vicarius

vRx vRadar

Full Vulnerability Scan

A Full Vulnerability Scan is an end-to-end assessment that identifies security weaknesses across all discovered hosts, ports, and services. It combines host discovery, port scanning, and deep vulnerability probing for the most complete coverage possible.

How it works

1. **Host discovery** - Detects active systems using ICMP, TCP, and ARP probes.
2. **Port scanning** - Identifies open TCP/UDP ports across the full range.
3. **Service detection** - Determines type and version of every running service.
4. **Vulnerability testing** - Inference engine runs targeted checks — each detected service triggers specific modules, results activate deeper checks.
5. **Credentialed scanning** - Optional — with admin credentials, checks missing patches, registry entries, and config issues.

What you get

- **Vulnerability details: severity, CVE references**
- **Affected host, service, and proof-of-concept evidence**
- **Prioritization by severity and exploitability**
- **Actionable remediation and patching guidance**

Why it's important

- **Comprehensive risk visibility across network and application layers**
- **Patch validation and compliance reporting in a single pass**
- **Reduces attack surface by identifying exploitable weaknesses early**

Comparison to Competitors

Capability	vRadar	Nessus / Tenable	Qualys	Rapid7 InsightVM	OpenVAS
Core Approach	**Full: discovery → deep vuln testing**	Strong plugin orchestration	Cloud-based detection	Multi-phase + asset context	Basic, limited plugin accuracy
Coverage	**Full network, OS, app library**	Broad plugin-based	Cloud-integrated library	Wide + contextual priority	Community-maintained
Credentialed	**Windows, SSH, OS-level**	Full coverage	Trusted scanning	Agent-assisted	Limited by plugin scope
Customization	**Policy-based: Full, Patch Tue, Net Device...**	Template selection	Prebuilt cloud profiles	Flexible site-based	Manual setup required
Exploit Integ.	**SAINTexploit (optional)**	External tools	None	Metasploit integrated	None