PROJECT

Multi-tenant cybersecurity operations centre designed as an open cloud service with machine learning elements

Supporting document for V4

Selection and implementation of a vulnerability scanning tool

Linked to work package KPB2 – Design of the SOCaaS service

Funded by the European Union NextGenerationEU

RECOVERY AND RESILIENCE PLAN

GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC

Contents

1. Selection and implementation of the Greenbone vulnerability scanning tool 3

1.1. Functions and capabilities of the Greenbone Vulnerability Management tool 3

1.2. Deployment options 8

1.2.1. Greenbone Community Edition: 8

1.2.2. Greenbone Enterprise Appliance: 9

1.2.3. Greenbone Community Edition 9

1.2.4. Greenbone Enterprise Appliance 11

1.3. Summary 12

List of sources 13

1. SELECTION AND IMPLEMENTATION OF THE GREENBONE VULNERABILITY SCANNING TOOL

The Greenbone Vulnerability Management (GVM) tool has the following properties that are important for this project:

- **Free version with regular updates**: Unlike other tools, GVM also offers a free version that receives regular updates of vulnerability tests. Although the scope of these tests is limited compared with the paid version, it is still sufficient to ensure a minimum level of security.
- **Open-source solution**: GVM is an open-source tool, which provides the possibility of flexibly supplementing its functionality where needed, as well as verifying the security of this tool directly in the source code, thereby eliminating the risks associated with so-called "black-box" solutions.
- **On-premise deployment**: GVM supports on-premise implementation, which ensures better control over security processes.
- **No need for agents**: Unlike some competing tools, GVM does not require agents to be installed on the scanned devices.
- **Quality and compliance with standards**: The tool originates from Germany and meets the requirements of the GDPR and other standards, such as ISO/IEC 27001.

Tab. 1 - Comparison of vulnerability scanning tools

Tool	Free version	Licence price excluding VAT**	Open source	Agentless
Greenbone (GVM)	Yes, regular updates to a limited extent	€2,450 / year	Yes	Yes
Nessus	Yes, limited to 16 IP addresses	€4,549 / year	No	Yes
Nexpose	No, trial only (30 days)	~€6,000 / year (InsightVM)*	No	Yes

* The price of Nexpose is not publicly available. The stated value is based on the approximate price of the InsightVM cloud solution for 250 assets and indicates that the costs of Nexpose will be the same or higher.
** For each tool, the price of the cheapest available licence as of 5/4/2025 is given, namely Greenbone BASIC and Nessus Professional.

In this text, the names GVM, Greenbone, Greenbone Community Edition and OpenVAS will be used interchangeably. All these names are correct, because:

- **OpenVAS** was the original name of the project, which designated the vulnerability scanner. It is now the name of a specific module within the broader solution.
- **Greenbone** is the company that leads the development of OpenVAS and has added further components, resulting in a comprehensive solution.
- **GVM** (Greenbone Vulnerability Management) is the name for the entire vulnerability management solution, which includes OpenVAS and other components. This name will be used most often because it is the shortest.
- **Greenbone Community Edition** is the most recent name, in use since 2022, covering all of Greenbone's open-source software activities.

1.1. Functions and capabilities of the Greenbone Vulnerability Management tool

GVM is a

robust open-source vulnerability scanning tool. A detailed examination of its functions and capabilities is key to understanding how we can implement it effectively within the SOC centre and how significantly it can strengthen the level of cybersecurity across the entire infrastructure. This section focuses on a detailed analysis of the tool, including its functionality, technical requirements and architecture, in order to provide a clear overview of its benefits.

GVM functions

The functionality depends on which specific Greenbone vulnerability scanning product is selected. We analysed in detail the functions of several products, of which 3 basic types are available; we summarize them in table Tab. 2.

Tab. 2 - Comparison of Greenbone products

Properties and functions	Greenbone Community Edition	Greenbone Enterprise Appliances	Greenbone Cloud Service
System updates	Depending on the distribution, manual or custom implementation	Automatic, including security updates + LTS	Automatic, including security updates
Vulnerability test updates	Community Feed	Enterprise Feed (Daily)	Enterprise Feed (Daily)
Integrated protocols	Custom implementation required	NTP, GMP, OSP, HTTPS, SSH, SNMP, Syslog, IPv6, LDAP, RADIUS and others	NTP, GMP, HTTPS, SSH, SNMP, Syslog, LDAP, RADIUS and others
Integrations and connectors	Custom implementation required	PaloAlto, Fortinet, Cisco FireSight, Nagios, Splunk, Verinice and others	RESTful API for all functions
Backup and Recovery	Custom implementation required	User and system data via LVM, transfer via SCP or USB	Automatic
Notifications and task scheduling (scanning)	Custom implementation required	E-mail, HTTP, SMS, connector for a SIEM or ticketing system, and others Full support for task scheduling	E-mail, Slack or Microsoft Teams
Scanning architecture	Monolithic	Master/sensor, Airgap for highly secured parts of the network	Cloud scanner, gateway components for internal scanning
Remediation Tickets	Custom implementation required	Yes	Yes
Support	Community forum	Guaranteed through an SLA	Guaranteed through an SLA
The data were obtained from the official Greenbone website [6].			

As we can see in table Tab. 2 above, most of the additional functionality apart from scanning itself is found in Greenbone's paid products, and if we wanted to use the free Community Edition in the project, it would be necessary either to accept considerably limited and very basic

functionality, naturally also with a substantial investment of effort and time in the maintenance, operation and use of this tool, or to use our own implementations of the functionality we require.

The essential difference between these three products is that "Greenbone Enterprise Appliances" (GEA) and "Greenbone Community Edition" are on-premise solutions, whereas "Greenbone Cloud Service" is a cloud solution. GEA is further divided by deployment method into hardware and virtual solutions. This means that we either purchase a hardware appliance directly, or only a VM and use our own hardware. The available functionality also depends on which solution we choose. Interestingly, with a VM we cannot achieve the same scanning performance as is available when purchasing a GEA hardware solution. The manufacturer apparently deliberately disadvantages VMs in this way because of the higher profit from selling hardware solutions.

The company's licensing model is therefore based on limiting the usable performance for vulnerability scanning itself and, of course, also different functionality, as is customary with other manufacturers. In practice, this means that even if we allocate more resources to the VM, the vulnerability scanning "application" itself will not use them fully, but only up to the level permitted by the purchased licence. A detailed comparison of the individual hardware and virtual solutions (VMs) is available on the official Greenbone website in PDF format. It contains information on which solution includes which functionality and what the maximum usable scanning performance of the given solution is, i.e. what limitations it has. Since comparing Greenbone's individual solutions is not the main objective of the project, and the available solutions and their functionality may change over time and could thus very quickly become outdated, for this reason this information will not be given directly in this text.

We will now look at the vulnerability test updates themselves, the so-called "Feed", and at the difference between the paid Enterprise Feed and the free Community Feed. First, however, we will explain what the Feeds are used for and how they affect the functionality of the tool itself.

It should first be noted that the existence of a Common Vulnerabilities and Exposures (CVE) entry does not necessarily mean that we can detect this vulnerability with this or any other tool. First, in the case of Greenbone as well as other tools, we need the Common Platform Enumeration (CPE) so that, on its basis, we can identify as accurately as possible, for example, which software or service is running on a given IP. CPE is a standardized system for identifying software applications, operating systems and hardware components.
After identifying a running service, such as SSH on the target IP, we can move on to the vulnerabilities themselves. In order to be able to detect a vulnerability with this tool, we also need a so-called Network Vulnerability Test (NVT) for the relevant CVE, and only then can we detect this vulnerability. Put simply, the more vulnerability tests we have, the more vulnerabilities the tool can detect. To illustrate the differences between the Community and Enterprise Feeds, we give the figures in the following clear table Tab. 3.

Tab. 3 - Comparison of Greenbone Feeds - numerical

	Community Feed	**Enterprise Feed**
CVE	288 463	288 463
CPE	1 387 760	1 387 760
NVT	159 122	203 717
CERT-Bund Advisories	23 067	23 067

DFN-CERT Advisories	37 318	37 318
The data are current as of 5/4/2025. They were obtained from an installation of Greenbone Cummunity Edition and the SecInfo portal. [9]		

As we could see in table Tab. 3 above, as far as vulnerability scanning itself is concerned, the difference really lies mainly in the number of NVTs, which may not seem all that significant at first glance. The truth, however, is that Greenbone took care to withhold from the Community Feed precisely the most essential vulnerability tests, as we can also see in table Tab. 4 below, and these concern products intended specifically for enterprises. From this point of view they are of high value for improving the security level of an enterprise network, thereby contributing to effective protection against potential threats.

Tab. 4 - Comparison of Greenbone Feed functionality

	Community Feed	**Enterprise Feed**
Products intended for home use (e.g. Ubuntu Linux, TP-Link, MS Office)	✓	✓
German security policy IT-Grundschutz	✓	✓
Products intended for enterprises (e.g. MS Exchange, Palo Alto, Cisco, IoT/OT)	✗	✓
CIS compliance policies*	✗	✓
Additional compliance policies**	✗	✓
Access to Greenbone Enterprise support	✗	✓
Access to expert services	✗	✓
*Contains 23 policies. **Contains 5 policies (BSI TR-02102-4, BSI TR-03116, MS Win Registry Check, SiSyPHuS Win10, Win 10 ver 1809 Security Hardening). The data were obtained from a GEA installation and from the official website. [8]		

In addition to the NVTs already mentioned, there are also compliance policies for various standards, but these are mainly Center for Internet Security (CIS) policies, of which there were 23 as of 26/3/2025. Although these are American standards, they are also used and recognized in other parts of the world, because security requirements are almost identical everywhere apart from minor legislative differences. As regards the additional compliance policies, here we can find the German Bundesamt für Sicherheit in der Informationstechnik (BSI) policies, which are very thorough and also serve as a basis for the creation of other standards such as CIS. There are also compliance policies for the Windows 10 OS. These policies can also be very valuable, especially for enterprises that for various reasons must be compliant or want to maintain cybersecurity at a high level. Apart from, simply put, the additional functionality, the price of the Enterprise Feed also includes technical support for GEA products, with the exception of the newest product in the portfolio, called Greenbone BASIC, where the Enterprise Feed includes everything except technical support.

Apart from the difference in Feed updates, in the case of GEA, including Greenbone BASIC, and also with Greenbone Free, the version of Greenbone OS (GOS) may also be worth considering. The currently available versions and their product support can be seen in the clear table Tab. 5 below.

Tab. 5 - GOS versions

OS version	GEA, Greenbone BASIC	Greenbone Free
GOS 22.04	✓	✓
GOS 24.10	✓	✗

As we could see, the latest version is currently not available only in the case of the free product Greenbone Free; however, according to information on the official Greenbone website, it will also be available in this free version in the future. Since the End of Life (EOL) of GOS version 22.04 will occur on 1/2/2026, the Greenbone Free product will presumably receive the new version GOS 24.10 by this date at the latest.
For a comprehensive overview, we present an analysis of the difference in functionality between these two versions. To begin with, it should be said that additional functionality was added in version 24.10. We will not deal with the fact that individual components and system packages were updated and will list only the essential changes:

1. **Added support for the Exploit Prediction Scoring System (EPSS)**

EPSS provides an additional score for the vulnerabilities found, besides the already well-known CVSS, for even more effective prioritization. This score is based on the probability of the vulnerability being exploited in the real world within the next 30 days, based on various data. EPSS was developed by the FIRST organization and is free of charge. Greenbone only implemented it in its solution.

2. **New look of the web interface**

The main menu has been moved from the top vertically to the left side of the screen, which improves orientation, and in addition the colour scheme has been changed. Thanks to this new look, the entire web interface appears more modern and more user-friendly.

3. **Added support for CVSS v4.0**
4. **Added configurable report formats**

The formats make it possible to customize reports, for example in CSV format, where the columns included in the output can be changed, which makes the report clearer.

5. **Notus Scanner was replaced by openvasd**

To increase the speed of performing LSC during vulnerability scanning.

6. **Added support for Secure Boot**
7. **Added the option to configure SSH security parameters**
8. **Improved Feed update speed**

1.2. Deployment options

Depending on whether we have decided to use the free Greenbone Community Edition or the paid GEA, different deployment options are available to us.

1.2.1. Greenbone Community Edition:

1. **Compilation from source code**

This is the most complex deployment method, which requires advanced technical knowledge, such as knowledge of compiling complex source code in the C programming language, knowledge of CMake and make, and advanced knowledge of the Linux OS, its file structure and scripting.

2. **Docker**

Somewhat simpler than the first option, but still a fairly complex deployment method, mainly from the point of view of maintainability. Advanced knowledge of Docker, Docker Compose and the Linux OS is required.

3. **Installation from the Kali Linux repository**

This option requires advanced knowledge of the Linux OS in order to resolve the frequent problems with this deployment option. A disadvantage is that the Kali Linux repositories do not contain the current version of this tool, and it is always a somewhat older version, because this package is maintained not by Greenbone but by Offensive Security, which maintains the Kali Linux OS. Moreover, the tool is preinstalled and supported in one version of Kali Linux, but not in the next, and then again it is, so this is not a continuously supported type of deployment. If we only want to use the GVM tool for scanning, this is not a suitable solution, because it includes many additional tools, including the operating system's GUI, which consume unnecessary additional hardware resources. In addition, these additional tools are perceived as a potentially high security risk in the event of such a machine being compromised, assuming it were running continuously. A potential attacker would have things considerably easier, since they would not have to work out how to get these attack tools into the local network through the security solutions. Such a deployment is suitable only for occasional manual use for testing purposes.

4. **Community repositories for Linux**

There are also many community repositories with this tool, such as the one from Mohammad Razavi [10], which simply need to be added to a package manager such as APT, allowing us to install it more easily. However, nobody checks these repositories and their security is highly questionable, not only because a potential threat actor could deliberately create a repository in which malicious code is bundled with the tool, but also because of non-compliance with security best practices and the use of older SW versions when creating such a package, or rather installer, for this tool. At the same time, as in the case of the Kali Linux distribution, there is also the problem of how up to date the version of this tool is. In the Kali Linux distribution the Greenbone version is still usable, but in community repositories it is often rather historical. On the basis of this, I conclude that this variant is not suitable for use for any purpose, because it may cause more security risks than it eliminates.

5. **Pre-built VM**

Although this is a little-known deployment method, it is probably the most elegant officially supported way of deploying this tool. The pre-built VM called Greenbone Free is similar to the paid GEA solution. It is in fact its TRIAL version with limited functionality and the Community Feed. This method eliminates almost all the shortcomings of the previous deployment options, and knowledge of VM configuration, or rather of the hypervisor, such as VMware, is sufficient for successful deployment.

1.2.2. Greenbone Enterprise Appliance:

1. **Hardware appliance**

These hardware appliances contain the preinstalled GEA tool and provide a high level of security and performance. However, the high performance is not entirely due to extra-optimized hardware, but rather to Greenbone's business policy, since in a VM deployment it limits the usable hardware performance for scanning. This deployment does not require technical knowledge of hypervisor configuration, which may be practical for organizations with limited IT resources or if we do not want to look after hardware but still want an on-premise solution. The price also includes free replacement of the hardware in the event of a fault.

2. **Pre-built VM**

As in the case of Greenbone Free (for the Community Edition), GEA also offers a pre-built VM, which provides a simple and secure deployment option. The pre-built VM enables rapid deployment without the need for advanced technical knowledge, because all the necessary configurations are already part of the VM image. As with Greenbone Free, knowledge of VM configuration, or rather of the hypervisor, is sufficient. This option is suitable if we want to use our own hardware.

3. **SaaS (Cloud)**

This is the same GEA tool, but available as a service in the cloud. Deployment via SaaS eliminates the requirements for local installation and maintenance, which may be practical especially for organizations with limited IT resources. At the same time, it enables easy access to the tool from different locations, while updates of both the Feed and the software itself are fully handled by Greenbone. However, this option requires trust in the provider. This solution is, however, fully GDPR-compliant and operated in Germany, which guarantees compliance with data protection. For scanning non-public networks, it is possible to download a gateway and install it where scanning is needed. This is functionality similar to the master-sensor in Greenbone's on-premise products. The licensing model is based on the number of reserved IP addresses intended for scanning, which determines the final price. For scanning more than 250 IP addresses, an individual price offer can be agreed after contacting the sales team.

Architecture and technical requirements

Naturally, in this section too, as in the previous ones, it depends on whether we have chosen Greenbone Community Edition (GCE) or GEA. We discuss these two options in more detail because they were selected as two potential solutions for deployment at KIS FRI UNIZA. The official documentation for both products, i.e. for both GEA and GCE, was used as the source of information for this section, since each product has its own documentation.

1.2.3. Greenbone Community Edition

The **architecture** of this product consists of the following main parts:

1. **Scanning applications** (Notus Scanner and OpenVAS Scanner) perform vulnerability tests (VTs) on target systems.
   - **OpenVAS Scanner** is the main scanner, which uses regularly updated databases (Greenbone Community Feed or the paid Greenbone Enterprise Feed) for detailed vulnerability scanning. This scanner is controlled by another component via the Open Scanner Protocol (OSP).
   - **Notus Scanner** is a supplementary scanner that optimizes performance and reduces system resource consumption by comparing the list of installed software with known vulnerable versions. It thereby eliminates the need to run individual so-called NASL-based local security checks (LSC) and performs this comparison all at once.

2. **Greenbone Vulnerability Management Daemon** (gvmd): This is the central element that turns ordinary vulnerability scanning into a comprehensive vulnerability management solution. The daemon communicates with the OpenVAS Scanner component via OSP. It also manages the PostgreSQL database for configurations and scan results. It likewise manages users, groups, their roles and permissions within the tool. It also manages scheduled tasks such as regular scans. This component can be operated using the Greenbone Management Protocol (GMP) API, which is based on XML.
3.
3. **Greenbone Security Assistant** (GSA): This is a web interface that allows the user to easily control scanning and access results without having to use the API. Communication between this component and gvmd is handled via the **Greenbone Security Assistant Daemon** (gsad) component and the GMP protocol.

The architecture itself can be seen in the figure. It is also important to note that the only exception in this case is Greenbone Free, which uses the GEA architecture described on the following page.

Minimum technical requirements:

- CPU/vCPU cores: 2
- RAM: 4 GB
- HDD: 20 GB

Recommended technical requirements:

- CPU/vCPU cores: 4
- RAM: 8 GB
- HDD: 60 GB

When the minimum technical requirements are met, in practice this means that we will be able to run the tool successfully and scan approximately 1 device at a time at a reasonable speed, taking into account that we do not want to wait excessively long (several hours) for the scan result. However, if we do not mind waiting longer (several hours) for the scan result, or we want to use this tool only for home use with a small number of devices and do not have more powerful hardware available, it is an excellent choice. If, however, we wish to use this solution with a larger number of scanned devices or IP addresses (roughly above 20), it is more appropriate, mainly because of scanning speed, to choose at least the recommended technical requirements. As the number of scanned IPs grows, the hardware demands therefore also increase, and the best way to get an idea of what performance is suitable for our particular deployment is the official Greenbone documentation for GEA.

1.2.4. Greenbone Enterprise Appliance

The **architecture** of this product is built on the Greenbone Operating System (GOS), which is in fact a modified version of the Debian Linux distribution, providing simple and efficient control through a user-friendly menu based on a text-based user interface (TUI), which can be seen in the figure

GOS allows all services to be configured, started and stopped. Access to the system level is restricted and requires console access (serial, hypervisor, monitor/keyboard) or SSH. GEA also includes support for a master-sensor model, in which the master server communicates with the sensors via encrypted authentication over SSH. Control of the sensor, for example starting a scan and retrieving results, takes place via the Open Scanner Protocol (OSP) API, and all this communication is wrapped in an encrypted SSH tunnel. Just as the Feed is updated on the master unit, this Feed must also be updated on the sensor, which downloads the data directly from the master unit using rsync, and all this communication is likewise wrapped in an encrypted SSH tunnel.

In addition, GEA of course also contains the same components as GCE, the only difference being that this product has a few extra things. For the most part, this is not particularly revolutionary functionality; however, in this paid version it comes pre-installed and pre-configured without unnecessary effort or the need for technical knowledge. Apart from DNS, SSH and DHCP, which are also built into the free version, depending of course on the chosen distribution, all the others are available only in the paid version, and communication takes place on the following ports. Here we can see, for example, integration with Cisco FirePower or Verinice.PRO, as well as e-mail for delivering alerts and scan results, and much more.

The GEA architecture, which is very similar to that of GCE, but with the addition of GOS (on the right), which contains GOS Administration and the GOS Control Layer, which considerably simplify the administration and use of the entire tool. Another addition is the MQTT Broker, which, according to the GCE architecture figure in the documentation, is not part of GCE. However, the reason for its exclusion from GCE is not clear, but it is most likely just a matter of outdated documentation and it is in fact present in both products alike, as is also evidenced by the existence of an MQTT Broker container for the Community Edition on DockerHub. For our purposes, however, such deep details of the internal components are not that important. Priority is given above all to the API (GMP), the web interface and GOS Administration, since these components serve as the main points of communication with the system.

Minimum technical requirements for the VM:

- vCPU cores: 2
- RAM: 12 GB
- HDD: 500 GB

The technical requirements differ depending on which licence or product version we specifically purchase. An overview of these requirements for all GEA products can be found in a clear table in a PDF on the official Greenbone website . The number of IPs that this tool can scan in one day naturally also depends on performance, and this estimate is likewise included in the aforementioned document.
Features, the company's licensing model is thus based on limiting the performance usable for the vulnerability scanning itself. In practice, this means that even if we allocated the VM more performance than is stated in the table for the relevant licence or version, it would not actually use it during scanning.

Advantages and disadvantages

Advantages:

- **Free version with regular updates:** GVM offers a free version with regular updates of vulnerability tests, which is advantageous for smaller organizations with a limited budget.
- **Open-source solution:** The possibility of flexibly extending functionality and verifying security directly in the source code.
- **On-premise deployment:** Ensures better control over security processes and data.
- **No need for agents:** Simplifies deployment and reduces the administration demands on scanned devices.
- **Compliance with standards:** Meets the requirements of the GDPR and other standards, which increases the trustworthiness and security of the solution.

Disadvantages:

- **Limited functionality of the free version:** The free version has a limited range of vulnerability tests and requires more effort for maintenance and operation.
- **Performance limitations:** Virtual solutions do not achieve the same performance as hardware solutions, which may be limiting for larger deployments.
- **Deployment complexity:** Some deployment options, such as compiling from source code or using Docker, require advanced technical knowledge.
- **Licensing model:** Limits usable performance and functionality based on the purchased licence, which may be disadvantageous for organizations with higher requirements.

1.3. Summary

Based on the analysis of the GVM tool, we can conclude that it is a robust and flexible vulnerability scanning solution that is suitable for a variety of enterprise environments. Its main advantages are the free version with regular updates, its open-source nature and the possibility of on-premise deployment. On the other hand, the limited functionality of the free version and the performance limitations of the VM may pose challenges for some larger organizations. Overall, however, GVM offers a reliable and secure vulnerability management solution that can significantly contribute to improving the level of cybersecurity.

LIST OF SOURCES

1. **Check Point Software Technologies Ltd..** *Check Point Software's 2025 Security Report Finds Alarming 44% Increase in Cyber-Attacks Amid Maturing Cyber Threat Ecosystem.* [online]. 17/2/2025 Available at: < https://www.checkpoint.com/press-releases/check-point-softwares-2025-security-report-finds-alarming-44-increase-in-cyber-attacks-amid-maturing-cyber-threat-ecosystem/>
2. **Tlačová agentúra Slovenskej republiky.** *SIS Won't Comment on Cyber-attack on Land-Registry Office, It's Live Case.* [online]. 17/2/2025. Available at: < https://www.tasr.sk/tasr-clanok/TASR:2025011000000195>
3. **Tlačová agentúra Slovenskej republiky.** *M.Chren: Ani po mnohých dňoch nefunguje kataster naplno,odráža sa to na službách.* [online]. 17/2/2025. Available at: <https://www.tasr.sk/tasr-clanok/TASR:2025020600000155>
4. **Národný bezpečnostný úrad.** *Varovanie pred zvýšeným rizikom kybernetických bezpečnostných útokov.* [online]. 17/2/2025. Available at: <https://www.nbu.gov.sk/28493-sk/varovanie-pred-zvysenym-rizikom-kybernetickych-bezpecnostnych-utokov/>
5. **Greenbone AG,** *Greenbone, GVM, OpenVAS and How They Are Connected.* [online]. 3/4/2025. Available at: <https://greenbone.github.io/docs/latest/background.html#greenbone-gvm-openvas-and-how-they-are-connected>
6. **Greenbone AG,** *Product Comparison.* [online]. 3/4/2025. Available at: <https://www.greenbone.net/en/product-comparison/>
7. **Greenbone AG,** *Product Overview of the Different Solutions.* [online]. 3/4/2025. Available at: <https://www.greenbone.net/wp-content/uploads/solution_overview_en.pdf >
8. **Greenbone AG,** *Feed Comparison.* [online]. 3/4/2025. Available at: <https://www.greenbone.net/en/feed-comparison/>
9. **Greenbone AG,** *SecInfo Portal.* [online]. 5/4/2025. Available at: <https://www.greenbone.net/en/secinfo-portal/>
10. **Mohammad Razavi,** *Greenbone Vulnerability Management.* [online]. 5/4/2025. Available at: <https://launchpad.net/~mrazavi/+archive/ubuntu/gvm>
11. **Greenbone AG,** *18 Architecture.* [online]. 5/4/2025. Available at: <https://docs.greenbone.net/GSM-Manual/gos-22.04/en/architecture.html>
12. **Greenbone AG,** *Architecture.* [online]. 5/4/2025. Available at: <https://greenbone.github.io/docs/latest/architecture.html>
13. **greenbone,** *greenbone/mqtt-broker.* [online]. 5/4/2025. Available at: <https://hub.docker.com/r/greenbone/mqtt-broker>
14. **Greenbone AG,** *Roadmap & Lifecycle.* [online]. 6/4/2025. Available at: <https://www.greenbone.net/en/roadmap-lifecycle/>
15. **Greenbone AG,** *4 Setting up the Greenbone Enterprise Appliance.* [online]. 6/4/2025. Available at: <https://docs.greenbone.net/GSM-Manual/gos-22.04/en/setting-up-the-appliance.html#setup-requirements>
16. **U.S. Department of Homeland Security,** *Use Strong Passwords.* [online]. 8/4/2025. Available at: <https://www.cisa.gov/secure-our-world/use-strong-passwords>
17. **Greenbone AG,** *Greenbone Free.* [online]. 8/4/2025. Available at: <https://www.greenbone.net/en/greenbone-free/#toggle-id-4>

18. **Greenbone AG,** *10 Reports and Vulnerability Management.* [online]. 8/4/2025. Available at: <https://docs.greenbone.net/GSM-Manual/gos-24.10/en/reports.html>
19. **Greenbone AG,** *11 Performing Compliance Scans and Special Scans.* [online]. 8/4/2025. Available at: <https://docs.greenbone.net/GSM-Manual/gos-24.10/en/compliance-and-special-scans.html>
20. **Greenbone AG,** *8.5 Using a Central User Management.* [online]. 8/4/2025. Available at: <https://docs.greenbone.net/GSM-Manual/gos-24.10/en/web-interface-access.html#using-a-central-user-management>
21. **Greenbone AG,** *9 Scanning a System.* [online]. 9/4/2025. Available at: <https://docs.greenbone.net/GSM-Manual/gos-24.10/en/scanning.html>
22. **Community,** *GVM Example Scripts.* [online]. 9/4/2025. Available at: <https://github.com/greenbone/gvm-tools/blob/main/scripts/README.md>
23. **Greenbone AG,** *14 Using the Greenbone Management Protocol.* [online]. 9/4/2025. Available at: <https://docs.greenbone.net/GSM-Manual/gos-24.10/en/gmp.html>