Quick Infrastructure Security Assessment Scanner

Quick Infrastructure Security Assessment Scanner

This tool provides a rapid assessment of an organization's security posture by scanning publicly available information about their digital infrastructure. Use this scanner to identify potential security gaps before conducting a comprehensive assessment.

1. Domain & Email Security Assessment

Check	Tool/Method	What to Look For	Security Implication
SPF Record	Dig command or MXToolbox	Valid SPF record with appropriate restrictions	Prevents email spoofing from unauthorized servers
DKIM Implementation	Email header analysis	DKIM signatures in email headers	Ensures email authenticity and prevents tampering
DMARC Policy	MXToolbox or dmarcian	DMARC record with appropriate policy (none/quarantine/reject)	Provides instructions on handling authentication failures
SSL/TLS Certificate	SSL Labs or Qualys SSL Scanner	Valid certificate, strong ciphers, no vulnerabilities	Secures communications and prevents MitM attacks
DNSSEC Implementation	DNSViz or Verisign DNSSEC Debugger	Properly signed DNS records	Prevents DNS poisoning and hijacking attacks

2. Web Infrastructure Assessment

Check	Tool/Method	What to Look For	Security Implication
Website Security Headers	SecurityHeaders.com	Proper implementation of CSP, HSTS, X-Frame-Options	Protects against common web vulnerabilities
CMS Version	Wappalyzer or BuiltWith	Up-to-date CMS version	Outdated CMS versions may contain known vulnerabilities
Open Ports	Shodan or Censys	Unnecessary open ports or services	Reduces attack surface and potential entry points
Content Delivery Network	HTTP headers analysis	CDN implementation and security features	CDNs can provide DDoS protection and WAF capabilities
Web Application Firewall	WafW00f or custom HTTP requests	WAF presence and configuration	Protects web applications from common attacks

3. Cloud Services & SaaS Assessment

Check	Tool/Method	What to Look For	Security Implication
Cloud Storage Exposure	GrayhatWarfare or custom scripts	Publicly accessible cloud storage buckets	Prevents data leakage from misconfigured storage
SaaS Security Settings	Admin console review (with permission)	MFA enforcement, session policies, sharing restrictions	Ensures SaaS applications follow security best practices
API Security	API documentation review	Authentication requirements, rate limiting	Prevents unauthorized access or API abuse
Shadow IT Detection	DNS traffic analysis, browser extension scan	Unauthorized SaaS applications	Identifies unmanaged services that may pose security risks

SSO Implementation	Login page analysis	Single Sign-On with strong authentication	Centralizes authentication and enhances security controls

4. Social Engineering Vulnerability Assessment

Check	Tool/Method	What to Look For	Security Implication
Email Format Analysis	Email header analysis	Consistent email naming conventions	Helps users identify phishing attempts with unusual formats
Employee Information Exposure	LinkedIn, public directories	Excessive personal or role information	Could be used for targeted social engineering attacks
Password Policy Indicators	Password reset process analysis	Strong password requirements	Indicates overall security maturity and prevents brute force
Security Awareness Indicators	Email footer analysis, public documentation	Security awareness messaging	Suggests employee security training and awareness level
Social Media Presence	Social media platform analysis	Excessive information sharing, location data	Could reveal sensitive information useful for attackers

5. CRM and Business Systems Assessment

Check	Tool/Method	What to Look For	Security Implication
CRM Security Features	Documentation review (with permission)	Data encryption, access controls, audit logging	Ensures customer data is properly protected
Third-Party Integrations	API endpoint analysis	Secure API connections, OAuth implementation	Prevents unauthorized access through connected systems
Mobile App Security	Mobile app analysis tools	Secure data storage, transport security	Prevents data leakage through mobile applications

Authentication Methods	Login page analysis	MFA options, SSO integration	Strong authentication prevents account compromise
Session Management	Session cookie analysis	Secure cookies, appropriate timeout settings	Prevents session hijacking and unauthorized access

6. Assessment Process

6.1 Information Gathering

- Request the following information from the client:
- Primary domain names
- Email domains
- Key SaaS platforms used (CRM, marketing tools, etc.)
- Cloud service providers
- Public-facing web applications

6.2 Quick Scan Execution

- Perform automated checks using the tools listed above
- Document findings in the assessment report template
- Categorize issues by severity (Critical, High, Medium, Low)
- Note any limitations of the quick scan approach

6.3 Reporting

- Compile findings into an executive summary highlighting key risks
- Provide detailed technical findings with evidence
- Include actionable recommendations for each issue
- Suggest areas for deeper assessment where needed

7. Sample Assessment Report Template

Executive Summary

This quick infrastructure security assessment evaluated [Company Name]'s external security posture based on publicly available information and provided information about their digital infrastructure. The assessment identified [X] critical, [X] high, [X] medium, and [X] low-severity issues that should be addressed to improve security.

Key Findings:

- Finding 1 (Severity: Critical/High/Medium/Low)
- Finding 2 (Severity: Critical/High/Medium/Low)
- Finding 3 (Severity: Critical/High/Medium/Low)

Recommended Next Steps:

- Immediate action 1
- Short-term action 2
- Long-term security improvement 3

8. Limitations and Next Steps

Important Note: This quick assessment is designed to identify obvious security gaps using publicly available information and basic scanning techniques. It is not a substitute for a comprehensive security audit as outlined in the AI Security Audit Assessment Technical Specification. Findings should be validated with more thorough testing before implementing major changes.

8.1 Recommended Follow-up Assessments

- Comprehensive vulnerability assessment
- Penetration testing of critical systems
- Internal network security assessment
- Data protection and privacy compliance review

- Cloud security configuration review

9. Tool References

Tool	URL	Purpose
MXToolbox	https://mxtoolbox.com/	Email and DNS security checking
SSL Labs	https://www.ssllabs.com/ssl-test/	SSL/TLS configuration analysis
SecurityHeaders.com	https://securityheaders.com/	Web security header analysis
Shodan	https://www.shodan.io/	Internet-connected device discovery
DNSViz	https://dnsviz.net/	DNS and DNSSEC visualization and analysis
Wappalyzer	https://www.wappalyzer.com/	Web technology stack identification
GrayhatWarfare	https://grayhatwarfare.com/	Public cloud storage bucket discovery