Job Title: Offensive Security Pentest Engineer

Job Description:
Facebook's Security team is looking for an Offensive Security Pentest Engineer that can deliver technical expertise for our offensive security Penetration Testing team and execute tactical, offensive assessments across our environments. This individual should have extensive experience across the attack lifecycle and a demonstrated capacity to lead, design, and execute a penetration test against various technologies and stacks. Candidates are expected to scope, prepare and deliver technology-oriented assessments that positively benefit the overall security posture of the organization. This role requires a desire to help drive fixes after testing cycles, both as short term mitigations and long term improvements.

- Conduct penetration tests focused on both the unique systems and technologies used at Facebook, as well as approved third party software and vendors
- Help in the building of tooling to automate portions of pentests, scoping or other offensive security work, and use this model to inform and drive our assessments, as well as assist other teams with Facebook security efforts
- Design, scope, and lead deep technical assessments on internal and external facing systems
- Perform research to identify new ways of achieving your mission
- Work with vulnerability management, production security and other security programs to align remediation efforts and best protect the company from known threats
- Experience performing internal and external assessments
- Experience in leading a team during penetration tests
- Knowledge of server (Linux, Windows) and client (Windows, OS X, Linux) operating systems
- Knowledge and understanding of attack surfaces for enterprise systems and services
- Experience in at least one of PHP/Hack, Python, C/C++, Go or Java
- Experience working in cross-functional programs
- Experience translating technical concepts into language that is understood to audiences including software engineers, business and technical leaders
- 5+ years of experience practicing application security assessments and penetration tests
- Experience performing and leading whitebox and blackbox style assessments
- Experience with complex, multi-stage, multi-person pentests for new internal customers or external vendors
- Networking knowledge, including network virtualization technologies and ideally IPv6

Terms:

- Penetration Test (Pentest)

  A penetration test is an authorized test that is designed to check a security level of a computer system by simulating quite a few cyberattacks.

- Security Analyst

  A security analyst's main job is to monitor and to analyze private data for security to make a decision to protect the data, for example by changing its software system if needed.

- Security Administrator

  A security administrator's main job is to understand the whole security system for administering, installing, and troubleshooting problems of a company's cyber security system.

- Security Specialist

  A security specialist's main job is to defend a company's information assets in the cyber security system.

- Security Engineer

  A security engineer's main job is to monitor and to protect data or a security system from cybercrime.

- IT Help Desk Technician

  An IT help desk technician's main job is to provide any technical support for troubleshooting computer issues.

- Network Administrator

  A network administrator's main job is to manage and to maintain a company's computer technological network up to date.

- SOC Analyst

  A security operations center (SOC) analyst is similar to the security analyst, its main job is to detect and report a cyberattack and to try changes to protect data from the attacks.

- Incident Response Analyst

  An incident response analyst's main job is to monitor and to analyze a company's security systems to detect intrusions.

- Quality Assurance Specialist

  A quality assurance specialist's main job is to check if the quality system implements well or not by monitoring the system processes.