FANSHAWE

INFO-6065

Ethical Hacking & Exploits

Automated Scanners

OpenVAS

Open Vulnerability Assessment Scanner

Agenda

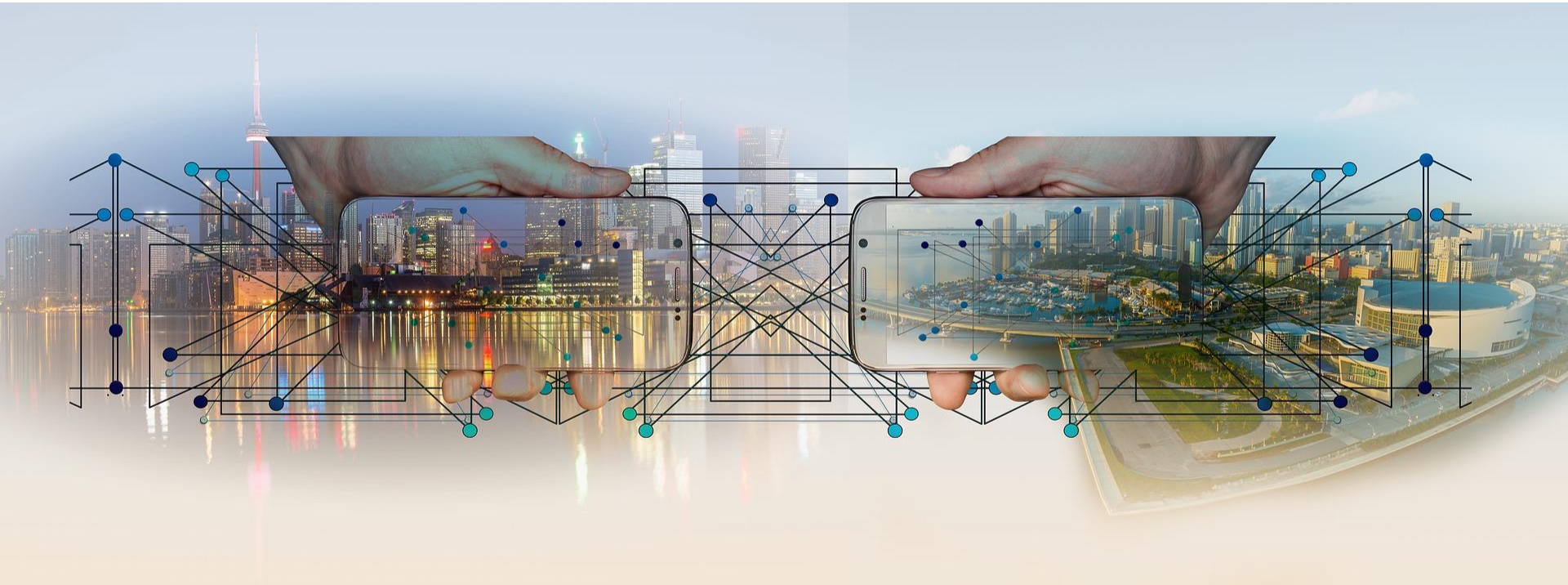
- Vulnerability Management
- Automated Vulnerability Scanners
- OpenVAS Lab-03

FANSHAWE

Terminology

Vulnerability Mapping:

- Process of identifying and analyzing the security flaws in a target environment



Terminology

Types of Vulnerabilities:

Design: Weakness in software specifications

Implementation: Technical problems found in the code of the system

Operational: Improper configuration and/or deployment

Local & Remote

Local Vulnerabilities

- Attacker requires local access to the system to trigger the vulnerability

Remote Vulnerabilities

- Performed across the network against a machine the attacker has had no previous access to

Patch Tuesday

- Microsoft releases Security Bulletins on “Patch Tuesday”
- This is the second Tuesday of every month

msrc.microsoft.com/update-guide

Microsoft | MSRC | Security Updates | Acknowledgements | {} Developer

Release ...	Product	Platform	Impact	Max Severity	Article	Download	Details
Sep 13, 2022	Microsoft .NET Framework 3.5 AND 4.8	Windows 10 Version 20H2 for x64-based Systems	Remote Code Execution	Important	5017498	Security Update	CVE-2022-26929
Sep 13, 2022	Microsoft .NET Framework 3.5 AND 4.8	Windows Server 2022 (Server Core installation)	Remote Code Execution	Important	5017501	Security Update	CVE-2022-26929
Sep 13, 2022	Microsoft .NET Framework 3.5 AND 4.8	Windows Server 2022	Remote Code Execution	Important	5017501	Security Update	CVE-2022-26929
Sep 13, 2022	Microsoft .NET Framework 3.5 AND 4.8	Windows Server 2019 (Server Core installation)	Remote Code Execution	Important	5017315	Security Update	CVE-2022-26929
Sep 13, 2022	Microsoft .NET Framework 3.5 AND 4.8	Windows Server 2019	Remote Code Execution	Important	5017315	Security Update	CVE-2022-26929

Checking for Security Updates

- Example update from Microsoft

Microsoft | Support Microsoft 365 Office Windows Surface Xbox Deals Buy Microsoft 365

Products Devices What's new Account & billing Templates More support

September 13, 2022-KB5017024 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 11

.NET

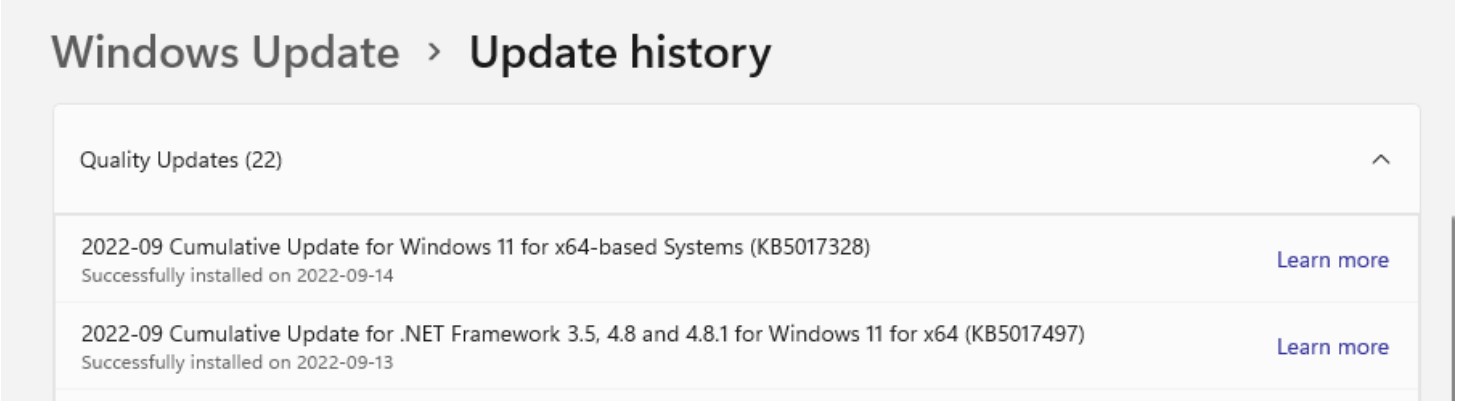
Release Date:
September 13, 2022

Version:
.NET Framework 3.5 and 4.8

The September 13, 2022 update for Windows 11 includes cumulative reliability improvements in .NET Framework 3.5 and 4.8. We recommend that you apply this update as part of your regular maintenance routines. Before you install this update, see the Prerequisites and Restart requirement sections.

Microsoft Security Updates

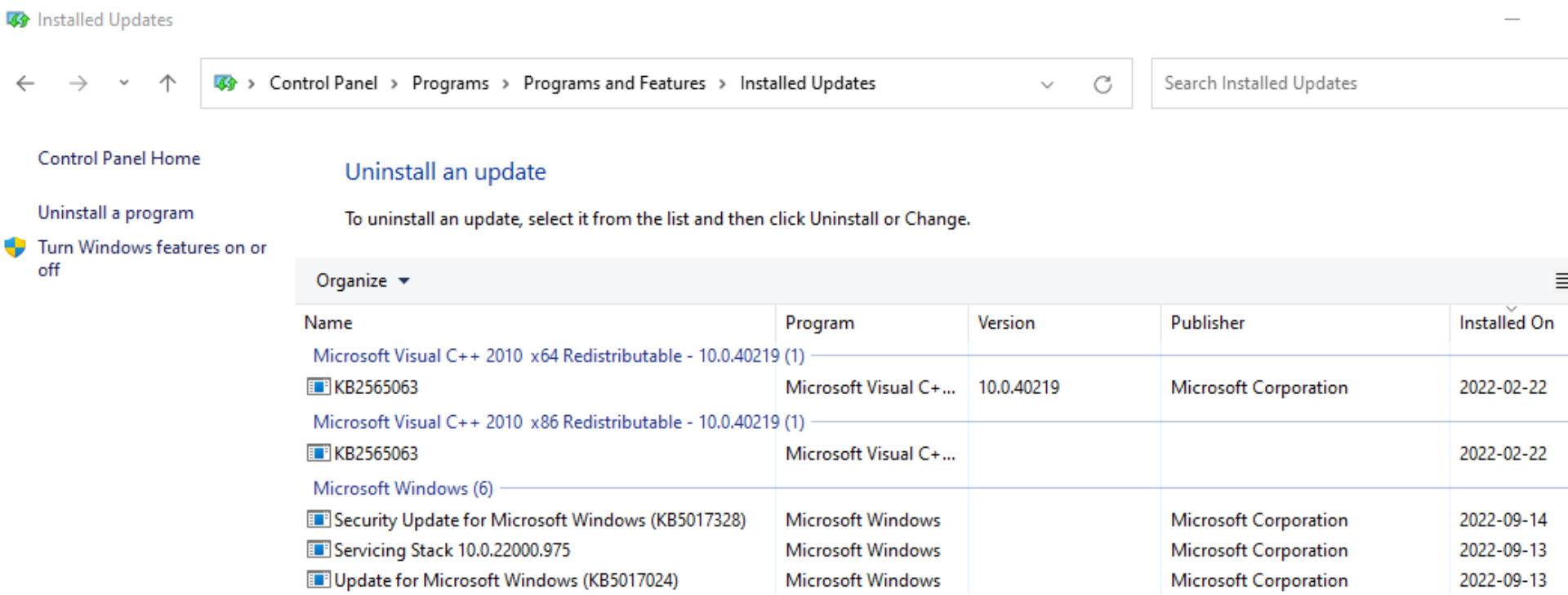
- Microsoft Windows will list updates with a **KB** number (aka. KBnnnnn)
- One way you can check if you have the required updates is by using Windows Update History



Checking for Security Updates

- Another way to check is to run **appwiz.cpl** or:

Programs -> Programs and Features -> Installed Updates



Checking for Security Updates

- Windows also allows CMD or PowerShell checks:

wmic qfe list full /format:table

Command Prompt

```
Microsoft Windows [Version 10.0.22000.978]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Venkman>wmic qfe list full /format:table
Caption                                    CSName   Description      FixComments  HotFixID   InstallDate  InstalledBy          InstalledOn
http://support.microsoft.com/?kbid=5017024 VENKMAN  Update                        KB5017024               NT AUTHORITY\SYSTEM  9/14/2022
https://support.microsoft.com/help/5007575 VENKMAN  Update                        KB5007575               NT AUTHORITY\SYSTEM  2/24/2022
https://support.microsoft.com/help/5012170 VENKMAN  Security Update               KB5012170               NT AUTHORITY\SYSTEM  8/10/2022
https://support.microsoft.com/help/5017328 VENKMAN  Security Update               KB5017328               NT AUTHORITY\SYSTEM  9/14/2022
                                           VENKMAN  Update                        KB5015898               NT AUTHORITY\SYSTEM  8/10/2022
                                           VENKMAN  Security Update               KB5018291               NT AUTHORITY\SYSTEM  9/14/2022
```

Checking for Security Updates

- Below is an example of a KB check in Windows PowerShell:

Get-HotFix

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> Get-HotFix

Source        Description      HotFixID      InstalledBy          InstalledOn
------        -----------      --------      -----------          -----------
VENKMAN       Update           KB5017024     NT AUTHORITY\SYSTEM  2022-09-14 12:00:00 AM
VENKMAN       Update           KB5007575     NT AUTHORITY\SYSTEM  2022-02-24 12:00:00 AM
VENKMAN       Security Update  KB5012170     NT AUTHORITY\SYSTEM  2022-08-10 12:00:00 AM
VENKMAN       Security Update  KB5017328     NT AUTHORITY\SYSTEM  2022-09-14 12:00:00 AM
VENKMAN       Update           KB5015898     NT AUTHORITY\SYSTEM  2022-08-10 12:00:00 AM
VENKMAN       Security Update  KB5018291     NT AUTHORITY\SYSTEM  2022-09-14 12:00:00 AM
```

Here we can see that according to PowerShell, KB5017024 was installed the next day

Automated Vulnerability Scanners

Vulnerability Scanners

Network or Vulnerability Scanners typically check for any known vulnerabilities in devices connected to the IP network

- Operating systems
- Applications
- Default configurations
- Mobile devices
- Network devices
- Network protocols

Automated Vulnerability Scanners

Automated Scanners make it easy to perform scans, but this can have some drawbacks

- Can produce more false positives and false negatives than manual scanning
- Only find vulnerabilities that are part of the library of vulnerabilities
- Don’t require as high a skill level to run, which can lead to situations where the auditor doesn’t understand the results and can’t act on them

Automated Vulnerability Scanners

Pros of automated network vulnerability scanners:

- Capable of scanning many systems and devices in a short amount of time
- They can detect vulnerabilities that might be missed by manual testing
- They can schedule regular scans to identify new vulnerabilities as they are introduced
- They can provide detailed and actionable reports that can be used to prioritize and address vulnerabilities
- They can be integrated with other security tools and systems to provide a more comprehensive security solution

Automated Vulnerability Scanners

Cons of automated network vulnerability scanners:

- May produce numerous false positives, which can be time-consuming to sort through
- They may not be able to detect all vulnerabilities, particularly those that are unknown to the scanner or zero-day
- They may not consider the specific configuration of a network or system, which could result in missed vulnerabilities
- Typically require a significant number of resources, including hardware, software and personnel to maintain and operate
- They can be expensive to acquire and maintain
- They may not be able to detect vulnerabilities in a custom application, or those that are only exploitable under certain conditions

Vulnerability Management

Vulnerability scanners play an important role in "patch management"

Organizations rely on them to keep track of missing patches, new vulnerabilities, and mitigation solutions

Automated Vulnerability Scanners

False Positive: scanner thinks there is a vulnerability, but there isn't one

False Negative: scanner thinks there is no vulnerability, but in fact, one exists

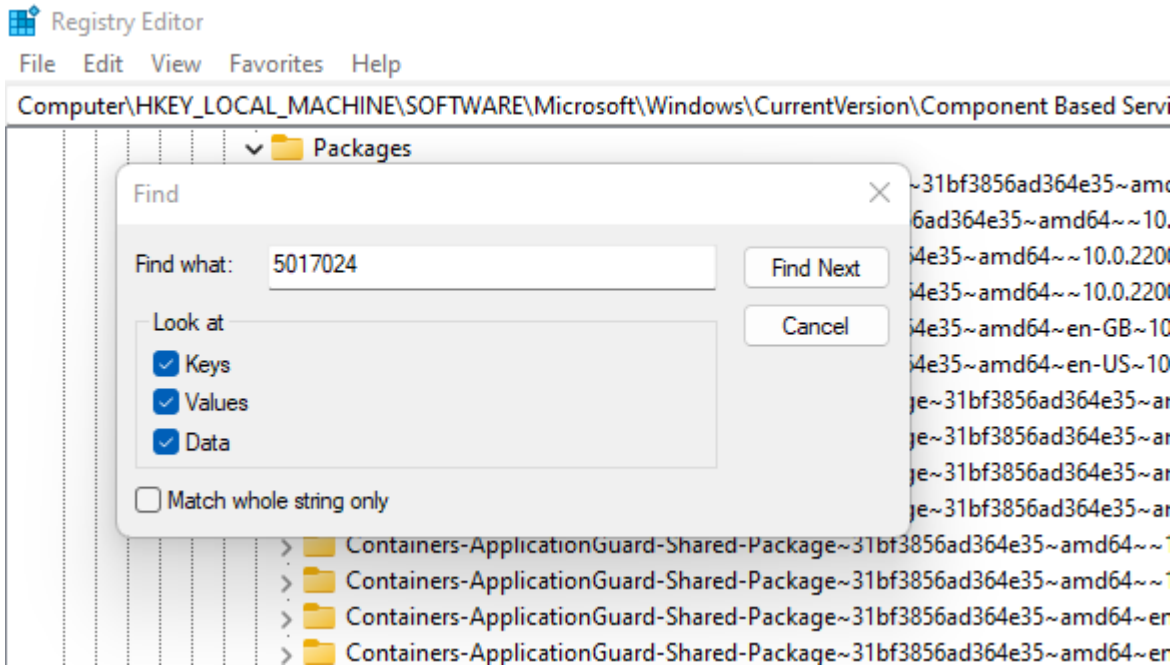
Credentialed Scans

- Scanners offer credentialed scans, where the administrator provides a valid login to the machines being scanned
- This allows the scanner to fully scan a system for missing security patches
- This allows for Registry checks in addition to shell commands

Credentialed Scans

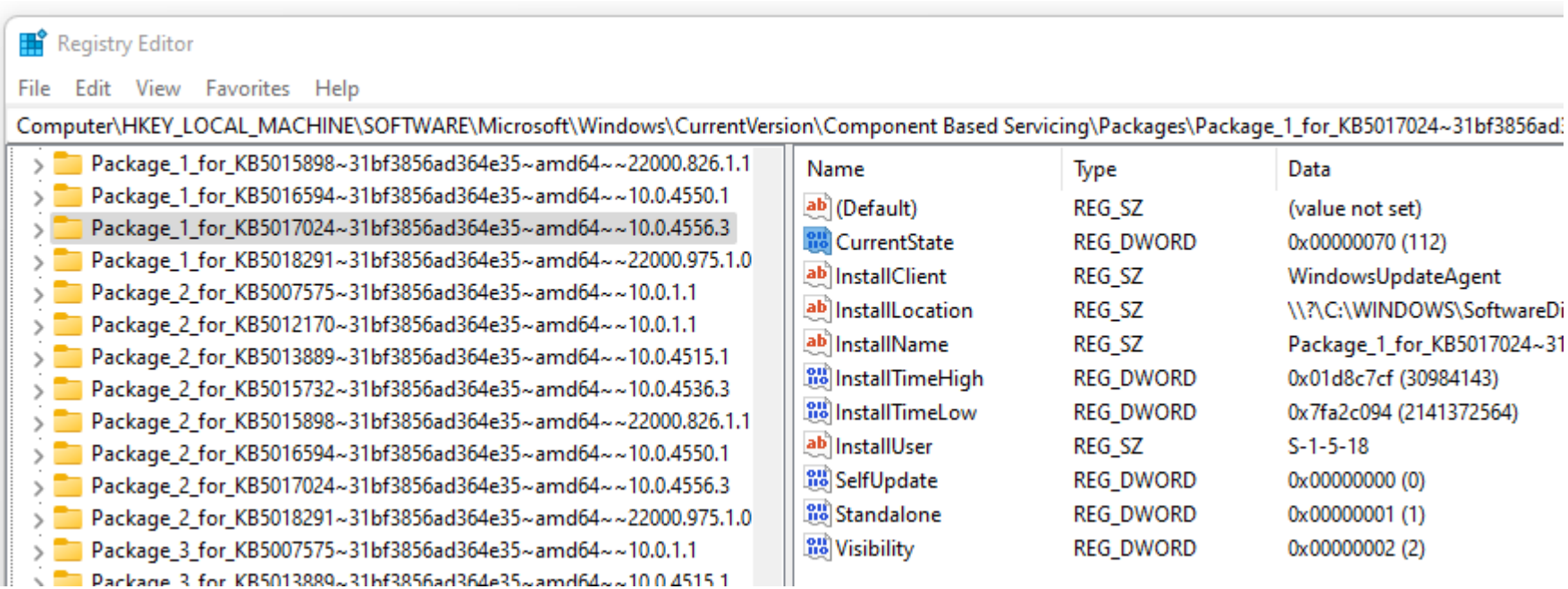
- Use **edit -> find** to search for KB5017024

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing\Packages



Credentialed Scans

- The value data for "**CurrentState**" will read 0x00000070 (112) if the update was successfully installed



Credentialed Scans

Package location: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing\Packages\<package name>

Applicable/Current State	Hex	Dec
Absent	0	0
Uninstall Pending	0x5	5
Resolving	0x10	16
Resolved	0x20	32
Staging	0x30	48
Staged	0x40	64
Superseded	0x50	80
Install Pending	0x60	96
Partially Installed	0x65	101
Installed	0x70	112
Permanent	0x80	128

https://learn.microsoft.com/en-us/archive/blogs/tip_of_the_day/tip-of-the-day-cbs-servicing-states-chart-refresher

FANSHAWE

Commercial Scanners

Nessus

tenable.com/products/nessus

tenable

Platform Products Solutions Resources Partners Support Company Try Buy

NESSUS IS #1 FOR VULNERABILITY ASSESSMENT

From the beginning, we've worked hand-in-hand with the security community. We continuously optimize Nessus based on community feedback to make it the most accurate and comprehensive vulnerability assessment solution in the market. 20 years later and we're still laser focused on community collaboration and product innovation to provide the most accurate and complete vulnerability data - so you don't miss critical issues which could put your organization at risk.

Today, Nessus is trusted by tens of thousands of organizations worldwide as one of the most widely deployed security technologies on the planet - and the gold standard for vulnerability assessment. See for yourself - explore the product here.

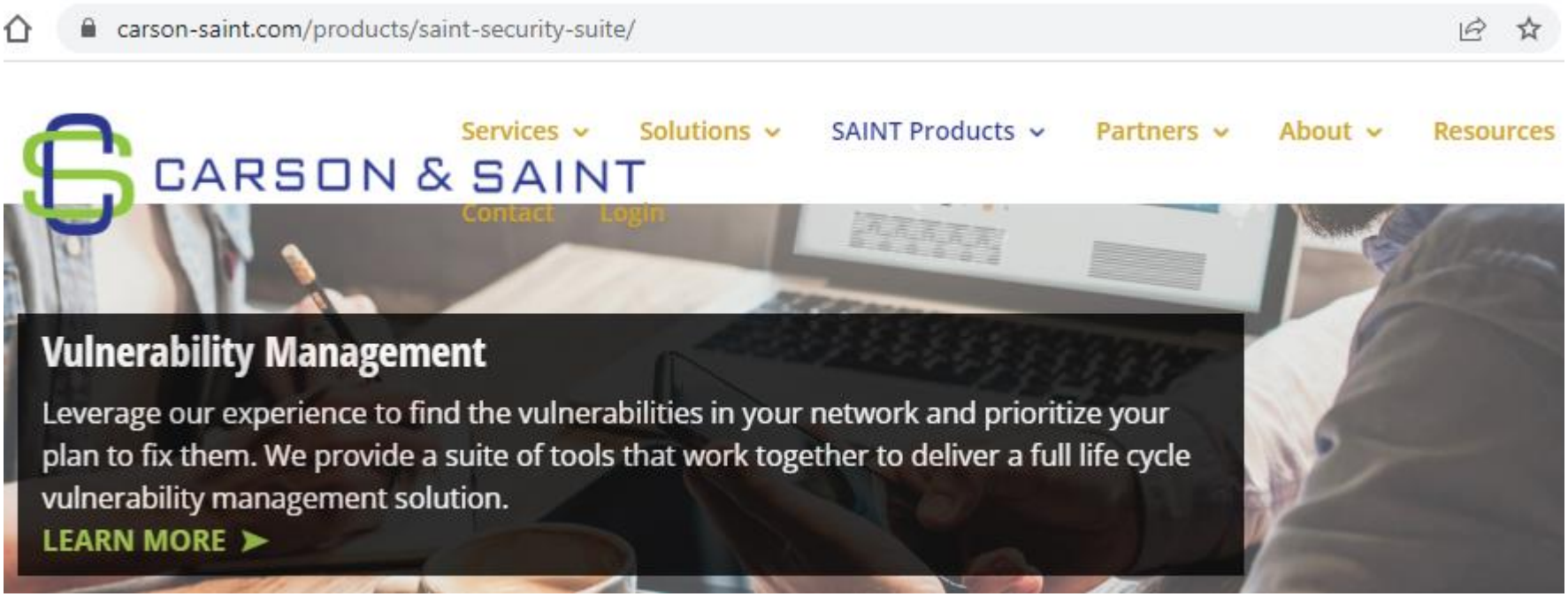
73K+	180,000+	100+
CVEs	Plugins	new plugins released weekly

Tenable's Zero Day Research provides 24/7 updates into new and emergent vulnerabilities so you'll always have full situational awareness.

Commercial Scanners

SAINT

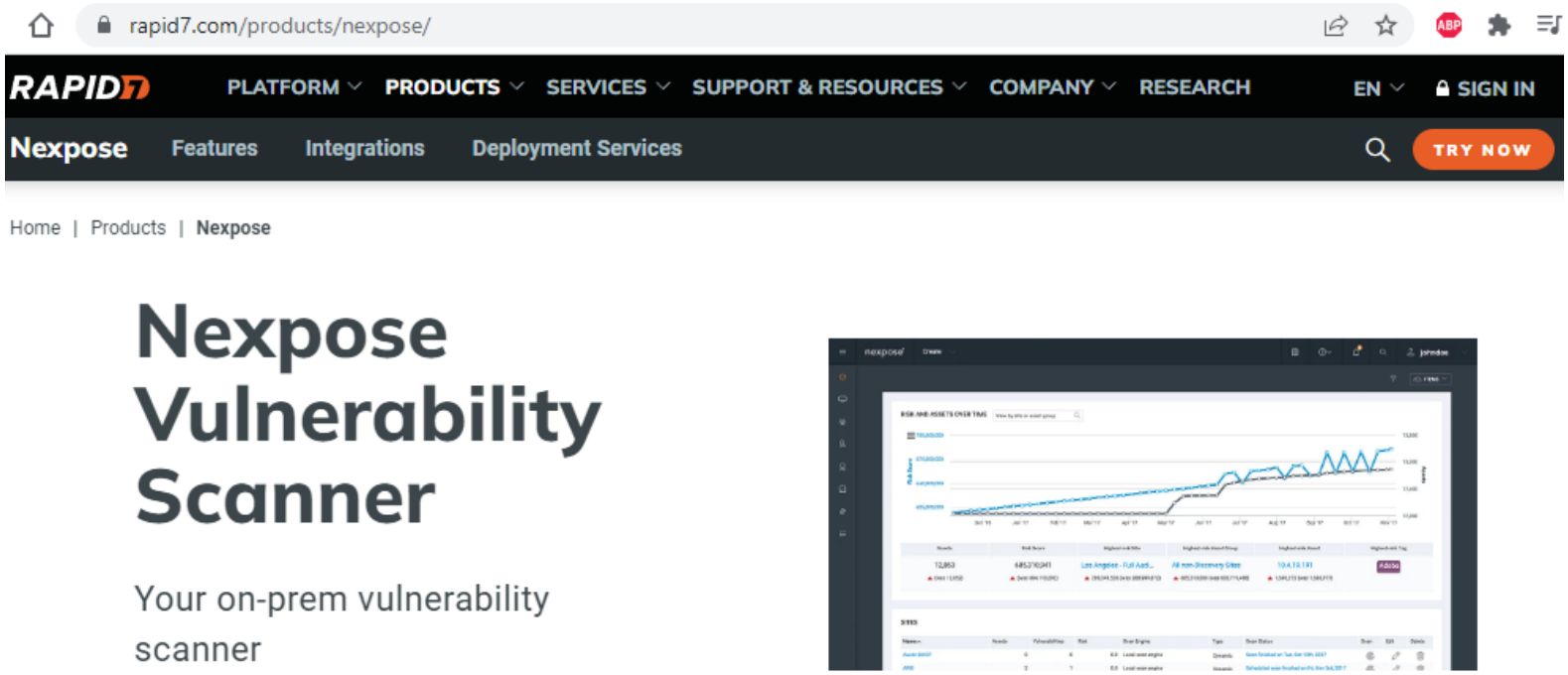
- Standalone, cloud and appliance versions
- Vulnerability Assessment, Penetration Testing, Compliance Auditing, Configuration Assessments



Commercial Scanners

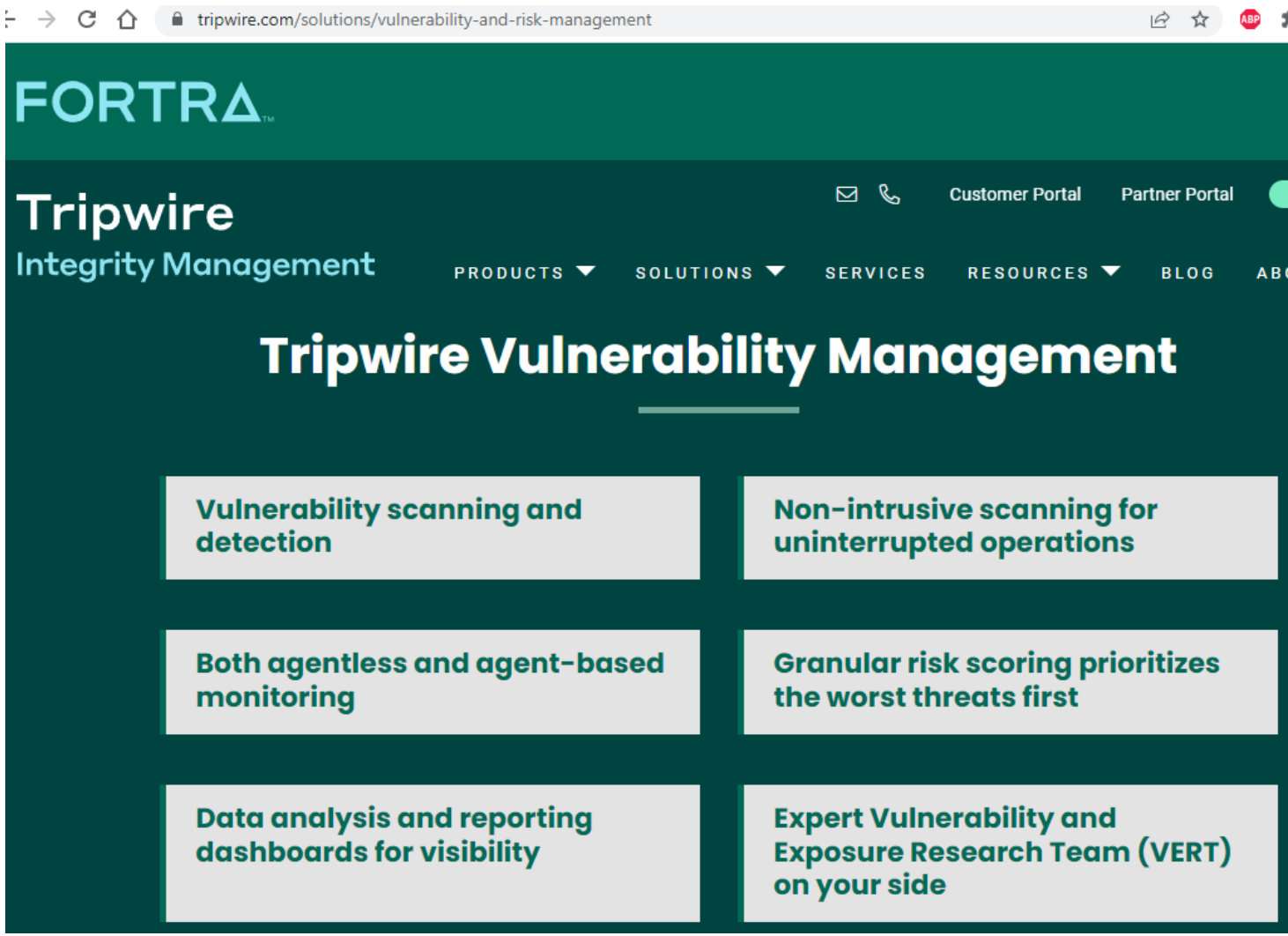
Nexpose

- Vulnerability Assessment, Compliance Auditing
- Integrated with Metasploit



Commercial Scanners

- Tripwire



OpenVAS

openvas.org

openvas.org

Greenbone OpenVAS

Open Vulnerability Assessment Scanner

Greenbone OpenVAS

OpenVAS is a full-featured vulnerability scanner. Its capabilities include unauthenticated and authenticated testing, various high-level and low-level internet and industrial protocols, performance tuning for large-scale scans and a powerful internal programming language to implement any type of vulnerability test.
The scanner obtains the tests for detecting vulnerabilities from a feed that has a long history and daily updates.

OpenVAS has been developed and driven forward by the company Greenbone Networks since 2006. As part of the commercial vulnerability management product family Greenbone Enterprise Appliance, the scanner forms the Greenbone Community Edition together with other open-source modules.

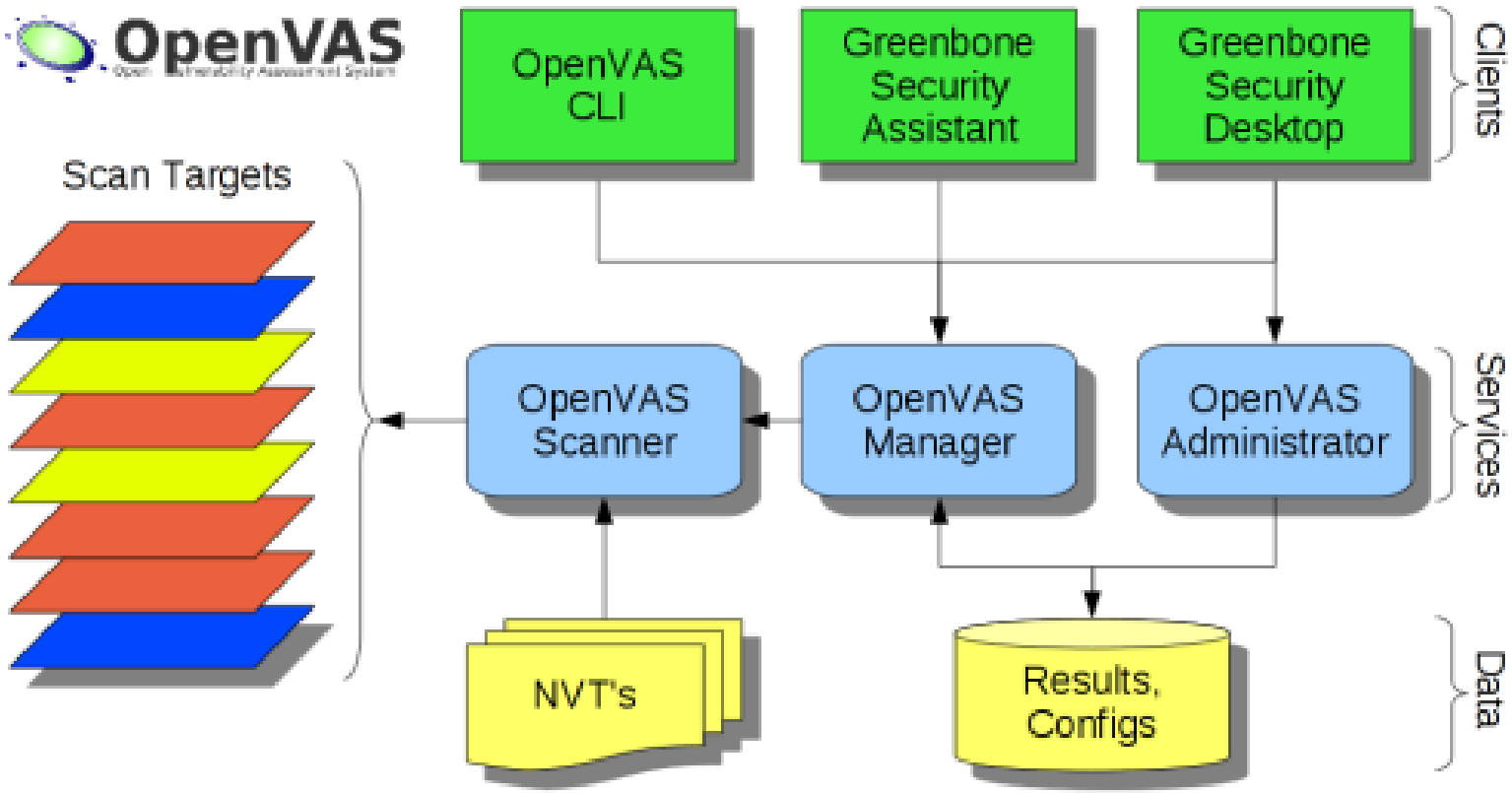
Read more about the history of OpenVAS here.

OpenVAS

- OpenVAS
  - **O**pen **V**ulnerability **A**ssessment **S**ystem
  - Free Vulnerability Scanner
  - Forked off the Nessus project
  - Uses NVTs (Network Vulnerability Tests)

OpenVAS Architecture

- Clients, Services, Data and Targets



OpenVAS Clients

Ways you can interact with OpenVAS

OpenVAS CLI

- Command line interface
- Similar to using msfconsole

Greenbone Security Assistant

- Web interface
- Connects via port 9392
- Similar to using Metasploit via web interface

Greenbone Security Desktop

- Desktop client
- Similar to using Armitage

OpenVAS Services

OpenVAS Scanner

- Manages the execution of NVTs

OpenVAS Manager

- Manages scan results
- Schedules scans
- Handles reporting

OpenVAS Administrator

- User management
- Feed synchronization
- Feed status

OpenVAS Data

NVTs

- Network Vulnerability Tests
- Over 110,000

Results, Configs

- SQLite Database

Greenbone Security Assistant

- Web based graphical user interface
- Connects to the OpenVAS Manager via OMP
  - OpenVAS Management Protocol
- Interface is broken into seven main tabs
  - Scan Management
  - Asset Management
  - SecInfo Management
  - Configuration
  - Extras
  - Administration
  - Help

Greenbone Security Assistant

Scan Management

- Creation and management on tasks

Asset Management

- Information about the hosts found

SecInfo Management

- Information about NVTs, CVEs, CPEs, etc.

Configuration

- Various Configuration parameters
- This is where you set up new targets
- A target must be set up before it can be scanned

Greenbone Security Assistant

Extras

- Trashcan, personalized settings and performance statistics

Administration

- User management
- Feed management

Help

- Limited Help Files, but there is some good information in there

GSA Reports

After you scan a target, you are presented with a variety of information:

- Identified Security Issues
  - High, Medium, Low, Log, False Positive
- Ability to filter results
- CVSS Score
- Description of Vulnerability
- Relevant CVE identifiers
- Links to more information
- Possible solutions

Scanner Comparison

- You can go to the site below for the full article

  http://hackertarget.com/nessus-openvas-nexpose-vs-metasploitable/

Nessus 5 External Network Profile	Critical **3** High **6** Medium **22** Low **8** Info **137**
OpenVAS 5 Full Audit Scan Profile	High **38** Medium **24** Low **36** Log **44**
Nexpose Full Audit Scan Profile	Critical **49** Severe **103** Moderate **18**

Comparison

The author of the article came to several conclusions:

- You need to tune the scanner to your needs
- You need to analyze the results in detail
- You need to run secondary scans based on the information provided
  - nmap
  - platform specific scanners

Lab 03: Details

- Configure OpenVAS
- Set up a variety of targets and task
- Investigate scheduling options
- Investigate access controls built into OpenVAS
- Investigate vulnerability details
- Find an exploit metasploitable2 based on vulnerability information found in scan