PENTESTERRA
SEE THE REAL RISK

INITIAL ACCESS → EXPLOITATION → PRIVILEGE ESCALATION → LATERAL MOVEMENT → IMPACT

ATTACK CHAIN MODULE

Attack Chain Analysis

Not a CVE list — a graph of how an attacker actually gets from the internet to your database.

Combines web, network, and code findings into directed kill-chain paths, scored by exploitability and blast radius.

FIND THE PATH
UNDERSTAND THE RISK
STOP THE NEXT ATTACK

REAL ATTACK PATHS
REAL CONTEXT
REAL SECURITY
REAL BUSINESS IMPACT

PENTESTERRA — Attack Chain / Explore / Analyze — Live Analysis

- Dashboard
- API Pentest
- Network Scan
- DevGuard
- Attack Chain
- Attack Graph
- Findings
- Reports
- Compliance
- Integrations
- Settings

Attack Chain Graph

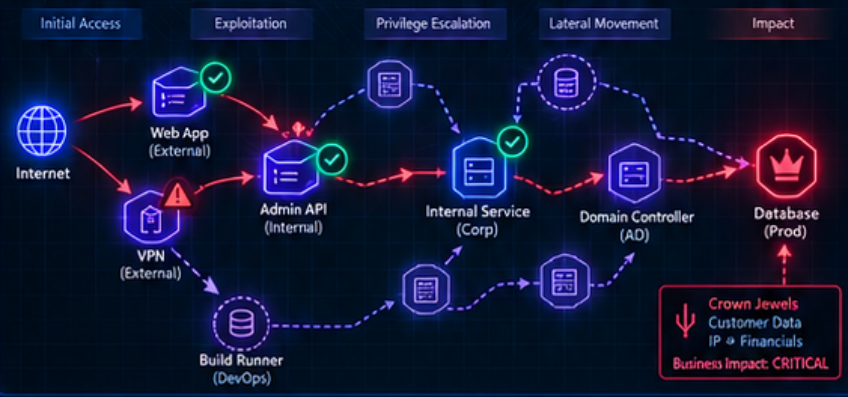
Cross-domain attack paths from initial access to business impact

New Analysis

1,842	12	28	5
Findings Ingested	Attack Chains	Confirmed Steps	Critical Paths
412 Web/API | 892 Network | 538 DevGuard	(up to depth 5)	Real findings	High business impact

Attack Chain Graph

Confirmed · Potential · Attack Path



Evidence for This Step

Admin API (Internal) — View Finding

Source	Web/API Pentest
Finding	Information Disclosure (Unauthenticated /admin endpoint)
Severity	Info
Evidence	GET /admin returns system info, version details, internal endpoints
CVE	—
MITRE	T1592 - Gather Victim Host Info

Request | Response | Headers

```
GET /admin HTTP/1.1
Host: api.acme-corp.com
...
{
  "version": "1.4.2",
  "internal": true,
  "env": "prod"
}
```

Top Attack Chains

#	Chain (Path Summary)	Source Mix	Confirmed Steps	Risk	Status
1	VPN → Admin API → Build Runner → DB	Network + Web + DevGuard	3 / 4	CRITICAL	Confirmed
2	Web App → Internal Service → DB	Web + Network	2 / 3	HIGH	Confirmed
3	Exposed Git → Build Runner → Internal → DB	DevGuard + Network	1 / 4	HIGH	Potential
4	Web App → AD → File Server → DB	Web + Network	2 / 4	MEDIUM	Potential
5	VPN → Internal Service → AD → DB	Network	1 / 3	MEDIUM	Potential

Executive Narrative

Generated by Pentesterra AI

Chain 1: VPN → Admin API → Build Runner → DB

An attacker can first exploit a medium severity vulnerability in the VPN to gain initial access to the internal network. From there, they can leverage an information disclosure issue in the internal admin API to discover build infrastructure. The build runner contains exposed credentials, which can be used to escalate privileges and access the production database. This chain results in potential access to customer data and financial records.

High business impact — affects customer data, financial systems, and regulatory compliance (PCI-DSS, GDPR).

What it does

- Pulls findings from 3 sources in one graph: web/API pentest, network scan, DevGuard (code/secrets/supply chain) — a medium on a VPN + an info on an admin API + a low on a build runner can become one critical path
- DFS-based engine computes up to 20 attack chains, depth ≤ 5, mapped to MITRE ATT&CK kill-chain phases: Initial Access → Exploitation → Privilege Escalation → Lateral Movement → Impact
- Each chain step marked confirmed (real finding exists) vs potential (theoretical vector)
- LLM-generated executive narrative per chain — explains the path in plain language for non-technical stakeholders
- Business impact scoring + compliance gap mapping (OWASP, PCI-DSS, GDPR, NIST, ISO) per chain
- Force-directed interactive graph in the UI, drill-down to evidence per step

Why Pentesterra

- The only platform that unifies web pentest + network scan + DevGuard (code/secrets) in one graph — many competitors stop at only network or only code
- Confirmed vs potential separation — clearly shows where a real finding exists and where a path remains theoretical

From scattered findings to real attacker logic.
— PENTESTERRA

LESS NOISE
MORE CONTEXT
REAL ATTACK PATHS
REAL BUSINESS IMPACT

THE ATTACK CHAIN WORKFLOW

1. **Discover** — Ingest findings
2. **Correlate** — Link across sources
3. **Build Paths** — Find attack chains
4. **Score Impact** — Rank and prioritize
5. **Explain** — Generate narratives

Web + API Findings · Network Findings · DevGuard Code / Secrets · Confirmed vs Potential · MITRE Mapped · Compliance Mapping · Executive Narrative · Interactive Graph

See how isolated findings become real attack paths.

Explore Attack Chain Analysis →

PEOPLE
PROCESS
TECHNOLOGY
STRONGER
TOGETHER

PENTESTERRA

ATTACK CHAIN ANALYSIS

Not a CVE List - A Graph of How an Attacker Gets In

Combines web, network, and code findings into directed kill-chain paths, scored by exploitability and blast radius.

5 Sources

Network, web, API, code, OSINT in one graph

ATT&CK

Every node mapped to a tactic and technique

Verified

Chains built from proven, not theoretical, steps

WHY NOW

Three separate teams each closed their own medium-severity ticket last quarter - none of them knew the three combined into one critical path. A vulnerability report scores findings in isolation. An attacker doesn't - they chain them. That gap is exactly where a breach starts.

HOW IT WORKS

Cross-Domain Correlation

The engine pulls findings from every source - network scan, web and API pentest, code analysis, OSINT - and builds a graph of how they connect. A medium on a VPN, an info on an admin API, and a low on a build runner can become one path from the internet to the database.

- → Network + web + API + code + OSINT findings in one graph
- → The artifact from step one is the input to step two
- → Not a list of vulnerabilities - realistic exploitation routes
- → Recomputed on every assessment cycle

MITRE ATT&CK Mapped

Every node in a chain is mapped to an ATT&CK tactic and technique - initial access, execution, privilege escalation, lateral movement, impact.

- → Per-node tactic and technique mapping
- → Phase view from initial access to business impact
- → Chain diff between cycles: new, closed, changed

Business Impact & Compliance Context

A chain that ends at a payment database matters more than one that ends at a marketing microsite. Each path is scored for business impact and mapped to the compliance frameworks it touches.

- → Business-process and asset-criticality scoring
- → Compliance mapping: OWASP, PCI-DSS, GDPR, NIST, ISO
- → Executive summary plus the single highest-leverage fix

Powered by Real Verification

Chains are built from verified findings, not CVSS guesses. Where a step is exploitable, the engine has a proof of concept, and after a fix lands, the whole chain is re-run to confirm it is actually broken.

- → Every chain step backed by exploit verification
- → Regression detection when a fixed step reopens
- → Confirmed vs. potential separation - clearly shows where a real finding exists

WHY PENTESTERRA

The only platform that unifies web pentest + network scan + DevGuard (code/secrets) in one graph - many competitors stop at only network or only code. Up to 20 attack chains computed per cycle, at depth ≤ 5.

FREQUENTLY ASKED QUESTIONS

What is attack chain analysis?

The process of correlating individual security findings into multi-step attack paths - showing how an attacker moves from an entry point through several weaknesses to a high-value target - instead of treating each finding as an isolated ticket.

How is it different from a vulnerability report?

A vulnerability report scores each finding independently. Attack chain analysis models the artifact an attacker carries between steps - a shell, a token, a session - so a set of low and medium findings can add up to a critical path that no single score reflects.

Which sources feed the chains?

Network scanning, web and API penetration testing, code and supply chain analysis, and OSINT. If a module has a finding, the chain engine can use it.

Does it re-check after remediation?

Yes. When a fix is applied anywhere on a chain, the engine re-runs the whole path and reports whether it is genuinely broken, and it raises a regression alert if a previously closed step reopens.

See how isolated findings become real attack paths

Point Pentesterra at your environment and let the graph build itself.

info@pentesterra.com

pentesterra.com/attack-chain-analysis