Haxoris

GET HACKED BY US!

SERVICE PORTFOLIO

PROFESSIONAL ETHICAL HACKING SERVICES

01 PENETRATION TESTING

- Web
- Mobile
- API
- Infrastructure
- AI/ML Security

02 RED TEAMING

- Real Attack Simulations
- Physical Breach
- Phishing, Vishing and more
- Open-Source Intelligence
- Cybersecurity Training

03 CLOUD SECURITY

- Cloud Security Assessment
- Cloud Infrastructure Audits
- Cloud Configuration Audits

04 PHISHING

- Phishing, Smishing, Vishing
- Spear Phishing
- Open-Source Intelligence

05 VULNERABILITY ASSESSMENT

- Automated Vulnerability Scanning
- Manual Security Audits
- Risk Assessment Reports

06 EMPLOYEE TRAININGS

- Phishing Awareness Workshops
- Security Best Practices

APPLICATION PENETRATION TESTING

WEB APPLICATION

We assess your web applications for vulnerabilities that could lead to data breaches, unauthorized access, or service disruption. Our testing simulates real-world attacks, including OWASP Top 10 risks, to ensure your application is secure against evolving threats.

API

APIs often act as the backbone of modern applications. We test your APIs for flaws in authentication, authorization, data exposure, and injection vulnerabilities, ensuring secure data exchange and robust access control mechanisms.

MOBILE APP

From insecure data storage to improper platform usage, mobile apps introduce unique attack surfaces. We conduct in-depth testing on Android and iOS applications, examining both the client-side code and backend communication for potential weaknesses.

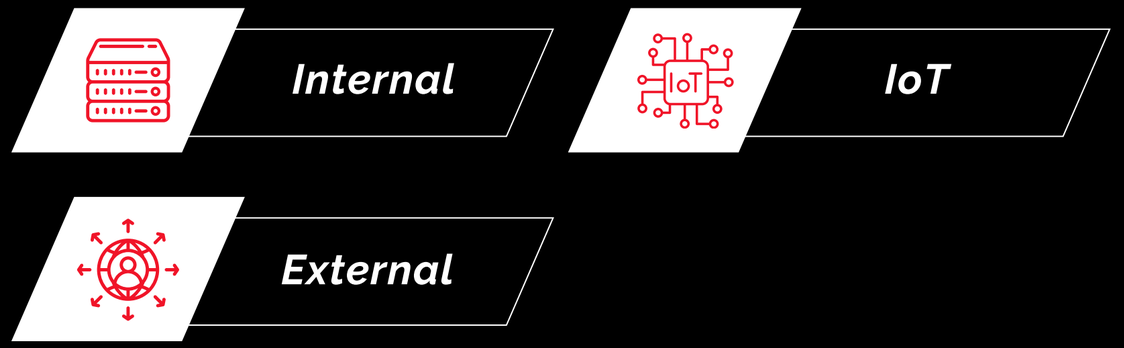
DESKTOP

Desktop applications, whether native or cross-platform, can hold critical business logic and sensitive data. We evaluate your desktop software for binary-level vulnerabilities, insecure storage, weak encryption, and privilege escalation risks.

INFRASTRUCTURE PENETRATION TESTING

INTERNAL

We simulate an attacker who has gained a foothold inside your network—whether through a rogue employee, compromised device, or social engineering. This test identifies weaknesses in internal systems, misconfigurations, privilege escalation paths, and lateral movement opportunities.



EXTERNAL

We evaluate your internet-facing assets, such as web servers, firewalls, email gateways, and cloud services, for vulnerabilities that can be exploited from the outside. This testing replicates real-world attack scenarios and helps ensure your perimeter is fortified against unauthorized access.

IOT

IoT devices often introduce security gaps due to limited protection mechanisms. We assess firmware, communication protocols, APIs, and cloud integrations to uncover flaws that could lead to device compromise, data leakage, or control manipulation.

RED TEAMING

1 Reconnaissance

We begin by gathering intelligence on your organization, infrastructure, employees, and supply chain to simulate realistic adversary behavior. This phase lays the groundwork for identifying potential attack paths and high-value targets.

2 Initial Access

Using tactics like phishing, physical intrusion, or exploiting exposed systems, we attempt to gain a foothold in your environment. Once inside, we establish persistence while remaining undetected—mimicking real-world attacker techniques.

3 Privilege Escalation

After establishing access, we escalate privileges, bypass controls, and move laterally across the network. This step aims to demonstrate how deep an attacker could go without being noticed by existing defenses.

4 Reporting

We pursue defined objectives (e.g., data exfiltration, domain takeover) while documenting every action taken. Finally, we deliver a detailed report including timelines, TTPs, detection gaps, and actionable recommendations to harden your defenses.

CLOUD SECURITY

GOOGLE CLOUD PLATFORM (GCP)

We assess your GCP environment for misconfigurations, overly permissive IAM roles, unsecured storage buckets, and exposed services. Our testing ensures compliance with best practices and reduces your cloud attack surface.

MICROSOFT AZURE

Our Azure security assessments focus on identity protection, network configuration, and secure deployment of services. We evaluate risks across Azure AD, resource groups, and hybrid integrations to help you secure every layer.

AMAZON WEB SERVICES (AWS)

We analyze your AWS infrastructure for security gaps including public S3 buckets, IAM privilege escalation, exposed Lambda functions, and misconfigured security groups. Our approach combines automated scans with manual review for accuracy and depth.

PHISHING

We simulate real-world phishing attacks to assess how your employees respond to social engineering threats. By crafting realistic emails, landing pages, and lures, we uncover vulnerabilities in user behavior and awareness, helping you strengthen your human firewall.

Targeted phishing emails are delivered to selected users.

Email Sending

We track which recipients open the phishing email.

Email Opened

We monitor if users enter credentials or sensitive info.

Data Submitted

You receive statistics and user reaction description.

Reporting

VULNERABILITY ASSESMENT

IDENTIFY. PRIORITIZE. SECURE.

Our vulnerability assessments utilize automated tools to identify common issues, but we take it a step further by incorporating manual checks performed by our experienced ethical hackers. This combined approach ensures a thorough and accurate assessment of your systems, identifying both high-risk and nuanced vulnerabilities that automated tools alone might miss.

05

EMPLOYEE TRAININGS

EMPOWER YOUR FIRST LINE OF DEFENSE.

We deliver interactive cybersecurity training sessions that raise awareness of phishing, social engineering, and best security practices. Tailored for both technical and non-technical staff to reduce human risk.

06

PCI DSS – PENETRATION TESTING REQUIREMENTS

11.4.2
Requirement

Internal penetration testing

11.4.3
Requirement

External penetration testing

11.4.5
Requirement

Segmentation testing

PCI DSS COMPLIANT

Other requirements

6.4
Penetration testing of public-facing web applications and APIs

11.2
Wireless security and detection of rogue access points

11.3
Internal and external vulnerability scans

Pentests must take place at least annually and after relevant changes.
Segmentation tests must happen twice a year.

OUR PROJECT TIMELINE

NDA | PRICE | CONTRACT | HACKING | REPORTING

NDA Signing
We establish confidentiality and mutual trust to ensure full discretion and protection of sensitive information.

Price Proposal
We present a tailored service package with clear deliverables, timeline, and pricing—aligned with your business goals.

Contract Signing
We finalize scope, timelines, and legal terms to officially launch the engagement.

HACKING
We execute controlled attacks to uncover vulnerabilities before real adversaries do.

Report Delivery
We deliver a detailed breakdown of vulnerabilities, proof-of-concept exploits, and clear remediation steps.

TIMELINE

OUR EXPERIENCED TEAM

Ing. Andrej Šebeň

Ing. Marek Mlynček

Ing. Lukáš Václavík

Ing. Adam Žilla

Marek Kerekes

CISSP Certified

OFFENSIVE SECURITY OSCP

OFFENSIVE SECURITY OSWE

EC-Council C|EH CERTIFIED ETHICAL HACKING

ADVANCED INFRASTRUCTURE HACKING — NotSoSecure Training

aws certified Security SPECIALTY

aws certified Solutions Architect ASSOCIATE

eMAPT

INTERMEDIATE HACKING AND SECURING CLOUD INFRASTRUCTURE — NotSoSecure Training

CompTIA Security+

CompTIA PenTest+

Haxoris

GET HACKED BY US!

OUR REFERENCES

Ultima Payments

> The decision to collaborate with Haxoris for the penetration testing of our web application was an excellent choice. Thanks to their professional approach, thorough testing, and outstanding communication, we were able to identify and eliminate multiple vulnerabilities. Their detailed final report provided us with a clear overview of our application's security status and specific recommendations for its protection. I can wholeheartedly recommend Haxoris to any company – their services are of a high professional standard, and the results exceeded our expectations.

Amerge

> The team has approached penetration testing professionally and impartially, while keeping an open line with our DevOps, frontend and backend developers to ensure proper isolation of production environments. The level of testing and subject-matter expertise was impressive, even compared to other world-class companies in the industry we've worked with. The depth of vulnerability testing and the findings clearly outlined our strengths and areas for improvement, helping us increase our security standards even further.

Digital Systems

> Professional services, client-oriented approach, we would order again :)

PIXELFEDERATION players to players
danube.pay
ALISON
DITEC
SanaClis
butteland®
piano
ULTIMA PAYMENTS
amerge
DIGITAL SYSTEMS
wezeo
CERTIFICATION DT-CA AUTHORITY

Haxoris
GET HACKED BY US!

CONTACT US

+421 911 430 315
info@haxoris.com
www.haxoris.com

THANK YOU