Task ‘Nessus Vulnerability Scan Unit 3

Nessus Vulnerability Scan Analysis Report

Introduction

The purpose of this vulnerability assessment was to evaluate the security posture of a network-connected Cisco Wireless Access Point (WAP) using Nessus Essentials, the free version of the Nessus Essentials vulnerability scanner developed by Tenable. Automated vulnerability scanning plays a crucial role in cybersecurity by identifying known security weaknesses, misconfigurations, outdated software, and exposed services across networked devices. Contrary to dynamic penetration testing, which uses methods to leverage real attacks to actively exploit weaknesses, automated vulnerability scanning systematically inspects systems. It does so against comprehensive vulnerability databases. Some researchers suggest that automated vulnerability scanning plays a fundamental role in proactive security management. Such methods enable organizations to detect and address issues early on. It also helps reduce the probability of negative impact.

(ENISA, 2023; Ahammed, 2025).

This assessment demonstrates how automated tools can identify risks in commonly overlooked devices such as Wireless Access Points, which are frequently connected to corporate networks but insufficiently secured or hardened and can target many attacks. Or alternatively such Wireless Access Points could be weaponized and used

The full vulnerability report is available on the GitHub E-portfolio at:
https://am25251.github.io/uoe-eportfolio/files/03-Network_Security_January_2026/Unit_3/Cisco_WAP561_Wireless_Access_Point_Redacted.pdf

offensively to attack legitimate networks, for instance Rough Access Point (AP), Evil twin and more attacks that could be utilized by threat actors.

(Alghareeb, et al 2024)

Methodology

Setup

Nessus Essentials was downloaded from Tenable’s official website and installed on a Kali Linux virtual machine using the following commands:

- *sudo dpkg -i /home/kali/Downloads/Nessus-10.11.2-debian10_amd64.deb*.
- *sudo systemctl start nessusd* – To start the service
- *sudo systemctl start nessusd* – To enable the service
- *sudo systemctl start nessusd* – To check the status

The full vulnerability report is available on the GitHub E-portfolio at: https://am25251.github.io/uoe-eportfolio/files/03-Network_Security_January_2026/Unit_3/Cisco_WAP561_Wireless_Access_Point_Redacted.pdf

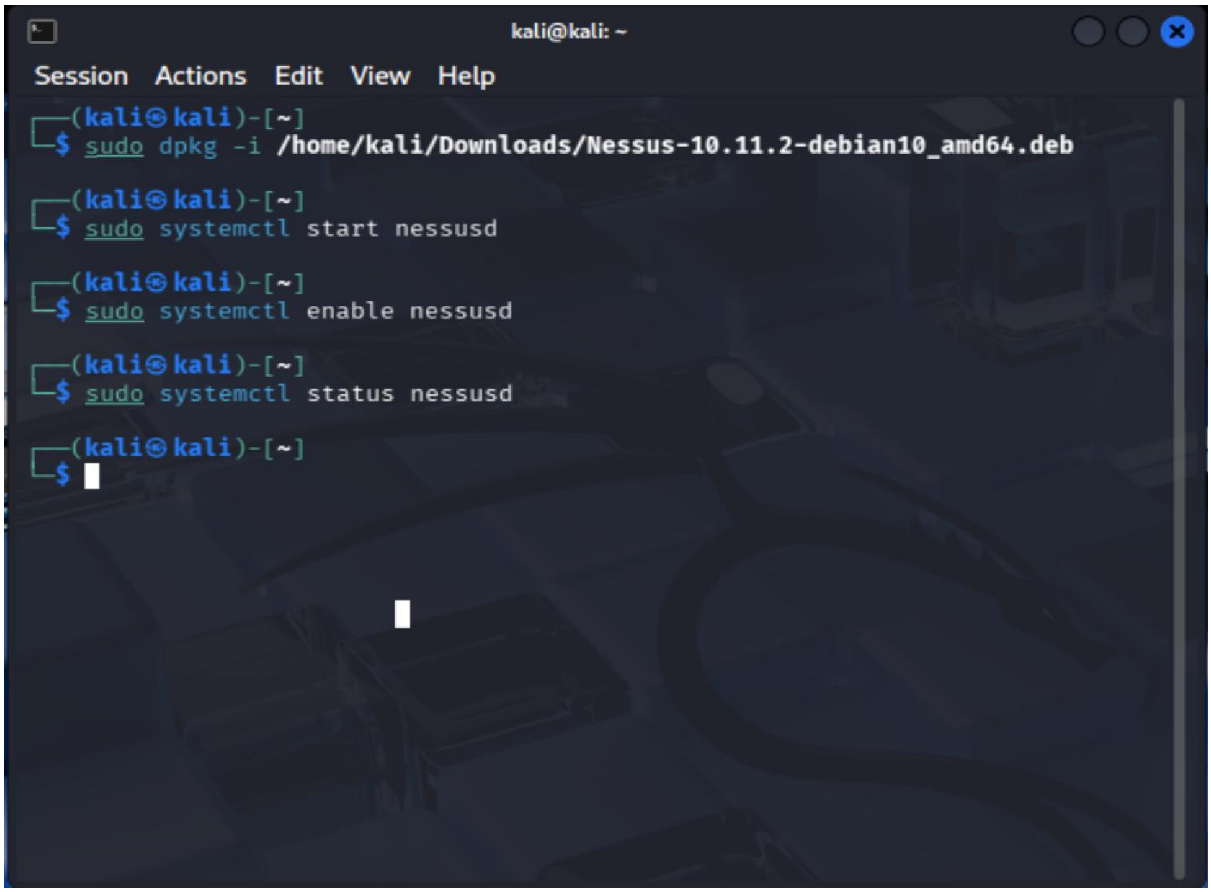


Figure 1: Nessus Service start, enable and status

The full vulnerability report is available on the GitHub E-portfolio at: https://am25251.github.io/uoe-eportfolio/files/03-Network_Security_January_2026/Unit_3/Cisco_WAP561_Wireless_Access_Point_Redacted.pdf

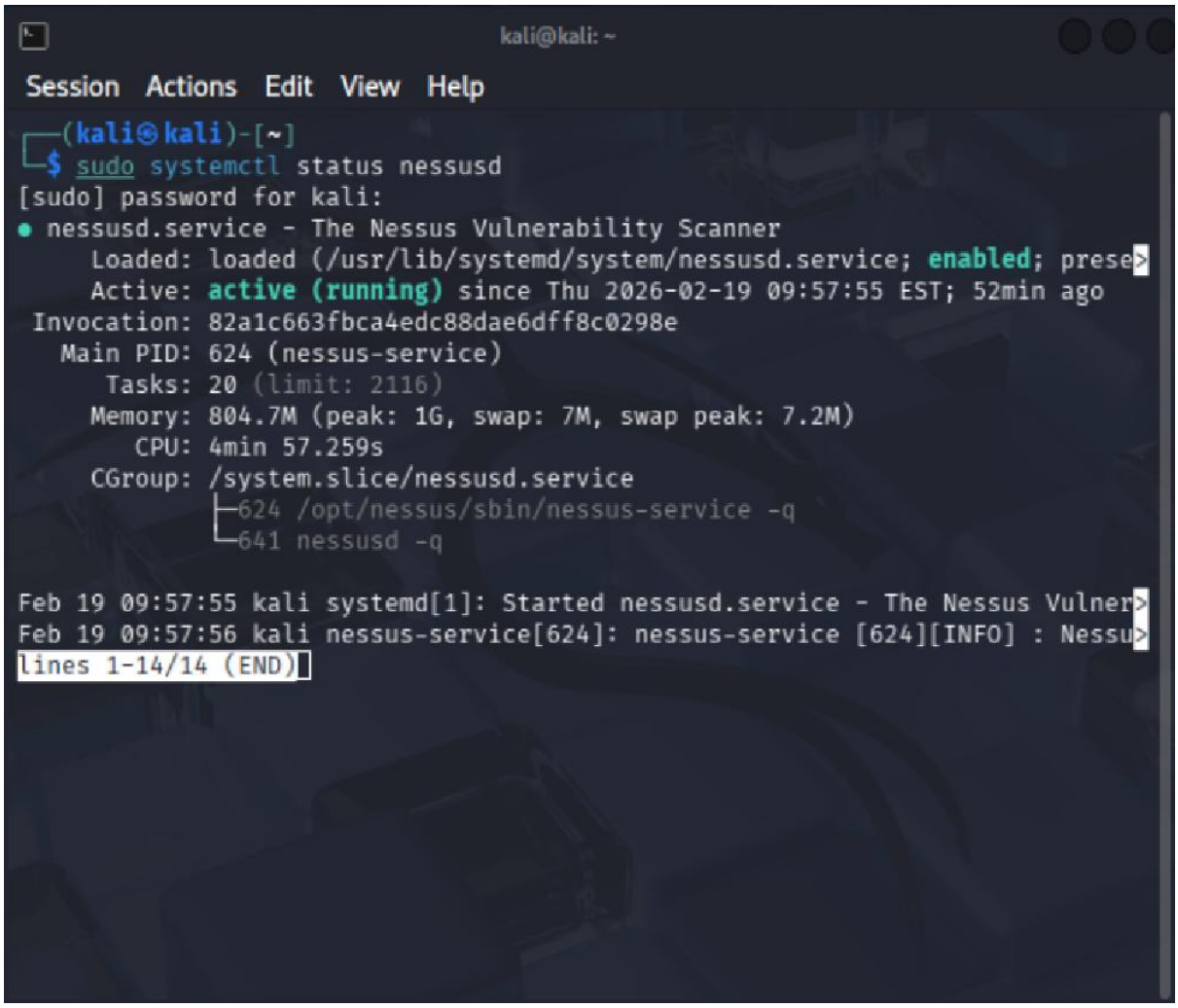


Figure 2: Nessus Status Enabled

The software was registered using a free activation code to unlock scanning functionality. Once installed, the Nessus web interface was accessed via HTTPS and configured for internal network scanning.

I had to restore the VM from a snapshot and reinstall Nessus for this task due to issues with Nessus not being initialized after few days.

The Target, a Cisco Wireless Access Point was connected to the network, using DHCP to my Netgate’s PFsense firewall which serves as the DHCP and the DNS server.

The full vulnerability report is available on the GitHub E-portfolio at: https://am25251.github.io/uoe-eportfolio/files/03-Network_Security_January_2026/Unit_3/Cisco_WAP561_Wireless_Access_Point_Redacted.pdf

(Netgate, 2025)

Figure 3: Cisco WAP561 Wireless Access Point

The full vulnerability report is available on the GitHub E-portfolio at: https://am25251.github.io/uoe-eportfolio/files/03-Network_Security_January_2026/Unit_3/Cisco_WAP561_Wireless_Access_Point_Redacted.pdf

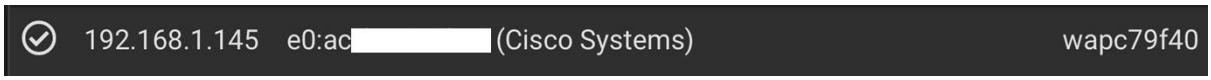


Figure 4: WAP DHCP Details on PFsense

(Netgate, 2025)

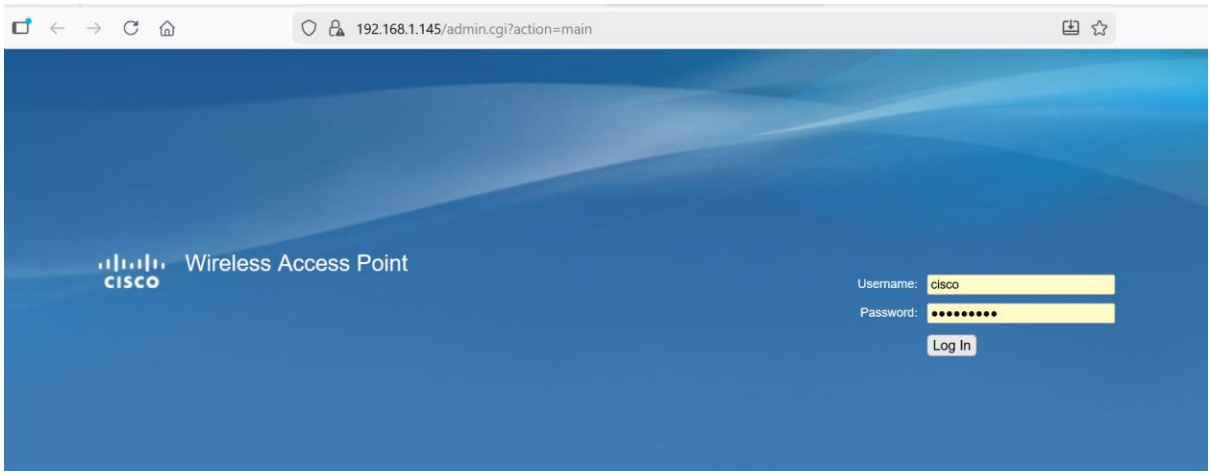


Figure 5: Cisco WAP management interface

(Cisco Systems, Inc., 2026)

Scope Definition

The selected target device was a Cisco Wireless Access Point (WAP) with IP address 192.168.1.145. The Nessus scanner was hosted on a separate system within the same VLAN (192.168.1.140). Ensuring both devices were on the same local network allowed accurate service discovery and vulnerability detection without firewall interference. This target for vulnerability scan was selected because it is a legacy device and not in use. The main reason for choosing it is to prevent the leakage of confidential information regarding live devices used on the network daily. It's also

The full vulnerability report is available on the GitHub E-portfolio at: https://am25251.github.io/uoe-eportfolio/files/03-Network_Security_January_2026/Unit_3/Cisco_WAP561_Wireless_Access_Point_Redacted.pdf

chosen because it's owned by the author and is a non-productive target for ethical reasons.

Scan Configuration

A new scan was created using the **Advanced Scan template** in Nessus Essentials. The target IP (192.168.1.145) was entered into the scan configuration panel. Default discovery settings were retained to simulate a standard internal vulnerability assessment scenario. The scan was initiated from the Nessus dashboard and monitored until completion.

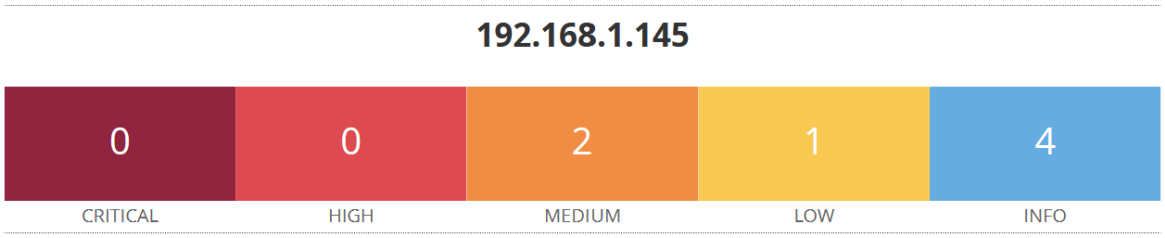
scan results will be presented, based on typical vulnerabilities found in network connected Wireless Access Points.

(Tenable, 2024)

Findings Summary

After completion, Nessus categorized identified vulnerabilities into five severity levels: Critical, High, Medium, Low, and Informational.

The full vulnerability report is available on the GitHub E-portfolio at:
https://am25251.github.io/uoe-eportfolio/files/03-Network_Security_January_2026/Unit_3/Cisco_WAP561_Wireless_Access_Point_Redacted.pdf



Host Information

DNS Name:	wapc79f40.int. com
IP:	192.168.1.145
MAC Address:	E0:AC
OS:	Dell iDRAC Controller, KYOCERA Printer, Linux Kernel 2.6

Summary of Results

Severity Level	# of Findings
Critical	0
High	0
Medium	4
Low	2
Informational	38
Overall	44

Table 1: Number of Finding

Vulnerabilities

Risk Factor	Number	Synopsis	CVSS V3.0
Medium	51192	The SSL certificate for this service cannot be trusted	6.5
	15901	The remote server SSL certificate had expired	5.3
Low	69551	SSL Certificate Chain Contains RSA keys less than 2048 bits	-
Informational	10863	SSL Certificate Information - This plugin displays the SSL certificate	-
	70544	SSL Cipher Block Chaining Cipher Suites Supported	-
	21643	SSL Cipher Suites Supported	-
	57041	SSL Perfect Forward Secrecy Cipher Suites Supported	-

The full vulnerability report is available on the GitHub E-portfolio at: https://am25251.github.io/uoe-eportfolio/files/03-Network_Security_January_2026/Unit_3/Cisco_WAP561_Wireless_Access_Point_Redacted.pdf

Table 2: Finding Results

(Tenable, 2024)

Analysis

The most significant risk identified was Medium, with codes 51192 ("The SSL certificate for this service cannot be trusted") and 15901 ("The remote server SSL certificate had expired"). Deprecated TLS and SSL protocols, weaken encrypted communication. Self-signed SSL or TLS certificates could be used by attackers to impersonate to a legitimate identity and leverage so-called man-in-the-middle (MitM) attacks. In a corporate network, this could enable lateral movement, confidential data interception and additional use of legitimate resources as a pivot point for further attacks.

(Tenable 2024).

Devices such as wireless access points, which are often deployed autonomously, are frequently overlooked in vulnerability management and sometimes also in patch management practices. Studies show that these devices significantly increase an organization's attack-surface from a nearby compromise standpoint. Examples include attacks on SSIDs, outdated device software on the WAP, as well as unprotected management interfaces over the internet. Other examples mentioned above include rogue AP and Evil Twin, impose a treat to organizations and individuals.

The full vulnerability report is available on the GitHub E-portfolio at: https://am25251.github.io/uoe-eportfolio/files/03-Network_Security_January_2026/Unit_3/Cisco_WAP561_Wireless_Access_Point_Redacted.pdf

(Alghareeb, et al., 2024).

This scan demonstrates how even a single peripheral device may introduce multiple security risks.

Recommendations for Action / Mitigation

1. **Strengthening Governance and Risk Management**

   Organization needs to implement structured governance and risk management practices that address security risks holistically rather than in isolation. Although this report focuses on specific findings, a broader enterprise-wide risk framework is essential to ensure sustainable and proactive security management.

2. **Maintain Up-to-Date Software**

   Keep all autonomous Wireless Access Points (WAP) and Wireless Controllers firmware updated to the latest vendor-supported version to remediate known vulnerabilities. Establish a formal patch management process to ensure timely updates in the future.

3. **Replace Default Credentials**

   Default administrative credentials must be changed to strong, unique passwords. In this case, this was required to be done immediately after resetting the WAP to factory settings. Password policies should enforce length, complexity and periodic review.

4. **Unnecessary Disability Services \ Secure (Harden) Necessary Services**

The full vulnerability report is available on the GitHub E-portfolio at: https://am25251.github.io/uoe-eportfolio/files/03-Network_Security_January_2026/Unit_3/Cisco_WAP561_Wireless_Access_Point_Redacted.pdf

Disable unused or insecure services such as FTP, unused SMB services, and SNMPv2. Replace them with secure alternatives, for instance SNMPv3. Wireless networks (SSID) signals should not be enabled without proper protection, such as WPA2, WPA3, or enterprise (802.11X) encryption. Where possible, implement a centralized wireless controller to manage access points effectively and improve visibility.

5. **Enforce Strong TLS and PKI Controls**

Ensure to disablement of SSL, TLS v1.0, and TLS v1.1 in full. Configure only TLS 1.2 or higher. Implement certificate management through a trusted centralized Public Key Infrastructure (PKI).

6. **Implement Network Segmentation**

Place the Wireless Access Point within a dedicated VLAN. Use Next-Generation Firewalls and micro-segmentation solutions aligned with a Zero Trust approach to reduce lateral movement risks. This can be cost-effective in virtualized environments.

7. **Conduct Regular Security Scanning and Auditing**

Integrate proactive vulnerability scanning and reviews into regular security operations. Perform regular internal and external audits to develop Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) metrics to measure success and failure, assess security maturity and guide continuous improvement. Such improvements help to significantly reduce the risk and improve resilience.

(Максимов, 2025)

The full vulnerability report is available on the GitHub E-portfolio at:
https://am25251.github.io/uoe-eportfolio/files/03-Network_Security_January_2026/Unit_3/Cisco_WAP561_Wireless_Access_Point_Redacted.pdf

Task ‘Nessus Vulnerability Scan Unit 3

Reflection

This exercise had supported the value of conducting automated vulnerability scanning in identifying security weaknesses quickly and systematically. Nessus Essentials proved appropriate for this task due to its comprehensive plugin database, severity classification system, and user-friendly reporting features.

The activity strongly supported the argument that automated scanning differs greatly from manual penetration testing by concentrating on detection of weakness rather than the exploitation of such. While it does not simulate attacker creativity and demonstrates determination, it provides a flexible and efficient method to detect known weaknesses across many systems early enough, reflecting the opportunities involved.

Reviewing the results reinforced the importance of securing and hardening IT assets in this case, Autonomous Wireless Access Points. Even in a small home, lab environment or enterprise network, such vulnerabilities can pose substantial risks. Using automated tools like Nessus organizations and individuals can achieve visibility into these hidden exposures and form a critical component of modern cybersecurity practice.

Use of Digital Tools

The full vulnerability report is available on the GitHub E-portfolio at: https://am25251.github.io/uoe-eportfolio/files/03-Network_Security_January_2026/Unit_3/Cisco_WAP561_Wireless_Access_Point_Redacted.pdf

This report has been produced for educational purposes. All references, names, and trademarks remain the property of their respective owners. ensuring accuracy and reproducibility under given conditions and limitations, Grammarly was used for proofreading and language clarity, and ChatGPT was used for preliminary literature exploration and language refinement. All academic writing, analysis, argumentation, and conclusions represent the original work of the author.

References

- Ahammed, M.F., (2025). Zero-Trust Architectures for Securing US Critical Infrastructure. Frontiers in Computer Science and Artificial Intelligence, 4(3), pp.09-16.
- Alghareeb, M.S., Almaiah, M. and Badr, Y., (2024). Cyber Security Threats in Wireless LAN: A Literature Review. International Journal of Cybersecurity Engineering and Innovation, 2024(1).
- Orzach, Y. and Khuanna, D. (2022) Network Protocols for Security Professionals. Birmingham: Packt Publishing.
- Cisco Systems, Inc. (2026) Cisco Systems. Available at: https://www.cisco.com/ [Accessed: 19 February 2026].
- ENISA (2023) Threat Landscape 2023. European Union Agency for Cybersecurity.
- Tenable (2024) Nessus Essentials User Guide. Tenable Inc.
- Максимов, В., (2025). ARCHITECTURAL PRINCIPLES AND OPERATIONAL PRACTICES FOR BUILDING SECURE DIGITAL INFRASTRUCTURE IN CLOUD ENVIRONMENTS. *Територія безпеки*, *1*(2), pp.47-56.

The full vulnerability report is available on the GitHub E-portfolio at: https://am25251.github.io/uoe-eportfolio/files/03-Network_Security_January_2026/Unit_3/Cisco_WAP561_Wireless_Access_Point_Redacted.pdf

- Netgate (2025) pfSense software. Available at: https://www.pfsense.org/ [Accessed: 19 February 2026]

The full vulnerability report is available on the GitHub E-portfolio at: https://am25251.github.io/uoe-eportfolio/files/03-Network_Security_January_2026/Unit_3/Cisco_WAP561_Wireless_Access_Point_Redacted.pdf