ONSEC

Network Infrastructure security audit methodology

Intro

The methodology is a sequence of actions carried out by the Contractor to perform an analysis of the security of the internal infrastructure of the Customer. It also implies the use of other methods of the Contractor to analyze the security of information systems and the application of the following international standards and practices:

- Penetration Testing Execution Standard (PTES);
- Special Publications NIST 800-115 Technical Guide to Information Security Testing and Assessment;
- The Open Source Security Testing Methodology Manual (OSSTMM);
- Information Systems Security Assessment Framework (ISSAF);
- Web Application Security Consortium (WASC) Threat Classification;
- Open Web Application Security Project (OWASP) Testing Guide;
- Payment Card Industry Data Security Standard (PCI DSS);
- Center for Internet Security (CIS) standards.

The purpose of the security analysis is to identify shortcomings and the possibility of exploiting vulnerabilities that lead to unauthorized access to the closed components of the network, and the possibility of their operation up to obtaining full control over the infrastructure of the Customer.

It is assumed that the main purpose of the attacker is to gain access to the IT infrastructure and critical information stored, processed and transmitted in the Customer's information systems, or to manage the components of this infrastructure.

The result of the work is a final report containing an expert assessment of the current level of protection of the external infrastructure of the Customer, a description of the testing progress with information about all identified vulnerabilities, as well as confirmation of their presence and the result of the operation by the Contractor's specialists.

Attacker model

In the course the work, the Contractor's specialists simulate the actions of an attacker, whose purpose is to detect and exploit vulnerabilities existing in the Customer's infrastructure. It is assumed that the attacker is a highly qualified specialist with skills comparable to those of the Contractor.

As part of the ongoing work, the Contractor's specialists can act in accordance with the model of the attacker, which has one or more of the privileges set forth below:

- User account in the Customer infrastructure;
- DMZ network access;
- Access to the guest network segment;
- Access to a custom network segment;
- Also, the contractor's specialists can act in accordance with the model of the offender, which does not have any privileges in the Customer's network.

The scope of work

Work on the analysis of the security of the internal infrastructure is carried out in accordance with the following stages:

- Collection of information on internal infrastructure;
- Security analysis and attempts to compromise internal Customer services;
- Wireless network security analysis (optional);
- Preparation of a report on the results of analysis

Detailed description of the scope of work

Collection of information on internal infrastructure

Within the framework of this stage:

1. Passive data collection

- domain names and subdomains;
- network protocols used by The customer on the local network;
- network equipment;
- the mail server;
- DNS server;
- network component;
- protection means used.

2. Active data collection

- the external system is reflected in the internal network;
- OS types and versions;
- types and versions of SOFTWARE used;
- types and versions of devices used.

Security analysis and attempts to compromise internal Customer services

The purpose of this stage is to search for the possibility of gaining access to the LAN of the Customer's object, as well as unauthorized access to confidential data and protected network segments by an attacker who has the required network access, but does not have sufficient privileges in the applications, operating system or services of the Customer.

1. Network perimeter security analysis

- identification of available network devices and communication protocols;
- identification of types of devices as well as families and versions of the software that implements the network protocols;
- search for remote access interfaces and other interfaces;
- checking the possibility of redirecting network traffic using the features of the channel and network layer protocols, creating false network services for automatic addressing, name resolution, etc.;
- selection of the authentication data based on the common dictionary meanings;

- the interception and re-sending authentication data;
- check the ability to bypass network perimeter security;
- identification of available web interfaces and non-standard communication protocols for further analysis;
- check of possibility of implementation of network attacks according to infrastructure of the Customer.

2. Security analysis of used operating systems services(optional)

- identification of OS network services by typical attributes (standard parameters of network protocols, characteristic response to connection establishment, characteristic features of implementation of network protocols), presence of characteristic service messages in network traffic;
- verification of the correctness of the restriction of access to network services of the operating system, including the use of anonymous / guest access, password matching, interception and repeated / multiple use of authentication data;
- selection of authentication data based on the dictionaries of common values;
- verification of the correctness of anti-password matching, including assessment of the ability of an attacker to block user accounts with multiple unsuccessful authentication attempts;
- verification of the possibility of obtaining confidential information by an attacker using service network protocols (SNMP, RPC, CIFS);
- verify that attacks using network service vulnerabilities can be implemented;
- check the ability to transfer control of the operating system to a remote computer by establishing a reverse connection and tunneling network protocols;
- attempt to remove a copy of the domain tree (Active Directory Tree);
- check the possibility of loading the operating system in a special mode or from an external media (with physical access to the computer);
- checking the possibility of loading the operating system in a special mode (with physical access to the computer);

- view event log data and residual information (deleted files, RAM images stored during crashes);
- search for user authentication data in residual information, software configuration parameters, application and script source code;
- to test the ability to escalate privileges using locally-operated security vulnerabilities and configuration errors software;
- verify that virtualization management interfaces and protected objects can be accessed;
- checking the possibility of matching passwords to management interfaces;
- validates user access rights to virtualization objects, including the ability to read and modify virtual disks, RAM images, configuration files, and virtual machine snapshots without authorization;
- identification of the vulnerabilities of the hypervisor and management tools virtualization environment.

3. Application security analysis (optional)

- identification of vulnerabilities in services and applications using manual inspection and automated vulnerability scanners;
- DBMS security testing;
- web application security testing;
- selection of the authentication data based on the common dictionary meanings.

Wireless network security analysis (if applicable)

At this stage, the Contractor's specialists analyze the security of wireless networks and identify the possibility of penetration into the internal network of the Customer.

This stage is carried out in accordance with the following list of works:

- scanning of the network traffic;
- detect wireless network devices and their identifiers that are available to a potential external attacker;
- determination of the current radio visibility zone;
- collecting information about client devices;

- the collection of available identifiers of networks;
- definition of encryption algorithms used;
- identification of shortcomings in the configuration of built-in cryptographic protection of wireless devices;
- creating false access points or duplicates of existing ones in order to cause the client device to connect to an illegitimate access point;
- connect to a wireless network and identify available corporate network resources;
- detection of unauthorized personal wireless access points within a secure perimeter.

Report preparation

- General information about the testing;
- Goals and objectives;
- Test condition;
- Information about vulnerabilities that lead to the possibility of obtaining critical Customer data;
- Information about the Customer's resources to which unauthorized access was obtained (in case of successful implementation of attacks);
- Expert assessment of the current level of security of the customer's information systems;
- General recommendations to address identified vulnerabilities;
- Detailed information about the vulnerabilities found, including a detailed description, severity level, location, operating example, and Troubleshooting recommendations.

Verification of the remediation of detected vulnerabilities (optional)

Service conditions

On the Customer side, a responsible person is allocated for interaction with the Contractor. Interaction includes coordination of the inspections carried out during the performance of work. The responsible person provides contact information to the Contractor for the possibility of operational interaction.

In case of detection of vulnerabilities that may affect system availability, checks and time slots for testing are negotiated separately with the Customer.

If necessary, the Customer forms a description of the limits of the objects included in the work.

The Contractor's specialists check the vulnerabilities described in the report after a specified number of days from the completion of the main testing. Based on the results of the recheck, a final report is generated containing the status of each previously detected vulnerability.