CSW Cyber SecurityWorks

# Penetration Testing as a Service

Identify vulnerabilities to reduce risk and exposure

**Our penetration testing simulates a real-world attack on digital assets. We adopt a hacker's perspective to detect and exploit vulnerabilities in an organization's environment to determine if we can move laterally and compromise the entire IT infrastructure.**

## THE CHALLENGE

Attackers are targeting critical assets around the world. To stay safe, organizations need to assess their defenses continuously to understand inherent vulnerabilities and weaknesses that could attract attackers. The challenge here is that most organizations fail to understand an attacker's mindset and attack chaining capabilities.

## OUR METHODOLOGY

Our methodology follows the MITRE ATT&CK framework and NIST 800-115 along with the latest Techniques, Tactics, and Procedures (TTPs) used by attackers.

### RECONNAISSANCE:

We gather information about ports, protocols, and services by scanning assets and discovering your attack surface.

### VULNERABILITY VALIDATION & EXPOSURE ANALYSIS:

We identify vulnerabilities, flag false positives, and analyze all vulnerabilities based on their potential to be exploited and used maliciously against the organization.

### PENETRATION TESTING:

We perform automated and manual penetration tests to exploit vulnerabilities by attempting to bypass existing security controls. We mimic a hacker's stealth attack methods to gain an initial foothold, escalate privileges, and perform lateral movements without being detected.

### PRIORITIZATION OF VULNERABILITIES:

We prioritize vulnerabilities based on weaponization and exploitability and tell you what to fix first.

### STRATEGIC REPORTS & DELIVERY DELIVERY:

Our results are delivered through a Risk-based Vulnerability Management (RBVM) platform that can be easily integrated with your existing security tools and ticketing systems.

**Detect, Prioritize and Remediate**

**100+**
**Pen Testers & Threat Hunters**

**49**
**zero days discovered**

CVE

**Is your current Pen Testing company a CVE Numbering Authority?**

CISSP Certified Information Systems Security Professional

OSCP

PCI DSS COMPLIANT

PCI Security Standards Council
APPROVED SCANNING VENDOR

CISA Certified Information Systems Auditor. An ISACA Certification

CISCO CERTIFIED CCNA

OWASP

## AN AWARD-WINNING RBVM PLATFORM PROVIDES PREDICTIVE ANALYSIS AND EARLY WARNING

Our reports are delivered through an award-winning RBVM platform that provides a detailed analysis of an attacker's predictive behavior and advisory-based recommendations about new exploits as they emerge or trend.

# Penetration Testing as a Service

Identify vulnerabilities to reduce risk and exposure

## CSW PENETRATION TESTING SERVICES

### EXTERNAL PENETRATION TESTING:

A simulated external test on internet-facing assets to help identify vulnerabilities that an attacker could exploit.

### INTERNAL PENETRATION TESTING:

An assessment that emulates an attacker with minimal access privileges to identify exploitable weaknesses enabling vulnerability chaining and lateral movement. The attacker aims to acquire privileged access to sensitive data and compromise the organization's entire infrastructure.

### WEB/MOBILE APPLICATION:

A comprehensive penetration test of web or mobile applications to identify weaknesses that could compromise sensitive data. All vulnerabilities are then mapped to OWASP and MITRE's CWE Top 25 Dangerous Software Weaknesses.

### CONTAINERS PENETRATION TESTING:

An assessment of container images to identify vulnerabilities, weaknesses, misconfigurations, and sensitive information, which could lead an attacker to compromise critical functions.

### CLOUD PENETRATION TESTING:

An assessment of cloud infrastructure from an attacker's perspective with the least level of authorization. This will identify vulnerabilities and misconfigurations that aid attackers to infiltrate infrastructure.

### API PENETRATION TESTING:

An assessment of vulnerabilities in API security with the aim to understand how an internal or external attacker could exploit them.

### SAAS PENETRATION TESTING:

An active security assessment of the SaaS platform includes testing the resilience of all tech stacks (application, storage, and underlying infrastructure). It identifies vulnerabilities or weaknesses within these layers that could lead to exposure.

## WHY CSW?

CSW is a CVE Numbering Authority (CNA) sponsored by the Department of Homeland Security (DHS) USA. We bring a decade of expertise in vulnerability and exploit research with 49 zero day discoveries to our credit. We have worked with hundreds of organizations, improving their security posture and building resilience against threats.

## BENEFITS

### Know Your Exposure:

We find the gaps, blind spots, misconfigurations, missing patches, coding errors, and critical weaknesses in your organization.

### Know What to Fix First:

We highlight vulnerabilities based on weaponization and exploitability. Knowing what to fix first reduces the burden on your security team.

### Validated Results:

We provide you with a validated list of vulnerabilities after eliminating the false positives to enable fast remediation.

### Synchronized Results:

Synchronized delivery of results allows our customers to view identified vulnerabilities within hours of commencing the assessment, thus enabling fast remediation. We present multiple threat scenarios and highlight strengths and vulnerabilities based on a collective analysis of all internal and external findings.

### Meet Industry Requirements:

We help clients comply with industry standards such as ISO 27001, PCI-DSS, and SOC 2.

### Support & Remediation:

We provide comprehensive and prescriptive remediation with advisory details.

**Reach out to us to reduce risk and exposure.**

**To schedule a consultation write to info@cybersecurityworks.com**