



Reverse Engineering Intro Practical Course

Version: 2020-11-11

1. Training Program

The “Reverse Engineering Intro Practical Course” training allows participants to gain a wide set of knowledge to maintain secure IT infrastructure. You will have all the required skills to face the most difficult problems, which include:

- vulnerability exploitation;
- malware analysis;
- performance troubleshooting and optimization;
- understanding of how software and hardware works “under the hood”.

This is practical training. You immediately will be able to work. The training is developed for the audience with different backgrounds.

Duration: 5 days.

COURSE AGENDA

1. Fundamentals of computer architecture
2. Intel IA-32 CPU architecture (x86)
3. x64
4. ARM
5. The stack
6. The heaps
7. Exceptions
8. Windows APIs
9. Windows Internals
10. Win32 executable formats and image sections (PE)
11. ELF file format
12. Mach-O file format
13. Linux internals
14. Bytecode (Java)
15. Java Virtual Machine fundamentals



16. Managed code (.NET)
17. .NET runtime fundamentals
18. JavaScript and DOM fundamentals
19. How debugging works
20. Binary code structures
21. Frames and functions calling conventions
22. Variables
23. Pointers
24. Strings
25. Arrays
26. Conditional statements
27. Loops
28. Unpacking
29. Obfuscation
30. Anti-debugging
31. Monitoring registry changes
32. Monitoring filesystem changes
33. Monitoring network activity
34. Mutli-threaded programs
35. Virtual machines and bytecode
36. Compilers optimization
37. Identifying the Win32 API
38. Process hijacking
39. Encodings and Compression
40. Patching
41. Analysis of Malicious Document Files
42. Android reversing
43. .NET reversing

The training will include group work and practice tests.

2. Why us?

We are an international provider of information security services. Highest qualification, flexibility, and reliability are our main distinctions:



Experience in information security. Since 2001, our employees have gained rich information security experience in the State sector, industry, pharmacy, telecom, retail, banking, IT outsourcing, etc. Late in 2015, we initiated the H-X project.



International security certifications. The specialists of H-X earned and keep up-to-date internationally recognized security certifications (CISSP, CISA, ISO 27001, OSCP, CEH, CLPTP, etc.). These certifications cannot be obtained without confirmed years of experience and grueling exams passed. The certifications prove high professionalism and do not allow illegal or unethical behavior, otherwise, they are immediately revoked.



Absolute legitimacy and confidentiality. The employees of H-X technologies strictly adhere to laws, regulations, corporate Code of Ethics, and Penetration Testing Code of Ethics. We are ethical, white-hat hackers. Our legal support takes into account not only our and your rights and interests but also the legitimate rights and interests of third parties. Our specialists sign your commitment forms personally, just like your employees.



Highest customization and flexibility. We provide professional cybersecurity service for any budget. We provide even [free security assessment services](#). Our [Express Pentest](#) service is deeper than just vulnerability scanning but cheaper than pentests. We study every customer's needs carefully to prepare for the project. Unlike other companies, our pre-engagement documentation includes a comprehensive set of detailed penetration testing parameters. Our approach allows the customer to understand more accurately what they pay for. During many projects, we have developed and continually improve our security assessment and implementation methodologies. This is our know-how and our distinction from competitors.



Highest quality. H-X uses modern comprehensive security assessment tools. Besides automatic vulnerability scanning, we do manual work. We do not claim that automatic vulnerability scanning is a pentest like others do. H-X not only finds vulnerabilities and not just shows how exactly hackers can exploit them, but also helps customers eliminate the vulnerabilities and reduce risks. In every project, we develop suggestions for continuous improvement and are tracking changes in the security of our customers over the years.



3. Overview of Services and Competences



Security Assessment

- Security audit of the organization
- Vulnerability scanning
- Penetration testing
- Red Team
- Source code security audit
- Industrial IT audit
- Audit of smart contracts



Managed compliance

- ISO 27001 implementation
- PCI DSS, GDPR implementation
- VDA, TISAX implementation
- Remote security manager
- Training for programmers
- Training for pentesters
- Risk management



IT security and development

- Website protection
- Application security
- Software development
- Development of smart contracts
- Industrial IT security
- Incident response
- Forensic investigations

We have a wide, deep, and unique experience and competence in IT and corporate security. Both in GRC (Governance, Risk management, and Compliance), and in technical security. Both in Defensive Security and Offensive Security:

- **Security Assessment:** IT audits, information security audits, a security review of source code, audit of smart contracts.
- **Managed compliance** with GDPR, ISO 27001, PCI DSS, HIPAA, ITIL, ISF, NIST, COBIT, etc.
- **Application Security** and Software Engineering: Secure Software Development Lifecycle (SDLC) management and Security DevOps of specific software products.
- **Training and workshops** on Secure Software Development (SDLC, Secure DevOps). Personnel Security Awareness and Behavior Management. People-Centric Security.
- **Security Operations Center (SOC)** Implementation and SOC as a Service, including technical vulnerability management, security event monitoring, security incident response, and investigations, etc.
- **Enterprise Risk Management** and IT-related Risk Management.
- **Business Continuity Management** and Disaster Recovery Planning.
- Physical security and other security areas.



4. Our Customers



BI Group (Kazakhstan). The largest investment and construction holding company in Kazakhstan. 8000 workers. Annual turnover of \$1.4 billion. World TOP 200 construction companies. <https://bi.group>.



Intecracy Group (Ukraine, Kazakhstan, Azerbaijan, Georgia, USA, and Western Europe). The information technology group includes 12 companies from 8 countries. Founded in 2007. <https://intecracy.com>.



Ameria (Germany and Ukraine). This publicly-traded company is a global leader in the digitization of sales floors. They create interactive advertising solutions that are unique in the global market. Their clients are LEGO, Microsoft, Telefónica. <https://ameria.de>.



FluentPro (USA and Ukraine). The company develops software solutions for Work Management and also Enterprise Portfolio/Project Management. Over 1000 customers are using their software — the majority are multinational enterprises, many are from Fortune 500. <https://fluentpro.com>.



Cantemo (Sweden). The company develops innovative Media Asset Management solutions. <https://www.cantemo.com>.



HealthJoy (USA and Ukraine). The company develops software for the USA healthcare industry to simplify the healthcare experience in a way that provides access to better care at a lower cost. <http://healthjoy.com>.



5. Customer Feedbacks

"We are very pleased that we have had the opportunity to work with such a team of professionals as H-X Technologies. We have only positive impressions. Working with the H-X team was pleasant and interesting. Everything was done according to the conditions specified in the statement of works and exactly on schedule. Both the security assessment process itself and the provided reporting showed a high level of professionalism. We don't regret that we decided to cooperate with H-X Technologies. We look forward to further cooperation."

Sergey Krivich, Head of Information Security, BI Group

Alтынay Lebakina, Head of Information and Analytical Department, BI Group

"The H-X team has conducted a detailed project planning to assess the security of our infrastructure. They have shown a creative approach, and have properly implemented the security assessment plan. The security assessment has provided valuable information on priorities of security enhancements for our company, including strategic objectives and tactical activities."

Dmytro Dniprovskyi, Information Security Manager, Intecracy Group

"We were facing serious challenges related to our customers' requirements for formal compliance with international and industry information security standards. The H-X team very quickly helped to evaluate and fill the current organizational and technical gaps, and they continue to help."

Artem Savotin, Managing Director, Ameria

"The H-X team has completed a technical security assessment of one of our products, and we've been surprised by the high quality of the results. H-X specialists have provided detailed consultation on secure software development. They've helped to improve the quality of our development and testing processes."

Viktoriia Pogrebniak, IT Manager, FluentPro

6. Conclusion

Our distinction is building real tangible security, not only security for formal compliance. At the same time, we have considerable experience in GRC (Governance, Risk management, and Compliance) services, as well as in the implementation and maintenance of security management systems.

We help you to harden your security, protect your assets from cybercrime, and get official recognition of your new security status.

Moreover, we train your personnel on how to develop secure software and how to test its security.

Learn more about us and our services at <https://h-xtech.com>.



Please ask your questions, try our free automated security assessment services, order an Express Penetration Test or get a quote for a Full-scale Penetration Test at h-xtech.com/services, or call us at +380958860891