

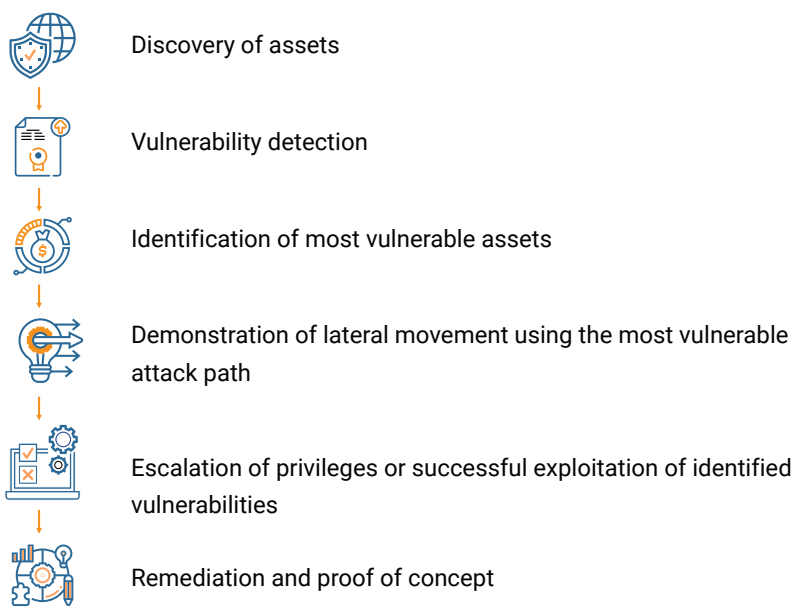
Internal Network Pentesting

Assess your internal assets to stay secure

COMPREHENSIVE CYBERSECURITY SOLUTIONS

CSW's internal penetration testing allows organizations to test if an attacker with internal access can escalate privileges or expose and misuse unauthorized data. We simulate a controlled attack from the perspective of a hacker or internal threat. Multiple attacks are also chained together to determine the true risk of the vulnerability.

OUR INTERNAL NETWORK PENTESTING PROCESS



SERVICE CAPABILITIES

- SYNCHRONOUS REPORTING**
We provide results within hours of initiating the assessment.
- EXPERT PENTESTERS**
Our team comprises of skilled pentesters who have reported numerous zero-days.
- TRANSPARENT PROCESS**
We follow a transparent process from start to finish.

RBVM PLATFORM

We deliver our results through an award-winning **RBVM** platform.

KEY BENEFITS

- COMPLETE COVERAGE**
Secure all your ports, protocols, and services.
- STAY A LEAP AHEAD OF AN ATTACKER**
Identify and mitigate security vulnerabilities & misconfigurations before an attacker exploits them.
- ASSURANCE**
Test the security of your network architecture in a controlled, non-destructive attack scenario.
- ACTIONABLE INSIGHTS**
Know whether your critical data is at risk and how easily a malicious actor may access it.
- WE DO MORE THAN SCANNING**
Go beyond an automated scan to identify risks based on TTPs used by attackers.
- SUPPORT**
Get guided remediation to deal with prioritized vulnerabilities.
- TRANSPARENCY**
Track the whole process from start to finish.


Internal Network Pentesting

Assess your internal assets to stay secure

OUR APPROACH


CSW identifies security vulnerabilities on internal networks and systems from an attacker’s point of view.

INTERNAL RECONNAISSANCE




- Discovery of IP assets
- Footprinting
Enumeration of ports, protocols, services, and operating systems

AUTOMATED VULNERABILITY SCANNING




- Vulnerability identification
 - Missing patches
 - Misconfigurations
 - End-of-life products

PENETRATION TESTING



- Manual validation of identified vulnerabilities
- Attempted exploitation of identified weaknesses using a combination of publicly available exploits

REPORTING



- Prioritized vulnerabilities and guided remediation
- Actionable reports with evidence

WHAT TO EXPECT IN OUR REPORT



Executive summary



Detailed findings mapped to vulnerabilities



Threat correlation



Documented exploits of infiltration vectors and the lateral kill chain




Prioritization of vulnerabilities




Remediation on demand


ATTACK SURFACES WE FOCUS ON




Network



Servers




Network Devices




Applications

Reach out to us to reduce risk and exposure.



To schedule a consultation write to info@cybersecurityworks.com



CVE

OSCP

CISSP

Certified Information Systems Security Professional

PCI DSS COMPLIANT

PCI Security Standards Council

CISA

Certified Information Systems Auditor
An ISACA Certification

CISCO CERTIFIED CCNA

OWASP