

Internal and Confidential

Netradyne Vulnerability Assessment and Penetration Testing Process and Procedure

v1.3

Table of Contents

[1. Purpose 2](#_Toc205244992)

[2. Scope 3](#_Toc205244993)

[3. Roles and Responsibilities 3](#_Toc205244994)

[4. Roles and responsibilities specific to this document are included below: 3](#_Toc205244995)

[5. VAPT Process 3](#_Toc205244996)

[6 Tools 4](#_Toc205244997)

[7 VAPT Standard Operating Procedure 5](#_Toc205244998)

[7.2 VAPT Checklist and Objective 5](#_Toc205245000)

[8 Conduct 9](#_Toc205245001)

[9 Exception 9](#_Toc205245002)

[10 Terms/Acronyms 9](#_Toc205245003)

[11 References 9](#_Toc205245004)

[12 Appendix A: Document RACI Matrix 9](#_Toc205245005)

**Document Control**

|  |  |
| --- | --- |
| **Document ID** | NDVAPT2022001 |
| **Document Name** | Netradyne Vulnerability Assessment and Penetration Testing Process & Procedure |
| **Document Status** | Released |
| **Document Released Date** | 13-08-2022 |
| **Document Author** | Gautam Kumar |
| **Document Content Contributors** | Gautam Kumar |
| **Document Signatory** | Saravanan Sankaran |
| **Document Owner** | Saravanan Sankaran |
| **Document Version** | v1.3 |
| **Information Classification** | Internal |

**Document Edit History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Additions/Modifications** | **Prepared/Revised By** |
| V1.0 | 04-AUG-2022 | Initial Document | Gautam Kumar |
| V1.1 | 24-JUL-2023 | Updated Document with additional information | Gautam Kumar |
| V1.2 | 01-FEB-2024 | Added Timeline and Tool description | Gautam Kumar |
| V1.3 | 31-JAN-2025 | Reviewed with no changes | Gautam Kumar |

**Document Review/Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Signatory Name** | **Organization/Signatory Title** | **Comments** |
| 07-AUG-2022 | Saravanan Sankaran | Senior Director - Info Security & IT | Approved |
| 24-JUL-2023 | Saravanan Sankaran | Senior Director - Info Security & IT | Approved |
| 07-FEB-2024 | Saravanan Sankaran | Senior Director - Info Security & IT | Approved |
| 04-FEB-2025 | Saravanan Sankaran | Senior Director - Info Security & IT | Approved |

**Distribution of Final Document**

|  |  |
| --- | --- |
| **Name** | **Organization/Title** |
| All Stakeholders | Netradyne Inc |
|  |  |
|  |  |
|  |  |
|  |  |

# Purpose

The purpose of Netradyne Vulnerability Assessment and Penetration Testing Process and procedure is to layout the process and standard operating procedures for vulnerability assessment and penetration test performed against Netradyne assets (e.g., IDMS application, Netradyne Website, Infra, IT, Network, Mobile applications etc.).

# Scope

This SOP applies to all NETRADYNE technology assets, facilities, employees, contractors (as provided by law or contract), partners, and visitors, in achieving NETRADYNE missions, programs, projects, and institutional and compliance requirements.

# Roles and Responsibilities

# Roles and responsibilities specific to this document are included below:

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Owner | * Team or SME responsible for the process area needs to ensure this document is up to date and compliant with governing requirements. * Is the point of contact for the document. * Responsible for initiating and managing document review and the approval process from start to finish including gathering or delegating the collection of content including diagrams, formatting etc. as well as identifying stakeholders to participate in the peer review process. |
| Reviewers/Stakeholders | Representations from teams that can affect or be affected by the document under review (e.g., Operation, Security, Compliance, Quality) |
| Approvers | The Person(s) of authority to validate the document and sign-off on the latest version. Such Person include Document owner, Functional Team Lead, Security Lead, Product Delivery Lead. |
| Document Release | Document Owner/team to work with repository administrator to make release version available. |

# VAPT Process

Vulnerability assessment and Penetration testing(VAPT) is an activity in which a test team (hereafter referred to as "Pen Tester") attempts to circumvent the security processes and controls of a computer system. Posing as either internal or external unauthorized intruders, the test team attempts to obtain privileged access, extract information, and demonstrate the ability to manipulate the target computer in unauthorized ways if it had happened outside the scope of the test.

VAPT activity helps an organisation to meet customer obligations and various compliance requirements such as ISMS, GDPR, HIPAA etc.  ​It helps in securing assets from both internal and external malicious threats by identifying security vulnerabilities in our Products, Applications, and Infrastructure to keep our organisational and customer data safe (including PII, PHI/e-PHI and other sensitive data).

Vulnerability Assessments/Penetration Tests are conducted periodically on Infrastructure, Application, APIs, Devices to detect new vulnerabilities. Relevant stakeholders should research and remediate "Critical," "High", "Medium" or “Low” severity vulnerabilities within the prescribed timeline.

Due to the sensitive nature of the testing, specific rules of engagement are necessary to ensure that testing is performed in a manner that minimizes impact on operations while maximizing the usefulness of the test results.

#### VAPT Scope

VAPT assessment covers all the critical assets/products that includes applications, APIs, IT Infra, Cloud Infra and Devices. Below is the list of all critical assets that are covered in VAPT scope.

|  |  |
| --- | --- |
| Asset Type | Scope of Assessment |
| Application | IDMS Application, Netradyne Website, Mobile Application, Driveri Store Application |
|
| IT Infra | Internal Network Assessment |
| AWS Infra | All critical instances in AWS |
| Device | All critical Device SKUs |
| API | All Platform and Data product API |

#### Methodology

#### Black Box testing:

In a black box pen test, the penetration tester has no access or internal knowledge of the target environment.  The pen tester needs to perform their own reconnaissance and identify a vulnerability to exploit for initial access to the environment. Black box pen testing is designed to emulate most closely a true cyberattack.

#### Grey Box Testing:

Gray box penetration tests provide the pen tester with a greater level of access and knowledge about the target environment.  Instead of starting from completely outside, the penetration tester is provided with a legitimate account and limited knowledge of the enterprise environment.

#### White Box Testing:

White box techniques involve direct analysis of the application’s source code. A penetration tester has the greatest level of knowledge and access in a white box assessment.  In this form of penetration test, a tester is given full documentation and privileged access to the enterprise network.

#### Timeline Estimation

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Application | IDMS Web Application | Netradyne Web Application | APIs | Driveri Store | IT  Infra | AWS  Infra | Device |
| Timeline | 2 Weeks | 2 Weeks | TBD | 2 Weeks | 2 Weeks | 2 Weeks | 4 Weeks/SKU |

TBD (To Be decided): Based on actual number of APIs in scope.

# Tools

|  |  |
| --- | --- |
| Application | Burp: It is a web proxy tool used to intercept traffic between client and the server and also performs basic vulnerability scanning of the target application  Nessus: It is an industry standard automated network scanner Kali Linux: Kali Linux is a Linux distribution designed for digital forensics and penetration testing.  ZAP: It is an open-source web application security scanner  Metasploit: The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. |
| INFRA | Nmap: Nmap is a network scanner used to discover hosts and services on a computer network by sending packets and analysing the responses.,  Nessus: It is an industry standard automated network scanner  Zenmap: Zenmap is the official cross-platform GUI for the Nmap Security Scanner.  Metasploit : The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.  Kali Linux: Kali Linux is a Linux distribution designed for digital forensics and penetration testing. |

# 

# VAPT Standard Operating Procedure

#### Stakeholders Roles and Responsibilities

#### Application/ Infra/ Device Point of Contact (POC)

* + - Be responsible for coordination of the penetration test activities and schedules, and notify management (e.g., Functional Leads, Security Manager, etc.) of planned activities.
    - Coordinate the penetration test with the Infosec POC.
    - Be the recipient of all data generated by and related to the Security Penetration test.
    - Shall be responsible for ensuring that all access to the environment and application provided for the security test are revoked after the completion of the activity.

# **InfoSec Point of Contact (POC)**

* Be responsible for the penetration test team and be the primary interface with the Application/ Infra/ Device POC for all penetration test activities.
* Develop the documentation and plans for the penetration test.
* Identify and assign roles to both the Pen Tester's team and the test participants, identify major milestones for the tasks of the Tester's team, identify estimated dates upon which the major milestones will be completed, and indicate the critical path.
* Identify the steps that will be taken to protect the Test Plan, results, and final deliverables.
* Coordinate the internal VAPT with Application / Infra POC.

# VAPT Checklist and Objective

#### End-to-End Security Testing

Is End-to-End Security Testing done for this Project?

Yes

No

\*If not, the project team must ensure the end-to-end testing scheduled before the product release.

#### Precautions

* Testing on production systems is not recommended.
* For application security testing on a production system, Automated scanning and DoS is prohibited unless the PT requests for an automated scan.
* Automated scans should be run with safe checks.
* Ask the PT to take back up of the databases / applications and settings if a scanning must be done on a production system so that if something goes wrong, it can be restored.
* It is recommended not to perform any other testing (functional testing, stress testing, etc.) during the security testing.
* Prior permission should be taken from the third party, to avoid any possible contractual violations while reverse engineering the application.

#### Testing Logistics

Connection through VPN

Accessible from Netradyne Network

Public access

VM installed in the Product Security lab

Installer sent to Product Security lab

The Physical system sent to Product Security lab

#### Pre-conditions to be meet.

Relevant Product/application documentation provided.

Product installation and Setup done.

Application accessible.

Demo and sample data given.

Approvals required for testing.

#### Test Suspension criteria

Testing may be suspended for a single functional area or the entire system if any of the following condition arises: -

* Explicitly asked by the PT.
* If defects of the systems negatively affect security testing.
* If any of the preconditions mentioned in the above section are not met.

#### VAPT Workflow

*VAPT Process Diagram*

#### Planning

In the planning phase, rules are identified, management approval is finalized and documented, and testing goals are set. The planning phase sets the groundwork for a successful penetration test. No actual testing occurs in this phase. The process starts with a Kick-off call with stakeholders to make them aware of the activities planned. Initiate a Jira ticket with timelines which will run till completion. For remediation of identified vulnerabilities, sub-tickets can also be raised.

#### Reconnaissance & Scanning

The next step is to understand how the target application will respond to various intrusion attempts. This can be done by performing reconnaissance of the asset under test to gather as much information as possible which helps in performing the VAPT activity. Scanning is performed to find the basic security vulnerabilities of the asset under test This is typically done using:

#### Dynamic analysis

Inspecting an application’s code in a running state. This is a more practical way of scanning, as it provides a real-time view into an application’s performance.

#### Static analysis

Static analysis is a process of evaluating application’s code without executing the application. This can be done only if the pen tester has access to the code base of the application.

#### **Discovery**

The discovery phase of penetration testing includes two parts. The first part is the start of actual testing and covers information gathering and scanning. Network port and service identification is conducted to identify potential targets. In addition to port and service identification, other techniques are used to gather information on the targeted network:

* Host name and IP address information can be gathered through many methods, including DNS interrogation, InterNIC (WHOIS) queries, and network sniffing (generally only during internal tests)
* Employee names and contact information can be obtained by searching the organization’s Web servers or directory servers.
* System information, such as names and shares can be found through methods such as NetBIOS enumeration (generally only during internal tests) and Network Information System (NIS) (generally only during internal tests)
* Application and service information, such as version numbers, can be recorded through banner grabbing.

#### Analysis and Exploitation

While vulnerability scanners check only for the possible existence of a vulnerability, the attack phase of a penetration test exploits the vulnerability to confirm its existence. Penetration testing teams follows OWASP top 10 for finding vulnerabilities.

#### Reporting

At the conclusion of the test, a report is prepared the vendor(external)/security analyst (internal) to describe identified vulnerabilities, present a risk rating, and give guidance on how to mitigate the discovered weaknesses. A brief executive summary is also prepared based on the detailed report as a reference to the leadership.

#### Review

After the detailed vulnerability report has been prepared, test team share the report with relevant Subject matter experts and stakeholders to review and confirm the reported vulnerabilities. Based on the review of the stakeholders, the report is modified accordingly if needed and published with all the stakeholders for remediation and tracking.

#### Tracking and Remediation

Once the vulnerabilities are remediated, the test team performs a final scanning of the application / assets under scope to verify the remediation of all the vulnerabilities. If any vulnerability is still identified as an open item, it is sent to the respective team for closure and the same is updated in the respective Jira ticket.

#### Final Scanning

Once the vulnerabilities are remediated, the test team performs a final scanning of the application / assets under scope to verify the remediation of all the vulnerabilities. If any vulnerability is still identified as an open item, it is sent to the respective team for closure and the same is updated in the respective Jira ticket.

#### Verification and Conclusion

Once the final vulnerability scan is performed on the assets and the verification of all the open vulnerabilities is done, a conclusion communication is sent to all the stakeholders.

#### VAPT Remediation Timeline

All the identified vulnerabilities during the VAPT assessment should be remediated within the timeline as per the PVM process. Below is the defined timeline for remediation of vulnerabilities:

|  |  |  |
| --- | --- | --- |
| **Vulnerability Severity** | **Remediation Timeline (Software)** | **Remediation Timeline (Firmware/Hardware)** |
| Critical | 5 Days | 3 Months |
| High | 30 Days | 6 Months |
| Medium | 3 Month | 12 Months |
| Low | 12 Months | 18 Months |

All the vulnerabilities that are not remediated as per the above-mentioned timelines are moved to the Netradyne risk register.

# Conduct

Compliance Checks to this process to be performed through various methods, including but not limited to reports, internal/external audits, Awareness training/assessments and feedback to the process owner. Non-compliance will be escalated to the Netradyne leadership team.

# Exception

Exception to this procedure must be approved through the Netradyne Exception Process.

# Terms/Acronyms

|  |  |
| --- | --- |
| **Term/Acronym** | **Definition** |
| PT | Product Team |
| TBD | To Be Disclosed |
| NA | Not Applicable |
| VAPT | Vulnerability Assessment and Penetration Testing |
| ISO | International Organization for Standardization |
| PHI | Protected health information |
| OWASP | Open Worldwide Application Security Project |
| PVM | Patch and Vulnerability Management |

# References

Templates

NA

Policies

[Netradyne Information Security Policy & Procedure.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/Netradyne%20Information%20Security%20Policy%20%26%20Procedure.pdf?csf=1&web=1&e=mRSIq4)

[Netradyne Information Security Exception Process.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/Netradyne%20Information%20Security%20Exception%20Process.pdf?csf=1&web=1&e=RbfEhO)

[Acceptable Usage Policy.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/Acceptable%20Usage%20Policy.pdf?csf=1&web=1&e=2jMnrk)

Standards

ISO 27001:2022

# Appendix A: Document RACI Matrix

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Role/Activity | Document Owner/Functional Area Lead | Document Contributor | ND Leadership | Functional Area Team | InfoSec | All ND Member(s) |
| Ensure document is kept current | A | R | I, C | R, C | C | I |
| Ensure stakeholders are kept informed | A | R | - | R | C | - |
| Ensure document contains all relevant information | A | R | I, C | R, C | C | I |
| Ensure document adheres to document governance policy | A, R | R | I | R, C | R, C | I |
| Provide SME advice | I, R | A, R | I | R, C | I, C | I |
| Gathering and adding document contents | I | A, R | I, C | R, C | C | I |
| Document Approval | A | R | I, R | I | I, R | I |

|  |  |
| --- | --- |
| Key |  |
| R | Responsible |
| A | Accountable |
| C | Consulted |
| I | Informed |