Pre-Class Activity

Pre-Class Activity – Setup Sandbox – I

1. Run `pa211_setup` command on a school computer.
2. Change your working directory to the clone of repository from the previous week
   https://gitlab.fi.muni.cz/cybersec/pa211/management.git
3. Run `git pull`.
4. Change directory to `openvas`. This directory should contain `Vagrantfile`.
5. Run `vagrant up`.
6. We will use only one **Kali host** named `student`. Use credentials `kali:kali`.
   You may need to **login twice**.

Pre-Class Activity – Setup Sandbox – II

- Use **port forwarding** command to access services from your host:
  1. `vagrant ssh student -- -L 9392:localhost:9392`
- Verify that you can **access** `http://localhost:9392`
- Log into **Greenbone Security Assistant**
  - credentials are `admin:admin`

Pre-Class Activity – Import Test Data

- **ospd-openvas** container's logs
  - **Start**

    ```
    Loading VTs. Scans will be [requested|queued] until VTs are loaded. This may take a
    few minutes, please wait...
    ```
  - **End**

    ```
    Finished loading VTs. The VT cache has been updated from version X to Y.
    ```
- **gvmd** container' logs
  - After **ospd-openvas** successfully **loaded data**, scan can be **started**
  - **Start**

    ```
    OSP service has different VT status (version X) from database (version (Y), Z VTs).
    Starting update ...
    ```
  - **End**

    ```
    Updating VTs in database ... done (X VTs).
    ```

MUNI
FI

Vulnerability Management – Seminar

PA211 Advanced Topics of Cyber Security

September 27, 2022

Lukáš Sadlek, Pavel Čeleda, and Jan Vykopal

Goals of this tutorial

- Become acquainted with:
  - **Vulnerability** scanning
  - Assessment of **vulnerability scan results**

Prerequisites – I

1. Run **`pa211_setup`** command on a school computer.
2. Change your working directory to the clone of repository from the previous week
   https://gitlab.fi.muni.cz/cybersec/pa211/management.git
3. Run **`git pull`**.
4. Change directory to **`openvas`**. This directory should contain **`Vagrantfile`**.
5. Run **`vagrant up.`**
6. We will use only one **Kali host** named **`student.`** Use credentials `kali:kali.`
   You may need to **login twice**.

Prerequisites – II

- Use **port forwarding** command to access services from your host:
  1. `vagrant ssh student -- -L 9392:localhost:9392`
- Verify that you can **access** `http://localhost:9392`
- Log into **Greenbone Security Assistant**
  - credentials are `admin:admin`

Troubleshooting – I

- **Destroy** and **create** a virtual machine:
  - `vagrant destroy <machine_name> -f`
  - `Vagrant up <machine_name>`
- **Rerun** ansible tasks, if ansible script **failed**:
  - `vagrant provision <machine_name>`
- **Start all** containers:
  - `sudo docker start $(sudo docker ps –aq)`
- **List all** (not only running) containers:
  - `sudo docker container ls –a`

Troubleshooting – II

- List **open ports** on device:
  - `sudo netstat -tulpn`
- **Check logs** of a specific **container** for issues:
  - `sudo docker logs <container_id>`
- Completed scan is **a formality**
  - Target contains much **more vulnerabilities** than needed
- Tasks **can** be solved, **even if** the scan was **interrupted**
  - Solutions describe **how** to reveal the **results**

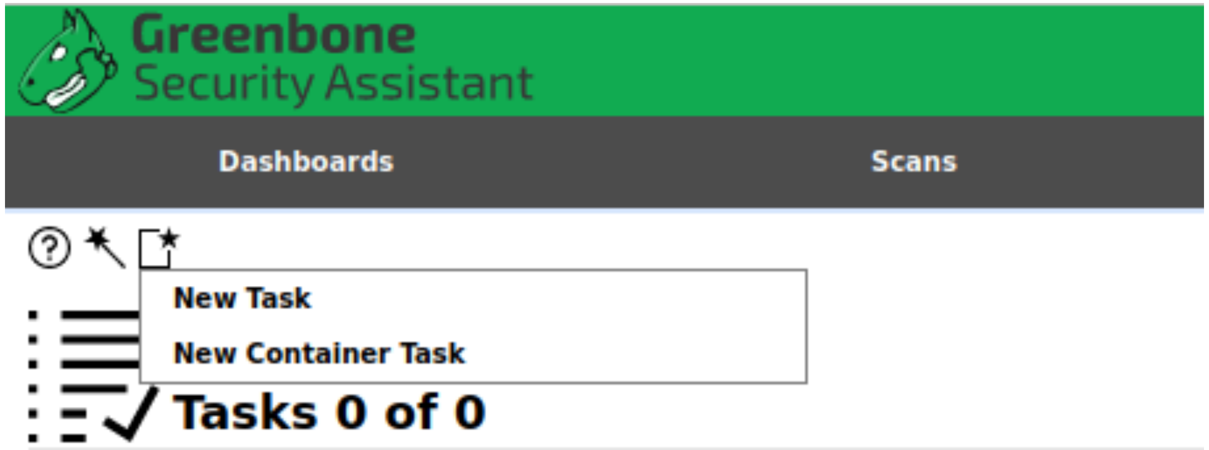
Vulnerability scanning

Greenbone Vulnerability Management

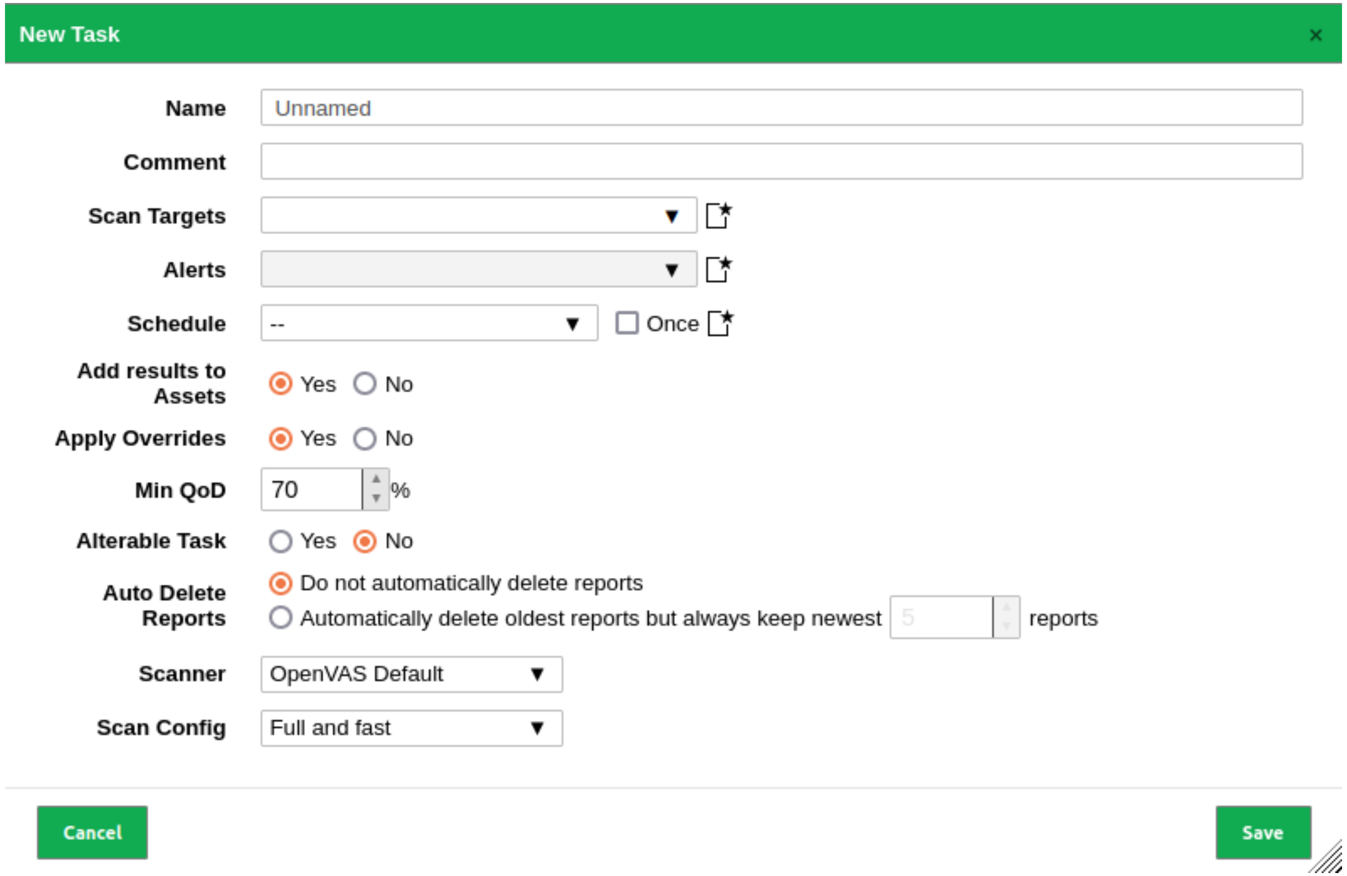
- Previous name **OpenVAS** (Open Vulnerability Assessment Scanner)
- **Full-featured** open-source vulnerability scanner
- **Greenbone Security Assistant** – web-based user interface
- **NVT** – network vulnerability test
- **Override** – rules for **disallowing** some results (**false positives**)
- **Documentation** for more details **[1]**
- **Main menu** – demonstration

Greenbone Security Assistant – new task

- **New Task** can be created in menu option **Scans**
- Requires to create **new schedule** and **new target**
  - In **Configuration** part of menu
  - Directly in **New Task window**
  - See the **following slides**

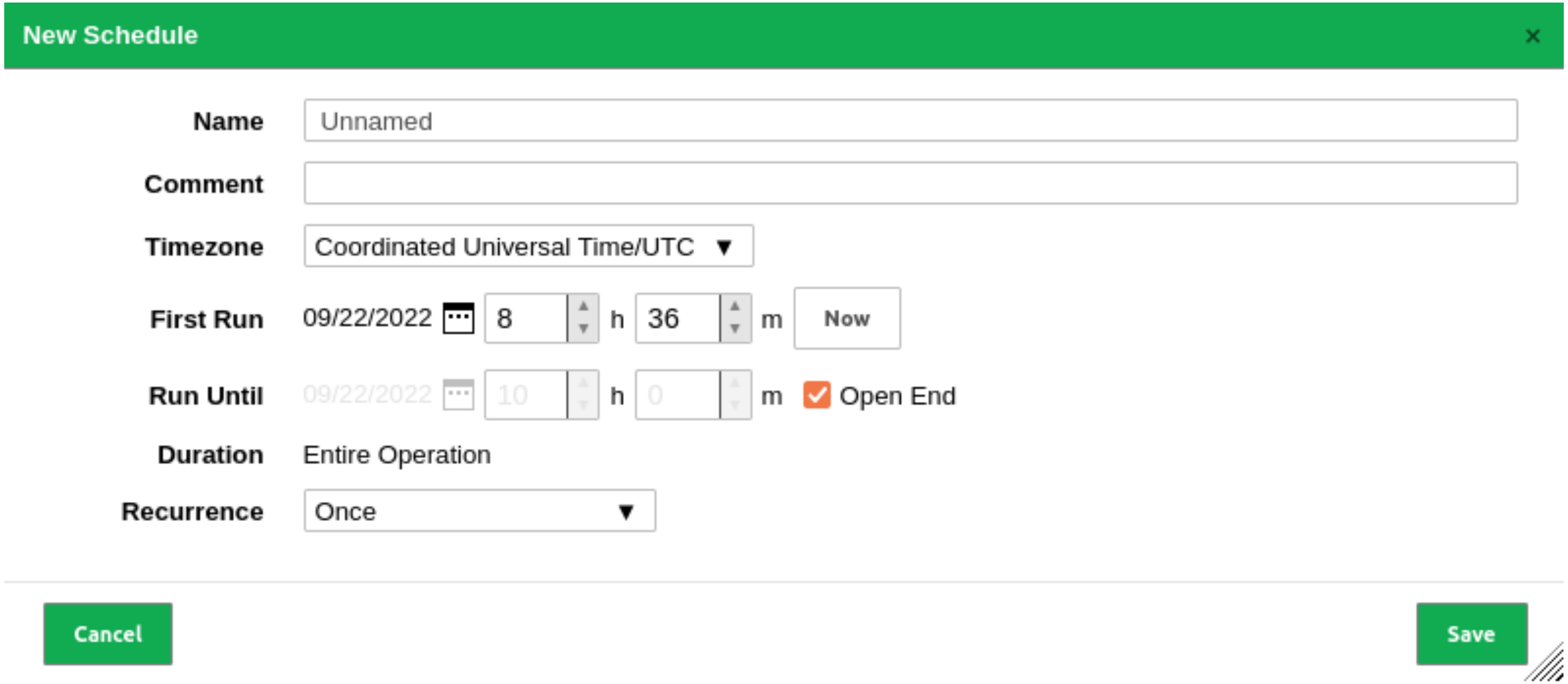


New Task window



Name	Unnamed
Comment	
Scan Targets	▼
Alerts	▼
Schedule	-- ▼ □ Once
Add results to Assets	● Yes ○ No
Apply Overrides	● Yes ○ No
Min QoD	70 %
Alterable Task	○ Yes ● No
Auto Delete Reports	● Do not automatically delete reports ○ Automatically delete oldest reports but always keep newest 5 reports
Scanner	OpenVAS Default ▼
Scan Config	Full and fast ▼

New Schedule window

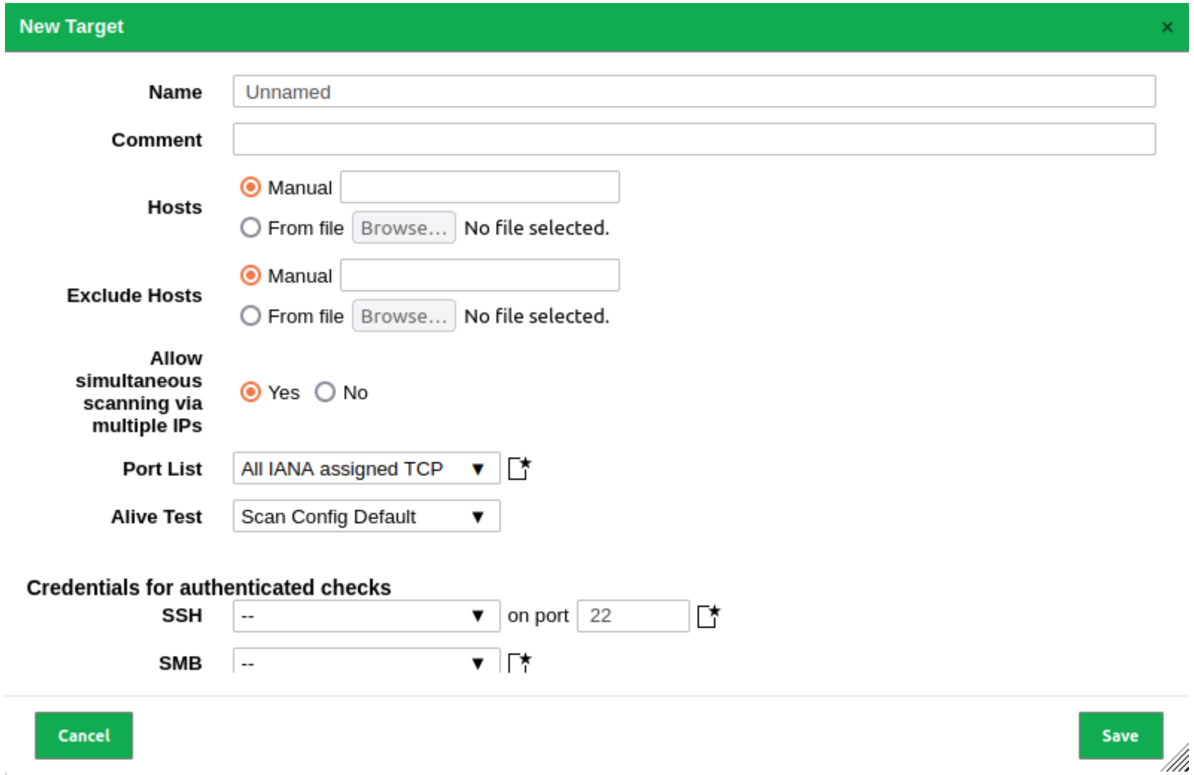


New Schedule

Name	Unnamed
Comment	
Timezone	Coordinated Universal Time/UTC ▼
First Run	09/22/2022 8 h 36 m
Run Until	09/22/2022 10 h 0 m ☑ Open End
Duration	Entire Operation
Recurrence	Once ▼

New Target window

- **Hosts** can be specified using
  - IP address
  - IP address CIDR range
  - Hostname
  - Other options



New Target ×

Name: Unnamed

Comment:

Hosts: ● Manual / ○ From file Browse… No file selected.

Exclude Hosts: ● Manual / ○ From file Browse… No file selected.

Allow simultaneous scanning via multiple IPs: ● Yes ○ No

Port List: All IANA assigned TCP ▼

Alive Test: Scan Config Default ▼

Credentials for authenticated checks

SSH: -- ▼ on port 22

SMB: -- ▼

Loading vulnerability test data

- **ospd-openvas** container's logs
  - **Start**

    ```
    Loading VTs. Scans will be [requested|queued] until VTs are loaded. This may take a
    few minutes, please wait...
    ```
  - **End**

    ```
    Finished loading VTs. The VT cache has been updated from version X to Y.
    ```
- **gvmd** container' logs
  - After **ospd-openvas** successfully **loaded data**, scan can be **started**
  - **Start**

    ```
    OSP service has different VT status (version X) from database (version (Y), Z VTs).
    Starting update ...
    ```
  - **End**

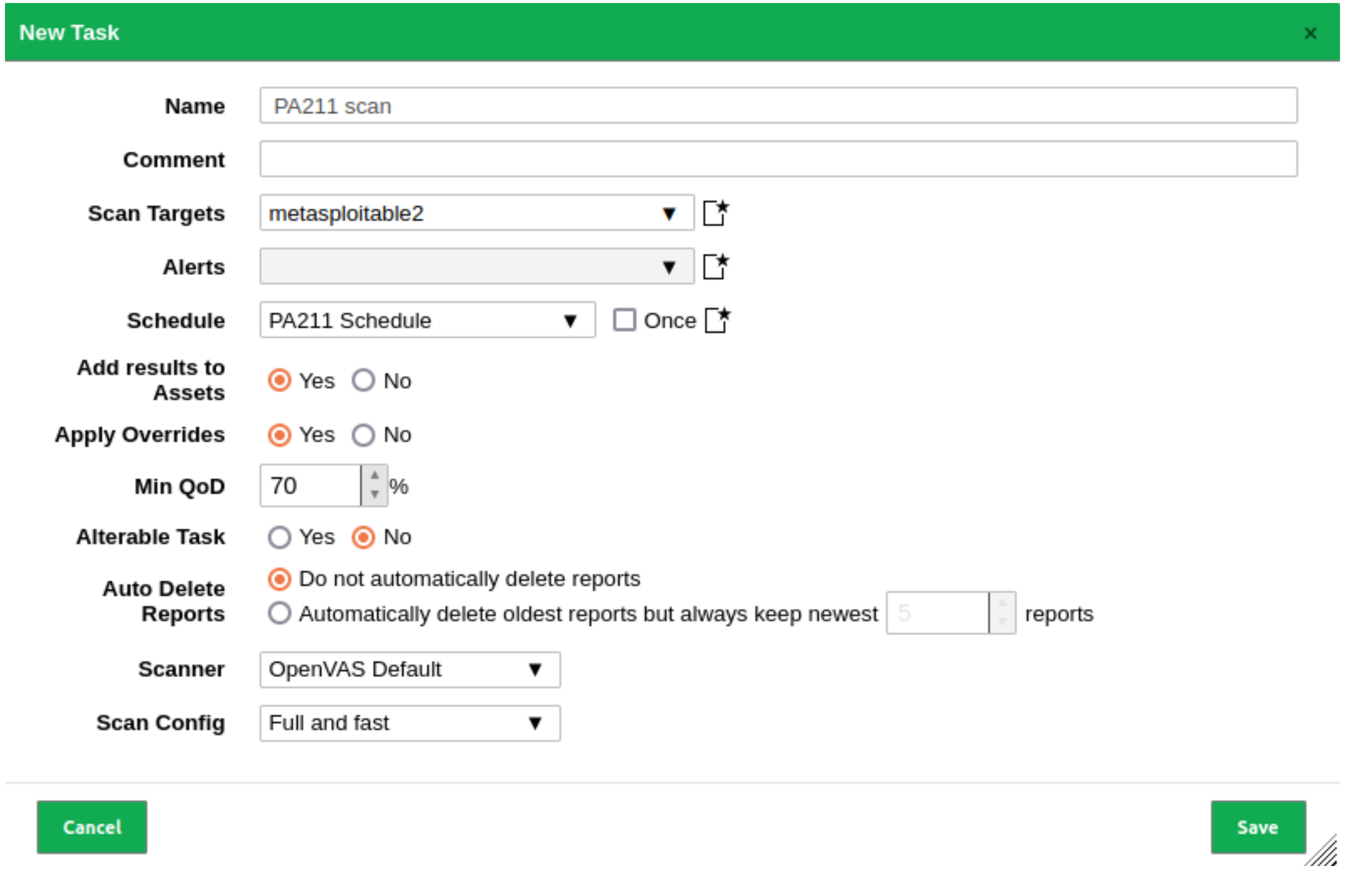
    ```
    Updating VTs in database ... done (X VTs).
    ```

Task 1 – first scan

1. In section Scans, create **New Task** (in the left upper corner). Its name should be "**PA211 Scan**".
2. Create a scan **target** called "**metasploitable2**". Its hostname is `metasploitable2.`
3. Create "**PA211 Schedule**" and schedule its start in **three minutes**.
4. All other fields should have **default or empty** values.

The scan takes **approximately** 45 minutes.

Solution 1 – new task



New Task

Name	PA211 scan
Comment	
Scan Targets	metasploitable2 ▼
Alerts	▼
Schedule	PA211 Schedule ▼ □ Once
Add results to Assets	● Yes ○ No
Apply Overrides	● Yes ○ No
Min QoD	70 %
Alterable Task	○ Yes ● No
Auto Delete Reports	● Do not automatically delete reports ○ Automatically delete oldest reports but always keep newest 5 reports
Scanner	OpenVAS Default ▼
Scan Config	Full and fast ▼

Possible bug in user interface

- Task may obtain **interrupted status** despite being **finished** [1]
- Check for the **status** of your scan
  - Get **container id** for image **`greenbone/ospd-openvas:stable`**

    ```
    sudo docker container ls
    ```
  - **Connect** to the **bash inside** of the container

    ```
    sudo docker exec -it <container_id> bash
    ```
  - Change **working directory** into `var/log/gvm` containing file `openvas.log`
  - It should contain **no errors**:

    ```
    Vulnerability scan <id> finished in <count> seconds: 1 alive hosts of 1
    ```
- If true, then UI shows **the wrong status,** but scan was **successful**

Vulnerability management lifecycle

- Our seminar targets **the first stages** of the lifecycle
- Stages:
  1. **Discover**
  2. **Prioritize / Asses**
  3. **Report** – similar to **pentesting report** (lectures 7 and 8)
  4. **Fix** – **subset** of approaches from lectures 9 – 12 about **hardening**
  5. **Verify** – scan again

Metasploitable 2

- **Intentionally** vulnerable version of **Ubuntu Linux**
- **Services**
  - FTP, SSH, Telnet, SMTP, ...
- **Issues**
  - Misconfigured services allow **remote access** from any hosts
  - **Exported root** of the file system **("/")**
  - **Some ports** are used by application **containing backdoors**
  - **Weak passwords**, e.g., postgres:postgres
  - Purposely **vulnerable web services**

Metasploitable 2

- **Warning:** do not expose its ports!
- **Our instances**
  - **Docker container** from Dockerhub's **community** content
  - **Most of the services** are enabled
- **Read more** about Metasploitable2 [1]

GVM – docker

- Set up using **official documentation** at [1]
- **Several containers**
  - `redis-server` containing **Redis server**
  - `pg-gvm` running **PostgreSQL service**
  - `gvmd` running **Greenbone Vulnerability Management Daemon**
  - `gsa` running `gsad` – a webserver providing **GSA application**
  - `ospd-openvas` – a container providing **the vulnerability scanner**
  - **Other containers** specified by documentation
- Other scanners (e.g., **Nessus** [2]) also provided as **docker containers**

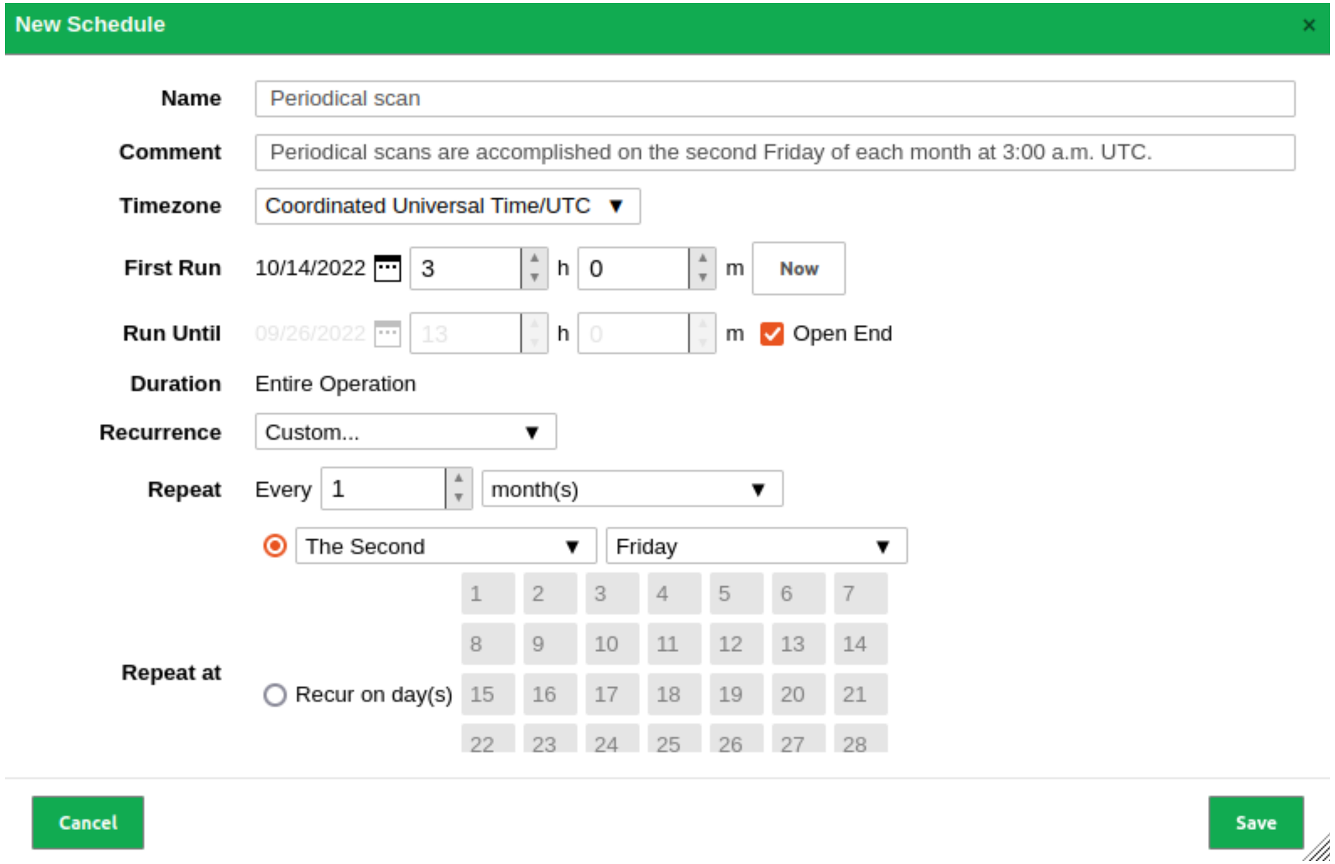
Task 2 – scanning policy

Your organization has a **scanning policy** that conforms to the **following rules**:

1. Periodical scans are accomplished on the **second Friday** of **each month at 3:00 a.m. UTC**.
2. The **scope of** scanned **assets** includes hosts **`10.1.26.2`** (hostname `server`) and **`10.1.26.9`** (hostname `elk`).
3. Only TCP ports and **essential** UDP ports should be scanned.
4. The scanner must check whether targets are **up** similarly to using **`ping` command** that internally uses **ICMP ping**.

Determine what values will be filled into **New Task, New Target,** and **New Schedule** windows but **do not** execute any tasks.

Solution 2 – New Schedule window



New Schedule ×

Name: Periodical scan

Comment: Periodical scans are accomplished on the second Friday of each month at 3:00 a.m. UTC.

Timezone: Coordinated Universal Time/UTC ▼

First Run: 10/14/2022 3 h 0 m Now

Run Until: 09/26/2022 13 h 0 m ☑ Open End

Duration: Entire Operation

Recurrence: Custom... ▼

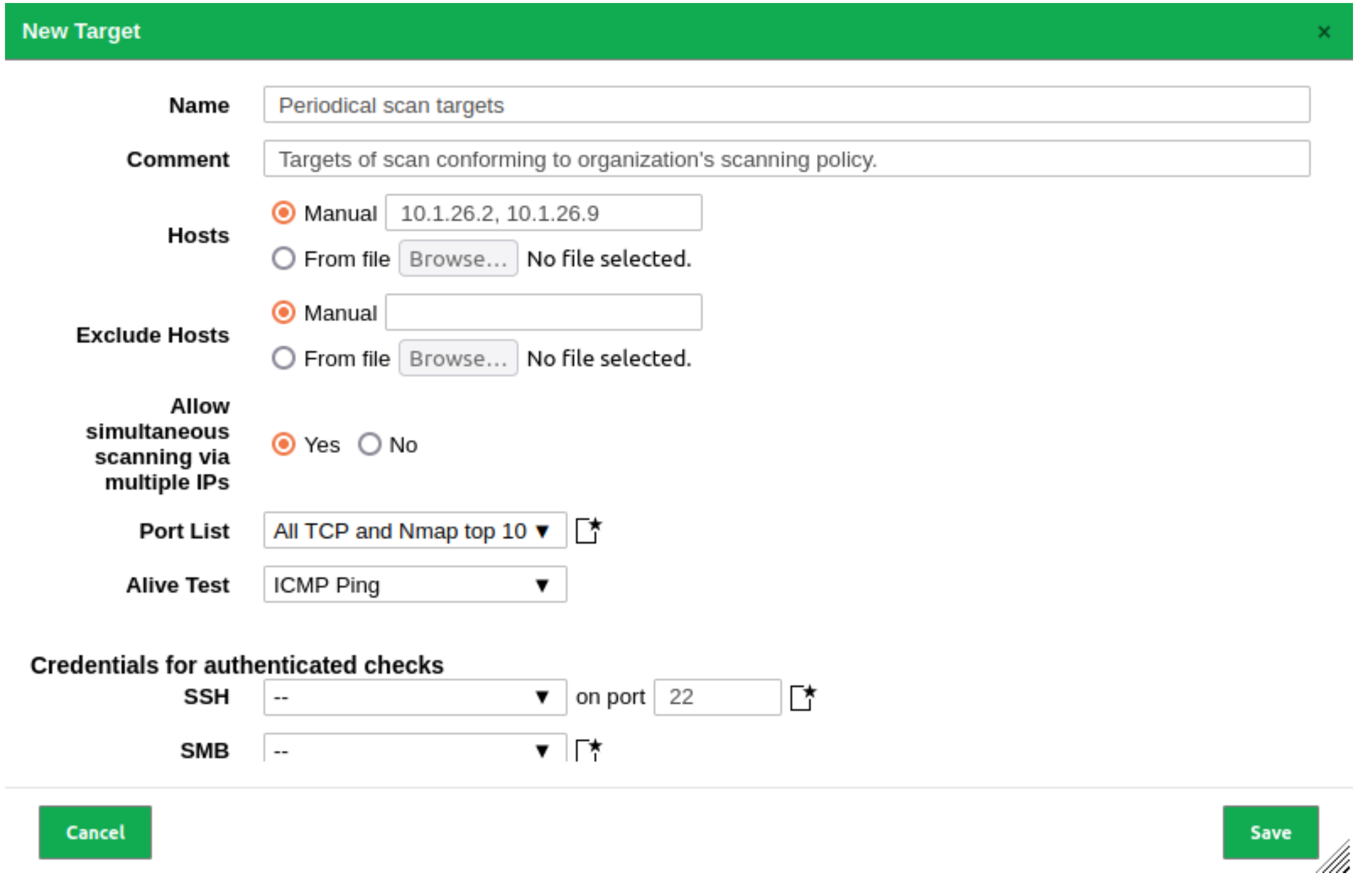
Repeat: Every 1 month(s) ▼

Repeat at: ● The Second ▼ Friday ▼

○ Recur on day(s)

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28

Solution 2 – New Target window



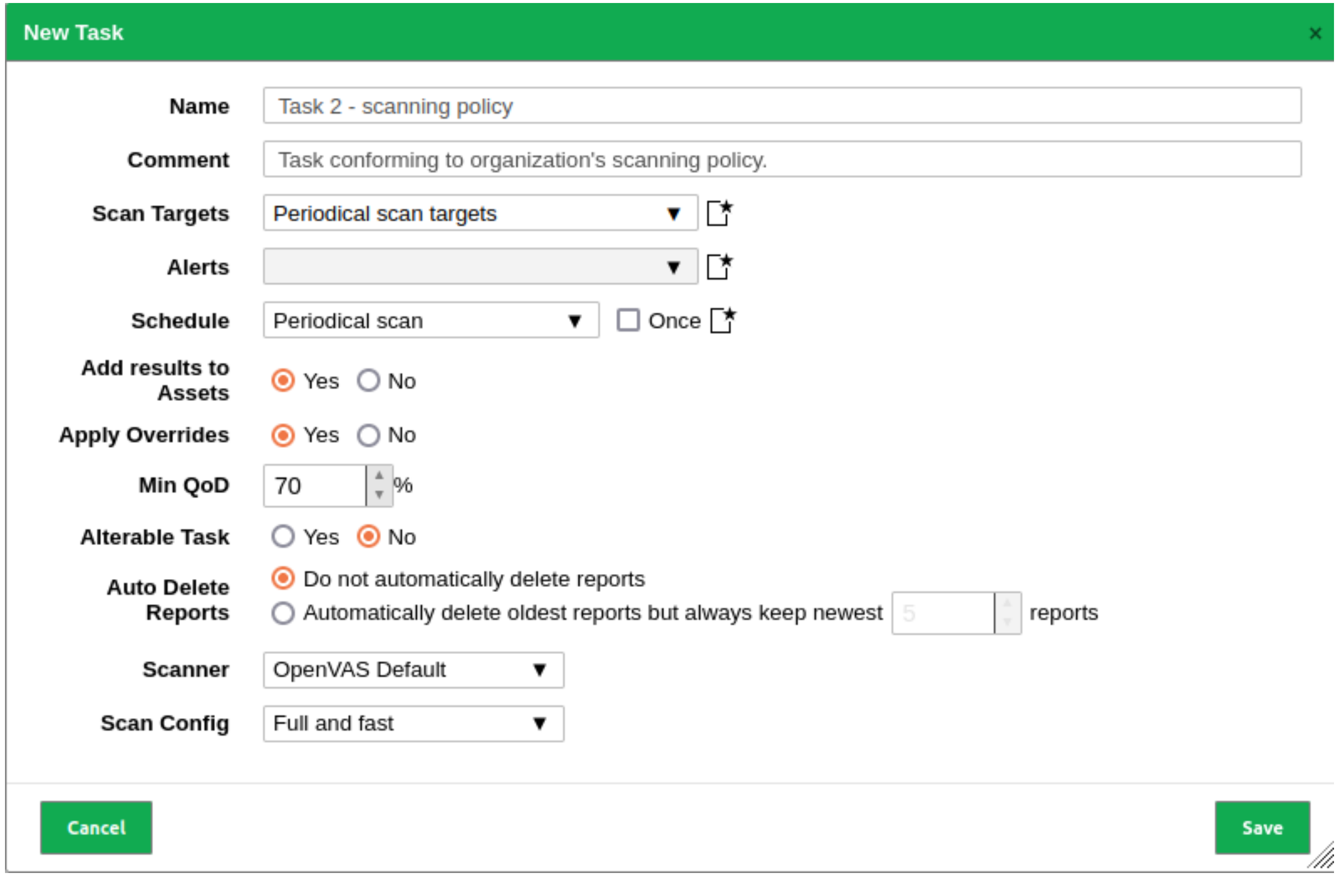
New Target ×

Name	Periodical scan targets
Comment	Targets of scan conforming to organization's scanning policy.
Hosts	● Manual 10.1.26.2, 10.1.26.9 ○ From file Browse… No file selected.
Exclude Hosts	● Manual ○ From file Browse… No file selected.
Allow simultaneous scanning via multiple IPs	● Yes ○ No
Port List	All TCP and Nmap top 10 ▼
Alive Test	ICMP Ping ▼

Credentials for authenticated checks

SSH	-- ▼ on port 22
SMB	-- ▼

Solution 2 – New Task window



New Task ×

Name: Task 2 - scanning policy

Comment: Task conforming to organization's scanning policy.

Scan Targets: Periodical scan targets ▼

Alerts: ▼

Schedule: Periodical scan ▼ □ Once

Add results to Assets: ● Yes ○ No

Apply Overrides: ● Yes ○ No

Min QoD: 70 %

Alterable Task: ○ Yes ● No

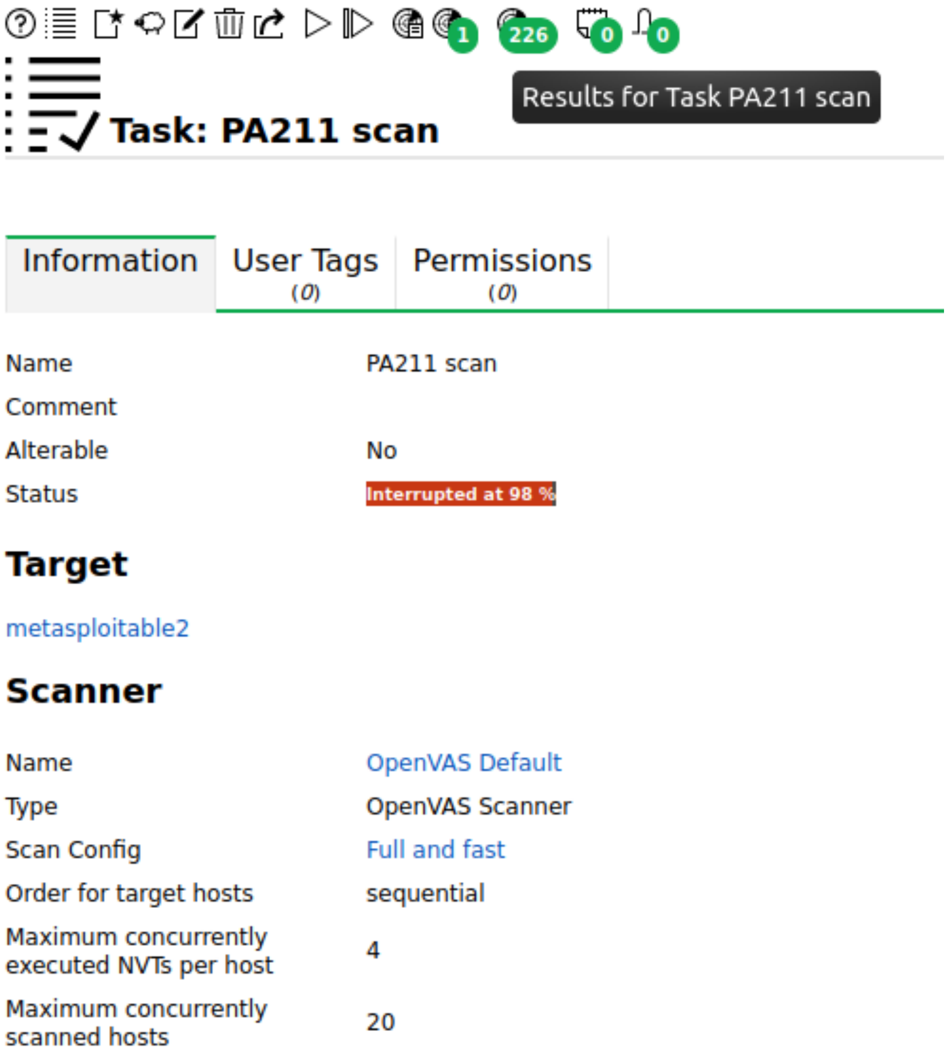
Auto Delete Reports:
- ● Do not automatically delete reports
- ○ Automatically delete oldest reports but always keep newest 5 reports

Scanner: OpenVAS Default ▼

Scan Config: Full and fast ▼

Solution 1 – results – I

1. **Open all details** for your vulnerability scan from Task 1
2. **Results** are the **third symbol** from the **right** (number 226)



Task: PA211 scan

Information | User Tags (0) | Permissions (0)

Name	PA211 scan
Comment	
Alterable	No
Status	Interrupted at 98 %

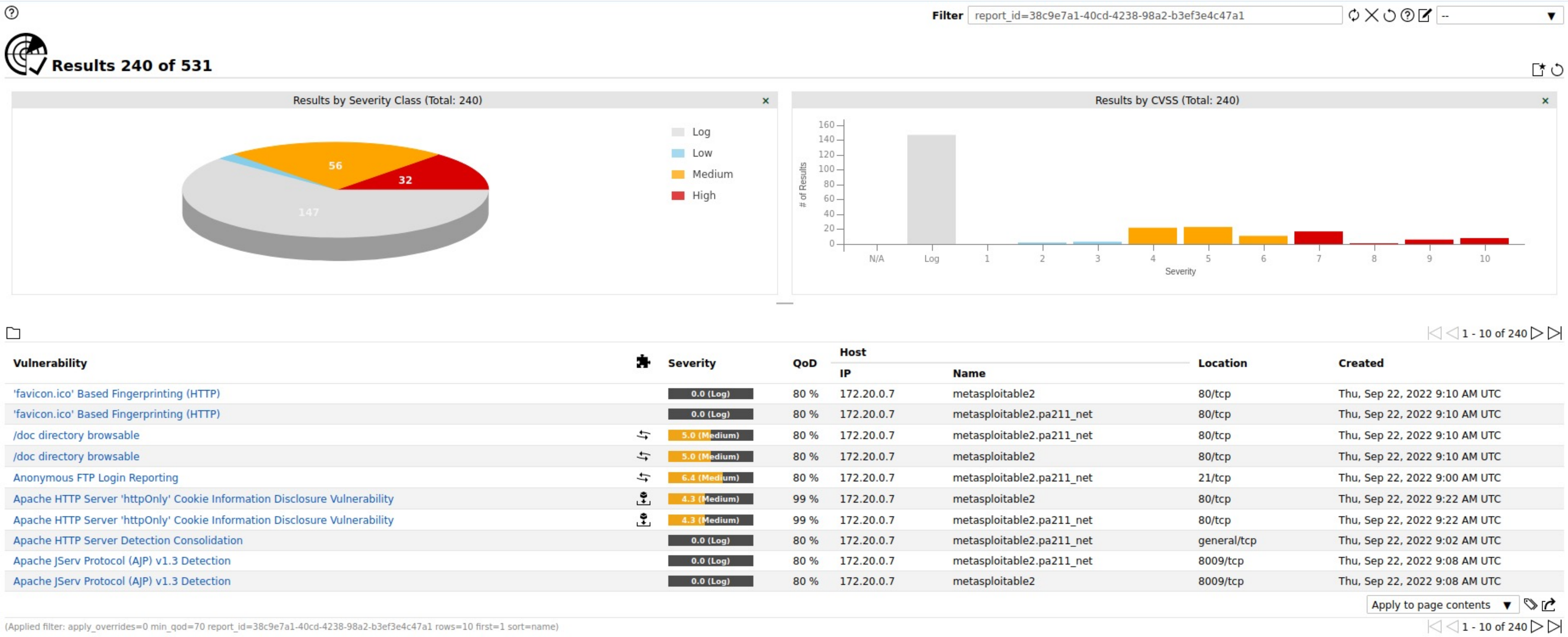
Target

metasploitable2

Scanner

Name	OpenVAS Default
Type	OpenVAS Scanner
Scan Config	Full and fast
Order for target hosts	sequential
Maximum concurrently executed NVTs per host	4
Maximum concurrently scanned hosts	20

Solution 1 – layout – II



Filter report_id=38c9e7a1-40cd-4238-98a2-b3ef3e4c47a1

Results 240 of 531

Results by Severity Class (Total: 240)

Results by CVSS (Total: 240)

1 - 10 of 240

Vulnerability		Severity	QoD	Host		Location	Created
				IP	Name		
'favicon.ico' Based Fingerprinting (HTTP)		0.0 (Log)	80 %	172.20.0.7	metasploitable2	80/tcp	Thu, Sep 22, 2022 9:10 AM UTC
'favicon.ico' Based Fingerprinting (HTTP)		0.0 (Log)	80 %	172.20.0.7	metasploitable2.pa211_net	80/tcp	Thu, Sep 22, 2022 9:10 AM UTC
/doc directory browsable	⇆	5.0 (Medium)	80 %	172.20.0.7	metasploitable2.pa211_net	80/tcp	Thu, Sep 22, 2022 9:10 AM UTC
/doc directory browsable	⇆	5.0 (Medium)	80 %	172.20.0.7	metasploitable2	80/tcp	Thu, Sep 22, 2022 9:10 AM UTC
Anonymous FTP Login Reporting	⇆	6.4 (Medium)	80 %	172.20.0.7	metasploitable2.pa211_net	21/tcp	Thu, Sep 22, 2022 9:00 AM UTC
Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	⚲	4.3 (Medium)	99 %	172.20.0.7	metasploitable2	80/tcp	Thu, Sep 22, 2022 9:22 AM UTC
Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	⚲	4.3 (Medium)	99 %	172.20.0.7	metasploitable2.pa211_net	80/tcp	Thu, Sep 22, 2022 9:22 AM UTC
Apache HTTP Server Detection Consolidation		0.0 (Log)	80 %	172.20.0.7	metasploitable2.pa211_net	general/tcp	Thu, Sep 22, 2022 9:02 AM UTC
Apache JServ Protocol (AJP) v1.3 Detection		0.0 (Log)	80 %	172.20.0.7	metasploitable2.pa211_net	8009/tcp	Thu, Sep 22, 2022 9:08 AM UTC
Apache JServ Protocol (AJP) v1.3 Detection		0.0 (Log)	80 %	172.20.0.7	metasploitable2	8009/tcp	Thu, Sep 22, 2022 9:08 AM UTC

Apply to page contents ▼

(Applied filter: apply_overrides=0 min_qod=70 report_id=38c9e7a1-40cd-4238-98a2-b3ef3e4c47a1 rows=10 first=1 sort=name)

1 - 10 of 240

Solution 1 – III

- **Layout** contains **graphs** and a **table**
- **Additional filters**
  - `rows=<number>` will adjust **number of rows**
  - `min_qod=<number>` will filter results with **quality of detection above** number
  - **Spaces** are used **between** filters

Assessment of results

Task 3 – processing results

Analyzing properties of results, such as their **severity and quality,** may provide a **general overview** of security posture.

a) **How many** vulnerabilities in the dashboard have **medium** or **high severity**?

b) **How many** results were detected with a **quality** of **at least 95%**?

c) Check results with the **severity score** of **10.0**. Does the host **operating system** have **the most recent** version?

Solution 3

a) The value can be obtained **directly from a graph** in the dashboard.

b) **Sort table** with results according to column severity descending or **add filter** min_qod=95 (with **space** between filters) and determine the **final count**.

c) There is a vulnerability named **Operating System (OS) End of Life (EOL) Detection**.

Task 4 – report

An **inevitable task** of vulnerability management is to **report the security posture** of an organization. Currently, **vulnerability scanners** can **streamline** this process.

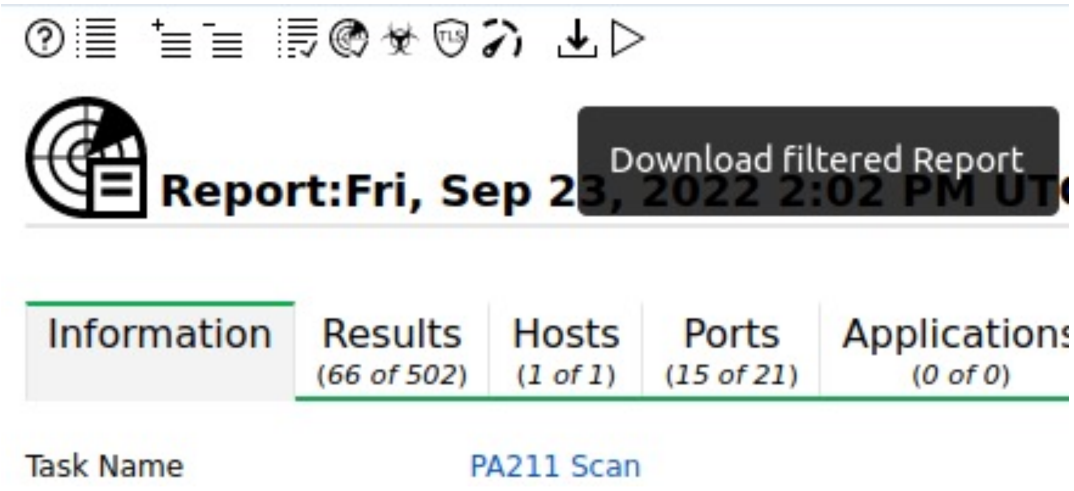
a) **Find** Greenbone Security Assistant's functionality for **generating reports** individually. Generate **report** containing results **in PDF file**. What **content** does it have?

b) **Years,** when vulnerabilities were **published,** may reveal the **efficacy of patching** in the organization. Determine the **two most recent** vulnerabilities.

c) What are their **CWEs in the NVD**?

Solution 4 a)

In **menu** of GSA, choose **Scans –> Reports**. Then click on the **date** in the table. This site will provide **Download filtered report** option.



Report:Fri, Sep 23, 2022 2:02 PM UT

Task Name PA211 Scan

Solution 4 b) c)

- A possible solution is to use the **generated report** and **standardized CVE identifiers** with the form CVE-YYYY-NNNN. Search for string **CVE-year**.
- Answer **b)** depends on the **completeness of the scan**, e.g., CVE-2018-20212, CVE-2020-1938.
- Their **CWEs** can be found **in the NVD** [1]. In our example, it is CWE-79 = Cross-site scripting, NVD-CWE-Other.

Task 5 – analysis

Consider vulnerabilities that **did not** have the **severity of 10.0**.

Find **three vulnerabilities** among them that had **the highest severity**. **Which** of these vulnerabilities, **according to CVSS**:

a) allows **remote** exploit from **unrelated parts** of the Internet,
b) **requires** user interaction,
c) **impacts availability** of the vulnerable product?

Solution 5

Concrete vulnerabilities depend on the **completeness** of the scan. There are **general rules**:

a) The **access vector** from CVSSv2 should be **NETWORK,** or the **attack vector** from CVSSv3 should be **NETWORK**.

b) **User interaction** in CVSSv3 is set to **REQUIRED**.

c) **Availability impact** in CVSSv2 or CVSSv3 is **not NONE**.

How was it today?

Please fill in an **anonymous** exit ticket:

https://muni.cz/go/pa211-22-03

MUNI

FI