CCTV

NETWORK VULNERABILITY SCANNING SYSTEM

1. Product Overview

Expert in Global Asset Risk Detection, Safeguarding the Lifeline of Enterprise Network Security

The Viruni CCTV Network Vulnerability Scanning System (CCTV-VSS) integrates best practical experience accumulated over the years in information security vulnerability mining, penetration testing technology research, and vulnerability inspection methods. It is a new-generation self-developed vulnerability scanning product. Driven by an "active + passive" dual engine,

It integrates capabilities of host vulnerability, website vulnerability, database vulnerability, container image vulnerability, event content detection, and configuration compliance verification. It can accurately assess security risks of assets from multiple dimensions, including security vulnerabilities, security configuration issues, weak passwords, and security events, helping users improve network security protection performance and damage resistance.

2. Product Advantages

Comprehensive scan task types to accurately complete security risk detection

The CCTV-VSS, driven by an "active + passive" dual engine, can comprehensively cover various asset types such as hosts, websites, databases, and container images, and accurately detect risks such as security vulnerabilities, configuration issues, weak passwords, and sensitive events. The system supports multi-dimensional risk assessment, combined with the CVE vulnerability database and the OWASP Top 10 threat model, to ensure the accuracy and comprehensiveness of detection results, helping users quickly identify and fix potential security threats.

It allows administrators to quickly validate vulnerabilities using system-provided parameters and HTTP request/response data, with one-click verification. Also supports penetration testing validation for Struts2 remote code execution vulnerabilities, including command execution and file upload operations.

Empowered by intelligent collaboration to enhance operation and maintenance efficiency

The innovative collaborative scanning mode completes asset detection, host and Web vulnerability scanning with one click, realizes "asset-vulnerability-risk" correlation analysis, and significantly improves detection efficiency and coverage in complex network environments. The non-intrusive scanning technology does not require active packet sending, can identify potential vulnerabilities through asset fingerprint matching, completes risk assessment without affecting the operation of business systems, and is especially suitable for scenarios with extremely high requirements for network stability such as finance and operators. Asset information can be entered manually, selected from an asset tree, or imported in bulk via structured tenplates.

Full-stack technology compatibility to escort digital transformation

It supports the scanning of new-type assets such as basic network environments (operating systems, databases, middleware), IoT devices, big data platforms, and multi-cloud architectures. The vulnerability database is updated synchronously with international/domestic mainstream standards to ensure the risk detection capability for emerging technology stacks. Through pre-detection of container image vulnerabilities and baseline verification, it helps implement the DevSecOps process and ensures the security and compliance of infrastructure and business applications in the digital transformation.

Leading large model asset and risk investigation to reduce exposure risks

Based on a powerful asset engine, it can collect information such as IP addresses, ports, types, model manufacturers, and model names of large models, and can perform vulnerability scanning on large model website applications, service frameworks, etc., such as Ollama security vulnerabilities, vLLM security vulnerabilities, Open WebUI security vulnerabilities, Gradio security vulnerabilities, etc.

Flexible deployment and easy to use

The system supports multiple deployment methods, including local deployment, cloud deployment, and hybrid deployment, and can adapt to network environments of different scales and complexities. The interface is simple and intuitive, easy to operate, and supports custom report generation to meet the needs of different users.

Detection for the effectiveness of ransomware protection

CCTV-VSS supports the ransomware risk detection module evaluates the protective capabilities of the target network environment against ransomware risks by simulating ransomware attack paths.

Configuration of user access

The system supports detailed configuration of user access validity periods-including unrestricted access, specific daily time windows, designated weekdays or custom date ranges within a month.

3. Main Features

System Scan

The system scanning module is mainly used to analyze and identify security vulnerabilities in the network and weak links in the system under test, provide detailed detection reports, and offer corresponding repair measures and security suggestions for the detected network security risks. It is a mainstream function for improving the security protection performance and damage resistance of internal networks, detecting and evaluating the security performance of operational networks, and providing real-time security suggestions for network system administrators.

Web Scan

The Web scanning module fully supports OWASP_TOP10 detection, enabling users to gain comprehensive insights into potential security risks in their web applications. It facilitates the establishment of secure and reliable web application services, enhances the application system's resilience against various web-based attacks (such as injection attacks, cross-site scripting, file inclusion, deserialization vulnerabilities, code execution, directory traversal, weak passwords, information leakage, form bypass, etc.), and assists users in meeting compliance requirements such as Classified Protection, PCI, and internal control audits.

DB Scan

The consequences of security risks in databases being maliciously exploited are well-known. The database scanning module helps users fully understand the security vulnerabilities in their databases, and enhances the risk resistance of various databases through regular security self-detection and evaluation. It also assists users in evaluating the effectiveness of database construction, as well as analyzing, investigating, and tracking database security incidents.

It supports professional vulnerability detection and analysis of for example Oracle, MSSQL, MySQL, DB2, Informix, PostgreSQL, DM, KingbaseES databases and so on.

Baseline Scan

"Security baseline" refers to the minimum-security guarantee for an information system, that is, the most basic security requirements that the information system needs to meet. The security of information systems often requires a balance between security costs and tolerable security risks, and the security baseline is precisely the reasonable demarcation line for this balance. Relying on years of accumulation and research in network security, the CCTV-VSS has a built-in standard compliance baseline library, while supporting customized baseline configuration to flexibly adapt to regulatory requirements of different industries. Through automated scanning and intelligent report generation, it significantly shortens the compliance inspection cycle and reduces manual verification costs.

Event Content Scan

It can detect events and sensitive content such as hidden links, broken links, embedded malware, mining scripts, black pages, ID card information, and inappropriate comments on websites, preventing website owners from being notified and held accountable due to

website security incidents.

Collaborative Scan

It supports automatically detecting live targets and their open Web services by inputting an IP or IP range. A single task can complete asset detection, host vulnerability scanning, and Web vulnerability scanning. It enables seamless and comprehensive risk detection for both hosts and Web services, and combines the CVE vulnerability database and OWASP Top 10 threat model to achieve multi-dimensional risk detection, significantly improving the efficiency and coverage of security assessments in complex environments.

Non-Intrusive Scan

No packet sending detection is required. Potential vulnerability risks can be automatically identified by importing asset fingerprints or using existing ones, combined with the software and versions affected by vulnerabilities.

Specialized Scan

It supports the specialized scanning strategy that simultaneously detects high-risk vulnerabilities, high-risk open ports and weak authentication credentials across both host and web assets within a single task. Scan results explicitly whether critical ports are exposed, providing actionable insights for risk mitigation.

It also supports the offline weak password detection tool that supports the generation of transformed dictionaries based on user-specific keywords.

4. Technical Specifications

CCTV - VSS	
Model	CCTV-VSS-E3000-V
Performance	
Concurrency Tasks Number	15
Concurrency Scanning Hosts Number	100
Technical Specifications	
CPU (Number of Cores)	8
Memory (GB)	16
Recommended Minimum Disk	1TB
Recommended Operating System	openEuler 20.03 LTS、openEuler 20.03 LTS-SP3、openEuler 22.03 LTS、 openEuler 22.03 LTS-SP3 CentOS7.5~7.9 X64;