

Tenable and Synack

Integrating vulnerability management & security testing for better remediation and patch verification

The Challenge

Scanning identifies potential vulnerabilities but may not confirm what is exploitable. Scanning is also voluminous, making it challenging to zero in on the vulnerabilities that matter most. Security testing, meanwhile, confirms exploitability and provides detailed analysis, paths to remediation and patch verification. Security testing identifies exploitable, real-world application interactions that scanning may miss.

Each is vital, but vulnerability scanning and security testing results are too often siloed. As a result, it takes too long to isolate and fix exploitable vulnerabilities.

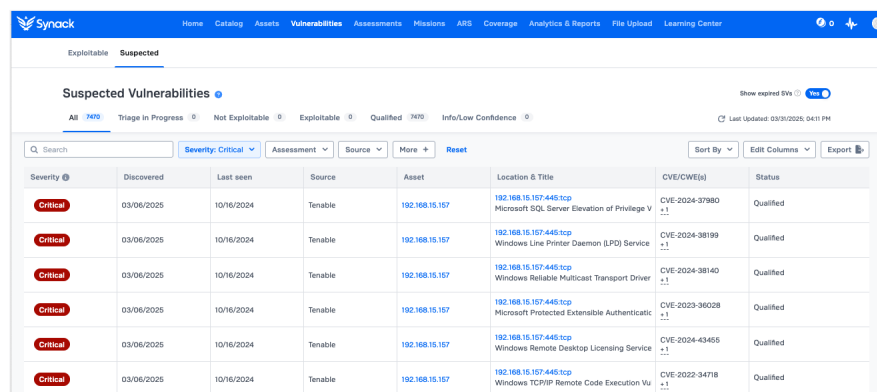
The Solution

Synack, the leader in Penetration Testing as a Service (PTaaS), has partnered with cutting-edge Tenable Vulnerability Management (VM) to offer customers the best of both worlds—broad insights from automated scanning integrated with the deep and detailed expertise of human-led security research.

Tenable Vulnerability Management, part of Tenable One, enables customers to scan host resources to see if what is running on them is exposed to cyber weaknesses, such as those identified by the Common Vulnerability Exposure (CVE) catalogue and other threat intelligence. Resources may be vulnerable due to various factors, including out-of-date security updates, which Tenable VM reports. This automated vulnerability scanning effectively provides complete visibility into potential cyber risk across customer IT environments.

Benefits of the Integration

- Improves vulnerability triage to isolate exploitable vulns that matter most
- Reduces noise by distinguishing vulns that aren't accessible by bad actors
- Combines the strengths of automated scanning and human-led analysis
- Mimics real-world behavior of bad actors to find threats that scanning may miss
- Overcomes the static nature of traditional penetration testing
- Integrates end-to-end workflows for faster remediation and patch verification
- Provides access to an expert, vetted team of security testers on demand
- Relieves IT/security teams from time-consuming exploit & patch verification



| Severity | Discovered | Last seen | Source | Asset | Location & Title | CVE/CWE(s) | Status |
|----------|------------|------------|---------|----------------|---|----------------------|-----------|
| Critical | 03/06/2025 | 10/16/2024 | Tenable | 192.168.15.157 | 192.168.15.157:445/tcp Microsoft SQL Server Elevation of Privilege V | CVE-2024-37980 +1 | Qualified |
| Critical | 03/06/2025 | 10/16/2024 | Tenable | 192.168.15.157 | 192.168.15.157:445/tcp Windows Line Printer Daemon (LPD) Service | CVE-2024-38199 +1 | Qualified |
| Critical | 03/06/2025 | 10/16/2024 | Tenable | 192.168.15.157 | 192.168.15.157:445/tcp Windows Reliable Multicast Transport Driver | CVE-2024-38140 +1 | Qualified |
| Critical | 03/06/2025 | 10/16/2024 | Tenable | 192.168.15.157 | 192.168.15.157:445/tcp Microsoft Protected Extensible Authenticatio | CVE-2023-36028 +1 | Qualified |
| Critical | 03/06/2025 | 10/16/2024 | Tenable | 192.168.15.157 | 192.168.15.157:445/tcp Windows Remote Desktop Licensing Service | CVE-2024-43455 +1 | Qualified |
| Critical | 03/06/2025 | 10/16/2024 | Tenable | 192.168.15.157 | 192.168.15.157:445/tcp Windows TCP/IP Remote Code Execution Vu | CVE-2022-34718 +1 | Qualified |

Powered by the Synack PTaaS platform, the Synack Red Team (SRT) acts as an extension to customer IT and security teams, assisting in quick triage, isolation and remediation of the most urgent security gaps. The SRT leverages context from scanning results and applies testing techniques from individual knowledge and experience. SRT researchers

confirm which vulnerabilities are actually exploitable in the customer's environment, provide detailed exploit analysis, recommendations for remediation and verification of successful patching. Synack PTaaS can run continuously to quickly address security gaps that yearly compliance-driven penetration testing misses.

About Tenable

Tenable exists to expose and close priority security gaps that put businesses at risk. Our industry-leading exposure management platform radically unifies security visibility, insight and action across the attack surface, equipping modern organizations to protect against attacks, from IT infrastructure to the cloud to OT and everywhere in between. By protecting digital and critical infrastructure from exposures, Tenable reduces business risk for more than 44,000 customers around the globe.

About Synack

Synack's Penetration Testing as a Service platform manages customers' attack surfaces by discovering new assets, pentesting for critical vulnerabilities and gaining visibility into the root causes of security risks. We are committed to making the world more secure by harnessing a talented, vetted community of security researchers to deliver continuous penetration testing and vulnerability management, with actionable results. Synack's PTaaS platform has uncovered more than 83,000 exploitable vulnerabilities to date, protecting a growing list of Global 2000 customers and U.S. agencies in a FedRAMP Moderate Authorized environment.

More information

The new integration is available at no additional charge to Synack PTaaS platform customers who have valid Tenable One Vulnerability Management subscriptions. Please read the [Integration Guide](#) for further information on enabling the integration in your Synack platform. You may also contact help@synack.com with any questions.