SCENARIO BASED RED TEAM

OFFENSIVE SECURITY

IMQ Intuity offers two different types of Red Teaming exercises: **Business Focused** and **Scenario Based** In both cases, the goal is to create a strong awareness of the level of risk a company is subject to, simulating situations as close to reality as possible, using real mentalities and techniques.

BUSINESS FOCUSED RED TEAM:

The most realistic and comprehensive cyber attack simulation for businesses

The first service, called **Business Focused Red Team**, is an exercise during which a real cyber attack is simulated, with a time development of 2 months or more and is strongly characterized by a fully Black Box approach.

The exercise aims to demonstrate whether it is possible to create a business damage to the company, putting yourself exactly in the condition in which an external striker is located. A real attacker, in fact, profiles his victim, looks for the most critical vulnerabilities, both technological and human, and uses them to achieve its purpose. IMQ Intuity's specialists do the same. In the case of a Business Focused Red Team, the "perimeter" is constituted by the company itself in its "totality" and the search for the attack vector is an integral part of the service itself.

SCENARIO BASED RED TEAM:

For **Scenario Based Red Team** instead, we mean a simulation of attack limited to one or more predefined scenarios. This type of exercise has as its main objective to thoroughly test a specific context, indicated by the customer or by IMQ Intuity. In these contexts, the attacker moves freely. The scenario based test has a variable duration depending on its complexity, objectives and timing.

Headquarter: Via Brunello Rutoli, 6 35129 | Padova
Headquarter : Via Nazionale, 230 CAP 00184 | Roma
Registered Office: Via M. F. Quintiliano, 45 - 20138 | Milano

Tel: 049 817 0850
E-mail: info@intuity.it

DEFINITION OF OPERATIONAL SCENARIO

Context: Hypothetical situation to simulate.

Objectives to reach: what you want to verify, what are the conditions for which the simulation is considered finished with success.

Starting Point: where the attacker is and in what condition he operates.

Expected Tests: type of tests proposed; for some generic scenarios it is difficult to predict exhaustively the tests that can be carried out.

SCENARIO BASED PURPLE TEAM

Scenario Based Purple Team is an in-depth analysis of attack techniques carried out during scenarios, in which a comparison between Red Team and Blue Team takes place. The sharing of information between the two teams, allows an exchange of perspectives that promotes continuous improvement.

Headquarter: Via Brunello Rutoli, 6 35129 | Padova
Headquarter : Via Nazionale, 230 CAP 00184 | Roma
Registered Office: Via M. F. Quintiliano, 45 - 20138 | Milano

Tel: 049 817 0850
E-mail: info@intuity.it

EXAMPLES OF SCENARIOS

SCENARIO "A"

Context: An employee's PC is compromised, the attacker managed to access and take possession of the PC itself, in fact it is located in the corporate network with user privileges.

Objectives to reach: access to the file server, compromise of a domain account.

Expected Tests: what it can be done by having remote access to a device, such as, priviledge escalation, blocking local antimalware, scanning the network, vlan hopping, lateral movement, reverse shell, software installation, password cracking.

SCENARIO "B"

Context: A consultant/guest/outside attacker is inside the organization. The attacker has his own PC with which he will try to perform malicious activities.

Objectives to reach: access to confidential documents.

Starting point: IMQ Intuity staff will have access to the corporate premises with a network connection provided for external users.

Expected Tests: ethical hacking, lateral movement, WiFi cracking, Socail Engineering activities and physical document search, access to unsecured PCs, connection to unauthorized network points, vlan hopping.

EXAMPLES OF SCENARIOS

SCENARIO "C"

Context: A hacker wants to create a block to the distribution service of electricity and natural gas.

Objectives to reach: access to the control network of distribution systems, access to systems relevant to the provision of critical services.

Starting point: IMQ Intuity personnel are connected to an internal network with their own device. He won't have any technical and infrastructure information related to distribution services: the purpose of IMQ Intuity team will be to identify such information within the network and develop a useful strategy to achieve the defined objectives.

Expected Tests: production systems enumeration, default credential search, OSINT research activities, passive fingerprinting of production systems, lateral movement, Social Engineering activities.

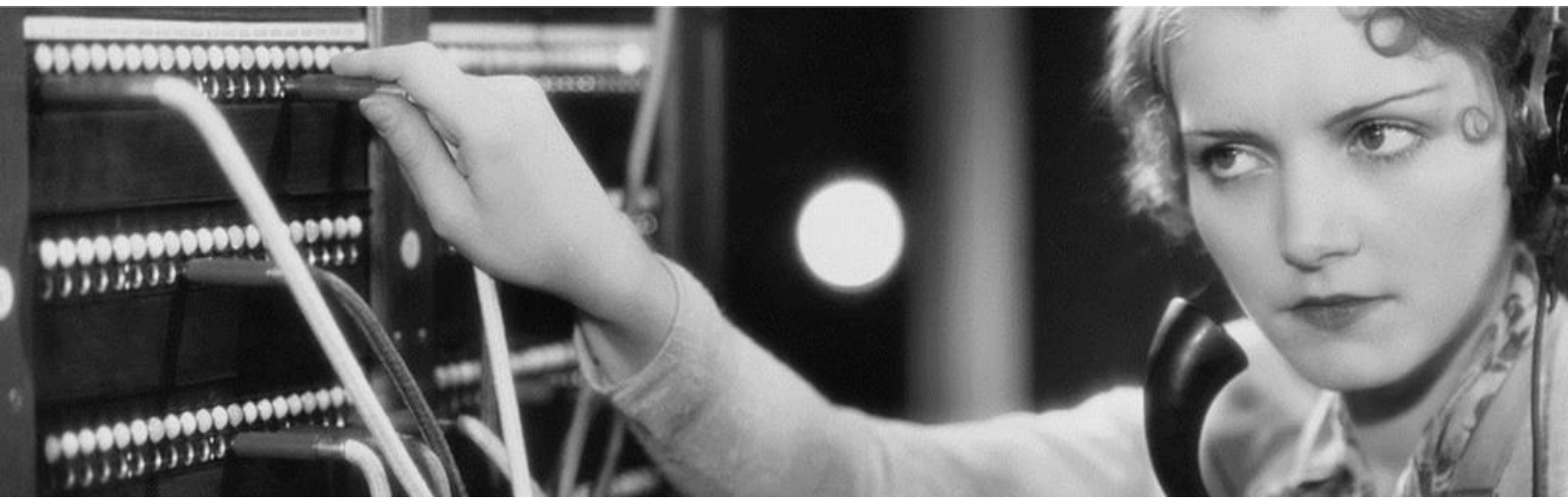
SCENARIO "D"

Context: GDO Company. The stores represent a critical point if not properly managed. The company wants to understand the level of risk represented by a store being attacked.

Objectives to reach: access cash systems, get to the central systems by exploiting the connection between the stores and the headquarters.

Starting point: IMQ Intuity staff acts as an attacker, goes to the store with their equipment and tries to take advantage of the available entry points. The task starts in Black Box modality initially, then, it can continue in a different mode.

Expected Tests: connection to available network points, WiFi system cracking, Social Engineering activities, hacking of the systems reachable through the obtained connectivity, hacking of other physical devices present in the store (electronic payment systems, access control systems, etc), badge cloning.



Headquarter: Via Brunello Rutoli, 6 35129 | Padova
Headquarter : Via Nazionale, 230 CAP 00184 | Roma
Registered Office: Via M. F. Quintiliano, 45 - 20138 | Milano

Tel: 049 817 0850
E-mail: info@intuity.it