What is attack path validation?

Attack Path Validation (APV) proves whether an attacker could chain individual weaknesses, an exposed service, a crackable credential, a misconfigured permission, into a complete route to a high-value target such as domain administrator or a sensitive data store. Where a single-technique test asks 'does this work?', APV asks 'can these steps be strung together to reach the objective?'. It emulates full-chain adversary behavior from initial access through lateral movement and privilege escalation, safely and without red-team headcount, and it is a core capability within adversarial exposure validation.

HOW IT WORKS

01 Why does the path matter more than the finding?

Vulnerability scanners rank findings in isolation, which buries the real risk. A medium-severity misconfiguration can be the single hop that turns a contained foothold into full domain compromise, while a critical CVE on an unreachable host changes nothing.

APV reframes prioritization around reachability and impact. Instead of a flat list of thousands of findings, it produces a small number of proven paths to what matters, and it names the choke points where one fix removes an entire route. That is a far more actionable output than severity scores alone.

02 How does APV work?

APV runs the intrusion the way a real attacker would, then records the chain:

- Start from a realistic position. External access, or an assumed-breach foothold inside the network.
- Move and escalate. Emulate credential access, lateral movement, and privilege escalation techniques, mapped to frameworks like MITRE ATT&CK.
- Reach for the objective. Attempt to reach a defined crown-jewel asset or full domain administrator control.
- Report the path and the choke point. Show the exact sequence and the highest-leverage step to remediate.

SOURCES

[1] MITRE ATT&CK Framework

[2] MITRE ATT&CK Lateral Movement

[3] NIST SP 800-115 Technical Guide to Information Security Testing

Because it is automated and repeatable, APV can re-check whether hardening actually closed a path after remediation.

03 APV vs BAS vs penetration testing

The three answer different questions:

- Breach and attack simulation asks whether individual techniques are blocked and detected.
- Attack path validation chains those techniques to ask whether an attacker could reach the objective.
- Penetration testing brings human creativity to discover novel paths and business-logic chains automation would miss.

All three are part of adversarial exposure validation. APV is the one most focused on lateral movement and privilege escalation, the phases where a single foothold becomes a breach.

04 How do you get started with APV?

Define the objectives that would actually hurt, domain admin, a production database, a key SaaS tenant, and validate whether a path to each exists from a realistic starting point. Fix the choke points first, then re-run to confirm the path is gone.

APV can run through a continuous automated validation platform that emulates full-chain behavior without red-team headcount, or through human penetration testing for the deepest, most creative path discovery. Most mature programs use both.

Find the path before an attacker does.
securelayer7.net/learn/pentest/what-is-attack-path-validation

Open online