****

**🔴 Red Team – Offensive Security**

**✅ Objective**

To simulate real-world cyberattacks and identify security vulnerabilities **before** malicious hackers can exploit them.

**🧠 Mindset**

"Think like an attacker." The Red Team behaves like real-world adversaries to test an organization’s detection and response capabilities.

**🔧 Common Responsibilities**

* Penetration testing (network, web, cloud, physical)
* Social engineering (e.g., phishing, tailgating)
* Exploit development
* Malware crafting and delivery
* Bypassing defenses (e.g., antivirus, firewalls, EDR)
* Reporting vulnerabilities with proof of concept

**🛠️ Tools Used**

* **Metasploit**
* **Nmap**
* **Burp Suite**
* **Cobalt Strike**
* **Impacket**
* **Empire / Sliver**
* Custom scripts (Python, Bash, PowerShell)

**🧑‍💻 Key Skills**

* Deep technical understanding (OS internals, networking, protocols)
* Coding/scripting (Python, C, PowerShell)
* Offensive tools and exploit frameworks
* Creative and adversarial thinking

**🔵 Blue Team – Defensive Security**

**✅ Objective**

To **detect, respond to, and mitigate** cyberattacks and improve security infrastructure.

**🧠 Mindset**

"Defend and detect." The Blue Team works to **build resilient systems** and identify threats **before or as they happen**.

**🔧 Common Responsibilities**

* Monitoring logs and network traffic
* Incident detection and response
* Threat hunting
* Digital forensics and root cause analysis
* Patch management and hardening systems
* Security policy development and enforcement

**🛠️ Tools Used**

* **SIEM** (e.g., Splunk, ELK, QRadar)
* **EDR** (e.g., CrowdStrike, SentinelOne)
* **Firewalls / IDS / IPS**
* **Forensic tools** (e.g., Autopsy, FTK)
* **Threat intelligence platforms**

**🧑‍💻 Key Skills**

* Incident response and investigation
* Log analysis and anomaly detection
* Networking protocols and system admin knowledge
* Scripting (e.g., Python, Bash, PowerShell)
* Familiarity with Windows, Linux, and cloud platforms

**Please find the Job roles for both teams in the next page-**

|  |  |  |  |
| --- | --- | --- | --- |
| **Job Title** | **Team** | **Coding Required** | **Technical Knowledge Required** |
| Penetration Tester (Ethical Hacker) | Red Team | Yes | Yes |
| Red Team Operator | Red Team | Yes | Yes |
| Exploit Developer | Red Team | Yes (Advanced) | Yes (Deep) |
| Social Engineering Specialist | Red Team | No | No/Some |
| Malware Analyst | Red Team | Yes | Yes |
| Reverse Engineer | Red Team | Yes (Advanced) | Yes (Deep) |
| Security Researcher | Red Team | Yes | Yes |
| Vulnerability Analyst | Red Team | Some | Yes |
| Incident Responder | Blue Team | Some | Yes |
| Security Operations Center (SOC) Analyst | Blue Team | No/Some | Yes |
| Threat Intelligence Analyst | Blue Team | No/Some | Some |
| Digital Forensics Analyst | Blue Team | No/Some | Yes |
| Security Engineer | Blue Team | Yes | Yes |
| Network Security Engineer | Blue Team | Yes | Yes |
| SIEM Engineer | Blue Team | Yes | Yes |
| Cloud Security Analyst | Blue Team | Yes | Yes |
| Governance, Risk & Compliance (GRC) Analyst | Blue Team | No | Some |
| Identity & Access Management (IAM) Specialist | Blue Team | Some | Yes |

**Non-Tech roles –**

Non-technical roles focus on the strategic, legal, procedural, and human elements of cybersecurity. These professionals do not write code or configure systems, but they work closely with technical teams to define security standards, manage risks, enforce compliance, and raise organizational awareness.

They play a crucial part in building a strong security culture, ensuring that organizations not only defend against threats but also meet legal, regulatory, and ethical obligations.

**Skills Needed for Non-Technical Roles**

* Understanding of cybersecurity frameworks (e.g., NIST, ISO 27001, CIS)
* Knowledge of laws and regulations (e.g., GDPR, HIPAA, SOX, PCI-DSS)
* Risk assessment methodologies
* Policy writing and compliance reporting
* Communication and stakeholder management

|  |  |  |  |
| --- | --- | --- | --- |
| **Job Title** | **Coding Required** | **Technical Knowledge Required** | **Primary Focus** |
| **Governance, Risk & Compliance (GRC) Analyst** | No | Some | Risk assessment, regulatory compliance |
| **Cybersecurity Policy Analyst** | No | Some | Writing, enforcing, and reviewing security policies |
| **Information Security Auditor** | No | Some | Auditing controls and systems (e.g. ISO 27001) |
| **Data Privacy Officer (DPO)** | No | No/Some | Ensuring data privacy (GDPR, CCPA) |
| **Cybersecurity Project Manager** | No | No/Some | Leading and coordinating cybersecurity projects |
| **Security Awareness Trainer** | No | No | Educating employees on secure behavior |
| **Cybersecurity Legal/Compliance Counsel** | No | No | Legal compliance, breach handling, contract risk |
| **Third-Party Risk Manager** | No | Some | Assessing vendors/supply chain security posture |
| **Business Continuity & Disaster Recovery Planner** | No | Some | Planning for outages, incident preparedness |
| **Compliance Program Manager** | No | Some | Developing enterprise-wide compliance programs |
| **Privacy Compliance Analyst** | No | Some | Mapping and managing personal data handling |

**Bonus –**

**⚔️ Purple Team (Collaboration)**

The **Purple Team** isn’t always a separate team—often, it's a **collaborative approach** where Red and Blue teams work together to:

* Improve detection of attack techniques
* Test and refine defensive capabilities
* Share knowledge and close visibility gaps