Pentest Tools

From farce to pass: ending the compliance circus with audit-ready evidence

A guide to meeting compliance requirements with validated vulnerability assessments

Index

How validated evidence bridges the gap between security and compliance

Compliance frameworks don't ask for raw scanner output; they want proof.

Auditors expect evidence that shows you have **validated, retested, and mapped** vulnerabilities to controls. Most scanners just provide raw lists of potential issues.

Turning those reports into audit-ready evidence can take hours.
And every hour spent reformatting and validating findings is an hour not spent reducing risk.

Auditor-ready reports out of the box solve that problem.

In this white paper, we'll show how validated vulnerability assessments cut wasted effort and deliver **credible, compliance-ready evidence** – explaining what proof auditors accept, when automation is enough, and where manual validation still matters.

The current state of vulnerability assessments and compliance

Attack surfaces are complex, sprawling, and dynamic.

Organizations run recurring assessments across internal networks, web apps, APIs, and cloud environments. On paper, these results should feed directly into compliance. In practice, compliance expectations need far more than “a scan was run.”

Auditors need to see:

- **Proof of remediation**: before-and-after evidence that vulnerabilities were fixed.
- **Alignment to controls**: findings mapped to the exact clauses in the framework.
- **Consistency over time**: results that show testing is routine and reproducible, not a one-off.

Many automated reports don’t meet these standards.

Scanners flood teams with CVEs, plugin IDs, and raw data - outputs auditors routinely reject because they don’t validate exploitability, track fixes, or tie results to compliance requirements.

Even worse, those reports lean heavily on CVSS scores, which can misrepresent risk.

For example, a CVSS 9.8 on an internal service that isn’t exposed externally may look critical on paper, but it carries little compliance weight. A CVSS 6.5 on a public payments API, however, could be far more urgent. Certification bodies know this, which is why they demand proof of exploitability, recurrence, and control mapping instead of raw severity scores.

Security consultants

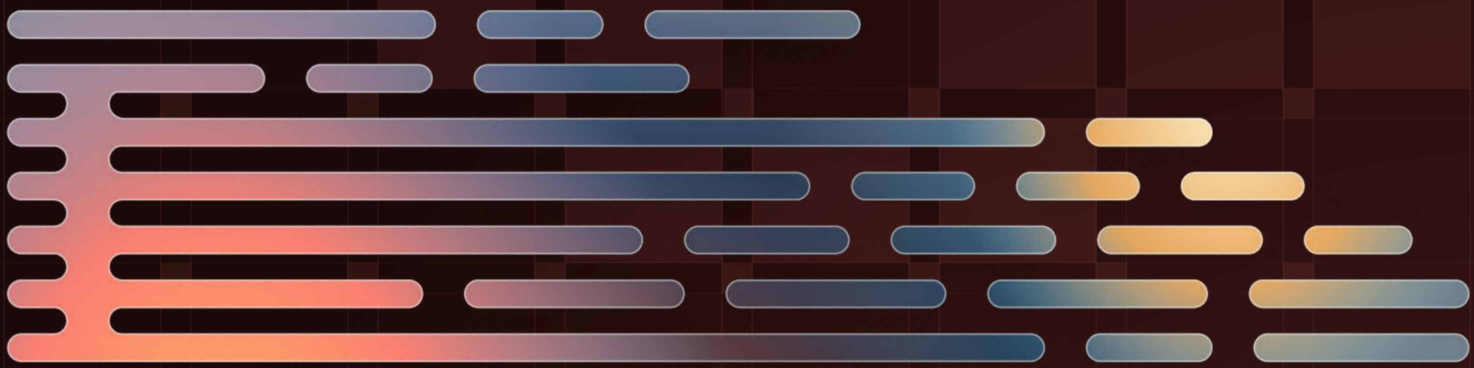
still get asked for manual attestations, spend hours rewriting technical output for auditors, and lose margin to noise and false positives.

Internal security teams

must show recurrence, remediation progress, and ownership – but instead burn cycles reformatting scanner outputs to fit Jira or GRC schemas while fighting status drift between tickets and scan results.

MSPs and MSSPs

need standardized client deliverables, yet juggle brittle evidence attachments, multi-tenant complexity, and auditor requests for manual pentests alongside automated scans.



This is the gap Pentest-Tools.com closes.

By combining continuous automation with optional human validation, the product produces audit-ready evidence that meets compliance expectations, and cuts manual work adjustments.

The anatomy of audit-ready evidence

So, if raw scanner output doesn't cut it, what does audit-ready evidence look like? Findings must contain four key traits:

Proof

Evidence must show the vulnerability in action, not just list a CVE.

Screenshots of a successful XSS payload rendering, request/response pairs from a SQL injection, or exploit traces from a code execution are undeniable confirmation. This goes beyond a "vulnerability found" notification and gives auditors irrefutable artifacts that the issue exists and matters.

Reproducibility

One-off results don't survive audit review.

Findings need to hold up under retest, with enough detail to repeat them reliably. That means documenting the exact endpoint, preserving the request/response data, and showing retests or before/after screenshots. This allows auditors – or internal teams – to recreate the exploit and confirm the issue persists until resolved.

Context

Auditors need more than “critical” or “high” labels.

They expect findings to be situated in context – what the vulnerability is, how attackers could exploit it, and why it matters to the business. That means:

- **Technical classification** like CVE or CWE mapping for precision.
- **Exploitability signals**, like EPSS or inclusion in CISA KEV.
- **Business impact**, including exposure level, affected data, or regulatory scope.

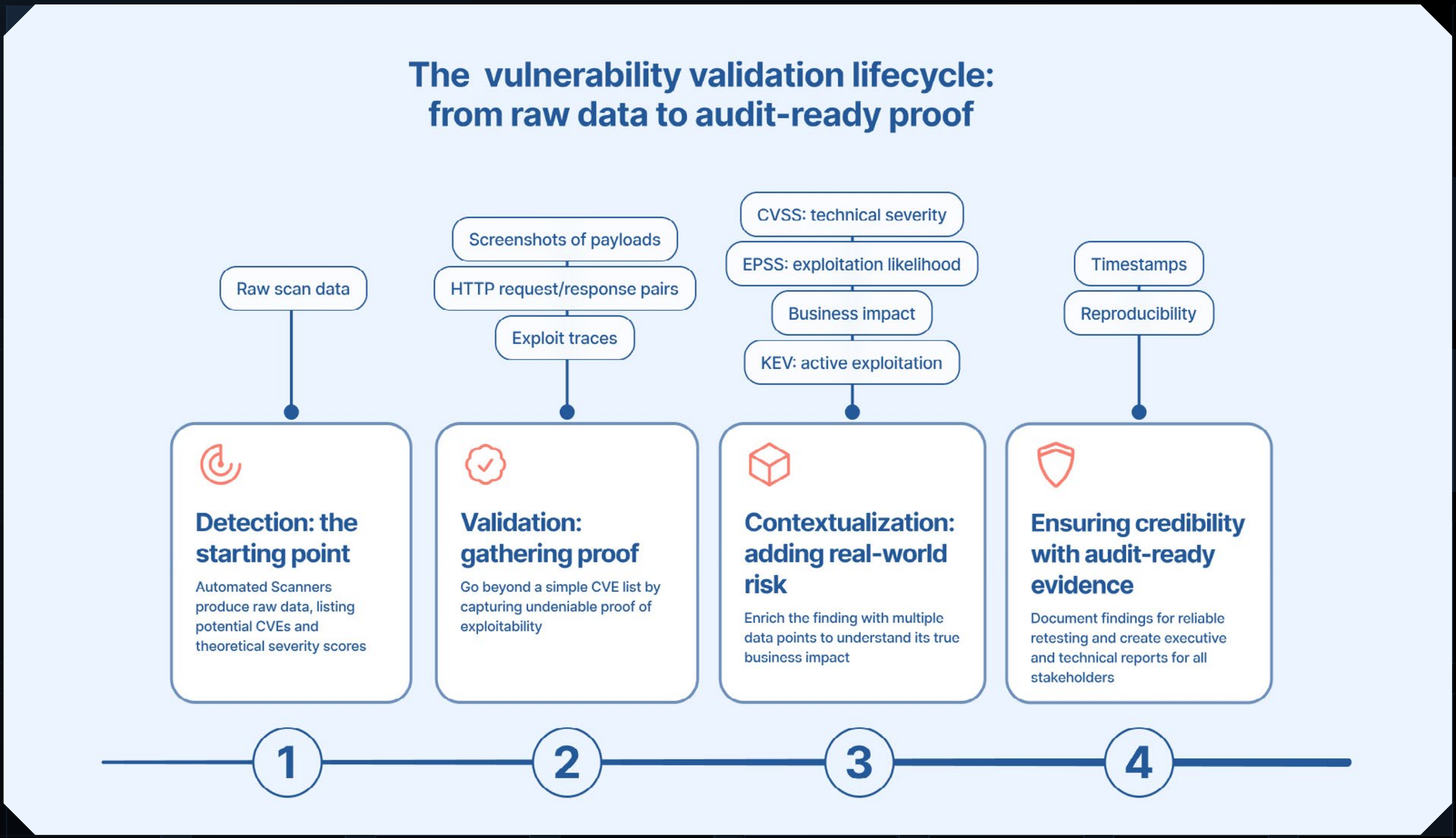
Without this, you risk auditors dismissing evidence as checkbox reporting. With it, findings show auditors you have validated, prioritized, and tied issues to real-world impact.

Clarity

Reports must bridge technical and business audiences.

Technical detail is necessary for remediation, but it’s equally important that non-technical stakeholders can understand and absorb the information. Executive summaries, plain-language titles, and clause references make the same technical findings credible in an audit.

Together, these four traits transform raw detection data into credible, compliance-ready proof.



The vulnerability validation lifecycle: from raw data to audit-ready proof

Raw scan data

1 Detection: the starting point

Automated Scanners produce raw data, listing potential CVEs and theoretical severity scores

Screenshots of payloads

HTTP request/response pairs

Exploit traces

2 Validation: gathering proof

Go beyond a simple CVE list by capturing undeniable proof of exploitability

CVSS: technical severity

EPSS: exploitation likelihood

Business impact

KEV: active exploitation

3 Contextualization: adding real-world risk

Enrich the finding with multiple data points to understand its true business impact

Timestamps

Reproducibility

4 Ensuring credibility with audit-ready evidence

Document findings for reliable retesting and create executive and technical reports for all stakeholders

What ‘compliance in action’ looks like

Compliance is a process, not a destination.

Likewise, compliance isn’t only about producing evidence – it’s about **making that evidence usable** across multiple frameworks, clients, and environments. The goal is to treat compliance as a natural by-product of operations, not an afterthought.

Map once, reuse everywhere

Tying findings to compliance clauses once, then reusing that mapping across multiple frameworks saves teams time and effort. Look for tools that align findings to SOC 2, ISO 27001, PCI DSS, DORA, and HIPAA clauses or other standards without forcing staff to rewrite results every time.

Deliver actionable reporting

Your assessments should be actionable and understandable for technical and non-technical staff. Include executive summaries for leadership alongside detailed findings, remediation steps, and live evidence IDs for auditors. This dual output ensures business leaders see risk posture while auditors can verify proof without extra formatting.

Organize reports for clarity at scale

Separating compliance work by client, business unit, or region keeps reporting clear and avoids duplicate tasks. For example, managing a client operating in both the EU and US in one place, with each region's compliance requirements tracked separately, will ensure you streamline your compliance efforts.

Unify coverage, avoid silos

Collect evidence across all relevant environments - web apps, networks, APIs, and cloud environments – and keep it centralized, not scattered across teams or tools. This way, you create consistent, reusable, and audit-evidence that can scale across frameworks and environments.

The bottom line?

Bolting on evidence at the end isn't a sustainable approach to compliance. You need to bake it into your daily workflow. **Validate evidence as you collect it**, map it across frameworks, organize it in dedicated workspaces, and package it in a way that works for both executives and auditors. Tools that support this approach will help your team avoid drowning in raw scan data or reducing compliance to a check-box exercise.

The Pentest-Tools.com approach to producing audit-ready evidence

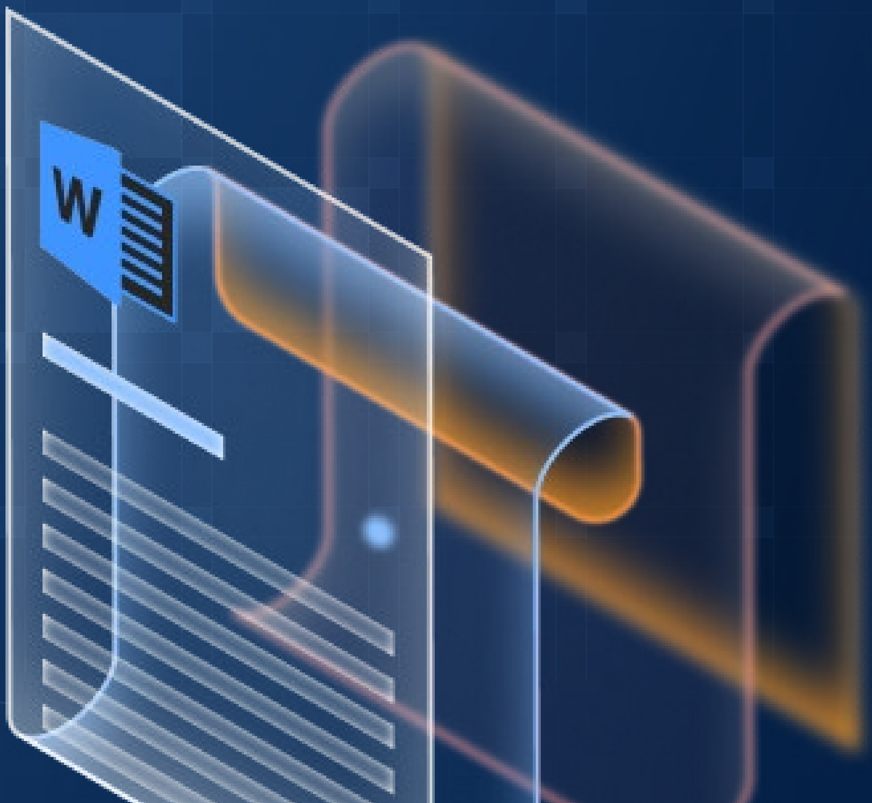
Pentest-Tools.com has spent over a decade working alongside customers to develop an approach to compliance that makes life easier for security teams, auditors, and consultants.

What have we learnt?

Compliance can't be a bolt-on or an afterthought. (Well, it can be, but it's a lot of additional, duplicated effort.) So, we built it in from the start.

At Pentest-Tools.com, we understand that compliance and offensive security share key principles: **proactive insight and prevention**. Compliance isn't just another feature; it's a foundational part of our product.

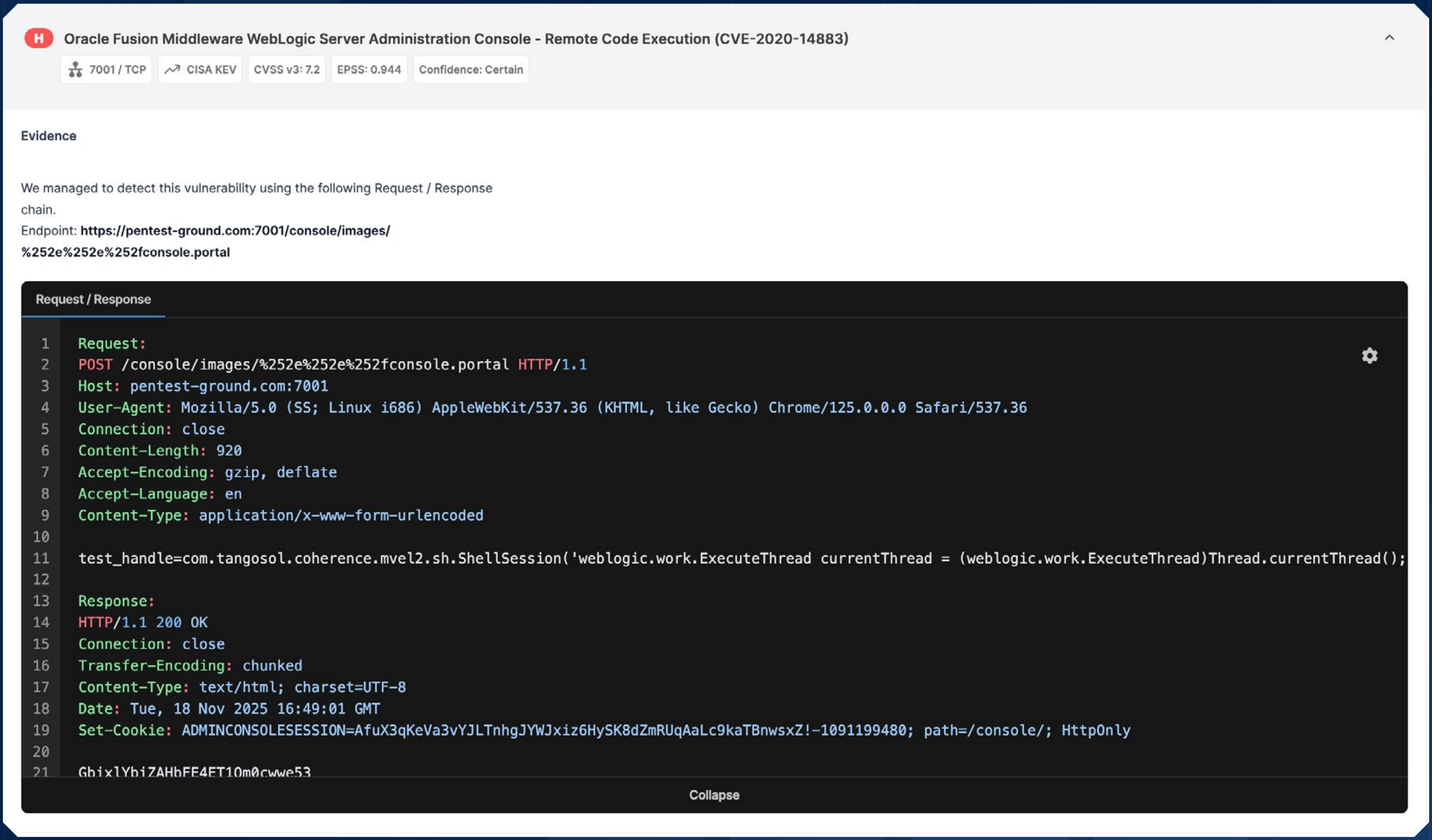
Other tools drown you in noise. We flipped that. **Evidence, validation, and audit-ready reporting come first**. Everything else follows.



Evidence-first accuracy

When our tools find a vulnerability, they capture concrete proof that stands up to scrutiny. Our scan results include:

HTTP request/response traces that show the issue in action.



Oracle Fusion Middleware WebLogic Server Administration Console - Remote Code Execution (CVE-2020-14883)

Evidence

We managed to detect this vulnerability using the following Request / Response chain.
Endpoint: **https://pentest-ground.com:7001/console/images/%252e%252e%252fconsole.portal**

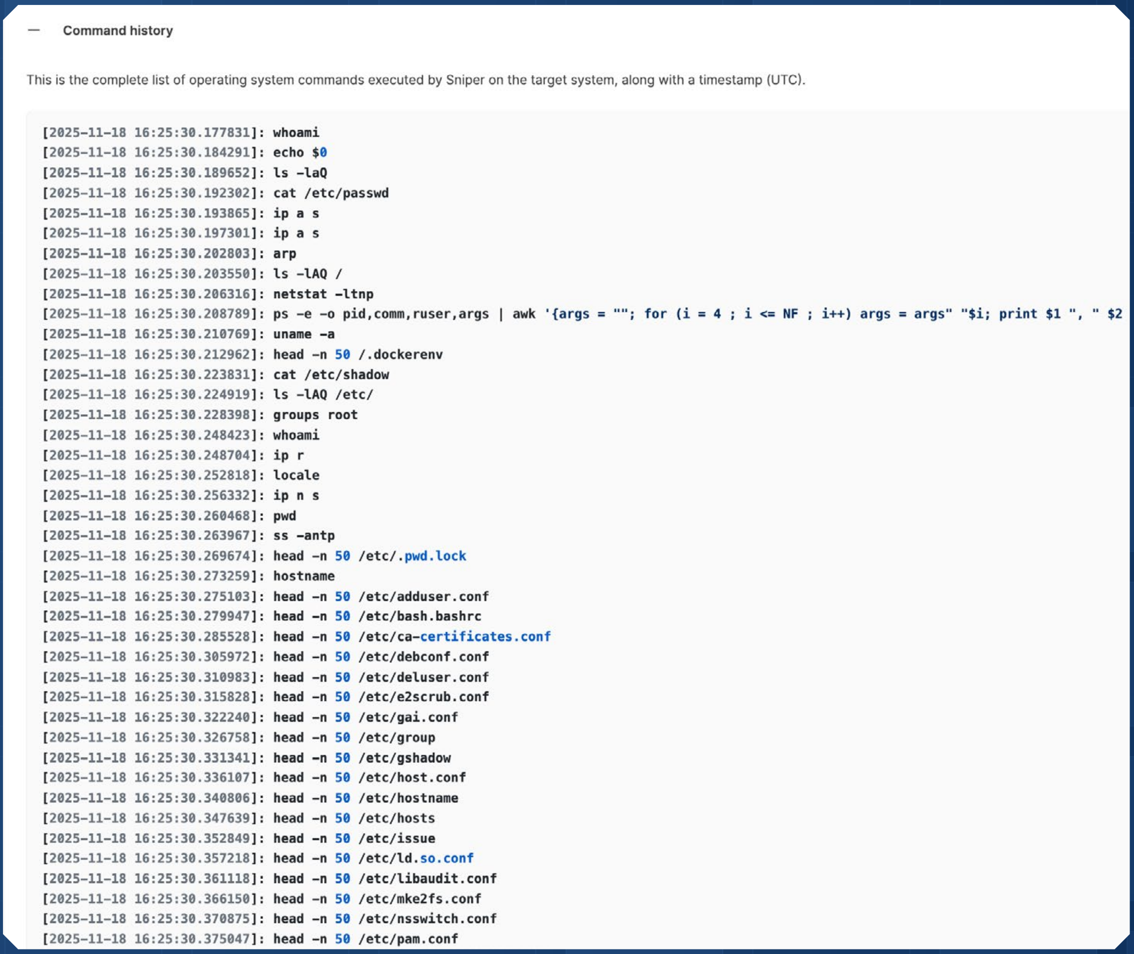
```
Request:
POST /console/images/%252e%252e%252fconsole.portal HTTP/1.1
Host: pentest-ground.com:7001
User-Agent: Mozilla/5.0 (SS; Linux i686) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Connection: close
Content-Length: 920
Accept-Encoding: gzip, deflate
Accept-Language: en
Content-Type: application/x-www-form-urlencoded

test_handle=com.tangosol.coherence.mvel2.sh.ShellSession('weblogic.work.ExecuteThread currentThread = (weblogic.work.ExecuteThread)Thread.currentThread();

Response:
HTTP/1.1 200 OK
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
Date: Tue, 18 Nov 2025 16:49:01 GMT
Set-Cookie: ADMINCONSOLESESSION=AfuX3qKeVa3vYJLTnhgJYWJxiz6HySK8dZmRUqAaLc9kaTBnwsxZ!-1091199480; path=/console/; HttpOnly

GbixlYbiZAHbFE4ET1Om0cwwe53
```

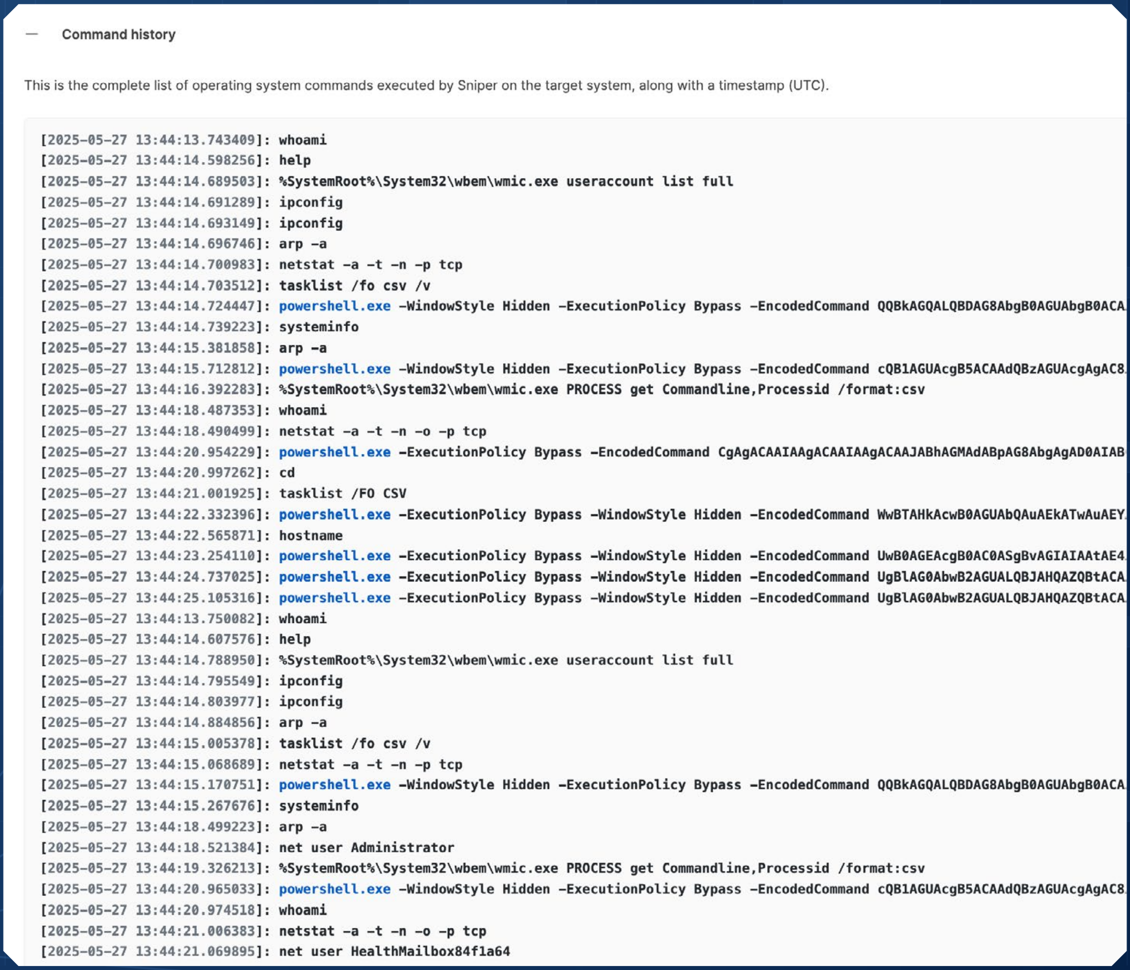
Replay steps confirming reproducibility



— Command history

This is the complete list of operating system commands executed by Sniper on the target system, along with a timestamp (UTC).

```
[2025-11-18 16:25:30.177831]: whoami
[2025-11-18 16:25:30.184291]: echo $0
[2025-11-18 16:25:30.189652]: ls -laQ
[2025-11-18 16:25:30.192302]: cat /etc/passwd
[2025-11-18 16:25:30.193865]: ip a s
[2025-11-18 16:25:30.197301]: ip a s
[2025-11-18 16:25:30.202803]: arp
[2025-11-18 16:25:30.203550]: ls -lAQ /
[2025-11-18 16:25:30.206316]: netstat -ltnp
[2025-11-18 16:25:30.208789]: ps -e -o pid,comm,ruser,args | awk '{args = ""; for (i = 4 ; i <= NF ; i++) args = args" "$i; print $1 ", " $2
[2025-11-18 16:25:30.210769]: uname -a
[2025-11-18 16:25:30.212962]: head -n 50 /.dockerenv
[2025-11-18 16:25:30.223831]: cat /etc/shadow
[2025-11-18 16:25:30.224919]: ls -lAQ /etc/
[2025-11-18 16:25:30.228398]: groups root
[2025-11-18 16:25:30.248423]: whoami
[2025-11-18 16:25:30.248704]: ip r
[2025-11-18 16:25:30.252818]: locale
[2025-11-18 16:25:30.256332]: ip n s
[2025-11-18 16:25:30.260468]: pwd
[2025-11-18 16:25:30.263967]: ss -antp
[2025-11-18 16:25:30.269674]: head -n 50 /etc/.pwd.lock
[2025-11-18 16:25:30.273259]: hostname
[2025-11-18 16:25:30.275103]: head -n 50 /etc/adduser.conf
[2025-11-18 16:25:30.279947]: head -n 50 /etc/bash.bashrc
[2025-11-18 16:25:30.285528]: head -n 50 /etc/ca-certificates.conf
[2025-11-18 16:25:30.305972]: head -n 50 /etc/debconf.conf
[2025-11-18 16:25:30.310983]: head -n 50 /etc/deluser.conf
[2025-11-18 16:25:30.315828]: head -n 50 /etc/e2scrub.conf
[2025-11-18 16:25:30.322240]: head -n 50 /etc/gai.conf
[2025-11-18 16:25:30.326758]: head -n 50 /etc/group
[2025-11-18 16:25:30.331341]: head -n 50 /etc/gshadow
[2025-11-18 16:25:30.336107]: head -n 50 /etc/host.conf
[2025-11-18 16:25:30.340806]: head -n 50 /etc/hostname
[2025-11-18 16:25:30.347639]: head -n 50 /etc/hosts
[2025-11-18 16:25:30.352849]: head -n 50 /etc/issue
[2025-11-18 16:25:30.357218]: head -n 50 /etc/ld.so.conf
[2025-11-18 16:25:30.361118]: head -n 50 /etc/libaudit.conf
[2025-11-18 16:25:30.366150]: head -n 50 /etc/mke2fs.conf
[2025-11-18 16:25:30.370875]: head -n 50 /etc/nsswitch.conf
[2025-11-18 16:25:30.375047]: head -n 50 /etc/pam.conf
```

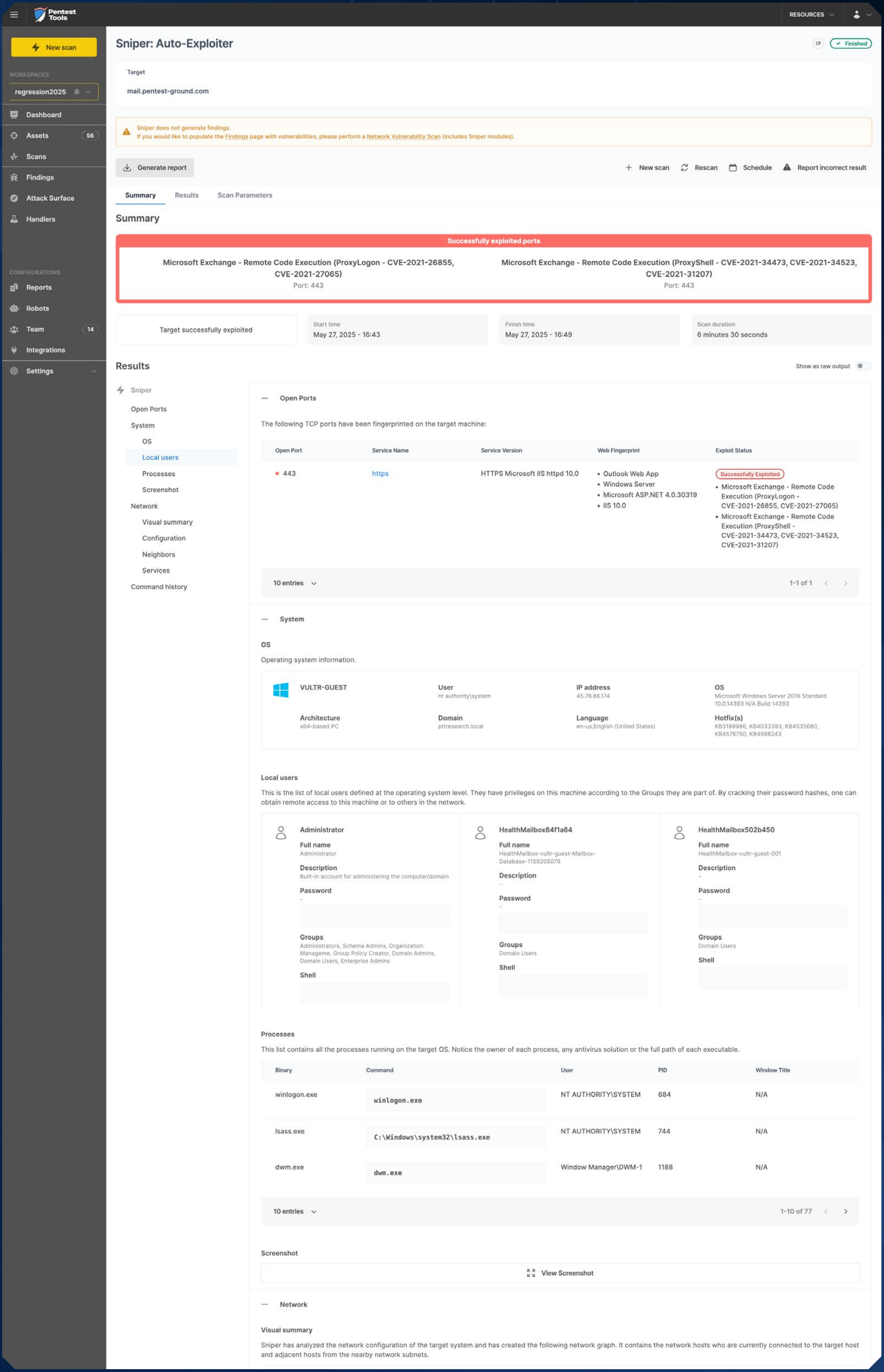


— Command history

This is the complete list of operating system commands executed by Sniper on the target system, along with a timestamp (UTC).

```
[2025-05-27 13:44:13.743409]: whoami
[2025-05-27 13:44:14.598256]: help
[2025-05-27 13:44:14.689503]: %SystemRoot%\System32\wbem\wmic.exe useraccount list full
[2025-05-27 13:44:14.691289]: ipconfig
[2025-05-27 13:44:14.693149]: ipconfig
[2025-05-27 13:44:14.696746]: arp -a
[2025-05-27 13:44:14.700983]: netstat -a -t -n -p tcp
[2025-05-27 13:44:14.703512]: tasklist /fo csv /v
[2025-05-27 13:44:14.724447]: powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -EncodedCommand QQBkAGQALQBDAG8AbgB0AGUAbgB0ACA
[2025-05-27 13:44:14.739223]: systeminfo
[2025-05-27 13:44:15.381858]: arp -a
[2025-05-27 13:44:15.712812]: powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -EncodedCommand cQB1AGUAcgB5ACAAdQBzAGUAcgAgAC8
[2025-05-27 13:44:16.392283]: %SystemRoot%\System32\wbem\wmic.exe PROCESS get Commandline,Processid /format:csv
[2025-05-27 13:44:18.487353]: whoami
[2025-05-27 13:44:18.490499]: netstat -a -t -n -o -p tcp
[2025-05-27 13:44:20.954229]: powershell.exe -ExecutionPolicy Bypass -EncodedCommand CgAgACAAIAAgACAAIAAgACAAJABhAGMAdABpAG8AbgAgAD0AIAB
[2025-05-27 13:44:20.997262]: cd
[2025-05-27 13:44:21.001925]: tasklist /FO CSV
[2025-05-27 13:44:22.332396]: powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -EncodedCommand WwBTAHkAcwB0AGUAbQAuAEkATwAuAEY
[2025-05-27 13:44:22.565871]: hostname
[2025-05-27 13:44:23.254110]: powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -EncodedCommand UwB0AGEAcgB0AC0ASgBvAGIAIAAtAE4
[2025-05-27 13:44:24.737025]: powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -EncodedCommand UgBlAG0AbwB2AGUALQBJAHQAZQBtACA
[2025-05-27 13:44:25.105316]: powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -EncodedCommand UgBlAG0AbwB2AGUALQBJAHQAZQBtACA
[2025-05-27 13:44:13.750082]: whoami
[2025-05-27 13:44:14.607576]: help
[2025-05-27 13:44:14.788950]: %SystemRoot%\System32\wbem\wmic.exe useraccount list full
[2025-05-27 13:44:14.795549]: ipconfig
[2025-05-27 13:44:14.803977]: ipconfig
[2025-05-27 13:44:14.884856]: arp -a
[2025-05-27 13:44:15.005378]: tasklist /fo csv /v
[2025-05-27 13:44:15.068689]: netstat -a -t -n -p tcp
[2025-05-27 13:44:15.170751]: powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -EncodedCommand QQBkAGQALQBDAG8AbgB0AGUAbgB0ACA
[2025-05-27 13:44:15.267676]: systeminfo
[2025-05-27 13:44:18.499223]: arp -a
[2025-05-27 13:44:18.521384]: net user Administrator
[2025-05-27 13:44:19.326213]: %SystemRoot%\System32\wbem\wmic.exe PROCESS get Commandline,Processid /format:csv
[2025-05-27 13:44:20.965033]: powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -EncodedCommand cQB1AGUAcgB5ACAAdQBzAGUAcgAgAC8
[2025-05-27 13:44:20.974518]: whoami
[2025-05-27 13:44:21.006383]: netstat -a -t -n -o -p tcp
[2025-05-27 13:44:21.069895]: net user HealthMailbox84f1a64
```

Local user and process listings, network maps, or file system artifacts, where relevant.



Sniper: Auto-Exploiter

Target

mail.pentest-ground.com

Sniper does not generate findings.
If you would like to populate the Findings page with vulnerabilities, please perform a Network Vulnerability Scan (includes Sniper modules).

Summary

Successfully exploited ports

Microsoft Exchange - Remote Code Execution (ProxyLogon - CVE-2021-26855, CVE-2021-27065)
Port: 443

Microsoft Exchange - Remote Code Execution (ProxyShell - CVE-2021-34473, CVE-2021-34523, CVE-2021-31207)
Port: 443

Target successfully exploited

Start time
May 27, 2025 - 16:43

Finish time
May 27, 2025 - 16:49

Scan duration
6 minutes 30 seconds

Results

— Open Ports

The following TCP ports have been fingerprinted on the target machine:

Open Port	Service Name	Service Version	Web Fingerprint	Exploit Status
● 443	https	HTTPS Microsoft IIS httpd 10.0	• Outlook Web App • Windows Server • Microsoft ASP.NET 4.0.30319 • IIS 10.0	Successfully Exploited • Microsoft Exchange - Remote Code Execution (ProxyLogon - CVE-2021-26855, CVE-2021-27065) • Microsoft Exchange - Remote Code Execution (ProxyShell - CVE-2021-34473, CVE-2021-34523, CVE-2021-31207)

10 entries   1-1 of 1

— System

OS

Operating system information.

VULTR-GUEST

User
nt authority\system

IP address
45.76.86.174

OS
Microsoft Windows Server 2016 Standard 10.0.14393 N/A Build 14393

Architecture
x64-based PC

Domain
pttresearch.local

Language
en-us;English (United States)

Hotfix(s)
KB3199986, KB4033393, KB4535680, KB4576750, KB4598243

Local users

This is the list of local users defined at the operating system level. They have privileges on this machine according to the Groups they are part of. By cracking their password hashes, one can obtain remote access to this machine or to others in the network.

Administrator
Full name
Administrator
Description
Built-in account for administering the computer/domain
Password
-
Groups
Administrators, Schema Admins, Organization Manageme, Group Policy Creator, Domain Admins, Domain Users, Enterprise Admins
Shell

HealthMailbox84f1a64
Full name
HealthMailbox-vultr-guest-Mailbox-Database-1159205079
Description
-
Password
-
Groups
Domain Users
Shell

HealthMailbox502b450
Full name
HealthMailbox-vultr-guest-001
Description
-
Password
-
Groups
Domain Users
Shell

Processes

This list contains all the processes running on the target OS. Notice the owner of each process, any antivirus solution or the full path of each executable.

Binary	Command	User	PID	Window Title
winlogon.exe	`winlogon.exe`	NT AUTHORITY\SYSTEM	684	N/A
lsass.exe	`C:\Windows\system32\lsass.exe`	NT AUTHORITY\SYSTEM	744	N/A
dwm.exe	`dwm.exe`	Window Manager\DWM-1	1188	N/A

10 entries   1-10 of 77

Screenshot

View Screenshot

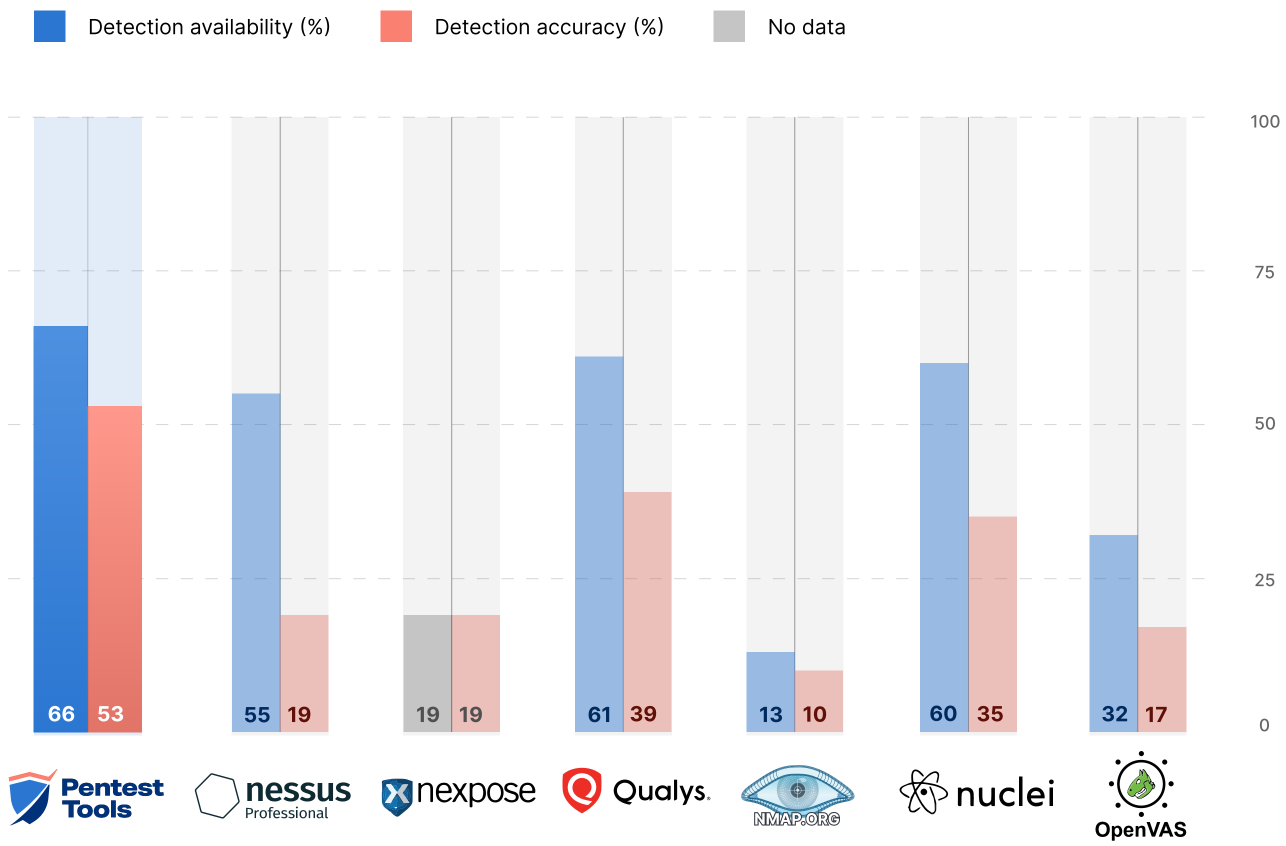
— Network

Visual summary

Sniper has analyzed the network configuration of the target system and has created the following network graph. It contains the network hosts who are currently connected to the target host and adjacent hosts from the nearby network subnets.

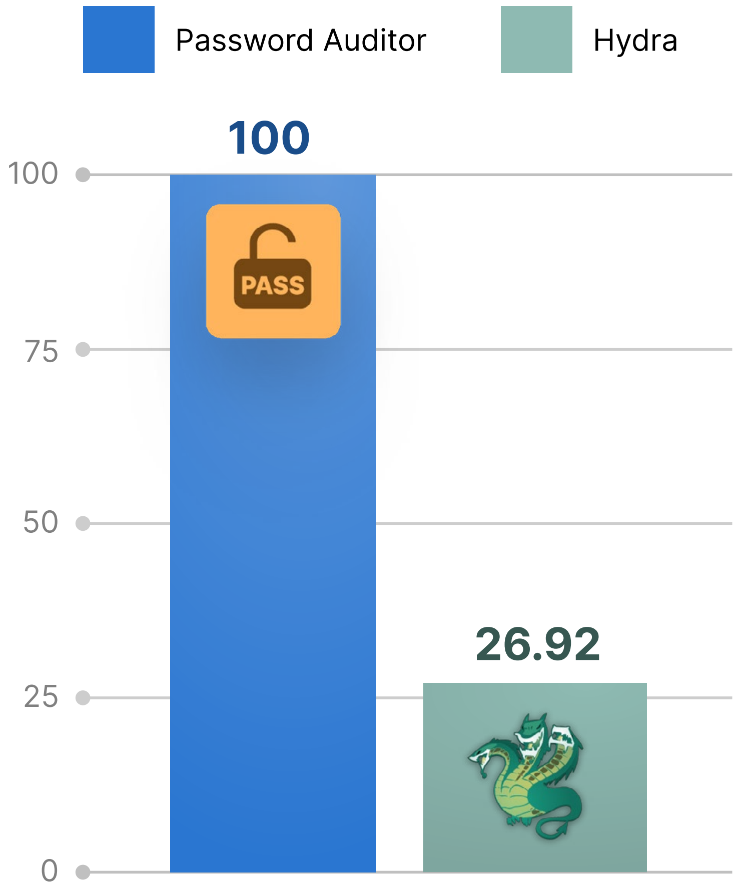
1. Validation built in, not bolted on

Unlike tools that stop at validation, **Pentest-Tools.com incorporates validation** into every stage of the assessment. A layered vulnerability detection system integrates multiple engines designed for different surfaces



Network Vulnerability Scanner

Combines four complementary scanning engines to identify **external and internal exposures** and prioritize practical, high-impact issues. In a 2024 benchmark across 167 vulnerable environments (128 with remotely detectable CVEs), the scanner ranked #1 for overall detection and remote detection versus six other popular tools.

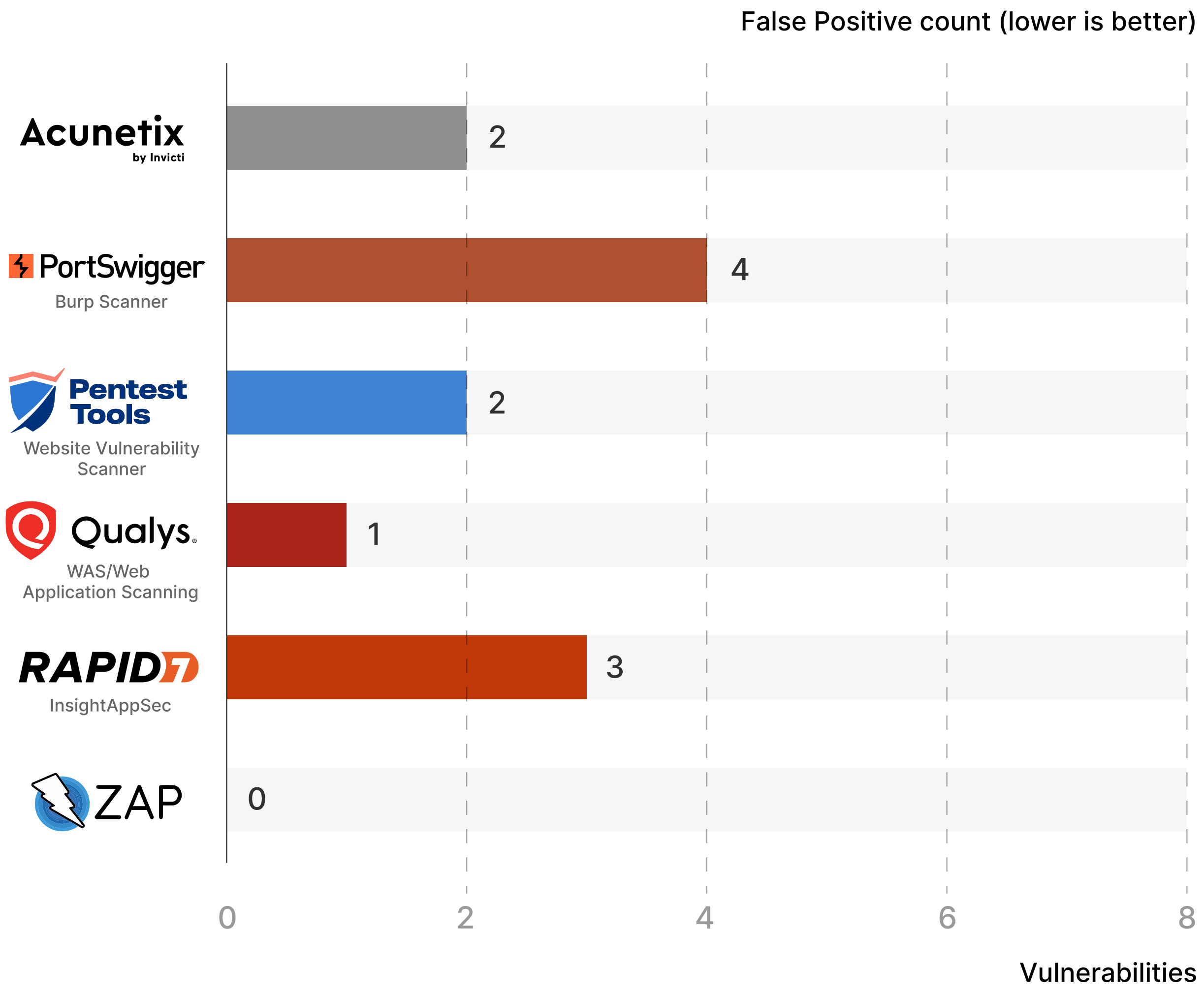


Detection percentage - **Lab scenario**

Password Auditor

Goes beyond “weak password” flags by **demonstrating valid credential compromise**. In benchmark tests across 26 target apps with multiple credentials, it identified valid credentials in 84% of cases, compared to just 15% for Hydra, the most popular open-source tool of choice for offensive security professionals.

Benchmark results against Broken Crystals



Website Vulnerability Scanner

Uses Machine Learning, out-of-band techniques, and proprietary payloads to validate exploitability while keeping false positives low. In a benchmark evaluating detection and accuracy rates across two targets - Broken Crystals and DVWA (Damn Vulnerable Web Application) - which include multiple vulnerable technologies, our scanner consistently reported higher accuracy in web app vulnerability detection. Plus, it also provides multiple authentication mechanisms to find vulnerabilities accessible only to logged in users.

ML Classifier

Built into the Website Scanner and URL Fuzzer, our ML classifier automatically sorts every HTML response, filters out junk, and highlights high-value targets. The result: cleaner, faster results with far fewer false positives, out of the box and without manual tuning.

Sniper: Auto-Exploiter

Simulates remote and client-side attacks safely and extracts indisputable proof - exploit traces, highlighted attack paths, and a visual network map.

Together, these tools (and the many more in our toolbox) form a fast, trustworthy system that prioritizes exploitable vulnerabilities. The result is **high-confidence findings** that save time and support defensible compliance reporting.

Tool	Benchmark highlights
Network Vulnerability Scanner	Ranked #1 in overall detection and remote detection across 167 environments (128 with detectable CVEs), outperforming six other tools.
Password Auditor	Valid credential compromise detected in 84% of test cases across 26 target apps with multiple credentials, vs 15% for Hydra.
Website Vulnerability Scanner	Higher detection accuracy across Broken Crystals and DVWA targets.

2. Private environment workflows

Pentest-Tools.com supports secure, private environment testing with:

- Lightweight AWS and Azure VPN agents for **scanning local networks and private clouds.**
- **VPN profile integration** to connect workspaces to fenced-off on-prem or private networks.
- Workspaces to group assets by client, business unit, or region, **keeping evidence structured** and separated.

3. Continuous compliance assurance

Audit-ready evidence requires recurrence, not just snapshots. Pentest-Tools.com enables:

- **Scheduled weekly/monthly scans** to show ongoing monitoring.
- **Vulnerability diffing** to highlight changes between scans.
- Automated report delivery via email to stakeholders, complete with executive summaries and technical appendices.

4. Manual flexibility when required

Some frameworks don't just accept automated scans; they require manual verification steps or a methodology section to prove that a human has validated findings.

Pentest-Tools.com supports this by:

- Letting consultants or analysts **add manual findings** – like privilege escalation chains, business logic flaws, or Burp Suite discoveries – directly into the same workspace as automated evidence.
- Allowing teams to **attach risk adjustments and analyst notes** to findings, creating a clear audit trail of human judgement.
- Generating reports that **bundle automated proof with manual attestations**, so outputs satisfy both compliance frameworks and auditor expectations.

5. Compliance-ready integrations

Compliance relies on evidence reaching the right stakeholders, in the right format. Pentest-Tools.com avoids the brittle “export and copy/paste” by integrating and pushing findings directly into the platforms where teams already manage security and compliance:

Vanta: Deliver scheduled scan reports straight into Vanta dashboards. Validated findings, remediation diffs, and retest

Jira: Push selected findings directly into Jira issues, alongside plans for automated, notification-based issue creation. This ensures developers can see remediation tasks in their existing workflow, and compliance teams can track closure without juggling tickets and separate reports.

Burp Suite: Pentesters can send findings from Burp Suite to Pentest-Tools.com in one click, consolidating manual evidence with automated scans in a single audit-ready report. This eliminates the need to maintain separate document sets for internal validation vs. auditor reporting.

AWS: Import AWS assets and deploy a lightweight agent from the AWS Marketplace. Combined with VPN workspace profiles, this enables internal VPC scanning, ensuring compliance coverage extends beyond public assets.

The integrations eliminate status drift. By syncing scan data with tickets and dashboards, **Pentest-Tools.com keeps audit evidence consistent and current.**

How Pentest-Tools.com supports teams through the compliance process

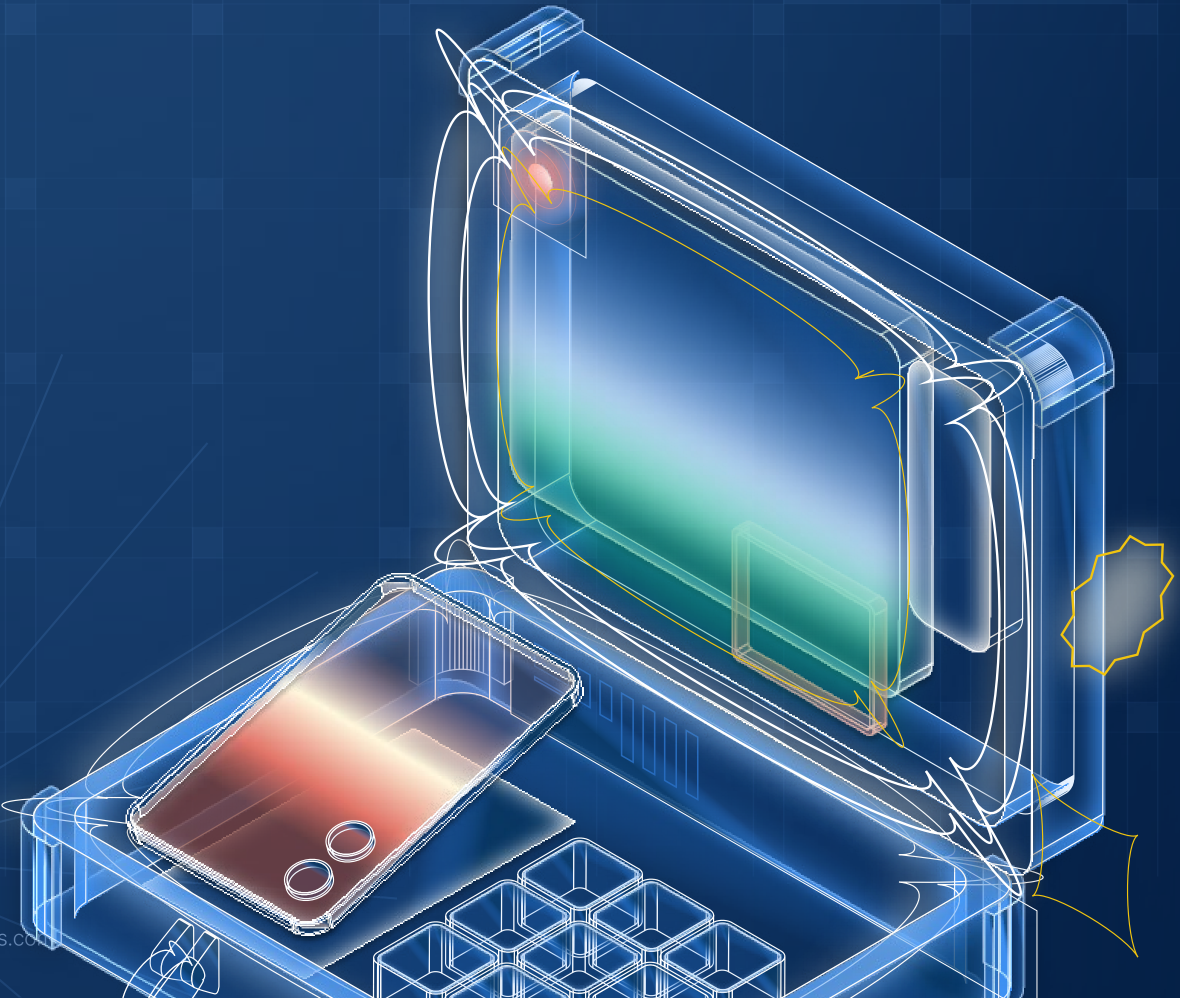
All good security professionals know that compliance is an ongoing process.

Whether you're a consultant, an internal security team, or an MSP/MSSP, the core challenge is the same: scanners produce raw data, while auditors demand validated proof.

That's the gap Pentest-Tools.com fills.

We help you transform findings into proof that stands up to audit review, streamlines your reporting, and keeps you credible in front of clients, auditors, and leadership.

We've got you covered throughout the entire compliance journey, around the clock.



Security consultants: less noise, more credibility

Clients will often tell security consultants that scans alone don't satisfy auditors. They still ask for attestations, methodology sections, and manual checks. Consultants must rewrite traditional scanner reports for certification bodies, draining time and margin.

Pentest-Tools.com supports security consultants by allowing them to:

- Use Sniper: Auto-Exploiter modules to **safely validate high-risk CVEs**, producing proof without leaving shells behind.
- **Generate dual-audience** reports that combine auditor-ready summaries with technical appendices.
- **Save time digging through and refining details** by providing key context: descriptions, how to reproduce, where to find more details, and how to mitigate.

> *I like Pentest-Tools.com because the platform allows me to confirm open ports - if any - in a quarterly review for my client services. Providing reports of checks, scans, etc. is crucial in my industry and with these tools, it is fast and easy.*
> - Joshua Brown, IT Consultant

> *We use this tool to scan our customers' websites. We particularly like that we can subscribe to the tool monthly. The simple operation makes it easier for us to design our work professionally. The results of the scan are very good. Pentest-tools.com is a reliable partner for us. We are very satisfied. Use it and you will learn to love it!*
> - Marco Kuhl, IT Consultant at Kuhlma IT Solutions

From our case study:

> *Pentest-Tools.com's customer support makes a big difference. When small issues popped up, Pentest-Tools.com fixed them within hours, not weeks. That responsiveness builds trust.*
> - Amy Vaillancourt, COO at Arco IT

Internal security teams: proof of recurrence and remediation

For internal teams, the hardest part isn't finding vulnerabilities - it's proving to auditors that issues are tracked, fixed, and retested in a consistent, repeatable way.

Pentest-Tools supports internal security teams throughout the compliance process by providing:

- **Scheduled scans and vulnerability diffs**, providing continuous monitoring and showing exactly what changed.
- **Before/after artifacts**, like screenshots and payload traces, to demonstrate remediation.
- **Executive summaries and technical detail** in the same report – clear enough for leadership, precise enough for auditors.
- **Seamless exports** to Jira and Vanta, cutting manual copy/paste.

> “ *I have been very appreciative of the work Pentest-Tools.com has put into the product. For over 20 years, in my previous business, we were spending thousands of dollars per year to run the very same tests, and often we were just given results, without suggestions or link to articles on how to fix the issues. We were paying for consultants extra to do that work.*
> - Pirooz A, President, Financial Services

> “ Pentest-Tools.com offers an integration feature with JIRA, which helps us address findings more efficiently. The configuration of the tool is simple and straightforward, and the support team is also very good at providing prompt feedback and solutions.
> - Brenda W, Senior Information Security Analyst

From our case study:

> “ *We were spending too much time correlating threat data manually, and not enough on helping clients act on the real risks.*
> - Ratnesh Pandey, VP of Engineering at Elpha Secure

MSPs and MSSPs: standardized compliance at scale

For service providers, the challenge is bigger. Juggling dozens of clients, different standards, and constant auditor demands for more than "just scans" can make the compliance process confusing, time-consuming, and expensive.

Pentest-Tools.com works with MSPs and MSSPs to make compliance evidence consistent, scalable, and trustworthy. They can:

- **Standardize deliverables** with consistent templates, control mapping, and workspace separation across clients and regions.
- **Bundle automated and manual evidence**: upload analyst notes or Burp Suite findings alongside validated scan results in a single report.
- **Automate recurring reporting**: schedule scans and direct reports to Jira or Vanta dashboards.
- **Maintain credibility**: provide validated exploit traces and immutable evidence links auditors can trust. details, and how to mitigate.

> *PC Dial uses Pentest-Tools.com to help us prepare for PCI compliance on behalf of our customers. The tools are easy to use and all in one place rather than having to load up several tools for different scanning tasks. The reports produced are clear with good information on any issues found with clear advice on possible fixes. Thank you Pentest-Tools.com for a great product!*
>
> - Jeremy Gardner Technical Director at PCDial.com

> *Pentest-Tools.com provides an efficient way to ensure that clients meet the scanning requirements mandated by the FTC. By leveraging this platform, businesses can easily stay on top of their security posture, ensuring that they are not only compliant with regulations but also protected against potential vulnerabilities. Pentest-Tools.com is truly a comprehensive solution that gets the job done efficiently and effectively, making it an invaluable asset for any security team.*
>
> - Troy Johnson, Owner/President at Northwest Networks, LLC

Your concerns, answered

“ *We already use Nessus/Qualys.*

Keep them. Pentest-Tools.com complements these with validated, low-noise findings and retests designed for auditors.

“ *We use Vanta/Drata.*

These are great for tracking policies, but they don’t validate vulnerabilities. Pentest-Tools.com integrated directly, feeding them real evidence instead of screenshots.

“ *We need human verification.*

You can bundle manual findings, such as results from Burp Suite, or other details from your human-driven pentests with automated findings – all in one compliance-ready package.

“ *We don’t have time to learn another tool.*

Start small: one workspace, one weekly scheduled scans with diffing, one monthly report.

“ *False positives will waste our time. / Our team is small and we can’t triage noisy results.*

Findings include proof (request/response, screenshots, exploit traces, Sniper artifacts) and context (CWE, EPSS, CISA KEV) to keep noise low.

“ *How will external auditors know this evidence hasn’t been edited?*

Findings are recorded and assessed with 100% visibility for the whole team. View and evaluate all findings, complete with timestamps, hyperlinks, and records of any changes or edits, whether automatic or human-originated.

“ *We have to scan private networks, not just internet-facing assets.*

Use the lightweight agent and VPN profile to bring internal hosts into scope; import AWS assets for continuous coverage.

“ *Are your exploit checks safe in production?*

Sniper modules are built and tested in-house to be non-persistent and cleaned up after execution, providing proof without leaving traces.

“ *Our reports are too technical./ Our leadership needs a one-page view.*

Reports include an executive summary for managers and a detailed technical section for addressing complex findings and remediation options for engineers.

“ *We manage many clients and regions.*

Separate scope with workspaces (client, business unit) and reuse shared templates to keep deliverables consistent.

“ *We need evidence to live with our tickets and dashboards / “We need to work in Jira and GRC, not another portal.*

Push selected issues to Jira and sync vulnerabilities to Vanta. Route notifications via email, Slack, Teams, or webhooks.

“ *How fast can we show progress to an auditor?*

Schedule scans, enable diff alerts, and run targeted rescans/retests so the next report includes before/after proof.

“ *Pricing is a concern for smaller teams. / Pricing is a concern during slow periods.*

Use only what you need: choose a number of assets based on your scope, and the pricing plan which includes you know you’ll use. Scope by workspace and cadence, and pay for the assets you need to evaluate and/or monitor, avoiding shelfware tied to unused capabilities.

❝ *We want to keep our existing scanners. / We can't completely remove Nessus/Qualys.*

Do it. Use them for breadth and use Pentest-Tools.com to validate exploitability (with Sniper: Auto-Exploiter), cut noise, and easily assemble evidence auditors accept through integrations with Vanta, Nucleus Security, and Jira.

❝ *We can't give external scanners access to our private network.*

Use the lightweight agent and a VPN profile to scan internal hosts through a secured connection; limit scope by workspace and asset group.

❝ *We don't want exploits running in production.*

Use validation where it's safe and appropriate. However, Sniper modules are non-persistent, built and tested in-house, and clean up after execution.

❝ *Our auditors insist on a manual pentest.*

Keep it. Bundle manual notes and pentest results alongside automated findings, diffs, and retest proof in the same report for even more credibility.

❝ *We already use Burp during engagements.*

Push Burp issues into the same workspace so manual and automated findings ship in one export.

❝ *We need reports with our branding and structure.*

Upload your logo once, and every report or download will feature branded reports with your company identity. No vendor watermarks, no manual formatting. If you need to send reports from your domain, you can quickly set it up so stakeholders see reports coming from you.

If you prefer more editorial control, you can export customizable DOCX reports and use your cover, sections, and headers while keeping the executive summary, findings, and remediation appendixes.

“ *We have strict maintenance windows.*

Schedule scans during allowed windows, enable diff alerts, and run targeted retests only on changed items.

“ *We must provide change history for every item.*

Each finding can carry owner, notes, and retest date. Your next report includes before/after evidence.

“ *We worry about storing sensitive evidence (keys, dumps).*

Redact in the report where required and attach system-derived artifacts with timestamps so the source is clear.

“ *We need an API to automate checks and exports.*

You can automate and manage reports directly through the API. Use exports and other types of reports (CSV, JSON, DOCX, PDF) to pull findings, send issues, and attach reports to reviews. Full integration into your workflows, no account login needed.

“ *Auditors ask for screenshots; engineers want raw traces.*

Provide both: screenshots for quick review and request/response or command output for reproducibility.

“ *We only scan web apps today and compliance wants infrastructure too.*

Cover web, network, API, and cloud from one place and keep the evidence together in the same report.

Go beyond check-box compliance with audit-ready evidence

Compliance can seem like the mountain you'll never summit. Often teams are left scrambling to repackage raw scan data, validate findings, and answer auditor questions. And it pulls focus from what really matters: risk reduction.

With validation, proof, and compliance mapping built directly into your workflow, audits are less painful and more routine. Internal security teams can spend more time reducing risk. Consultants can provide more value to their clients. Service providers can juggle disparate customer demands without drowning in manual work.

Better reports are just the beginning. Pentest-Tools.com gives you the tools you need to make compliance an easy climb, helping you cut manual work, add value, and boost efficiency:

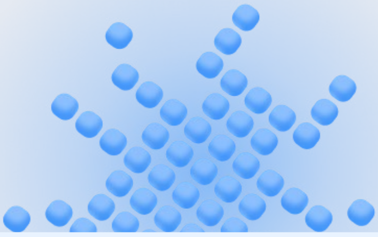
- **Faster acceptance in audits**: Proof backed by screenshots, payload traces, and validation removes doubt and speeds up certification reviews. Access auditors you can trust without back-and-forth.
- **Less manual adjusting**: Dual-audience reports, control mapping, and direct integrations mean no more manual reformatting for executives, engineers, and auditors.
- **Clearer remediation ownership**: Before/after artifacts and real-time sync with Jira and Vanta keep teams aligned. Everyone can see when an issue was found, fixed, and retested – without status drift.
- **Predictable compliance cycles**: Weekly scans, diffs, and recurring reporting make compliance routine, not episodic. Teams stay consistent with tracking and build a defensible history of continuous monitoring.

This is how you get from messy, time-sink processes with unbranded, clogged-up reports to simple, automated, digestible (and beautiful) compliance documents. Pentest-Tools.com makes the process repeatable, affordable, and auditor-credible.

Legacy scanners bury teams in noise, GRC dashboards reduce compliance to checklists; the process is a headache. With Pentest-Tools.com, you can save time, automate away the grunt work, and focus on closing the gap between security validation and compliance reporting quickly and permanently. You can be confident that your evidence will hold up – every time.

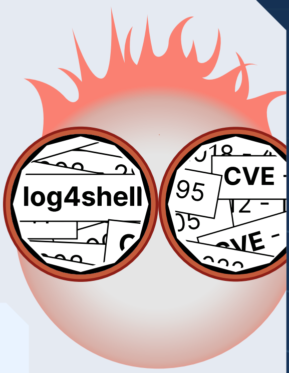
Discover how Pentest-Tools.com delivers simple, automated compliance reporting so you can spend less time stuck in the details, and more time hitting targets.

Explore our toolkit



Browse our Vulnerability & exploit database

Unpack our capabilities



Meet our team

Pentest Tools

Discover what’s possible. Prove what’s **real**.
With proprietary tech and key **offensive security** experts.

Europe, Romania, Bucharest
48 Bvd. Iancu de Hunedoara

support@pentest-tools.com
pentest-tools.com

Join our community of ethical hackers!