


Trabajando en Seguridad Ofensiva





```
$>whoami
```

- Aníbal Irrera
 - Security Researcher y Pentester en Immunity Inc. by Appgate
 - Auditoría de código de alto nivel y web hacking
 - Trainings en Ekoparty y en Infiltrate
 - @airrera
- 

Agenda

- Motivo de la charla
- ¿Qué es la seguridad ofensiva?
- ¿Qué no es seguridad ofensiva?
- Primeros pasos para iniciar
- Preguntas



Motivo de la charla

- Idea general sobre la seguridad ofensiva
- ¿Como es el trabajo en ese ámbito?
- Conocimientos y requerimientos
- **Aclaración: No voy a hablar de cosas técnicas**



Seguridad Ofensiva

- Ethical Hacker
 - Test de Penetración o Pentest
 - Interno
 - Externo
 - White box
 - Auditoría de código
 - Black box
 - Grey box
 - Análisis de vulnerabilidades
 - Detección
 - Explotación
 - Post-Explotación
 - Análisis - Determinación de riesgo asociado



Seguridad Ofensiva

- Reporte
 - Sección Ejecutiva
 - Sección Técnica
 - Explicación de la vulnerabilidad
 - Severidad
 - Impacto
 - Demostración
 - Remediación

El reporte no debería ser “copiar y pegar” el output de una tool



¿Seguridad Ofensiva?

- Threat Intelligence
- Vulnerability Management
- Vulnerability Scans
- Malware Analysis
- Red Team



¿ Que necesito saber ?

- Requerimientos básicos
 - Base de un carrera de sistemas (Ideal, no estrictamente necesario)
 - Desarrollo / Programación en al menos un lenguaje
 - Estructura de computadoras
 - Redes
 - Linux
 - Base de datos



¿ Que necesito saber ?

- Requerimientos adicionales
 - Capacitaciones
 - Diplomaturas (UTN)
 - Cursos (Hackademy)
 - Trainings en conferencias (Ekoparty, BH, Recon, etc)
 - Trainings online
 - HackTheBox
 - TryHackMe
 - Web Security Academy de Portswigger
 - Certificaciones (bueno tenerlas pero no estrictamente necesarias)
 - OSCP
 - OSWE



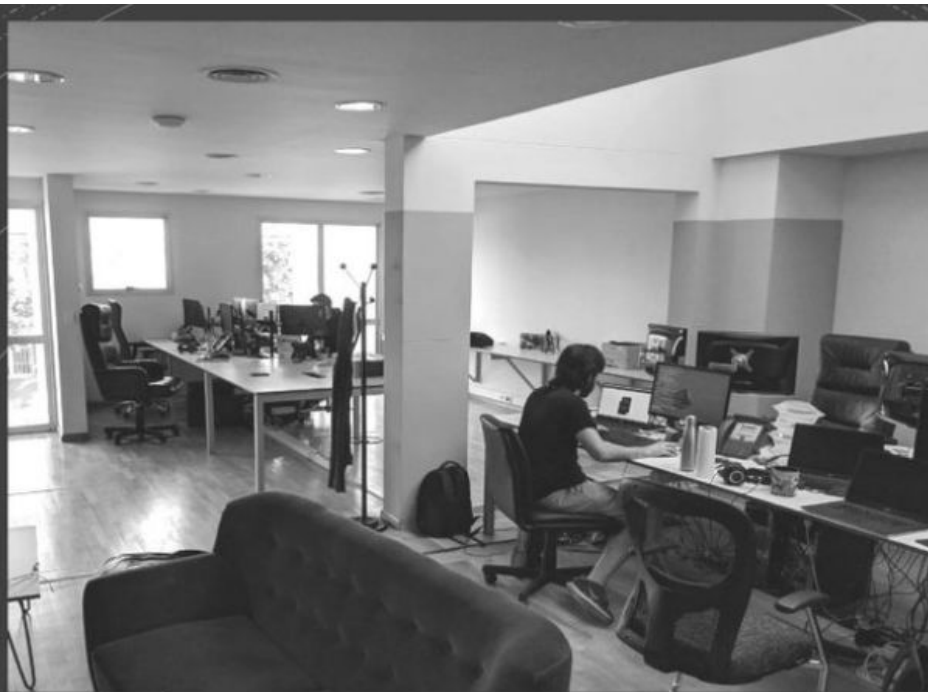
¿ Que necesito saber ?

- Requisitos adicionales
 - Participar en CTFs
 - CTFs más “reales”
 - <https://ctftime.org/ctfs>
 - <https://ctf.hacker101.com/>
 - Trabajo en equipo
 - Proactivo y autodidacta
 - Investigar, leer y probar
 - Seguir en redes a referentes y empresas de seguridad
 - Manejar la frustración
 - Bajar expectativas, ser realista
 - Aumentar mi conocimiento - Armar Knowledge base



¿Preguntas?





We're hiring Mid-Level/Senior Security Researcher



Must-Have

- Prior infosec experience (offensive side)
- Experience performing penetration tests (web, cloud, mobile, desktop, network, etc.)
- Scripting experience (to assist in testing your attack theories)
- Passionate about security and willingness to learn new things
- Teamworking and knowledge sharing
- Desire to work on a wide-variety of assessments in a wide-variety of industries.
- English proficiency

Nice to Have:

- Experience auditing source code
- Research skills (showing creativity to solve problems and find new methods)
- Exploit development experience (we are known for delivering working exploits during assessments)
- Being a specialist on a specific security subject (proven by talks, CVEs, tools, trainings, etc.)

If interested, please send your cv to
the following address:

hr.latam@appgate.com

appgate