1. Computers & Workstations

You'll need systems that can run multiple virtual machines (VMs):

• High-performance PC / Desktop
  - CPU: 6–12 cores (Intel i7 / AMD Ryzen 7 or better)
  - RAM: 32 GB+ (64 GB recommended)
  - Storage: 1 TB SSD minimum
  - GPU: Optional (for GPU-based security/machine learning work)

Tip: Desktop systems are cheaper and allow easier upgrades compared with laptops.

2. Servers / Virtualization Hardware

For advanced labs and simulations:

• Rack/Blade server or mini server
  - Intel Xeon / AMD EPYC CPUs
  - 64 GB+ RAM
  - Multiple NICs (Network Interface Cards)

• Network Attached Storage (NAS)
  - For storing VM images, backups, datasets

3. Network Gear

Switches, routers, and firewalls allow you to create segmented labs:

• Managed Switch (Layer 2/3) with VLAN support
• Routers (Cisco / Juniper used in enterprise labs)
• Hardware Firewall / UTM
  - pfSense appliance / FortiGate / Cisco ASA
• Wireless Access Point
  - For Wi-Fi security experiments

4. Networking Accessories

• Ethernet cables (Cat 6 or higher)
• Patch panels
• Rack cabinet
• Power strips / UPS (Uninterruptible Power Supply)

5. Virtualization Platform

Most cyber labs run multiple VMs:

• VirtualBox (free)
• VMware Workstation / Fusion
• Proxmox / ESXi (for enterprise-style virtualization)
• Docker / Kubernetes for container-based workloads

6. Security Tool Stack (Software)

Install key tools for different domains:

Penetration Testing Tools:

• Kali Linux / Parrot OS / BlackArch
• Metasploit
• Burp Suite
• Nmap, Wireshark
• SQLmap, Hydra
• OWASP ZAP

Defensive & Monitoring Tools:
• ELK Stack (Elasticsearch, Logstash, Kibana)
• Splunk / Graylog
• Suricata, Snort IDS/IPS
• Security Onion

Cloud Security Tools:
• AWS / Azure / GCP free tiers
• Terraform / Ansible
• Cloud-based security tools

Forensics & Reverse Engineering Tools:
• Autopsy, Volatility
• Ghidra, IDA Free
• PEStudio, Radare2

7. Specialized Hardware (Optional but Useful)

• Raspberry Pi cluster – Network tools, honeypots, CTFs
• Hardware security devices:
  - USB fuzzer

- RFID/NFC readers
- IoT hardware for security testing

8. Learning & Practice Platforms

These aren't physical hardware but are essential:

• HackTheBox, TryHackMe
• VulnHub VMs
• CTF platforms (OverTheWire, picoCTF)
• OWASP Juice Shop

9. Simulation & Testing Tools

• Virtual network simulation: GNS3 / Cisco Packet Tracer
• Cuckoo Sandbox (malware analysis)
• WebGoat / DVWA (web security)

10. Documentation & Collaboration Tools

• Confluence / Notion / Obsidian – for lab notes
• Git / GitHub – version control
• Ticketing / issue tracking (Jira, Trello)

Budget Estimates (India)

Item	Approx Cost (INR)

High-end PC	70,000 – 1,50,000
Server grade hardware	1,00,000 – 4,00,000+
Managed switch	5,000 – 40,000
Firewall appliance	10,000 – 1,00,000+
UPS & accessories	8,000 – 30,000
Software licenses	Varies (some free, some paid)

Tip: You don't need all at once — start with a capable PC + virtualization + Kali Linux, and expand gradually.

How to Set Up Your Cyber Security Lab

1. Install a hypervisor (VMware/Proxmox/VirtualBox)
2. Create isolated network segments (VLANs)
3. Deploy VMs for attacker & defender roles:
   - Kali Linux (attacker)
   - Windows Server, Windows 10/11 (targets)
   - Linux servers (web app, DB)
4. Add security tools and monitoring
5. Practice real scenarios:
   - Vulnerability scanning
   - Exploit development
   - Traffic analysis
   - Incident response
6. Document everything — learning is in notes!