



**UNIVERSITY
OF TRENTO**

Vulnerability Assessment OpenVAS

Lab 5 Report
Network Security Course 2020/21

Eros Zaupa
211455

Julien Sabot
225482

Riccardo Scilla
213723

May 25, 2021

Contents

1	Vulnerability assessment	2
1.1	How?	3
1.1.1	Conduct Risk Identification And Analysis	3
1.1.2	Develop Vulnerability Scanning Policies	3
1.1.3	Identify The Type Of Scans	3
1.1.4	Configure The Scan	3
1.1.5	Perform The Scan	4
1.1.6	Evaluate And Consider Possible Risks	4
1.1.7	Interpret The Scan Results	4
1.1.8	Create A Remediation & Mitigation Plan	4
2	GVM Architecture	5
2.1	Greenbone Vulnerability Manager Daemon (gvmd)	5
2.2	Greenbone Security Assistant (GSA)	5
2.3	OpenVAS Scanner	5
2.4	Greenbone Community Feed (GCF)	6
2.4.1	NVTs (Network Vulnerability Tests)	6
2.4.2	SCAP (Security Content Automation Protocol)	6
2.4.3	CERT (Computer Emergency Response Team)	7
3	First steps	7
4	Web Interface	9
4.1	Administration Tab	9
4.2	Configuration Tab	9
4.2.1	Create a new Target	10
4.2.2	Default Scan Configs	10
4.3	SecInfo Tab	10
4.4	Scans Tab	11
4.4.1	Create a new Task	11
5	Advanced Scans	11
5.1	Custom Scans Configuration	11
6	Scan analysis	12
6.1	Dashboard	12
6.2	Global architecture	13
6.3	Full And Fast scan analysis	13
6.4	Detection Scan result analysis	14
6.5	Additional features	15
6.5.1	Filtering	15
6.5.2	Exploitation	15
7	Second Custom Exercise	16
7.1	Instructions	16
7.2	Practice	16
7.3	Results	17
8	Alternatives	18
8.1	Business Models	18
8.2	Performance and Speciality	18

1 Vulnerability assessment¹

No business wants to expose itself to **unnecessary risks** (or be the headline story for the latest cyber attack): from [Ponemon Institute survey](#), in 2019

- 60% of breaches involved **unpatched vulnerabilities**
- 62% of the organizations were **unaware** they were vulnerable prior to the data breach
- 52% of the organizations say they are at a disadvantage in responding to vulnerabilities because they use **manual processes**

One way to mitigate risks is by performing **routine** network vulnerability assessments.

Network vulnerability assessment Process of identifying security vulnerabilities in systems, quantifying and analyzing them, and remediating those vulnerabilities based on predefined risks

Assessments Essential part of a holistic security program, cited by many industry standards and compliance regulations

Security experts Can

- Conduct **vulnerability analysis** of the network scans to prioritize threats identified
- Create an **action plan** with steps to remediate vulnerabilities (e.g. maintain up to date patches)

System hardening Identify possible vectors of attack and close them down (e.g. close down unnecessary ports/services)

Compliance Becoming compliant to regulations (HIPAA, PCI DSS, GDPR, ISO 27001, SOX, FISMA, GLBA, and many others) is impossible without an assessment

Maintain strong security Routine vulnerability assessments allow identification and mitigation of attacks

Frequency Depends on compliance, changes in infrastructure and business needs

Costs Between \$2,000 \$4,000 per report, costs vary depending on

- Network complexity
- Goals of the assessment

You should also notice how vulnerability assessment and penetration testing have different goals

Vulnerability scanning Identifies known vulnerabilities, lack of security controls, common misconfigurations within systems.

Penetration testing Simulates an attack to exploit weaknesses in order to prove the effectiveness of your network's security. While vulnerability scanning is used for both defensive and offensive cybersecurity strategies, penetration testing is offensive in nature

¹Strahinja Stankovic. "How To Perform A Successful Network Security Vulnerability Assessment". In: *PurpleSec* (2020). URL: <https://purplesec.us/perform-successful-network-vulnerability-assessment/#respond>.

1.1 How?

1.1.1 Conduct Risk Identification And Analysis

Identifying risks for each asset and possible threats they face is a complex task that requires to

1. Redact a **centralized document** with all the assets that are a part of an information system in the company.
2. Assign **risks** to assets by determining the impact and likelihood of each threat materializing. This allows to **focus** on prioritizing assets that have the highest risk assigned and those most critically affected by known weaknesses or vulnerabilities.

1.1.2 Develop Vulnerability Scanning Policies

In order to have a structured and successful scanning methodology. A document with **policies** and **procedures** should be redacted to set a pre-determined course of actions needed to be taken with all aspects of vulnerability scanning. Such a document should be duty of an **official owner**, that is responsible for everything that is written inside, and approved by **upper management** before taking effect.

1.1.3 Identify The Type Of Scans

Depending on the software that is running on the system you need to scan and secure, you need to determine the type of scan to be performed in order to get the most benefit. Vulnerability scanning can be performed by network administrators, information security analysts and all technical IT staff that are trained and assigned the function of conducting a vulnerability scan. Types of scans may include

Network Vulnerability Scans The most common type of vulnerability scan is a network based scan. This scan includes networks, their communication channels and the networking equipment used in an environment. Some of the major software and hardware devices that are in the scope of a network scan are hubs, switches, routers, firewalls, clusters, and servers. A network scan will detect and classify all vulnerabilities that it finds on these devices.

Host Based Vulnerability Scans Host-based scans address vulnerabilities related to hosts on the network including computers, laptops and servers. More specifically, this scan investigates the host configuration, its user directories, file systems, memory settings and other information that can be found on a host. This scan focuses more on the endpoints and their internal system setup and functionality.

Wireless Based Vulnerability Scans A successful wireless vulnerability requires to know all the wireless devices that are in your network and to map out the attributes for each device in order to know how to properly configure the scan.

Application Based Vulnerability Scans This type of vulnerability scan is often forgotten and is in the shadows of an application penetration test. Nevertheless, if you are not conducting an application penetration test, scanning your applications for vulnerabilities should be very high on your priority list. By choosing from a variety of application vulnerability scanning tools, you can automate your security tasks and increase the security of your applications

1.1.4 Configure The Scan

Even with many vulnerability scanning vendors to choose from, the configuration of any scan can still be addressed by identifying general objectives and the type of system you want to scan. A general vulnerability scan should include

Listing target IPs The IP addresses where the target systems are hosted need to be inputted into the vulnerability scanning software in order for a scan to be performed.

Defining Port Range And Protocols After adding the target IPs it is important to specify the port range you want to scan and which protocol you wish to use in the process.

Defining The Targets In this step, you need to specify if your target IPs are databases, windows servers, applications, wireless devices etc. By making your scan more specific, you will get more accurate results.

Setting Up The Aggressiveness Of The Scan, Time And Notifications Defining how aggressive your scan will be can influence the performance of the devices you are going to scan. To avoid any downtime on the target systems, it is recommended to set up a scan to be executed at a certain time, usually non-business hours.

1.1.5 Perform The Scan

Depending on the size of the target set and the intrusiveness of the scan, it can take minutes to hours for it to complete. The scanning tool will execute a vulnerability scan by following three phases

Scanning Fingerprint the specified targets to gather basic information about them.

Enumerate The targets and gather more detailed specifications such as ports and services that are up and running

Vulnerability detection Map out vulnerabilities in the targets, if any are present.

1.1.6 Evaluate And Consider Possible Risks

When performing a scan on critical systems and production systems, extra caution should be exercised, and the scan should be performed after hours when the traffic to the target is minimal, in order to avoid overload: if the links and connections cannot handle the traffic load generated by the scan, the remote target can shut down and become unavailable.

1.1.7 Interpret The Scan Results

While each vulnerability scanning tool will prioritize vulnerabilities automatically, certain types of vulnerabilities should be given a priority and knowledge of the scanned system is also important in order to properly prioritize remediation efforts.

1.1.8 Create A Remediation & Mitigation Plan

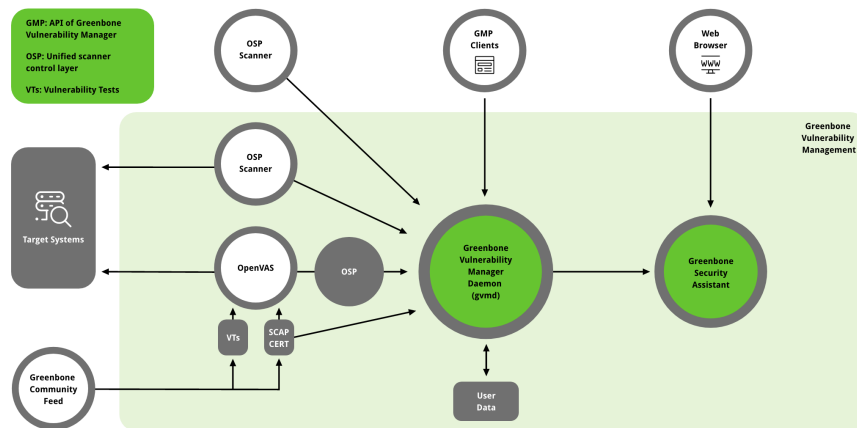
Information security staff should prioritize the mitigation of each vulnerability. The Information security staff and IT staff need to communicate and work closely together in the vulnerability mitigation phase to formulate a resolution process. Numerous follow-up scans are usually performed during the back and forth problem-solving between teams until all vulnerabilities that need to be mitigated no longer appear in the reports.

2 GVM Architecture²³⁴

OpenVAS is a component of a more general framework: the Greenbone Vulnerability Management (GVM). The GVM was originally built as a community project named “OpenVAS” and is primarily developed and forwarded by Greenbone Networks.

It consists of three main parts: Greenbone Vulnerability Manager Daemon (gvmd), the Greenbone Security Assistant (GSA) and the OpenVAS Scanner that runs vulnerability tests (VT) against some target systems.

Here is an architecture overview for GVM-20.08 and GVM-21.04.



2.1 Greenbone Vulnerability Manager Daemon (gvmd)

The Greenbone Vulnerability Manager Daemon (gvmd) represent the central management service between the security scanners and the user clients.

It controls the scanner OpenVAS using the internal protocol called Open Scanner Protocol (OSP), which also supports the integration with other scanners. The gvmd uses the Greenbone Management Protocol (GMP) to access the data, control commands and the workflow; it also controls an SQL database (PostgreSQL) where all configuration and scan result data is centrally stored. Furthermore, gvmd handles user management including permissions control with groups and roles.

2.2 Greenbone Security Assistant (GSA)

The Greenbone Security Assistant (GSA) is the web interface of GVM that a user controls scans and accesses vulnerability information with. It the main contact point for a user with GVM.

It connects to gvmd via the web server Greenbone Security Assistant Daemon (gsad) to provide a full-featured web application for vulnerability management.

2.3 OpenVAS Scanner

The main scanner OpenVAS Scanner is a full-featured scan engine that executes vulnerability tests (VTs) against target systems.

²³Architecture. URL: <https://docs.greenbone.net/GSM-Manual/gos-20.08/en/architecture.html>.

³Kristin Schlosser. *About GVM 20.08 and 21.04 Architecture*. 2021. URL: <https://community.greenbone.net/t/about-gvm-20-08-and-21-04-architecture/8449>.

⁴Vulnerability Assessment – GCE/GSM. URL: <https://www.anthesia.net/2020/05/14/vulnerability-assessment-gce-gsm/>.

The OpenVAS Scanner is controlled via OSP. The OSP Daemon for the OpenVAS Scanner (osspd-openvas) communicates with gvm via OSP: VT data is collected, scans are started and stopped, and scan results are transferred to gvm via ospd.

To collect the data, the scanner uses some daily updated and comprehensive feeds. There are two feeds:

1. commercial Greenbone Security Feed (GSF)
2. free available Greenbone Community Feed (GCF)

2.4 Greenbone Community Feed (GCF)

In this lab, the Community Feed is used. Greenbone internally maintains a public feed of Network Vulnerability Tests (NVTs) for OpenVAS: it contains more than 60,000 NVTs, growing on a permanent basis. There are two other feeds used by the Scanner:

- the “Greenbone [Community] SCAP Feed”
- the “Greenbone [Community] CERT Feed”

These ones contain information published by third-party organizations or vendors, and are only updated by Greenbone if new information is available.

2.4.1 NVTs (Network Vulnerability Tests)

NVTs are test routines used by the GVM. For each one, the information provided are:

Name	Name of the VT
Family	Family to which the VT belongs
Created	Date and time of creation
Modified	Date and time of last modification
CVE	CVE that is checked for using the VT
Solution Type	Solution for the vulnerability
Severity	The severity of the vulnerability expressed by the CVSS
QoD	Quality of Detection that represents how reliable the detection of the vulnerability is

2.4.2 SCAP (Security Content Automation Protocol)

The National Institute of Standards and Technology (NIST) provides the National Vulnerability Database (NVD), which is a data repository for the vulnerability management of the US government. The NVD utilizes the Security Content Automation Protocol (SCAP): SCAP is a combination of different interoperable standards.

The Greenbone Security Manager (GSM) uses OVAL, CVE, CPE and CVSS. By utilizing these standards the interoperability with other systems is guaranteed. The standards also allow comparing the results.

CVE Common Vulnerabilities and Exposure (CVE) project found by MITRE.

At each vulnerability is assigned a unique identifier consisting of the release year and a simple number.

CPE Common Platform Enumeration (CPE) is a structured naming scheme for applications, operating systems and hardware devices initiated by MITRE and is maintained by NIST as a part of the NVD. A CPE name is a URI with the syntax:

`cpe:/part:vendor:product:version:update:edition:language`

OVAL Open Vulnerability and Assessment Language (OVAL) is a language to describe vulnerabilities, configuration settings (compliance), patches and applications (inventory). The XML based definitions allow simple processing by automated systems and describe the discovery of individual systems and vulnerabilities.

CVSS Common Vulnerability Scoring System (CVSS) allows a shared system of metrics to analyze and measure vulnerabilities.

2.4.3 CERT (Computer Emergency Response Team)

CERT stands for Computer Emergency Response Team, but can be also intended as “Computer Emergency Readiness Team” to underline the idea of risk prevention.

There are two different CERT:

CERT-Bund Advisories Information service only available to federal agencies. These advisories describe current information about security critical incidents in computer systems and present detailed measures to remediate security risks.

DFN-CERT Advisories It is a service that includes the categorization, distribution and rating of advisories issued by different software vendors and distributors.

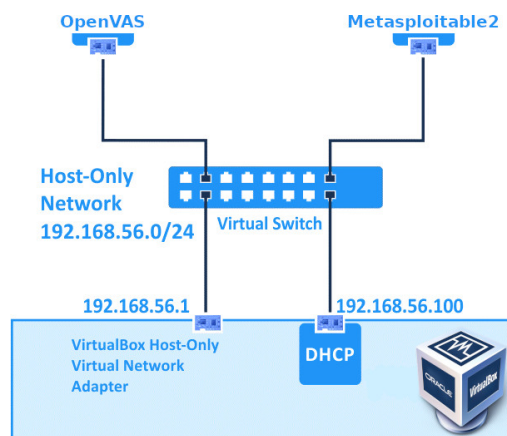
3 First steps

Before using the VMs be sure to have them connected through a host-only network: we don't want to expose our VMs to the network, especially the vulnerable target. To setup a Host-only Adapter

- Go to File > Host Network Manager...
- Click on Create, take note of the name of the adapter (e.g. vboxnet0)
- Click on Properties > DHCP Server > Enable Server
- Click Apply and close the window

To connect a VM select it and go to Settings > Network. On the tab Adapter 1 set Attached to: Host-only Adapter and set the right adapter (e.g. vboxnet0). Start the virtual machine.

The network topology should look like this:



We have the following environment setup

- OpenVAS virtual machine

Greenbone Administration panel admin:admin

Greenbone Web panel admin:admin

- Metasploitable2 virtual machine

Metasploitable2 panel msfadmin:msfadmin

- The two VMs are connected to a host-only network (see more in the section Network setup)

First of all, we need to check what is the actual IP address assigned by the DHCP server, in our case

OpenVAS (e.g. 192.168.56.102) The IP address is prompted in the console when the machine is started

Metasploitable2 (e.g. 192.168.56.103) Login and use `ifconfig` to find out the IP address

From now on we are going to interact only through the Greenbone Web panel: connect to it through a web browser and login with the credentials admin:admin.

The first thing we can do is scheduling a network scan to find out who is connected to the network. From the top menu, go to Scans > Tasks and move the cursor to the magic wand icon, select Advanced Task Wizard.

Input the following settings and then click on Create

Task name Network discovery

Scan Config Discovery

Target Host(s) The IP address of the host-only subnet created in VirtualBox (e.g. 192.168.56.0/24)

Start Time Start immediately

We repeat the same process to create another task, this time with the following settings

Task name Target scan

Scan Config Full and fast

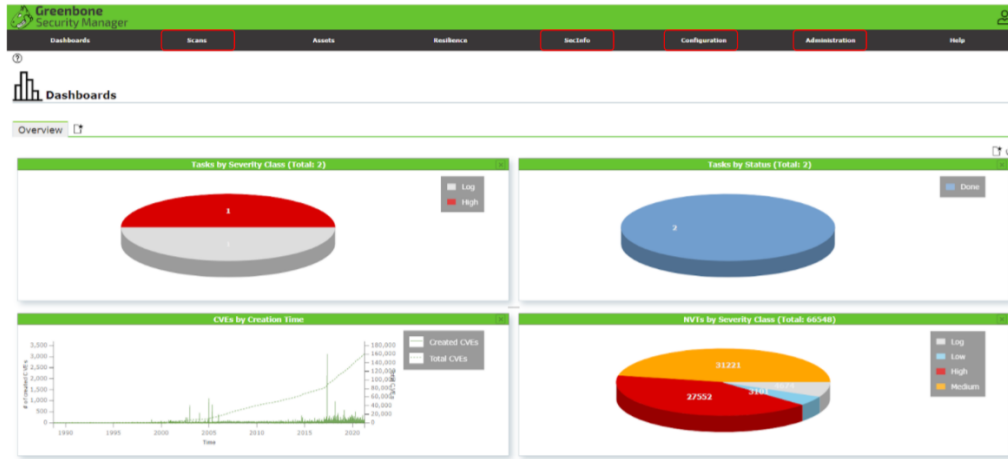
Target Host(s) The IP address of the Metasploitable2 VM (e.g. 192.168.56.4)

Start Time Start immediately

The two scans will take few minutes to complete.

4 Web Interface

Once we log in we find the Dashboard Tab: here we can find information regarding the tasks previously ran and their status, together with some NVTs information.



4.1 Administration Tab

In the Administration Tab we can manage Users, Groups, Roles and Permissions. We can also have a look at the Feed Status: here the information regarding the feed explained before are displayed. In this case the Status is not updated because of the host-only configuration.

Feed Status				
Type	Content	Origin	Version	Status
NVT	NVTs	Greenbone Community Feed	20210414T1028	29 days old
SCAP	CVEs CPEs OVAL Definitions	Greenbone Community SCAP Feed	20210414T0130	Too old (30 days) Please check the automatic synchronization of your system.
CERT	CERT-Bund Advisories DFN-CERT Advisories	Greenbone Community CERT Feed	20210414T0030	Too old (30 days) Please check the automatic synchronization of your system.
GVM_DATA	Compliance Policies Port Lists Report Formats Scan Configs	Greenbone Community GVMd data Feed	20210406T0959	Too old (37 days) Please check the automatic synchronization of your system.

4.2 Configuration Tab

In the Configuration Tab we can manage:

- Targets that we want to scan
- Port Lists to set specific ports to scan
- Credentials of different services
- Scan Configs to see the characteristics of the default configs or create some custom ones
- Report format that are available to download the Results
- Scanner available (OpenVAS by default) or to upload some custom ones.

Configuration
Targets
Port Lists
Credentials
Scan Configs
Report Formats
Scanners
Filters
Tags

4.2.1 Create a new Target

From the Targets section we can create a new Target. Here we can specify the name of the target, its IP (or network) the Port List to scan and the Credentials.

Additionally we can select the Alive Test: during a typical scan, the Scanner will first ping to verify the availability of the destination. If the destination does not respond to the ping request, we can assume that the destination is not active. Sometimes firewalls or other configurations could suppress this response. To solve this, we have alternative methods to verify if the destination is active or not: for example we can try with a TCP ping or a ARP ping. We can also set the Alive Test to Consider Alive to scan without performing the ping in advance.

The 'New Target' dialog box is shown with the following configuration:

- Name:** metasploitable2
- Comment:** (empty)
- Hosts:** Manual (selected), 192.168.56.101
- Exclude Hosts:** Manual (selected)
- Port List:** All IANA assigned TCP
- Alive Test:** Scan Config Default
- Credentials for authenticated checks:**
 - SSH: -- on port 22
 - SMB: --
 - ESXi: --
 - SNMP: --

4.2.2 Default Scan Configs

Base Basic configuration template with a minimum set of NVTs required for a scan.

Discovery only NVTs to get information about the target systems. We don't get vulnerabilities but we just scan for open ports, used hardware, firewalls, used services, installed software and certificates.

Host Discovery only NVTs to detect the target systems. It Ping Hosts to detect whether a host is alive and create a list of systems.

System Discovery only NVTs used to detect target systems (operating systems and hardware).

Full & Fast Based on the information gathered in the previous port scan and uses almost all NVTs. VTs are optimized in the best possible way to keep the potential false negative rate especially low. This configuration is a common choice to perform as first scan.

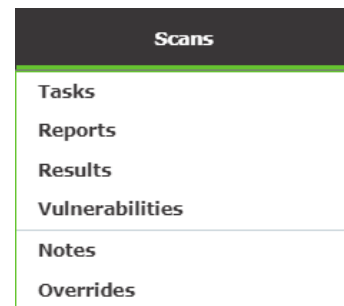
4.3 SecInfo Tab

In the SecInfo Tab are listed all the NVTs, SCAP and CERT information provided by the feeds. Regarding the NVTs, some plots are displayed such as the distribution of the NVTs by Severity, Creation Time and NVT Family.

4.4 Scans Tab

In the Scans Tab we can manage:

- Tasks present all the tasks created. We can see their status, the maximum severity value and perform some actions (start / stop / pause).
- Reports present the distribution of the vulnerabilities per severity class (high / medium / low / log)
- Results shows a list of all vulnerabilities found in the tasks with some information



4.4.1 Create a new Task

From the Task section we can create a new Task. Here we can specify the name of the task, the Target that we want to scan (created previously).

We can also set the minimum QoD (70% by default), the Scanner and the Scan Config.

5 Advanced Scans⁵

So far, we have only used the default scan configurations such as system discovery and Full & Fast. We might not want to run a scan all NVTs on a given target and only test for a few specific vulnerabilities. In this case we can create our own custom scan configuration and select only the NVTs that we want to test for. This also us to reduce the time required for a scan.

5.1 Custom Scans Configuration

We want to create a Custom Configuration with a specific NVT Family. To be sure to get good results, we have first investigate the Full & Fast scan to get what are the Families of vulnerabilities inside the metasploitable target.

Here is a list of the NVT Families:

Web Application Abuses
SMTP problems

Web Servers
Gain a shell remotely

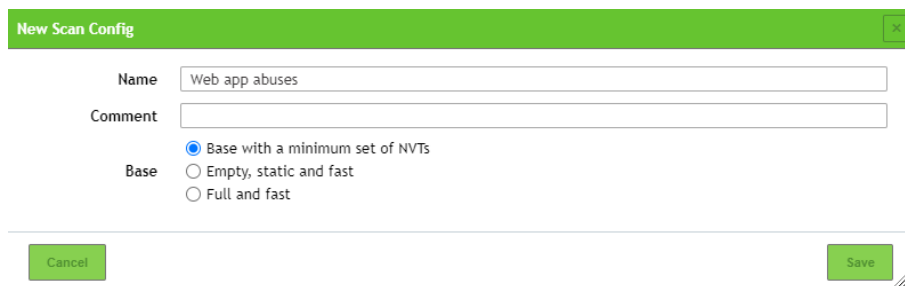
Useless services
SSL and TLS

As an exercise we will search for Web Application Abuses. Here are the different steps of our custom scan:

1. Create a New Scan Config

In the Scan Config section we can select to create a New Scan Config on the top left corner. It will pop a window that allows to select the Name of the configuration and the Base. This is the starting point of our custom configuration and because we just want to scan for a single NVT Family, we will choose the Base with a minimum set of NVTs option.

⁵Hacking Tutorials. *Vulnerability Scanning with OpenVAS 9 part 4: Custom scan configurations*. 2020. URL: <https://www.hackingtutorials.org/scanning-tutorials/openvas-9-part-4-custom-scan-configurations/>.



New Scan Config

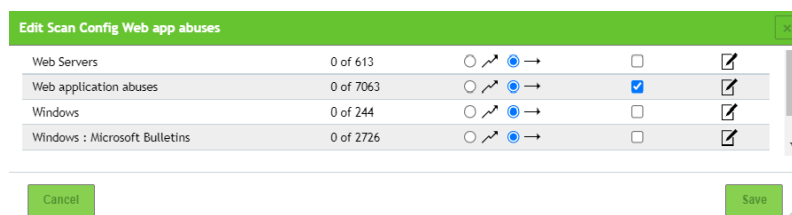
Name:

Comment:

Base: ☒ Base with a minimum set of NVTs
☐ Empty, static and fast
☐ Full and fast

2. Edit the Custom Scan Config

Now our new custom configuration is displayed in the list together with the other Default Configs. In the Action column we can go in Edit Scan Configs to edit it. Here we can select the NVT families we want scan for, in our case the Web Application Abuses.

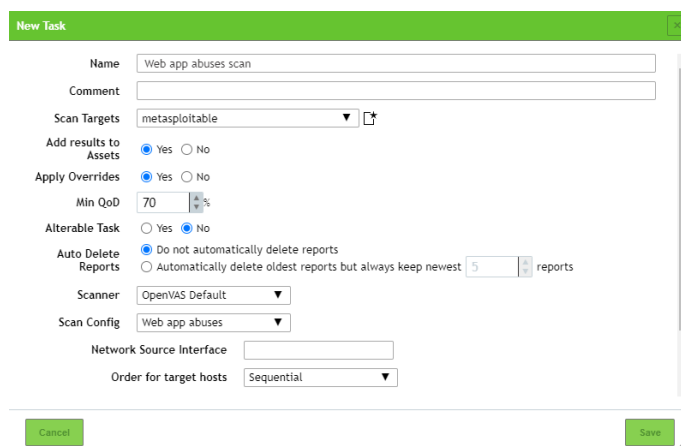


Edit Scan Config Web app abuses

Web Servers	0 of 613	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Web application abuses	0 of 7063	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Windows	0 of 244	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Windows : Microsoft Bulletins	0 of 2726	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>

3. Create a new task

In the Tasks section we can create a new Task using as Target the metasploitable machine and as Scan Config the create custom configuration.



New Task

Name:

Comment:

Scan Targets:

Add results to Assets: ☒ Yes ☐ No

Apply Overrides: ☒ Yes ☐ No

Min QoD: %

Alterable Task: ☐ Yes ☒ No

Auto Delete Reports: ☒ Do not automatically delete reports
☐ Automatically delete oldest reports but always keep newest reports

Scanner:

Scan Config:

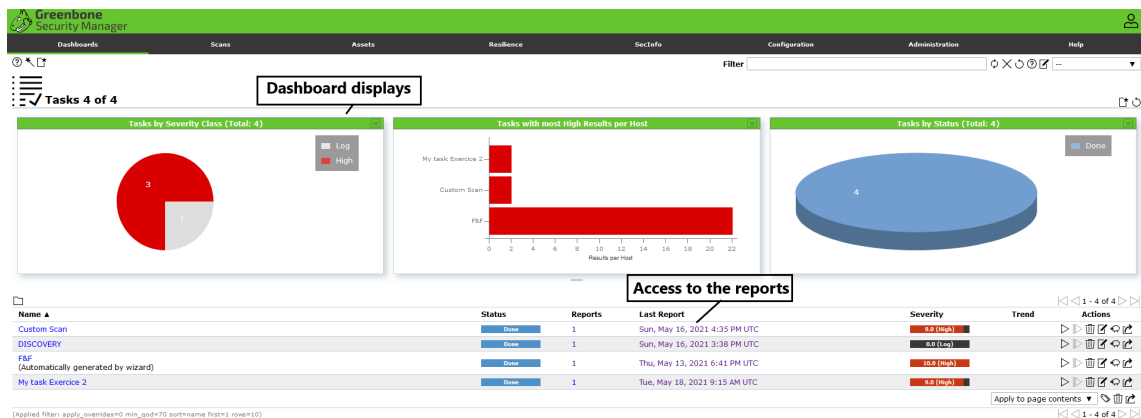
Network Source Interface:

Order for target hosts:

6 Scan analysis

6.1 Dashboard

The Dashboard displays features about the scans already performed. You can edit the type of information you want to oversee among a complete range of attributes : NVTs, status, CVSS overall score, CVEs, QoD, ...



6.2 Global architecture

After accessing the results of any scan, we will always keep the same template of report. So, whatever the type of scans performing, the different vulnerabilities detected will be shared among the same categories :

Results	Global list of detailed vulnerabilities detected by the scan
Hosts	Vulnerabilities grouped by hosts and Hosts overview
Ports	Ports and protocols of communication scanned by the scanner
Applications	Applications detected in the system
Operating Systems	overview of the OS detected by the scanner
CVEs	Vulnerabilities grouped by CVEs
TLS certificates	overview of certificates status

6.3 Full And Fast scan analysis

The full and fast scan takes about one hour to be successfully performed. After the scan has completed you will see a list of results with the default filter.

The screenshot shows a report titled 'Report: Thu, May 13, 2021 6:41 PM UTC'. It includes a table with columns: Vulnerability, Severity, QoD, Host IP, Name, Location, and Created. The table lists various vulnerabilities such as 'The nmap service is running', 'Distributed Ruby (DRuby/DRS) Multiple Remote Code Execution Vulnerabilities', 'Twiki XSS and Command Execution Vulnerabilities', 'High Privilege Login', 'OS End of Life Detection', 'Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability', 'Possible Backdoor: Ingress', 'Docker Remote Code Execution Vulnerability', 'PostgreSQL weak password', 'VNC Brute Force Login', 'MySQL / MariaDB weak password', 'Test HTTP dangerous methods', 'phpinfo() index Reporting', 'FTP Brute Force Login Reporting', 'FTP Brute Force Login Reporting', 'SSH Brute Force Login With Default Credentials Reporting', 'PHP-CSS based extens vulnerability when parsing query string parameters from php Req.', 'Apache Tomcat AJP RCE Vulnerability (Shirocat)', 'vulnCompromised Source Packages Backdoor Vulnerability', 'vulnCompromised Source Packages Backdoor Vulnerability', 'rsync Unauthenticated Chained Login', 'The nmap service is running', 'Twiki Cross-Site Request Forgery vulnerability - Sup10', and 'Multiple vendors SMARTPLS Implementation Plaintext Arbitrary Command Injection vulnerability'.



From the results section, you can access to the complete description of any vulnerability including (Severity score, title, CVEs associated, CERT, Insights, Solution Type, Host of detection, Location of detection). These key information can be sorted by any of these features just by clicking on the top of the appropriate column. The result section cannot be sufficient when you want to assess vulnerabilities among narrowed criteria.

Indeed we can firstly access privilege information by switching the template to the other sections.

We can for example perform a complete assessment of the vulnerable applications.

Information	Results (60 of 455)	Hosts (2 of 2)	Ports (18 of 23)	Applications (34 of 34)	Operating Systems (1 of 1)	CVEs (24 of 24)	Closed CVEs (0 of 0)	TLS Certificates (2 of 2)	Error Messages (0 of 0)	User Tags (0)
Application CPE										
cpe:/a:oracle:mysql:5.0.51a		1		1						
cpe:/a:postgresql:postgresql:9.3.1		1		1						
cpe:/a:samba:samba:3.0.20		1		1						
cpe:/a:apache:http_server:2.2.8		1		1						

In case you perform a scan on multiple hosts as network, you will also be able to check the vulnerable hosts of your sub network.

Information	Results (60 of 455)	Hosts (2 of 2)	Ports (18 of 23)	Applications (34 of 34)	Operating Systems (1 of 1)	CVEs (24 of 24)	Closed CVEs (0 of 0)	TLS Certificates (2 of 2)	Error Messages (0 of 0)	User Tags (0)					
IP Address											1 - 1 of 1				
IP Address	Hostname	OS	Ports	Apps	Distance	Auth	Start	End	High	Medium	Low	Log	False Positive	Total	Severity
192.168.56.101			19	14			Thu, May 13, 2021 6:43 PM UTC	Thu, May 13, 2021 7:24 PM UTC	22	36	2	0	0	60	10.0 (high)
(Applied filter: appv_overrides=0 levels=html row=100 min_ops=70 first=1 sort=reverse=severity)															
											1 - 1 of 1				

6.4 Detection Scan result analysis

Detection scans keeps the same template of result of the Full and Fast Scan. The differences are the kind of information provided by each section. Indeed during this particular scan openVAS just detect hosts, services, applications and certificates without any search of vulnerability into the sub network.

So, the vulnerabilities displayed represent the successful detections operated. Therefore we loose information about solution type and severity score.

We can see after performing the scan that it lasts about the same time as the Full and Fast scan with a bigger subset of hosts to analyse. Then the real value of the discovery scan comparing to the full and fast scan is the reduction of time.

Report:Sun, May 16, 2021 3:38 PM UTC										
ID: d6d7a4a3-6899-4101-8a67-85638085793a Created: Sun, May 16, 2021 3:38 PM UTC Modified: Sun, May 16, 2021 3:38 PM UTC Owner: admin										
Information	Results (100 of 100)	Hosts (4 of 254)	Ports (30 of 30)	Applications (17 of 17)	Operating Systems (4 of 4)	CVEs (1 of 1)	Closed CVEs (0 of 0)	TLS Certificates (3 of 3)	Error Messages (0 of 0)	User Tags (0)
Vulnerability										
HTTP Server type and version		?	80 %	192.168.56.1	DESKTOP-JUK1BE2	3357/tcp				Sun, May 16, 2021 4:05 PM UTC
HTTP Server type and version		?	80 %	192.168.56.101	METASPLOITABLE	80/tcp				Sun, May 16, 2021 5:30 PM UTC
Hidden WWW server name		?	70 %	192.168.56.1	DESKTOP-JUK1BE2	2869/tcp				Sun, May 16, 2021 4:05 PM UTC
Hostname Determination Reporting		?	80 %	192.168.56.1	DESKTOP-JUK1BE2	general/tcp				Sun, May 16, 2021 4:10 PM UTC
OS Detection Consolidation and Reporting		?	80 %	192.168.56.101	METASPLOITABLE	general/tcp				Sun, May 16, 2021 5:37 PM UTC
Twiki Version Detection		?	80 %	192.168.56.101	METASPLOITABLE	80/tcp				Sun, May 16, 2021 5:37 PM UTC
PHP Detection (HTTP)		?	80 %	192.168.56.101	METASPLOITABLE	80/tcp				Sun, May 16, 2021 5:38 PM UTC
jQuery Detection (HTTP)		?	80 %	192.168.56.101	METASPLOITABLE	80/tcp				Sun, May 16, 2021 5:38 PM UTC
phpMyAdmin Detection		?	80 %	192.168.56.101	METASPLOITABLE	80/tcp				Sun, May 16, 2021 5:38 PM UTC
ICMP Timestamp Detection		?	80 %	192.168.56.101	METASPLOITABLE	general/cmp				Sun, May 16, 2021 5:38 PM UTC
Hostname Determination Reporting		?	80 %	192.168.56.101	METASPLOITABLE	general/tcp				Sun, May 16, 2021 5:38 PM UTC
RPC Portmapper Service Detection (TCP)		?	80 %	192.168.56.101	METASPLOITABLE	111/tcp				Sun, May 16, 2021 5:19 PM UTC
DNS Server Detection (UDP)		?	80 %	192.168.56.101	METASPLOITABLE	53/udp				Sun, May 16, 2021 5:19 PM UTC
Obtain list of all port mapper registered programs via RPC		?	80 %	192.168.56.101	METASPLOITABLE	111/tcp				Sun, May 16, 2021 5:19 PM UTC
Services		?	80 %	192.168.56.101	METASPLOITABLE	3306/tcp				Sun, May 16, 2021 5:19 PM UTC
Services		?	80 %	192.168.56.101	METASPLOITABLE	2121/tcp				Sun, May 16, 2021 5:19 PM UTC
Services		?	80 %	192.168.56.101	METASPLOITABLE	80/tcp				Sun, May 16, 2021 5:19 PM UTC

Nevertheless with the same amount of time as the full and fast scan we have been able to detect 4 hosts including : Metasploitable VM, Host machine, Greenbone VM.

Greenbone

Security Manager

<

6.5 Additional features

6.5.1 Filtering

Filtering option allows you to reduce/increase the amount of vulnerabilities displayed in the results section. Here you can select the minimum QoD you want to analyse, the range of CVSS score you want to analyse, or any kind of narrowing you might need for your analysis (Host targeting, location targeting, etc).

Update Filter

Filter

Apply Overrides ☐ Yes ☒ No

Auto-FP ☐ Trust vendor security updates ☐ Full CVE match ☐ Partial CVE match

Only show hosts that have results ☐

QoD must be at least 70 %

Severity (Class) ☒ High ☒ Medium ☒ Low ☐ Log ☐ False Pos.

Severity is equal to 0

Solution Type ☒ All ☐ Vendor fix ☐ Workaround ☐ None available ☐ Mitigation ☐ Will not fix

Vulnerability

Host (IP)

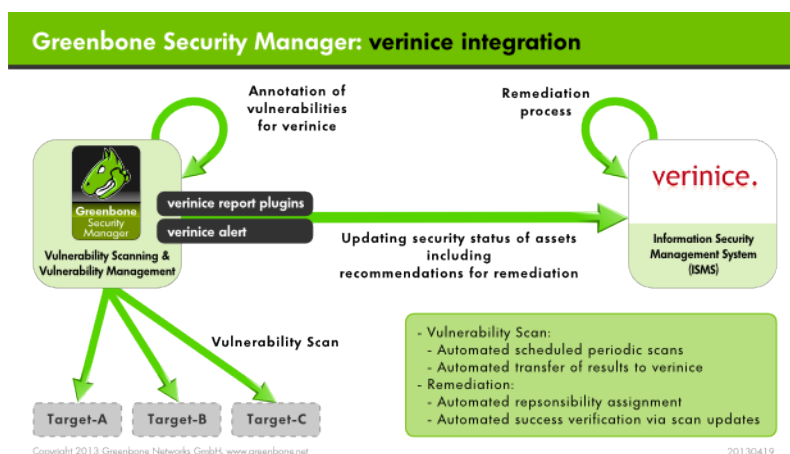
Location (eg. port/protocol)

First result 1

Cancel Update

6.5.2 Exportation⁶

OpenVAS allows also to export the reports in different formats : CSV, PNG, XML. The exportation features allows you to manage your history of scans from outside the Greenbone environment and also to perform ISMS by importing report in additional tools such as ISMS (Information and Security management systems). Greenbone provides instructions to connect itself to one of this tool : Verinice. Verinice is an open source software that aims to perform risk assessment by managing updates of vulnerability scanner reports.



⁶Connecting the Greenbone Security Manager to Other Systems. URL: <https://docs.greenbone.net/GSM-Manual/gos-5/en/connecting-other-systems.htmls>.

7 Second Custom Exercise

7.1 Instructions

The time consumption is the critical issue we faced during the full and fast scan. So, another possibility to reduce the duration could also be to narrow the assets you want to analyse the vulnerabilities. In the following scan we will target the databases applications we already detected in the previous full and fast scan. There, we expect the outcome to be a subset of the results of the full and fast scans.

7.2 Practice

Here is the different steps of our custom scan :

- 1. Identify the databases application you want to detect.
There are two possibilities. The first one is the case you already know the applications and you just have to pick the port and protocol associated (UDP or TCP). The second one is you don't already know the ports within your target and you edit a range the standard port for the standard databases application Here we provide the list of application we expect to detect with the port associated :

SQL application	Port
Microsoft SQL Server	1433
MySQL	3306
Firebird	3050
PostgreSQL	5432
Persuasive SQL	3351

- 2. Add the correct custom port list.
You will simply enter the 5 ports scans in the custom port range. Here TCP is sufficient to make our scan successful

- 3. Add a custom target
The custom target will include our previous custom port list and the IP address of the target host we already used.

- 4. Request a scan of our custom target
This step is the same as we have already done with the full and fast scan. However we select our custom target instead of just inputting the target host.

7.3 Results

Now you must be able to see 11 results with the default filter in a few minutes. As we expected we manage to detect vulnerabilities of two SQL applications : *PostgreSQL* and *MySQL*.

Information	Results (11 of 115)	Hosts (1 of 1)	Ports (2 of 2)	Applications (3 of 3)	Operating Systems (1 of 1)	CVEs (9 of 9)	Closed CVEs (0 of 0)	TLS Certificates (1 of 1)	Error Messages (0 of 0)	User Tags (0)
Application CPE										
	cpe:/a:oracle:mysql:5.0.51a	1								
	cpe:/a:postgresql:postgresql:8.3.1	1								
	cpe:/a:mysql:mysql:5.0.51a	1								

8 Alternatives⁷⁸

8.1 Business Models

OpenVAS as an open source vulnerability scanner can be compared to many concurrent tools. We can identify among the most famous : OpenSCAP, Nessus, Nexpose, Retina.

All of these alternatives are not opensource but many offer the same business model as Greenbone : a free version designed to perform the basic purpose of performing vulnerability scans and a subscription which provides to their customers the full content version of the tool, and additional support.

The extended content is usually better by increasing the range of possible targets and configuration features.

For the extended versions, the annual cost differs but the professional oriented versions usually average a fee of several thousands dollars : 3 000 USD/year for Nessus, N/A for Greenbone (fees are custom-made/depending of the Ip Gap).

8.2 Performance and Speciality

Every vulnerability scanner has its own interface and philosophy. Indeed OpenVAS is as a versatile vulnerability scanner but some are specialised on different types of content, depending of the policies you need for your system to comply with (PCI-DSS, ISO 27005, ...).

The performances are the simplest criteria to compare the different vulnerabilities. In the end, there is no evident differences and comparisons must be done separately. The criteria of difference can be resumed with the criteria listed below :

- Number of CVEs covered
- Guarantees : a patch is delivered in an average of couple of days for full support subscriptions
- Dashboard features
- Scanning templates : Possibility to access custom reports according to policy compliance, custom threats, custom assets, ...
- Rate of false positives : only the QoD is provided by OpenVAS but no real guarantees are given in the free version
- The quality of support : this service is more oriented for professional (and not free) versions of the tool.

⁷Kushe R. *Comparative study of vulnerability tools*. 2017. URL: <https://stumejournals.com/journals/confsec/2017/2/69.full.pdf>.

⁸Kushe R. *Testing and comparing web vulnerability tools for sql injection and xss attack*. 2008. URL: https://www.researchgate.net/publication/4322871_Testing_and_Comparing_Web_Vulnerability_Scanning_Tools_for_SQL_Injection_and_XSS_Attacks.

References

- 19 Architecture. URL: <https://docs.greenbone.net/GSM-Manual/gos-20.08/en/architecture.html>.
- Connecting the Greenbone Security Manager to Other Systems. URL: <https://docs.greenbone.net/GSM-Manual/gos-5/en/connecting-other-systems.htmls>.
- R., Kushe. *Comparative study of vulnerability tools*. 2017. URL: <https://stumejournals.com/journals/confsec/2017/2/69.full.pdf>.
- *Testing and comparing web vulnerability tools for sql injection and xss attack*. 2008. URL: https://www.researchgate.net/publication/4322871_Testing_and_Comparing_Web_Vulnerability_Scanning_Tools_for_SQL_Injection_and_XSS_Attacks.
- Schlosser, Kristin. *About GVM 20.08 and 21.04 Architecture*. 2021. URL: <https://community.greenbone.net/t/about-gvm-20-08-and-21-04-architecture/8449>.
- Stankovic, Strahinja. "How To Perform A Successful Network Security Vulnerability Assessment". In: *PurpleSec* (2020). URL: <https://purplesec.us/perform-successful-network-vulnerability-assessment/#respond>.
- Tutorials, Hacking. *Vulnerability Scanning with OpenVAS 9 part 4: Custom scan configurations*. 2020. URL: <https://www.hackingtutorials.org/scanning-tutorials/openvas-9-part-4-custom-scan-configurations/>.
- Vulnerability Assessment – GCE/GSM. URL: <https://www.anthesia.net/2020/05/14/vulnerability-assessment-gce-gsm/>.