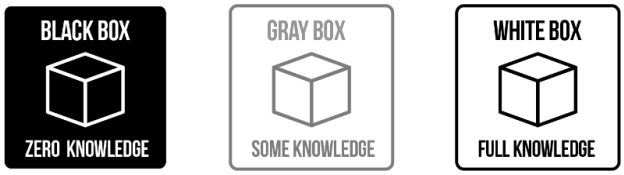
VULNERABILITY ASSESSMENT & PENETRATION TESTING

Our Vulnerability Assessment (**VA**) & Penetration Testing (**PT**) provides a comprehensive evaluation and complete view of your organizations' security posture. Our assessments are designed to proactively identify and prevent any potential exploitation of any existing security vulnerability. Our CyberArq experts' objectives are to identify cybersecurity flaws and thoroughly test the extent of an intrusions effect compromising the network infrastructure through exploitation.

CYBERARQS' BOX CLEVER APPROACH



KNOW THE DIFFERENCE!

	VULNERABILITY ASSESSMENT	PENETRATION TESTING
Frequency	Monthly, plus additional test after changes to network	At least yearly, typically quarterly or semi-annually
Reporting	Comprehensive list of vulnerabilities, including false positives	A detailed document listing all vulnerabilities successfully exploited
Performed By	In-house security or third-party vendor like **CyberArq**	Third-party penetration testing services provider like **CyberArq**
Value	Uncovers a wide range of possible vulnerabilities	Identifies & reduces weaknesses by validating through exploitation

ADVISORY SOLUTIONS

	VULNERABILITY ASSESSMENT	PENETRATION TESTING
Network	Network devices vulnerabilities; servers, switches & laptops etc	Network devices vulnerabilities exploited (internal & External Hosts)
Web Apps	Identification of web app vulnerabilities using OWASP Top 10	Exploiting web app vulnerabilities to identify & remediate flaws
IoT	Exposing smart devices vulnerabilities connected on the network	Testing IoT defenses, uncovering vulnerabilities and exploiting them
Wireless		Attempting to gain unauthorized access to wireless networks
Mobile		Testing of iOS (IPA) & Android (APK) apps through exploitation
Social Eng		Testing human defenses of an organization; emails, USB, phone etc.
Continuous PT		Continuous testing for frequent changes and newly developed code
Active Directory		Reconnaissance of active directory to attempt account takeovers

CYBERARQS APPROACH & METHODOLOGY

VA	*PT*		
X	X	*Define Scope*	Detailed outline with the customer to define what assets are in scope.
X	X	*Information Gathering*	Map out the corporate infrastructure based on services, ports, hardware, software and operating system.
X	X	*Threat Modeling*	Determine mission critical and connected assets to corporate data through white, gray or black box approach.
X	X	*Vulnerability Analysis*	Utilize enterprise and custom scanning tools to uncover vulnerabilities.
	X	*Exploitation*	Exploit vulnerabilities discovered in the vulnerability analysis stage with custom and generic exploitation scripts.
	X	*Post Exploitation*	Successful exploitation's lead to privilege escalation and new vulnerabilities to test for exploitation.
X	X	*Reporting*	Creation of Executive and Detail technical reports for both management and remediation team.
X	X	*Exit Call*	Call scheduled with customers management & remediation team explaining detailed findings.

WHAT YOU RECEIVE

EXECUTIVE SUMMARY REPORT

Designed for managers, executives and board of directors.

This report contains a high overview of the organization's overall security posture with vulnerabilities and, or successful exploitation's ranging from critical to low.

DETAILED TECHINCAL REPORT

Designed for technical teams apart of the remediation.

This report contains a detailed description of all vulnerabilities and, or successful exploitation's ranging from critical to low with remediation recommendations.