EUROPEAN CENTRAL BANK

EUROSYSTEM

TIBER-EU

Red Team Test Plan Guidance

January 2025

Contents

1 Introduction

The Red Team Test Plan (RTTP) represents the overall plan for the active testing and describes which attack steps are to be performed, which techniques are planned to be used, when and how to provide leg-ups when milestones cannot be reached, as well as what flags to aim for at the target systems. As such, it provides the common base for the following test conduct for all stakeholders. It therefore serves as a starting point for the red team testers (RTT) to conduct the active testing.

1.1 Purpose of this document

The purpose of this document is to provide the relevant stakeholders with information on the requirements[1] for the content and format of a TIBER-EU RTTP. It also aims at providing guidance on important aspects to be considered during drafting as well as supporting material.

1.2 Target audience

This TIBER-EU guidance for the RTTP is mainly aimed at the RTT creating a RTTP in the scope of a TIBER test. Beyond that, it is useful to read for all stakeholders of a TIBER engagement to understand the nature of its content.

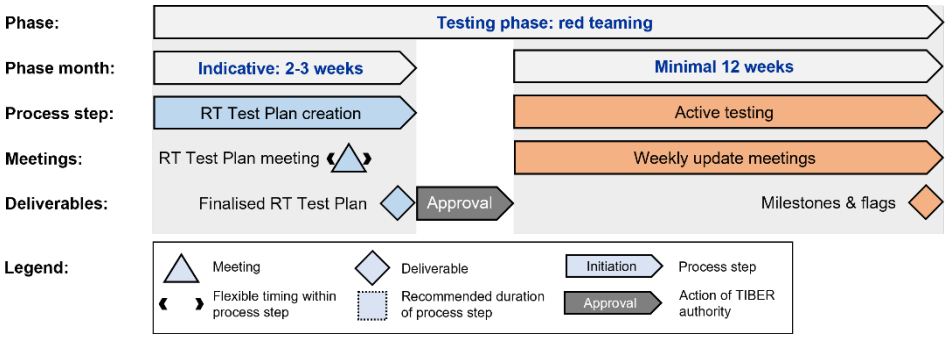
1.3 Location within testing process

The RTTP is to be drafted at the beginning of the testing phase in the RTTP process step.

[1] In addition to the minimum requirements for complying with the TLPT obligations under DORA, this document also includes operational TIBER-EU guidance based on best practices, knowledge and experience from numerous previous tests.

Figure 1[2]

RTTP creation process step



[2] Note that only the actions of the TIBER authority are included in the figure that have an impact on the timelines of the test. The figure is not an exhaustive overview of all actions to be undertaken by the involved stakeholders.

2 Required content of the RTTP

The RTTP shall include information on:

- communication channels and procedures to be used;
- the tactics, techniques and procedures (TTP) allowed and not-allowed for use in the attack, including ethical boundaries for social engineering, and how the privacy of involved parties is being safeguarded;
- risk management measures to be followed by the RTT;
- a description for each scenario, including:
    - the simulated threat actor;
    - their intent, motivation and goals;
    - the target function(s) and the supporting ICT system or systems;
    - the targeted confidentiality, integrity, availability and authenticity aspects;
    - the flags;
- a detailed description of each expected attack path, including pre-requisites and possible leg-ups to be provided by the control team (CT), including deadlines for their provision and potential usage;
- the scheduling of red teaming activities, including time planning for the execution of each scenario, at a minimum split according to the three phases a tester takes throughout the testing phase, respectively i) entering financial entities' ICT systems, ii) moving through the ICT systems and ultimately executing actions on objectives and iii) eventually extracting itself from the ICT systems (in, through and out phases);
- particularities of the financial entities' infrastructure to be considered during testing;
- if any, additional information or other resources necessary to the testers for executing the scenarios.

3 Considerations when drafting the RTTP

During the Targeted Threat Intelligence Report (TTIR) meeting, the threat intelligence provider (TIP) will provide a detailed explanation of the TTIR along with the threat scenarios for testing. The RTT should gain insights from this meeting and build on the TIBER-EU Scope Specification document (SSD) along with the TTIR to construct and finalise the RTTP. This information and documentation provides the evidential basis for designing and justifying the proposed RTTP and attack scenarios.

3.1 Organisation of the test

The RTT should ensure that its RTTP contains a dedicated section on the organisation of the test. When the RTT draft this section, they should use this chapter as a guide and at minimum cover the key points raised below. The section on the organisation of the test should provide the CT and the test manager (TM) with clarity on the RTT that will be employed to conduct it; the communication protocols for the test; and the overall risk management approach that will be taken by the RTT.

3.2 Red team composition

The RTT must meet the requirements set out in the TIBER-EU framework & Guidance for Service Provider Procurement. The RTT should disclose with full transparency the composition of the red team that will take part in the TIBER-EU test, setting out the experience of each team member and their specific roles and responsibilities in the test. A red team manager along with a deputy should always be appointed for the conduct of the test.

The RTT should ensure and document that the team has the competencies that match the scope. For instance, if most systems are Linux or Mainframe based, it would be beneficial if the RTT have experience within these systems. The RTT should provide some explanation for the selection of the team, and the rationale for specific skill sets contained within the team. Any changes to the RTT composition must be communicated in a timely manner to the TM and CTL, and included in a revised version of the RTTP.

The red team manager is the single point of contact for the CT, TM and TIP. However, to ensure that the RTT may always be reached, contact details for all RTT must be clearly disclosed.

3.3 Communication protocols

3.3.1 Code name

Throughout the RTTP, the RTT should use the code name assigned to the test instead of the real name of the entity.

3.3.2 Communication channels

The RTT should indicate in the RTTP how they are planning to keep the stakeholders (i.e. CT, TMs and TIP) updated during the testing process. All communication must be conducted via secured channels, for example, end-to-end encrypted chat and email. During active communications in the test, the participants should refer to the test by its codename instead of the entity name to minimize risk in case of communication leaks. In addition, all communication between the RTT, CT and TM should be safely stored in order to ensure evidence of approval(s) and communication conducted via secure channels.

Throughout the active red team testing phase, the RTT report on the progress made during status meetings, which are held at least on a weekly basis and involve the RTT, CT, TM, and the TIP as optional participant. It is highly recommended to ensure the arrangement of multiple additional meetings on a weekly basis to ensure and facilitate the necessary information flow. Such meetings should ideally be held daily.

Furthermore, during the test the RTT may need to communicate directly, immediately and urgently with the CT. For example, before advancing further in the test to achieve a flag or in case an issue arises.

The Red Team Test Report (RTTR) should clearly set out how, when and in what circumstances communication will be conducted between the different stakeholders.

3.4 Risk management

In the RTTP, the RTT should set out details of their risk management approach. The risk management approach should set out how the RTT will take the appropriate actions before, during and after the test. The RTT should liaise with the CT to confirm the intended risk management approach.

For example, in the RTTP, the RTT should share all infrastructure, domain names, hashes, emails (i.e. so called indicators of attack), used by the RTT, with the CT and TM before the test starts – to the extent possible at this stage. This will allow the CT to differentiate between the TIBER test and potentially real attacks, allowing the CT to take the appropriate steps to manage a potentially real cyber-attack. RTT should share the details with the CT on the risk management approach taken on securing the Red Team infrastructure set-up before start of the test. This includes:

- guardrails in place to secure RTT's infrastructure;
- the location of the RTT's infrastructure;
- the security considerations that are in place during exfiltration of the data from the entity.

This is to make sure the RTT infrastructure or any other assets used as part of the Red Teaming activity are protected. The RTTP should include the tactics, techniques and procedures (TTP) which are allowed and prohibited for use in the attack, including ethical boundaries for social engineering, and how the privacy of involved parties is being safeguarded.

Furthermore, the RTT should set out instructions in the RTTP, which provide insight on what the CT should or should not do during the test. For example, the RTT should indicate that the CT must refrain from visiting certain domains, as this may alert the BT.

Finally, the RTT should set out how they intend to log all their actions during the test, and how it will secure and use this information after the test, e.g. in the RTTR and the replay exercise. RTT should follow the process of deleting all the sensitive artefacts of the entity from the RTT's workstation and red team infrastructure on completion of the final deliverables.

3.5 Leg-up process

During the testing process, the RTT may be unable to progress to the next stage owing to time constraints, business knowledge constraints or because the entity has been successful in protecting itself. In such scenarios, the RTT, with agreement from the CT and TM, may be given a leg-up. This means that the entity gives the RTT assistance or information (e.g. access to its system, internal network, devices or any additional information on target systems and technology) to allow the RTT to continue with the test and focus on the next flag/target where they are not able to advance on their own, and where no other reasonable alternative exists. The CT, TM and TIP should be consulted regarding the preparation and use-cases for leg-up activation. The leg-ups may exceed beyond the aforementioned access, whereas the CT is free to determine the nature of the leg-ups.

The RTT should discuss with the CT, TIP and TM the process for leg-ups and the circumstances in which they will be granted, ahead of the test. An early discussion will allow the test to progress more smoothly and efficiently, without potential delays. Following this discussion, the RTT should clearly set out in the RTTP the process for invoking leg-ups and the potential scenario-related leg-ups that will be needed. This information will allow the CT to take the appropriate steps in preparation for granting the leg-ups. It is essential that the CT is well prepared, in advance of the test, to invoke the agreed upon leg-ups, so the test can run smoothly and efficiently.

3.6 Attack phase planning

Due to the complexity of a TIBER test, it is essential that the RTT and CT plan for the test, and have a clear planning in place, to ensure a successful completion. The plan should be prepared as early as possible, and should illustrate any relationships between the different scenarios and the dependencies on leg-ups to visualize the orchestration of the test. The creation of a more structured and perspective timeline will enhance the opportunity to capture all the prescribed flags by the RTT. If the RTT is not able to get to the next phase or flag within the test time, they can request the envisioned leg-up.

In this section of the RTTP, the RTT should also provide a general timeline that is used for the execution of the scenarios. At a minimum, timelines should be divided according to the 'in, through and out' phases a tester takes throughout the testing phase. This timeline should include inter alia the key milestones, dates of meetings, activities and deliverables. This may be represented in the form of an illustration to provide a clear and accessible overview. The minimum time span of the active red team test is 12 weeks (which excludes RTTP creation and report writing of the RTTR), although this could be longer depending on the specificities of the entity.

Information that is shared by the CT, as part of a grey-box approach, should be indicated at a high level in the RTTP, including any particularities of the financial entities' infrastructure to be considered during testing. If any, additional information or other resources necessary to the testers for executing the scenarios. The RTT should set out how it envisages to conduct the test, step-by-step, in a timeline. The timeline should be clear and should include the key milestones, dates of meetings, activities, deliverables, etc. The project plan should also illustrate any relationships between the different scenarios and the dependencies on leg-ups in order to visualize the orchestration of the test.

It is important that the RTT can map timelines to flags and end goals, although the timelines may change during the test due to the unpredictability of a TIBER test. Setting out more structured and prescriptive timelines ensures that the RTT can attempt to capture all the prescribed flags. As the timelines are likely to change during the test, the CT and RTT can align expectations and ensure the right amount of time is spent on respective activities, ensuring all important parts of the entity are tested, as is expected and required in a TIBER test. This more prescriptive timeline will also allow the CT to highlight issues that may interfere with test activities. For instance, freeze periods or test activities on specific infrastructure that collides with internal deliveries like quarterly financial statements.

3.7 Attack scenarios

The core elements of the RTTP are the attack scenarios. The attack scenarios are written from the attacker's point of view and should define the concrete targets to be reached (i.e. the flags to be captured), and can be executed in sequence or in parallel, but must be independent from each other. The RTT should indicate various

creative options in each of the attack phases based on various TTPs used by advanced attackers to anticipate changing circumstances or in case the first option does not work. The scenario writing is a creative process.

The TTPs do not simply reflect real-life attacks seen in the past but combine the techniques of the various relevant threat actors. It is common for the RTT to include more than one threat actor in some scenarios, as some threat actors have similar motivations and/or objectives, and hence it is possible to include additional test activities and for the RTT to have more freedom in selecting the attack methods based on a broader set of TTPs.

The attack scenarios are predicated on the threat scenarios derived from the TTIR, selected in the scenario selection meeting. The RTT should apply the following methodology when developing the attack scenarios. In this regard, please also refer to the TIBER-EU Targeted Threat Intelligence Report Guidance.

During the finalisation of the TTIR, which brings together the CT, TM and TIP/RTT, the stakeholders should finalise the scope and flags. Based on the finalised flags, the RTT should develop appropriate attack scenarios related to each flag.

In the RTTP, the RTT should clearly explain, for each attack scenario, in addition to a detailed description for each expected attack path and killchain:

- **Critical or important functions (CIF), the supporting ICT systems and flags**: The relevance of the critical or important function being tested, and how the flag/objective relates to the critical or important function and its underlying systems and services.

- **Simulated threat actor, their motive, intent and goals**: Based on the collected threat intelligence in the TTIR, elaborate in further detail and more precisely what the motives, intent and goals of the threat actors are; how they would seek to target the specified CIFs; which of the CIA triad (Confidentiality, Integrity, Availability) they would seek to compromise; and how they would focus their efforts on achieving the final flags.

- **Tactics, techniques and procedures (TTP)**: What tactics, techniques and procedures the threat actor would use to achieve the specific flags. These TTPs should be set out in line with the **MITRE ATT&CK Framework**[3]**.** In some cases, the implementation of the framework (TIBER-XX) may also include using TTPs which look to breach the physical security of the entity to gain access to the network or plant a device.

- **Leg-ups**: The potential leg-ups that will be required in case the RTT are unable to achieve the flag/objective within its specified timeline (as prescribed in the project plan). For each leg-up, the RTT should clearly state what it entails, who is responsible for granting it by which deadline, and what process and protocol must be invoked to use the leg-up.

[3] https://attack.mitre.org/

- **Risk management controls**: The risk management controls that the RTT will have in place to manage any risk stemming from implementing the attack scenario. Due to the inherent risk in conducting a TIBER test, it is essential that the RTT applies appropriate controls for each attack scenario and communicates these to the CT.

- **Scenario X:** in addition to these scenarios, an RTT may develop other types of scenarios. In many cases, the use of conventional TTPs may not be successful in achieving a target or may be easily discovered by the blue team (BT) based on known intelligence or based on the RTT's knowledge obtained before or during the test, which might deem the techniques as obsolete. Therefore, to emulate a real-life attacker in such a case, the RTT could deploy creative and innovative TTPs. The RTT can leverage its full range of professional knowledge, research, expertise and tools to build forward-looking scenarios based on TTPs that have not yet been seen but are expected in the future.

The RTT should, if possible, set out clearly other possible attack scenarios it wants to apply in case of need during the test. This should be described and accounted for in the RTTP and consulted with the TIP. Moreover, depending on the nature of the test and its progress in real time, the RTT may deviate from the TTPs, remaining agile and dynamic. However, it is not always possible to document these deviations in advance. The RTT should retain a degree of flexibility to improvise during the test, even if the TTPs are not included in the RTTP.

4 Drafting format

The TIBER-EU RTTP might be drafted in any preferred format, provided that all required information is included. All content that needs to be provided in order to complete this document is indicated in Chapter 2.

© European Central Bank, 2025

Postal address 60640 Frankfurt am Main, Germany
Telephone +49 69 1344 0
Website www.ecb.europa.eu

All rights reserved. Reproduction for educational and non-commercial purposes is permitted provided that the source is acknowledged.

For specific terminology please refer to the ECB glossary (available in English only).

PDF ISBN 987-xx-xxx-xxxx-x, ISSN xxxx-xxxx, doi:xx.xxxx/xxxxxx, QB-xx-xx-xxx-EN-N
HTML ISBN 987-xx-xxx-xxxx-x, ISSN xxxx-xxxx, doi:xx.xxxx/xxxxxx, QB-xx-xx-xxx-EN-Q