Professional Services

Market Landscape

Maintaining an in-depth understanding of organizational security levels can be time consuming and complex. The penetration testing services offered by Outpost24 provide organizations with a clear understanding of their current security level and offer advice on how to further improve defenses.

Outpost24's highly skilled team has years of experience in penetration testing as well as expertise in vulnerability management, incident response and information security strategies. Outpost24's penetration testers hold 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

Network & Infrastructure Assessments
- Internal & External Audits
- Wireless Network Audits
- IPv4 & IPv6

Web Application Testing
- Authenticated
- Unauthenticated
- Stress & DoS Testing
- Applets
- REST
- HTML5

Mobile Application Testing
- iOS
- Android
- Windows Mobile

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).

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.

Classic v. Scenario-Based Testing

Classic Penetration 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 Penetration Testing

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.