MANOJ

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

@manojcybertrack //Manoj -

SKILLS

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

PROJECT

- ❖ TryHackMe — Cybersecurity Hands-on Labs
  Completed multiple structured cybersecurity labs covering offensive, defensive, networking, and web security concepts. Gained practical experience in reconnaissance, enumeration, exploitation basics, Linux operations, and security analysis.
  - Key learning areas included:
    - Offensive Security and Pentesting Fundamentals
    - Defensive Security, SOC concepts, and network monitoring
    - Linux fundamentals, permissions, and command-line operations
    - Web security concepts including HTTP, DNS, and common vulnerabilities
    - Red Team fundamentals such as recon and initial access techniques

Demonstrated consistent progress through rooms such as Offensive Security Intro, Defensive Security Intro, Linux Fundamentals Part 1, Pentesting Fundamentals, DNS in Detail, Network Security Essentials, and others.

EXPERIENCE

- ❖ Cybersecurity Trainee (Self-Practice)
  Independently completed structured hands-on cybersecurity training through platforms like TryHackMe, focusing on offensive security, defensive security, SOC fundamentals, networking, and Linux operations.

- Performed reconnaissance and network scanning using Nmap in controlled test environments.
- Developed foundational skills in Linux permissions, file system navigation, shell operations, and basic scripting
- Explored entry-level web vulnerabilities such as SQL Injection and Cross-Site Scripting (XSS) in safe, lab setups.
- Performed enumeration, directory brute forcing (Gobuster), and traffic analysis using Wireshark.
- Built a solid foundation in vulnerability assessment and basic exploitation techniques.

EDUCATION

- GSSS School — Class 12 (Humanities / Social Science)

  Pursuing higher secondary education while actively building core skills in cybersecurity, networking, and technology through structured self-learning.

ACHIEVEMENTS

- Learning Discipline:

  Demonstrated strong learning consistency through structured study routines and continuous skill development in cybersecurity.

- Real-world Observation:

  Identified an unusual network behavior during a practice environment review, improving awareness of potential security anomalies.