🔥 **NOPALCYBER – CYBER SECURITY ANALYST**

ULTIMATE PREPARATION WORKSHEET / CHEAT SHEET (2025)

(Crisp, exam-ready, interview-ready, no extra theory)

🟦 SECTION 1 — APTITUDE TEST PREPARATION

1. Quantitative Aptitude (Must Practice)

- Number Systems
- Percentages & Profit/Loss
- Ratios & Proportions
- Time & Work
- Time, Speed, Distance
- Simple/Compound Interest
- Basic Probability
- Permutations & Combinations
- Data Interpretation (tables, graphs, charts)

2. Logical Reasoning

- Blood Relations
- Coding–Decoding
- Directions
- Seating Arrangements
- Puzzles
- Syllogisms
- Venn Diagrams
- Pattern recognition

3. English / Communication

- Reading comprehension
- Synonyms/Antonyms
- Basic grammar correction
- Email writing format
- Active–passive voice

🟩 SECTION 2 — CORE CYBERSECURITY TOPICS (MOST IMPORTANT)

🔐 1. Networking (MOST IMPORTANT for SOC/Pentesting)

- OSI layers (mnemonics + functions)
- TCP/IP model
- Common ports
    - 21, 22, 23, 25, 53, 80, 443, 3306, 8080
- TCP vs UDP
- IP addressing and subnets
- DHCP, DNS, NAT, ARP
- VPN concept
- Firewalls (stateless/stateful)

🖥️ 2. Operating Systems (Windows + Linux basics)

Linux:

- Basic commands:
  ls, cd, pwd, cat, grep, chmod, chown, ps, top, netstat, systemctl
- File permissions
- Processes & services
- Log file locations

Windows:

- Event Viewer
- Registry basics
- Services
- Task Manager
- CMD + PowerShell basics

🛡️ 3. Security Fundamentals

- CIA Triad
- Threat vs Vulnerability vs Risk
- Malware Types:
  Virus, Worm, Trojan, Ransomware, Spyware

- Social Engineering attacks
- DDoS basics
- Zero-day
- Patch management
- Encryption basics (AES, RSA)
- Hashing (SHA-256, MD5 differences)

🟧 SECTION 3 — DOMAIN-WISE PREPARATION FOR THEIR ROTATION

1️⃣ SOC (Security Operations Center)

Tools to know:

- SIEM (Splunk, QRadar, Sentinel)
- EDR/XDR basics

Concepts:

- What is a SIEM?
- What are logs? Types of logs (syslog, event logs, auth logs)
- Incident types:
    - Malware
    - Brute force
    - Privilege escalation
    - Unauthorized login
- Basic SOC process:

1. Monitor
2. Detect
3. Triage
4. Investigate
5. Escalate
6. Resolve

Important terms:

- IOC (Indicators of Compromise)
- IOA (Indicators of Attack)

- MITRE ATT&CK basics

2️⃣ Attack Surface Reduction (Pentesting + VA/PT)

Important topics:

- OWASP Top 10 (memorize 10 names!)
- SQL Injection basics
- XSS basics
- CSRF
- Directory traversal
- Password cracking concepts
- Vulnerability scanning tools (Nmap, Nessus)
- Common misconfigurations
- Weak passwords
- Unpatched software

Commands to revise:

- nmap -sV
- nmap -A
- nikto basics

3️⃣ Advisory (Audits + Compliance)

Important frameworks:

- ISO 27001 (Annex A controls basics)
- NIST CSF (Identify, Protect, Detect, Respond, Recover)
- GDPR basics (PII, user rights)
- Risk Assessment steps
- Policy examples:
    - Password policy
    - Access control policy
    - Incident response policy

4️⃣ Security Engineering (DE + SIEM + Automation)

Know these concepts well:

- Log sources (Windows, Linux, Cloud)
- Creating detection rules
- Alerts vs Correlation rules
- SIEM architecture
- SOAR basics
- Scripting:
    - Python basics
    - Bash basics
- YAML & JSON basics
- Cloud:
    - AWS IAM
    - VPC basics
    - S3 security basics

5️⃣ Product Development (AI/GenAI + Security Tools)

You should know:

- What is GenAI?
- LLM basics
- Prompt engineering basics
- What is automation in security?
- Python libraries for automation:
    - requests
    - pandas
    - re
    - json

Topics they may ask:

- How AI helps SOC
- How automation reduces alert fatigue

🟦 SECTION 4 — CASE-BASED INTERVIEW PREPARATION

Prepare short answers for scenarios:

1. If you see multiple failed login attempts… what will you do?

- Check source IP
- Verify user
- Look for successful login
- Block IP if malicious
- Escalate if brute force

2. If a website is vulnerable to SQL Injection?

- Confirm the finding
- Capture POC
- Rate severity
- Recommend parameterized queries

3. If ransomware is detected?

- Disconnect system
- Isolate network segment
- Identify spread
- Pull logs
- Escalate to IR team

4. If you find a critical vulnerability in client server?

- Report immediately
- Provide risk rating
- Suggest patching
- Validate after fix

🟩 SECTION 5 — PROGRAMMING TOPICS (Minimum Required)

Python

- Variables
- Lists, dicts
- Loops
- Reading log files
- Regex basics

- JSON handling

Bash

- grep
- awk
- sed
- chmod/chown
- cron jobs

SQL

- SELECT
- WHERE
- GROUP BY
- JOIN

🟪 SECTION 6 — HR + BEHAVIORAL QUESTIONS

Prepare answers for:

- Tell me about yourself.
- Why cybersecurity?
- Why NopalCyber?
- Your biggest challenge in cybersecurity learning.
- Example of teamwork.
- Example of solving a problem.
- Where do you see yourself after 2 years?

🟥 SECTION 7 — ONE-WEEK STUDY PLAN (VERY EFFECTIVE)

Day 1: Networking + Ports + OSI

Day 2: Linux + Windows + Logs

Day 3: SOC Concepts + SIEM

Day 4: Attack Surface + OWASP + Nmap

Day 5: Advisory + Frameworks + Policies

Day 6: Python + Bash + SQL

Day 7: Mock interview + Case studies + Resume reading