Internal and external vulnerability scanning

Turn a scan output into decisions and remediation. Understand the observation point, what was actually tested and how findings are closed.

Vulnerability scanning systematically checks scoped assets for known software weaknesses, missing patches, risky services and security configuration issues. Its output is a set of candidate findings to validate. It provides a point-in-time view; it is not, by itself, a penetration test, proof of compromise or a guarantee of security.

Two distinct viewpoints

Internal scanning

From an internal network or approved VPN / scanning sensor

Assess weaknesses in servers, endpoints and network devices visible from an internal access point. Separate network segments need distinct viewpoints.

Missing patches, unsupported versions, unnecessary services, weak configurations and reachability boundaries. Credentialed checks can inspect local state more deeply.

One sensor does not represent the entire network. Assets blocked by firewalls or failed authentication cannot be interpreted as having no vulnerabilities.

External scanning

From an approved location outside the organization’s internet boundary

Understand the public attack surface and security posture of internet-reachable services. The external view does not replace internal access.

Unexpected exposed ports, public management surfaces, outdated services, TLS issues and application alerts. Validate each finding with the service owner.

A CDN/WAF may expose only the edge; a filtered port does not prove the service is absent. Do not infer the state of unobserved internal patches.

Vantage point and authentication are independent dimensions.

No. Vantage point and authentication are independent dimensions. An internal scan can be uncredentialed; an internet-facing application can be assessed using a test account. Record both dimensions separately.

Scanning workflow

1. Define scope and engagement rules

Record the owner, IP/CIDR and domain list, exclusions, schedule, source IP, request limits and emergency contact. Confirm third-party assets separately.

Verify segment reachability internally and DNS, CDN and asset ownership externally. Separate critical services from the small pilot group.

Deliverable: Approved scope inventory + rules of engagement

Common pitfall: A domain using an organization's name may not belong to it.

2. Validate visibility and inventory

Reconcile CMDB, cloud inventory and DNS records. Perform controlled service discovery only on approved targets; map each asset to technical and business owners.

Separate reachable, unreachable and excluded assets. Record sensor placement and firewall effects in the report.

Deliverable: Target–owner–sensor mapping + reachability gaps

Common pitfall: An open port alone is neither a vulnerability nor evidence of unauthorized access.

3. Prepare the scanning profile

Choose current check feeds, a scope-appropriate port list, timeouts and concurrency. For credentialed scans use a separate, traceable account with required permissions; keep passwords out of reports.

Check authentication success in tool output. For web scans verify that sessions remain authenticated and out-of-scope URLs are excluded.

Deliverable: Versioned profile + successful access validation

Common pitfall: A successful login does not prove every local check executed.

Scanning workflow

4. Start with a small monitored pilot

Begin with a representative, lower-impact asset group. Monitor service health, latency and errors with operations. Stop when agreed load or outage thresholds are exceeded.

Expand scope gradually after the pilot. Validate active web tests in non-production first; do not apply generic IT profiles to OT/ICS without vendor approval and a safety assessment.

Deliverable: Pilot record + execution timeline + stop events

Common pitfall: Even a tool using passive analysis can generate HTTP traffic through a browser or spider.

5. Validate candidate findings

Deduplicate by asset and root cause. Check version, installed package, configuration, backported fixes and reachability evidence. Do not execute an exploit when safe inspection is sufficient.

Record evidence and rationale for false positives, and uncertainty for untested areas. Redact personal data, tokens and passwords in attachments.

Deliverable: Validated finding + evidence reference + confidence

Common pitfall: A scanner-suggested CVE is not confirmed until product and version applicability are checked.

6. Prioritize using business risk

Assess CVSS technical severity alongside internet exposure, known exploitation, EPSS, asset criticality, data and existing controls. Do not add unlike scores as though they measure the same thing.

Assign each validated finding an owner, organization-approved deadline and remediation plan. Document temporary mitigation and time-bound risk acceptance when delayed.

Deliverable: Prioritized backlog + owner + due date

Common pitfall: Absence from KEV does not mean safe; EPSS measures neither business impact nor your own compromise probability.

7. Remediate, retest and measure

Apply patches, configuration or access restrictions through change management. Retest from the same viewpoint with appropriate checks; also verify that the service still works.

Retain before/after evidence, profile version and retest date. Reassess after new assets or significant changes; choose cadence based on risk and applicable requirements.

Deliverable: Retest evidence + closure decision + tracking metrics

Common pitfall: Closing a ticket does not replace technical closure evidence.

Tool selection and limits

Nmap / Discovery / service inventory

Inventory visible ports and services to narrow the next scanning profile.

Not a complete patch or vulnerability assessment; validate service identification.

Source available; review its custom licence terms.

Download / setup: https://nmap.org/download.html

Documentation: https://nmap.org/book/man.html

Greenbone / OpenVAS / Network vulnerability scanning

Assess known weaknesses and supported authenticated local checks.

Feed freshness and profiles matter. The community container guide is for learning/testing; assess production design separately.

Community and commercial options

Download / setup: https://greenbone.github.io/docs/latest/22.4/container/index.html

Documentation: https://greenbone.github.io/docs/latest/

Tenable Nessus / Network / local checks

Server and device checks, including local patch and configuration review with credentials.

Verify that credentialed checks actually ran. Check licence scope before downloading.

Commercial; edition and usage terms vary.

Download / setup: https://www.tenable.com/downloads/nessus

Documentation: https://docs.tenable.com/nessus/

Qualys VMDR / Enterprise vulnerability management

Manage sensor/agent coverage, finding tracking and remediation workflows across distributed assets.

Not a single downloadable desktop scanner; plan sensor placement and subscription scope.

Commercial platform / trial request

Download / setup: https://www.qualys.com/free-trial-new

Documentation: https://www.qualys.com/apps/vulnerability-management-detection-response

Tool selection and limits

ZAP / Web / API dynamic analysis

Passive alerts in web traffic and separately enabled active application tests.

The baseline spider makes HTTP requests; passive analysis is not zero traffic. Active testing needs separate scope and test accounts.

Free, open source

Download / setup: https://www.zaproxy.org/download/

Documentation: https://www.zaproxy.org/docs/docker/baseline-scan/

Burp Suite / Web validation / dynamic analysis

Validate candidate findings with a proxy and manual inspection; automated scanning in eligible paid editions.

Community does not include automated Burp Scanner. Sessions, object permissions and business logic need separate attention.

Community and paid editions

Download / setup: https://portswigger.net/burp/releases

Documentation: https://portswigger.net/burp/documentation/desktop/running-scans

Nuclei / Template-based checks

Repeat specific checks on authorized targets with selected, reviewed templates.

Template impact varies. Pin scope, request limits and template version; do not blindly execute every template.

Open source

Download / setup: https://docs.projectdiscovery.io/opensource/nuclei/install

Documentation: https://docs.projectdiscovery.io/opensource/nuclei/overview

Trivy / Container / dependency / IaC

Inspect component vulnerabilities and misconfigurations in images, filesystems and configuration artifacts.

Not a network port scanner. Assess fixed-version availability, package reachability and runtime context separately.

Open source

Download / setup: https://trivy.dev/docs/latest/getting-started/installation/

Documentation: https://trivy.dev/docs/latest/guide/

Interpret findings correctly

Fictional teaching examples; not findings from real systems.

Public management service

An external sensor reaches an unexpected management port on 203.0.113.20. The address is fictional.

First confirm ownership and that the service really is a management interface. Do not label an open port as a breach or confirmed CVE.

Restrict internet reachability to required sources, and review strong authentication and patch status. Retest from the external sensor.

High-severity package alert

An internal scanner flags an apparently old package; the vendor may have backported the fix.

Check the distribution security advisory and installed patch evidence alongside the package version. CVSS alone does not prove applicability.

Patch or mitigate a confirmed weakness; retain an evidenced exception for a false positive. Reassess exceptions after version changes.

Zero findings, failed authentication

40 internal servers are in scope; the scanner account cannot log in to 12. These are teaching figures.

Successful authentication coverage is 28/40 = 70%. This is not a security pass mark. Local-check coverage is incomplete on 12 servers.

Resolve permission/network problems and rescan. Include gaps in management reporting; do not close the systems as clean.

Web header alert

Passive analysis reports a missing security header. The scan observed only unauthenticated pages.

Inspect the response, redirects and relevance of the header to this content. The alert does not establish XSS or an account access vulnerability.

Test an appropriate header policy; separately plan authenticated workflow and business-logic coverage.

Reporting and common questions

CVSS expresses technical severity; retain the version and vector. KEV records known exploitation; absence is not assurance. EPSS estimates the probability of a CVE being exploited in the wild within the next 30 days; it is not your organization’s risk score.

• Coverage: successfully assessed / approved assets. Show unreachable assets separately.

• Authentication: targets with successful local checks / targets intended for credentialed scanning.

• Risk: validated open findings that are internet-reachable and business-critical.

• Time: elapsed time from first validation to technical closure; track reopened findings separately.

• Tracking: overdue work, temporary mitigations and expiry dates for accepted risks.

• Zero findings: not positive assurance without verified scope, profiles, feeds and access success.

How does scanning differ from penetration testing?

Scanning mainly checks known patterns and configurations systematically. A penetration test may also investigate manual validation, business logic and attack chains against an authorized objective. A clean automated result does not rule these out.

How often should scans run?

There is no single universal interval. Build a schedule around criticality, change rate, internet exposure and applicable contractual/standard requirements. Significant changes and remediation retests are separate triggers.

Can OT / ICS be scanned in the same way?

Do not directly apply a generic IT scanning profile. Involve production and safety owners, vendor support, a suitable maintenance window and a separate risk assessment. Passive inventory may be preferable initially; active testing must be controlled and approved.

Workpapers and official sources

This is a practical guide; it does not connect to targets or launch scans. A real engagement defines written asset-owner authorization, explicit scope, a maintenance window and stop conditions.

Pack: scope inventory (CSV), findings tracker (CSV), checklist (MD), report template (MD), tool catalogue (CSV) and this guide. Examples are fictional. Files contain no personal data or secrets.

Original SecNet educational content; not a publication or endorsement by source organizations. Consult publisher documentation for features, versions and licence terms.

NIST SP 800-115

https://csrc.nist.gov/pubs/sp/800/115/final

NIST SP 800-82 Rev. 3 · OT

https://csrc.nist.gov/pubs/sp/800/82/r3/final

Nmap reference

https://nmap.org/book/man.html

Greenbone Community documentation

https://greenbone.github.io/docs/latest/22.4/container/index.html

Tenable · credentialed checks

https://docs.tenable.com/nessus/Content/CredentialedChecksOnWindows.htm

ZAP · baseline scan

https://www.zaproxy.org/docs/docker/baseline-scan/

PortSwigger · running scans

https://portswigger.net/burp/documentation/desktop/running-scans

ProjectDiscovery · Nuclei

https://docs.projectdiscovery.io/opensource/nuclei/overview

Trivy documentation

https://trivy.dev/docs/latest/guide/

Qualys VMDR

https://www.qualys.com/apps/vulnerability-management-detection-response

FIRST · CVSS

https://www.first.org/cvss/

FIRST · EPSS

https://www.first.org/epss/

CISA · KEV official mirror

https://github.com/cisagov/kev-data