

Real-World Cybersecurity Skills Guide

What Are Real-World Skills in Cybersecurity?

Skill Area	What It Means	Example
Tools / Platforms		
-----	-----	-----

Hands-on Tool Use	Use real security tools in real situations	
Nmap, Wireshark, Burp Suite, Metasploit		
Problem Solving	Spot and fix security issues	
TryHackMe, HackTheBox labs		
System Setup & Attacks	Build lab and simulate attacks	
VirtualBox, Kali, vulnerable machines		
Log Analysis	Investigate attacks via logs/SIEM	
Splunk, ELK, QRadar		
Web/Network Pen Testing	Find real bugs and perform ethical hacking	
PortSwigger, Bugcrowd		
Cloud Security Skills	Secure cloud infrastructure	
AWS IAM, S3 Bucket Security, CloudTrail		
Coding for Security	Automate or analyze security tasks	
Python, Bash		
Reporting	Write professional reports	PDF,
Markdown		

How to Build These Skills (Daily / Weekly Plan)

1. Set Up Your Personal Hacking Lab (Free)

- **Tools: VirtualBox, Kali Linux, Metasploitable, DVWA, OWASP Juice Shop**

2. Practice Platforms

- **TryHackMe: Beginner to Pro hacking**
- **HackTheBox: Advanced red team labs**
- **PortSwigger Academy: Web app security**
- **Bugcrowd / HackerOne: Bug bounty programs**
- **Blue Team Labs Online: SOC/Blue Team skills**

3. Do Projects & Publish Them

- **Build a firewall using iptables (Linux)**
- **Port scanner in Python**
- **Fake phishing page (educational use)**
- **Malware analysis (strings, Ghidra)**
- **Secure AWS S3 bucket setup**

Pro Tips for Growth

- **Practice > Theory**
- **Search & solve problems on your own**
- **Join cybersecurity Discords and forums**
- **Watch real pros on YouTube (John Hammond, Cyber Mentor)**
- **Publish writeups/blogs on GitHub or Medium**

Summary:

Real-World Skills = Hands-on + Self-practice + Projects + Documentation