MANOJ

manoj.cybertrack@gmail.com | (+91) 9588229797

@manojcybertrack /Manoj -

TECHNICAL SKILLS

- Networking & Systems:
  Strong knowledge of computer networks, OSI & TCP/IP models, subnetting, routing concepts, VLANs, DHCP, DNS, and Windows Server administration.
- Security Tools:
  Nmap, Wireshark, Burp Suite, John the Ripper, Metasploit Framework, Metal, Postman API collections.
- Testing & Security:
  API testing, cryptography fundamentals, vulnerability assessment, penetration testing methodology, exploit development basics.
- Programming & Frameworks:
  Laravel (API design & backend fundamentals), basic scripting (Python/Bash).
- Cloud & Virtualization:
  Basic experience with deploying test environments on cloud platforms (AWS/Parrot/Kali).
- Operating Systems:
  Hands-on experience with Windows OS, Windows Server, Parrot OS, and Kali Linux.

PROJECT

- TryHackMe (Rooms)
  Offensive Security Intro, Defensive Security Intro, Careers in Cyber, What is Networking?, Pentesting Fundamentals, Search Skills, Linux Fundamentals Part 1, Network Security Essentials, Security Engineer Intro, DNS in Detail, Junior Security Analyst Intro, HTTP in Detail, Putting It All Together, Red Team Fundamentals.

EXPERIENCE

- Cybersecurity Trainee (Self-Practice)
  Completed 14 hands-on TryHackMe rooms covering offensive security, defensive security, SOC basics, networking, and Linux.
  Practiced reconnaissance and port scanning using Nmap; experimented with mobile device scanning for learning.
  Gained foundational skills in Linux file permissions, basic scripting, and command-line operations.
  Explored web vulnerabilities including SQL Injection and XSS.
  Familiar with tools like Nmap, Burp Suite basics, Gobuster, Hydra, and Linux utilities.

EDUCATION

- GSSS School — Class 12 (Humanities / Social Science)
  Pursuing higher secondary education with active self-learning in cybersecurity and technology.

ACHIEVEMENTS

- Learning Discipline:
  Maintained a consistent study routine, managing long 8–9 hour sessions as well as effective short-time learning phases.
- Real-world Observation:
  Identified a potential weak behavior resembling RCE/backdoor activity in a personal mobile network during practice sessions.