Ayesha Shoukat - Cybersecurity Portfolio

Summary

An enthusiastic and self-motivated cybersecurity learner with hands-on experience in digital forensics, malware analysis, and network investigation. Completed a wide range of challenges across CyberDefenders and TryHackMe, showcasing strong foundational knowledge in endpoint forensics, threat intelligence, and reverse engineering. Continuously learning and practicing to become job-ready in the cybersecurity field.

Tools & Skills

- **Forensics:** Volatility, Ree, FTK Imager
- **Network Analysis:** Wireshark, tcpdump, Tshark
- **Malware Analysis:** Ghidra, x64dbg, Scdbg, PE-bear, CyberChef
- **Threat Intelligence:** VirusTotal, Hybrid Analysis, Any.run, URLScan.io
- **Scripting/Other:** Burp Suite (file upload fuzzing), certutil, basic Linux commands
- **Platforms:** CyberDefenders, TryHackMe

Completed Challenges (CyberDefenders) *(continuing)*

Malware Analysis:

- Emprisa Maldoc
- RE101
- GetPDF
- FakeGPT
- BlueSky Ransomware
- XLMRat

Network Forensics:

- EscapeRoom
- PacketMaze
- HawkEye
- OpenWire
- Acoustic
- DanaBot
- PoisonedCredentials
- Web Investigation
- Tomcat Takeover
- PsExec Hunt
- WebStrike

Threat Intelligence:

- PhishStrike
- Intel101
- GrabThePhisher
- 3CX Supply Chain
- IcedID
- Tusk Infostealer
- Red Stealer
- Lespion
- Yellow RAT
- Oski

Endpoint Forensics:

- Reveal
- Silent Breach
- BlackEnergy
- Insider
- The Crime

TryHackMe Rooms Completed *(continuing)*

- Cyber Kill Chain
- Putting It All Together
- Windows Fundamentals (1, 2, 3)
- Introductory Networking
- Passive Reconnaissance
- Web Application Security
- Intro to Digital Forensics
- SQL Injection
- Security Principles
- Common Attacks
- Unified Kill Chain
- Pentesting Fundamentals
- Networking Concepts
- Careers in Cyber
- Intro to Cyber Threat Intel
- Threat Intelligence Tools
- Phishing Analysis Fundamentals
- Phishing Emails in Action
- Red Team Threat Intel
- Traffic Analysis Essentials
- Snort

Research Focus & Labs (Ongoing)

- Shellcode debugging using Scdbg & Speakeasy
- Linux Memory Forensics with Volatility 2.6.1
- PDF Malware & CVE Exploit Analysis (CVE-2010-0188, CVE-2008-2992)
- Web exploitation (File Upload Bypass + PHP Reverse Shell)
- Reverse engineering using Ghidra + x64dbg

Soft Skills

- Analytical Thinking & Problem Solving
- Detail-Oriented Forensic Investigation
- Persistent & Eager to Learn
- Self-paced Learner with Consistency

Future Goals

- Continue hands-on learning and become confident in SOC analysis, malware reversing, and digital forensics
- Build public write-ups and GitHub projects to share research
- Get a junior role or internship in cybersecurity in the next 3–6 months

---

Contact

Name: Ayesha Shoukat

Role: Aspiring Cybersecurity Analyst\ **Location:** Pakistan (Remote-friendly)\ **LinkedIn/GitHub:** https://github.com/123-321-cpu/Ayesha-cybersecurity-portfolio