# CYBERGYM Penetration Test

## Mapping the weakest points in your cyber defenses

As an established provider of live cyber training and true-to-life qualification and certification solutions, CYBERGYM is proud to introduce our complementary penetration testing service. Now you can subject both your personnel and your technology to real-life testing, through one, trusted service provider.

Whether you need to prove regulatory compliance, satisfy a request from senior management, or demonstrate security maturity to your clients, CYBERGYM's penetration test service enables you to test the effectiveness of your security technologies, policies and human skills in the safest, most realistic environment.

All the techniques and tools we use are open sourced and White Hat approved. Carried out under the supervision of CYBERGYM's technical experts, in our completely remote environments, you can be sure that no sensitive information will be compromised

## How we do it

Scalable and customizable to any organization size, distribution model, environment or workforce profile, CYBERGYM's penetration testing enables you to discover and map your organization's weak points.

// Defining the scope of the test, the systems to be addressed, the testing methods to be used and the end-goals

// Gathering intelligence & reconnaissance (e.g. network and mail server systems, software versions, plugins, hardware vendors, CV dumpster diving, social media activity and more)

// Carrying out a vulnerability analysis of the gathered intelligence, mapping security weaknesses and system-entry tactics

// Causing mayhem in real life! At one of our live training facilities and in an operational environment, we use phishing, whaling, brute force attacks and other strategies to exploit vulnerabilities, escalating privilege to gain access to the target system, network or individual

// Producing a summary and recommendations report, tailored to suit your specific needs, with sections dedicated to senior-level management, executive-level personnel, and specific divisions (e.g. system, storage, network, security posture, development)

// Producing a regulation-specific report (e.g. for ISO, PCI, GDPR, HIPAA, NIST, OWASP, SOX and more)

# Penetration test types

In the course of testing, our teams will perform several types of tests, including:

- **Internal & external penetration testing**
  - Internally from within the network - simulating a rogue employee or the misuse of an account.
  - Externally - checking the strength of the organization's perimeter and external sites, using company assets that are visible from the internet (website, email server, DNS and more).
- **A choice of three testing methodologies,** depending on your preferred trade-off between speed, efficiency and coverage:
  - White box – based on complete knowledge of the system and network.
  - Black box – testing with no prior knowledge of the system or network, either blind or double-blind, to test the processes, controls and the awareness of the security teams, if and when a real attack occurs.
  - Gray box – testing based on partial knowledge of the network.
- **Unique application-level penetration tests,** testing specific vulnerabilities within the application of the organization, such as:
  - SQL Injection
  - Logical Attacks
  - Parameter and User Input Tampering
  - State & Session Management Attacks
  - Session ID Replay/Brute Force
  - XML Poisoning
  - Injection Attacks
  - Cross Site Scripting
- **VoIP penetration tests,** identifying specific vulnerabilities within your IP communication system and services, to ensure that they can withstand a denial-of-service (DoS) attack, and to prevent the use of eavesdropping to gain access to the network/organization or even to conduct fraud.

# What to expect from CYBERGYM's penetration testing

- **Expertise -** our Red Team is comprised of elite ethical hackers, who have compiled a collection of self-written or team-written scripts and tools designed to automate common or complicated processes that come up in the course of their engagements.
- **Comprehensiveness -** knowledge accumulated over the course of perpetrating hundreds of offensive live-training attacks on organizations from every sector, all around the world.
- **Dedicated Training & Testing Facilities -** our live-training arenas enable both an automated and manual approach, maximizing the level of threat detection, and optimizing the value of our recommendations.
- **Coverage -** the comprehensive tools implemented by our team of experts throughout testing minimize the chance that vulnerabilities will be missed.
- **Flexibility and scalability -** regardless of the size of your organization, even if it has a distributed environment with many remote locations, and no matter the level of knowledge within your IT and security teams, CYBERGYM penetration testing can be carried out at any time and any location.
- **Complementary training -** for further qualification of your IT and security teams, post-test, the CYBERGYM live-training arenas enable you to implement the actionable insights gained from the tests into your team's daily work.

# About CYBERGYM

CYBERGYM provides tailored cyber-training solutions to organizations around the world. With the most relevant threat model and a technological environment configured to your technological setup, we make sure your people gain the experience they need, as individuals and as a team. CYBERGYM further qualifies your general workforce and executives, delivering an all-inclusive, organization-wide solution.

**Founded in 2013 by experienced veterans of Israel's prestigious intelligence organizations, CYBERGYM gives you peace of mind knowing that your teams are always ready, and cyber investments are maximized.**