CLOUDSWITCHED

FREE RESOURCE — CYBER SECURITY GUIDE

Vulnerability Assessment Guide for SMEs

A practical guide to understanding, performing, and acting on vulnerability assessments — from scan types and CVSS scoring through to remediation prioritisation and Cyber Essentials Plus alignment.

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UK SMES RUNNING OUTDATED SOFTWARE	CE+ CRITICAL PATCH WINDOW	INDUSTRY SEVERITY SCORING STANDARD	ATTACKS PREVENTABLE WITH THE BASICS

SCAN TYPES · CVSS SCORING · PRIORITISATION · CE+ ALIGNMENT

PREPARED FOR	PREPARED BY	VERSION	FORMAT
Cloudswitched Knowledge Library	Cloudswitched Ltd.	2026 Edition	Read-only PDF

01

What is vulnerability scanning?

A **vulnerability scan** (also called a vulnerability assessment) is an automated process that identifies known security weaknesses in your IT systems, networks, and applications. Scanning tools compare your estate against databases of known vulnerabilities — such as the National Vulnerability Database — and report findings with severity ratings and remediation guidance. It is a **proactive, preventive** control: it finds weaknesses before attackers do, and is a fundamental requirement of Cyber Essentials Plus.

Internal vs external scans

External vulnerability scan

- Scans from the **outside** — what an internet attacker sees
- Targets public-facing IPs and domains
- Open ports, exposed services, misconfigurations
- Tests SSL / TLS and certificate validity

Internal vulnerability scan

- Scans from the **inside** — what is visible within your network
- Targets workstations, servers, printers, network devices
- Missing patches, weak configs, EOL software
- Authenticated mode gives far deeper analysis

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 — chains vulnerabilities together to 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
CE+ requirement	Yes — internal and external both required	Not required (but recommended annually)

DO YOU NEED BOTH?

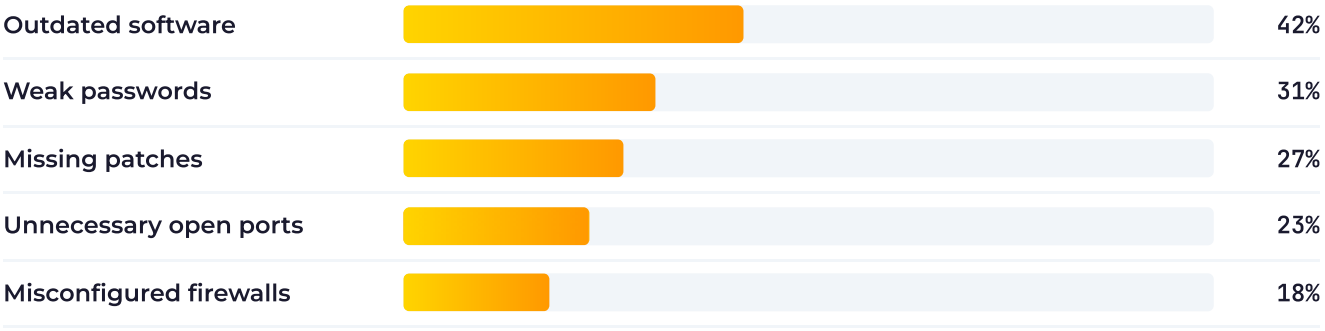
Yes — the two are complementary. Scanning gives you **breadth** (known issues across the whole estate); penetration testing gives you **depth** (whether vulnerabilities are actually exploitable). Scanning is mandatory for CE+; pentesting is a best practice on top.

02

Common vulnerabilities found in SMEs

Based on aggregated UK SME scan data, these are the most frequently discovered vulnerabilities — with typical fix windows and risk levels.

Prevalence in UK SMEs



Vulnerability type breakdown

VULNERABILITY TYPE	RISK	TYPICAL FIX TIME
Outdated OS (e.g. Windows 10 EOL)	CRITICAL	1–4 weeks (upgrade or replace)
Missing security patches	HIGH	1–14 days (patch deployment)
Weak / default passwords	HIGH	1–2 days (reset and policy)
Unsecured remote access (RDP / VPN)	CRITICAL	1–3 days (reconfigure, add MFA)
Outdated SSL / TLS	MEDIUM	1–3 days (update config)
Misconfigured firewalls	HIGH	2–5 days (rule audit)
End-of-life applications (Java, old browsers)	MEDIUM	1–2 weeks (remove or replace)

03

Understanding CVSS scoring

The **Common Vulnerability Scoring System** (CVSS) rates severity on a 0.0–10.0 scale — the higher the score, the more severe the vulnerability. The number reflects how easily an issue is exploited, whether network access or user interaction is required, and the potential impact on confidentiality, integrity, and availability.

CVSS score ranges & CE+ patching requirements

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

How CVSS scoring is constructed

Attack vector. Network, adjacent, local, or physical — how close an attacker has to be.

Attack complexity. How much skill or specific conditions are required to exploit.

Privileges required. None, low, or high — does the attacker need authenticated access first?

User interaction. Whether a victim has to click something for the exploit to land.

Impact — CIA. Confidentiality, integrity, and availability impact: none, low, or high.

CONTEXT MATTERS MORE THAN SCORE ALONE

A CVSS 6.5 (Medium) on an internet-facing web server may be more urgent than a 9.0 (Critical) on an isolated system. Always factor in **business context**: is the system internet-facing, does it hold sensitive data, is it business-critical? Prioritise on context × score, not score alone.

04

How to interpret scan results

Understanding your scan report and knowing what to prioritise is essential. Each finding in a typical report carries a CVE identifier, a CVSS score, the affected system, a technical description, recommended solution, and references — the building blocks of an effective remediation plan.

Anatomy of a scan finding

CVE identifier & CVSS score. A unique reference (e.g. `CVE-2024-12345`) plus a 0.0–10.0 severity score reflecting exploitability and impact.

Affected system. The specific host, IP, or application where the vulnerability was found.

Solution & references. Recommended patches or configuration changes, plus links to vendor advisories, NIST NVD, and exploit databases.

Remediation prioritisation matrix

SEVERITY	INTERNET-FACING	INTERNAL (AUTHENTICATED)	ISOLATED / AIR-GAPPED
CRITICAL	**24–48 hours**	Within 7 days	Within 14 days
HIGH	Within 7 days	Within 14 days	Within 30 days
MEDIUM	Within 14 days	Within 30 days	Next maintenance window
LOW	Within 30 days	Next maintenance window	Accept risk or schedule

Prioritisation order — remediate in this sequence

1. **Critical / High on internet-facing systems** — actively targetable, greatest immediate risk.
2. **Critical on internal systems** — exploitable after an initial breach for lateral movement.
3. **High on internal systems** holding sensitive data, PII, or financial information.
4. **Medium on internet-facing systems** — unnecessary risk on exposed assets.
5. **Remaining Medium and Low** — address during regular maintenance cycles.

FALSE POSITIVES ARE REAL

Verify Critical and High findings before significant remediation effort — scanners sometimes flag items already mitigated by compensating controls or where the version was misidentified.

05

Scanning tools & frequency

Choosing the right tools and establishing a regular cadence is essential for maintaining a strong security posture. The recommended platforms below cover the spectrum from enterprise to open-source.

Recommended vulnerability scanning tools

Nessus (Tenable)

Industry-leading scanner with an extensive plugin library covering over 80,000 CVEs. Strong compliance checking including CIS Benchmarks. Agent-based and network-based scanning.

COMMERCIAL | INTERNAL + EXTERNAL | FROM £2,500 / YR

Qualys VMDR

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

COMMERCIAL | CLOUD-BASED | PER-ASSET PRICING

OpenVAS (Greenbone)

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

OPEN SOURCE | INTERNAL + EXTERNAL | FREE (COMMUNITY)

Microsoft Defender Vulnerability Management

Built into M365 E5 and Defender for Endpoint. Continuous assessment for Windows, macOS, Linux, iOS, and Android without separate scanning infrastructure.

INCLUDED IN M365 E5 | AGENT-BASED | MICROSOFT ECOSYSTEM

PICK WHAT YOUR TEAM WILL ACTUALLY RUN

The best scanner is the one that gets used. For Microsoft-centric SMEs, Defender VM removes friction. For mixed estates with stronger compliance requirements, Nessus and Qualys are well-trodden choices. OpenVAS suits teams with the time to manage it themselves.

05

Scanning frequency & authenticated scans

How often you scan depends on what is being scanned and how exposed it is — the cadence below covers most UK SMEs.

Scanning frequency — minimum vs recommended

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

Authenticated vs unauthenticated scans

Authenticated scans

- Scanner logs in with credentials
- Detects 3–5× more vulnerabilities
- Sees missing app-level patches and local config
- Required for CE+ internal assessment

Unauthenticated scans

- Probes from outside without credentials
- Good for quick perimeter checks
- Cannot see installed software or patches
- Misses most internal vulnerabilities

ALWAYS RUN AUTHENTICATED SCANS FOR CE+

The CE+ assessment requires **authenticated internal scans** on a representative sample of devices. Unauthenticated scans miss most of what the assessor will find — configure credentialed service accounts before scanning.

06

Vulnerability scanning & Cyber Essentials Plus

Vulnerability scanning is a **core component** of the CE+ assessment. During the hands-on technical verification, the Certification Body assessor will conduct vulnerability scans across your external perimeter and a sample of internal devices — understanding what they test helps you prepare effectively.

What the assessor will scan

External vulnerability scan. All public-facing IPs in scope, for known vulnerabilities, open ports, misconfigurations, and outdated software. Any Critical or High on internet-facing systems is a fail.

Internal authenticated scan. Authenticated scans on a representative sample of workstations, laptops, and servers — covering each device type, OS, and location within scope.

Sample-based approach. Not every device is scanned, but if any sampled device fails the assessor can expand the sample size or require remediation across all similar devices before passing.

What assessors look for — and where SMEs typically fail

CHECK	PASS CRITERIA	COMMON FAILURE REASONS
Missing OS patches	No Critical/High patches older than 14 days	Windows updates deferred, macOS not updated, kernels outdated
Missing app patches	Apps at latest stable or within 14-day window	Outdated Chrome, Firefox, Adobe, Java, Zoom, Teams
EOL software	No end-of-life software present	Old Office versions, Windows 10 past EOL, Python 2.x, IE
External open ports	Only explicitly justified ports open	Forgotten test servers, legacy services, RDP exposed
SSL / TLS	TLS 1.2+ only, valid certificates	TLS 1.0/1.1 enabled, expired certs, self-signed on public
Default credentials	None on any in-scope system	Router admin passwords, printers, NAS devices

06

Pre-assessment preparation

The single biggest predictor of a CE+ first-time pass is preparation in the **two weeks before** the assessment date. Work through the items below in order — they line up with the most common failure modes on the day.

Pre-assessment checklist — do this first

- **Run your own external 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 every Critical and High** within the 14-day window across all in-scope devices.
- **Remove all end-of-life software** — OS and applications — from every in-scope device.
- **Close unnecessary external ports**; document business justification for any that remain open.
- **Verify SSL / TLS** — disable TLS 1.0/1.1, replace expired or self-signed certificates on public services.
- **Change all default passwords** on routers, firewalls, printers, NAS devices, and other network equipment.

CLOUDSWITCHED CE+ PACKAGES INCLUDE VULNERABILITY SCANNING

Every Cloudswitched CE+ package includes pre-assessment vulnerability scanning — both external and authenticated internal — using the same tools and methodology as accredited assessors. We identify and help you remediate all findings before your official assessment, maximising your chance of passing first time.

CLOUDSWITCHED

VULNERABILITY ASSESSMENT & CYBER ESSENTIALS PLUS

info@cloudswitched.com

New London House, 6 London St
London EC3R 7LP · United Kingdom