EUROPEAN CENTRAL BANK

EUROSYSTEM

TIBER-EU

Guidance for the Red Team Test Plan

July 2020

Contents

1 Introduction

1.1 Purpose of this document

Following completion of the targeted threat intelligence process, the red team (RT) provider takes the lead. During the red team testing phase, the RT provider plans and executes a TIBER-EU intelligence-led red team test of the target systems and services that underpin each critical function in scope. This is followed by a review of the test and issues arising.

Prior to the commencement of the test, the TI provider must have a handover session with the RT provider, providing a detailed explanation of the Targeted Threat Intelligence (TTI) Report and discussing possible threat scenarios for the testing. The RT provider should gain insight from this handover meeting and further review the TIBER-EU Scope Specification, the GTL Report (if produced) and the TTI Report to finalise the Red Team Test Plan. This information and documentation provides the evidential basis for designing and justifying the proposed Red Team Test Plan and attack scenarios.

The TIBER-EU Guidance for the Red Team Test Plan aims to provide RT providers with a standardised approach and structure for producing the Red Team Test Plan, focussing on how to: organise the testing phase; plan the organisation and management of the test; and develop the attack scenarios, which build on the threat scenarios from the TTI Report. The Red Team Test Plan is a key document that helps inform the White Team and TIBER Cyber Teams (TCTs) involved in the TIBER test of the attack scenarios, the risk management controls that will be applied to ensure a safe and controlled test, the overall project plan which will allow the White Team to adjust its own project plan (if required) and to ensure the attacks are intelligence-led with indication of the intent and capabilities of the threat actor(s).

The Red Team Test Plan has to be agreed by the White Team of the tested entity and approved by the TIBER Cyber Team (TCT). For more detail on the overall processes in a TIBER test, please consult the TIBER-EU Framework[1] and related TIBER documentation.

1.2 Who is this document for?

This TIBER-EU Guidance for the Red Team Test Plan is aimed at:

- White Team of the entity undertaking the TIBER test;
- Threat intelligence provider and Red team provider.
- TIBER Cyber Teams (TCTs) involved in the TIBER test;

[1] https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

1.3 Structure of this document

This document is structured as follows:

- Section 2: Organisation of the test;
- Section 3: Project planning;
- Section 4: Attack scenarios; and
- Section 5: Approach of the red team provider.

Due to the sensitive nature of the information contained within the Red Team Test Plan, once complete, it should be handled and treated as highly confidential and stored in a manner commensurate with this classification (e.g. TLP Amber).

2 Organisation of the test

The RT provider should ensure that its Red Team Test Plan contains a dedicated section on the organisation of the test. When the RT provider drafts this section, it should use this chapter as a guide and cover, at the very least, the key points raised below. The section on the organisation of the test should provide the White Team and the TCT with clarity on how the team that will be employed to conduct it; the communication protocols for the test; and the overall risk management approach that will be taken.

2.1 Team composition

The RT provider 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. The Red Team must meet the requirements set out in the TIBER-EU Services Procurement Guidelines.

The RT provider should select a team that has the competencies that match the scope. For instance if most systems are Linux or Mainframe based, it would be beneficial if the RT team has experience within these systems. The RT provider should provide some explanation for the selection of the team, and the rationale for specific skill sets contained within the team.

The Red Team Test Manager is the single point of contact for the White Team, TCT and TI provider, and the contact details must be clearly disclosed.

2.2 Communication protocols

2.2.1 Code name

Throughout the Red Team Test Plan, the RT provider should use the code name assigned to the entity instead of the real name of the entity.

2.2.2 Communication channels

The RT provider should indicate how they are planning to keep the stakeholders (i.e. White Team, TCT and TI provider) 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 entity by its codename instead of the real name to minimize risk in case of communication leaks.

There can be different lines and frequencies of communication during the test. Often the White Team gets more detailed information on a more frequent basis (e.g. daily), whilst the TCT is kept up-to-date about the progress of the test on a weekly basis. Furthermore, during the test the RT provider may need to communicate directly, immediately and urgently with the White Team, for example, before advancing further in the test to achieve a flag or in case an issue arises.

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

2.3 Risk management

In the Red Team Test Plan, the RT provider should set out details of its risk management approach. The risk management approach should set out how the RT provider will take the appropriate actions before, during and after the test.

For example, in the Red Team Test Plan, the RT provider should share all infrastructure, domain names, hashes, emails (i.e. so called indicators of attack), used by the RT provider, with the White Team and TCT before the test starts. This will allow the White Team to differentiate between the TIBER test and potentially real attacks, and allow the White Team to take the appropriate steps to manage a potentially real cyber attack.

Furthermore, the RT provider should set out instructions in the Red Team Test Plan, which provide insight on what the White Team should or should not do during the test. For example, the RT provider should indicate that the White Team must refrain from visiting certain domains, as this may alert the Blue Team.

Finally, the RT provider should set out how it intends to log all its actions during the test, and how it will secure and use this information after the test, e.g. in the Red Team Test Report and the Replay session.

2.4 Leg-up process

During the testing process, the RT provider 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 RT provider, with agreement from the White Team and TCT, may be given a “leg-up”, where the entity essentially gives the RT provider access to its system, internal network, etc. to continue with the test and focus on the next flag/target.

The RT provider should discuss with the White Team and TCT 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, without potential delays. Following this discussion, the RT provider should set out clearly in the Red Team Test Plan the process for invoking leg-ups and the potential scenario-related leg-ups that will be needed. This information will allow the White Team to take the appropriate

steps in preparation for granting the leg-ups. It is essential that the White Team is well prepared, in advance of the test, to invoke the agreed upon leg-ups, so the test can run smoothly and efficiently.

3 Project planning

Due to the complexity of a TIBER test, it is essential that the RT provider and White Team plan for the test, and have a clear project plan in place, to ensure a successful implementation. In this section of the Red Team Test Plan, the RT provider should provide a general timeline that is used for the execution of the scenarios. The time span of the Red Team test should be approximately 10-12 weeks, although this could be longer depending on the specificities of the entity.

The RT provider 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.

Although the timelines will change during the test, due to the unpredictability of a TIBER test, it is important that the RT provider can map timelines to flags and end goals. Setting out more structured and prescriptive timelines will allow the Red Team to ensure that they can attempt to capture all the prescribed flags and if the Red Team is not able to get to the next phase within the set test time, they can request a “leg up”. This will ensure that the overall test is more efficient and value-added to the entity.

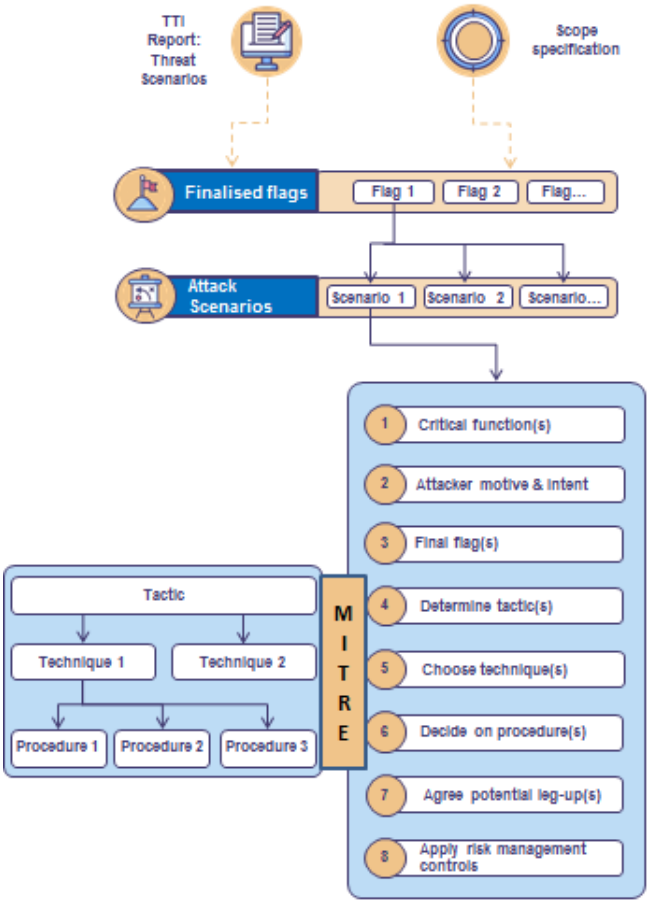
The timelines are likely to change during the course of the test and it is important that the White Team and RT provider can align expectations and ensure the right amount of time is spent on respective activities, ensuring all important parts of the test are tested as expected and required to be accepted as a TIBER test. This more prescriptive timeline will also allow the White Team to highlight issues with test activities that might interfere with, for instance, freeze periods or test activities on specific infrastructure that collides with internal deliveries like quarterly financial statements.

4 Attack scenarios

The core parts of the Red Team Test Plan 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). The RT provider 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 mimic scenarios seen in the past, but combine the techniques of the various relevant threat actors. It is common for the RT provider to suggest more than one threat actor for 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 RT provider 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 TTI Report, and RT providers should apply the following methodology when developing the attack scenarios:



During the handover of the TTI Report, which brings together the White Team, TCT and TI/RT providers, the stakeholders should finalise the scope and flags. Based on the finalised flags, the RT provider should develop appropriate attack scenarios related to each flag.

In the Red Team Test Plan, the RT provider should clearly explain, for each attack scenario:

Critical functions: The relevance of the critical function being tested, and how the flag/objective relates to the critical function and its underlying systems and services.

Attacker motive and intent: Based on the collected threat intelligence in the TTI Report, elaborate in further detail and more precisely what the motives and intent of the threat actors are; how they would seek to target the specified critical functions; which of the CIA triad they would seek to compromise; and how they would focus their efforts on achieving the final flags.

Tactics, techniques and procedures (TTPs): 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.**[2] 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.

In addition to these scenarios, an RT provider 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 based on known intelligence or based on the RT provider's knowledge obtained before or during the test, which might deem the techniques as obsolete; to emulate a real-life attacker in such a case, the RT provider could deploy creative and innovative TTPs, stretching itself to its absolute limits. The RT provider 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 RT provider should, if possible, set out clearly other possible attack scenarios it wants to apply in case of need during the test. Differences in approaches are expected and are quite common but should be described and accounted for in the Red Team Test Plan and the TI provider should be consulted. It should be noted that during the test, the RT provider may deviate from the TTPs, remaining agile and dynamic, depending on the nature of the test and its progress in real time. It is not always possible to document these deviations in advance, and the RT provider should retain a degree of flexibility to improvise during the test even if the TTPs are not included in the Red Team Test Plan.

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

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

leg-up. It should also illustrate any relationship between the different scenarios and show dependencies on leg-ups in order to visualize the orchestration of the test.

Risk management controls: The risk management controls that the RT provider 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 RT provider applies appropriate controls for each attack scenario, and communicates these to the White Team.

5 Approach of the RT provider

The TIBER-EU Guidance for the Red Team Test Plan aims to provide a standardised approach to develop the Red Team Test Plan. The RT provider should use the Scope Specification document and the TTI Report as a basis for producing the attack scenarios.

RT providers will differ in their approaches and their documentation. The TIBER-EU Guidance for the Red Team Test Plan does not aim to prescribe how RT providers should format their reports, but aims to provide a structured approach to the testing phase.

The **Attack scenarios** section aims to provide a logical approach to determining the attack scenarios for the test, and ensure that the output is detailed and useful for the Red Team that will execute the test in a safe and controlled manner.

The final Red Team Test Report should provide detailed sections on: the organisation of the test; the project management planning; the attack scenarios; and the risk management measures that the RT provider will apply to ensure safety.

The red team testing phase will take approximately 12 weeks, and must be conducted by RT providers that meet the requirements set out in the TIBER-EU Services Procurement Guidelines.

The RT provider is expected to liaise and work with the TI provider throughout the testing in order to update the threat intelligence assessment and attack scenarios with relevant and up-to-date intelligence. Lastly, the RT provider is expected to work with the TI provider in order to design and deliver the final report issued to the entity.

Finally, the RT provider makes it explicit that they will apply creative freedom during their testing, which may entail deviating from the attack scenarios, as long as they are generally in line with the TTPs of the mimicked threat actor.

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

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