

Infopulse Penetration testing service

White paper ver. 2010-05-17

Overview

The world's leading countries openly admit the presence of a serious threat represented by the phenomenon of cyber-terrorism and, therefore, acknowledge the necessity to be war-ready in the Internet space. Modern intelligence services open specialized departments dealing with computer spying and infrastructure attacks. Apart from the state bodies, it is mainly businesses that often find themselves under various network attacks. The unequal fights with cyber-criminals can solely be saved by effective defense systems. In modern days, business enterprises spend vast amounts on information security mechanisms, but, in reality, how secure are they? How adequate will be the staff's actions, should an attack really happen? Do our security procedures and drafts truly and fully reflect a potentially real situation or do they only describe the way we see it?

Any security standards as they are require penetration testing, since the latter has proved to be the most reliable indicator of an information security system's efficiency. As computer incident statistic data reveals, most commonly, the weakest links of system defense fall a victim of attacks, since the attackers tend to use a whole inventory of all possible tools. The criminals do not only try and test external system interfaces, but also human resources and companies' business processes, primarily, by applying the cutting edge technical knowledge combined with superb social engineering acting skills. Most companies fail such tests and prove unprepared for threats of the kind, simply because their mitigation procedures are overlooked, while the existing controls – not effective enough. In the meantime, security service departments in large companies neither have a deep enough understanding of the way hackers and industrial spies operate, nor have their skills. One can obtain such skills only under conditions of sufficient investments into information security scientific research. That is why Infopulse's Penetration testing service is the very effective solution a business might be looking for. This service perfectly imitates the threats of cyber-crimes and allows security departments to engage into real war games, while the security management system is undergoing most thorough testing.

By offering most complex penetration testing and through analyzing a team's possible actions, Infopulse helps your business achieve the maximum level of resistance against cyber-threats. Our penetration team is comprised in compliance with your company's peculiarities, and the team's activity is aimed at reaching specific relevant goals (industrial espionage, unauthorized payments, etc.). The technologies we use include the following: using vulnerable network services, social engineering methods, using Trojans and viruses, physical penetration to the customer's areas and connecting to the infrastructure, DoS attacks and phishing. Upon the realization of attaches, the actions of customer's personnel are analyzed, and respective comprehensive recommendations are offered. To make a security management system work smoothly and efficiently any security team should periodically engage into war games featuring penetration testing.

Table 1. Summary of Infopulse’s penetration testing service activities and benefits

Activity	Benefit
Infrastructure vulnerability assessment	Detecting the risks of the services accessible through network being misused
Web application assessment	Defense against specialized professional web-hacking attacks
Customer and employee security, social engineering testing	Reduction of those customer and employee risks, which may negatively affect your business
DOS test	Practical approach to processing company’s business unit interaction, ISP coordination and customer communication scenarios
Business logic analysis, defense against insiders	Most reliable method of defense against fraudsters within and outside the Company
Stabilizing integrity and confidentiality defense mechanisms for financial data exchange between client and server	Allows to safely use the Internet channel, public Internet access areas and portable devices open to interception of sessions
Physical threat analysis	Defense against theft and vandalism aimed at client terminals, bifactor authorization tools and datacenter infrastructure with the e-banking server part
Combined sessions of attack and defense flow analysis	Essential possibility of self-analysis and self-improvement for information security process participants
Complex mitigation plan development	Economically effective risk management

Service Lifecycle

The service implementation features the following steps:

- Defining penetration goals, acceptable attack methods, delivery artifacts and work timelines
- Penetration attempts
- Discussing attack and defense flow
- Composing recommendations
- Penetration upon significant changes introduced to company structure
- Periodic penetration attempts for the purpose of maintaining the efficiency of the security management system



In order to adjust Infopulse's penetration testing service to the unique needs of your business, infrastructure and budget, the service can be focused on particular domains of your application security and test the processes exposed to the most risks. In the course of the penetration limits determination the highest priority work types are pointed out, and acceptable attack methods with regard to the business infrastructure, staff and customers are defined. The testing procedures are carried out in close cooperation with the customer's departments, which allows keeping the penetration activities under strict control. Collaborative sessions make it possible to exchange experience and point out the problematic areas in security controls. Penetration tests are highly recommended after serious modifications for the purpose of diminishing the possible related risks. Infopulse attentively follows all latest updates dedicated to the given testing methods, while periodic penetration tests help to ensure that company security is adequately prepared to resist new cyber-threats.

Deliverables

The present service deliverables include the following:

- Penetration scope definition
- Penetration schedule
- Attack and defense flow report

- Recommendations on improving the security management system

Performance metrics

1. Objective: Penetration should be done in accordance with the schedule
 Measurement: % of the passed tests exceeding the approved time slots
2. Objective: Penetration should reach the goals (CIA compromise)
 Measurement: # of reached goals
3. Objective: Penetration should result in an acceptable amount of damage
 Measurement: \$ of damage over agreed limit
4. Objective: Penetration actions should not dissatisfy/irritate employee/customers
 Measurement: % of dissatisfied/irritated employees/customers
5. Objective: Off-schedule tests in case of critical business changes or a new threat should be performed
 Measurement: # of days between tests execution and the initial request

Service Team

Service delivery team is created depending on the specifics of the customer's environment and business, although it typically includes the following competences:

<ul style="list-style-type: none"> • Network security • Web security • Windows security • Unix security • Fraud • Information security • IT architecture • Wireless security 	<ul style="list-style-type: none"> • Social engineering • DOS • Phishing • Client side attacks and Trojans • Physical security • Risk management • Project management • Portable device security
--	--

The penetration methodology is based on the best approaches used all over the world and includes unique aspects of Infopulse's experience. We use the following essentials:

- OSTMM
- OWASP
- Offensive security
- SANS publications
- Black-hat and other conferences
- @Daily-dave, @pen-test, @websecurity other mail lists
- McAfee, F-Secure, other enterprise and private blogs
- Fraud and phishing reports
- Criminal chronicles
- ISACA publications