CYBER SECURITY ROADMAP

120 concepts to become a cyber security analyst

8 areas, 15 concepts each. Every concept explained in one line, the order to study each area, and two practice questions to test yourself.

How to use it: one area at a time, tick each concept only when you can explain it out loud in under a minute, then answer the two practice questions without notes.

@chalkesahil · chalkesahil.ai

AREA 01 / 08

Networking

Study order: You can't protect a network you don't understand; start here.

01	**OSI model**	Seven layers and what happens at each.
02	**TCP/IP model**	The four layers the internet actually uses.
03	**IP addresses**	IPv4, IPv6 and private ranges.
04	**Subnetting**	Split networks with CIDR.
05	**TCP vs UDP**	Reliable vs fast.
06	**Three-way handshake**	How a TCP connection starts.
07	**Common ports**	22, 53, 80, 443, 3389 and what runs on them.
08	**DNS**	How names become IP addresses.
09	**DHCP**	How devices get an IP.
10	**HTTP and HTTPS**	Web traffic and its encrypted version.
11	**Routers and switches**	Moving packets between and within networks.
12	**NAT**	Many devices sharing one public IP.
13	**VPN**	Encrypted tunnel over the internet.
14	**Firewalls**	Allow or block traffic by rules.
15	**Wireshark**	Capture and read real packets.

Practice

1. What happens when you type a URL and press Enter?
2. Find the DNS queries in a Wireshark capture.

AREA 02 / 08

Linux

Study order: Most security tools run on Linux; live in the terminal.

01	**File system**	/etc, /var, /home and what's in them.
02	**Basic commands**	ls, cd, cp, mv, cat and grep.
03	**Permissions**	chmod, chown and what rwx means.
04	**Users and groups**	Who can do what.
05	**sudo**	Run as admin, and why it's dangerous.
06	**Processes**	ps, top and kill.
07	**Services**	systemctl to start and stop them.
08	**Logs**	/var/log and journalctl.
09	**Networking commands**	ip, ss, ping, curl and dig.
10	**Package managers**	apt and installing tools.
11	**SSH**	Secure remote login with keys.
12	**Bash scripting**	Automate repeated checks.
13	**Cron jobs**	Scheduled tasks, and how attackers abuse them.
14	**Kali Linux**	The distro packed with security tools.
15	**Hardening basics**	Disable what you don't need.

Practice

1. Find every file in /home that anyone can write to.
2. A server is slow. Which processes and connections do you check?

AREA 03 / 08

Security basics

Study order: Learn the vocabulary; every interview starts here.

01	**CIA triad**	Confidentiality, integrity and availability.
02	**Threats, vulnerabilities, risks**	What each word means.
03	**Authentication vs authorisation**	Who you are vs what you can do.
04	**MFA**	Something you know, have or are.
05	**Hashing**	One-way fingerprints of data.
06	**Encryption**	Symmetric vs asymmetric.
07	**Digital certificates**	How HTTPS proves a site is real.
08	**Malware types**	Virus, worm, trojan and ransomware.
09	**Phishing**	The most common way attacks start.
10	**Social engineering**	Tricking people instead of machines.
11	**Password attacks**	Brute force and credential stuffing.
12	**Least privilege**	Give only the access needed.
13	**Defence in depth**	Several layers of protection.
14	**Zero trust**	Verify every request, inside or outside.
15	**Incident response**	Prepare, detect, contain, recover.

Practice

1. Hashing vs encryption: what's the difference?
2. An employee clicked a phishing link. What do you do first?

AREA 04 / 08

Web security

Study order: Practise every attack on deliberately vulnerable labs, never real sites.

01	**How web apps work**	Browser, server, database.
02	**OWASP Top 10**	The most common web risks.
03	**SQL injection**	Untrusted input running as a query.
04	**Cross-site scripting**	Injected scripts in someone else's page.
05	**CSRF**	Tricking a logged-in user's browser.
06	**Broken access control**	Seeing data you shouldn't.
07	**IDOR**	Changing an ID in the URL to see others' data.
08	**Authentication flaws**	Weak login and session handling.
09	**Security headers**	CSP, HSTS and friends.
10	**Cookies and sessions**	httpOnly, secure and SameSite.
11	**File upload attacks**	Uploading a script instead of an image.
12	**SSRF**	Making the server fetch internal URLs.
13	**Burp Suite**	Intercept and modify web requests.
14	**DVWA and Juice Shop**	Safe practice apps.
15	**Bug bounty basics**	Report bugs legally for rewards.

Practice

1. Explain SQL injection and how to prevent it.
2. A URL has ?user_id=105. What would you test?

AREA 05 / 08

Ethical hacking tools

Study order: Only test machines you own or have written permission for.

01	**Pentest phases**	Recon, scanning, exploitation, reporting.
02	**Reconnaissance**	Gather public information first.
03	**Nmap**	Find open ports and services.
04	**Service enumeration**	Find versions and weak spots.
05	**Vulnerability scanning**	Nessus or OpenVAS.
06	**Metasploit**	A framework for known exploits.
07	**Password cracking**	John the Ripper and Hashcat.
08	**Privilege escalation**	Going from user to admin.
09	**Reverse shells**	How attackers get remote access.
10	**Wi-Fi security**	WPA2, WPA3 and why weak passwords fail.
11	**Directory brute forcing**	Find hidden pages with gobuster.
12	**Writing a report**	Findings, impact and fixes.
13	**CVEs**	How known vulnerabilities are tracked.
14	**Legal boundaries**	Permission and scope, always in writing.
15	**TryHackMe and Hack The Box**	Legal labs to practise on.

Practice

1. Scan a lab machine and list what's running on it.
2. What goes into a good pentest report?

AREA 06 / 08

SOC and SIEM

Study order: Most fresher jobs are SOC analyst roles; learn what they do all day.

01	**What a SOC is**	The team that watches for attacks.
02	**SOC tiers**	L1 triage, L2 investigation, L3 hunting.
03	**SIEM**	Collect and search logs from everywhere.
04	**Splunk basics**	Search logs with SPL.
05	**Microsoft Sentinel**	Cloud SIEM used widely.
06	**Windows event logs**	Login events like 4624 and 4625.
07	**Alerts and triage**	Real attack or false positive?
08	**IOCs**	IPs, hashes and domains linked to attacks.
09	**Threat intelligence**	Known bad actors and their tools.
10	**MITRE ATT&CK**	The map of attacker techniques.
11	**EDR**	Endpoint tools that watch every laptop.
12	**Email analysis**	Headers and links in suspicious mail.
13	**Malware analysis basics**	Check files safely in a sandbox.
14	**Playbooks**	Step-by-step response for each alert type.
15	**Shift handover**	Write notes the next analyst can act on.

Practice

1. You see 500 failed logins in 5 minutes. Walk through your triage.
2. How would you check if an email attachment is malicious?

AREA 07 / 08

Cloud security

Study order: Companies moved to the cloud, and so did the attacks.

01	**Shared responsibility**	What the cloud secures vs what you secure.
02	**IAM**	Users, roles and policies.
03	**Least privilege in cloud**	No admin access for everyone.
04	**MFA for cloud accounts**	Protect the root account first.
05	**Security groups**	Cloud firewalls.
06	**Public S3 buckets**	The classic data leak.
07	**Encryption at rest**	Disks and storage encrypted.
08	**Secrets management**	Keys out of code.
09	**Cloud logging**	CloudTrail and activity logs.
10	**Misconfiguration**	The top cause of cloud breaches.
11	**Container security**	Scan images before running them.
12	**Kubernetes security**	RBAC and network policies.
13	**CSPM tools**	Find risky settings automatically.
14	**Backups and recovery**	Recover from ransomware.
15	**Compliance basics**	ISO 27001 and what audits check.

Practice

1. An S3 bucket is public. What do you check and fix?
2. How would you secure a new cloud account on day one?

AREA 08 / 08

Certifications and labs

Study order: Hands-on lab work gets you hired more than certificates alone.

01	**CompTIA Security+**	The common starting certificate.
02	**Google Cybersecurity Certificate**	Beginner course with labs.
03	**CEH**	Ethical hacking certificate many Indian jobs list.
04	**eJPT**	Practical beginner pentesting exam.
05	**TryHackMe paths**	Guided rooms from zero.
06	**Hack The Box**	Harder machines once you're ready.
07	**CTFs**	Capture the flag competitions.
08	**Home lab**	Virtual machines to attack and defend.
09	**Write-ups**	Document every lab you solve.
10	**GitHub portfolio**	Scripts and notes recruiters can see.
11	**Python for security**	Automate scans and log checks.
12	**Resume for SOC roles**	Labs, tools and what you found.
13	**Interview questions**	Ports, attacks and incident response.
14	**Ethics**	Never test without permission.
15	**AI in security**	Attackers and defenders both use it now.

Practice

1. Explain one lab you solved from start to finish.
2. Why should we hire you for a SOC L1 role?