RoE (Rules of Engagement)

# Introduction

This document describes the unified rules for customers wishing to perform a penetration test against their Infrastructure components. Care must be taken to limit all penetration tests to your assets and avoid unintended consequences. These Rules of Engagement are designed to allow to effectively evaluate the security of your assets while preventing harm to other infrastructure’s components not belonging to the customer. All penetration tests must follow the Rules of Engagement as detailed on this page.

# Customer Details

Company Name:

| Contact Name | Email/Phone | Role | Preferred Contact |
| --- | --- | --- | --- |
| X | A | B | C |
| Y | C | D | E |
| Z | E | F | G |

# Scoping

Why is the customer having the penetration test performed against their environment?

Is the penetration test required for a specific compliance requirement?

When does the customer want the active portions (scanning, enumeration, exploitation, etc...) of the penetration test conducted?

* During business hours?
* After business hours?
* On the weekends?

Are there any devices in place that may impact the results of a penetration test such as a firewall, intrusion detection/prevention system, web application firewall, or load balancer?

Allowed IP/URL/Domains/Subdomains?

Denied IP/URL/Domains/Subdomains?

Does the customer own all those infrastructure components?

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

* Perform a local vulnerability assessment on the compromised machine?
* Attempt to gain the highest privileges (root on Unix machines, SYSTEM or Administrator on Windows machines) on the compromised machine?

Perform no, minimal, dictionary, or exhaustive password attacks against local password hashes obtained (for example, /etc/shadow on Unix machines)?

# Key Assumptions

There’s inherent risk of data loss due to this assessment, however no activities will result in “intentional” data loss. This assessment will not replicate adversarial action as such activity(s) fall outside the scope of the assessment.

# Termination of testing

If the Penetration tester is not able to gain access to target environment systems in accordance with the budgeted level of effort, the testing will cease. If the Penetration Testing Team can gain access, revealing the capability for exploitation, the vulnerability shall be documented accordingly. In addition, the testing will terminate if:

* Unexpected occurrences are encountered that prohibit further testing.
* The customer reports that testing procedures materially affect computer operations in a negative manner.

# Data Handling

All sensitive data, at rest or in transit, must be encrypted. All deliverables will be protected and marked as sensitive.

Upon completion of testing and delivery of all final reports, any data collected during the test shall be destroyed unless otherwise agreed upon in writing.

# Reporting

The assessment team will provide a final penetration test report within an agreed upon time frame after the conclusion of the test. The report will contain the scope of the assessment also found in this document, the list of activities performed, the results of the assessment and recommendations on remediation of the findings. The final report is provided as-is and for information purposes only.

Date:

Signed and approved by:

IP Solutions AB [Customer company name]

Name: [Your name] Name: [Customer name]

Title: [Your title] Title: [Your title]