CYBERSECURITY ASSESSMENT

Sample report

Vulnerability Scan Report

TARGET

192.168.8.111

SCAN DATE

Sunday, May 3, 2026

TOTAL FINDINGS

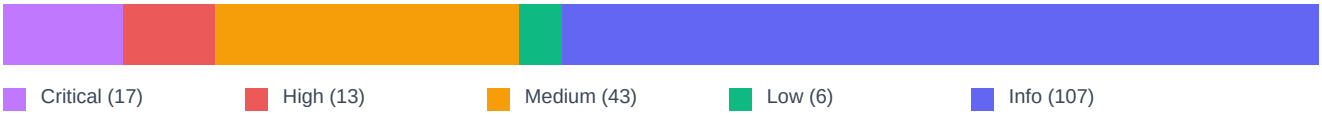
186

17	13	43	6	107
CRITICAL	HIGH	MEDIUM	LOW	INFO

Findings Overview

This automated scan identified 186 findings on 192.168.8.111. Severity ratings follow the CVSS v3.1 scoring framework. Critical and High findings should be addressed first.

Severity Distribution



Target	Critical	High	Medium	Low	Info	Total
192.168.8.111	17	13	43	6	107	**186**

Severity	CVSS	Vulnerability	Host	Port
Info	0.0	'favicon.ico' Based Fingerprinting (HTTP)	192.168.8.111	8180/tcp
Info	0.0	'favicon.ico' Based Fingerprinting (HTTP)	192.168.8.111	80/tcp
Medium	5.0	/doc directory browsable	192.168.8.111	80/tcp
Medium	6.4	Anonymous FTP Login Reporting	192.168.8.111	21/tcp
Medium	4.3	Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	192.168.8.111	80/tcp
Info	0.0	Apache HTTP Server Detection Consolidation	192.168.8.111	80/tcp
Info	0.0	Apache JServ Protocol (AJP) v1.3 Detection (TCP)	192.168.8.111	8009/tcp
Info	0.0	Apache Struts Detection Consolidation	192.168.8.111	—
Medium	4.3	Apache Tomcat 'cal2.jsp' XSS Vulnerability - Active Check	192.168.8.111	8180/tcp
Critical	9.8	Apache Tomcat AJP RCE Vulnerability (Ghostcat) - Active Check	192.168.8.111	8009/tcp
Info	0.0	Apache Tomcat Detection Consolidation	192.168.8.111	8180/tcp
Critical	9.8	Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Credentials (	192.168.8.111	8180/tcp
Critical	10.0	Apache Tomcat Server Administration Default/Hardcoded Credentials (HTTP)	192.168.8.111	8180/tcp
Medium	5.0	awiki <= 20100125 Multiple LFI Vulnerabilities - Active Check	192.168.8.111	80/tcp
Medium	5.0	Check if Mailserver answer to VRFY and EXPN requests	192.168.8.111	25/tcp
Medium	4.8	Cleartext Transmission of Sensitive Information via HTTP	192.168.8.111	8180/tcp
Medium	4.8	Cleartext Transmission of Sensitive Information via HTTP	192.168.8.111	80/tcp
Info	0.0	CPE Inventory	192.168.8.111	—
Info	0.0	Database Open Access Information Disclosure Vulnerability	192.168.8.111	3306/tcp
Info	0.0	DistCC Detection	192.168.8.111	3632/tcp

Severity	CVSS	Vulnerability	Host	Port
Critical	9.3	DistCC RCE Vulnerability (CVE-2004-2687)	192.168.8.111	3632/tcp
Critical	10.0	Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities	192.168.8.111	8787/tcp
Medium	5.0	DNS Cache Snooping Vulnerability (UDP) - Active Check	192.168.8.111	53/udp
Info	0.0	DNS Recursion Enabled (UDP) - Active Check	192.168.8.111	53/udp
Info	0.0	DNS Server Detection (TCP)	192.168.8.111	53/tcp
Info	0.0	DNS Server Detection (UDP)	192.168.8.111	53/udp
High	7.5	EasyPHP Webserver <= 12.1 Multiple Vulnerabilities - Active Check	192.168.8.111	80/tcp
Info	0.0	FTP Banner Detection	192.168.8.111	21/tcp
Info	0.0	FTP Banner Detection	192.168.8.111	2121/tcp
High	7.5	FTP Brute Force Logins With Default Credentials Reporting	192.168.8.111	2121/tcp
High	7.5	FTP Brute Force Logins With Default Credentials Reporting	192.168.8.111	21/tcp
Medium	4.8	FTP Unencrypted Cleartext Login	192.168.8.111	21/tcp
Medium	4.8	FTP Unencrypted Cleartext Login	192.168.8.111	2121/tcp
Info	0.0	Hostname Determination Reporting	192.168.8.111	—
Critical	9.8	HTTP Brute Force Logins With Default Credentials Reporting	192.168.8.111	8180/tcp
Medium	5.8	HTTP Debugging Methods (TRACE/TRACK) Enabled	192.168.8.111	80/tcp
Info	0.0	HTTP Security Headers Detection	192.168.8.111	8180/tcp
Info	0.0	HTTP Security Headers Detection	192.168.8.111	80/tcp
Info	0.0	HTTP Server Banner Enumeration	192.168.8.111	8180/tcp
Info	0.0	HTTP Server Banner Enumeration	192.168.8.111	80/tcp
Info	0.0	HTTP Server type and version	192.168.8.111	8180/tc

Severity	CVSS	Vulnerability	Host	Port
				p
Info	0.0	HTTP Server type and version	192.168.8.111	80/tcp
Low	2.1	ICMP Timestamp Reply Information Disclosure	192.168.8.111	—
Info	0.0	IRC Server Banner Detection	192.168.8.111	6697/tcp
Info	0.0	IRC Server Banner Detection	192.168.8.111	6667/tcp
Info	0.0	ISC BIND Detection Consolidation	192.168.8.111	53/tcp, 53/udp
High	7.5	Java RMI Server Insecure Default Configuration RCE Vulnerability - Active Check	192.168.8.111	56320/tcp, 29209/tcp
High	7.5	Java RMI Server Insecure Default Configuration RCE Vulnerability - Active Check	192.168.8.111	1099/tcp, 24528/tcp
Medium	4.3	jQuery < 1.6.3 XSS Vulnerability	192.168.8.111	80/tcp
Medium	6.1	jQuery < 1.9.0 XSS Vulnerability	192.168.8.111	80/tcp
Info	0.0	jQuery Detection Consolidation	192.168.8.111	—
Info	0.0	MariaDB / Oracle MySQL Detection (MySQL Protocol)	192.168.8.111	3306/tcp
Info	0.0	Microsoft SMB Signing Disabled	192.168.8.111	445/tcp
Info	0.0	Microsoft Windows SMB Accessible Shares	192.168.8.111	445/tcp
Medium	6.8	Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection V	192.168.8.111	25/tcp
Critical	9.8	MySQL / MariaDB Default Credentials (MySQL Protocol)	192.168.8.111	3306/tcp
Info	0.0	Obtain list of all port mapper registered programs via RPC	192.168.8.111	111/tcp, 2049/tcp, 49151/tcp, 56126/tcp, 58273/tcp, 111/udp, 2049/udp, 49264/u

Severity	CVSS	Vulnerability	Host	Port
				dp, 50769/udp, 58241/udp
Info	0.0	OpenSSH Detection Consolidation	192.168.8.111	22/tcp
Critical	10.0	Operating System (OS) End of Life (EOL) Detection	192.168.8.111	—
Info	0.0	OS Detection Consolidation and Reporting	192.168.8.111	22/tcp, 21/tcp, 2121/tcp, 445/tcp, 80/tcp, 25/tcp, 23/tcp, 3306/tcp, 137/udp
Critical	9.8	PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities - Active Check	192.168.8.111	80/tcp
Info	0.0	PHP Detection Consolidation	192.168.8.111	80/tcp
Medium	5.3	phpinfo() Output Reporting (HTTP)	192.168.8.111	80/tcp
Medium	4.3	phpMyAdmin 'error.php' Cross Site Scripting Vulnerability	192.168.8.111	80/tcp
Info	0.0	phpMyAdmin Detection (HTTP)	192.168.8.111	80/tcp
Critical	10.0	Possible Backdoor: Ingreslock	192.168.8.111	1524/tcp
Info	0.0	Postfix SMTP Server Detection (SMTP)	192.168.8.111	25/tcp
Critical	9.0	PostgreSQL Default Credentials (PostgreSQL Protocol)	192.168.8.111	5432/tcp
Info	0.0	PostgreSQL Detection (TCP)	192.168.8.111	5432/tcp
Info	0.0	PostgreSQL Detection Consolidation	192.168.8.111	5432/tcp
Info	0.0	PQC Key Exchange (KEX) Algorithm(s) Missing (SSH)	192.168.8.111	22/tcp
Info	0.0	ProFTPD Detection Consolidation	192.168.8.111	2121/tcp
Medium	5.0	QWikiwiki directory traversal vulnerability	192.168.8.111	80/tcp

Severity	CVSS	Vulnerability	Host	Port
Info	0.0	rexec Detection	192.168.8.111	512/tcp
Critical	10.0	rlogin Passwordless Login	192.168.8.111	513/tcp
Info	0.0	RMI Registry Service Detection	192.168.8.111	1099/tcp
Info	0.0	RMI Registry Service Detection	192.168.8.111	56320/tcp
Info	0.0	RPC Portmapper Service Detection (TCP)	192.168.8.111	111/tcp
Info	0.0	RPC Portmapper Service Detection (UDP)	192.168.8.111	111/udp
Info	0.0	rsh Service Detection	192.168.8.111	514/tcp
High	7.5	rsh Unencrypted Cleartext Login	192.168.8.111	514/tcp
Medium	6.0	Samba 3.0.0 <= 3.0.25rc3 MS-RPC Remote Shell Command Execution Vulnerability - A	192.168.8.111	445/tcp
Info	0.0	Service Detection with 'BINARY' Request	192.168.8.111	512/tcp
Info	0.0	Service Detection with 'BINARY' Request	192.168.8.111	513/tcp
Info	0.0	Service Detection with 'GET' Request	192.168.8.111	1524/tcp
Info	0.0	Service Detection with 'GET' Request	192.168.8.111	8787/tcp
Info	0.0	Service Detection with 'GET' Request	192.168.8.111	6667/tcp
Info	0.0	Service Detection with 'GET' Request	192.168.8.111	6697/tcp
Info	0.0	Services	192.168.8.111	2121/tcp
Info	0.0	Services	192.168.8.111	80/tcp
Info	0.0	Services	192.168.8.111	3306/tcp
Info	0.0	Services	192.168.8.111	25/tcp
Info	0.0	Services	192.168.8.111	21/tcp

Severity	CVSS	Vulnerability	Host	Port
Info	0.0	Services	192.168.8.111	5432/tcp
Info	0.0	Services	192.168.8.111	23/tcp
Info	0.0	Services	192.168.8.111	22/tcp
Info	0.0	Services	192.168.8.111	8180/tcp
Info	0.0	SMB log in	192.168.8.111	445/tcp
Info	0.0	SMB Login Successful For Authenticated Checks	192.168.8.111	445/tcp
Info	0.0	SMB NativeLanMan	192.168.8.111	445/tcp
Info	0.0	SMB Remote Version Detection	192.168.8.111	445/tcp
Info	0.0	SMB/CIFS Server Detection	192.168.8.111	445/tcp
Info	0.0	SMB/CIFS Server Detection	192.168.8.111	139/tcp
Info	0.0	SMBv1 Enabled - Active Check	192.168.8.111	445/tcp
Info	0.0	SMTP Server type and version	192.168.8.111	25/tcp
Info	0.0	SSH Protocol Algorithms Supported	192.168.8.111	22/tcp
Info	0.0	SSH Protocol Versions Supported	192.168.8.111	22/tcp
Info	0.0	SSH Server type and version	192.168.8.111	22/tcp
Low	3.7	SSL/TLS: 'DHE_EXPORT' MITM Security Bypass Vulnerability (LogJam)	192.168.8.111	25/tcp
Info	0.0	SSL/TLS: Certificate - Self-Signed Certificate Detection	192.168.8.111	5432/tcp
Info	0.0	SSL/TLS: Certificate - Self-Signed Certificate Detection	192.168.8.111	25/tcp
Medium	5.0	SSL/TLS: Certificate Expired	192.168.8.111	25/tcp
Medium	5.0	SSL/TLS: Certificate Expired	192.168.8.111	5432/tcp
Medium	4.0	SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	192.168.8.111	5432/tcp
Medium	4.0	SSL/TLS: Certificate Signed Using A Weak Signature	192.168.8.111	25/tcp

Severity	CVSS	Vulnerability	Host	Port
		Algorithm		
Info	0.0	SSL/TLS: Collect and Report Certificate Details	192.168.8.111	5432/tcp
Info	0.0	SSL/TLS: Collect and Report Certificate Details	192.168.8.111	25/tcp
Medium	5.9	SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	192.168.8.111	25/tcp
Medium	5.9	SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	192.168.8.111	5432/tcp
Medium	4.3	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	192.168.8.111	25/tcp
Medium	4.3	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	192.168.8.111	5432/tcp
Medium	4.0	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabilit	192.168.8.111	5432/tcp
Medium	4.0	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabilit	192.168.8.111	25/tcp
Info	0.0	SSL/TLS: FTP Missing Support For AUTH TLS	192.168.8.111	2121/tcp
Info	0.0	SSL/TLS: FTP Missing Support For AUTH TLS	192.168.8.111	21/tcp
Info	0.0	SSL/TLS: Hostname discovery from server certificate	192.168.8.111	—
High	7.4	SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	192.168.8.111	5432/tcp
Info	0.0	SSL/TLS: PostgreSQL SSL/TLS Support Detection (PostgreSQL Protocol)	192.168.8.111	5432/tcp
Medium	5.0	SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	192.168.8.111	25/tcp
Medium	5.0	SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	192.168.8.111	5432/tcp
Info	0.0	SSL/TLS: Report Medium Cipher Suites	192.168.8.111	5432/tcp
Info	0.0	SSL/TLS: Report Medium Cipher Suites	192.168.8.111	25/tcp
Info	0.0	SSL/TLS: Report Non Weak Cipher Suites	192.168.8.111	5432/tcp

Severity	CVSS	Vulnerability	Host	Port
Info	0.0	SSL/TLS: Report Non Weak Cipher Suites	192.168.8.111	25/tcp
Info	0.0	SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites	192.168.8.111	25/tcp
Info	0.0	SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites	192.168.8.111	5432/tcp
Info	0.0	SSL/TLS: Report Supported Cipher Suites	192.168.8.111	5432/tcp
Info	0.0	SSL/TLS: Report Supported Cipher Suites	192.168.8.111	25/tcp
Info	0.0	SSL/TLS: Report Weak Cipher Suites	192.168.8.111	25/tcp
Medium	5.9	SSL/TLS: Report Weak Cipher Suites	192.168.8.111	5432/tcp
Medium	4.3	SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)	192.168.8.111	25/tcp
Info	0.0	SSL/TLS: Safe/Secure Renegotiation Support Status	192.168.8.111	25/tcp
Info	0.0	SSL/TLS: Safe/Secure Renegotiation Support Status	192.168.8.111	5432/tcp
Medium	5.3	SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048	192.168.8.111	25/tcp
Medium	5.3	SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048	192.168.8.111	5432/tcp
Info	0.0	SSL/TLS: SMTP 'STARTTLS' Command Detection	192.168.8.111	25/tcp
Low	3.4	SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (	192.168.8.111	25/tcp
Low	3.4	SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (	192.168.8.111	5432/tcp
Info	0.0	SSL/TLS: Untrusted Certificate Detection	192.168.8.111	25/tcp
Info	0.0	SSL/TLS: Untrusted Certificate Detection	192.168.8.111	5432/tcp
Info	0.0	SSL/TLS: Version Detection	192.168.8.111	25/tcp
Info	0.0	SSL/TLS: Version Detection	192.168.8.111	5432/tcp
Low	2.6	TCP Timestamps Information Disclosure	192.168.8.111	—

Severity	CVSS	Vulnerability	Host	Port
Info	0.0	Telnet Banner Reporting	192.168.8.111	23/tcp
Info	0.0	Telnet Service Detection	192.168.8.111	23/tcp
Medium	4.8	Telnet Unencrypted Cleartext Login	192.168.8.111	23/tcp
High	7.5	Test HTTP dangerous methods	192.168.8.111	80/tcp
Critical	10.0	The rexec service is running	192.168.8.111	512/tcp
High	7.5	The rlogin service is running	192.168.8.111	513/tcp
Info	0.0	Traceroute	192.168.8.111	—
Critical	10.0	TWiki < 4.2.4 Multiple XSS / Command Execution Vulnerabilities	192.168.8.111	80/tcp
Medium	6.1	TWiki < 6.1.0 XSS Vulnerability	192.168.8.111	80/tcp
Medium	6.8	TWiki Cross-Site Request Forgery Vulnerability (Sep 2010)	192.168.8.111	80/tcp
Medium	6.0	TWiki CSRF Vulnerability	192.168.8.111	80/tcp
Info	0.0	TWiki Version Detection	192.168.8.111	80/tcp
High	8.1	UnrealIRCd Authentication Spoofing Vulnerability	192.168.8.111	6697/tcp
High	8.1	UnrealIRCd Authentication Spoofing Vulnerability	192.168.8.111	6667/tcp
High	7.5	UnrealIRCd Backdoor	192.168.8.111	6667/tcp
High	7.5	UnrealIRCd Backdoor	192.168.8.111	6697/tcp
Info	0.0	UnrealIRCd Detection	192.168.8.111	6697/tcp
Info	0.0	UnrealIRCd Detection	192.168.8.111	6667/tcp
Info	0.0	Using NetBIOS to retrieve information from a SMB host	192.168.8.111	137/udp
Critical	9.0	VNC Brute Force Login	192.168.8.111	5900/tcp
Info	0.0	VNC Server and Protocol Version Detection (TCP)	192.168.8.111	5900/tc

Severity	CVSS	Vulnerability	Host	Port
				p
Medium	4.8	VNC Server Unencrypted Data Transmission	192.168.8.111	5900/tcp
Info	0.0	VNC Supported 'security types' Detection (TCP)	192.168.8.111	5900/tcp
Critical	9.8	vsftpd Compromised Source Packages Backdoor Vulnerability - Active Check	192.168.8.111	6200/tcp
Critical	9.8	vsftpd Compromised Source Packages Backdoor Vulnerability - Active Check	192.168.8.111	21/tcp
Info	0.0	vsftpd FTP Server Detection (FTP)	192.168.8.111	21/tcp
Medium	4.3	Weak Encryption Algorithm(s) Supported (SSH)	192.168.8.111	22/tcp
Medium	5.3	Weak Host Key Algorithm(s) (SSH)	192.168.8.111	22/tcp
Medium	5.3	Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	192.168.8.111	22/tcp
Low	2.6	Weak MAC Algorithm(s) Supported (SSH)	192.168.8.111	22/tcp
Info	0.0	Web Application Scanning Consolidation / Info Reporting	192.168.8.111	80/tcp
Info	0.0	Web Application Scanning Consolidation / Info Reporting	192.168.8.111	8180/tcp
Info	0.0	X Server Detection	192.168.8.111	6000/tcp