

## 职业目标

---

致力于在网络安全领域，发挥红队技能，通过模拟攻击提升组织的安全防御能力。

## 专业技能

---

- **渗透测试:** 网络扫描、漏洞利用、后渗透操作
- **社会工程学:** 钓鱼攻击、社交媒体工程
- **工具:** Metasploit, Burp Suite, Nmap, Empire, Cobalt Strike
- **开发技能:** Python, Bash, PowerShell

## 专业认证

---

- OSCP (Offensive Security Certified Professional)
- CEH (Certified Ethical Hacker)
- CRTO (Certified Red Team Operator)

## 工作经验

---

### 红队工程师 | Acme Security Solutions | 2018 年 6 月 - 2023 年 8 月

- 领导团队成功模拟针对金融行业的 APT 攻击，提高了客户的入侵检测率达 30%。
- 设计并执行社交工程学攻击演练，成功获取目标组织 80% 的员工凭证。

### 渗透测试工程师 | Global Cyber Security | 2016 年 7 月 - 2018 年 5 月

- 通过渗透测试发现 15 个严重漏洞，帮助企业减少 80% 的潜在风险。
- 进行网络扫描和漏洞利用，使用 Metasploit、Burp Suite 等工具识别和利用多个零日漏洞。

## 项目经验

---

### 全球零售企业渗透测试项目 | 2022 年 3 月 - 2022 年 5 月

- 使用 Nmap 和 Nessus 对企业网络进行全面扫描，识别开放端口和服务。
- 成功执行横向移动，获取了目标企业 70% 的关键服务器访问权限。

## 教育背景

---

某某大学 | 信息安全，理学学士 | 2016 年 6 月毕业

- 相关课程：网络安全概论、渗透测试与漏洞分析、加密技术

## 开源项目与社区参与 (可选)

---

### 开源贡献

- 贡献代码至 Metasploit Framework，开发了多个漏洞利用模块。

### 社区参与

- 参与 CTF 竞赛，获得全球排名前 10%。