Key Features of the Acunetix Network Security Scanner

Acunestx 网络安全扫描器的主要特点

Comprehensive security audits require a detailed inspection of the perimeter of your public-facing network assets. Acunetix uses the popular OpenVAS scanner to provide a comprehensive perimeter network security scan engine that integrates seamlessly with your web application security testing. The network security scanner is directly available in Acunetix Online and automatically integrates with Acunetix for Windows and Acunetix for Linux.

全面的安全审核要求对您面向公众的网络资产的外围进行详细检查。Acunetix 使用流行的 OpenVAS 扫描仪提供一个全面的外围网络安全扫描引擎，它可以无缝地集成到 Web 应用程序安全测试中。网络安全扫描器可直接在 Acunetix 在线上使用，并自动与 Acunetix for Windows 和 Acundex for Linux 集成。

Scan Network Perimeter Services

扫描网络外围服务

Insecure network perimeters are still the cause of most data breaches. The perimeter is, therefore, one of the most important areas of your network to secure against vulnerabilities, misconfiguration, and other security threats that could compromise security or availability of network services. Acunetix provides you with a perspective of your network perimeter just like an attacker would see it. Use it to:

不安全的网络边界仍然是大多数数据泄露的原因。因此，外围是网络中最重要的区域之一，可以防止漏洞、错误配置和其他可能危及网络服务安全性或可用性的安全威胁。Acunetix 为您提供了攻击者会看到的网络外围的透视图。用它来：

- Discover open ports and running services
- 发现打开的端口和正在运行的服务
- Test for over 50,000 known network vulnerabilities and misconfigurations
- 测试 50，000 多个已知的网络漏洞和错误配置

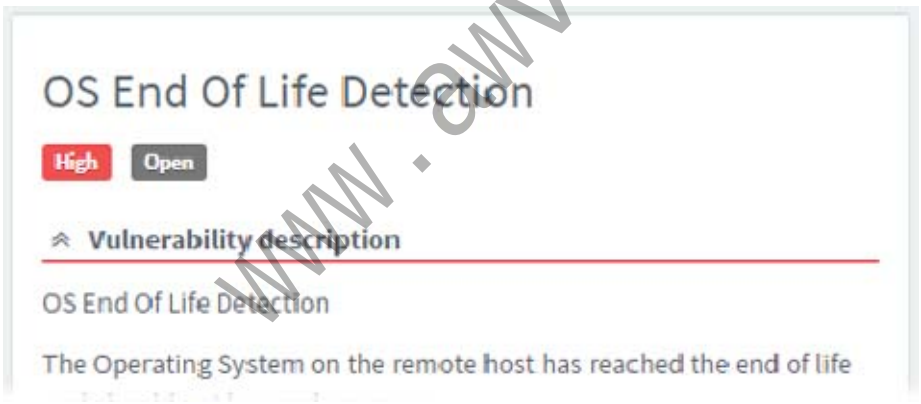
Testing for Network Vulnerabilities 网络漏洞检测

Acunetix scans your network for vulnerabilities and presents results in the Acunetix dashboard, from where a network security report can be easily generated.

- Assess the security of routers, firewalls, switches, and load balancers
- Test for weak passwords: FTP, IMAP, database servers, POP3, Socks, SSH, and Telnet
- Test for DNS zone transfer, open recursive DNS, and DNS cache poisoning attacks

Acunetix 扫描您的网络漏洞，并在 Acunetix 仪表板中显示结果，在该仪表板上可以轻松生成网络安全报告。

- 评估路由器、防火墙、交换机和负载平衡器的安全性。
- 测试弱密码：FTP、IMAP、数据库服务器、POP 3、SOCKS、SSH 和 Telnet
- 测试 dns 区域传输、打开递归 dns 和 dns 缓存中毒攻击。



Detecting Network Security Misconfigurations

检测网络安全配置错误

Acunetix can detect a wide array of network security misconfigurations that could lead to sensitive data disclosure, denial of service, or even compromise of hosts. Acunetix tests for:

- Anonymous FTP access and writable directories over FTP
- Badly configured proxy servers
- Weak SNMP community strings

- Weak TLS/SSL ciphers
- Acunetix 可以检测到各种各样的网络安全错误配置，这些错误配置可能导致敏感数据泄露、拒绝服务，甚至导致主机的危害。Acunetix 试验：
- FTP 上的匿名 FTP 访问和可写目录
- 配置不良的代理服务器
- 弱 SNMP 社区字符串
- 弱 TLS/SSL 密码