Co-funded by the Erasmus+ Programme of the European Union

ISSES

ISSES – Information Security Services Education in Serbia

Supported by the Erasmus+ Capacity Building in the field of Higher Education (CBHE) grant N° 586474-EPP-1-2017-1-RS-EPPKA2-CBHE-JP

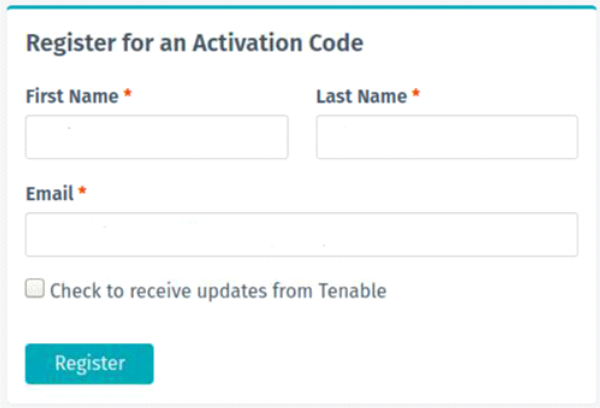
Penetration testing and ethical hacking

- Laboratory exercise -

1. Enter the following address in the browser:

- `https://www.tenable.com/tenable-for-education/nessus-essentials`

and register for a free account. After opening a new page, click the *Download* button.



2. Find the appropriate version of the *Nessus* tool and download the installation file.

3. Position yourself in the folder with the downloaded installation file (`cd Downloads`) and enter the following command:

- `sudo dpkg -i Nessus-8.10.0-ubuntu1110_amd64.deb`

4. After installation, enter the following command to run the tool:

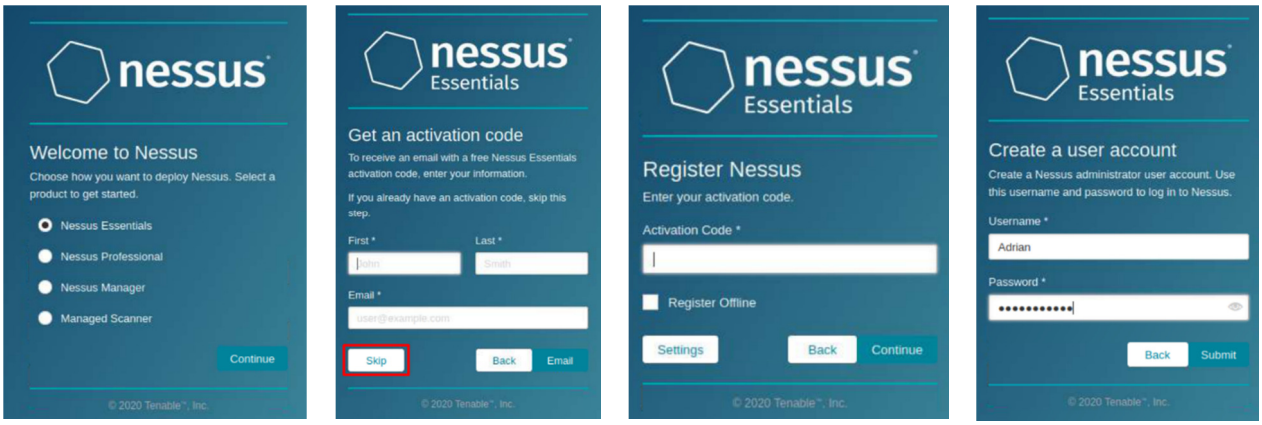
- `sudo /etc/init.d/nessusd start`

Then enter the following address in the browser to start configuring the scanner:

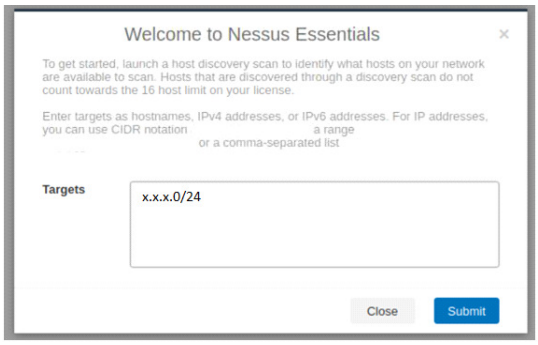
- `https://localhost:8834/`

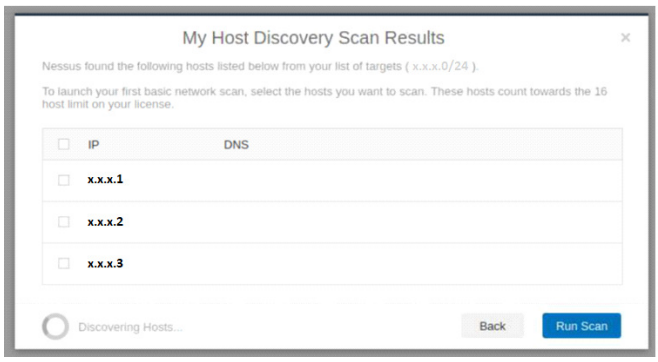
In case the browser displays a warning of a potential risk, click on *Advanced..* and go to the tool configuration page.

5. Select *Nessus Essentials* and click *Continue*. Skip the next step with account registration because it has already been done in step 1 by clicking the *Skip* button. In the next field, enter the activation code that arrived at the e-mail address you entered during registration (step 1), and then click on the *Continue* button. Finally, create an account with the desired username and password and click the *Submit* button. After that, the process of initializing the *Nessus* tool starts and it can take some time.



6. After opening the tool, it is possible to search for available hosts by entering the range of *IP* addresses to search. Enter the data as shown in the picture and click *Submit*.





7. After the search, the addresses of the hosts that have been found will appear in the window. The tool provides the ability to run a default scan, but we will first create our scan configuration. Click the *Back* button, and then click *Close*.

8. Before creating the configuration, enable some services (optional) on VM2 that will be scanned:

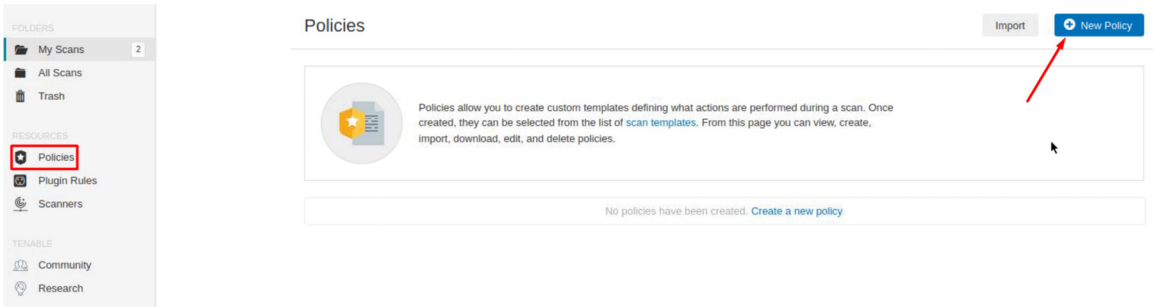
- Enable routing with the command:
  - `sudo sysctl -w net.ipv4.ip_forward=1`
- Install the *FTP* server using the command:
  - `sudo apt install vsftpd`
- Start the *FTP* server with the command:
  - `sudo systemctl restart vsftpd.service`
- Use *WinSCP* to connect to VM3 (same address and credentials as for *SSH* connection) and place the *SimpleAuthServer.py* file in a folder in the path `home/student/Documents/web/`

- Use the command `cd Documents/web` to position yourself in the folder and start the web server using command:
  - `sudo python SimpleAuthServer.py 80 username:password`
- Install an older version of *ApacheDS*. Download the desired old version from the following page:
  - `https://directory.apache.org/apacheds/download-old-versions.html`

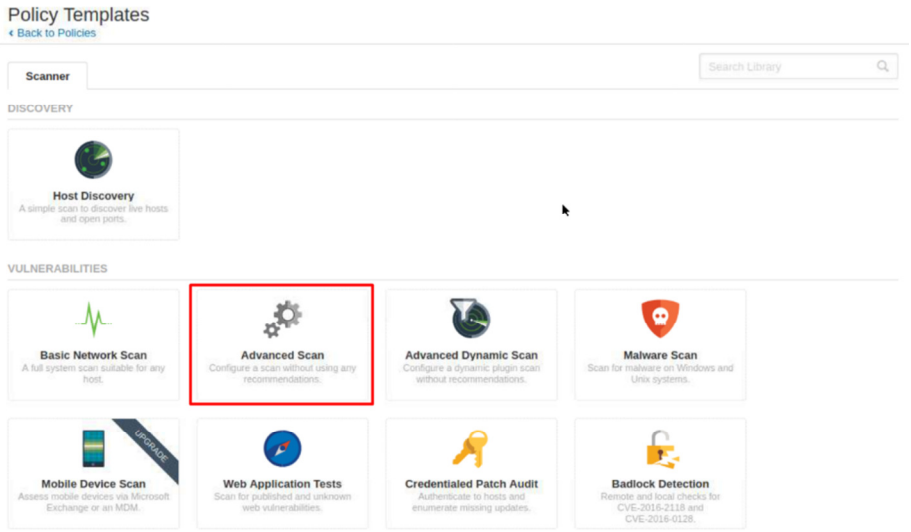
ApacheDS 2.0.0-M6	Download	29/Feb/2012
ApacheDS 2.0.0-M5	Download, Javadoc, Xref	07/Feb/2012
ApacheDS 2.0.0-M4	Download, Javadoc, Xref	09/Jan/2012
ApacheDS 2.0.0-M3	Download, Javadoc, Xref	12/Sep/2011
ApacheDS 2.0.0-M2	Download, Javadoc, Xref	22/Aug/2011
ApacheDS 2.0.0-M1	Download, Javadoc, Xref	25/Jun/2011

- Position yourself in the folder where the installation file was downloaded (`cd Downloads`) and perform the installation:
  - `sudo dpkg -i apacheds-2.0.0-M4-amd64.deb`
- Java is required to run the service. Install Java using command:
  - `sudo apt install default-jre`
- Start service with the command:
  - `sudo /etc/init.d/apacheds-2.0.0-M4-default start`
- Students are encouraged to try activating different services than those given in this example before scanning, as well.

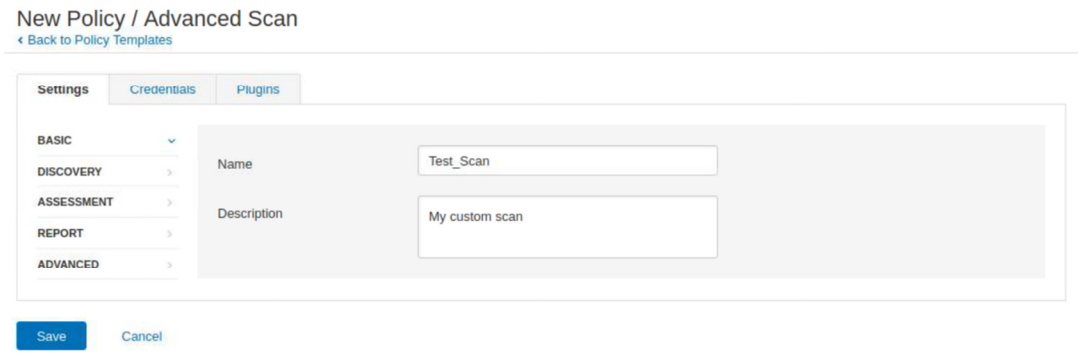
9. In the menu on the left, click *Policies*, and then click *New Policy*.



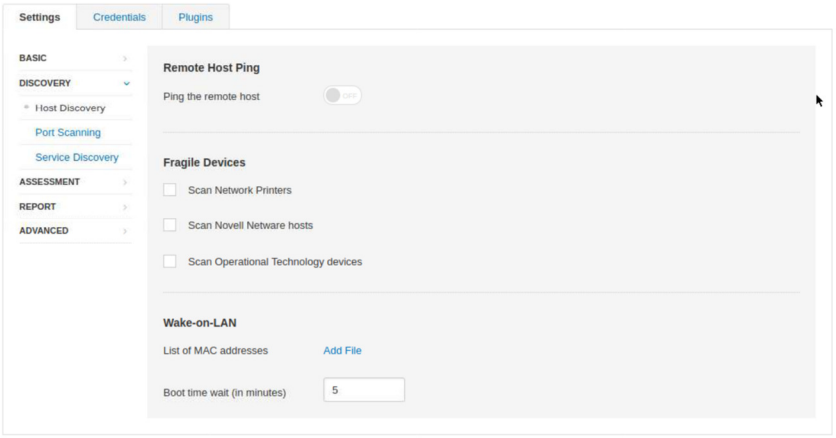
10. From the templates provided, select *Advanced Scan*.



11. Enter the desired policy name and optional description.

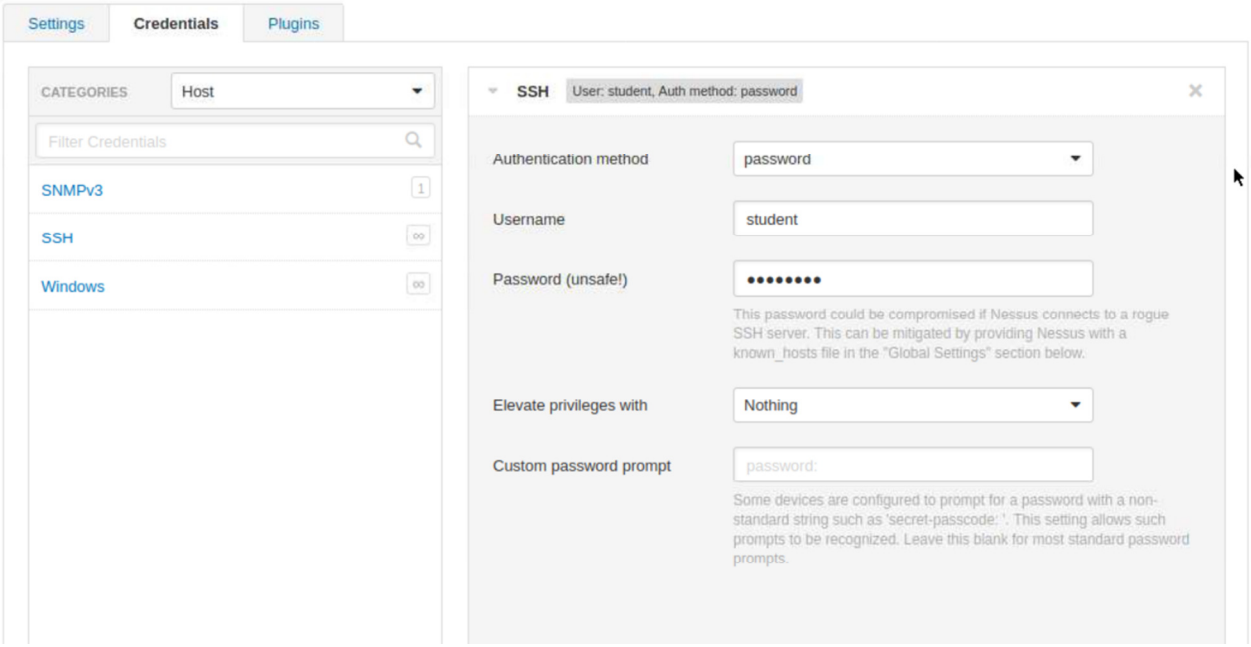


12. Clicking on *Discovery* opens a form that should be filled out as follows.

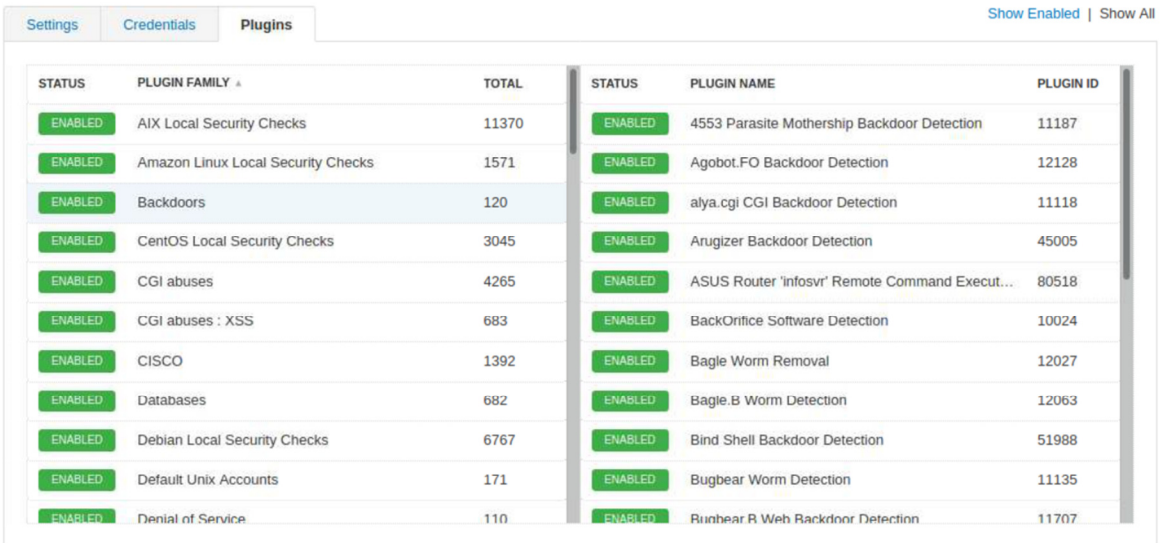


The rest of the configuration can remain as default. Students are advised to try different configurations after working with this one.

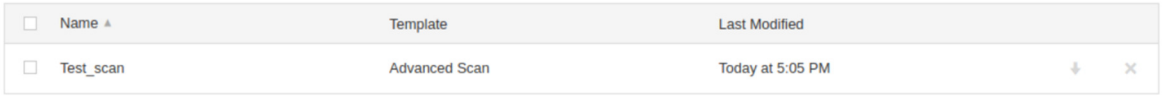
13. Click on the *Credentials* tab, select the *SSH* option and select the password for the authentication method, and then enter the necessary data.



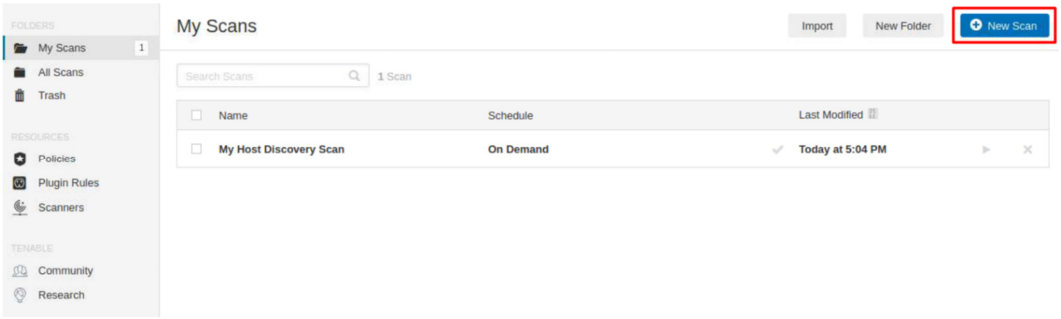
14. On the *Plugins* tab, you can select the plugins as desired.



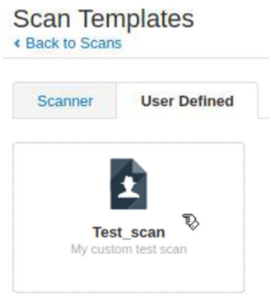
15. Save the changes by clicking *Save*, then click *Back to policies*. A newly created policy should have appeared.



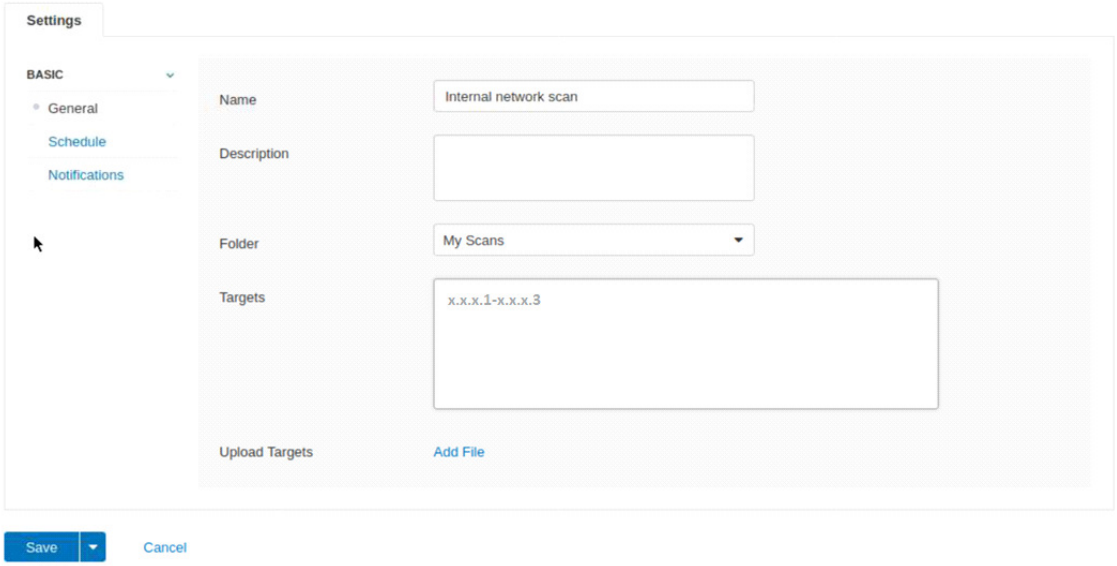
16. In the menu on the left, select *Scans*, then click *New scan*.



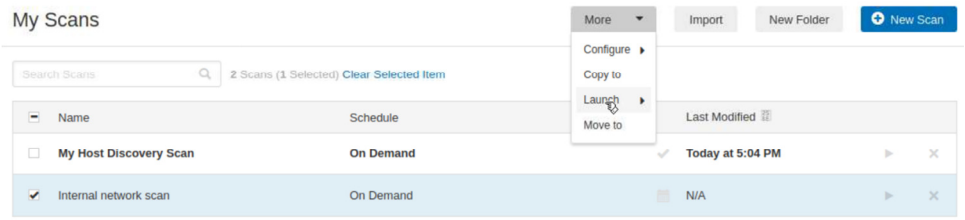
17. Go to the tab of user-defined templates and from there select the created template.



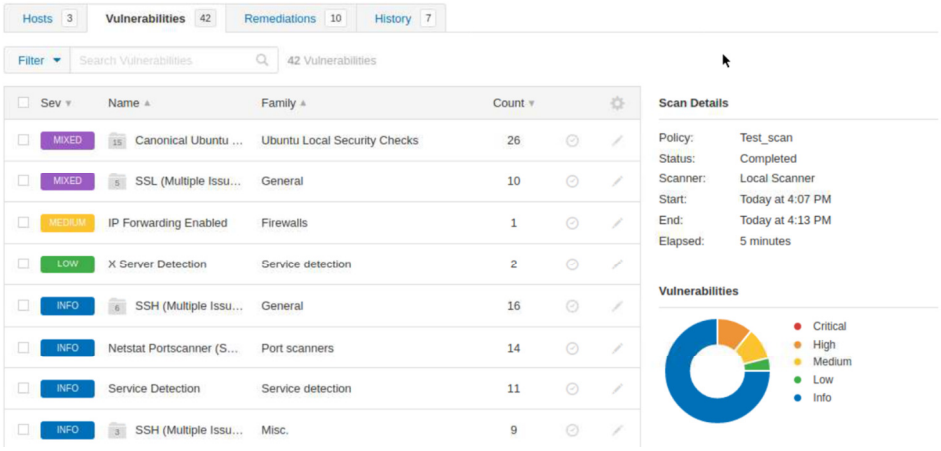
18. Enter the scan name and desired addresses. Save changes and go back.



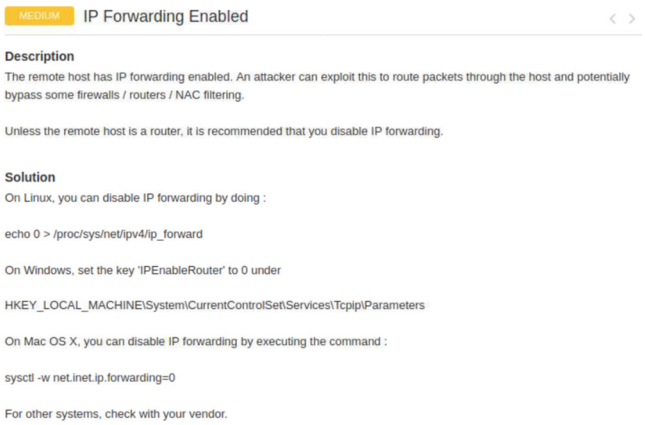
19. Select the created scan and run it as shown in the figure.



20. After the scan is complete, you can read the report details by clicking on the completed scan. You can see the hosts found in the Hosts tab, as well as the scan details in the *Vulnerabilities* tab.



21. By clicking on the found weakness you can see the details of the weakness and the recommendations for resolution.



22. Selecting *Export/HTML* generates an *HTML* document with a detailed report.

NOTICE FOR STUDENTS

Topics of this laboratory exercise may involve the study of various mechanisms that violate information security and make intrusions into computer systems and networks.

The application of these mechanisms when executed towards the systems of individuals and legal entities, which are not familiar with them and are not consentient with the activities on checking vulnerability and testing intrusions into their systems, is punishable under the Criminal Law of the Republic of Serbia (Articles 298 to 304a).

Students performing this laboratory exercise may use these methods for study purposes only within the closed laboratory environment provided for teaching the Advanced Network and System Security course and described in Network Security Laboratory (NS Lab) Design and Hybrid NS and Crypto Lab Implementation documents available at: https://isses.etf.bg.ac.rs/labs/

Students may not imply that they are in any way encouraged or that they are recommended to use these methods toward systems of any third party entity or individual.

Any eventual activity that a student would undertake using these methods and mechanisms according to systems that are not within the laboratory on the course is the sole responsibility of the student.