Vulnerability Assessment Guide for SMEs

A practical guide to understanding, performing, and acting on vulnerability assessments for your business.

42%	14d	CVSS	80%
SMES WITH OUTDATED SOFTWARE	CE+ CRITICAL PATCH WINDOW	INDUSTRY SCORING STANDARD	ATTACKS PREVENTABLE WITH BASICS

1 What is Vulnerability Scanning?

A **vulnerability scan** (also known as a vulnerability assessment) is an automated process that identifies known security weaknesses in your IT systems, networks, and applications. Scanning tools compare your systems against databases of known vulnerabilities (such as the National Vulnerability Database) and report any that are found, along with severity ratings and remediation guidance.

Vulnerability scanning is a **proactive, preventive measure** — it finds weaknesses before attackers do. It is a fundamental component of any cybersecurity programme and is specifically required for Cyber Essentials Plus certification.

Internal vs External Scans

External Vulnerability Scan

Scans your organisation from the **outside** — simulating what an attacker on the internet can see and exploit.

- ✓ Targets public-facing IP addresses and domains
- ✓ Identifies open ports, exposed services, and misconfigurations
- ✓ Checks for known CVEs on internet-facing systems
- ✓ Tests SSL/TLS configuration and certificate validity
- ✓ Does not require access to internal network

Internal Vulnerability Scan

Scans your organisation from the **inside** — identifying vulnerabilities visible from within your network.

- ✓ Targets workstations, servers, printers, and network devices
- ✓ Identifies missing patches, weak configurations, and EOL software
- ✓ Can be authenticated (with credentials) for deeper analysis
- ✓ Finds vulnerabilities not visible from the internet
- ✓ Requires network access or an agent installed on devices

Vulnerability Scanning vs Penetration Testing

ASPECT	VULNERABILITY SCANNING	PENETRATION TESTING
Approach	Automated tool-based scanning against known vulnerability databases	Manual, human-led testing that attempts to exploit vulnerabilities
Depth	Broad coverage — identifies known weaknesses across many systems	Deep — attempts to chain vulnerabilities and achieve specific objectives
Frequency	Monthly or quarterly (automated, repeatable)	Annual or after significant changes
Cost	£500 – £3,000 per scan	£5,000 – £30,000+ per engagement
Output	Automated report with CVE references and remediation advice	Detailed narrative report with proof-of-concept exploits
CE+ Requirement	Yes — both internal and external scans required	Not required for CE+ (but recommended annually)

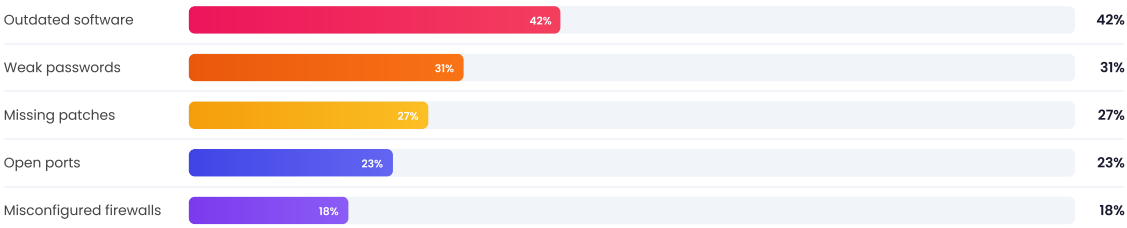
Do You Need Both?

Yes. Vulnerability scanning and penetration testing serve different purposes and are complementary. Scanning provides **breadth** (finding known issues across your entire estate), while penetration testing provides **depth** (testing whether vulnerabilities can actually be exploited to cause harm). For CE+ compliance, vulnerability scanning is mandatory. Penetration testing is an additional best practice.

2 Common Vulnerabilities Found in SMEs

Based on aggregated scan data, these are the most frequently discovered vulnerabilities in small and medium-sized businesses.

Vulnerability Prevalence in UK SMEs



Vulnerability Type Breakdown

VULNERABILITY TYPE	DESCRIPTION	RISK LEVEL	TYPICAL FIX TIME
Outdated OS (e.g., Windows 10 EOL)	Operating systems no longer receiving vendor security patches, exposed to all future vulnerabilities	CRITICAL	1–4 weeks (upgrade/replace)
Missing security patches	Known vulnerabilities with available patches not yet applied to systems	HIGH	1–14 days (patch deployment)
Weak/default passwords	Systems using factory defaults, common passwords, or credentials found in breach databases	HIGH	1–2 days (password reset)
Unsecured remote access	RDP, VPN, or remote management exposed to internet without MFA or IP restrictions	CRITICAL	1–3 days (reconfigure)
Unnecessary open ports	Network services exposed to the internet that are not required for business operations	MEDIUM	1–2 days (close ports)
Outdated SSL/TLS	Weak encryption protocols (TLS 1.0/1.1) or expired/misconfigured certificates	MEDIUM	1–3 days (update config)
Misconfigured firewalls	Overly permissive rules, unused rules, or firewall bypasses allowing unintended traffic	HIGH	2–5 days (rule audit)
Missing anti-malware	Devices without active, up-to-date endpoint protection	HIGH	1 day (deploy and configure)
End-of-life applications	Third-party software (Java, Flash, old browsers) no longer receiving security updates	MEDIUM	1–2 weeks (remove/replace)
Information disclosure	Server banners, error pages, or directory listings revealing software versions and system details	LOW	1 day (configuration change)

3 Understanding CVSS Scoring

The Common Vulnerability Scoring System (CVSS) provides a standardised way to rate the severity of security vulnerabilities.

CVSS scores range from **0.0 to 10.0**, with higher scores indicating more severe vulnerabilities. The score considers factors including how easily the vulnerability can be exploited, whether network access is required, whether user interaction is needed, and the potential impact on confidentiality, integrity, and availability.

SCORE RANGE	RATING	DESCRIPTION	CE+ PATCHING REQUIREMENT
9.0 – 10.0	CRITICAL	Easily exploitable, significant impact, often remotely exploitable without authentication	Must be patched within **14 days**. Immediate if actively exploited.
7.0 – 8.9	HIGH	Significant impact, may require some conditions to exploit but remains a serious threat	Must be patched within **14 days**.
4.0 – 6.9	MEDIUM	Moderate impact, may require specific conditions, local access, or user interaction to exploit	Should be patched within **30 days**.
0.1 – 3.9	LOW	Limited impact, difficult to exploit, or requires unlikely conditions to be effective	Patch at next scheduled maintenance window.

Context Matters More Than Score Alone

A CVSS score of 6.5 (Medium) on an internet-facing web server may be more urgent than a 9.0 (Critical) on a system isolated from the network. Always consider the **business context**: is the system internet-facing? Does it hold sensitive data? Is it a critical business system? Prioritise accordingly.

4 How to Interpret Scan Results

Understanding your scan report and knowing what to prioritise is essential for effective remediation.

Anatomy of a Scan Report

A typical vulnerability scan report contains the following key elements for each finding:

- **CVE Identifier:** A unique identifier (e.g., CVE-2024-12345) from the Common Vulnerabilities and Exposures database. This allows you to research the specific vulnerability and find vendor patches.
- **CVSS Score:** The numerical severity rating (0.0–10.0) indicating how serious the vulnerability is based on exploitability and impact factors.
- **Affected System:** The specific host, IP address, or application where the vulnerability was found.
- **Description:** A technical explanation of the vulnerability, what it affects, and how it could be exploited.
- **Solution:** Recommended remediation steps, typically including specific patches, configuration changes, or version upgrades required.
- **References:** Links to vendor advisories, NIST NVD entries, and exploit databases for further research.

Remediation Prioritisation Matrix

Not all vulnerabilities need to be fixed immediately. Use this matrix to determine your remediation priority based on both **severity** and **exposure**:

SEVERITY / EXPOSURE	INTERNET-FACING SYSTEMS	INTERNAL (AUTHENTICATED)	ISOLATED / AIR-GAPPED
CRITICAL (9.0+)	Fix immediately (24–48 hrs)	Fix within 7 days	Fix within 14 days
HIGH (7.0–8.9)	Fix within 7 days	Fix within 14 days	Fix within 30 days
MEDIUM (4.0–6.9)	Fix within 14 days	Fix within 30 days	Next maintenance window
LOW (0.1–3.9)	Fix within 30 days	Next maintenance window	Accept risk or schedule

Prioritisation Order

When faced with a long list of vulnerabilities, remediate in this order:

- **Priority 1:** Critical and High vulnerabilities on internet-facing systems — these are actively targetable by attackers and represent the greatest immediate risk.
- **Priority 2:** Critical vulnerabilities on internal systems — while not directly internet-exposed, these could be exploited after an initial breach for lateral movement.
- **Priority 3:** High vulnerabilities on internal systems, particularly those holding sensitive data, PII, or financial information.
- **Priority 4:** Medium vulnerabilities on internet-facing systems — these may be harder to exploit but still represent unnecessary risk on exposed assets.
- **Priority 5:** Remaining Medium and Low vulnerabilities — address during regular maintenance cycles to maintain a clean security posture.

Example Scan Report Breakdown

A typical SME with 50 devices might see a scan report containing: **2–5 Critical** findings (often missing OS patches or EOL software), **10–20 High** findings (missing application patches, weak configurations), **30–50 Medium** findings (outdated SSL, information disclosure), and **50+ Low/Informational** findings (minor configuration issues). Focus your immediate effort on the Critical and High findings — these are what will fail a CE+ assessment.

False Positives

Not every finding in a scan report is a genuine vulnerability. Scanners sometimes report **false positives** — items flagged as vulnerable that are actually mitigated by other controls, compensating measures, or where the scanner has misidentified the software version. Always verify Critical and High findings before investing significant remediation effort. Document any confirmed false positives for your records.

5 Scanning Tools & Frequency

Choosing the right tools and establishing a regular scanning cadence is essential for maintaining a strong security posture.

Recommended Vulnerability Scanning Tools

Nessus (Tenable)

Industry-leading vulnerability scanner with extensive plugin library covering over 80,000 CVEs. Offers both agent-based and network-based scanning. Strong compliance checking capabilities including CIS Benchmarks.

Commercial | Internal + External | Agent & Network | From £2,500/yr

Qualys VMDR

Cloud-based vulnerability management, detection, and response platform. Excellent for organisations with distributed environments. Real-time visibility with continuous monitoring and automated prioritisation.

Commercial | Cloud-Based | Agent & Scanner | Per-asset pricing

OpenVAS (Greenbone)

Open-source vulnerability scanner with a comprehensive feed of network vulnerability tests. Good option for budget-conscious organisations. Community edition is free; enterprise edition available for commercial support.

Open Source / Commercial | Internal + External | Network Scanner | Free (community)

Microsoft Defender Vulnerability Management

Built into Microsoft 365 E5 and Defender for Endpoint. Ideal for Microsoft-centric environments. Provides continuous vulnerability assessment for Windows, macOS, Linux, iOS, and Android devices without additional scanning infrastructure.

Included in M365 E5 | Agent-Based | Continuous | Microsoft ecosystem

Scanning Frequency Recommendations

SCAN TYPE	MINIMUM	RECOMMENDED	TRIGGER EVENTS
External vulnerability scan	Quarterly	**Monthly**	New public-facing services, IP changes, after firewall changes
Internal vulnerability scan	Quarterly	**Monthly**	New devices added, OS upgrades, after major deployments
Authenticated scan (internal)	Quarterly	**Monthly**	After patch cycles, new software deployments, policy changes
Web application scan	Quarterly	**After every release**	Code changes, new features, third-party library updates
Pre-CE+ assessment scan	Before assessment	**2 weeks before**	Always run before scheduling your CE+ assessment

Authenticated vs Unauthenticated Scans

Authenticated Scans

The scanner logs into each device using provided credentials, gaining **deeper visibility** into installed software, patch levels, and configurations.

- ✓ Detects significantly more vulnerabilities (3–5x more findings)
- ✓ Identifies missing patches at the application level
- ✓ Checks local configurations and registry settings
- ✓ Required for CE+ internal device assessment
- ✓ Requires service account credentials (read-only)

Unauthenticated Scans

The scanner probes systems **from outside** without credentials, seeing only what is visible over the network.

- ✓ Good for quick external perimeter checks
- ✓ Identifies open ports and exposed services
- ✓ Detects remotely exploitable vulnerabilities
- ✓ Cannot see installed software or patch levels
- ✓ Will miss many internal vulnerabilities

Always Run Authenticated Scans for CE+

The CE+ assessment requires **authenticated internal scans** on a representative sample of your devices. An unauthenticated scan alone is not sufficient — it will miss the majority of missing patches and configuration issues that the assessor will find. Ensure your scanning tool supports credential-based scanning and that you have appropriate service accounts configured.

6 Vulnerability Scanning & Cyber Essentials Plus

Vulnerability scanning is a core component of the CE+ assessment. Here is exactly what is required and what assessors look for.

CE+ Scanning Requirements

During the Cyber Essentials Plus assessment, the Certification Body assessor will conduct vulnerability scans as part of the hands-on technical verification. Understanding what they test helps you prepare effectively.

- → **External vulnerability scan:** The assessor scans all public-facing IP addresses in scope for known vulnerabilities, open ports, misconfigurations, and outdated software. Any Critical or High vulnerabilities on internet-facing systems will result in a fail.
- → **Internal authenticated scan:** The assessor runs authenticated scans on a representative sample of internal devices (workstations, laptops, servers). The sample covers each device type, operating system, and location within the defined scope.
- → **Sample-based approach:** Not every device is scanned, but if any sampled device fails, the assessor may expand the sample size or require remediation across all similar devices before passing.

What Assessors Look For

CHECK	PASS CRITERIA	COMMON FAILURE REASONS
Missing OS patches	No Critical/High patches older than 14 days	Windows updates deferred, macOS not updated, Linux kernels outdated
Missing app patches	All applications at latest stable version or within 14-day window	Outdated Chrome, Firefox, Adobe, Java, Zoom, Teams
EOL software present	No end-of-life software installed	Old Office versions, Windows 10 past EOL, Python 2.x, IE
Open ports (external)	Only explicitly justified ports open	Forgotten test servers, legacy services, RDP exposed
SSL/TLS configuration	TLS 1.2+ only, valid certificates	TLS 1.0/1.1 still enabled, expired certs, self-signed certs on public services
Default credentials	No factory-default passwords on any system	Router admin passwords, printer management, NAS devices

Pre-Assessment Checklist

- ☐ **Run your own external vulnerability scan** at least 2 weeks before the assessment and remediate all Critical/High findings
- ☐ **Run authenticated internal scans** on a sample matching what the assessor will test (each OS type, each device type)
- ☐ **Patch all Critical and High vulnerabilities** — ensure no critical/high patch is older than 14 days on any in-scope device
- ☐ **Remove all end-of-life software** from every device in scope (check both OS and applications)
- ☐ **Close unnecessary open ports** on your external perimeter and document justification for any that remain open
- ☐ **Verify SSL/TLS configuration** — disable TLS 1.0/1.1, ensure all certificates are valid and properly configured
- ☐ **Change all default passwords** on routers, firewalls, printers, NAS devices, and any other network equipment
- ☐ **Test EICAR file downloads** through browsers and email on sample devices to verify malware protection blocks them

Cloudswitched Includes Vulnerability Scanning in All CE+ Packages

Every Cloudswitched CE+ package includes comprehensive pre-assessment vulnerability scanning — both external and internal authenticated scans. We identify and help you remediate all findings before your official assessment, maximising your chance of passing first time. Our scans use the same tools and methodology as accredited assessors, so there are no surprises on examination day.

Our Scanning Services Include

- ✓ External perimeter vulnerability scan
- ✓ Internal authenticated device scanning
- ✓ Prioritised remediation report

Ongoing Scanning Options

- ✓ Monthly scheduled vulnerability scans
- ✓ Continuous monitoring dashboards
- ✓ Automated alerting for critical findings

Ready to Assess Your Vulnerabilities?

Cloudswitched includes vulnerability scanning in all CE+ packages — find and fix issues before your assessor does.

www.cloudswitched.com/services/cyber-essentials

info@cloudswitched.com