Professional Services

Maintaining an in-depth understanding of organizational security levels can be time consuming and complex. The penetration testing services performed by our Ghost Labs help you uncover hidden risks with a clear understanding of their current security level and offer advice on how to further improve defenses.

Ghost Labs is the specialist security unit within Outpost24. Our team consists of highly skilled ethical hackers with certifications in the following relevant fields: CISSP, ISSAP, OPSA, CTA, OPST, OPSE and OWSE. We have performed penetration tests for organizations in industries ranging from governmental and insurance, to retail and finance.

Our services:

Advanced Network & Infrastructure Assessments, Web Application & Mobile Application Testing

Scopes for Penetration Testing
Outpost24 offers penetration testing on networks, web applications and mobile applications. Our security consultants will work closely with organizations to choose which testing option best suits their requirements.

Network & Infrastructure Assessments:
We offer network infrastructure tests on internal, external and wireless networks. These are manual tests performed by our team using a variety of network penetration techniques and tools.

Web Application Assessments:
We offer web application testing ranging from highly automated to in-depth manual penetration testing. Security testers will test for technical flaws (e.g. SQL Injection, XSS) and business logic flaws (e.g. negative quantity in a webshop order) against OWASP Top 10.

Mobile Application Assessments:
Many companies are including mobile applications as part of their product portfolio or as a marketing medium. We have seen that many fundamental security design flaws/ mistakes from web applications are re-introduced in the mobile application landscape. Outpost24's security testers can analyze mobile applications for classic flaws and mobile-specific security issues. We are trained and experienced in testing applications running on both IOS and Android.

Phishing
Outpost24 offers organizations the possibility to simulate e-mail based phishing attacks in order to assess and increase the IT security awareness level of its employees. The selection of possible scenarios varies from average phishing attacks to more personalized spearphishing attacks. Each phishing campaign is customizable to fit the needs of your organization. Whether it is a small-scale generic e-mail campaign or a more advanced spearphishing scenario, Outpost24 has the tools and expertise to launch, analyse and report the results of a phishing attack simulation on your organization's employees.

Ghost Labs

Red Teaming: Classic vs Scenario-based Testing

Classic penetration testing consists of well-organized, methodical testing with each possible point of attack examined, evaluated and documented. In a classic penetration test we aim to identify all weak points in a given area.

Our security consultants work with organizations to establish a scope for the testing to define which systems should be tested and to what extent—in order to meet budget and security needs. Scenario-based testing is more agile than the classical model. It focuses on threats and risks using creative testing and established strategies. Full coverage of all potential risks is not the main goal of this test model.

The ideal scenario-based test starts with our security consultants discussing different scenarios with the goal of finding vulnerabilities or risks unique to an organization's network /system. This type of testing is best suited for organizations that are looking for answers on specific threats within their networks and systems.