NEUROSOFT S.A.

Penetration Tester (Cyber Security)

REF_PT_02.19

Neurosoft S.A., is a leading software, networking and information security provider in financial, telecommunication, transportation, gaming and government sectors, providing solutions and services aiming to increase operating efficiency and security. Listed in the Italian Stock Exchange since 2009, currently employees 200+ highly skilled professionals with in depth expertise in their field.

We have an open vacancy for a Penetration Tester to join our Cyber Security Services team. The candidate will conduct security testing in terms of technical assessments on web and mobile applications, servers, networks, hardware, advance social engineering and physical facilities to provide high quality of security services to our clients.

Roles' Responsibilities

- Conducts internal and external penetration testing and vulnerability assessments
- Conducts advanced social engineering and phishing attacks
- Supports Red team engagements for specialized scenarios and organizations
- Explains, presents, demonstrates and documents, as needed, the operational impact of any vulnerability
- Develops exploits and tools for assessments or attacks
- Deploys testing methodologies and collects data
- Reports on findings to stakeholders and makes suggestions for security improvements
- Enhances existing methodology material
- Assists customer with implementing policies and tactics, techniques and procedures for conducting assessments
- Analyzes, disassembles and reverse engineers code to discern weaknesses for exploitation

Professional Experience & Qualifications

- Bachelor's/Master's degree in Information Technology, Information Security or any other relevant field
- At least 3 years of penetration testing experience of systems, web-based applications and networks
- Solid knowledge and experience of using a variety of penetration testing or threat modelling tools
- Excellent understanding of web technologies and services, networking, operating systems, server services/applications, wireless technologies and hardware
- In depth understanding of security technologies such as firewalls, IDS/IPS, application gateways/filters, anti-virus, encryption, security information and event management (SIEM), mobile security, asset discovery, identity authentication management and access control
- Strong understanding of security community best practices and methodologies such as OWASP and OSSTMM
- High ability to understand complex issues quickly, to apply knowledge to effectively analyze business/IT risks and controls and clearly report findings
- Strong analytical skills, critical thinking and attention to detail
- Good communication skills and a customer-orientation approach
- Ability to work efficiently both independently and within a team
- Fluency in Greek and English languages with excellent ability in technical and business writing

Preferred Skills and Qualifications

- Industry Certifications (e.g. OSCP, OSCE, etc.)
- Writing code with scripting languages such as Python, Ruby, Perl and shells
- Experienced with mobile penetration testing applications
- Ability to perform secure code review, reverse engineering and exploit writing

We Offer

A competitive compensation package, a stable and enjoyable working environment, excellent opportunities for professional development and advancement, working on leading-edge technology and industry trends and … A lot of hacking!