**Customers Penetration Testing Request**

Because penetration testing/vulnerability scans could have adverse effect on RDC or RDC customer’s environments RDC has established a process for customers to request permission to conduct penetration tests/vulnerability scans to or originated from RDC environment.

RDC customer is responsible to ensure that contracted third-parties perform penetration testing/vulnerability scans in a manner that does not violate RDC instructions.

Furthermore, the customer is responsible for any damages to RDC or other RDC customers that are caused by his penetration testing activities.

**Kindly make sure that you are aware of the following important points:**

* Permission is required for all penetration tests/vulnerability scans.
* The testing will be limited to the source and destination IP addresses, network bandwidth, and instance-level resources (such as CPU, memory and input/output), the times, and all other conditions specified in the request form.
* The test is subject to the terms of the RDC Web Services customer agreement.
* Testing is not authorized until RDC validates the information and sends an authorization email.
* The penetration tests/vulnerability scans shouldn’t require any configuration modification for RDC environment.
* RDC is flexible regarding the used tools to perform penetration testing/vulnerability scan, while caring to protect other RDC customers and ensuring quality-of-service across RDC.
* Customer is prohibited from utilizing any tools in a manner that perform Denial-of-Service (DoS) attacks or simulations of such attacks against any of RDC resources.
* Requesting companies should prevent the used tools from exploiting any vulnerability that has a potential adverse impacts on resources that may be shared with other customers.
* The authorization form will be reviewed and approved within 3 business days (completed forms only). Please adjust your plans as required and ensure that your request includes all information.
* Any discoveries of vulnerabilities or other issues that are affecting RDC environment must be communicated to RDC security team ASAP. The performance of the Testing and the results are considered RDC Confidential Information.
* The information you will share with RDC as part of this process will be kept confidential.
* Please send your requests/security concerns to rdc-sec-pen@rayadatacenter.com

In order to request permission to conduct vulnerability and penetration testing directed to or originating from RDC environments, the following information is required.

Upon receipt and validation of the sent information, an authorization email approving the test plan will be sent to the addresses provided below. Testing is not allowed until receiving the authorization.

Please complete and submit the authorization request for penetration testing/vulnerability scans to or originating from any RDC environments to the following email:

“[rdc-sec-pen@rayadatacenter.com](mailto:rdc-sec-pen@rayadatacenter.com)”

|  |  |
| --- | --- |
| Contact Name |  |
| Email Address(s) |  |
| Mobile |  |
| Company Name |  |
| Used Services |  |
| Affected Resources |  |
| Target Date |  |
| Source IP Address |  |
| Source Location |  |
| Destination IP Address |  |
| Destination Location |  |
| Testing Company |  |
| Contacts of Testing Company |  |
| Company Email |  |
| Company Phone No. |  |
| Test Type | * Vulnerability Assessment * Penetration Testing |
| Test Objectives |  |
| Expected Required BW |  |
| Expected Peak Requests/Sec |  |
| Expected Start Time |  |
| Expected End Time |  |
| Emergency Phone Number  “In case we need to stop the test” |  |
| Additional Information |  |