Types of Vulnerability Testing Tools

Dale Meredith

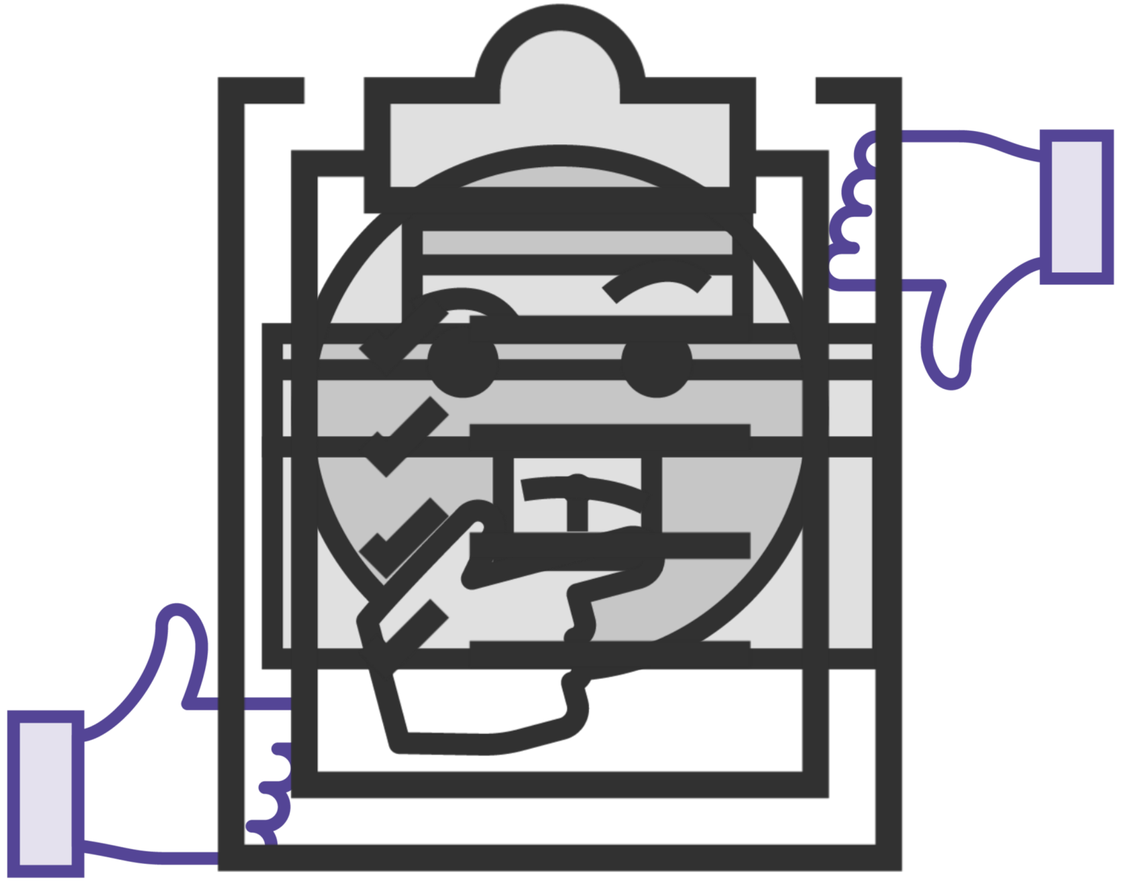
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith

Comparing Approaches to Vulnerability Assessments

Vulnerability Assessment Approaches

- **Product-based solutions**
- **Service-based solutions**
- **Tree-based assessments**
- **Inference-based assessments**
- **The hybrid approach**



Product-based Solutions

Installed on an organization's internal network

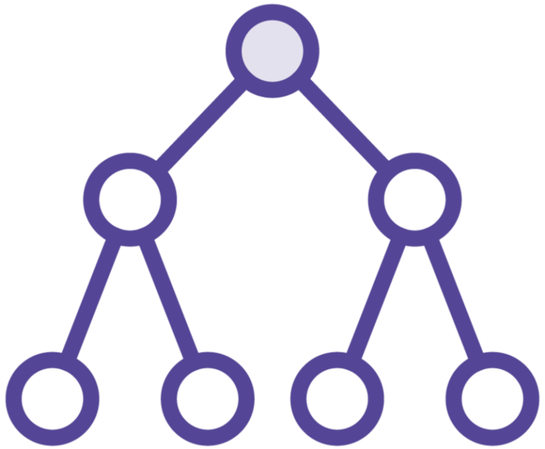
May not detect outside assaults if they are behind a firewall

Service-based Solutions

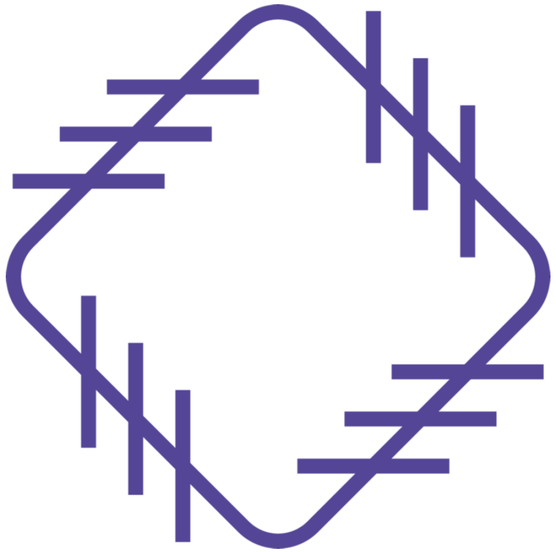
Offered as a managed service

Provide a continuous and real-time assessment

Tree-based Assessment



Top-down approach



Prioritizes where to patch

Time-consuming

Requires a comprehensive network list

Inference-based Assessment

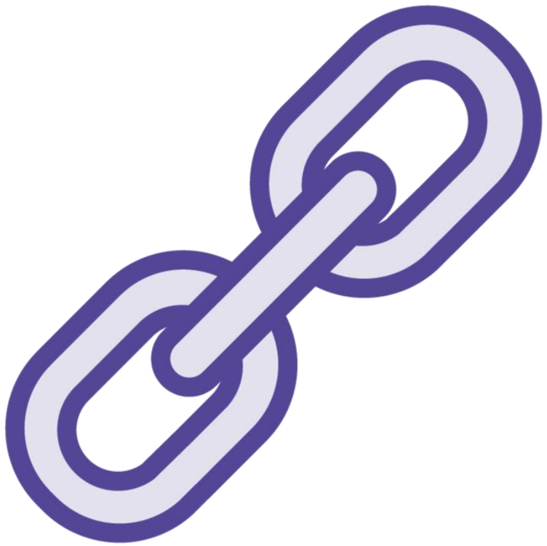
Bottom-up approach

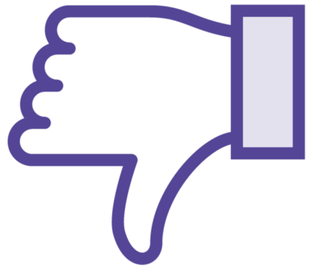
Starts with least critical needs

Less time-consuming

The Hybrid Approach

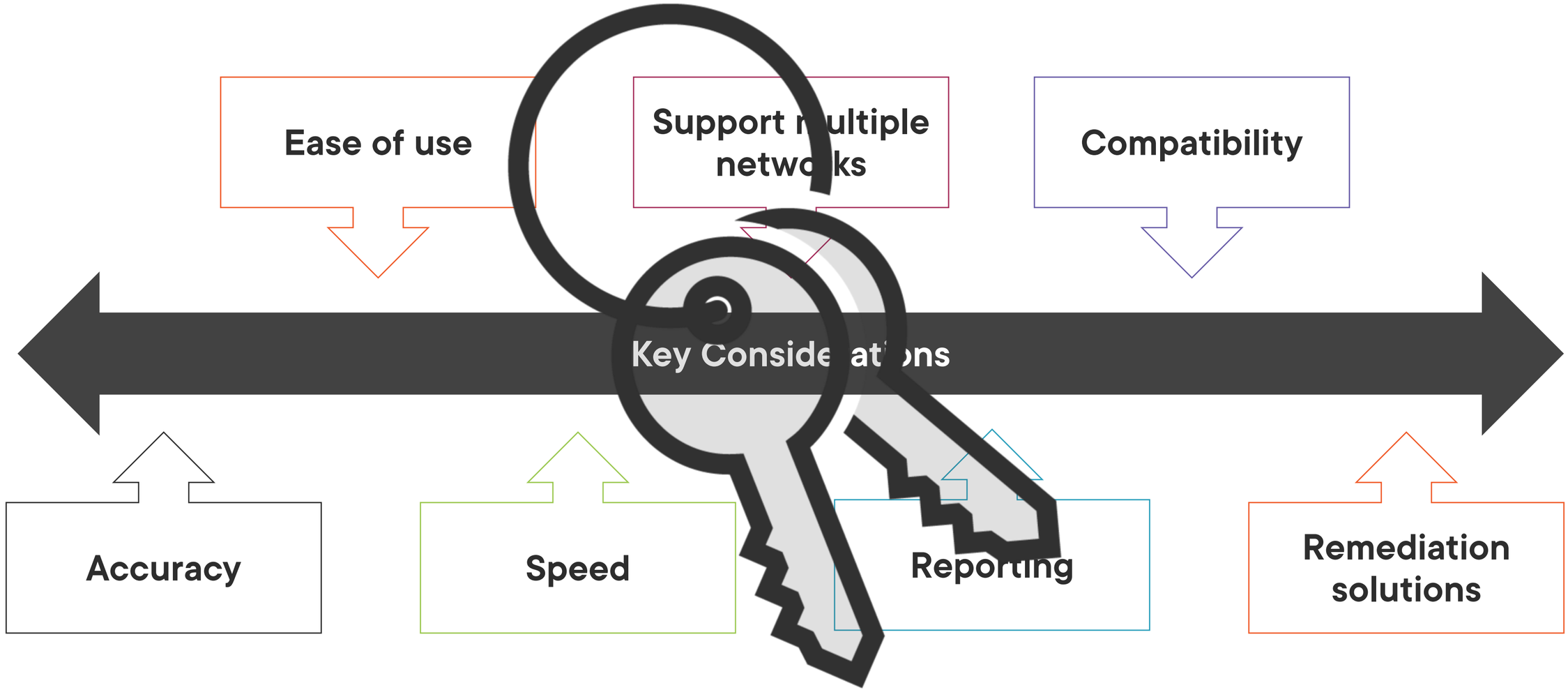
Comprehensive





Time-consuming

Characteristics to Look for in a Vulnerability Assessment Software?



Commercial and Open-source Tools

Nessus

OpenVAS

Nikto

QualysGuard

Rapid7 Nexpose

Workings of Vulnerability Scanning Solutions

Vulnerability Scanning Solutions

Discovery

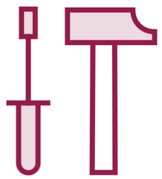
OS and Services Discovery

Vulnerability Assessment

Types of Vulnerability Assessment Tools

Vulnerability Assessment Tools

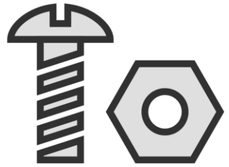
Host-based tools



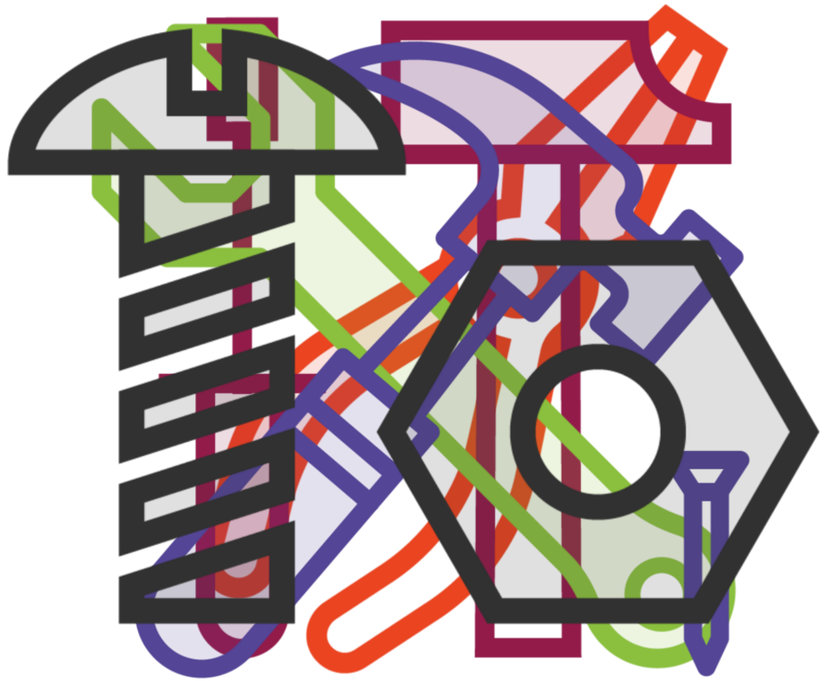
Depth assessment tools

Application-layer tools

Scope Assessment tools



Active and Passive tools



Vulnerability Assessment Tools

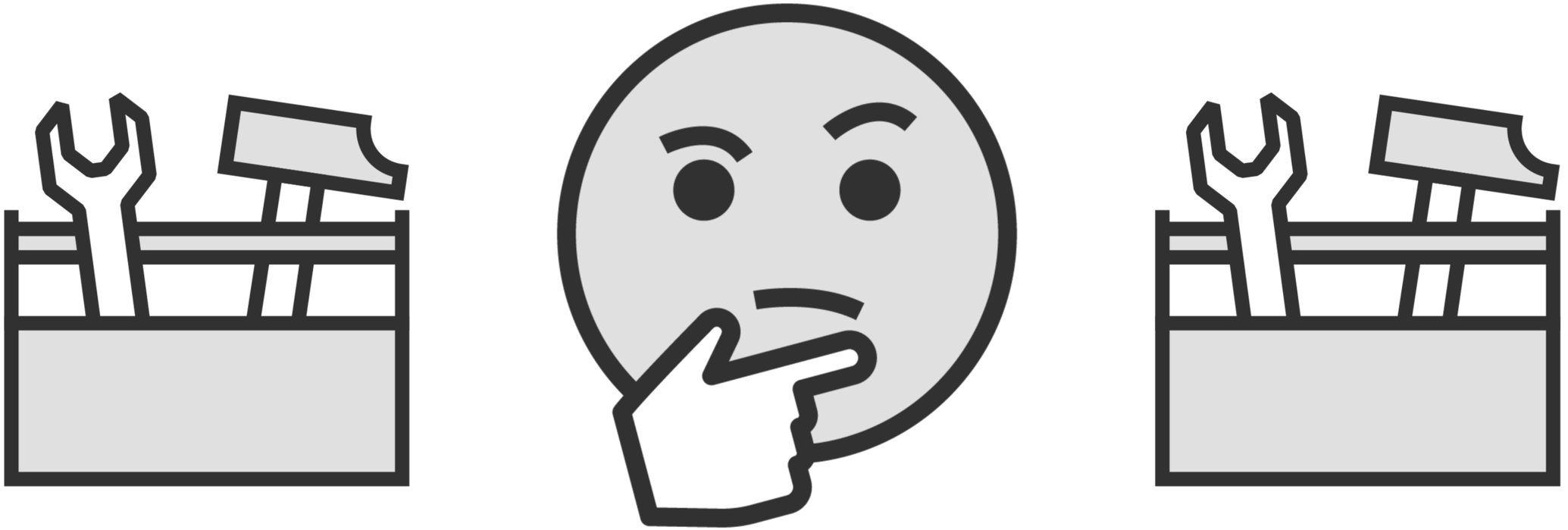
Network-based scanner

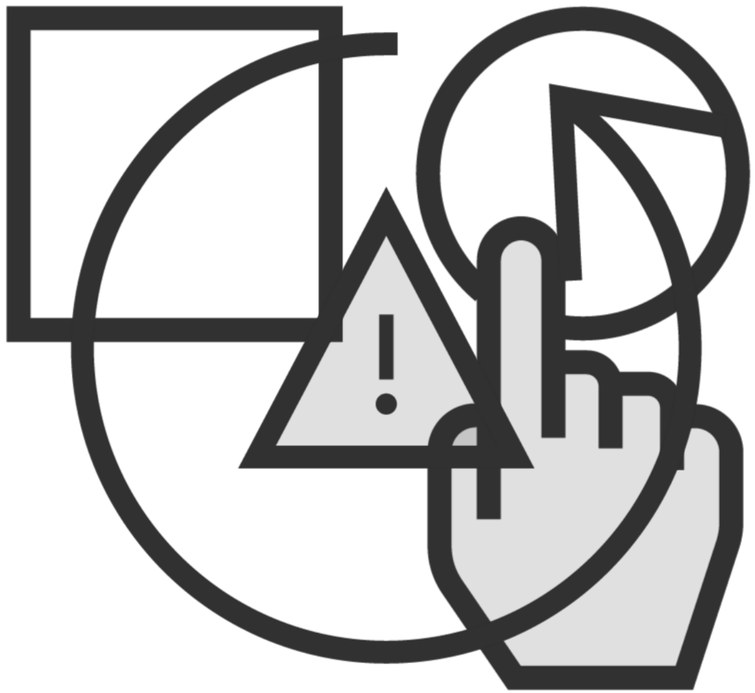
Agent-based scanner

Proxy scanner

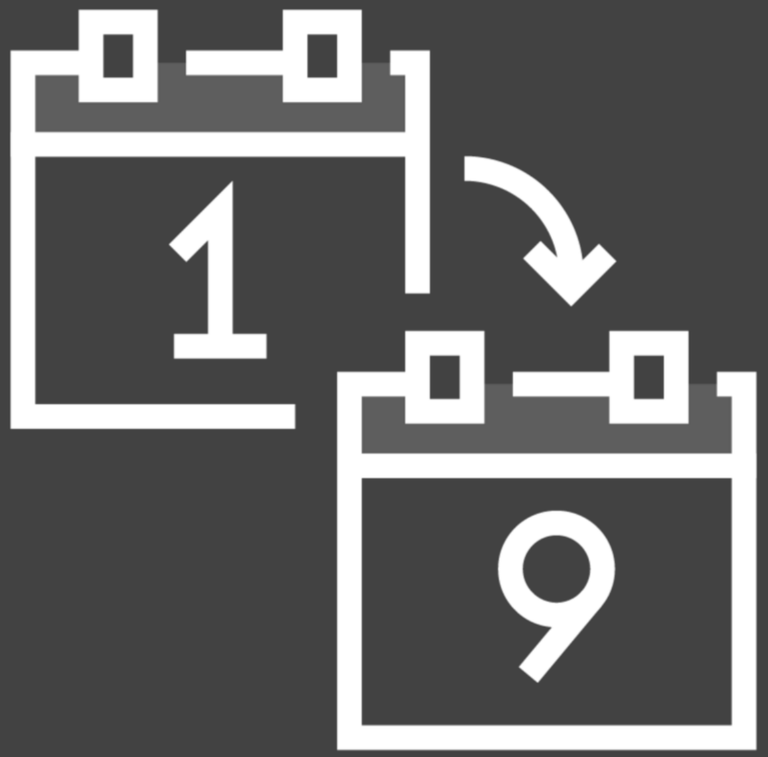
Cluster scanner

Choosing a Vulnerability Assessment Tool





- High capacity
- Large database and up-to-date attack signatures
- Matches the environment
- Up to date scan engine
- Accurate network mapping, application mapping, and penetration testing
- Updated vulnerability scrips
- Implement required patches
- Adequate reports



Demo

OpenVAS

Demo

Nikto

Vulnerability Assessment Tools for Mobile

Vulnerability Assessment Tools for Mobile

Vulners Scanner

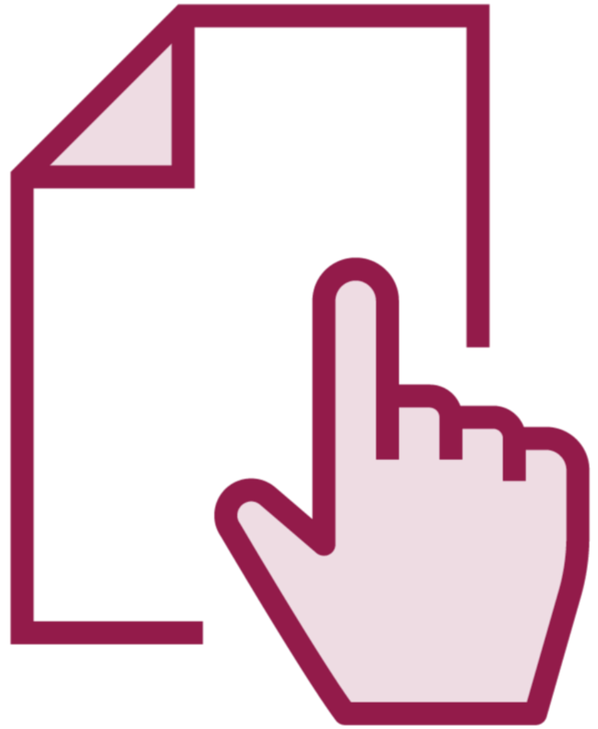
Netsparker

SecurityMetrics

Learning Check

Learning Check

- **Tree-based**
- **Discovery**
- **OS and Service**
- **Cluster**



Up Next:
Analyzing Your Vulnerability Assessment Reports