vicarius

vRX vRadar

Discovery Scan

A discovery scan identifies which hosts in a network are active before deeper scanning begins. It is the first phase in any vulnerability assessment, used to build an accurate inventory of reachable devices and prevent wasted time scanning inactive IPs.

How it works

1. **ICMP echo sweep** - Sends ping requests to each target IP.
2. **TCP SYN/ACK probes** - If ICMP fails, sends SYN packets to common ports (22, 80, 443) and interprets replies as “alive”.
3. **ARP requests (local)** - Uses ARP or IPv6 ND to discover devices even when ICMP/TCP is blocked.
4. **Nmap integration** - Runs Nmap discovery with multiple techniques – SYN, ACK, UDP.
5. **Extensive mode** - Scans all IPs without discovery filtering for full coverage, at cost of speed.

What you get

- **Reachable hosts with IP and optional hostname**
- **No CVE data – forms input list for subsequent scans**
- **Exportable as an asset inventory baseline**

Why it’s important

- **Ensures resources target only active systems**
- **Reduces false negatives via multiple probe types**
- **Missed hosts here create blind spots in all subsequent scans**

Comparison to Competitors

Feature	vRadar	Nessus / Tenable	Qualys	Rapid7	OpenVAS
ICMP Ping Sweep	✓ **Native**	✓	✓	✓	✓
TCP / UDP Probes	✓ **Selectable**	✓	✓	✓	✓
ARP / IPv6 ND	✓ **Built-in**	✓	✓	✓	Partial
Nmap Integration	**Native full flags**	None native – internal engine	None native – internal engine	None native – internal engine	Partial
Fine-tuned control	**ICMP, SYN, ACK, UDP**	Limited	Limited	Limited	Moderate