Whitepaper

Network Security of Scan2Net Scanners

Abstract

All Scan2Net scanners, like all Bookeye and WideTEK scanners as well as OEM versions of these, have a network connection to communicate with local hosts and resources on the company's network of the end-user. Since all resources connected to a network could potentially be at risk for a virus, malware, phishing and other attacks by Hackers, the user must be aware of this and should consult the network administrator to protect the scanners against any attacks.
To evaluate the risk, many penetration tools are available, but the results can be misleading without further research. This white paper will outline the security features Scan2Net scanners have and will also explain why some penetration tools might report security risks that are not accurate.

Title	Network Security of Scan2Net Scanners
Revision	1.0
Date:	01.07.2022
Category	White Papers
Owner	Image Access GmbH, Germany
Authors	TI

1. Confidentiality

Status	Interested Party	Source	PDF
Public Information	Image Access Support	Yes	Yes
	Authorized Service Providers	No	Yes
	Image Access Customers	No	Yes

2. Revision History

Date	Rev.	Name	Description of Change	Reason of Change
21.06.2022	1.0	TI	Initial Version	

3. Table of Contents

4. References

Ref.	*Document*	*Content*
[1]	*www.debian.org/*	*Debian is an operating system and a distribution of free software. It is maintained and updated through the work of many users.*
[2]	*https://www.youtube.com/watch?v=UH-yZVweZkY&t=5s*	*IT-security of Scan2Net Scanners. YouTube video describing the security concept of Scan2Net scanners.*
[3]		
[4]		

5. Scope

This document will describe how Scan2Net scanners network security is achieved and maintained. It will also explain how to interpret the reports from various penetration tools.

6. Introduction

All Scan2Net scanners, WideTEK, Bookeye and OEM brands, have one thing in common: The core of the scanner's internal firmware is a Linux based system. Today (06/2022) the current version of the Linux is a Debian 10.12 distribution. This version is a stable version and is fully supported in respect to security fixes and the user can patch it via the Debian website at any time with an internet connected scanner. Whenever the support of a stable Linux distribution ends, we will upgrade to a newer distribution after extensive testing.

It should be noted that the scanners are very fast and therefore the Linux and all other software must be thoroughly tested for its real time behavior and performance. This implies that we will not always install the latest and greatest software but only fully tested and specified versions of the Linux system.

7. Difference between a Scanner and a PC

In a PC environment, there will be at least one user with admin rights and maybe other users with limited rights. Since these users actively go into the Internet and can also actively download malicious code through e-mails extensions, infected web sites, USB sticks and other means, they themselves and their conscious or unconscious behavior pose a security risk. If you run a Linux PC, the risk is significantly reduced because most attacks are run against Windows based systems. A PC environment whether Windows or Linux based is in stark contrast to the architecture of the Scan2Net-scanners firmware.

The scanner basically behaves like a web server, of which there are hundreds of millions found on the Internet. It can be accessed through the network using standard TCP/IP protocols and its HTML based graphical user interface called GUI. All scanner functions are accessible this way. In contrast to a PC, you cannot login to the scanner´s Linux under normal circumstances. The software that is presented to a user like the ScanWizard has the lowest user rights on the Linux system.

The scanner being a web server also allows users to login like a User, Poweruser and Admin. This is not the same as login into Linux because these users are shielded through the software from any access to Linux. It can be thought of as the login to an internet store with your personal credentials which does not mean that you are logged into the operating system.

This architecture greatly reduces the risk to open any backdoors into the scanner, as compared to standard workstations. Almost all exploits need a user interaction with access rights to the operation system, which does not happen in the scanner firmware. Also, a typical Scan2Net scanner will only be visible in the Intranet and all attacks can typically only come from inside the network that the scanner is connected to.

NOTE!	**Scan2Net scanners are like web servers and not like PCs. There is no login into Linux from the outside, reducing the risk of injecting malicious code by users into the system to almost zero.**

8. Penetration Testing

Penetration testing is a process used to simulate an attack against one's own system, in this case against a Scan2Net scanner. The goal of this controlled and monitored attack is to collect as much data as possible and uncover security vulnerabilities. A penetration test actually performs the attack under observed conditions. We at Image Access perform these tests on a regular basis to keep our scanners safe.

Penetration testing does not refer to a predefined process to simulate an attack but is rather an umbrella term to summarize different practical attack methods. In addition, a Pen Test should be separated from a Vulnerability Assessment, as the latter is primarily a scan and assessment of security mechanisms.

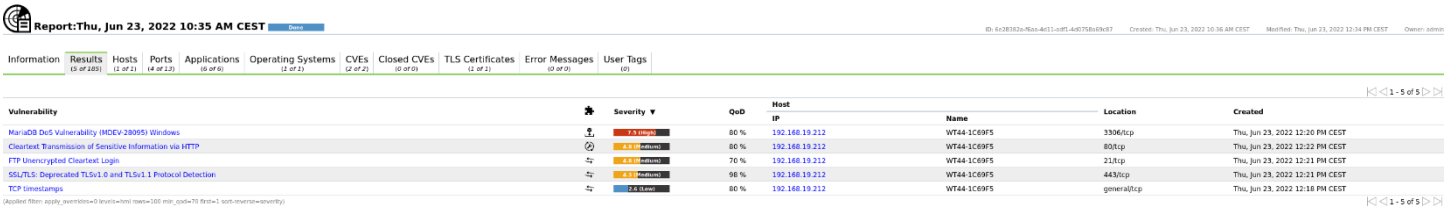
A Vulnerability Test is also performed on a regular basis. Among other things these tests check many thousands of known CVEs. Many of these tests may report vulnerabilities incorrectly, i.e. when they do not analyze the patch level. For example, a CVE scan finds Apache HTTP Server 2.4.37 and reports the **CVE-2019-0215**. In a case described in chapter 9.6, this happened but it could be proven that the security patch performed earlier did actually remove this vulnerability.

As a result, any problems reported by a penetration test or a CVE scan should be further evaluated for relevance in general and also for the relevance in the specific scanner environment.

NOTE!	**Do not accept the results of a penetration test or a CVE scan and declare the scanner unsafe without evaluating the findings for their relevance.**

9. Results of a Penetration Test

A penetration test was performed with OpenVAS / Greenbone Security Assistant 21.4.3 with today's (June 24, 2022) update of the Network Vulnerability Testing Patterns in the Full and Fast configuration on a WideTEK 44 - 600 with firmware 7.30 and a previously upgraded Linux. After two hours of penetration, the following result was obtained:



Report:Thu, Jun 23, 2022 10:35 AM CEST

Information | Results (5 of 185) | Hosts (1 of 1) | Ports (4 of 13) | Applications (6 of 6) | Operating Systems (1 of 1) | CVEs (2 of 2) | Closed CVEs (0 of 0) | TLS Certificates (1 of 1) | Error Messages (0 of 0) | User Tags (0)

1 - 5 of 5

Vulnerability	Severity ▼	QoD	Host IP	Name	Location	Created
MariaDB DoS Vulnerability (MDEV-28095) Windows	7.5 (High)	80 %	192.168.19.212	WT44-1C69F5	3306/tcp	Thu, Jun 23, 2022 12:20 PM CEST
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %	192.168.19.212	WT44-1C69F5	80/tcp	Thu, Jun 23, 2022 12:22 PM CEST
FTP Unencrypted Cleartext Login	4.8 (Medium)	70 %	192.168.19.212	WT44-1C69F5	21/tcp	Thu, Jun 23, 2022 12:21 PM CEST
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	192.168.19.212	WT44-1C69F5	443/tcp	Thu, Jun 23, 2022 12:21 PM CEST
TCP timestamps	2.6 (Low)	80 %	192.168.19.212	WT44-1C69F5	general/tcp	Thu, Jun 23, 2022 12:18 PM CEST

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

1 - 5 of 5

As a result, 5 out of 185 results were assessed as vulnerabilities. These must be evaluated further to determine whether these potential vulnerabilities do play a role in the Scan2Net environment. Let us investigate the details:

9.1. MariaDB DoS Vulnerability (MDEV-28095) Windows

Description: https://security-tracker.debian.org/tracker/CVE-2022-27448
Solution: None
Severity: Not a real problem in a Scan2Net scanner.

To produce the crash of the database you must perform a *multi update* with *implicit grouping*. Although the firmware of the scanner uses a database, it is not exposed to any external user. The Login and password are only known to the machine and are encrypted with a 128bit key. Furthermore, we do not use multi-updates and even if all this would not prevent someone exploiting this vulnerability, no access to secret data will be granted. Instead, the system crashes and as a result must be rebooted.

9.2. Cleartext Transmission of Sensitive Information via HTTP

Description: The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.
Solution: Block port 80 in the firewall setup of the scanner or redirect HTTP requests to HTTPS requests
Severity: An avoidable problem in a Scan2Net scanner.

The customer's admin should ensure that communications with the scanner are using https instead of http.

9.3. FTP Unencrypted Cleartext Login

Description: The remote host is running an FTP service that allows cleartext logins over unencrypted connections.
Solution: Block port 21
Severity: An avoidable problem in a Scan2Net scanner.

The customer's admin should ensure that nobody uses unencrypted connections to the scanner or blocks port 21 when FTP server on the scanner is not used at all.

9.4. SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Description: It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
Solution: Use TLSv1.2 and TLSv1.3 on the host.
Severity: Very low.

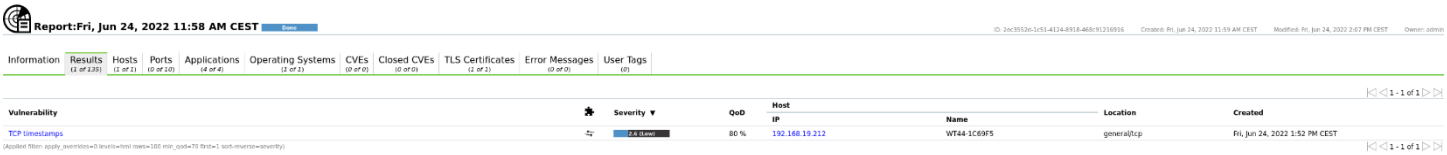
The customer's admin should ensure that nobody uses TLSv1.0 and/or TLSv1.1 protocols in communication with the scanner. The depreciated older versions are still running on the scanner for compatibility reasons.

9.5. TCP timestamps

Description: The remote host implements TCP timestamps and therefore allows to compute the uptime.
Solution: None
Severity: None

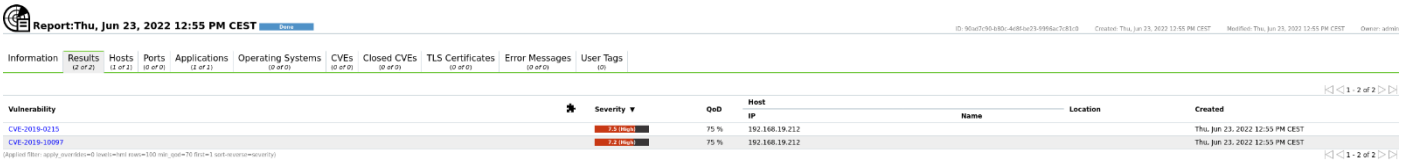
The uptime of the scanner is no secret and is available to all users in ScanWizard or on the touch control screen.

After the beforementioned solutions were implemented, the penetration test report looked like this:



9.6. CVE Test

The next test was the CVE test, which reported two vulnerabilities which the test flagged because of the Apache server's version number. Both have been fixed through the previous Debian update, but the tool did not take the patch level into consideration.



CVE-2019-0215 In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod_ssl when using per-location client certificate verification with TLSv1.3 allowed a client to bypass configured access control restrictions. Status in 2.4.38-3+deb10u7: fixed, https://security-tracker.debian.org/tracker/CVE-2019-0215

CVE-2019-10097 In Apache HTTP Server 2.4.32-2.4.39, when mod_remoteip was configured to use a trusted intermediary proxy server using the "PROXY" protocol, a specially crafted PROXY header could trigger a stack buffer overflow or NULL pointer deference. This vulnerability could only be triggered by a trusted proxy and not by untrusted HTTP clients. Status in 2.4.38-3+deb10u7: fixed, https://security-tracker.debian.org/tracker/CVE-2019-10097

Solution: None because it is already fixed
Severity: None

NOTE!	**Scan2Net scanners are very safe and any remaining safety concerns could be addressed via changing various network settings in the scanner.**

10. Isolate Scanner Network from Intranet

Another way of making sure only one user can work with the scanner, is a private network. Connect the scanner to a second network port and establish a point-to-point connection with the scanner. The disadvantage of this configuration is, that the scanner can only transfer data to the local computer and not directly to a resource in the Intranet.

11. Further Information

For more information see our Internet Security Video found on our YouTube channel.

End of document