

Vulnerability Scanners



Table 1: Feature Comparison

	BindView RMS	GFI LANguard N.S.S	Nessus	NetIQ Vulnerability Manager	Retina	SNSI
Basic Requirements						
Agent installation	Optional	No	No	At least one per domain	No	No
Back-end database support	SQL Server, MSDE	SQL Server, MSDE, Microsoft Access	MySQL, file	SQL Server	file	Access
Uses intrusive techniques	Yes	No	Yes	No	No	No
Capabilities						
Automatically updates signatures	Yes	Yes	Yes	Yes	Yes	Yes
Can create custom security checks	Yes	Yes	Yes	Yes	Yes	No
Lists groups	Yes	Yes	Yes	Yes	No	No
Lists missing patches	Yes	Yes	No	Yes	No	No
Lists services	Yes	Yes	Yes	Yes	Yes	Yes
Lists shares	Yes	Yes	Yes	Yes	Yes	Yes
Lists users	Yes	Yes	Yes	Yes	Yes	No
Performs port scans	Yes	Yes	Yes	Yes	Yes	Yes
Primary supported platforms and programs	AD, Check Point Software Technologies' Firewall-I, Microsoft Exchange Server, Novell Directory Services (NDS), Novell eDirectory, Novell NetWare, OS/400, SAP, SQL Server, UNIX, Web services and Internet, Windows	BIND DNS, CGI, FTP, mail servers, registry, remote procedure call (RPC), UNIX, Windows	Cisco Systems, NetWare, UNIX, Windows	Apache, Check Point's VPN-I, IBM iSeries, Linux, Microsoft IIS, NetWare, Oracle, Sun Microsystems' Sun ONE, Sybase, UNIX, Windows	BSD, CGI, DNS, FTP, HTTP, Lightweight Directory Access Protocol (LDAP), Linux, NetBIOS, POP3, registry, SMTP, Sun's Solaris, TCP/IP, UDP, Windows	Cisco Systems' routers, HP printers, HP-UX, Linux, Solaris, Windows
Scans with alternate credentials	External scan uses null credentials; internal scan depends on user role	Null, user-specified	Null, user-specified	Depends on console users and roles	Null, user-specified	Null, user-specified
Target selection method	Domain, IP address (single or range), subnet, target system name	Domain, import from file, IP address (single or range), list of computers, target system name	Import from file, IP address (single or range), named host, subnet	DNS, domain, import from file, IP address, Network Information Service (NIS), TCP	Address groups, IP address (single or range), named host, subnet	Domain enumeration, IP address (single or range), subnet
Vulnerability database	Two databases: one for intrusive external scans; one for nonintrusive internal scans and audits	Small vulnerability database and multiple security information checks	Large community-supported database	Large database that extends beyond traditional vulnerability auditing	Large database with excellent descriptions	Large database includes robust descriptions
Offers automatic remediation	Yes	No	No	Yes	No	No
Provides remediation steps	Yes	Only links to third-party sites	Yes	Yes, some lack detail	Yes, excellent	Yes, very robust
Reporting						
Report formats	.csv, .dbf, .doc, html, .mdb, .pdf, .rtf, SQL Server, .tsv, .txt, .xls, .xml	.html, .txt, .xml	.csv, .html, MySQL, .pdf, .txt	Crystal Reports, .doc, .pdf, .rtf, .xls,	.doc, .html, .txt	Crystal Reports
Types of reports	Category, chart, devices, exceptions, grid, group name, host IP address, host name, security hole, severity, summary	Auditing policies, computer properties, groups, full, missing patches, open ports, open shares, password policies, users, vulnerabilities	Full	Full, data view, graphs	Full, remediation, vulnerabilities	Compact, detailed, history, simple, summary
Rating	◆◆◆◆◆	◆◆◆◆◆	◆◆◆◆◆	◆◆◆◆◆	◆◆◆◆◆	◆◆◆◆◆
Recommendation	More appropriate as the cornerstone of a security data-collection program than as a standalone scanner	A nimble, easy-to-use scanner that would be best used in conjunction with another, more comprehensive product	Good for those who don't have money to spend but who have UNIX experience and a tolerance for the greater risk associated with intrusive scanning	A good choice for administrators who want to customize scans but don't mind prefab reports	A feature-rich, highly efficient, but costly scanner best suited for those who need high-level performance and aren't on a budget	A fairly robust and user-friendly scanner; good for those who are concerned with the learning curve