CSW Cyber SecurityWorks

Network Penetration Testing Datasheet

Introduction

CSW focuses on identifying the gaps and vulnerabilities in a network and validates the vulnerabilities. CSW evaluates the network and recommends corrective actions to mitigate the exposed risks.

The primary objective for a network penetration test is to validate the exploitable vulnerabilities in networks, systems, hosts and network devices before hackers can discover and exploit them. As a result of our network penetration tests, you'll be able to view your systems through the eyes of a threat actor. This insight will highlight the real threat and will urge you to improve the security posture.

CSW approach to every penetration test is unique for every organization. Our methodology is performed by the industry's top security testers, leveraging our proprietary tactics and intelligence. Our penetration testing methodology includes an attack simulation carried out by our highly trained security analysts to:

- Identify security vulnerabilities present in the environment;
- Validate the vulnerabilities using exploits;
- Demonstrate the potential impact by lateral movement across the enterprise;
- Understand the level of risk for your organization; and
- List the specific fixes for the identified network security flaws

The comprehensive penetration tests offered by CSW are tailored to specific areas of your network

- Internal penetration test
- External penetration test
- Wireless network penetration test

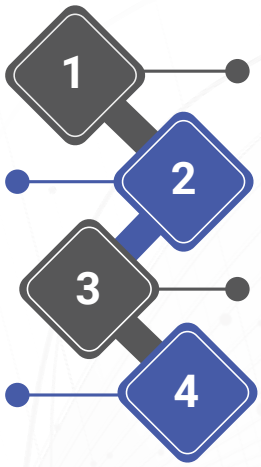
Our penetration tests are designed to show how an adversary would gain unauthorized access to the environment by using similar tactics and techniques. During internal testing, CSW can leverage your entire network to compromise a subset of target systems. During external testing, CSW will leverage tactics such as OSINT and credential testing to compromise the target systems. CSW delivers the findings in a final report and provides a customized course of action for both leadership and technical audiences.

Our Approach

Automated Testing
Publicly known exploits, Security miss-configurations, missing security updates and patches.

Manual Testing
Verify false positives, combination of low vulnerabilities to provide critical exploits, escalating privilege.

Reporting
Document, Deliver, rank, and prioritize the findings to generate an actionable report with evidence for all the stakeholders.



Discovery
Discovery of all accessible systems and their respective services to obtain as much information as possible.

Analysis and Validation
Analyze and validate the findings to develop the plan of attack and carry out an attempt to exploit the identified weakness using well know and custom exploits.

Benefits

- Go beyond an automated scan to identify real risks based on TTPs used by real adversaries in real attacks.
- Know whether your critical data is at risk and how easily it may be obtained by a malicious actor.
- Test the security of your network architecture in a controlled, non-destructive attack scenario.
- Identify and mitigate complex security vulnerabilities and misconfigurations before an attacker exploits them.

Deliverables

- **Executive Report**

Summary for executives and senior-level management

- **Detailed report**

Technical details with step-by-step information that allows you to reproduce our findings. Fact-based risk analysis to know a critical finding is relevant to your environment. Provide tactical recommendations for immediate improvement. Strategic recommendations for long-term improvement.

We conduct professional penetration tests against systems within your network perimeter to expose hosts that lack adequate security, and then attempt to gain control of them.

Although systems may be encroached during the penetration test, we will never attempt to erase, alter or harm any of your company's systems or data. These tests are carried out with the absolute safety of your infrastructure in mind. Engagements typically range from a few days to two weeks.

PCI Security Standards Council
APPROVED SCANNING VENDOR

Corporate Office Address:
IITM Research Park, No.6 A-Block, 3rd Floor, Kanagam Main Road,Taramani, Chennai - 600 113.
P: +91 44 4208 9337 | E: info@cybersecurityworks.com | W: www.cybersecurityworks.com