IVAN GLINKIN
mail@ivanglinkin.com | www.ivanglinkin.com | www.linkedin.com/in/ivanglinkin

CYBER SECURITY ANALYST

SUMMARY

8+ years combined operational work experience in penetration tests of enterprise networks and web application, physical social engineering and privilege escalation.

As a member of the Enterprise Security and Risk Team, I conduct enterprise wide security risk assessments by infiltrating its systems and breach its physical perimeters. This highlights gaps in the organization's technical security that require fixing as well as being involved in executing the security awareness plan.

Knowledge of **Bash Scripting, PHP, SQL, Python** and **C-based program languages** allows me to create my own applications for automation and optimization company's security.

Passed both the CEH knowledge-based MCQ and the CEH Practical exam on 92,8% and 90% respectively allowed me to become the **TOP 10** in the World **Global Ethical Hacking LeaderBoard**!

I am the **offensive security** and my goal does not end at gaining full access – that is only a starting point.

PROFESSIONAL EXPERIENCE

DataMe (AGGA Empire)
Information Security Manager, June 2017 – till present

- Cooperation with key account clients like Deloitte, Unilever, Valio, Miro, Heinemann, IFF Frutarom
- Develop tools to aid penetration test automation and effectiveness such as Fast-Google-Dork-Scan, CA "Hydra", Host- and Port Enumeration
- Perform internal and external pentest, web application testing (OWASP Top 10), and full-scope red teams
- Create threat models that result in more secure application design
- Write comprehensive and accurate reports, test plan documents, and mitigation recommendations

JSC Transneft
Lead Information Security Analyst, December 2014 – July 2017
Senior Information Security Analyst, July 2013 – December 2014

- Coached and managed a team of company's security up to 12 people

- Tested the company's information systems for penetration using BackTrack and Kali Linux applications like NMap, WFuzz, John the Ripper, SQLMap, Metasploit, Burpsuite, Wireshark, etc.
- Recognized and safely utilized attacker tools, tactics, and procedures
- Developed and implemented policies and procedures throughout the life cycle of the automatic leak detection system which prevented of unauthorized user's actions
- Developed information systems and databases for automation and optimization company's security officers
- Develop policies, procedures and contingency plans to minimize the effects of security breaches from client's staff and criminals

Investigative Committee of Russia
Investigator, August 2009 – July 2013

- Monitored and investigated suspicions situations and unusual activities in state's information systems
- Managed a team of three detectives to investigate information technology criminal cases
- Prepared cases for trial, attended court and testified as a witness
- Carried out crime prevention work with the citizens

EDUCATION

- **The Russian Presidential Academy of National Economy and Public Administration**
  ECE and WES approved as Master's degree | IT Management for Business
  2015 – 2018
- **Military University of the Ministry of Defense**
  ECE and WES approved as Master's degree | Jurisprudence
  2004 – 2009

CERTIFICATION

- Offensive Security Certified Professional (OSCP), 2021
- Certified Ethical Hacker (Master), 2020-2023
- Certified Ethical Hacker (Practical), 2020-2023
- Certified Network Defense Architect (CNDA), 2020-2023
- Certified Ethical Hacker (CEH), 2020-2023
- Certified Network Defender (CND), 2020-2023

PUBLICATIONS

- **Data leaks without hacking** - Hakin9 (IT Security Magazine), 02.2021
  https://hakin9.org/data-leaks-without-hacking/
- **Fast Google Dork Scan** – KitPloit (PenTest Tools for your Security Arsenal), 06.2020
  https://www.kitploit.com/2020/06/fast-google-dorks-scan-fast-google.html