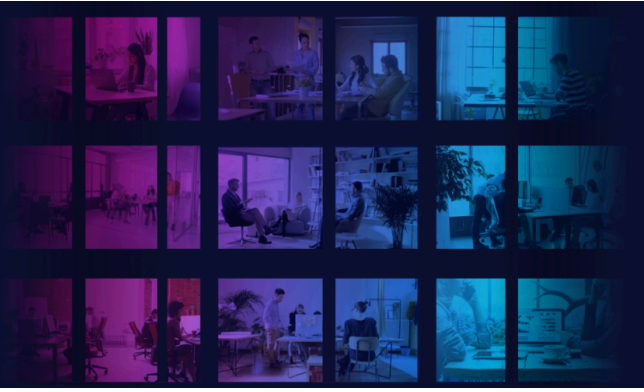
IMMERSIVELABS

Immersive Labs - Latest Labs Content

03-20-2024



Introduction

TeamSim scenarios from Immersive Labs offer a unique and immersive way for organizations to simulate and practice their response to cyber incidents. These scenarios are designed to replicate real-world cyber threats and challenges, allowing teams to collaborate, communicate, and make critical decisions in a controlled environment. By engaging in TeamSim scenarios, participants can enhance their incident response capabilities, test their cybersecurity procedures, and improve their overall cyber resilience. With a focus on teamwork, problem-solving, and decision-making under pressure, TeamSim scenarios provide a valuable training experience that prepares organizations to effectively respond to cyber incidents and protect their assets.

The following scenarios are currently provided for Team Sim:

Scenario Name	Category	Difficulty	Description
Artica - Offensive	Offensive	Beginner	Artica - Offensive is an offensive TeamSim scenario consisting of a Windows AD environment. Users need to enumerate and attack machines in succession in order to move laterally through the environment with the final goal of compromising the Domain Controller. Each user is afforded a Kali machine to attack from, or can choose to VPN into the environment and attack from their own testing system.
Boot2Root Beginner	Offensive	Beginner	Boot2Root is an offensive TeamSim scenario in which users attack 5 machines simultaneously in order to gain access and escalate privileges and obtain flags per task, with each machine having two flags.

Scenario Name	Category	Difficulty	Description
Mythical - Offensive	Offensive	Beginner	Mythical is an Offensive scenario in TeamSim, aimed at Junior Security Professionals, in which users are tasked to perform ‘Pentest-like’ activities against a Linux network. Users are also given a small diagram that helps them with the path they have to take in the network. The goal of the scenario is to move through the network and completely compromise every single machine by getting access to and then escalating privileges on it.
Qing - Offensive	Offensive	Intermediate	Qing - Offensive is an Offensive scenario in which a number of users are tasked to perform ‘Pentest-like’ activities against a fictional corporate network (qing.corp). Users will have to move through three different networks until they get to the target OT network. The scope of this penetration test is to gain access to the OT network.
Kween - Offensive	Offensive	Intermediate	Kween - Offensive is an Offensive scenario in which a number of users are tasked to perform ‘Pentest-like’ activities against a small network (kween.local). The network simulates a real-life situation where access from the outside world to the network was easily attainable and the internal network had a series of vulnerabilities that led to its compromise.
Operations - Offensive	Offensive	Intermediate	Operations is an Offensive scenario in TeamSim in which a number of users are tasked to perform ‘Pentest-like’ activities against a small Active Directory (AD) environment (operations.local) and are given credentials to access two different starting machines. The flow of the scenario is to move through the environment, achieving in most cases access to and then escalating privileges on a number of separate machines with logical misconfiguration flaws to be exploited, much in the style of a real world AD assessment.

Scenario Name	Category	Difficulty	Description
The Heist	Offensive	Advanced	The Heist is an Offensive CTF scenario where users take on the role of bank robbers who need to complete several technical challenges in three distinct networks – to open a 'vault' and obtain the final token to complete the scenario. The challenges are very much 'pentest' skill-focused and cover a variety of disciplines ranging from infrastructure to web application to reverse engineering. Attacking teams can choose to start against one of two networks, both of which can be attacked concurrently and have a distinct attack path to follow. The questions inside the sim environment guide users. Both networks must be completed to obtain credentials and information to attack the final network.
Artica - Defensive	Defensive	Beginner	Artica - Defensive is a small TeamSim scenario which gives users access to both Velociraptor and Splunk and asks them a series of questions in order to detect and understand an attack which runs in the background of the range using Metasploit and rudimentary automation to repeat the attack every 10-15 mins or so, with some jitter-time to add an element of randomisation.
Oilrig: A nation state compromise	Defensive	Beginner	Oilrig: A nation state compromise is a Defensive range scenario where users take on the role of a junior SOC analyst, employing various skills and techniques from defensive disciplines such as incident response and threat hunting. The user is presented with a set of tasks where they must uncover IOCs (indicators of compromise) relating to an attack against an organization called Lycia Pensions. The tasks test the user's ability to threat hunt through logs, and other digital forensic artifacts available within the range.

Scenario Name	Category	Difficulty	Description
Earth Lusca (TAG-22) - Defensive	Defensive	Beginner	Earth Lusca (TAG-22) is a Defensive scenario in TeamSim, aimed at SOC/IR Professionals, in which users are tasked with finding IoCs in a compromised network. The attack that had occurred mimics the techniques and tools employed by the APT group Earth Lusca. The tasks test the user's ability to threat hunt through logs. This will require users to look into running processes, commands that were issued, persistence techniques, lateral movement and more!
Operation Kobold - Defensive	Defensive	Beginner	Operation Kobold is a Defensive range scenario where users take on the role of a SOC analyst, employing various skills and techniques from defensive disciplines such as incident response and threat hunting. The user is presented with a set of tasks where they must uncover IOCs (indicators of compromise) relating to an attack against an organization called Somnium Technology. The tasks test the user's ability to threat hunt through logs, and other digital forensic artifacts available within the range. There are also a few basic reverse engineering-based tasks in order to test the user's skills to perform this.
Kween - Defensive	Defensive	Intermediate	Kween Defensive is a TeamSim scenario aimed at SOC Analysts / IR Professionals, the user is presented with a set of tasks where they must uncover IOCs (indicators of compromise) relating to an attack against an organization called Kween Industries. Kween Industries suspects that its network has been compromised by an unknown attacker, and you've been called in to investigate! The client has given you access to their Splunk and Velociraptor setups and has provided the following information about its network.

Scenario Name	Category	Difficulty	Description
Qing - Defensive	Defensive	Intermediate	Qing Defensive is a TeamSim scenario aimed at SOC Analysts / IR Professionals, the user is presented with a set of tasks where they must uncover IOCs (indicators of compromise) relating to an attack against an organization called the Qing Corporation. Users are provided with a set of defensive-based security tools which can be used to aid them in detecting the attack that has taken place.
Operation Chimera: Lycia Pensions	Defensive	Intermediate	Operation Chimera is a Defensive range scenario where users take on the role of a SOC analyst, employing various skills and techniques from defensive disciplines such as incident response and threat hunting. The user is presented with a set of tasks where they must uncover IOCs (indicators of compromise) relating to an attack against the Lycia Pensions domain on the range. The tasks test the user's ability to threat hunt through logs, and other digital forensic artifacts available within the range.
APT43 - Defensive	Defensive	Intermediate	APT43 – Defensive Scenario is a Team Sim where users take on the role of a SOC analyst. In it, you'll employ various skills and techniques from defensive disciplines such as incident response, threat hunting, and reverse engineering. APT43 scenario provides users with access to both Velociraptor and ElasticSearch, as well as Flare VM, the reverse engineering operating system.
Operation Lycan - Defensive	Defensive	Intermediate	Operation Lycan – Defensive Scenario is a Team Sim where users take on the role of a SOC analyst. In it, you'll employ various skills and techniques from defensive disciplines such as incident response, threat hunting, and reverse engineering. Op Lycan provides users with access to both Velociraptor and ElasticSearch, as well as Flare VM, the reverse engineering operating system. In this scenario, users are asked a series of questions in which they must identify indicators of compromise (IoCs) relating to an attack against the Lycan domain on the range to detect and understand the attack. There are also a few reverse engineering-based tasks that test the user's skills further.

Scenario Name	Category	Difficulty	Description
Operation Akela - Defensive	Defensive	Intermediate	Operation Akela is a Defensive range scenario where users take on the role of a SOC analyst, employing various skills and techniques from defensive disciplines such as incident response and threat hunting. The user is presented with a set of tasks where they must uncover IOCs (indicators of compromise) relating to an attack against the Lycia Pensions domain on the range. The tasks test the user's ability to threat hunt through logs, and other digital forensic artifacts available within the range. There are also a few reverse engineering-based tasks in order to test the user's skills to perform this.
Operation Typhon - Defensive	Defensive	Intermediate	Operation Typhon is a Defensive range scenario where users take on the role of a SOC analyst, employing various skills and techniques from defensive disciplines such as incident response and threat hunting. The user is presented with a set of tasks where they must uncover IOCs (indicators of compromise) relating to an attack against an organization called Somnium Technology. The tasks test the user's ability to threat hunt through logs, and other digital forensic artifacts available within the range.
Detecting Sliver	Defensive	Advanced	Originating from the Bishop Fox team, Sliver is an open-source, cross-platform, and extensible C2 framework. It's written primarily in Go, making it fast, portable, and easy to customize. This versatility makes it a popular choice among red teams for adversary emulation and as a learning tool for security enthusiasts. The Sliver C2 framework has features catering to both beginner and advanced users. One of its main attractions is the ability to generate dynamic payloads for multiple platforms, such as Windows, Linux, and macOS. These payloads, or "slivers," provide capabilities like establishing persistence, spawning a shell, and exfiltrating data. When it comes to communication, Sliver supports a wide range of communication protocols, including HTTP, HTTPS, DNS, TCP, and WireGuard. This ensures that C2 traffic is flexible, stealthy, and can blend in with normal network traffic.