CDNetworks

Vulnerability Scanning Service

White Paper

Phone: +65 6908 1198 Email: sales@cdnetworks.com

Industry Status and Challenges

With the rapid development of network information technology, network technology brings us not only convenience, but also huge security risks, and the rapid development of Internet, in particular, has posed unprecedented challenges to network security. The openness of network protocols, defects of system software and application design, negligence of system administrators and imperfection of information security system lead to frequent network security incidents and normalization of hacker attacks to enterprises. Whether attacking a network system from the outside or from the inside, an intruder exploits the vulnerabilities of the operating system and applications to realize the attack opportunities. Vulnerabilities in operating systems and applications that can be exploited by criminals or hackers are known as security holes.

Network security is developing dynamically. In the process of the construction and maintenance of the security system, vulnerability scanning can timely discover various security risks in the information system (server host, operating system, third-party middleware, database and user accounts, passwords and other security objects), so as to find flaws in the system before illegal intrusions, and timely fix and reinforce vulnerabilities, achieving the goal of protecting information assets, ensuring the continuous and effective operation of the business system, and eliminating hidden risks.

Service Introduction

Through comprehensive security vulnerability scanning of host system applications and Web applications by using vulnerability scanner, CDNetworks vulnerability scanning service can find the security vulnerabilities existing in the target and provide fixing guidance, so as to fundamentally avoid the possibility of website system applications being attacked by known vulnerabilities.

With its comprehensive computer vulnerability database, CDNetworks vulnerability scanner can discover all kinds of security vulnerabilities. Security professional strictly test and verify all kinds of scanning items, and timely follow up the latest exposure of Oday vulnerabilities on the network, to ensure the accuracy of scanning. CDNetworks security team will provide professional vulnerability scanning reports, as well as professional report interpretation and vulnerability fixing guidance according to the scanning results.

Phone: +65 6908 1198 Email: sales@cdnetworks.com www.cdnetworks.com

Applicable Scenarios

Newly launched business line

Vulnerability scanning can detect potential security risks before a new service system goes online, ensuring the secure and stable operation of the service system.

Regular network security self-check and evaluation

Regular vulnerability scanning checks network security periodically to eliminate potential security risks and discover and patch security vulnerabilities as early as possible.

Security plan evaluation and verification before and after network construction and network transformation

Network builders must establish an overall security plan to command the overall situation strategically, and strike the right balance between tolerable levels of risk and acceptable costs. Vulnerability scanning can be used for security plan evaluation and effectiveness verification.

Security testing before important tasks of the network

Before the network takes on important tasks, it is necessary to take more active security measures to prevent attack incidents, strengthen the importance of network security and information security from the technical and management aspects, form a comprehensive protection, turn from passive fixing to active prevention, and finally minimize the probability of accidents.

Analysis and investigation after network security incident

After a network security accident, it is possible to identify the vulnerability of network attacks through vulnerability scanning, help fix the vulnerability, and provide as much information as possible to facilitate the investigation of the attach source.

Preparation before a major network security incident

Before a major network security incident, vulnerability scanning can help website managers find out the hidden dangers and loopholes in the network in time, and assist users in fixing the loopholes in time.

Regulatory compliance checks

Information security certification involves security compliance check, vulnerability scanning can help website managers to actively respond to regulatory security checks.

Phone: +65 6908 1198 Email: sales@cdnetworks.com www.cdnetworks.com

Service Mode

Extranet scanning

It is possible to directly detect multi-dimensional vulnerabilities and configurations for Web services and servers on the Internet.

Intranet scanning

It is possible to use VPN or on-site scan to adapt to different enterprise network management scenarios for Web services and Intranet servers with access restrictions.

Service Content

Vulnerability scanning mainly uses evaluation tools to scan the systems and networks within the evaluation scope, and search for possible security risks, vulnerabilities and threats in server hosts, Web service/application and third-party middleware within the evaluation scope from both Intranet and extranet perspectives.

There are the following security vulnerability scanning items,

Host security

The security problems at this layer come from the operating systems running on the network, such as Linux, Unix, Windows, and dedicated operating systems. Security problems are manifested in the insecure factors of the operating system itself, including identity authentication, access control and system vulnerabilities, as well as the security configuration of the operating system.

Web Application security

Scanning for this layer is mainly for the consideration of Web application service security. Security vulnerability scanning can discover security vulnerabilities (OWASP TOP10, weak passwords, and CVE vulnerabilities, etc.) in Web applications to improve Web application security.

Middleware security

Scanning for this layer is mainly for the consideration of the security of third-party middleware (mainstream Web container, foreground development framework, background microservice technology stack, etc.). Security vulnerability scanning can identify the middleware in the server and its version, and find the vulnerability risk of the middleware in all respects.

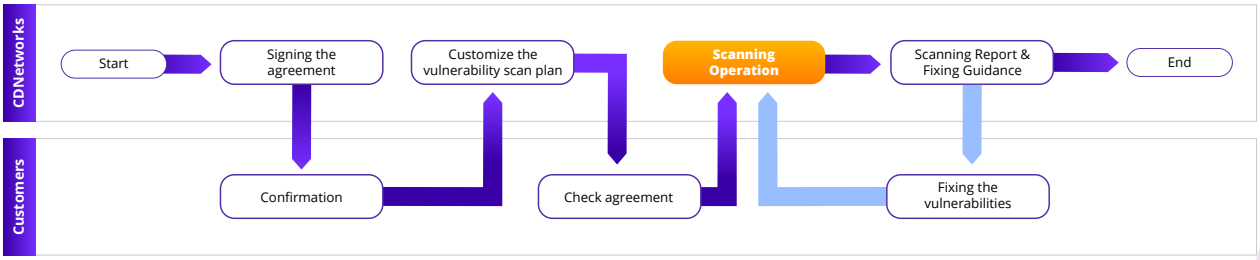
Phone: +65 6908 1198 Email: sales@cdnetworks.com www.cdnetworks.com

Feature	Description
Server host	• Port scanning • Weak password check • DNS domain transport vulnerability • Website Whois query • Server fingerprint • System service error • Nginx buffer overflow vulnerability • Nginx arbitrary file execution vulnerability • Windows SMB remote code execution vulnerability • Various buffer overflow vulnerability • DDOS (Distributed Denial of Service) • 3389 remote overflow
Web service	• OWASP TOP10 vulnerability scanning • CVE vulnerability scanning (buffer overflow vulnerability, remote command execution, etc.) • File inclusion vulnerability • URL redirection vulnerability • SVN/CVS file leak vulnerability • Directory traversal vulnerability • List of enumeration same-domain websites • Detection Robots information • Flash security configuration flaws • Detection system fingerprint • A dozen of parameter pollution strategies • A dozen of types of path pollution strategies • Web application fingerprint • Web background detection • Web background weak password • URL redirection detection • System service error • Path leak
Middleware	• Weak passwords in phpMyAdmin, tomcat, weblogic... • Weak passwords in Mysql, MSSql, Oracle, DB2... • PHP buffer overflow vulnerability • Struts command execution vulnerability • Weblogic deserialization vulnerability • Padding Oracle vulnerability • Various known CVE vulnerabilities • Middleware configuration error

Phone: +65 6908 1198 Email: sales@cdnetworks.com www.cdnetworks.com

Service Procedures

Information security certification involves security compliance check, vulnerability scanning can help website managers to actively respond to regulatory security checks.



Authorization agreement

The content of security vulnerability scanning, including implementation method, implementation time and implementation professional, shall be agreed with the customer, with an authorization to the Company from the customer in writing.
In addition, subject to the customer, security vulnerability scanning can only be performed upon the conclusion of a confidentiality agreement.

Plan formulation

Upon the written authorization from the customer, the security professional and the customer will further discuss the content of the agreement and develop a scanning plan, which must fully comply with the principle of standardization, controllability, minimum impact and confidentiality, with all the process being carried out under the supervision of the customer.

Scanning

Comprehensive scanning based on the asset information provided by customers shall be carried out at the established time with risks and threads under control.

Report output

Vulnerability Scanning Report shall be generated, which contains scanning description, purpose, application policy, un-scanned points for risk aversion, findings, and executable fixing suggestions.

Security double check

Upon the completion of the vulnerability scanning service, the customer can arrange personnel to fix the findings, and the security professional can provide guidance for fixing and double check the result after the fixing. In addition, the Company provides security professional assistance to fixing services at an additional charge.

Phone: +65 6908 1198 Email: sales@cdnetworks.com www.cdnetworks.com

Risk Aversion

Time strategy

Vulnerability scanning shall be carried out during off-peak hours to avoid the impact on the service system caused by the scanning.

Scanning strategy

During vulnerability scanning, the number of threads shall be controlled to prevent service system crashes caused by excessive thread scanning.

Backup strategy

Dirty data may be inserted during vulnerability scanning, and a complete data backup for business codes, database, etc. is required for the scanned target system.

Emergency strategy

The vulnerability scanning shall be carried out with the presence of the customer's technical staff. Upon abnormalities such as scanned target crash, no response and interruption, the scanning shall be terminated immediately, and may only proceed with the scanning again upon the consent of the customer after the identification of the cause and the system recovery with the help of the technical staff.

Service Advantage and Service Value

Multi-dimensional vulnerability detection

Professional vulnerability scanning for a variety of enterprise assets, including but not limited to Web applications, hosts, middleware, etc.

No need for deployment, scanning on demand

The customer does not need to install any hardware or software or change the current network infrastructure. Customer can scan on demand, saving customers' operating costs.

Rich vulnerability database

CDNetworks has a comprehensive vulnerability database established based on the international CVE standard, with more than 2,000 vulnerabilities, as well as real-time update capabilities. Each vulnerability contains detailed vulnerability descriptions and operable solutions, and security professional regularly update the vulnerability database.

High accuracy

Each scanning result will be manually verified by CDNetworks security professional to ensure its high accuracy.

Phone: +65 6908 1198 Email: sales@cdnetworks.com www.cdnetworks.com

Distributed scanning

CDNetworks vulnerability scanning service realizes real-time and regular vulnerability scanning and risk evaluation of large-scale networks through multiple scanners (PoPs) distributed on the network and centralized management by a central server.

Professional scanning report

The CDNetworks vulnerability scanning system analyzes the scanning results by reports and graphics, and can intuitively evaluate and check the security performance of customers. The scanning results are presented in a detailed written report, providing a basis for customers to discover potential security risks and improve the security level of the information system.

Skilled professional services

CDNetworks vulnerability scanning service provides many-to-one response by CDNetworks security team, helping enterprises discover security problems before attackers and fix them in time with its professional interpretation and guidance fixing services.

About CDNetworks Security Team

CDNetworks Security Laboratory consists of a team of security experts dedicated to researching, monitoring, detecting, investigating, and responding to cyberthreats around the clock. The team provides unparalleled security services that safeguard enterprises against attacks and breaches while reducing the capital expenditure and operating expenses associated with security. The CDNetworks Security team has over 100 security experts, many of whom have over 10 years of experience in cybersecurity and related fields. Our team boasts a diverse set of skills that, when combined, is instrumental to detecting, analyzing, and remediating threats. Our researchers also have broad knowledge of tried-and-true technologies for threat detection and prevention, as well as experience with today's advanced threat-detection techniques.

With over 2,800 Points of Presence located around the world, coupled with ample amounts of bandwidth resources, CDNetworks serves thousands of global customers in a myriad of industries. To protect our customer base, which includes over 200,000 servers worldwide, the CDNetworks Security Platform mitigates an average of over 3.3 billion cyberattacks daily.

In addition to mitigating attacks, the CDNetworks Security Platform collects massive amounts of attack and threat-intelligence data, which can be analyzed for weaknesses to determine whether a potential attack vector exists and, if it does, to develop effective defense mechanisms and strategies for deterring future attacks. This process instills confidence that customer websites and online resources will be hardened against future attacks, preserve business relationships, and affirm public trust.

Phone: +65 6908 1198 Email: sales@cdnetworks.com www.cdnetworks.com