CySeT - Security Testing Report

Security Scan Report

12/6/22

Disclaimer:

To protect plants, systems, machines, and networks against cyber threats, it is necessary to implement and continuously maintain a holistic, state-of-the-art security program. In such a program, the Software reports and suggests only one element. It is your responsibility to prevent unauthorized access to systems, machines, and networks that should only be connected to an enterprise network or the internet if and to the extent that such a connection is necessary, and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. Periodically, CySeT and/or its licensors update the Software. Such Updates should be applied as soon as they are available and the latest version should be used. Faultiness in reports generated may be increased by using outdated Update versions and failing to apply the latest Updates. In order to stay on top of the latest security threats, patches, and other related measures, CySeT encourages you to use the generated report as a means of keeping up with public security advisories.

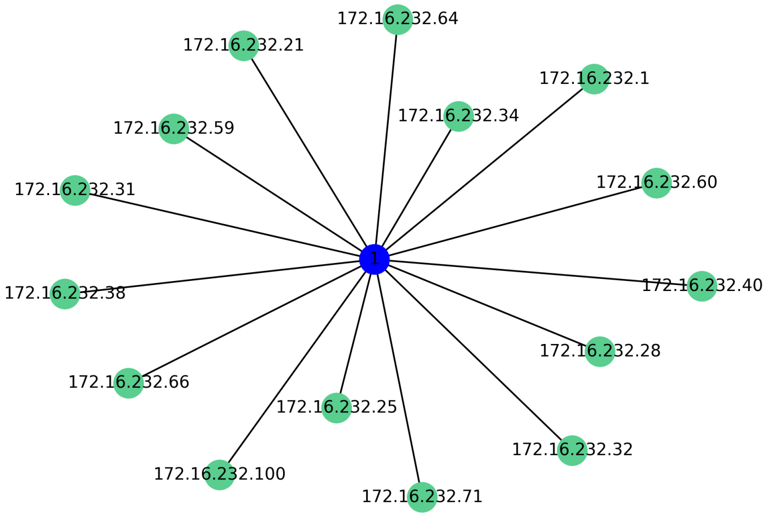
Note: It is important to note that even if the report indicates that the system is 100% safe, it does not necessarily mean that you are safe. Make sure you are protected from cyber threats, they are everywhere.

Scans Results:

The below figure and tables represent the results of the scan that was conducted to test the security of the system provided. Please note that, these results might not be 100% accurate and the figures were purposefully made for a better understanding.

1. Host Discovery:

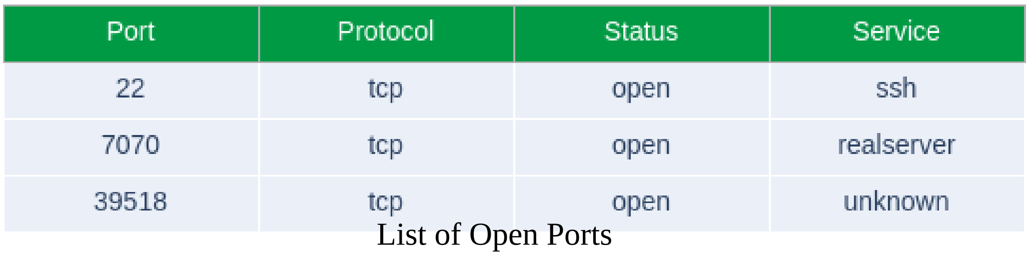
The scan is made on the network to identify the devices that are active on the network. The scan found these devices on your network. The figure visualizes the devices that are connected to your network.



Network Diagram

2. Open Ports:

The device was scanned for open ports, which resulted in the following table. The table depicts the ports that are open, the protocol in use and the services that are currently running. List of suggestive measures can be found in section x.x.

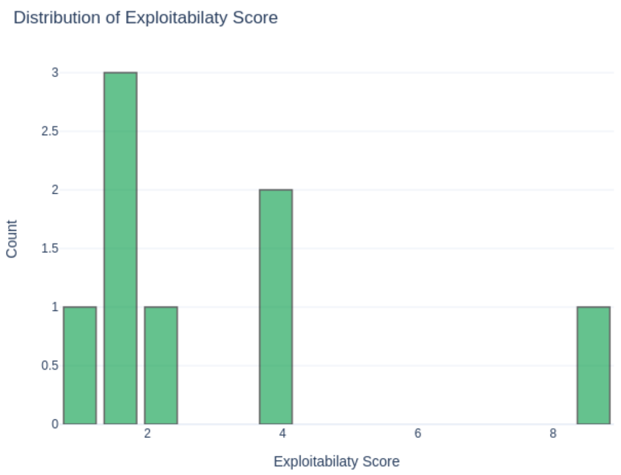


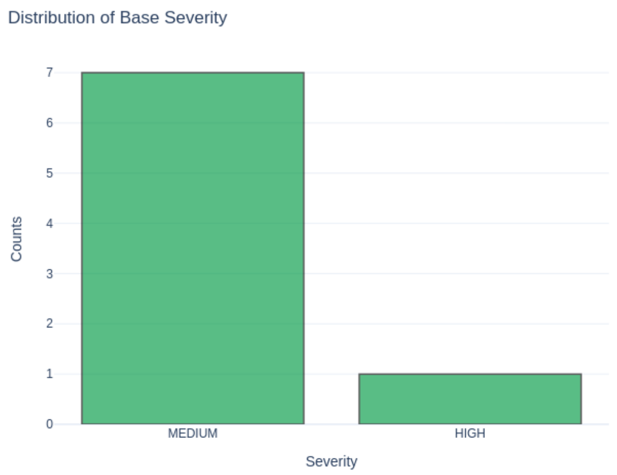
Port	Protocol	Status	Service
22	tcp	open	ssh
7070	tcp	open	realserver
39518	tcp	open	unknown

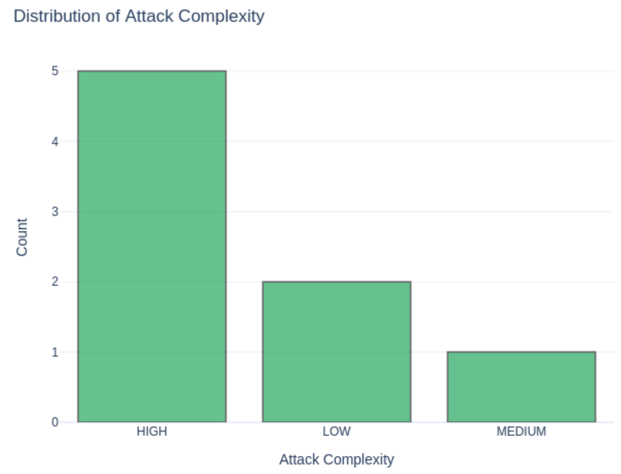
List of Open Ports

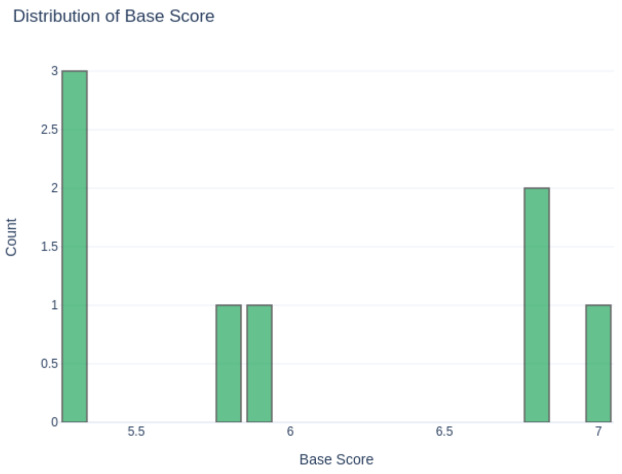
3. Vulnerabilities found:

The device is scanned for vulnerabilities, the following visualizations depict the severity of the vulnerabilities that are present in the system using various metrics.

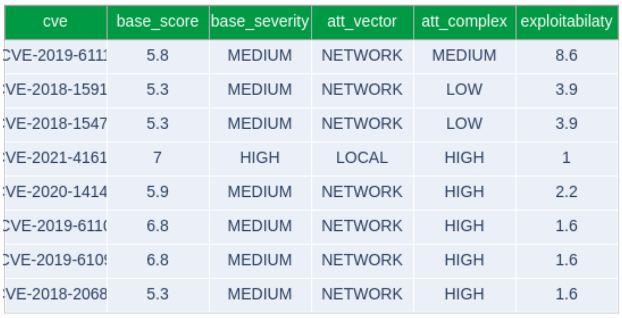








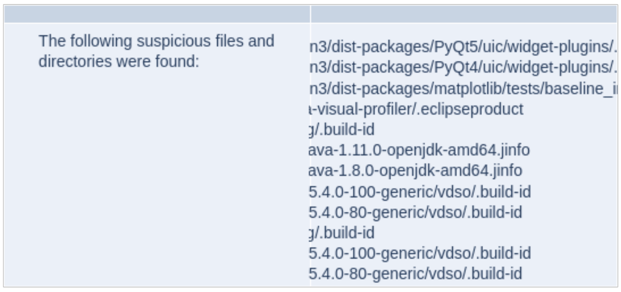
The vulnerabilities present in the scanned system are summarized in the following table.



cve	base_score	base_severity	att_vector	att_complex	exploitabilaty
CVE-2019-611	5.8	MEDIUM	NETWORK	MEDIUM	8.6
VE-2018-1591	5.3	MEDIUM	NETWORK	LOW	3.9
VE-2018-1547	5.3	MEDIUM	NETWORK	LOW	3.9
VE-2021-4161	7	HIGH	LOCAL	HIGH	1
VE-2020-1414	5.9	MEDIUM	NETWORK	HIGH	2.2
CVE-2019-611	6.8	MEDIUM	NETWORK	HIGH	1.6
CVE-2019-610	6.8	MEDIUM	NETWORK	HIGH	1.6
VE-2018-2068	5.3	MEDIUM	NETWORK	HIGH	1.6

4. Rootkit Scan:

The system is scanned to detect if there is any presence of rootkit (malware program) that can be used to compromise the device controls. The findings or result of the rootkit scan conducted is depicted below in the form of a table.



The following suspicious files and directories were found:	n3/dist-packages/PyQt5/uic/widget-plugins/. n3/dist-packages/PyQt4/uic/widget-plugins/. n3/dist-packages/matplotlib/tests/baseline_i -visual-profiler/.eclipseproduct g/.build-id ava-1.11.0-openjdk-amd64.jinfo ava-1.8.0-openjdk-amd64.jinfo 5.4.0-100-generic/vdso/.build-id 5.4.0-80-generic/vdso/.build-id g/.build-id 5.4.0-100-generic/vdso/.build-id 5.4.0-80-generic/vdso/.build-id