C&W Business

C&W Server Penetration Test

Learn about critical vulnerabilities that may affect your whole infrastructure and receive recommendations to act proactively.

In recent years, we have learned that all companies, no matter their size or industry, may be attacked by cyber criminals. These attacks often cause serious damage to the company's and its brands' reputation, as well as service unavailability.

C&W Server Penetration Test identifies the most critical vulnerabilities by monitoring computer and network systems through internationally-tested methodologies. Our experts simulate the same activities performed by hackers searching for both internal and external threats.

C&W Server Penetration Test aims to make a broad and comprehensive report on threats found. This report also includes recommendations to take the necessary steps to protect computers from a malicious hacker.

Companies do not need to be attacked to take action! C&W Server Penetration Test allows your company to act proactively and learn about security in your infrastructure.

Services

Server Penetration Test

Penetration Tests are normally referred to as ETHICAL HACKING. These are a security analysis service that focuses on detecting failures in networks and their infrastructure (for example, servers and its components). This test includes the active analysis of vulnerabilities detected in networks.

Web Applications Penetration Test

More than 70% of attacks are aimed at the application layer. This test monitors web applications from its coding in search of errors and SQL or cross-site-scripting injection problems. This test includes the active analysis of vulnerabilities detected.

SAP Environment Penetration Test

The SAP Penetration Test simulates actions by a malicious hacker when trying to access the SAP platform for espionage, sabotage, and fraud.

DDoS simulation

In case your company needs to perform a simulation of a DDoS (Distributed Denial-of-Service) or an attack in its own networks, our team of experts will perform extreme-load performance tests in your website or SOA services. Our distribution-test service can generate all the traffic needed to verify the protection mechanisms.

Public Cloud Penetration Test

This service will help you ensure that the Cloud services you are using are safe and will provide you with an action plan if vulnerabilities are detected. This test is made by performing real-time pro-active attacks with the same techniques used by malicious hackers in search of vulnerabilities to be analyzed.

Benefits

- Report on threats detected to implement security controls and mitigate risks found.
- Identification of vulnerabilities in your services.
- Security experts simulate attacks for our clients to prevent hackers from stealing information.
- Reduce the time and effort required to deal with a security attack in the company.

Questions

How can I detect vulnerabilities in my network?

How I can prevent hackers from stealing critical and sensitive information?

How can I learn about which security controls should be implemented in my network?

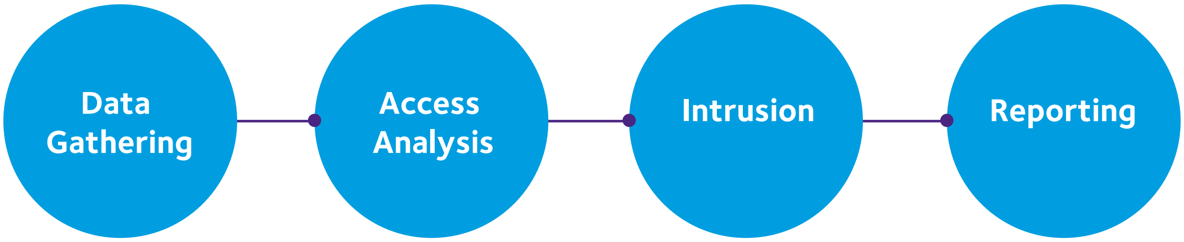
How I can know if the security controls implemented in my network have been configured correctly to protect my information?

How can I reduce the risk of a security attack from being effective?

C&W's certifications

- Certified Ethical Hacker (CEH)
- EC-Council Certified Security Analyst – (ECSA)
- Licensed Penetration Tester – (LPT)
- Computer Hacking Forensic Investigator – (CHFI)
- Cisco Certified: CCIE, CCSI, CCNA, CCNP, CCIP, CCIE, CCDA, CCDP, CCSP
- CCNA Wireless, CCNP Wireless
- Information Security Specialist, Firewall, ASA, IPS, VPN, NAC, MARS, Data Center Support, Data
- CNSS / NSA 4011 Recognition
- CNSS / NSA 4013 Recognition
- NSA INFOSEC Professional
- U.S. Army / DoD Information Assurance Awareness
- Certified Information Systems Security Professional (CISSP)
- ITIL Foundation Version 3
- Fortinet Certified Trainer
- Fortinet Certified Network Security Professional
- Fortinet Certified Network Security Administrator
- Certified in WatchGuard Firewall Basics with Fireware v11.0
- Trained in PAN-EDU-201 (PAN-OS 4.1)
- Certified in project management PMI v4
- Juniper Networks Certified Associate – Junos (JNCIA-Junos)
- Juniper Networks Sales Specialist (JNSS)
- Aruba Networks: Aruba Certified Mobility Associate
- McAfee: Network Security Platform ACE Engineer Risk And Compliance Engineer
- Alienvault: Certified Security Analyst. Certified Security Engineer
- Palo Alto Networks: Acredited Configuration Engineer
- Checkpoint: Checkpoint Certified Security Administrator - Checkpoint Certified Security Expert
- Inflobox: Inflobox Automation Architech – Certified Core Administrator
- Information Security Management System Auditor/Lead Auditor ISO27001:2005
- ISO27001:2005 Lead Auditor
- Official ISC2 Review Seminar
- McAffe Network Data Loss Protection

Penetration Test Methodology



Data Gathering

Access Analysis

Intrusion

Reporting

1. At this stage, the company gathers all information on the netowork's topology and access policies.

2. Based on the analysis of this information, the company will prepare a Diagnosis and Intrusion Plan, just as the potential attacker would do*.

3. Active intrusion; the different levels of risk are assessed.

4. Executive and technical report with the findings.

* The following techniques and tools will be used, among others: Assessment of area transfer, reverse DNS queries, approximations and TCP and UDP scans, port scan, Identification of the operating system, research and detection of vulnerabilities, trust relationships among systems, analysis of equipment, analysis of the operating system, attack on the network, test on Internet applications, back door detection, SQL injection and/or CGI scan.