OpenVAS guidance

v1.0

LOCAL DIGITAL Cyber

Overview

Outline guidance and approach of considerations to be given to the implementation of OpenVAS software for all applicable Local Authority information systems.

For further information on using Greenbone VMS (aka OpenVAS) please contact the Cyber Support Team at cybersupport@localdigital.gov.uk

LOCAL DIGITAL Cyber

What are vulnerability scans

- Vulnerability scanning products identify potential vulnerabilities but do not exploit the vulnerabilities.
- Vulnerability scans are run to identify potential vulnerabilities in an IT environment.
- It is generally an automated process with the focus of finding potential and known vulnerabilities within your system.
- The focal points for scanning are devices such as firewalls, routers, switches, servers, operating systems and applications.
- It should be noted such scans are ineffective at finding zero-day exploits, **but carrying out regular vulnerability scans is infinitely better than not doing so**.
- Vulnerability scanning scope should be business-wide and requires automated tools to manage a high number of assets.

LOCAL DIGITAL Cyber

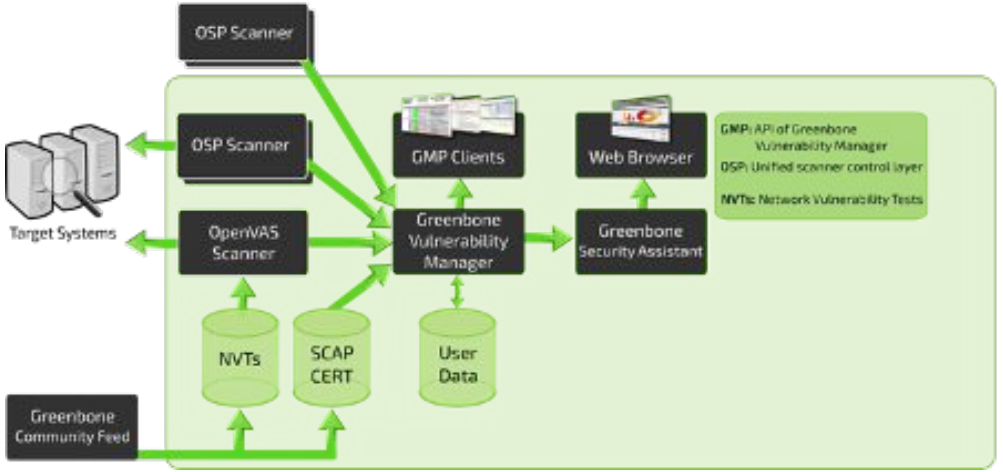
What is OpenVAS software ?

- Background:
  - OpenVAS began under the name of GNessUs, as a fork of the previously open source Nessus scanning tool, after its developers Tenable Network Security changed it to a proprietary (closed source) license in October 2005.
  - OpenVAS is a member project of Software in the Public Interest
  - OpenVAS is currently known as Greenbone Vulnerability Management
- Vulnerability Management
  - Vulnerability management is the process of identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them.
  - Taking the results from a Vulnerability Scan and acting on them is vital for organisations to prioritise the remediation of potential threats.

LOCAL DIGITAL Cyber

How does OpenVAS work ?

Once installed, the OpenVAS scanner and OSP scanner will carry out a series of vulnerability scans against the defined target systems. This data is then collated by the vulnerability manager (Greenbone GVM) and presented to the user via a web interface.



LOCAL DIGITAL Cyber

Why run vulnerability scans ?

Running vulnerability testing scans on a regular basis will identify any security vulnerabilities in your network.

Reasons to run these regularly include (but are not limited to):

- The simplest reason - **prevention is better than cure !**
- Scan results will help prioritise where and how to spend time, money and resource on system enhancements
- Reduce your exposure to known security threats (Threats are discovered and exploited on almost a daily basis at present).
- Peace of mind - Regularly running scans and acting on findings will hopefully allow you to believe you've done everything practicable to protect your assets.

LOCAL DIGITAL Cyber

How often to run a vulnerability scan?

There is no 100% correct answer. Estimates vary from weekly to annually !
They represent a snapshot of the vulnerabilities at the time the scan was ran.

The answer should be geared around how often you make system changes.
Any new software, hardware or application should be considered a possible trigger to run a scan.

Running them too often would give you little time to enact any required changes, and leaving long gaps between scans would leave you open to recently identified threats!

Quarterly scans are a good starting point, and you can increase or decrease frequency based on your feedback. Ultimately, the decision should be based around your own circumstances and risk averseness.

LOCAL DIGITAL Cyber

Now what?

The software will have identified vulnerabilities, so the next steps would be to:

- Triage the issues found
- Group them together
- Remediate the issues in order of priority / severity
- Integrate the fixes into your server build / server deployment planning so that future servers are not exposed in the same way.
- **Re-run the scans on a regular basis.**

Scan-->Remediate-->Plan
Repeat !

LOCAL DIGITAL Cyber

Installing OpenVAS

- Download the Local Digital Cyber Prepared Software from :-
  - https://github.com/communitiesuk/cyber-openvas-vm
- Installation Instructions are a part of this download
- Test access

LOCAL DIGITAL Cyber

Vulnerability scanning product options

- Many different Vulnerability Scanning tools exist, ranging from open source to commercial offerings.
- This document is built around an open source version of OpenVAS
- Principles of vulnerability scanning are the same across the spectrum of tools available.

LOCAL DIGITAL Cyber

Ministry of Housing,
Communities &
Local Government

Thank you

We welcome feedback on our cyber support service

@LDgovUK

www.localdigital.gov.uk

#LocalDigital #FixThePlumbing