basics.

<u>Free Beginner-Level Courses</u>

1. Introduction to Cybersecurity (Cisco Networking Academy)

- **Platform:** Cisco Networking Academy
- **Link:** Cisco NetAcad
- **Topics Covered:** Basics of cybersecurity, cyber threats, data protection, network security fundamentals.

2. Cybersecurity Fundamentals (SANS Cyber Aces)

- **Platform:** SANS
- **Link:** SANS Cyber Aces
- **Topics Covered:** Operating system security (Windows & Linux), networking fundamentals, and system administration basics.

3. Cybersecurity Essentials (ISC2)

- **Platform:** ISC2
- **Link:** ISC2 Course
- **Topics Covered:** Cybersecurity principles, network security, identity and access management.

4. CompTIA Security+ (Free Course on Cybrary)

- **Platform:** Cybrary
- **Link:** Cybrary Security+
- **Topics Covered:** Security threats, cryptography, risk management, identity and access management.

Intermediate Level

1. Dive Deeper into Cybersecurity Domains

Security Information and Event Management (SIEM)

- **Advanced Log Analysis:** Learn how to analyze logs from **Windows Event Viewer, Sysmon, Firewall Logs, IDS/IPS, VPN Logs, and Network Traffic Logs.**
- **SIEM Queries:** Master **Splunk SPL, ElasticSearch Query Language (EQL), and QRadar Query Language (AQL)** to create advanced alerts and dashboards.
- **Incident Detection and Threat Analysis:** Develop the ability to detect security incidents using correlation rules, anomaly detection, and custom-built dashboards.

Threat Intelligence & Incident Response

- **Cyber Kill Chain:** Understand how attackers move through different attack stages: **Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control (C2), Actions on Objectives.**
- **Threat Intelligence Platforms:** Work with **AlienVault OTX, MISP, Threat Intelligence Feeds (Recorded Future, Cisco Talos, IBM X-Force, FireEye).**
- **Incident Response Lifecycle:** Learn **Preparation, Detection & Analysis, Containment, Eradication, Recovery, and Post-Incident Review.**

Digital Forensics & Malware Analysis

- **Disk & Memory Forensics:** Learn about **disk imaging (Autopsy, FTK Imager), memory analysis (Volatility, Rekall), and forensic artifacts extraction.**

- **Static & Dynamic Malware Analysis:** Learn **PE file structure, debugging with OllyDbg, Ghidra, IDA Pro, and dynamic analysis in a sandbox environment.**

Learn Basic Penetration Testing

- **OWASP Top 10:** Master common web vulnerabilities such as **SQL Injection, XSS, CSRF, Insecure Direct Object References (IDOR), and Security Misconfigurations.**
- **Privilege Escalation:** Learn **Windows and Linux privilege escalation techniques.**

2. Hands-on Practice

- **Develop Playbooks for Incident Response.**
- **Simulate Cyber Attacks and Defend Against Them in a SOC Environment.**

3. Certifications (Optional)

- **Certified SOC Analyst (CSA).**
- **GIAC Security Essentials (GSEC).**
- **Microsoft SC-200 (Security Operations Analyst).**

Free Intermediate-Level Courses

1. Practical Ethical Hacking (TCM Security Academy)

- **Platform: TCM Security**
- **Link: TCM Security**
- **Topics Covered: Penetration testing, Linux basics, Active Directory attacks, web application hacking.**

2. Microsoft Cybersecurity Analyst Professional Certificate (Coursera)

- **Platform: Coursera (Free with financial aid)**
- **Link: Coursera Microsoft**
- **Topics Covered: Security operations, incident response, security frameworks, SOC operations.**

3. Cybersecurity Attack and Defense Fundamentals (IBM via edX)

- **Platform: edX**
- **Link: IBM Cybersecurity**
- **Topics Covered: Cybersecurity principles, malware, security operations, cryptography.**

4. Threat Intelligence and Incident Response (TryHackMe Free Labs)

- **Platform: TryHackMe**

- **Link: TryHackMe**
- **Topics Covered: Threat intelligence, incident handling, SIEM logs, cyber kill chain analysis.**

Advanced Level

1. Advanced Threat Detection & Threat Hunting

- **Learn about MITRE ATT&CK, TTPs, Threat Intelligence Platforms**
- **Hunt for Malicious Activity using SIEM (Splunk, Elastic, QRadar)**
- **Use Threat Intel Feeds (AlienVault OTX, MISP, Shodan, VirusTotal)**

2. Red Teaming & Advanced Penetration Testing

- **Exploit AD Environments (BloodHound, Mimikatz)**
- **Privilege Escalation (Windows & Linux)**
- **Hands-on with Cobalt Strike, Empire, Metasploit**

3. Cloud Security & DevSecOps

- **Learn Security in AWS, Azure, Google Cloud**
- **Cloud Security Tools (AWS GuardDuty, Microsoft Defender, Prisma)**
- **DevSecOps: CI/CD Security, Container Security (Docker, Kubernetes)**

4. Incident Response & Advanced Forensics

- **Build an Incident Response Playbook**
- **Simulate Phishing Attacks (GoPhish)**
- **Analyze Ransomware Attacks & Reverse Engineer Malware**

5. Hands-on Practice

- **Participate in Blue Team Labs (BTLO, CyberDefenders, RangeForce)**
- **Create & analyze custom YARA rules**
- **Build your own Threat Hunting Queries**

3. Certifications (Optional)

- **Certified Ethical Hacker (CEH).**
- **GIAC Certified Incident Handler (GCIH).**
- **Certified Threat Intelligence Analyst (CTIA).**

Free Advanced-Level Courses

1. Digital Forensics and Incident Response (DFIR Academy - Free Tier)

- **Platform: DFIR Academy**
- **Link: DFIR Academy**
- **Topics Covered: Digital forensics, disk imaging, malware analysis, memory forensics.**

2. Advanced Persistent Threat (APT) Analysis (MITRE ATT&CK)

- **Platform: MITRE ATT&CK**
- **Link: MITRE ATT&CK**
- **Topics Covered: Threat hunting, APT tracking, real-world cyberattack analysis.**

3. Google Cybersecurity Professional Certificate (Coursera - Financial Aid Available)

- **Platform: Coursera**
- **Link: Google Cybersecurity**
- **Topics Covered: Security operations, incident response, SIEM, risk management.**

Cybersecurity Analyst Learning Resources

Practice Platforms

- **TryHackMe**
- **Hack The Box**
- **Blue Team Labs Online (BTLO)**
- **CyberDefenders**

YouTube Channels

- **John Hammond**
- **NetworkChuck**
- **SimplyCyber**
- **Cyber Mentor**
- **David Bombal**
- **Professor Messer**

There are numerous free cybersecurity tools available for different purposes, including penetration testing, digital forensics, threat intelligence, SIEM, malware analysis, and network security. Below is a categorized list of the best free cybersecurity tools.

---

1. Network Security & Traffic Analysis

- **Wireshark**
  - Use: Packet analysis and network traffic monitoring.
  - Link: Wireshark
- **Nmap (Network Mapper)**
  - Use: Network discovery and vulnerability scanning.
  - Link: Nmap
- **Zeek (Formerly Bro)**
  - Use: Network intrusion detection system (NIDS).
  - Link: Zeek
- **Tcpdump**
  - Use: Command-line network traffic capture.
  - Link: Tcpdump

---

2. SIEM & Log Analysis

- **Splunk Free**
  - Use: Security Information and Event Management (SIEM) for log analysis.
  - Link: Splunk Free
- **ELK Stack (Elasticsearch, Logstash, Kibana)**
  - Use: Log management and threat detection.
  - Link: ELK Stack
- **Graylog**
  - Use: Log analysis and real-time threat monitoring.
  - Link: Graylog

---

3. Penetration Testing & Ethical Hacking

- **Kali Linux**

- **Use: Penetration testing with pre-installed tools like Metasploit, Nmap, and Burp Suite.**
- **Link: Kali Linux**

- **Metasploit Framework**
  - **Use: Exploit development and vulnerability testing.**
  - **Link: Metasploit**
- **Burp Suite Community Edition**
  - **Use: Web application security testing.**
  - **Link: Burp Suite**
- **Nikto**
  - **Use: Web vulnerability scanner.**
  - **Link: Nikto**
- **OWASP ZAP (Zed Attack Proxy)**
  - **Use: Web application security scanning.**
  - **Link: OWASP ZAP**

---

4. Threat Intelligence & Malware Analysis

- **VirusTotal**
  - **Use: Online malware scanning and file reputation analysis.**
  - **Link: VirusTotal**
- **Any.Run**
  - **Use: Interactive sandbox for malware analysis.**
  - **Link: Any.Run**
- **Hybrid Analysis**
  - **Use: Automated malware analysis.**
  - **Link: Hybrid Analysis**
- **MITRE ATT&CK**
  - **Use: Cyber threat intelligence framework.**
  - **Link: MITRE ATT&CK**

---

5. Digital Forensics & Incident Response (DFIR)

- **Autopsy**
  - **Use: Digital forensics and disk image analysis.**
  - **Link: Autopsy**
- **Volatility**
  - **Use: Memory forensics for incident response.**
  - **Link: Volatility**
- **FTK Imager**
  - **Use: Disk imaging and data recovery.**
  - **Link: FTK Imager**
- **REmux**
  - **Use: Reverse engineering and malware analysis.**
  - **Link: REmux**

---

6. Endpoint Security & Antivirus

- **OSSEC**
  - **Use: Host-based intrusion detection system (HIDS).**
  - **Link: OSSEC**
- **Snort**
  - **Use: Network intrusion detection system (NIDS).**
  - **Link: Snort**
- **ClamAV**
  - **Use: Open-source antivirus engine.**
  - **Link: ClamAV**
- **Cuckoo Sandbox**
  - **Use: Automated malware analysis in a virtualized environment.**
  - **Link: Cuckoo Sandbox**

Final Thoughts

Mastering cybersecurity requires continuous hands-on practice, certifications, and deep understanding of attack methodologies. Set goals, stay updated with emerging threats, and engage in real-world challenges to refine your skills.