Metaspoitable

Vulnerabilities by Host

Vulnerabilities by Host

192.168.50.101

2	2	3	0	29
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities   Total: 36

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
MEDIUM	6.5	3.6	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	5.9	5.1	136808	ISC BIND Denial of Service
MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	10223	RPC portmapper Service Detection
INFO	N/A	-	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	-	11002	DNS Server Detection
INFO	N/A	-	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

INFO	N/A	-	10437	NFS Share Export List
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	48243	PHP Version Detection
INFO	N/A	-	118224	PostgreSQL STARTTLS Support
INFO	N/A	-	26024	PostgreSQL Server Detection
INFO	N/A	-	11111	RPC Services Enumeration
INFO	N/A	-	53335	RPC portmapper (TCP)
INFO	N/A	-	25240	Samba Server Detection
INFO	N/A	-	104887	Samba Version
INFO	N/A	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	17975	Service Detection (GET request)
INFO	N/A	-	11153	Service Detection (HELP Request)
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	135860	WMI Not Available
INFO	N/A	-	11424	WebDAV Detection
INFO	N/A	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

* indicates the v3.0 score
was not available; the v2.0
score is shown