Examining Vulnerability Scans

Dale Meredith
MCT/CEI/CEH/Security Dude
Owner: Wayne Technologies

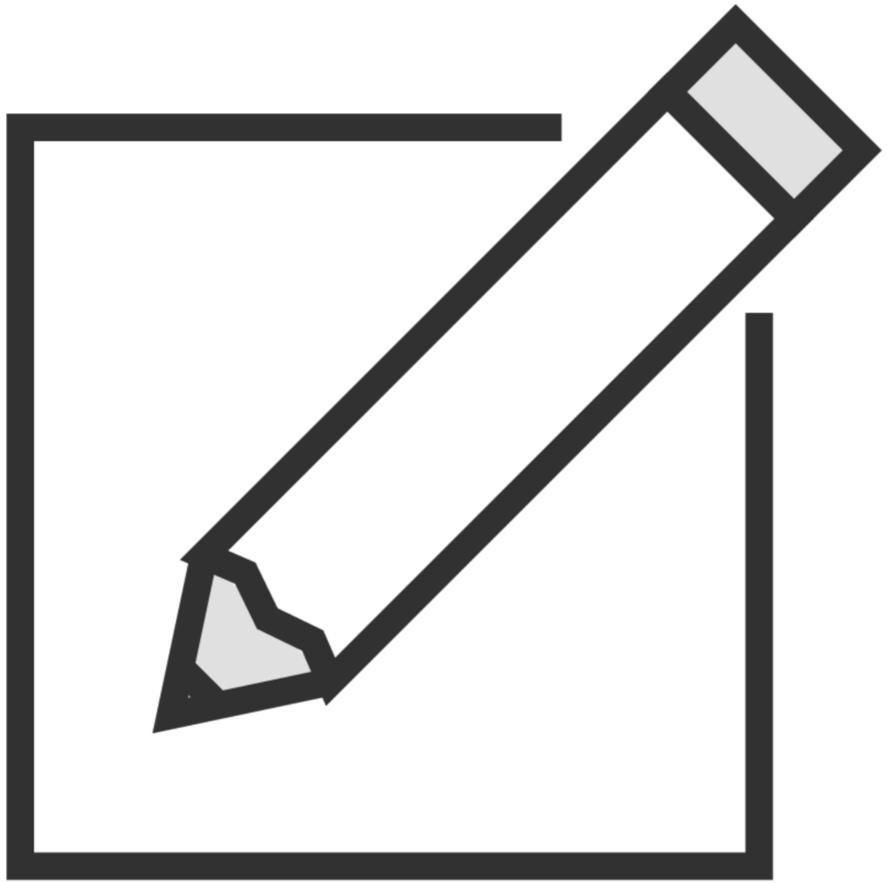
:@dalemeredith :daledumbsITdown :daledumbsITdown
:dalemeredith www.daledumbsITdown.com

A man’s got to know his limitations.

Harry Callahan

What Is Vulnerability Scanning

The Basics

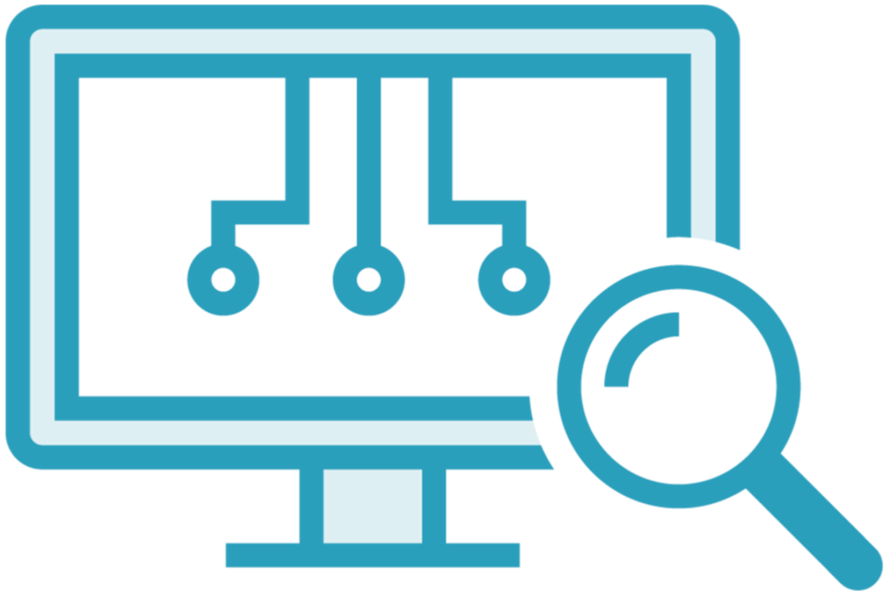


Software

Looks at

Network systems
Computers
Operating systems
Applications

The Basics

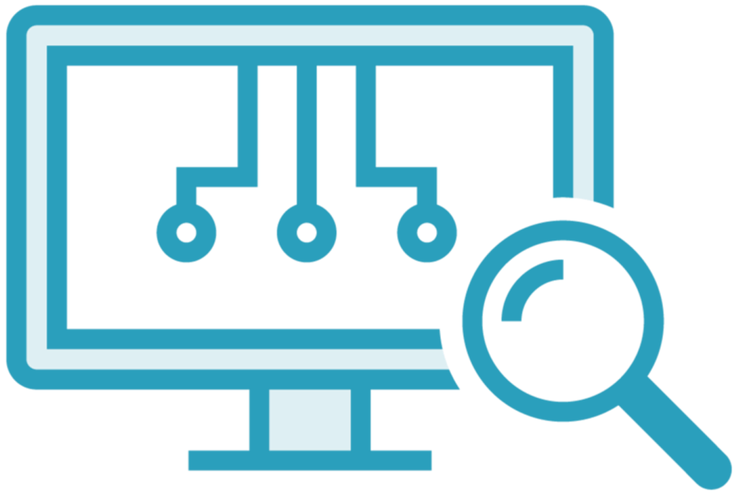


The causes of vulnerabilities

- User initiated
- Vendor created
- Sys Admin generated

Types of Scanners

Types of Scanners



Network based

- Web server scanners
- Port Scanners
- Web App Scanners

Host based

- Designed for specific hosts
- Look for signs of penetration
- Performs baselines checks

The Pros and Cons of Vulnerability Scanners

Limitations

Human judgment

It’s only a snapshot

Only “known” vulnerabilities

Parts is parts (or plugins)

Benefits

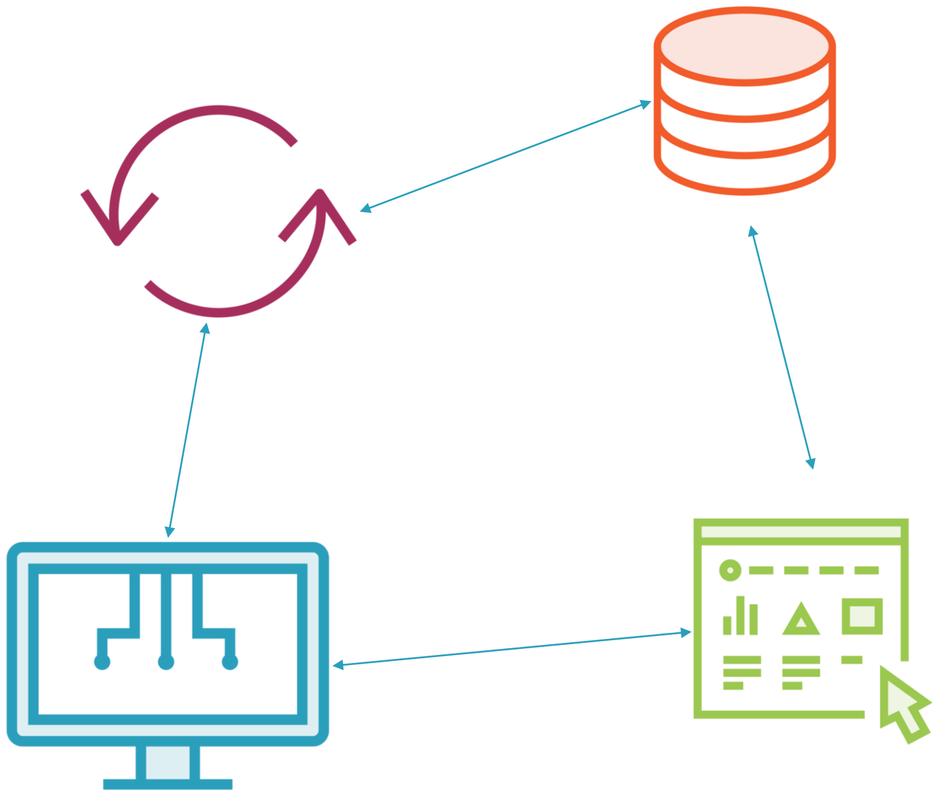
Detect & resolving of security issues

New device / rogue systems

Verify inventory

How Vulnerability Scanners Work

The Gears of Vulnerability Scanners



1) Engine runs security check
2) Database stores results/info
3) Reporting services
4) UI

Vulnerability Scanning Tools

So Many Choices, So Little Time

Considerations

Updates and plugins
Quality vs. accuracy
Reporting options

Deployment

Placement of scanner
Port ranges
Baseline setup
Post scanning practices

Possible Issues to Consider

Be Aware Of...

Possible issues

Potential threats

Handling results

Policies and actions

The Tools You Can Use

Tools, Tools, and More Tools

Saint

MBSA

Core Impact Pro

GFI LanGuard

Retina

Nessus

Demo

Vulnerability Scanning with Nessus

- Install Nessus
- Perform a scan
- View results

Next Up:
Building out Maps of The Network