M-kavach 2

Bitdefender Mobile Security

Norton / Norton 360 Mobile Security — real-time protection, web protection

Malwarebytes Mobile — adware/malware remove

Google Play Protect

Password checker :

https://www.passwordmonster.com/?utm_source=chatgpt.com

Fake WhatsApp Chat Generator

https://www.fakewhats.com/generator

Reverse Image Search – Find the Fake Profile

https://images.google.com/

https://haveibeenpwned.com/

checkphish.ai

Cybersecurity Jobs in 2025: Roles, Categories, Salaries, and Skills

Entry-Level Roles

1. Information Security / Cybersecurity Analyst

What You Do: Monitors networks/systems for security threats, investigates security events, and escalates incidents.

Known For: First line of defense against cyber threats, handling alerts and incidents.

Skills/Certifications: Networking, OS basics (Windows/Linux), SIEM tools, Python scripting, CompTIA Security+, CEH.

Salary (India 2025): ₹4.5 – ₹7 LPA (freshers), ₹6 – ₹10 LPA (2–3 years).

2. SOC Analyst (Security Operations Centre)

What You Do: Monitors real-time security events, analyses alerts, and escalates incidents to higher tiers.

Known For: Real-time monitoring and alert response specialist.

Skills/Certifications: SIEM tools, intrusion detection, network protocols, incident triage.

Salary (India 2025): ₹4 – ₹6 LPA (Tier I), ₹6 – ₹10 LPA (Tier II).

3. Vulnerability Assessor / Junior Penetration Tester

What You Do: Performs vulnerability scans and assists in penetration testing activities.

Known For: Finds weaknesses in systems and applications.

Skills/Certifications: Nmap, BurpSuite, OpenVAS, ethical hacking basics, CEH/OSCP aspirant.

Salary (India 2025): ₹6 – ₹8 LPA.

Mid-Level / Specialist Roles

4. Penetration Tester / Ethical Hacker

What You Do: Conducts simulated attacks to identify vulnerabilities in networks and systems.

Known For: Legal hacker skilled in exploiting vulnerabilities.

Skills/Certifications: OSCP, CEH, OWASP Top 10, scripting, automation, AI-driven tools.

Salary (India 2025): ₹10 – ₹15 LPA; experts ₹20 – ₹35 LPA.

5. Cloud Security Engineer

What You Do: Secures cloud infrastructure, manages IAM, and prevents misconfigurations.

Known For: Cloud security expert for AWS, Azure, and GCP environments.

Skills/Certifications: AWS/Azure/GCP certifications, Terraform, container security, Zero Trust architecture.

Salary (India 2025): ₹12 – ₹20 LPA; senior ₹22 – ₹40 LPA.

6. Incident Response / Digital Forensics Specialist

What You Do: Handles breaches, investigates cyber incidents, collects evidence, and performs root cause analysis.

Known For: Cybercrime investigator and digital evidence analyst.

Skills/Certifications: GCFA, GCIH, EnCase, Velociraptor, malware analysis.

Salary (India 2025): ₹10 – ₹25 LPA.

Senior / Leadership Roles

7. Security Architect / Consultant

What You Do: Designs organisation-wide cybersecurity architecture and strategy.

Known For: Big-picture security planner and advisor.

Skills/Certifications: CISSP, CISM, threat modelling, governance, architecture frameworks.

Salary (India 2025): ₹18 – ₹35 LPA.

8. Incident Response Manager / SOC Manager

What You Do: Leads security teams, manages crises, and ensures coordinated responses.

Known For: Crisis manager and incident response leader.

Skills/Certifications: Leadership, crisis management, technical IR, communication.

Salary (India 2025): ₹25 – ₹40 LPA.

9. Cybersecurity Risk Manager / GRC Lead

What You Do: Oversees governance, risk, and compliance with global standards.

Known For: Ensures security policies align with business and regulations.

Skills/Certifications: CISA, CRISC, ISO 27001, auditing, risk analysis.

Salary (India 2025): ₹22 – ₹38 LPA.

10. Chief Information Security Officer (CISO)

What You Do: Leads enterprise security strategy and manages all cybersecurity teams and policies.

Known For: Top-level executive for company-wide security posture.

Skills/Certifications: Leadership, communication, governance, budget control, CISSP/CISM.

Salary (India 2025): ₹35 – ₹80 LPA+ (up to ₹1 Cr in large firms).

Focus Areas: AI Cybersecurity & Digital Forensics

AI cybersecurity specialists use machine learning to detect anomalies, automate threat hunting, and defend against AI-powered attacks.
Digital forensics specialists trace, analyze, and document cyber incidents for recovery and legal proceedings.

Tools by category (with short purpose + where commonly used)

1) Reconnaissance / OSINT

- **theHarvester** — passive email/host harvest. (red / TryHackMe & HTB)
- **whois / dig / nslookup** — domain + DNS info. (red)

- **Maltego** — visual OSINT mapping (red / labs & CTFs).
- **shodan** — search internet-facing devices (red/cloud).

2) Port-scanning & Service discovery

- **Nmap** — port & service scanning (basic must-know). (red / ALL)
- **masscan** — very fast port scanning (large ranges). (red)
- **RustScan** — faster wrapper for Nmap. (red)

3) Network sniffing / packet analysis

- **Wireshark** — GUI packet capture & analysis. (blue / TryHackMe & BlueTeamLabs)
- **tcpdump** — command-line packet capture. (blue / red)

4) Web application testing

- **Burp Suite (Community/Pro)** — intercept/proxy, intruder, repeater. (red / TryHackMe & HTB web rooms)
- **OWASP ZAP** — alternative to Burp (red/blue).
- **Nikto** — web server scanner. (red)
- **DirBuster / Gobuster** — directory/file brute force on web servers. (red)
- **SQLmap** — automated SQL injection exploitation. (red)

5) Exploitation frameworks & payloads

- **Metasploit** — exploit development and payloads. (red / HTB)
- **msfvenom** — generate payloads. (red)
- **Exploit-DB / searchsploit** — find public exploits. (red)

6) Reverse shell / network tools

- **netcat (nc)** — raw TCP/UDP connection, basic shells. (red/blue)
- **socat** — advanced network relay & tunneling. (red)

7) Password cracking & brute force

- **John the Ripper** — password hash cracking. (red/forensics)
- **Hashcat** — GPU-accelerated password cracking. (red)
- **Hydra / Medusa** — service password brute-force (SSH, FTP, HTTP). (red)

8) Enumeration & vulnerability scanning

- **OpenVAS / Greenbone** — vulnerability scanner (blue/red).
- **Nessus** — commercial vulnerability scanner (blue/red).
- **WPScan** — WordPress vulnerability scanner. (red)

9) Web shells / post-exploitation utilities

- **PowerShell Empire (or equivalents)** — post-exploitation (Windows). (red)
- **Meterpreter** (part of Metasploit) — interactive post-exploit shell. (red)

10) Linux & Windows post-exploitation / privilege escalation

- **LinPEAS / WinPEAS** — local privilege escalation enumeration. (red)
- **GTFOBins** — useful binary abuse techniques (reference). (red)

11) Forensics & incident response (BlueTeamLabs heavy)

- **Autopsy / Sleuth Kit** — disk forensics & file analysis. (blue / BlueTeamLabs)
- **Volatility / Volatility3** — memory forensics. (blue)
- **FTK Imager** — forensic imaging & basic analysis. (blue)
- **OSForensics** — forensic toolkit. (blue)

12) Malware analysis & reverse engineering

- **Ghidra** — disassembler/decompiler (free). (blue / advanced HTB boxes)
- **IDA Pro / Binary Ninja** — reverse engineering platforms (commercial). (blue)
- **x64dbg / Immunity Debugger** — Windows debugging. (blue)

13) Detection, SIEM & Blue Stack

- **Splunk (free)** — log aggregation/search (blue). (BlueTeamLabs)
- **ELK Stack (Elasticsearch, Logstash, Kibana)** — logs and dashboards. (blue)
- **Wazuh** — host-based detection/endpoint monitoring. (blue)
- **Suricata / Snort** — network IDS/IPS. (blue)

14) Endpoint / Windows tools & scripts

- **Sysinternals Suite** (ProcMon, Autoruns, PsExec) — Windows internals and forensics. (blue)
- **PowerShell** — scripting & automation on Windows. (blue / red for PS-based attacks)
- **PSExec** — remote command execution (used both legitimately & in red teams).

15) Cloud security & infra tools (Cloud labs)

- **AWS CLI / Azure CLI / gcloud** — cloud service interaction/attacks. (cloud)
- **Terraform / Ansible** — infra as code (used in cloud security labs). (cloud / blue)

- **ScoutSuite / Prowler** — cloud security posture assessment. (cloud)

16) Container / Kubernetes tools

- **kubectl** — manage Kubernetes clusters (cloud labs).
- **kube-hunter / Trivy** — scan K8s & containers for vulnerabilities. (cloud / blue)

17) Wireless / RF pentesting

- **Aircrack-ng** — Wi-Fi cracking & analysis. (red)
- **Kismet** — wireless detection. (red)

18) Development / scripting & helpers

- **Python** (requests, pwntools) — scripting & exploit development. (red/blue)
- **Bash / PowerShell** — shell scripting basics. (red/blue)
- **Git** — version control for your projects. (ALL)

19) CTF / binary exploitation helpers

- **pwntools** (python) — exploit dev. (red)
- **ROPgadget / ROPemporium tools** — ROP chain assistance. (red)

20) Misc / utilities

- **Docker** — build isolated labs and environments (used in many rooms). (ALL)
- **VirtualBox / VMware** — virtual machines for labs. (ALL)
- **Burp extensions (e.g., Collaborator, BAppStore plugins)** — enhance Burp. (red)

Which tools are most used on which platform?

- **TryHackMe**: Nmap, Gobuster, Burp Suite, Wireshark, netcat, Python, Metasploit (introductory and step-by-step rooms). Good for learning basics & labs.
- **HackTheBox**: Nmap, smbclient, smbmap, Metasploit, LinPEAS/WinPEAS, Burp, Ghidra for advanced boxes. (more challenge/realistic)
- **BlueTeamLabs / Blue Team Rooms**: Wireshark, Volatility, Autopsy, Splunk, ELK, Suricata, Wazuh — focus on detection, IR, forensics.
