PENETRATION TESTING & VULNERABILITY SCANNING POLICY

Prepared by: Touchline Connect Pty Ltd

Last Modified: 07/03/2023

Contents

PURPOSE 3
SCOPE 3
POLICY GOALS 3
DEFINITIONS 4
PENETRATION TESTING ENGAGEMENT TYPES 5
1. Web Application testing 5
2. Social Engineering 5
3. Physical Testing 5
PENETRATION TESTING PERSPECTIVES 6
External Security testing 6
Internal Security testing 6
Routine & Frequency 6
ROLES & RESPONSIBILITIES 6
CEO/CISO 6
System Owner/Department Lead 8
Penetration Testing Lead Manager 8
Penetration Testing Team Members 9
COMMUNICATION PATHS 10
ACTIVITY SCOPE & LIMITATIONS 11
FRAMEWORKS & CYBER-THREAT INTELLIGENCE 11
RULES OF ENGAGEMENT 12
PRODUCTION SYSTEMS TESTING 12
PENETRATION TESTING PROCESS 13
INFORMATION GATHERING 13
EXPLOITATION 14
DOCUMENTATION & REPORTING 14
DOCUMENT HISTORY 15

PURPOSE

This policy framework document provides guidance for managing a penetration testing program and performing penetration testing activities with the goal of improving defensive IT security for REACH's infrastructure, systems, services, and applications. This document defines the roles and responsibilities of REACH's executives, managers, and IT security team personnel as well as external third-party security service providers.

This document also outlines a set of penetration testing activity terminology, definitions, scopes, limitations, and procedures that should be applied to ensure reliable and effective penetration test activities. This policy document also describes the high-level goals of REACH's penetration testing program as well as any formal requirements defined by REACH's responsibilities to its customers and partners through contracts, service level agreements, or compliance standards, and specific penetration testing activities that should be conducted to meet these goals and requirements.

SCOPE

The general scope of this policy applies to all equipment owned and/or operated by REACH, and to employees connecting to any REACH-owned network domains or cloud applications managed by REACH.

Defining the general scope of this policy ensures that penetration test activities are focused on relevant components and safeguard REACH against violating authorised system boundaries.

All penetration testing activity conducted on equipment owned or controlled by REACH must conform to all national and regional laws that govern the physical location of the asset and the nature of the data, as well as any acceptable use policy limitations imposed by the contracts and agreements between REACH and third-party infrastructure service providers and application licenses.

It should also be noted that this policy document does not provide a comprehensive definition of all scenarios, terminology, and activities that may be encountered during penetration testing activities. Therefore, all parties should also use their best judgment when performing pen testing activities and communication should be used to clarify any potentially conflicting situations.

POLICY GOALS

The primary goal of REACH's penetration testing program is to identify security gaps impacting the Confidentiality, Integrity, and Availability (CIA Triad) of all systems and data used by REACH.

Ultimately, the discovery of vulnerabilities shall facilitate risk remediation in line with internal corporate governance objectives. This includes meeting both internal risk objectives and external IT security standards including SOC-2 for the protection of customer personal data, and no further.

DEFINITIONS

Penetration Test

A penetration test is a simulated cyber-attack used to identify software vulnerabilities and security gaps, misconfigurations, and business logic flaws. The rest of this section defines key terminology and penetration testing types that may be encountered within this policy document or other related policy documents.

Activity

Activity refers to individual penetration testing processes that are conducted by the penetration testing team.

Engagement

A set of multiple penetration testing activities that comprise a single test defined by a specific service level agreement (SLA) and rules of engagement (RoE) documents and resulting in a single report.

Target

Any asset, infrastructure, device, network, application, or data that is within the scope of a particular penetration testing engagement.

White box tests

White Box tests are tests conducted by those with knowledge of the internal workings of target systems.

Grey box tests

Grey Box tests are tests conducted by those with some limited knowledge of the internal workings of target systems.

Black box tests

Black Box tests are tests conducted by those with no knowledge of internal workings.

Service level agreement (SLA)

A document related to a single penetration testing engagement that contains the level of service expected and may include metrics by which service is measured.

Rules of Engagement (RoE)

A document related to a single penetration testing engagement that contains the formal approvals, authorisations, scope, and other general guidelines or formal objectives necessary to execute a penetration testing engagement.

External tests

Security testing conducted from outside REACH's network security perimeter.

Internal tests

Security testing conducted from inside REACH's network security perimeter.

CIA Triad

CIA Triad to fundamental IT security components of Confidentiality, Integrity, and Availability.

PENETRATION TESTING ENGAGEMENT TYPES

The Reach penetration testing program will include the categories of testing engagements described below.

1. Web Application testing

Web application penetration testing is to identify any vulnerability, security flaws, or threats in web applications owned by REACH. Activities may use any known malicious attacks on the application including both manual and automated penetration testing activities.

The high-level goals of web-application penetration testing should include all vulnerabilities listed in the OWASP Top Ten web-application vulnerabilities, MITRE CWE software weaknesses, and attempt to evaluate the application's resilience against known attacker TTP included in the MITRE ATT&CK framework.

2. Social Engineering

Social engineering penetration testing is to increase security assurances to REACH's to business operations by testing personnel resilience to social engineering attacks and providing user awareness training where weaknesses are uncovered.

Social engineering penetration testing should include both technical and non-technical attempts to persuade or trick REACH's staff into performing actions that may reveal sensitive information. This should include both directly providing the sensitive information to an attacker, or performing actions that may result in giving an attacker access to sensitive information such as executing files provided by an attacker.

The high-level goal of social engineering pen testing activities is to educate personnel about the potential implications of the actions they perform in their day-to-day duties, and the various contexts in which a cyber-attack may involve them.

3. Physical Testing

Physical penetration testing seeks to gain access to restricted physical locations within REACH's buildings, critical IT infrastructure, systems, data, or employees. The primary benefit of a physical penetration test is to expose weaknesses and vulnerabilities in physical controls including but not limited to locks, elevators, barriers, surveillance cameras or systems, and access control technologies such as access card readers and biometric scanners.

These tests do not cover any third party providers who REACH uses in order to deliver the services outlined in the SLA for each customer.

The high-level goal of physical penetration testing is to eliminate security weaknesses that provide unauthorised physical access to REACH's assets.

PENETRATION TESTING PERSPECTIVES

Both internal and external testing will be performed in order to achieve the most comprehensive visibility into REACH network security resilience.

External Security testing

External security testing is conducted from outside REACH's network security perimeter — as seen from the Internet — to simulate the behavior of an attacker who has not penetrated the network or gained access to REACH's internal systems. This type of attack seeks to simulate the first stages of a cyber-attack where the attacker performs activities such as reconnaissance, passive or active scanning of the external attack surface, and weaponizing and deploying attacks that seek to gain initial access to REACH's network. The high-level goal of external penetration testing is to reduce the external attack surface of REACH's public IP endpoints and reveal as little information to attackers as possible.

Internal Security testing

Internal security testing is conducted from within the security perimeter and is meant to simulate a cyber-attack by a trusted insider or an attacker who has gained initial access to REACH's network. The high-level goal of internal security testing is to verify that a "defense in depth" approach is effectively protecting REACH's assets, systems, and data at all positions and layers within the network.

Routine & Frequency

Internal and external Penetration testing should be conducted randomly so that there is no system preparation undertaken to impact testing results.

Penetration testing is to be conducted at least twice per calendar year and no more than 8 months between each test.

ROLES & RESPONSIBILITIES

Maintaining a clear set of roles and responsibilities is critical for the execution of a reliable, effective, and efficient penetration testing program that is able to satisfy the program's intended goals and requirements.

The following section outlines the responsibilities of each stakeholder of the penetration testing program. These responsibilities include management of REACH's risk requirements, governance of the penetration testing program, scoping each penetration testing engagement, scheduling, and planning penetration testing activities, and ensuring that REACH's development and production systems and data are properly prepared for the penetration testing process.

CEO/CISO

The CEO and/or CISO is responsible for the overall governance of REACH's penetration testing program. This includes setting high-level goals and requirements and approving documents that grant the explicit permission for each pen testing engagement and outlines the expectations and limitations of each engagement. Under the direction of the CEO and/or CISO

specific target goals will be set including any compliance standard requirements that must be met by the penetration testing program's activities.

A summary of CEO and/or CISO responsibilities includes:

- Develops and relays the program's high-level goals and requirements.
- Develops the program's overall scope.
- Directs the development of the pen testing engagement schedule
- Outlines communication requirements for the program.
- Outlines the general requirements for pen testing SLAs and RoEs.
- Approves the pen testing SLAs and RoEs, schedule, budget, and types of pen testing engagements to be conducted.
- Signs each pen testing engagement SLA and RoE.

System Owner/Department Lead

The System Owner/Department Lead represents the IT system administrator who is responsible for the specific network, systems, and data targeted by a specific pen testing engagement. The System Owner/Department Lead is tasked with monitoring during the engagement and preparing the target environment for penetration testing activities by ensuring adequate failover servers and backups required for the restoration of systems to full functionality in the case of unexpected damage caused by penetration testing activities.

The System Owner/Department Lead is also tasked with provisioning any resources such as network access and user accounts required for the pen testing engagement.

A summary of System Owner/Department Lead responsibilities includes:

- Collects and manages system backups for all targets of a penetration testing engagement.
- Provisions and provides pen testers with network access to any required accounts.
- Provides pen testers with any required information for white-box or grey box tests.
- Defines an acceptable penetration testing time window for the target systems.
- Signs the rules of engagement RoE.
- Mitigation of vulnerabilities discovered during the pen testing engagement.

Penetration Testing Lead Manager

The Pen testing Lead Manager may be an internal employee of REACH or an assigned manager of a penetration testing engagement with a third-party penetration testing service provider and is responsible for planning and overseeing each pen testing engagement and penetration testing activities such that they adhere to the guidance provided by the pen testing frameworks listed below.

The ultimate responsibility of the Pen testing Lead Manager is to seek to identify all types of vulnerabilities within REACH's IT infrastructure that includes, but is not limited to those listed below. All planned and executed activities must be considered ethical, legal, and in line with

any existing contractual obligations and limitations between REACH and third-party service and infrastructure providers.

All penetration testing engagements will be explicitly approved by REACH's executive management including the Chief Executive Officer (CEO) and/or Chief Information Security Officer (CISO) prior to execution. This explicit permission will be formalised in an SLA that will be signed by members of REACH's executive management, the System Owner/Department Lead, the Pen testing Lead Manager, and all pen testing team members.

A summary of Pen testing Lead Manager responsibilities include:

- Manages the schedule of penetration testing engagements and related responsibilities.
- Selects and plans appropriate penetration testing activities based on each engagement's scope to meet the minimum requirements outlined in this document and any additional requirements specified by REACH's CEO and/or CISO executives.
- Develops appropriate RoE documents and submit them for approval by the CEO and/or CISO prior to pen testing engagement begins.
- Schedules meetings with pen testing team members to explain each engagement's SLA and RoE.
- Assigns specific tasks to penetration testing team members.
- Oversees penetration testing activities and ensures that activities are conducted properly.
- Ensures that evidence is collected and oversees the writing of reports to relay the findings uncovered by each pen testing engagement.
- Signs the SLA and RoE for each pen testing engagement.
- Ensures all penetration team members sign the required SLA and RoE for each pen testing engagement.

Penetration Testing Team Members

The Pen testing Team Members may be internal employees of REACH or direct employees of a third-party penetration testing service provider and are responsible for performing activities similar to those of a malicious actor with the purpose of simulating a real-world cyber-attack. All activities will be conducted ethically and must have explicit permission from the Pen testing Lead Manager who is acting on behalf of REACH's executive management including the CEO and/or CISO. This explicit permission will be formalised in a penetration testing service level agreement that will be signed by each individual Pen testing Team Member.

The summary of the general responsibilities of Pen testing Team Members include:

- Following the direction of the Pen testing Lead Manager.
- Performing and properly documenting penetration test activities.
- Compiling detailed information for each discovered vulnerability.

- Providing a risk score and rating for each discovered vulnerability.
- Compiling remediation recommendations for each discovered vulnerability.
- Verifying the remediation of each discovered vulnerability during retesting.
- Signing the required pen testing SLA and/or ROE

COMMUNICATION PATHS

During each pen testing engagement, it's important to ensure all parties involved are aware of REACH's pen testing communication policies. This protects the security of REACH's business operations during the pen testing process and supports the secure, reliable, effective, and efficient management of a pen testing engagement.

A summary of mandatory communication requirements during penetration testing engagements:

- Pen testing Lead Manager must have close communication with all assigned Pen testing Team Members throughout a pen testing engagement.
- All information including reports and emergency incident alerts communicated between the Pen testing Team Members and the System Owner/Department Lead should go through the Pen testing Lead Manager.
- Pen testing Team Members and Pen testing Lead Manager must have a direct line of contact during all penetration testing activities to enable an immediate response to potential critical security incidents, unexpected discoveries.
- In the case that a vulnerability is discovered with an actual or estimated CVSS score of 8.5 or higher, that information should be provided directly to the relevant System Owner/Department Lead within 24 hours of the discovery.
- After the completion of a pen testing engagement, Pen testing Lead Manager should provide the documented results to the System Owner/Department Lead in a timely manner to allow for the remediation of discovered vulnerabilities.
- After the completion of a pen testing engagement, Pen testing Lead Manager should provide the documented results to the CEO and/or CISO to allow a risk reassessment of business operations.
- After the delivery of reports the System Owner/Department Lead, System Owner/Department Lead, and CISO will meet directly to discuss remediation and review the management of any remaining vulnerabilities such as transferring or accepting the risk.
- After the full remediation of all vulnerabilities, the System Owner/Department Lead should notify the Pentesting Lead Manager so that retesting to verify the effectiveness of the remediation steps

ACTIVITY SCOPE & LIMITATIONS

Each penetration testing engagement has a scope that defines what is being tested and the engagement's limitations. Each engagement may also include specific requirements and contractual obligations such as service level agreements with REACH's customers, users, and compliance with formal IT security standards.

The scope of each engagement must also not fall outside of the bounds of any applicable national or regional regulations or REACH's contractual obligations. The scope should be developed into a formal RoE document by the Pen testing Lead Manager and approved by the CEO/CISO prior to the start of the engagement.

It is the responsibility of the Pen testing Lead Manager to translate the approved RoE into pen testing activities that are appropriate for achieving the high-level and engagement-specific requirements of each engagement.

Although the penetration testing frameworks and sources of cyber-threat intelligence listed below serve as a general starting point for scoping the design of penetration testing activities, in certain situations such as those described above, special consideration may be required when planning testing activities.

FRAMEWORKS & CYBER-THREAT INTELLIGENCE

The Pen testing Lead Manager is responsible for planning and implementing pen testing activities to verify that REACH's assets, systems, and data are resilient to common known vulnerabilities and attacks described in reliable IT security information repositories and penetration testing frameworks. This includes repositories of specific known vulnerabilities that have been identified in the hardware and software used in REACH's IT environment and other cyber-attack tactics, techniques, and procedures documented as threat actor methodology.

The lists below highlight some common examples of penetration testing methodology and sources of known vulnerabilities and cyber-attack strategies.

Relevant sources of standard penetration testing activity scope

- OWASP Testing Guide 4.1
- PTES Penetration Testing Execution Standard
- PTES-TG Penetration Testing Execution Standard Technical Guidelines

Relevant sources of vulnerability information

- CWE/SANS TOP 25 Most Dangerous Software Errors
- OWASP Serverless Top 10
- OWASP Top 10
- MITRE ATT&CK
- MITRE Common Vulnerability Enumeration (CVE)
- MITRE Common Weakness Enumeration (CWE)

RULES OF ENGAGEMENT

An RoE document for each pen testing engagement must be developed by the Pen testing Team Lead and submitted for approval by the CEO and/or CISO prior to the start of any penetration testing activity.

At a minimum RoE must contain the following information:

- The type of penetration test being conducted,
- A list of target systems with their IP address and hostname,
- Any limitations on the type of activities that can be used against the target systems,
- Any formal compliance standards that are being attested by the engagement,
- Contact information in case of an adverse event that causes damage to the target systems

For some engagements, regular meetings may also be scheduled between the System Owner/Department Lead and the Pentesting Team Lead and between the Pentesting team members and the Pentesting Team Lead to review engagement status reports issued by the testing team. These meetings can relay what vulnerabilities have been found up to that point and estimate the engagement completion time. The Owner/Department Lead can also relay whether IT security detection systems have issued any alerts resulting from the pentesting activities.

If sensitive information about the company, the system, and/or its users is discovered during the engagement, sensitive data handling procedures must be followed which should be formally documented in the RoE. These special procedures should include proper storage and communication measures that should be taken (for example, full disk encryption on the testers' computers, and encrypting reports if they are sent by email). Any applicable regulatory laws, data privacy laws, and formal contractual requirements may dictate that only authorised personnel view sensitive data.

PRODUCTION SYSTEMS TESTING

Special considerations are required for penetration testing Reach's production systems in addition to standard testing procedures. These special conditions are listed below.

- Ensure that fail-over servers are online and functioning normally prior to the start of testing activities.
- Monitor the availability of production systems during the penetration testing activities.
- Stop testing immediately and notify the Pen testing Lead Manager and System Owner/Department Lead immediately if unauthorised access is achieved on production systems.
- Stop testing immediately and notify the Pen testing Lead Manager and System Owner/Department Lead immediately if a previously unknown vulnerability on a production system with a CVSS V3 criticality rating above 7.0 (level high or critical) is discovered.

- Do not conduct any type of Denial of Service (DoS) attacks directly on production servers unless special authorisation has been granted by the CEO and/or CISO.

PENETRATION TESTING PROCESS

The pen testing procedure described in this document is used for testing and assessing the security posture of REACH's IT environment, information systems, and data. Each engagement should include activities within each phase of the testing process described in this policy to ensure that engagements produce a holistic and reliable set of findings. The results from each engagement should be organised into a report and used to remediate vulnerabilities and improve REACH's overall cyber resilience. Test findings should not be used to exclude other security processes.

Each pen testing engagement involves a testing process with four primary phases. These primary phases are described in the sections below.

INFORMATION GATHERING

The information gathering phase is intended to facilitate the discovery and recording of potentially exploitable vulnerabilities. Information gathering is critical to mapping the target system's attack surface.

The information gathering process should include methods of collecting data from publicly available sources of threat intelligence (also known as open source intelligence / OSINT) and from data sources that can be accessed from within REACH's internal network. The information gathering process will also include probing system entry points for flaws that can be used to generate errors, disrupt normal functions, gain unauthorised access to data, or gain control of a system.

During the information gathering phase, Pen testing Team Members must maintain documentation of all information collected as a record and accounting of the specific actions taken during the test for use in subsequent stages of the engagement and in the final report.

Information gathering activities should include but are not strictly limited to:

- Discovering OSINT that pertains to REACH and to the systems, software, and hardware that REACH uses
- Enumerating the public network interfaces/IP addresses of REACH's corporate network and REACH's cloud infrastructure
- Identifying system architecture and components within REACH's internal corporate network
- Mapping application flow and design
- Mapping internal business processes

EXPLOITATION

The exploitation phase is intended to determine whether vulnerabilities can be exploited in order to gain unauthorised access to systems and/or data. This phase depends on the information collected during the vulnerability discovery phase. During the exploitation phase, it is especially important to closely consider the established RoE and only perform activities that conform with the specifications outlined in that document.

During the exploitation phase, the Pen testing Team Lead and the Pen testing Team Members must maintain documentation of all information collected as a record and accounting of the specific actions taken during the test for use in subsequent stages of the engagement and in the final report. The System Owner/Department Lead should have access to all documentation during the pen testing process but are not authorised to remediate any of the discovered vulnerabilities until after the engagement window ends unless the engagement RoE has defined special circumstances.

Exploitation activities should include, but are not strictly limited to:

Business process/logic or design flaws:

- Registration flaws
- Account/password reset attacks
- Registration and account spoofing
- Input validation flaws
- Parameter manipulation
- Authentication bypass
- File, command, or script injection
- Privilege escalation
- Other forms of unauthorised access
- Social engineering attacks

Configuration flaws:

- Default access credentials
- Unauthorised access to administration commands, or systems
- Unpatched software and services
- Access relationship/token forgery
- Open service abuse
- Internal/shared configurations
- Unauthorised access to sensitive documents

DOCUMENTATION & REPORTING

The documentation phase is intended to provide a summary of findings and in-depth details about the findings. The final deliverable report will include a summary section that lists each testing activity conducted, the findings, and an analysis of the vulnerability's severity if a vulnerability was found. The final report will also include a main body that describes in-depth details for each vulnerability successfully exploited including specific steps taken to exploit the vulnerability, and evidence and links to any data that was accessed or other sensitive information that was gathered such as usernames and passwords, client certificates, or sensitive documents.

The description of an exploited vulnerability's severity should include a CVSS V3 severity rating, score, and vector string. The CVSS V3 rating, score, and vector string will be used to determine the ultimate risk to REACH's business operations. The final deliverable report will also include recommendations for mitigation or a technical solution for each exploited vulnerability.

The Pen testing Team lead should deliver each engagement's documentation and final report to the Owner/Department Lead and the CEO and/or CISO in a timely manner after the pen testing engagement activities have been completed.

DOCUMENT HISTORY

Date	Author	Notes
2023-03-07	Bradley J. Gibby CTO	Initial creation of document