
Joonas Piironen

# Preliminary Lansweeper integration testing for IT & OT asset management

Metropolia University of Applied Sciences

Bachelor of Engineering

Information and Communication technology

Bachelor's Thesis

16 March 2023

## Abstract


| | |
|---|---|
| Author: | Joonas Piironen |
| Title: | Preliminary Lansweeper integration for IT & OT asset management |
| Number of Pages: | 34 pages |
| Date: | 16 March 2023 |
| Degree: | Bachelor of Engineering |
| Degree Programme: | Information and Communication technology |
| Professional Major: | Smart IOT - Systems |
| Supervisors: | Kimmo Sauren, Head of major |


---


The objective of this bachelor's thesis was to devise a plan for integrating and implementing two distinct software tools, namely Lansweeper IT and OT, for daily use by the company. The primary purpose of the software's are to serve as both an inventory asset management tool and a network utility tool. To achieve this goal, the software's needs to be set up in a manner that automatically updates the asset inventory in the event of any changes to the listed assets. Additionally, it should alert the IT team if any new devices are detected on the company networks. This thesis was created for AB Enzymes OY.

The beginning of this thesis provides an overview of the software to be implemented and highlights the differences between the two available versions. The second part of the thesis is focused on introducing the network setup in which the deployment will take place.

The third part provides insight into the possible security impacts regarding the implementation of the software

In the final section of the thesis, the plan for the implementation of the permanent sensor into the different networks will be discussed, along with recommendations based on the findings that were made during the original discovery phase.



Keywords: Lansweeper, CMDB, OT

## Tiivistelmä


| | |
|---|---|
| Tekijä: | Joonas Piironen |
| Otsikko: | Alustava Lanseeper IT & OT -ohjelmiston integrointi ympäristöön |
| Sivumäärä: | 34 sivua |
| Aika: | 16.3.2023 |
| Tutkinto: | Insinööri (AMK) |
| Tutkinto-ohjelma: | Tieto- ja viestintätekniikan tutkinto-ohjelma |
| Ammatillinen pääaine: | Älykkäät IoT -järjestelmät |
| Ohjaajat: | Kimmo Sauren, Head of major |


---


Tämän insinöörityön tavoitteena oli laatia suunnitelma Lansweeperin IT- ja OT-versioiden integroimiseksi yrityksen päivittäiseen käyttöön. Ohjelmistoa on tarkoitus käyttää yritysten laitteiden tietokannan ylläpitoon sekä verkon ylläpidon apuvälineenä. Ohjelmisto on tarkoitus asentaa siten, että se päivittää tietokantoja automaattisesti, jos luetteloituun omaisuuteen tulee muutoksia, ja myös varoittaa IT-tiimiä, jos yrityksen verkossa havaitaan uusia tuntemattomia laitteita. Tämä opinnäytetyö tehtiin AB Enzymes OY:lle.

Opinnäytetyön alussa luodaan yleiskatsaus asennettaviin ohjelmistoihin ja tuodaan esiin kahden saatavilla olevan version väliset erot. Opinnäytetyön toisessa osassa keskitytään esittelemään verkkoasetelma ja ympäristö, jossa käyttöönotto tapahtuu.

Kolmannessa osassa perehdytään ohjelmiston integroinin mukana tuleviin mahdollisiin tietoturvariskeihin.

Opinnäytetyön viimeisessä osassa käsitellään suunnitelmaa pysyvien antureiden käyttöönotosta eri verkkoihin sekä annetaan suosituksia, jotka perustuvat alkuperäisen selvitysvaiheen aikana tehtyihin havaintoihin. Dokumentointia käyetään perustana ohjelmiston käyttöönottossa yrityksessä.



Avainsanat: Lansweeper, CMDB, OT

## Contents

List of Abbreviations

# Contents

## List of Abbreviations

| | |
|---|---|
| IT: | *Information Technology*, includes devices such as desktops, laptops and printers |
| OT: | *Operation Technology,* operational devices such as machines and sensors |
| IP: | *Internet Protocol,* the logical address a device has in a network |
| SQL: | *Structured Query Language,* a form of database structure |
| PC: | *Personal Computer,* computers such as laptops and desktops |
| LAN: | *Local Area Network,* the wired network |
| OS: | *Operating System,* software that manages all of the other application programs in a computer. |
| DMZ | Demilitarized Zone, a restricted subnet that is usually the gateway to the internet |
| MAC: | *Media Access Control,* physical address of a device |
| WLAN: | *Wireless Local Area Network,* The wireless network |
| AP: | *Access Point*, a wireless router that can provides internet access |
| PING: | *Packet Internet Groper,* a protocol used to query other devices |
| DNS: | *Domain Name System,* a protocol that automatically assigns free addresses to devices |

CIDR: *Classless Inter Domain Routing,* a way of marking down the range of addresses available

ARP: *Address Resolution Program,* used to discover the MAC address of a device by using the IP address

DHCP: *Dynamic Host Configuration Protocol,* a protocol that assigns unused IP addresses to devices on the network.

CMDB: *Configuration Management Database,* a general term meaning the database where the company stores their asset information.

# 1 Introduction

Managing an up-to-date inventory of IT assets is a complex task that poses a challenge for any company. This task becomes even more challenging when the assets include devices that need to be kept offline or behind a network that has no access to the internet. In such cases, it is difficult to maintain an accurate and up-to-date inventory.

Many companies rely on manually updated databases to keep track of their IT assets. However, such databases tend to be left un-updated for longer periods of time, until someone takes the initiative to go through all the assets. This approach can be very time consuming and is often done only when absolutely necessary due to time constraints.

Automating the process of upkeeping the devices for data about their status and plausible security, hardware or software issues would solve this and make managing an asset inventory much simpler. This approach would streamline the process of maintaining an asset inventory and make it more efficient. Additionally, by concentrating the data into a single application for diagnostics the process of diagnosing and resolving issues is simplified.

The purpose of this thesis is twofold: first, to provide an initial discovery and planning document for the implementation of Lansweeper IT & OT into the environment, and second, to offer recommendations for the permanent integration of the software sensors in the environment. Furthermore, it is intended to provide insights and best practices for ongoing asset management to improve efficiency and accuracy in maintaining an up-to-date inventory of IT assets.

# 2 Lansweeper

Lansweeper is an IT asset management tool and platform developed by a Belgian company of the same name. The platform helps you keep track of all the devices that are or have been connected to a specific or larger part of the network. It does this by either passively collecting and organising all the data that assets send across the network or actively polling the network to find connected assets. Lansweeper can be used by installing physical or virtual sensors into the environment. The sensors can be accessed remotely through the cloud platform that they have been synchronized with or locally via the software that is installed onto the sensor device. [1.]

The physical sensors are devices such as desktops or laptops which have the software installed onto them and are configured to probe the network. Virtual sensors are the same as physical sensors but installed onto VM’s or servers. In practice there is little to no difference in the way the software operates regarding where it is installed. [2.]

Scanning on both versions of the software follows the same principle. First a new scan is created. The scan is then given the protocols that it is to query when the scan is ran. In the IT version the protocols range from querying AWS or Azure regions to pinging a pre-determined IP-range. In the OT version of the software the protocols are chosen to communicate with the devices using the correct type of communication protocol as the devices may not reply if not queried using the correct one. [ 2; 3.]

These sensors scan the pre-configured LAN range and update the asset list inventory. The scanned asset inventory can be used to see what software is running on which device and to which networks the devices are connected. Lansweeper uses either a local SQL database or a server hosted SQL database to store the collected assets. Lansweeper can also be used to manage licenses, track software updates and patches, and monitor network performance. [1; 2; 3.]

After running a scan with Lansweeper, the assets are collected onto a locally hosted database. The software will begin to synchronize the collected assets to the cloud platform when it detects that an internet connection is available. [2.]

## 2.1 Lansweeper IT

The IT version of Lansweeper is mainly developed to scan and inventory the more commonly used IT assets, such as PCs, printers, and access points. Scanning these devices provides valuable information about the assets that have been scanned. The IT version of Lansweeper can extract specific information from these devices, such as installed software and license keys used for the software. The depth of the information that is extracted varies based on what kinds of access rights the sensor device is given. For example if the sensor is authenticated to access the company AD it would be able to provide more detailed descriptions of the users and devices that it can find listed.

In addition to detecting physical devices connected to the network, Lansweeper can obtain essential information about the assets such as the OS version, hostname, MAC address, and last logged-in user. This information is valuable when forming a database of assets, and it can be used to identify devices that are outdated, have not been updated with the latest patches and software, or are at risk of vulnerabilities. See figure 1 on the next page that illustrates how the asset inventory is displayed once it has been scanned.

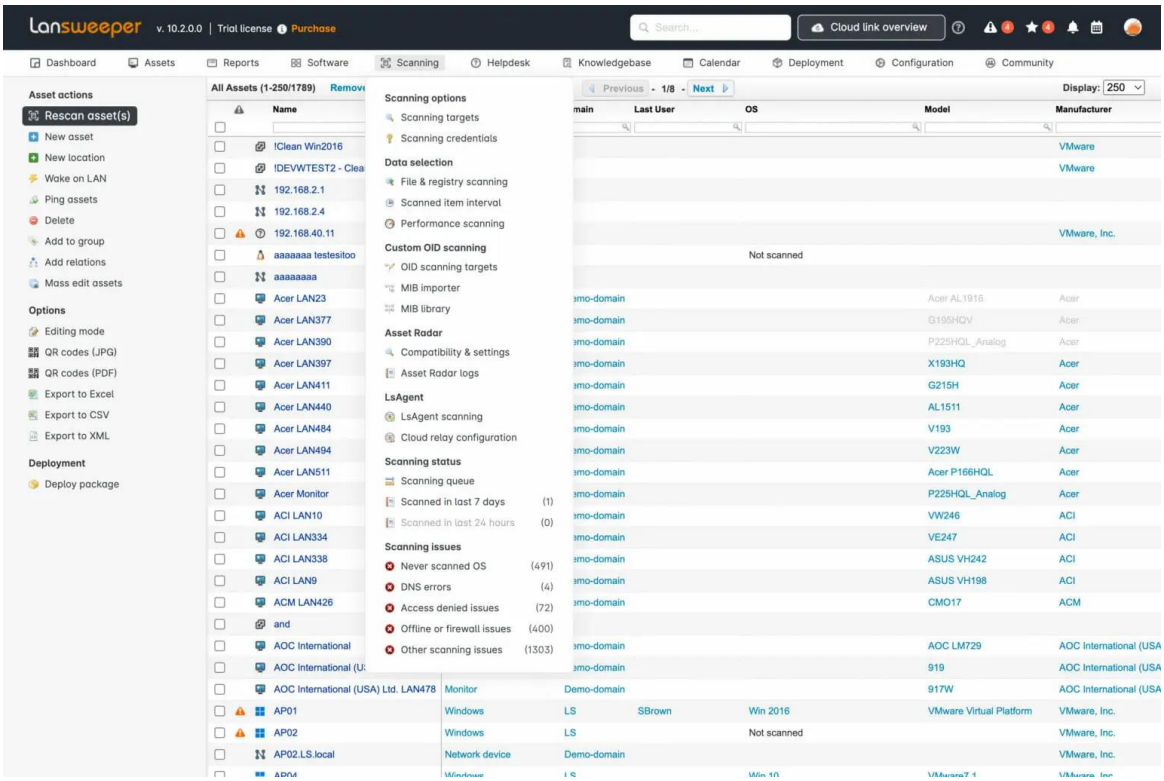


Figure 1. Lansweeper IT user interface.

Moreover, Lansweeper can help detect and identify unauthorized or rogue devices on the network. By continuously scanning the network and comparing the results against the database of known assets, it can alert network administrators when a new device is detected that does not match any known assets. [2.]

## 2.2 Lansweeper OT

The OT version of Lansweeper is more focused on the Operational technology side. As OT devices tend to use more specialized communication protocols in some cases the communication protocols are completely proprietary to the company that has developed the device. In such cases the standard IT focused version of Lansweeper may be insufficient. The more specialized version of the software includes libraries that have several communication protocols encoded

into it. The software can detect the manufacturer of the device and choose the right form of protocol to use for the communication. [4; 5.]

In addition, OT devices are more sensitive to the active scanning methods that are commonly used with the IT version. Using active scanning in an OT environment may result in additional network load that can cause communication errors with the devices.

The Lansweeper OT features Selective probing which provides a middle ground for discovering OT assets. Selective probing queries serially with sufficient time between the queries to validate a safe communication. This type of querying with a delay, reduces concurrent traffic load and helps to ensure that the devices do not get overloaded with commands thus further preventing the possibility of a communication error between a host and the device itself. [5; 6.]

After being scanned the assets, sensors and scan targets can be seen in the Lansweeper OT interface as can be seen in the overview in figure 2.

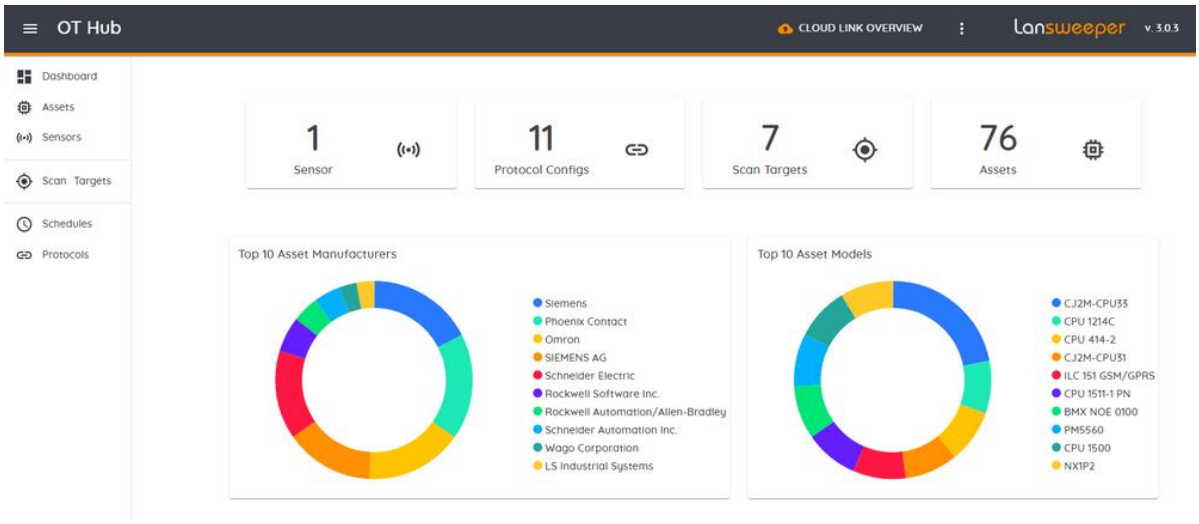


Figure 2. The Lansweeper OT homepage.

# 3 Networking

## 3.1 Subnets

A subnet, or subnetwork, is the technique for logically partitioning a single larger network into smaller subnetworks that connect devices based on the IP address and subnet mask. Each subnet has its own unique subnet mask and IP address range. Dividing a larger network into two smaller networks is depicted in figure 3. [7.]

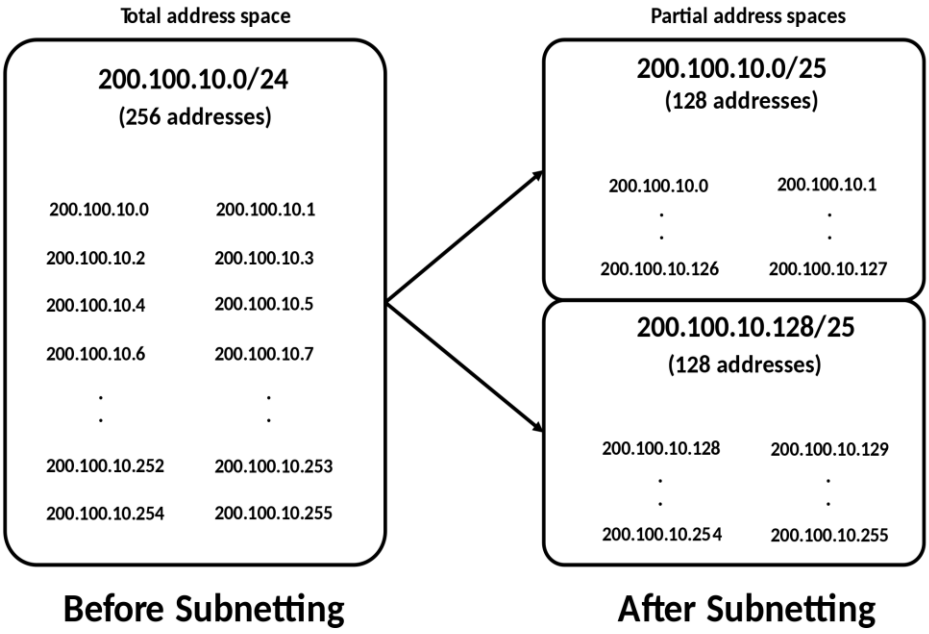


Figure 3. Splitting a single network containing 256 addresses into two smaller networks with 128 addresses. [8]

Dividing a network has several advantages over having one large network.
The main advantages are reduced network congestion and increased network security. By dividing traffic between specific parts of the network, subnetting can reduce network load and prevent traffic congestion. Devices within a subnet can communicate directly with each other, reducing the traffic that is routed through

a router. Subnetting additionally helps to efficiently allocate IP addresses and prevent large numbers of IP addresses from going unused. [7; 9.]
In addition, subnetting allows traffic to travel shorter distances to reach its destination by avoiding routing through unnecessary routers. This can result in faster communication an improved network performance. [9.]

## 3.2 DMZ

A DMZ, or demilitarized zone, is either a physical or logical subnet that acts as a buffer between a company's internal network and the public internet. The purpose of a DMZ is to improve network security by providing a secure, controlled environment for hosting public-facing assets, such as web or email servers.

Usually, a DMZ is set up using either one or two firewalls. More firewalls can be added and configured and even several DMZs can be deployed in the same network to further increase network security from external threats. However, setting up a single DMZ with two firewalls is the most cost-effective solution for most implementations. [10.]

**Single firewall**
A more modest approach to network architecture involves using a single firewall, with a minimum of three network interfaces.
Three network interfaces are required as a minimum for the system, as one is allocated for external traffic, another for internal traffic, and a third for the DMZ.

Demonstrated in Figure 4 is the DMZ placed behind a single firewall configuration, making the firewall a central hub for the flow of traffic between the internal network, external network, and the DMZ.

While this design can be cheaper and more straightforward, it also increases the risk of network failure as the firewall becomes the sole point of failure for the entire network. This can be seen visualized in figure 4. [10.]

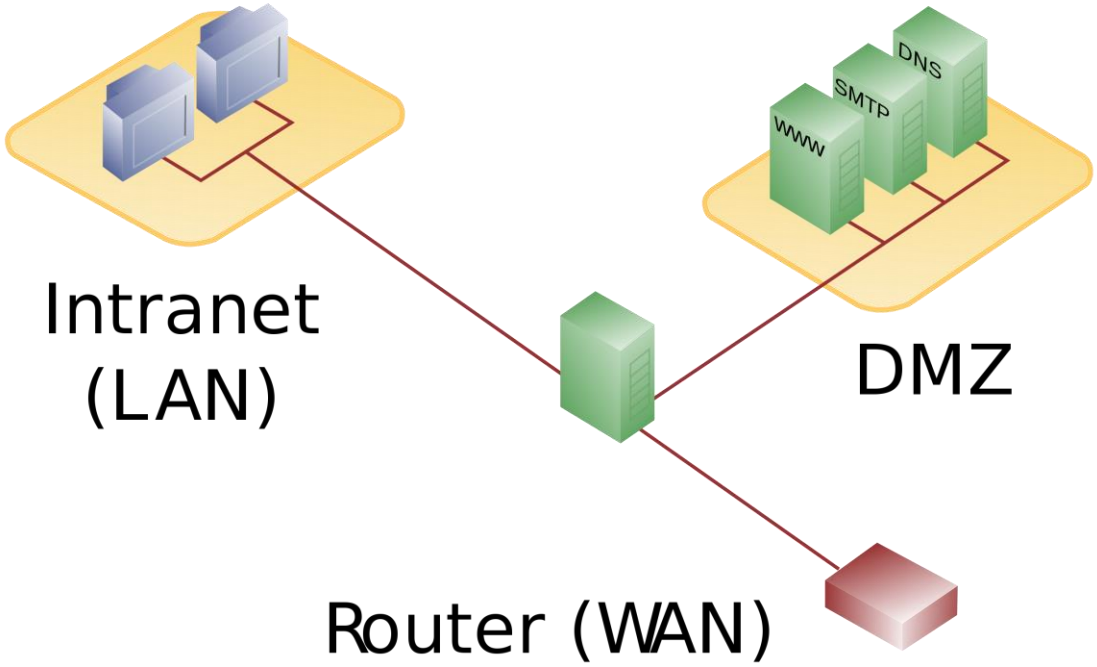


Figure 4. A network where the DMZ has been configured with a single firewall that acts as the central hub for all communications. [11]

As apparent in figure 4. the firewall becomes a chokepoint for all traffic passing through the network. Therefore, when designing the environment, one must consider that the single firewall must be capable of handling all the network traffic load from incoming and outgoing traffic, to ensure that both the internal network and the DMZ are protected and accessible. [10; 12.]

**Dual firewall**

A more secure approach is to employ two firewalls to form the DMZ. The first firewall which is referred to as the “frontend” firewall is configured to only allow traffic that is destined for the DMZ. The second firewall which is referred to as the “backend” firewall is configured to be only responsible for the traffic in the DMZ that is destined for the internal network. Additionally, this configuration helps

distribute the network load, reducing the risk of congestion and performance degradation. An example set up of a dual firewall DMZ can be seen in figure 5. [10.]

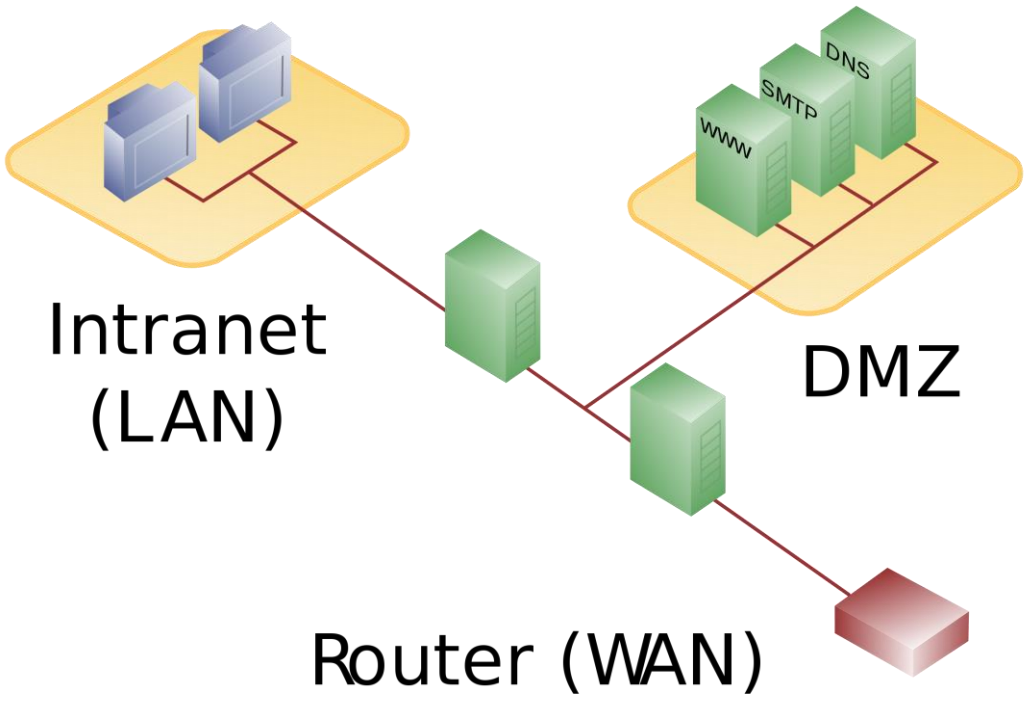


Figure 5. A network where the DMZ has been configured with two separate firewalls. [11]

Incoming external traffic is first routed through the external firewall to the DMZ then to the appropriate server e.g.: Emails are routed to the company's email server. Internal communications with servers should only be in contact with the internal facing firewall. Allowing the traffic to be split depending on the destination, thus reducing the likelihood of network traffic being congested. [12.]

# 4 Company networks

The company has three networks that are a part of the project. Two of the networks, the office network, and the laboratory network, are part of the same network but on different subnets. The third network, the OT network, is a separate network. During the preliminary scanning with the IT & OT versions of Lansweeper, only the laboratory network was scanned.

## 4.1 Office Network

The office network servers as the primary access point for employees to connect to various resources and applications required for their daily work. Including access to network drives, email and most importantly internet access.
This subnet houses a significant proportion of the company's IT assets.

To connect to the company WLAN, a PC must have the company's own version of the Windows image installation. This is done to ensure all devices connected to the network meet the company's security standards and protocols. An out-of-date device is not permitted full access until it has been updated.

## 4.2 Laboratory network

The laboratory network referenced to as the LAB network in the network diagrams, is designed to provide connectivity for a limited number of PC's and other devices that are unable to connect to the regular office network due to incompatibilities with the company's Image installation. The incompatibilities stem from laboratory devices needing their control PC's to be configured in a specific

way. Often the companies ship the control PC’s that have the software ready and configured with the laboratory device.

These pre-installed configurations are usually mandatory for the proper functioning of the laboratory devices, and any changes made to them can potentially cause system failures, incorrect readings or even malfunctions. Additionally, these configurations and software are not always readily available or easy to replicate, which makes it nearly impossible to deploy the device successfully if it is connected to a non-manufacturer provided control PC.

As mentioned before the network primarily hosts laboratory devices that require control PC’s and internet connectivity to function properly. The network does not have DHCP capabilities, meaning all devices connected to the network must be manually assigned a static IP-address.

## 4.3 OT network

The OT network is the production and factory areas network dedicated for the communication of manufacturing devices and systems. While the other networks are subnets of the same network, the OT network is a completely separate network. This separation is a precautionary measure aimed at preventing any accidental interference to the OT devices that maybe sensitive to unnecessary traffic. It also servers to enhance the overall security of the factory side where the devices are located.

The OT network is connected to the company network via a dedicated single firewall configuration DMZ. This configuration enables secure and controlled communication between the OT and company networks while limiting the potential for unauthorized access in case either of the networks are compromised.

# 5 Data collection and initial scans

Although the original plan was to test the IT scanner on the LAB network and the OT scanner directly on the OT network, it was discovered that a few OT devices were connected to the LAB network. To avoid the additional time required to identify and implement the appropriate range and static IP address to configure the sensor to the OT network, it was deemed more efficient to only test both versions of the software on the LAB network. This could be done as the OT devices found on the LAB network were not production critical equipment and were newer models less likely to be interfered with by the active scanning that the IT version of the software uses.

## 5.1 Hardware and software

For the sensor device there were two options to choose from. A HP ProBook G8 650 or a HP EliteBook 855 G8. The former of the two was chosen, mainly since this version of the laptop features an integrated ethernet port. The installation ofor both of the version of software is as easy as downloading their installers and running it. Both the IT and OT versions of the software were installed on the same laptop for convenience of use.

During initial testing, the Lansweeper software was installed on a laptop running the company’s customized Windows image referred to as the BSG version. However, the software crashed unexpectedly and repeatedly, possible due to the security restrictions on the operating system. It was decided that for the duration of the initial testing the laptop would be reinstalled with the OEM version of Windows 10.

## 5.2 Scanning networks with a single sensor

According to Lansweeper documentation, a single sensor device should be capable of scanning the entire network, including all of the subnetworks. [1.]
This would involve installing only one instance of the software, which would be connected to a central point in the network. Ideally, the sensor device should be a virtual installation, allowing it to be installed directly onto the server that the company's network is running from. The sensor would then be programmed to scan all of the IP ranges in the network, providing full visibility of the network.

In practice, however, this approach would require significant whitelisting to enable all traffic to move freely between the networks and reach the sensor. The need to whitelist several addresses and ports creates potential security vulnerabilities since any whitelisted address or port can be exploited by malicious actors.

In summary, while a single sensor device can provide full network visibility, implementing this approach would require significant effort whitelisting everything to ensure all the traffic will reach its destination which in turn can create security vulnerabilities. In addition, if the sensor device fails or goes offline, the entire network scanning process would be disrupted until the issue is resolved. This may result in critical network issues going undetected, potentially leading to downtime, data loss, or other serious consequences.

## 5.3 Initial scanning with IT Lansweeper

Initial scans with the IT Lansweeper were performed on the LAB network. The first steps in setting up the device was to consult the original network chart to figure out the subnets IP-range and subnet mask. Finding the range proved easy as the network chart clearly stated the range for the subnet was of 10.121.101.1/28.

As discussed in more detail in the Lansweeper IT chapter there are several options for the type of protocol that can be used while using the IT scanner. For the initial scan of the network the IP-range scan was used as the purpose of the first scan was to map which addresses were currently in use and by which devices.

The next step was to find an unused IP address in the network that could be given as a static address to the sensor device. This proved to be difficult as the network map used to reference which addresses were already allocated to devices in the LAB network had not been updated for several years.

A method for obtaining a temporary static IP address involved temporarily replacing a device in the laboratory network with the sensor device.
The selected laboratory device was one that not scheduled to be in use at the time of the initial scanning and was connected to the LAB network.
The Lansweeper sensor was assigned the IP-address of the replaced device and was connected to the LAB network via an ethernet cable. The initial scan was ran using the disconnected devices IP-address.

The IT version of Lansweeper is designed to query several addresses and ports simultaneously, which makes the network scanning process much more efficient. Scanning the entire network with the IT version of Lansweeper took only around 4 minutes to complete.

As seen in figure 6 the results from the initial scan provided insight into which IP-addresses had been allocated and which ones were still available to be allocated. The scan allowed the determination of an unused IP-address that could be dedicated to the Lansweeper sensor device.

**Assets without a location (24)**

| AssetName | Domain | Type | IPAddress | Description |
|---|---|---|---|---|
| | | | 10.121.101 | |
| ABEFIDC01 | ABE | Windows | 10.121.101.57 | |
| ABEFIDC02 | ABE | Windows | 10.121.101.67 | |
| ABPULPEYE | WORKGROUP | Windows | 10.121.101.41 | |
| Check Point Software Technologies 10.121.101.129 | | Linux | 10.121.101.129 | |
| DESKTOP-2K7RFB1 | WORKGROUP | Computer | 10.121.101.31 | |
| DESKTOP-R0QV647 | workgroup | Windows | 10.121.101.21 | |
| HP LaserJet 4050 Series | | Printer | 10.121.101.50 | |
| iLO-srv-bio1 | | Linux | 10.121.101.47 | |
| LTW7115 | ABE | Windows | 10.121.101.39 | |
| MC-110557 | WORKGROUP | Linux | 10.121.101.82 | |
| MFCS-ARCHSRV | ABE | Windows | 10.121.101.55 | |
| MFCS-SRV1 | ABE | Windows | 10.121.101.51 | |
| MFCS-SRV2 | ABE | Windows | 10.121.101.52 | |
| MFCS-SRV3 | ABE | Windows | 10.121.101.53 | |
| MFCS-TERMSRV | ABE | Windows | 10.121.101.54 | |
| NP5110A_9463 | | Appliance | 10.121.101.11 | NP5110A |
| NP5110A_9472 | | Appliance | 10.121.101.10 | NP5110A |
| SRV-VEEAM3 | ABE | Windows | 10.121.101.84 | |
| VMware 10.121.101.49 | | ESXi server | 10.121.101.49 | |
| WSW7139 | WORKGROUP | Windows | 10.121.101.30 | |
| ZBR5102901 | | Printer | 10.121.101.17 | ZebraNet Wired PS |
| ZBR5650726 | | Printer | 10.121.101.16 | ZebraNet Wired PS |
| ZBR5960713 | | Printer | 10.121.101.15 | ZebraNet Wired PS |
| ZBR5961440 | | Printer | 10.121.101.13 | ZebraNet Wired PS |

Figure 6. Scan result asset inventory from the Lansweeper IT application scan of the LAB network.

After the disconnected lab device was reconnected to the network, the sensor device was plugged in and given its new static IP-address.

Following the allocation of the previously unused IP-address to the Lansweeper sensor device, a second scan was conducted using the same parameters as in the first scan. As a results of this scan, one additional device that was not in the previous scan had been detected, the device that had been disconnected during the first scanning.

The first successful network scan produced a surprisingly large amount of valuable data about the assets connected to the network. The scan provided detailed information such as the OS version, MAC address, IP address, and manufacturer of most devices. Furthermore, the scan also revealed some interesting details that can be seen in figure 7. such as the ink levels and the number of pages the printer has printed, which highlights the level of information that can be obtained using Lansweeper.

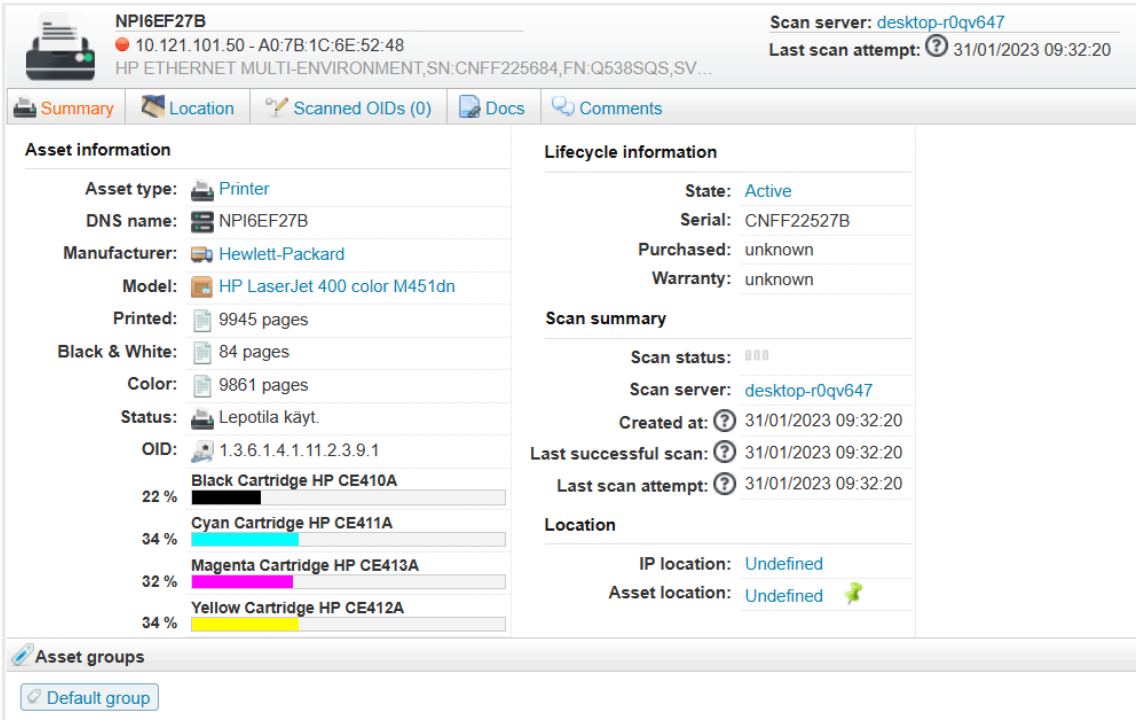


Figure. 7 Asset details page of an HP inkjet printer that was obtained during the initial scan with Lansweeper IT.

## 5.4 Initial scanning with OT Lansweeper

The initial scans for the OT Lansweeper were ran on the LAB network.
The test was ran using the same IP parameters as in the first one using the IT scanner. For the OT scanner the user must also choose what types of protocols they wish to scan for. Consulting the original network chart for information on

what OT devices were known to be on the network, protocols: BACnet, EthernetIP, Modbus, Moxa, Siemens S7-1200/1500, Arp and web port were chosen.

Due to the selective query probing used by the OT scanner, scanning a network can take several hours. By default, the software pings each address three times with a timeout of three seconds using each selected protocol. [6.]

As the OT version of the software is still in the early days of its development cycle there is no indicator for the progression of the scan to the user. The only way for a user to know how long the scan is going to take is to calculate how many protocols and how many ports the scan is set to probe. To make sure all of the selected protocols and addresses in the range were scanned the scan was left to run overnight.

When the scan had finished it had picked several objects that should not have been classified as OT devices. All of the false positives that the software detected were in fault of the Arp protocol that was chosen to be ran in the initial scan. Therefore, the scan was rerun using the same protocols as the first scan but excluding Arp to reduce the probability of receiving false positive detections.
Again, the scan was left to run overnight to make sure all of the queried protocols and addresses had sufficient time to be scanned.
As can be seen in figure 8. the second scan without the Arp protocol provided only 7 results in the environment. All of which were OT devices.

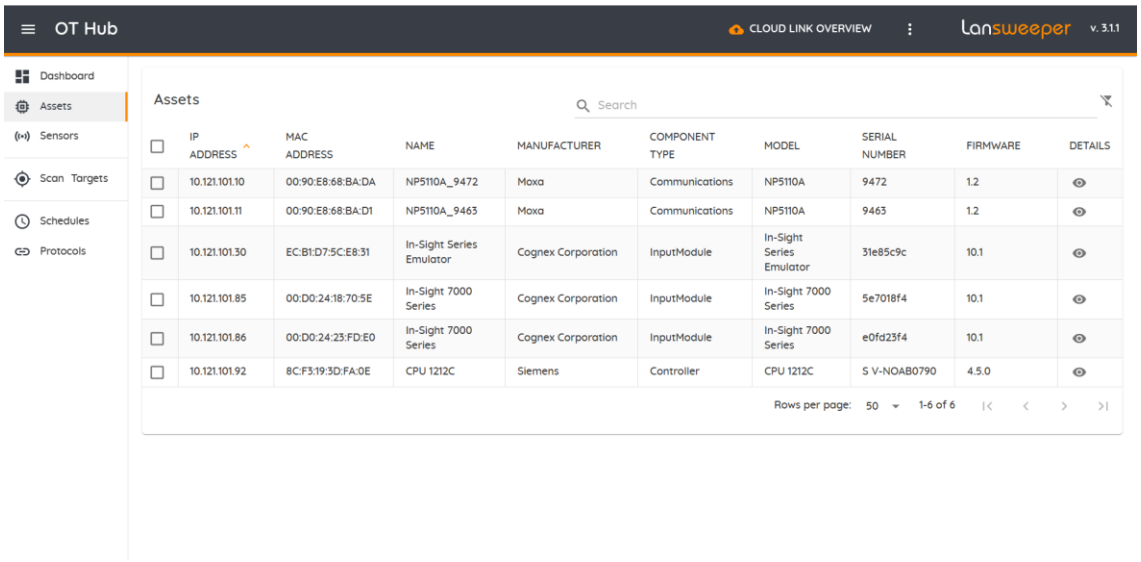


Figure 8. The first successful scan that included only the OT devices using the Lansweeper OT software.

As can be seen in Figure 6, the IT version of Lansweeper was able to detect two of the OT devices, namely the Moxa devices. However, it incorrectly labelled them as household appliances, whereas in figure 8, the OT version correctly categorized them as OT devices. This highlights the differences between the two versions of Lansweeper. While both versions are capable of detecting devices, they are not equally effective at extracting information from devices outside of their intended purpose. The IT version of Lansweeper is designed to inventory and scan more common IT assets, such as PCs, printers, and access points, whereas the OT version is tailored towards detecting and monitoring operational technology devices, such as industrial control systems, programmable logic controllers, and other specialized devices.

# 6 Network security impact

## 6.1 IT & OT network convergence

Due to the intentional design of the company and OT networks, which were implemented to operate independently and restrict communication to only when required, establishing a direct open connection between the two networks is not advisable. Such an action could have significant ramifications. In particular, the OT devices on the network may be overwhelmed with excessive traffic, which could lead to operational failures and disruptions. As such, careful consideration should be given to any connections between these two networks.

Industrial networks such as the OT network, that manage various processes are essential in maintaining operations and generating revenue for organizations. These networks include critical systems like supervisory control and data acquisition systems, distributed control systems, and customized applications. Compromising these systems can have severe consequences for an organization, making them appealing targets for malicious actors. Having the OT network completely cut off from the rest of the network would effectively eliminate these issues.

However, completely cutting off the network is not a recommended solution either. This approach would effectively eliminate all forms of remote management and maintenance capabilities, which are essential in case the devices encounter any errors. Maintaining remote access can significantly reduce downtime and costs associated with having to request external maintenance personnel to diagnose and fix the problem on-site. Moreover, remote access is also necessary to ensure that the devices receive critical software updates and security patches, which can protect the devices and the network from potential cyber threats.

Therefore, a small level of convergence between the networks can provide significant benefits without compromising security. For instance, integrating OT

data using the Lansweeper OT with the cloud platform allows for insights into production processes, equipment performance, and quality control.

With all connections a zero-trust approach should be mandated when connecting the two networks to ensure that the security remains robust on the OT network. Furthermore, with a converged network, organizations can implement a robust security framework that can identify and mitigate potential security threats across both IT and OT systems, ensuring that both networks are adequately protected.

In summary, while there are risks associated with IT/OT convergence, the benefits can be significant, making it a worthwhile investment to enhance operations and improve cybersecurity. However, it is crucial to implement a well-designed and comprehensive strategy that addresses the unique challenges and requirements of both IT and OT networks.

## 6.2 Software access rights

Implementing the base version of either of the Lansweeper software onto the network is a straightforward process that does not require granting the sensor devices any additional access or rights. By connecting the sensor device to the network, it is able to gather a wide range of data that can be useful in network management. In this form of an application the security benefits greatly outweigh the risks.

However, to increase the depth and accuracy of the information provided by the software, it may be necessary to it additional more access rights to the company's network and databases. With these additional rights, the software can provide more detailed insights into the software and versions of client devices on the network. This information is crucial for maintaining an up-to-date inventory of devices and software that are connected to the network. The information can be used for patch management and vulnerability assessment.

In addition to providing data about software and device inventories, the software can also collect data on network traffic, current active users, and other critical aspects of network performance and security. By analysing this data, network administrators can identify potential issues, prevent data breaches, and optimize network performance.

Moreover, with access to the cloud database of known software vulnerabilities, the software can automatically verify if any of the software versions that are running on the network have vulnerabilities that can be exploited. This information would be valuable for prioritizing and addressing vulnerabilities, reducing the risk of the company falling vulnerable to malicious actors.

When granting additional access to the software to improve the quality of the data it provides must not be done without review. It's important to consider that the more permissions a software has, the greater the risk it becomes in the event that the software is exploited.

Granting additional access to the software opens it up to potential exploits such as privilege escalation, which could lead to unauthorized access and potential data breaches. Consequently, it is important to carefully assess all the risks that are associated with granting additional access rights to the software. Also, to ensure that adequate security measures are in place to mitigate the risks that are presented with it.

Any additional access should be granted only if it is deemed absolutely necessary and if the benefits outweigh the potential risks. It's also important to regularly review and update the permissions that are granted to the software to ensure that they remain applicable to the software’s and the company's needs.

# 7 Discussion

## 7.1 Sensor implementation

When taking into consideration the network setup within the project scope, it would be recommended that a minimum of three sensors be utilized to provide a comprehensive scan overview. One of the sensors should be running the standard IT version of Lansweeper, while the second should be running the OT version, and finally the third version should be running both versions.

The first IT sensor should be integrated into the office network, the second sensors with the OT version should be installed withing the OT production environment to ensure comprehensive coverage of the network. Finally, the third sensor running both versions should be installed onto the LAB network.

## 7.2 Office network

When implementing the sensor onto the office network, the laptop needs to be running the company's BSG image installation of Windows to connect without further configuration. However, this would require troubleshooting the software to determine why it crashes on launch and addressing the issue.

If the problem cannot be resolved and the software cannot run reliably on the BSG installation, an alternative solution is to install the OEM version of Windows and try whitelist the PC so that it would be able to connect to the network. More

than likely the simpler solution is to try and troubleshoot why the program is unable to run on the company's image installation.

## 7.3 LAB network

Since the LAB network has already been scanned during the initial scans reported in this thesis, it is possible to determine that the sensor device would need to run both the IT and OT versions of the software to reliably scan both types of devices that are connected to the network. As it could be seen from the initial scanning that the IT scanner is not sufficient enough when the environment includes OT devices.

From a security standpoint, if the software can be run reliably on the company installation of Windows, it would be recommended to have the sensor PC run on that version. The company version is more secure than the OEM version due to the added security protocols and software installed with it.

## 7.4 OT network

For the OT network, it is highly recommended to install the OT Lansweeper on a BSG version of Windows if possible. This is due to the increased security requirements of the operational technology networks. By using a BSG version of Windows, the sensor device will have a higher level of protection against potential cyber threats that could harm the devices or system on the OT network.

Unlike the previous networks, the OT network is not able to directly access the internet, which means that the scanner data cannot be synchronized with the cloud platform. In order to overcome this issue, firstly it is recommended to implement the scanner behind the DMZ. This will allow the scanner to access the

OT network and query the devices without causing additional unnecessary traffic through the firewall.

Once the scanner is behind the DMZ, outbound connections to the Lansweeper cloud platform should be whitelisted. This will allow for active updates on device statuses and ensure that any potential issues or threats are identified and addressed in a timely manner.

Overall, implementing the sensor device on the OT network requires a higher level of caution and attention to detail than on the previous two network, due to the delicacy of the software and devices running on the network.

# 8 Conclusion

In conclusion, the software was successfully tested on the network, and the differences between the IT and OT versions of Lansweeper were apparent during the initial scans. The IT version has a more refined interface that the OT version lacks, but the OT version is capable of extracting more information from OT devices and detecting those that the IT version cannot.

As discussed in the previous chapters regarding permanent sensors, it is crucial to try and ensure that the software could be made to run on the BSG installation of Windows. This would significantly enhance the security of the devices and enable easy integration of the sensor device into the corporate network without having to undergo additional work such as whitelisting the device and updating it to meet security standards. In addition, running the software on the BSG installation would enable the sensor device to benefit from the remote management capabilities that are implemented in the installation as well as the automatic software updates.

The successful testing of the software on the network has demonstrated the benefits of using Lansweeper to improve the security and management of the network. From the identification of potential security vulnerabilities to the detection of unauthorized devices on the network. The software also proved its value when the initial scans were to be made and an unallocated IP-address could not be located easily. To maximize the benefits and minimize the risks associated with granting additional access to the network, a thorough review of the planned access must be made. This review should consider the specific needs of the sensor devices and the data they require, as well as the potential security implications of granting additional access.

# 6 References


1 Lansweeper: IT Asset Discovery Made Easy with Lansweeper https://content.lansweeper.com/Branded?utm_source=google&utm_medium. Accessed 20 January 2023

2 Lansweeper: Lansweeper for System Administrators. https://www.lansweeper.com/solution/system-administrator/. Accessed 20 January 2023

3 Lansweeper: Identifying your Lansweeper database. https://community.lansweeper.com/t5/lansweeper-maintenance/identify-which-database-server-lansweeper-is-using/ta-p/64506. Accessed 25 January 2023

4 Lansweeper: Use case – Lansweeper for OT Asset Management. Lansweeper for OT Asset Management - Lansweeper. Accessed 30 January 2023

5 Lansweeper: Operational technology security. https://www.lansweeper.com/cybersecurity/operational-technology-security-how-selective-probing-of-assets-reduces-risk-of-downtime/. Accessed 30 January 2023

6 Lansweeper: OT components and architecture. https://community.lansweeper.com/t5/lansweeper-ot/ot-components-and-architecture/ta-p/65726. Accessed 1 January 2023

7 Novell: Creating subnets http://www.novell.com/it-it/documentation/nias42/itcomm/rtcn_ita/data/h59r35qq.html. Accessed 1 February 2023

8 Subnetwork https://en.wikipedia.org/wiki/Subnetwork#/media/File:Subnetting_Concept.svg. Accessed 15 February 2023

9 Cloudflare: What is a subnet? https://www.cloudflare.com/en-gb/learning/network-layer/what-is-a-subnet/ Accessed 2 May 2023

10 Cisco: DMZ Basics. https://blogs.cisco.com/perspectives/dmz-basics. Accessed 6 February 2023

11 DMZ (computing) https://en.wikipedia.org/wiki/DMZ_(computing)>Accessed 16 February 2023

12 Barracuda: DMZ Network https://www.barracuda.com/support/glossary/dmz-network. Accessed 6 February 2023