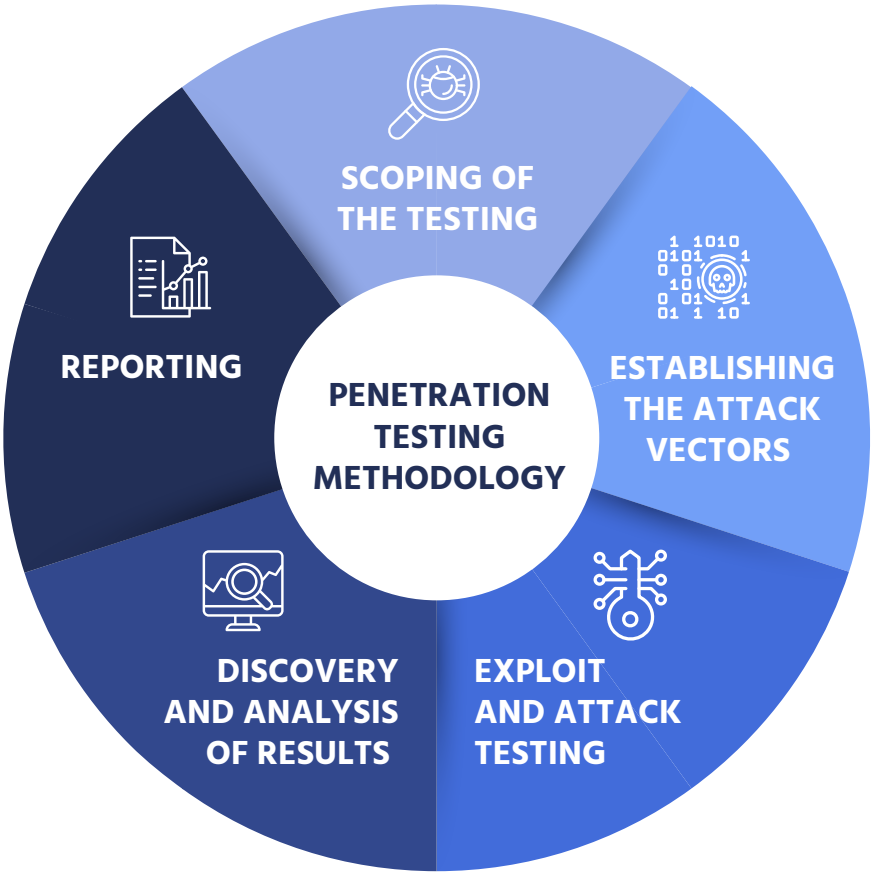
CYBRELLA
CYBERSECURITY EXPERTS

Penetration Testing Services

Cyber-circumstances have dramatically changed in the last few years. The new landscape is characterised by an overwhelming volume of sophisticated attacks and threats. Traditional VA (Vulnerability Assessment) should be taken up to the next level and simulates "real world" scenarios taken from the attacker point of view using real attacker TTPs (tactics , techniques and tools) seeking for the weakest link in the organization chain – the vulnerability that can be exploited to gain unauthorized remote access or attack the organization business service lines.

The Penetration Testing service is done using a hybrid methodology combing various TTPs from Black Box, Grey Box and White Box testing methods were Penetration Testing scope and goals can be defined according to the organizational specific needs.

A penetration Testing Methodology involved



CYBRELLA
CYBERSECURITY EXPERTS

Cybrella's Penetration Testing Services is a multiple layer service that includes:

Application Penetration Testing

Aimed to assessing one or more organizational Applications and/or Business Service from the attacker point of view to identify application related vulnerabilities that can be exploited to gain unauthorized access (e.g. using SQLi, OS Injections, Buffer Overflow), attack the organization end users (e.g. using XSS, CSRF, Cookie Manipulation, Session Hijacking) or even attack the organization business lines and/or SLA (e.g. using Application DoS or Business Logic Flaws).

Infrastructure Penetration Testing

Aimed to assessing part of the organizational network or subnetworks (e.g. public services, remote access services, supplier' extranets) from the attacker point of view and to identify OS and Networking related vulnerabilities that can be exploited to gain unauthorized access or performing attacks with larger or dedicated attack scenario. The testing will include the identification of both commonly known 3rd party component vulnerabilities, misconfigured and non-hardened servers and / or network components, Authentication / Brute Force and Elevation-of-Privilege (EoP) attacks, WiFi Network Testing, custom Protocol Fuzzing and more.

Combined Penetration Testing

Combination of both Application and Infrastructure Penetration Testing TTPs to assess specific service or business line from an attacker point of view when all the options are open and attacker is looking for the "weakest link in the chain" to exploit and gain unauthorized access.

The Penetration Testing Service is performed by highly skilled team with state-of-the-art technologies and proven methodologies, providing our customers with a clear view of their threat landscape, and actionable recommendation for improving security posture and business resiliency.

Our Risk Management Model

The System Risk Assessment will be performed according to a Hybrid Security RA Approach (HSRAA) developed by Cybrella Research Lab.

The Hybrid Security Risk Assessment Approach is based on a combination of a standard best-known methods and practices derived from different RA methodologies and tailored to fit a project and a specific customer requirement as described below.

- **White Box Application Security Testing/Audit** of system components with access to development resources, internal documentation and source code
- **Grey Box Application Security Testing/Audit** of system components with partial access to development resources and source code such as 3rd party components, libraries and tools
- **Black Box Application Security Penetration Testing/Audit** of system components with no available access to development resources or with a specific requirement to perform assessment from a limited access/limited knowledge Threat Source POV (e.g. "cleaning man" or malicious user scenarios)
- **A Source Code level review** to provide the additional insights often missed during the traditional Dynamic Security Testing methods (DAST). This review will include Automated, Manual as well as Hybrid Security Code Review techniques to systematically detect product security vulnerabilities in the source code. Upon completion, our experts will advise you on a practical mitigation technique.

Security Risks and Vulnerabilities will be analysed according to a qualitative Risk Rating Model based on NIST 800-30 and OWASP Risk Rating Model as seen in the picture below:

Table: Risk Level Matrix

	Impact		
Likelihood	Low	Moderate	High
Low	Note	Low	Medium
Medium	Low	Medium	High
High	Medium	High	Critical

CYBRELLA
CYBERSECURITY EXPERTS

Our Team

Our team of experts provides a leading edge in the cyber practice. They are certified and experienced professionals with diverse backgrounds in offensive & defense intelligence, network security, information technology, and cybersecurity solutions.

Cybrella's Red Team: World-class, highly trained and certified penetration testing team, acting as Ethical hackers to simulate possible attacks from the hacker's point of view.

About Cybrella

Cybrella is a world leader cybersecurity consulting company HQ in Boston with an office in Tel-Aviv, Israel. Cybrella provides consulting services for all aspects of modern cybersecurity requirements – Risk Management, Frauds & AML, Cloud Security, Technology, etc. Cybrella's consulting services are aimed at providing our clients with a multi-leveled information security analysis in the following areas:

- **Cybersecurity Management** - Cyber Readiness and Strategic consulting
- **Risk Management and Application Security** - SDL (Secure Development Lifecycle) Methodology, Penetration Tests, Application Firewall, Security Awareness Training
- **Infrastructure Security and Cloud Security** - Risk Analysis and High-Level Engineering, Forensics & Incident Analysis
- **GRC** (Governance, risk management, and compliance) - Accreditation preparation for compliance with standards and regulations, writing policies and regulations

For more information Contact us at boston@cybrella.io or call +1.617.454.1332

Contact us

CYBRELLA
CYBERSECURITY EXPERTS
https://cybrella.io/

Boston
233 Needham Street, Suite 450
Newton, MA 02464, United States
boston@cybrella.io
Tel: +1-617-454-1332

Tel Aviv
2 Habonim St 3rd Floor
Ramat Gan 5246206, Israel
tlv@cybrella.io
Tel: +972-50-622-4440

Follow us