PENETRATION TEST

RULES OF ENGAGEMENTS TEMPLATE

by Hoek from 0ut3r.space

**SCOPE**

Web application <APP\_NAME>

# CONTENTS

[CONTENTS 2](#_Toc125807615)

[DOCUMENT INFORMATION 3](#_Toc125807616)

[TEST METHODOLOGY 4](#_Toc125807617)

[SCOPING & EFFORT ESTIMATION 4](#_Toc125807618)

[TECHNICAL SPECIFICATIONS 4](#_Toc125807619)

[DEFINITION OF ORGANIZATIONALS DETAILS 4](#_Toc125807620)

[KICKOFF SUMMARY 4](#_Toc125807621)

[TOOLS 4](#_Toc125807622)

[RULES OF ENGAGEMENT 6](#_Toc125807623)

[PENETRATION TESTING TEAM CONTACT INFORMATION 6](#_Toc125807624)

[TARGET DEPARTMENT/ORGANIZATION CONTACT INFORMATION 6](#_Toc125807625)

[DETAILS AND SCOPE 6](#_Toc125807626)

# DOCUMENT INFORMATION

Rules of engagement (RoE) are meant to list the details of the penetration test. That’s the details behind what exactly will be tested when it will be tested, how it will be tested, and who the primary contacts will be throughout the engagement. This way, internal audit team conducting the penetration test and the organization being tested will know precisely what to expect from the test.

This document should be pre-filled by the person ordering the test, in cooperation with the owner and the team responsible for the condition and development of the service or application being tested. The document will then be discussed at a meeting with the audit team.

#

# TEST METHODOLOGY

Our penetration tests are based on standards such as OWASP, NIST, and PTES guidelines as well as internal good practices of conducting security tests developed by 0ut3r.space auditors.

The main objective of the Penetration Test is to discover potential vulnerabilities, misconfigurations, and other potential threads in order to improve the security level of the tested platforms by giving recommendations on how to address identified security vulnerabilities.

Below you can find general way of working and project initiation.

## SCOPING & EFFORT ESTIMATION

* Description of the assets in scope
* Definition of possible roles and users
* Walkthrough the application or assets to get to know the usual workflow
* Clarification of the background and goal of the penetration test

## TECHNICAL SPECIFICATIONS

* Description of the technical side of the assets (used frameworks, technologies, programming languages)
* Discussion of security measures already in place
* Short deep dive into highly sensitive functions and systems

## DEFINITION OF ORGANIZATIONALS DETAILS

* Identification of all stakeholders and their authorities
* Definition of central contact persons on SOC Team and client side
* Final discussion about the project plan and milestones

## KICKOFF SUMMARY

* Summary of all discussed details
* Defining of open tasks on client side and for SOC Team
* Note down of all deadlines, contact details and all other discussed items
* Send out of the summary to all relevant stakeholders

## TOOLS

During the test, auditors will use various tools, depends on scope of test, defined in this document. General list of tools used during penetration testing of web application, network, and servers:

* Burp Suite Professional
* OWASP ZAP
* hashcat
* nmap
* ffuf
* wfuzz
* sslscan/sslyze
* Shodan/Censys/ZoomEYE
* Google Dorks
* Nikto
* wafw00f
* Metasploit Framework
* Qualys
* Wireshark
* DirBuster
* Wapiti
* SkipFish

The auditors team reserves the right to use additional tools not listed above.

# RULES OF ENGAGEMENT

## PENETRATION TESTING TEAM CONTACT INFORMATION

Primary contact: <PRIMARY\_AUDITOR>

Position: Penetration Tester - Auditor 1

Mobile phone: <PRIMARY\_PHONE\_NUMBER>

Email address: <PRIMARY\_EMAIL\_NUMBER>

Secondary contact: <SECONDARY\_AUDITOR>

Position: Penetration Tester - Auditor 2

Mobile phone: <SECONDARY\_PHONE\_NUMBER>

Email address: <SECONDARY\_EMAIL\_NUMBER>

## TARGET DEPARTMENT/ORGANIZATION CONTACT INFORMATION

Depends on the test it should be penetration test requestor and system or application owner or a person from the company to contact during the test. If there are any additional questions from auditors or out-of-the-box situations not described in the following document which can occur during the testing, this contact listed below should be able to assist.

Primary contact name: Click or tap here to enter text.

Position: Click or tap here to enter text.

Role: Choose an item.

Mobile phone: Click or tap here to enter text.

Email address: Click or tap here to enter text.

Organization/department: Click or tap here to enter text. / Click or tap here to enter text.

Emergency contact: [ ]

Secondary contact name: Click or tap here to enter text.

Position: Click or tap here to enter text.

Role: Choose an item.

Mobile phone: Click or tap here to enter text.

Email address: Click or tap here to enter text.

Organization/department: Click or tap here to enter text. / Click or tap here to enter text.

Emergency contact: [ ]

Tertiary contact name: Click or tap here to enter text.

Position: Click or tap here to enter text.

Role: Choose an item.

Mobile phone: Click or tap here to enter text.

Email address: Click or tap here to enter text.

Organization/department: Click or tap here to enter text. / Click or tap here to enter text.

Emergency contact: [ ]

Preferred way of communication during the penetration test:

Primary: Choose an item. Secondary: Choose an item.

Daily Debriefing: Choose an item. If required, please provide choose contact Choose an item.

## DETAILS AND SCOPE

Preferred start date: Click or tap to enter a date.

Preferred end date: Click or tap to enter a date.

Type of test: Choose an item.[[1]](#footnote-1)

Testing occurs at the following times: Choose an item. If custom selected: Click or tap here to enter text.

Tests relate to: Choose an item.

General scope of testing[[2]](#footnote-2):

Click or tap here to enter text.

Will test be announced to target personnel or application/asset owner: Choose an item.

Will test be announced to the company monitoring/incident response team: Choose an item.

Will target department/organization try to detect and avoid IP addresses of attack systems: Choose an item.[[3]](#footnote-3)

Would detection and/or blocking of the attack system ends the test: Choose an item.

If not, what steps will be taken to continue if systems get blocked and what approval (if any) will be required:

Click or tap here to enter text.

IP addresses of penetration testing team's attack systems:

* <IP\_ADDRESS>

What is the policy regarding viewing data (including potentially sensitive/confidential data) on compromised hosts?[[4]](#footnote-4)

Click or tap here to enter text.

In the case that a system is penetrated, how should the testing team proceed?

Choose an item.

Are Disaster Recovery Procedures in place for the target asset? Choose an item.

Are backups tested on a regular basis for the target asset? Choose an item.

Reason for making a Penetration Test[[5]](#footnote-5):

Click or tap here to enter text.

What are the main goals/expectations[[6]](#footnote-6)?

Click or tap here to enter text.

Additional details that requestor would like to add:

Click or tap here to enter text.

Date of introduction/kick off meeting: Click or tap to enter a date.

Depending on the test request type, please complete the appropriate fields in tables below. For the Gray/Black Box test, you can skip some answers (Please delete tables not related to the requested test type).

|  |
| --- |
| Information required for the Web App/API/Server/Backend penetration test |
| What is the application name? |  |
| What is the application URL/IP? |  |
| What language is the application written in (ASP, PHP, Java etc.)? |  |
| What framework is used, if any? |  |
| Is it a Cloud hosted site? |  |
| Cloud provider name? |  |
| Have you submitted a testing request with the provider? |  |
| Is a web application firewall (WAF) being utilized? |  |
| If “YES”, will the WAF be disabled during testing, or is it possible to whitelist our IPS’s? |  |
| What is the backend database, if applicable (MySQL, Microsoft SQL, AWS Database, Oracle etc.)? |  |
| Does the application have multiple roles (unauthenticated, user, admin, manager)? |  |
| Does role-based testing is required? |  |
| What is the application login credentials, if required? (Please provide login and password of all roles which should be tested, administrator, editor, user, customer etc.) |  |
| Is the site hosted on a shared platform with other sites? |  |
| Is the site load balanced? |  |
| Are Administrators or Developers notified of errors via email? |  |
| Will the documentation of application be provided? |  |
| Is a backend in scope? |  |
| Is test data provided? |  |
| Type of environment[[7]](#footnote-7) (testing/stagging/production) |  |

|  |
| --- |
| Information required for the Network (external) penetration test |
| If systems are hosted outside the client managed network, please specify which hosting/cloud provider hosts these systems. |  |
| Have you received authorization for testing from provider? |  |
| How many external IP addresses are in scope for testing? |  |
| List the external IP ranges in scope for testing. |  |
| Are all systems being tested located within a client managed network? |  |
| Are perimeter/edge security controls configured to block known scans and attacks? |  |
| If “YES” to the above, will these controls be temporarily altered to fully test the target systems? |  |
| Is any target to be excluded? If so, please list targets and provide reasoning for exclusion. |  |

|  |
| --- |
| Information required for the Network (internal) penetration test |
| List the internal network subnets in scope for testing. |  |
| If systems are hosted outside the client managed network, please specify which /hosting/cloud provider hosts these systems. |  |
| Have you received authorization for testing from provider? |  |
| How many internal IP addresses are in scope for testing? |  |
| List the internal IP addresses in scope for testing. |  |
| Are internal network security controls configured to block known scans and attacks? |  |
| If “YES” to the above, will these controls be temporarily altered to fully test the target systems? Note: It is recommended to fully test in scope systems on the internal network(s). |  |
| Are any targets to be excluded? If so, please list targets and provide reasoning for exclusion. |  |

|  |
| --- |
| Information required for the Network (wireless) penetration test |
| At how many locations is wireless testing performed? |  |
| Please provide the physical addresses of the facilities in scope for wireless security testing. |  |
| Please provide the approved SSIDs for the company’s wireless access points. |  |
| Does the guest network require authentication? |  |
| Technologies in use? WPA, WPA2-PSK or EAP? Are all accessible over 2.4GHZ or some 5GHz? |  |
| Is there any Wireless Intrusion Prevention Systems, Network Access Control (NAC) or Rogue AP detection in use? |  |
| Are any SSIDs/wireless access points to be excluded? If so, please list here and provide reasoning for exclusion. |  |
| What type of encryption is used? |  |

The result of test will be presented in the form of a PDF report with a description of the activities carried out, the vulnerability findings with risk classification and the mitigation recommendations.

Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of contact representing target organization/department

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of head of Auditors team

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signatures of individual auditors:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Black Box - no knowledge about the target, Gray Box – partial information, White Box – full documentation, access and details provided. [↑](#footnote-ref-1)
2. URL, IP, API, Address, Application Name, Network Range, User Account etc. [↑](#footnote-ref-2)
3. E.g., blocking IP address of auditors on security alerts. [↑](#footnote-ref-3)
4. Related to GDPR. Transmission and Storage Methods, Retention and Destruction Policy [↑](#footnote-ref-4)
5. E.g., review of big changes in code, changes in configuration, checking the asset security, general health check, review before putting application on production, discover potential vulnerabilities, misconfigurations etc. [↑](#footnote-ref-5)
6. For example, gain unathorised access to the application, or only report with findings. [↑](#footnote-ref-6)
7. Testing or stagging is preferred if it is on similar version and functionality as production. [↑](#footnote-ref-7)