NORGES BANK

TIBER-NO
Leg-Up Guidance

Version 1.1

TLP:AMBER

Change log

Version	Date	Change
1.1	04.05.2023	Updated leg-up code syntax and fixed language errors.
1.0	21.04.2023	Initial version distributed to ongoing tests.

About

This document serves as a guide to the White Team, Threat Intelligence provider and Red Team provider in understanding the concept of leg-ups, what leg-ups are available, which are to be avoided, identifying possible leg-ups for TIBER-NO tests, and defining their criteria for activation. In addition, some examples are provided, and special considerations are described for certain leg-up types.

1 Introduction

In a TIBER test, the Red Team provider is subject to multiple limitations. The two most significant limitations encountered during TIBER tests is the time-boxed nature of the test and the grey-box approach to testing, leaving the Red Team often uninformed of the security controls implemented by the entity. Other limitations are the legal and ethical boundaries, which the Red Team must adhere to. Due to such limitations, it is likely the Red Team might face difficulties in executing a scenario as planned. The concept of leg-ups involves the activation of measures which enables the Red Team to proceed with scenarios.

A leg-up can be defined as an action through which the White Team assists the Red Team in executing an action in a proposed threat scenario. Leg-ups serve to maximize the value of a TIBER test as they allow the Red Team to proceed further in executing the scenarios, ultimately achieving learning and improvements for the entity.

2 Leg-up reasons and types

Leg-ups strongly depend on the scenarios being executed by the Red Team and therefore exist in many shapes and forms. Below, some information is given for each leg-up category and common leg-ups are listed together with some tips on their preparation.

In short, these are the reasons for providing leg-ups:

- **Time saving leg-ups – bypassing time constraining tasks**
- **Resource saving leg-ups – bypassing resource constraining tasks**
- **Ethical limitation leg-ups – compensating for stricter RT ethical boundaries**

Within these reasons, there are multiple types of leg-ups:

- **Information leg-ups – providing information about systems**
- **Access leg-ups – providing access to systems or accounts**
- **Assistance leg-ups – providing assistance for physical tasks**

Leg-ups should be applied in a prioritized order. Informational leg-ups are therefore preferred before access leg-ups, as they provide the RT less help than the other alternatives.

2.1 Leg-up reasoning

This section explains the main reasoning behind leg-ups, meaning why they are to be used, describing what they are compensating for. In short, this is time, resources or ethical limitations.

2.1.1 Time saving

Given the time-boxed nature of a TIBER-NO engagement, the Red Team has a limited time to perform the actions and TTPs defined in the scenario. In contrast, the real threat actors the Red Team tries to emulate do not have the same limitations. To account for these limitations and aid the Red Team in executing the scenario, a time saving leg-up can be activated. A time saving leg-up is not strictly necessary for the Red Team to continue the test but serves to expedite the execution of the test. Time saving leg-ups can and will likely include information and access leg-ups, but their goals might differ.

2.1.2 Resource saving

Threat actors often have significant resources, or financial capability to acquire such resources on demand. The Red Team can be far more limited in their resources or ability to aquire them, and these limitations cannot be enforced on real threat actors. To account for this, the RT can be aided to simulate. A typical example of a resource saving leg-up is providing access to the plaintext equivalent of a cracked password hash, given that the RT would have to spend a significant amount of money or computing time to achieve the same result a threat actor would.

2.1.3 Ethical limitations

The Red Team operates within specific ethical boundaries and guidelines which the simulated threat actor might not have. Threat actors frequently use pretexts for phishing, causing harm. Another example is setting off the fire alarm in a physical intrusion to evacuate the building. The Red Team cannot perform these actions within ethical boundaries, as they cause the entity either risk or unacceptable negative consequences, even if these actions would be realistic in the simulation of a threat actor or real attack. Therefore, an argument of ethical limitations can be applied to reason for leg-ups.

2.2 Leg-up types

2.2.1 Information leg-ups

In TIBER test information on the target is unavailable to the Red Team. What information is provided to the Red Team and how much is decided by the entity's White Team. In general, entities with a more complex structure and business process will provide more information upfront, making sure the Red Team understand the business and the flags they need to capture. The White Team can also choose to withhold some information from the Red Team, to see what the Red Team can discover on its own. More information can be provided to the Red Team on an as-needed basis throughout the test in the form of information leg-ups. Some examples of information leg-ups are listed below:

Example	Description
Software & versions used	The White Team can choose to provide the Red Team with information on the software used by the tested entity. This allows the Red Team to finetune their attacks and payloads so that they would have a higher chance of compromising the target.
Security controls in place	The White Team can inform which security controls are in place such that the Red Team can adjust their approach accordingly.
Target identification	Once access to the internal network is obtained, the Red Team will try to enumerate the network to identify interesting targets for advancing in the execution of the scenario. Internal networks can be vast and finding the right targets is often not straightforward. The White Team can therefore disclose interesting targets on the network.
General information	Like the target identification leg-up, the WT can provide any information to the Red Team to save them the time of searching for the information. The idea is that the Red Team would eventually find the information themselves if given enough time or resources.

2.2.2 Access leg-ups

Access leg-ups can be considered the most far-reaching type of leg-ups. With an access leg-up, the White Team would grant the Red Team access to (a part of) the internal network. In most cases, an access leg-up completely bypasses the IN-phase of a TIBER-NO test, moving to a more insider scenario. Nevertheless, insider scenarios are no less valid than and outside attack and testing of the internal network controls is an important part of every TIBER-NO assessment. The level of access granted to the Red Team can vary, as indicated by the examples listed below.

Example	Description
Access to computer devices	This leg-up involves providing access to a physical or virtual computer device, typically a user laptop / workstation.
Valid low-privilege user account	In case the perimeter security controls of the institution are sufficiently strong, and the Red Team is not able to gain a foothold on the internal network, the Red Team can be given access to a normal, low-privilege user account. This allows the test to move from the in-phase to the through-phase. Some scenarios (insider scenarios) can also require the Red Team starts testing from inside the internal network, requiring the preparation of this leg-up well before the actual start of the test.
Valid high-privilege user account	This leg-up can be granted when the Red Team fails to escalate privileges starting from a low-privilege user. However, some scenarios (e.g. supply chain attack) require the Red Team to start with a high-privilege user. Implant: Besides the provision of a user account, the Red Team can be granted access to the internal network directly by means of a physical implant. In this case, the Red Team can configure a physical implant with outbound communication capability (such as Bluetooth, or 4G). The White Team would then plug in the implant directly into the network.
Remote access	Providing the Red Team with remote access to the internal network does not always require the provision of a valid user account or implant. Other possibilities exist such as shipping a locked laptop to the Red Team (simulating the theft of a user laptop).

2.2.3 Assistance leg-ups

Assistance leg-ups typically provide access, so they do to some extent overlap with access leg-ups but are nonetheless distinct. Assistance leg-ups involve compensating for the lack of physical access or a physical task not easily performed by the Red Team.

Example	Description
Accomplice clicker	Compensates for the assumption that phishing will eventually succeed, thus saving time, and providing the RT with access. This leg-up involves the White Team using its access to aid the Red Team. In general, the White Team would consciously run a payload developed by the Red Team on a workstation or server connected to the internal network. This leg-up does not necessarily grant the Red Team access to the internal network.
Planting device	Compensates for the lack of physical access or having recruited an insider for the task.

3 Leg-ups to avoid

As elaborated above, the aim of a leg-up is to aid the Red Team to proceed in executing the scenario, resulting in more learning opportunities for the concerned institution. A leg-up therefore adds value to a TIBER-NO test. When granting a leg-up to the Red Team, this must be carefully considered. Some leg-up actions do not necessarily correspond to this goal of improving the learnings of the test or could make the test no longer representative. The use of such “leg-up” actions is therefore not permitted in a TIBER-NO engagement. Below, some examples are given of actions that are not allowed in a TIBER-NO test.

Leg-up action	Description
Disabling security controls	Disabling security controls would degrade the security posture of the entity. The test would no longer reflect the real capability of the entity and invalidate test results.
Direct access to flags	If a leg-up grants the Red Team direct access to a flag, no additional learning can be achieved. Note: This leg-up action is still possible in case of intermediate or lower value flags, (e.g., access to a specific set of credentials) as the scenario would not be completed, and some testing activity can still be performed by the Red Team.
Direct access to critical privileged accounts where risk for business impact is considerable	Some leg-ups proposed by the Red Team might give access to critical systems where uncontrolled actions can cause significant business impact. In general, such leg-ups can be allowed given the WT has sufficient knowledge of the system so the test can continue in a controlled manner. If the WT is unsure of its ability to adequately guide the Red Team on these critical systems, the WT can be extended with a subject matter expert (SME) to provide guidance.

4 Leg-up activation guidance

The main goal of a leg-up is to account for the limitations encountered by the Red Team where threat actors emulated by the Red Team have no such limitations, making the concept of leg-ups very useful in a TIBER context. Activating a leg-up, allows the Red Team to bypass these limitations and execute the scenario in a realistic way. Leg-ups can also go much further than just accounting for the differences between Red Team and real threat actors. A leg-up can be granted anytime the Red Team encounters difficulties in executing the scenario as planned. However, before making the decision to activate a leg-up, some considerations must be made.

4.1 When to activate leg-ups

One of the most important considerations to make when activating a leg-up is whether the leg-up could facilitate additional learning in the TIBER-NO test. If the leg-up does not enable the Red Team to further the execution of a scenario, or no additional learning can be achieved by the entity, there is no real use in activating a leg-up.

A consideration to make is whether the scenario being tested should cover the phases IN, THROUGH, OUT. If a dependent phase cannot be achieved, a leg-up can be provided to progress testing to the next phase, and thus ensure the testing of scenario covers all three phases.

4.2 How to activate leg-ups

Leg-ups should be anticipated as far as possible in time as some leg-ups might have to be prepared. It can occur unforeseen leg-ups are required. The WT should strive to accommodate this. Typically, a meeting between WT, RT and TCT is held to discuss any requests for new leg-ups and requirements for activating them, as well as solving the practicalities of activating any potential leg-ups.

4.3 Requirements for leg-up activation

The TIBER-EU framework and the TIBER-NO implementation specifies both the WT and the TCT must approve any leg-ups before activation.

Any leg-ups the White Team decides to activate must be documented in the final Red Team report and the Test Summary report. Documenting the leg-up allows for better framing and validation of the test results. It helps in the prioritization of remediation actions to be taken once the TIBER-NO assessment is finished.

5 Appendix: Leg-up design example

When drafting the Red Team plan, the RT provider will define potential leg-ups for each step of the agreed scenarios specified in the Targeted Threat Intelligence report. As some leg-ups may take some time to prepare, the White Team should start preparing leg-ups before the final delivery of the Red Team test plan.

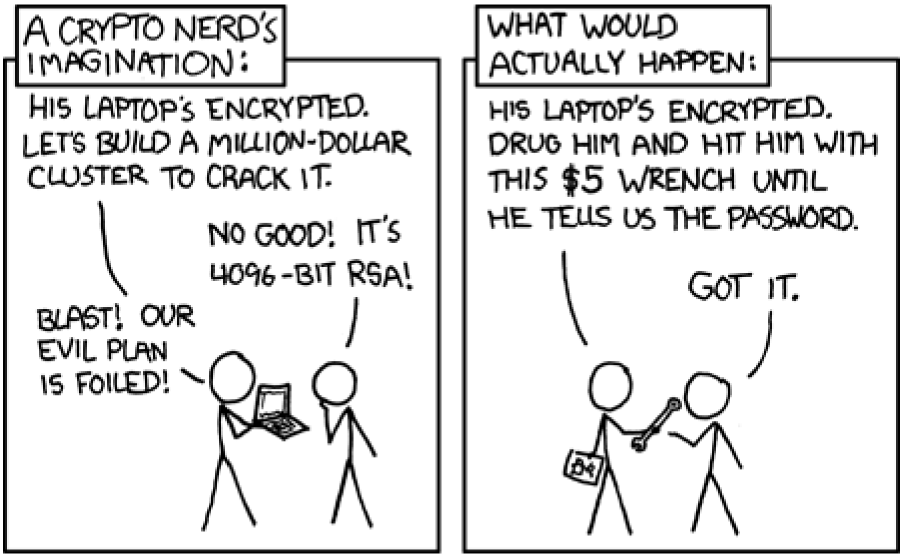
The leg-up examples below describe each leg-up with a code, reason, type, describing how the threat actor could achieve what the leg-up is compensating for, and the requirements for activating the leg-up.

The leg-up code will often be referred to in TIBER tests, and should follow the scenario. This requires that scenarios also have a consistent naming convention. TCT-NO suggests naming Scenarios with letters, for example example: SC-A, SC-B and SC-C. The syntax for leg-up codes then becomes LU-[scenario-code]-[numb], so example: LU-A-01 for Scenario A, and LU-B-01 for scenario B.

#	Leg-up	Reason	Leg-up type	Compensates for	Activation requirement
LU-A-01	IP addresses for target systems	Time saving	Information	The time a threat actor has available 1to exhaustively enumerate and identify target systems.	RT assesses after one or more attempts that identifying the target systems is too time consuming to provide value to the test. There must be a fair assumption it would be possible to achieve this result with enough time available.
LU-A-02	Endpoint detection and response (EDR) software name and version	Time saving Resources	Information	Knowledge a threat actor could gain with enough resources or time.	RT has repeatedly failed to evade EDR solution, not adequately simulating the same capabilities a threat actor has in the threat scenario.
LU-A-03	Accomplice clicker	Time saving Ethical	Access	The assumption a user will comply with phishing eventually, and a real threat actor has less or no ethical boundaries which the Red Team has.	Repeated phishing attempts have failed due to low user compliance, but *not* due to technical security controls (e.g. a payload being blocked).
LU-B-01	Remote Code	Time saving	Access	The assumption a zero-day eventually will be possible to exploit for	Multiple avenues of achieving RCE has been explored without

	Execution	Resources		remote access or can be acquired given enough resources.	success within a reasonable time frame.
LU-B-02	Planting physical device	Resources Ethical	Assistance Access	Compensating for RT not having recruited an Insider for the task.	A scenario has been proposed which is not feasible to execute within the ethical boundaries and/or resource limitations of the Red Team.
LU-B-03	Cracked password hashes	Resources Time saving	Information	The Red Team is sometimes able to extract password hashes from compromised systems. These hashes can then be cracked off-line. Cracking hashes, however, is a time-consuming exercise, especially if the password length and complexity is high. The White Team can provide the passwords, corresponding to the obtained hashes, to the Red Team. This should only be done in case the White Team deems it is possible to crack the hashes given sufficient time.	The Red Team has obtained and tried to crack a password hash without success. The password policy or the WT knows the password is such it might be possible to crack it given enough (feasible) time and resources.
LU-C-01	Improving network access	Time saving	Access	It is possible the Red Team succeeds in compromising a target and obtains a foothold on the internal network. In some cases, however, the command and control (C2) channel through which the Red Team communicates with the compromised target can only carry a limited amount of traffic without raising alerts to	Network access has been established, but significantly slows down the RT to the extent where it impacts the value provided by the test. An assumption must be made the new network access is similar to the existing access and does not provide a level of access which could not be obtained from the existing one.

				the Blue Team. This forces the Red Team to adopt a low-and-slow approach to avoid detection. When this occurs, the White Team could provide the Red Team with an alternative means of accessing the internal network with less limitations, for example launching a payload from a secondary, but largely similar point in the network. This would allow the Red Team to proceed without any delays caused by a limiting C2 channel.	


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.
D4

xkcd: Security

5.1 Preparation of access leg-ups

Granting access to the internal network is not always straightforward, especially without alerting the Blue Team. Access leg-ups therefore require thorough and timely preparation. It is recommended that the White Team investigates the processes to grant these leg-ups well before the start of the test, making sure no delays are incurred during testing when activating the leg-ups.

Best practice for the White Team is to create some user accounts with different levels of access before the test and investigate how the Red Team can access these accounts when necessary. Access leg-ups often need to be adjusted to the institution’s security control and therefor vary from test to test. Some important aspects to consider are:

How to create a low privilege user to be used in the test?

Creating an account to be used for testing can often take some time, the process should therefore be started well before the start of the test. In some advanced scenarios, the creation of an account might even involve the onboarding of a Red Team member. It is therefore advisable the White Team familiarizes itself with the processes required to execute such an onboarding.

How to give the Red Team access to the created user account?

Having an account which can be used is not enough, the Red Team should also have access to this account. This is not always straight-forward, especially when the Red Team operates from a remote location. In some cases, providing access to the Red Team requires shipping MFA tokens or a laptop to the Red Team. As this may take some time, adequate preparation is important

How to provide the Red Team with high privileges?

In general, creating a high-privilege user account for testing purposes is more difficult than creating a low-privilege user. If the creation of an account would be impossible, alternative options may be considered, such as the provision of credentials of an existing account.

5.1.1 Account provisioning best practices

A probable leg-up within access and information leg-up types is to provide the Red Team with valid accounts. Therefore, the following points should be given special consideration.

Pay attention when naming the account

A typical mistake is the use of clear names of the responsible Red Team testers when creating the account. This allows the Blue Team – e.g. by means of a brief internet search – to understand people with the same name are employed in the IT security industry. This can lead to the new account being watched particularly closely because the Blue Team might assume a Red Team test is pending.

In addition to these considerations, strict care should also be taken to ensure the name of the Red Team provider conducting the test is not mentioned anywhere in connection with the account creation.

Possible mitigating actions

Usage of generic and common (sur-) names with regard to account creation. Made-up names should also be checked using your own research (e.g., on sites such as LinkedIn) to see if, by chance, a name has been made up which belongs to someone related to cybersecurity or other relevant fields of profession.

Follow the usual procedures and use normal account characteristics

When onboarding new employees or creating new accounts for existing employees, employee accounts are often assigned to specific domain groups or have other typical characteristics fitting a specific organisational role. Accounts having "unusual" characteristics are often prone of detection or at least further investigation by the Blue Team. As such, accounts could be flagged as possible penetration testing accounts which are either put under more or even less scrutiny (as the account might be viewed as a mere testing account). In the latter case, the provider would receive an advantage, which could distort the results of the test.

Possible mitigating actions

When creating an account, it should be representative and does not deviate from "true" account characteristics and the usual account opening processes. Therefore, the ordinary process of account creation should be followed as much as possible (consideration shall be given to, e.g., the correct department, managers as well as related group memberships). Consideration can also be given to reanimating recently deactivated accounts (e.g., an employee who has left the company very recently and for whom the account has not yet been deactivated).

Do not allow for linking of accounts to one another

Sometimes it is useful or necessary to create several new accounts in connection with a TIBER exercise. If the accounts to be created have very similar characteristics (same applicant, same application time, same group membership, etc.), this can lead to other fake accounts being detected more quickly. This may be the case if, after detecting a fake account, the Blue Team searches for characteristics in other accounts similar to those of the discovered fake account.

Possible mitigating actions

Particular attention should be paid to eliminating the above risks as far as possible. This can be achieved by opening different tickets for account opening by different applicants at different times. Care should be taken to ensure other account characteristics differ from each other (accounts for different departments, etc.). In a nutshell, avoid accounts be linked to each other in any way.

NORGES BANK

Be careful when delivering hardware

Experience shows it may happen the address and name of the Red Team provider is used as the shipping address for the delivery of necessary hardware. This obviously bears the risk of detection by the Blue Team.

<u>Possible mitigating actions</u>

For example, it could be considered to send any hardware to a real address (to which the Red Team provider or one of its employees has access to, but one which cannot be associated with the RT Provider) using the fake name under which the account was opened.

NORGES BANK