Possehl Secure

CATALOG OF SERVICES PENETRATION TESTS

Possehl Secure GmbH

2025-08-08

Version 1.0

Possehl Secure GmbH
Eiler Straße 3N | 51107 Cologne | +49 221 466195-20 | info@possehl-secure.de
Management Board: Michael Gentzen (Managing Director), Michael Sieben (Managing Director), Christian Ehlen (Authorized representative)
Registered office of the company: Cologne | Register court: Amtsgericht Köln | Register number: HRB 62035 | VAT ID No. DE 814929728
Commerzbank AG | BIC: COBADEFF508 | IBAN: DE 74 5084 0005 0362 1869 00

www.possehl-secure.de

Version History

Version	Date	Description
1.0	2025-08-08	Initial Version

Content

1 Introduction

Possehl Secure GmbH is a consulting company specializing in IT security with extensive experience in testing, consulting, implementing, and operating security solutions. Possehl Secure GmbH has many years of professional experience in the field of penetration testing. The consultants are certified by recognized institutes – e.g., Offensive Security Certified Professional (OSCP), Offensive Security Experienced Pentester (OSEP), and Offensive Security Certified Expert 3 (OSCE3).

This document specifies the services we offer and our terms and conditions.

2 Specification of Services

2.1 External Penetration Test

An external penetration test refers to the testing of the network perimeter, i.e. IT services accessible via the public Internet.

2.1.1 Test Definition

The following services are provided:

- Identification of addresses and services accessible from the Internet
- Enumeration of software and versions
- Checking for known vulnerabilities and misconfigurations
- Demonstration of the exploitation of vulnerabilities and misconfigurations

A grey box method is used, i.e. the testers receive information about IP addresses and domain names in advance.

The services are performed using tactics, techniques, and procedures that a typical attacker would use.

2.1.2 Scope of Delivery

The following scope of delivery is agreed:

- Final report
    - Management Summary
    - List of vulnerabilities and misconfigurations
    - Risk-based prioritization of results
    - Detailed countermeasures
- *(Optional)* Presentation of results or workshop to discuss results

2.1.3 Obligations to Cooperate

The customer must fulfill the following obligations to cooperate:

- Designation of a contact person for technical questions
- Specification of the test period
- Specification of the desired language of the report (English/German)
- Provision of external IP addresses and domain names (scope)
- If necessary, whitelisting of web application firewalls (WAF) or intrusion prevention systems (IPS)

2.2 Internal Penetration Test

An internal penetration test is defined as the testing of the internal network. This involves a so-called “assume breach” approach, which assumes that a low-privileged user in the network has been compromised.

2.2.1 Test Definition

The following services are provided:

- Identification of addresses and services accessible within the internal network
- Enumeration of software and versions
- Checking for known vulnerabilities and misconfigurations
- Checking whether the Windows domain is configured securely
- Demonstration of the exploitation of vulnerabilities and misconfigurations
- Checking whether lateral movements (network propagation) and/or privilege escalation are possible

A grey box method is used, i.e. the testers receive information about IP addresses and domain names in advance, as well as a low-privilege user account.

The services are performed using tactics, techniques, and procedures that a typical attacker would use.

2.2.2 Scope of Delivery

The following scope of delivery is agreed:

- Final report
    - Management Summary
    - List of vulnerabilities and misconfigurations
    - Risk-based prioritization of results
    - Detailed countermeasures
- *(Optional)* Presentation of results or workshop to discuss results

2.2.3 Obligations to Cooperate

The customer must fulfill the following obligations to cooperate:

- Designation of a contact person for technical questions
- Specification of the test period
- Specification of the desired language of the report (English/German)
- Setup and operation as well as ensuring the availability of the provided Pentest VM (support from Possehl Secure available if required)
- Provision of a low-privileged domain user (“standard employee” account)

- If necessary, whitelisting of web application firewalls (WAF) or intrusion prevention systems (IPS)

2.3 Spear Phishing

Spear phishing refers to specific attacks on users via email. Users are tricked into clicking on a link and entering their login details, which are then intercepted. The aim of the campaign is to review the technical measures against spear phishing and to review user behavior.

2.3.1 Test Definition

The following services are provided:

- Carrying out specific attacks on users in a customized email campaign
- Examining user behavior when dealing with spear phishing emails
- Validating the effectiveness of current technical and organizational security measures in relation with email communication

2.3.2 Scope of Delivery

The following scope of delivery is agreed:

- Final report
    - Management Summary
    - Documentation of the completed campaign
    - Results of the completed campaign
    - Detailed countermeasures to reduce the effectiveness of spear phishing campaigns
- *(Optional)* Presentation of results or workshop to discuss results

2.3.3 Obligations to Cooperate

The customer must fulfill the following obligations to cooperate:

- Designation of a contact person for technical questions
- Specification of the test period
- Specification of the desired language of the report (English/German)
- Provision of the recipient list (email addresses)
- Provision of further information necessary for preparing the campaign in consultation with Possehl Secure (e.g. suitable senders, externally accessible portals, visual details, storyline)

2.4 Web Application Penetration Test

A web application penetration test is used to specifically analyze the security of a web-based application. The aim is to identify vulnerabilities that could be exploited by authenticated or anonymous attackers to gain unauthorized access or to manipulate or exfiltrate data.

2.4.1 Test Definition

The following services are provided:

- Identification and analysis of technical vulnerabilities based on the OWASP Top 10[1] (e.g., XSS, SQL injection, CSRF, IDOR)
- Review of access controls and user rights (horizontal and vertical)
- Analysis of authentication and session management mechanisms
- Identification of insecure configurations and outdated components
- Review of client-side security (e.g. JavaScript, local storage)
- *(Optional)* Review of APIs and mobile front ends of the application

A grey box method is used, i.e. testers are given access to user accounts with different permission levels within the application, if necessary.

2.4.2 Scope of Delivery

The following scope of delivery is agreed:

- Final report
  - Management Summary
  - List of vulnerabilities and misconfigurations
  - Risk-based prioritization of results
  - Detailed countermeasures
- *(Optional)* Presentation of results or workshop to discuss results

2.4.3 Obligations to Cooperate

The customer must fulfill the following obligations to cooperate:

- Designation of a contact person for technical questions
- Specification of the test period (including downtime or maintenance periods)
- Provision of information on scope (URLs)
- If necessary, whitelisting of web application firewalls (WAF) and credentials for upstream authentication mechanisms

[1] https://owasp.org/www-project-top-ten/

- Specification of the desired language of the report (English/German)
- Test user accounts with different permissions
- *(Optional)* Provision of API documentation
- *(Optional)* Provision of specific test data, e.g. coupon codes or discount promotions, dummy payment methods

2.5 White-Box (Web) Application Penetration Test

A white-box penetration test of a (web) application is an extension of the black-box test described in section 2.4. In addition, the source code of the application is examined for security gaps and vulnerabilities. This combined methodology of static and dynamic analysis increases the efficiency and depth of the test, as certain types of vulnerabilities – especially in access control or business logic – are easier to identify in the code than through external testing alone.

2.5.1 Test Definition

The following services are provided:

- Identification and analysis of technical vulnerabilities based on the OWASP Top 10[2] (e.g., XSS, SQL injection, CSRF, IDOR)
- Review of access controls and user rights (horizontal and vertical)
- Analysis of authentication and session management mechanisms
- Identification of insecure configurations and outdated components
- Review of client-side security (e.g. JavaScript, local storage)
- Verification of secure storage of sensitive data (passwords, tokens, keys; not possible with black box)
- Review of logging and error handling (not possible with black box)
- Review of business logic for potential misuse (often not possible with black box)
- *(Optional)* Review of APIs and mobile front ends of the application

2.5.2 Scope of Delivery

The following scope of delivery is agreed:

- Final report in English
  - Management Summary
  - Documentation of the implementation found and risk assessment, structured according to OWASP Top 10
  - List of vulnerabilities and misconfigurations

[2] https://owasp.org/www-project-top-ten/

    - Detailed countermeasures
- *(Optional)* Presentation of results or workshop to discuss results

2.5.3 Obligations to Cooperate

The customer must fulfill the following obligations to cooperate:

- Designation of a contact person for technical questions
- Specification of the test period
- Provision of information on scope (URLs)
- Provision of the application source code
- *(Optional)* Provision of documentation on architecture, interfaces, role model, API
- Test user accounts with different permissions
- *(Optional)* Provision of specific test data: e.g. coupon codes or discount promotions, dummy payment methods

2.6 Mobile App Assessment (Android)

The mobile app assessment is used to uncover potential vulnerabilities in Android applications that could be exploited to gain unauthorized access to company resources or sensitive data.

2.6.1 Test Definition

The following services are provided:

- Testing the frameworks and configurations used for possible vulnerabilities
- Checking whether unauthorized access to company resources or sensitive data could be gained

A grey box method is used, i.e. testers may be given access to low-privilege accounts in the app.

2.6.2 Scope of Delivery

The following scope of delivery is agreed:

- Final report
    - Management Summary
    - List of vulnerabilities and misconfigurations
    - Risk-based prioritization of results
    - Detailed countermeasures
- (Optional) Presentation of results or workshop to discuss results

2.6.3 Obligations to Cooperate

The customer must fulfill the following obligations to cooperate:

- Designation of a contact person for technical questions
- Provision of the Android application in apk format or as a link to Google Play
- *(Optional)* Provision of low-privilege accounts
- *(Optional)* Provision of test hardware
- Specification of the test period
- Specification of the desired language of the report (English/German)

2.7 USB Drop Assessment

A USB drop assessment simulates a realistic attack using specially prepared USB sticks that are deliberately placed in public locations near the company. The aim is to test employees' willingness to connect unknown devices and to check technical protective measures on end devices. The USB devices used simulate a keyboard (HID) and are not usually recognized as mass storage devices, which means that conventional EDR solutions often do not block them and code can therefore be executed.

2.7.1 Test Definition

The following services are provided:

- Provision of prepared USB sticks that use keyboard emulation (HID)
- Execution of simple to complex payloads (e.g. a curl command to a controlled server or a reverse shell) to record usage and response
- Optional: Two-stage test procedure:

  1) Technical test (if a customer laptop is provided):

     - Checking whether technical security measures (e.g. device control, execution prevention) can be bypassed
     - Attempting to establish a reverse shell or execute other persistent commands

  2) Social Engineering Test:

     - Distribution of USB sticks in the company environment (e.g. entrance areas, cafeteria, parking lots)
     - Recording of accesses via simple web requests to the control server

The assessment is performed as either a black box or grey box test.

- Black box, if only the USB sticks are distributed without any further information

- Grey box, if a customer laptop is also provided for technical testing, including user access, in order to specifically check security measures

2.7.2 Scope of Delivery

The following scope of delivery is agreed:

- Final report
  - Management Summary
  - List of vulnerabilities and misconfigurations
  - Risk-based prioritization of results
  - Detailed countermeasures
- *(Optional)* Presentation of results or workshop to discuss results

2.7.3 Obligations to Cooperate

The customer must fulfill the following obligations to cooperate:

- Designation of a contact person for technical questions
- Specification of the test period and, if applicable, desired distribution priorities (e.g. location, building)
- Specification of the desired language of the report (English/German)
- Consent to the placement of USB devices in public or semi-public areas of the company
- *(Optional)* Provision of a typical company end device (laptop/notebook) for technical testing. The device should have a typical setup with EDR (Endpoint Protection) and user configuration. A user account with appropriate access rights must also be provided.

2.8 Stolen Asset Assessment

A stolen asset assessment involves checking the security of a stolen device, such as a company laptop, in order to identify potential risks to the company.

2.8.1 Test Definition

The following services are provided:

- Identification and possible circumvention of physical security measures
- Identification and possible circumvention of technical security measures
- Verification of whether exfiltration of sensitive data is possible
- Verification of whether the asset can be used by an unauthorized third party to gain access to company resources

A black box procedure is used, i.e. the testers receive no further information from the customer apart from the device.

2.8.2 Scope of Delivery

The following scope of delivery is agreed:

- Final report
    - Management Summary
    - List of vulnerabilities and misconfigurations
    - Risk-based prioritization of results
    - Detailed countermeasures
- *(Optional)* Presentation of results or workshop to discuss results

2.8.3 Obligations to Cooperate

The customer must fulfill the following obligations to cooperate:

- Designation of a contact person for technical questions
- Specification of the test period
- Specification of the desired language of the report (English/German)
- Sending the asset to be tested

2.9 WiFi Assessment

The WiFi assessment serves to uncover vulnerabilities in the customer's WiFi infrastructure that could be exploited to gain unauthorized access to internal company resources.

2.9.1 Test Definition

The following services are provided:

- Testing the WiFi protocols and configurations used for possible vulnerabilities

A grey box method is used, i.e. the testers are given physical access to the respective company locations where the test is to take place.

2.9.2 Scope of Delivery

The following scope of delivery is agreed:

- Final report
    - Management Summary
    - List of vulnerabilities and misconfigurations
    - Risk-based prioritization of results
    - Detailed countermeasures

- *(Optional)* Presentation of results or workshop to discuss results

2.9.3 Obligations to Cooperate

The customer must fulfill the following obligations to cooperate:

- Designation of a contact person for technical questions
- Specification of the respective locations
- Access to the locations if testing is also to be carried out on the customer's premises
- Specification of the test period
- Specification of the desired language of the report (English/German)

2.10 Cloud Assessment

A cloud assessment involves systematically checking the cloud infrastructure and services used for security vulnerabilities, misconfigurations, and potential measures to improve security.

2.10.1 Test Definition

The following services are provided:

- Analysis of cloud configuration and permissions based on a provided user account with reading permissions
- Review of security policies, access controls, and role models
- Checking for potential misconfigurations, excessive permissions, and unused resources
- Evaluation of the implementation of security-related mechanisms such as encryption, network segmentation, and logging
- Identification of gaps in existing processes, e.g. missing emergency accounts

A grey box method is used, in which testers are given access to a user account with reading permissions in order to check the cloud configuration and security measures.

2.10.2 Scope of Delivery

The following scope of delivery is agreed:

- Final report
  - Management Summary
  - List of vulnerabilities and misconfigurations
  - Risk-based prioritization of results
  - Detailed countermeasures
- *(Optional)* Presentation of results or workshop to discuss results

2.10.3 Obligations to Cooperate

The customer must fulfill the following obligations to cooperate:

- Designation of a contact person for technical questions
- Specification of the test period
- Provision of a user account with reading permissions for the cloud project to be audited
- Specification of the desired language of the report (English/German)

2.11 Microsoft 365 Audit

During a Microsoft 365 (M365) audit, the Microsoft 365 and Entra ID configuration are systematically checked for misconfigurations and potential measures to improve security.

2.11.1 Test Definition

The following services are provided:

- Analysis of Microsoft 365 / Entra ID configuration and permissions based on a provided user account with the appropriate administrative role in Entra ID
- Review of conditional access policies, MFA, and other security policies according to the current Microsoft 365 Foundations Benchmark from the Center of Internet Security (CIS)
- Checking for potential misconfigurations
- Semi-automated review of the M365 tenant using security assessment tools (PowerShell script-based)
- Manual checks for completion of the audit

2.11.2 Scope of Delivery

The following scope of delivery is agreed:

- Final report
- Provision of the current M365 Foundations benchmark in PDF format
- Provision of the audit results in Excel format
- Provision of a PDF file with a summary of the M365 audit results
- *(Optional)* Presentation of results or workshop to discuss the results

2.11.3 Obligations to Cooperate

The customer must fulfill the following obligations to cooperate:

- Designation of a contact person for technical questions

- Provision of an admin user in the Microsoft 365 tenant to perform the audit (admin authorization is required for a maximum of 4-5 hours)
- Specification of the test period
- Selection of the desired language for the summary of results (English/German)

2.12 Red Team Assessment

The aim of a red team assessment is to test the organization's overall security situation by simulating a realistic attack without prior information about the company.

A target is defined (e.g. compromising a specific internal system or gaining access to specific internal data) that must be achieved without restricting the possible attack vectors. In addition to technical attacks, social engineering and the penetration of physical assets can also be used.

In general, only the direct client knows the scope, objectives, and execution period; the responsible internal departments (IT, SOC, or facility security) are not informed in advance.

2.12.1 Test Definition

The following services are provided:

- Assessment of the responsiveness and effectiveness of the protective mechanisms, processes, and technologies used by the customer in achieving a goal specified by the customer

A black box method is used, i.e. the testers do not receive any information about the company in advance that is not publicly available.

2.12.2 Scope of Delivery

The following scope of delivery is agreed:

- Final report
    - Management Summary
    - List of exploited vulnerabilities that led to the achievement of the objective
    - Detailed countermeasures
- *(Optional)* Presentation of results or workshop to discuss results

2.12.3 Obligations to Cooperate

The customer must fulfill the following obligations to cooperate:

- Designation of a contact person available 24/7 with the authority and ability to stop the assessment and inform the relevant departments/persons within the organization

- Issue of a document that identifies the respective testers to uninformed parties as authorized to carry out the test and includes the relevant contact persons ("Get out of Jail" card)
- Specification of the objectives to be achieved
- Specification of the test period
- Selection of the desired language for the summary of results (English/German)

2.12.4 Physical Assessment

The aim of a physical assessment within a Red Team Operation is to penetrate buildings on site by overcoming potential security systems and processes. A specific target is defined that must be achieved after successful penetration.

2.12.4.1 Test Definition

The following services are provided:

- Identification of vulnerabilities in existing security concepts on site
- Unnoticed intrusion into the building
- Connection of own hardware / provision of proof of successful intrusion

2.12.4.2 Scope of Delivery

The following scope of delivery is agreed:

- Final report
  - Management Summary
  - List of exploited vulnerabilities that led to the achievement of the objective
  - Detailed countermeasures
- *(Optional)* Presentation of results or workshop to discuss results

2.12.4.3 Obligations to Cooperate

The customer must fulfill the following obligations to cooperate:

- Designation of a contact person available 24/7 with the authority and ability to stop the assessment and inform the relevant departments/persons within the organization
- Issue of a document that identifies the respective testers to uninformed parties as authorized to carry out the test and includes the relevant contact persons ("Get out of Jail" card)
- Specification of the objectives to be achieved
- Specification of the test period
- Selection of the desired language for the summary of results (English/German)

3 Appendix

3.1 Definitions

Penetration Test: Controlled attempt to invade a specific computer system or network in order to identify and demonstrate existing vulnerabilities.

Black box: In a black box procedure, no information about the customer's environment and target systems (e.g. IP addresses) is available in advance. This means that the test is carried out from the perspective of an external attacker. However, this results in higher costs due to the need to collect information during the test.

White box: In a white box procedure, all information about the customer's environment and target systems (e.g. source code for a web application) is available in advance. This allows for a much more in-depth examination than is possible with black box or grey box procedures.

Grey box: A grey box procedure is a mixture of black box and white box procedures. Certain information about the environment and target systems is disclosed (e.g. IP addresses). This procedure offers a good balance between effort and results.