Security Intern

Location: Bangalore, India

Company: CyberWarFare Labs

About Us:

CyberWarFare Labs is an Ed-Tech Cyber Security Focused Platform which is totally engrossed in solving the problem of Cybersecurity by providing real-time hands-on manner solutions to problems of B2C & B2B Audience.

Job Overview:

We are looking for a Red Team Intern with exposure to either or all reverse engineering,cloud security and active directory. The role involves working on low-level system analysis, identifying vulnerabilities, and supporting security assessments in cloud environments.

Qualifications and Requirements:

- Pursuing/Graduated with B.S/B.E/B.Tech/BCA/M.Tech/MCA in Computer Science or related field
- Strong understanding of C / C++
- Basic to good knowledge of Assembly Language
- Understanding of CPU architecture, registers, and memory concepts
- Basic understanding of at least one cloud platform (AWS / Azure / GCP)
- Knowledge of IAM, compute, storage, and networking basics
- Familiarity with Windows APIs
- Basic scripting knowledge (Python / Bash / PowerShell – any one)
- Familiarity with CLI tools (AWS CLI / Azure CLI / GCP CLI – any one)
- Understanding of cloud security risks, misconfigurations, and basic privilege escalation concepts
- Strong problem-solving skills and interest in offensive security
- Basic understanding of Active Directory architecture
- Knowledge of AD components
- Familiarity with authentication protocols
- Understanding of common AD attacks

Tools Exposure (Good to Have):

- Reverse Engineering: Ghidra, IDA, x32dbg / x64dbg
- Cloud Security: CloudEnum / ScoutSuite / Prowler
- Azure tools (MicroBurst / AADInternals – optional)
- Active Directory tools: BloodHound / SharpHound / Rubeus / Mimikatz

Note: Candidates are not expected to know all tools; familiarity with any one is sufficient.

Role and Responsibilities:

- Perform basic reverse engineering and binary analysis
- Assist in identifying vulnerabilities in applications and cloud environments
- Run cloud security tools and analyze outputs
- Work with low-level system components and debugging tools
- Support red team simulations across application and cloud layers
- Write basic scripts for automation and testing
- Document findings, observations, and learning outcomes
- Assist in Active Directory enumeration and security assessments
- Identify misconfigurations, weak permissions, and privilege escalation paths in AD
- Support simulation of AD attack techniques (e.g., Kerberoasting, Pass-the-Hash)
- Analyze AD logs and monitor authentication-related activities

Stipend Offered - 15k per month (10% TDS is cut which can be claimed while filing ITR) 13.5k in hand will be received

Job Location - 3rd Floor, Cyberwarfare Labs. HustleHub H1907,240, 19th Main Rd, 4th Sector,HSR Layout, Bengaluru, Karnataka 560102

Internship time period - 3 months

After 3 months, Full time position will be offered based on performance