PENTESTERRA
SEE THE REAL RISK

ATTACK | VALIDATE | STRENGTHEN

HUMAN RISK
REAL IMPACT
LOWER EXPOSURE

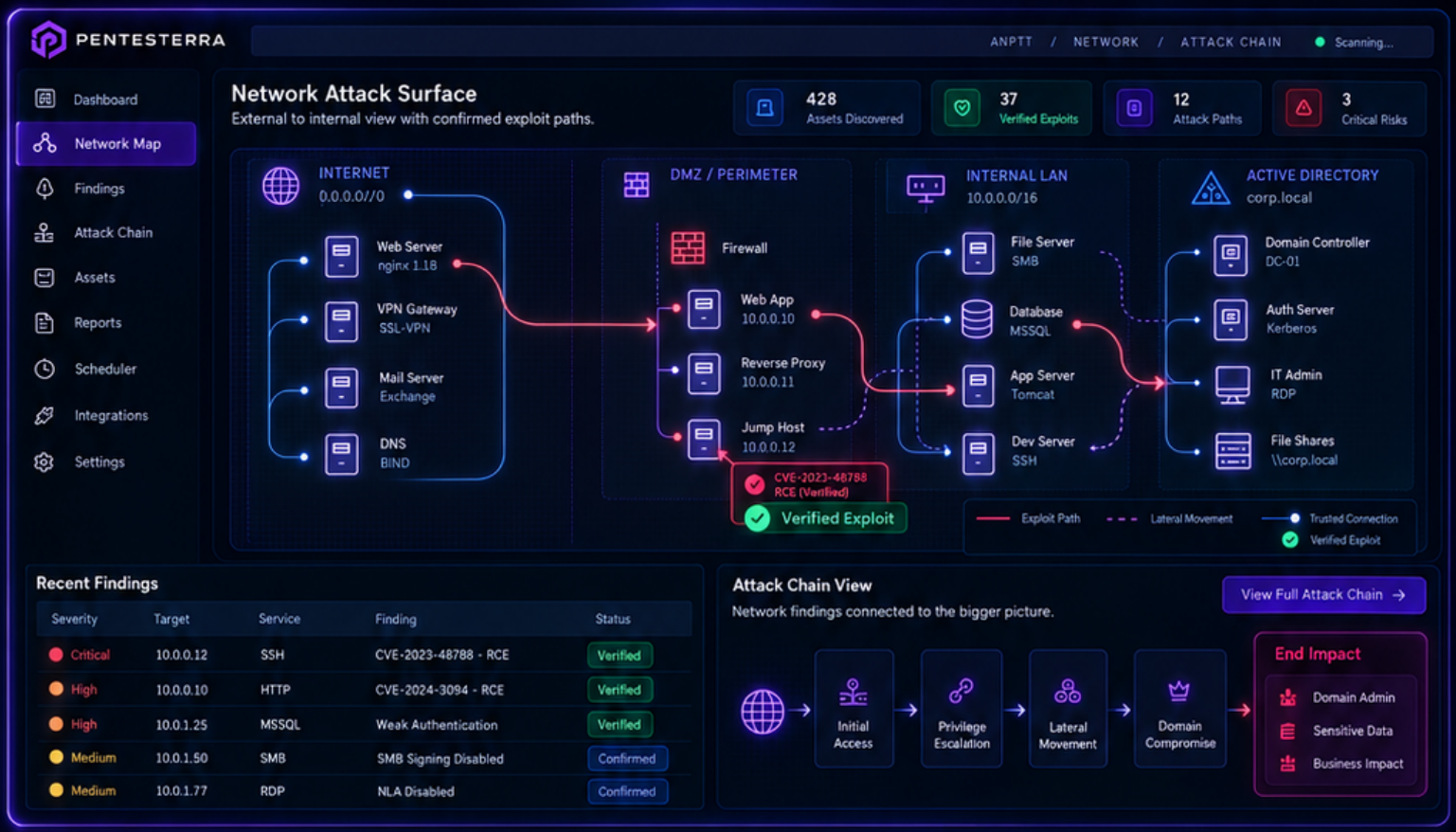
CONTINUOUS
OFFENSIVE SECURITY
FOR A MORE
RESILIENT TOMORROW.

ANPTT MODULE

Automated Network Penetration Testing.

From discovery to confirmed exploitation — continuously, not once a year.

Real exploits against real services — external and internal, on a schedule, with proof, not a CVSS guess.



Recent Findings

Severity	Target	Service	Finding	Status
Critical	10.0.0.12	SSH	CVE-2023-48788 - RCE	Verified
High	10.0.0.10	HTTP	CVE-2024-3094 - RCE	Verified
High	10.0.1.25	MSSQL	Weak Authentication	Verified
Medium	10.0.1.50	SMB	SMB Signing Disabled	Confirmed
Medium	10.0.1.77	RDP	NLA Disabled	Confirmed

Attack Chain View

Network findings connected to the bigger picture.

View Full Attack Chain →

Initial Access → Privilege Escalation → Lateral Movement → Domain Compromise → End Impact

- Domain Admin
- Sensitive Data
- Business Impact

What it does

- Distributed scanner nodes cover the external perimeter (internet-facing, agentless) and the internal LAN (Active Directory attack paths, lateral movement) from one platform
- Full discovery → service fingerprinting → CVE correlation (CISA KEV, Metasploit, ExploitDB) → non-destructive exploit verification → business-impact scoring
- Detects exposed databases (MySQL, PostgreSQL, MongoDB, Redis, MSSQL...), exposed admin services (SSH, RDP, VNC, Telnet, SMB...), weak TLS, unpatched OS
- Runs weekly/daily/on every infra change via schedule or API trigger — full audit trail + delta reporting per cycle
- Findings become nodes in the cross-domain Attack Chain graph — network + web + code in one exploitation path
- No agents to install; SaaS, dedicated PaaS, or fully air-gapped on-prem

Why Pentesterra

- Most network scanners stop at the CVE list — Pentesterra safely launches real exploit checks to confirm exploitability
- External and internal perimeter in one data model — not separate tools stitched together
- Not a sandbox-only view — production-safe testing by default, with staging and production isolation

> *Know what's actually exploitable.*
> *Not just what looks bad on paper.*
> — PENTESTERRA

REAL EXPLOITS
REAL ENVIRONMENTS
REAL SECURITY
REAL ADVANTAGE

THE ANPTT WORKFLOW

1. **Discover** — Map assets
2. **Fingerprint** — Identify services
3. **Correlate** — Match real exploit intel
4. **Verify** — Confirm safely
5. **Prioritize** — Score business impact

- **External + Internal** — One unified view
- **Non-Destructive** — Production-safe
- **Continuous** — On your schedule
- **Attack Chain Ready** — Full context
- **Air-Gapped Option** — On-prem capable

Validate what is truly exploitable.

Explore ANPTT →

PEOPLE
PROCESS
TECHNOLOGY
STRONGER
TOGETHER

PENTESTERRA

NETWORK PENTEST (ANPTT)

Real Exploits Against Real Services

Automated Network Penetration Testing (ANPTT) runs from discovery to confirmed exploitation - external and internal, on a schedule, with proof, not a CVSS guess.

24/7
Continuous coverage, not an annual engagement

In + Out
External perimeter and internal LAN, one data model

0 Agents
Nothing installed on the assets you scan

WHY NOW

Your last network pentest was in the annual budget cycle - a lot has changed on the network since. A new server stood up last month, a firewall rule opened for a vendor and never closed. The gap between "tested" and "exposed right now" is exactly where breaches happen.

HOW IT WORKS

Always-On, Not Once a Year

ANPTT runs on a schedule or API trigger - weekly, daily, or on every infrastructure change. Every cycle covers discovery, service fingerprinting, exploit validation, and lateral movement simulation.

- → Configurable cadence: scheduled, on-demand, or CI/CD-triggered
- → Full audit trail per cycle with delta reporting
- → Covers internal LAN, cloud, and hybrid topologies

Real Exploits, Verified Safely

Most network scanners stop at the CVE list. Pentesterra safely launches real exploit checks to confirm exploitability, using the same escalating verification chain as the rest of the platform.

- → CISA KEV → Metasploit modules → ExploitDB → custom non-destructive scripts
- → No data deletion, no denial-of-service payloads, nothing that exfiltrates data
- → Optional human-in-the-loop approval before active exploitation

External and Internal, One Data Model

Not separate tools stitched together. The same platform sees what an outside attacker sees and what an attacker already on the LAN sees, in one unified view.

→ Detects exposed databases (MySQL, PostgreSQL, MongoDB, Redis, MSSQL)

→ Exposed admin services (SSH, RDP, VNC, Telnet, SMB), weak TLS, unpatched OS

→ Findings become nodes in the cross-domain Attack Chain graph

Deploy However Your Environment Requires

SaaS with private scanner nodes, a dedicated single-tenant PaaS, or full on-premises with zero external connectivity - the same platform, three deployment tiers.

→ SaaS + private scanner nodes: cloud control plane, data never leaves your perimeter

→ Dedicated PaaS: isolated control plane, your own node fleet

→ Full on-prem GOV Edition: air-gapped and classified environments supported

FREQUENTLY ASKED QUESTIONS

Do I need to install agents?

No. Scanning is fully agentless. Distributed scanner nodes assess the external perimeter from outside and the internal perimeter from inside the network - there is no host software to deploy on the assets being scanned.

Is exploit verification safe to run on production?

Yes. Verification is non-destructive by default - no data deletion, no denial-of-service payloads, and nothing that reads or exfiltrates confidential data. Each scan has an explicitly defined scope, staging and production are isolated, and a human-in-the-loop mode can require analyst approval before any active exploitation step.

Can this run in an air-gapped environment?

Yes. The Full On-Premises (GOV Edition) tier runs every component - API, console, workers, scanner nodes - inside your data center with zero external connectivity, offline KB and CVE update channels, and support for classified networks.

Where do the findings go?

Into every other module. They set pentest scope and priorities, become nodes in cross-domain attack chains, correlate with DevGuard and web pentest findings, and feed compliance and business-impact reporting.

See what's actually exploitable on your network

Start with your external perimeter, add internal scanner nodes when ready.

info@pentesterra.com

pentesterra.com/continuous-pentest