

AUTOMATED VULNERABILITY ASSESSMENT REPORT

Vulnerability Assessment

SOAC Inc. SWANSEA.ACCA Domain Nessus Essentials Plus

STUDENT DETAILS

STUDENT NAME	David Lopez Rodriguez
STUDENT ID	2336542
INSTITUTION	UWTSD London Campus
MODULE	ACCB6000 Advanced Cybersecurity
TOOL	Nessus Essentials Plus (authenticated + unauthenticated)

August 2026

Executive Summary

This report presents the automated vulnerability assessment of the SWANSEA.ACCA enterprise network using Nessus Essentials Plus. A two-phase methodology was applied following the NIST Cybersecurity Framework 2.0 [1]: an unauthenticated scan (external attacker perspective) and an authenticated scan using domain credentials (white-box audit). Vulnerabilities are categorised using CVSS v3.1 [5].

Assessment Scope

Host	IP Address	OS	Auth	Vulnerabilities Found
S-DC1	192.168.1.1	Windows Server 2022	Pass	75 (auth) / 43 (no auth)
ClientS1	192.168.1.10	Windows 10	Fail	30 (info only)
L-CD	192.168.2.1	Debian Server 12	Fail	30 (info only)

Scan Statistics

Scan Type	Total	Critical	High	Medium	Low
Unauthenticated (black-box)	43	0	1	4	2
Authenticated (white-box)	75	1	1	4	2

Scan Overview

Phase 1: Unauthenticated Scan

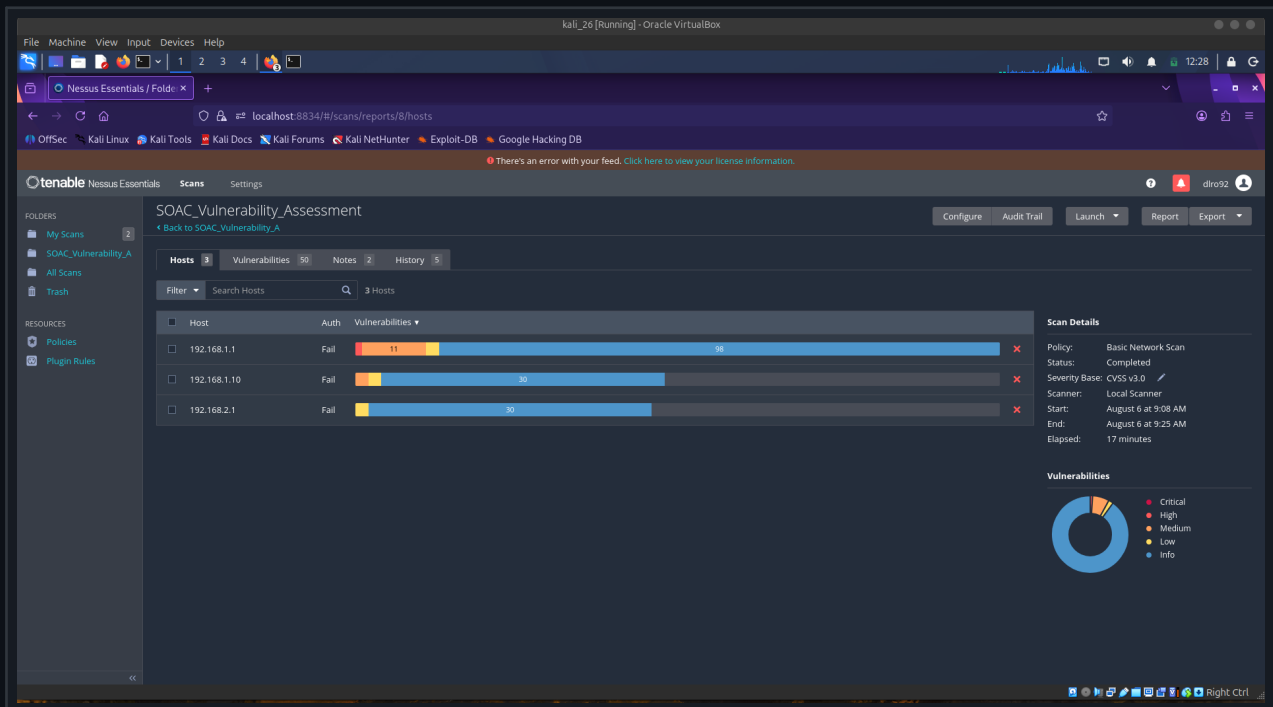


Figure 2.1 Unauthenticated scan 43 vulnerabilities S-DC1 Auth: Fail

Phase 2: Authenticated Scan

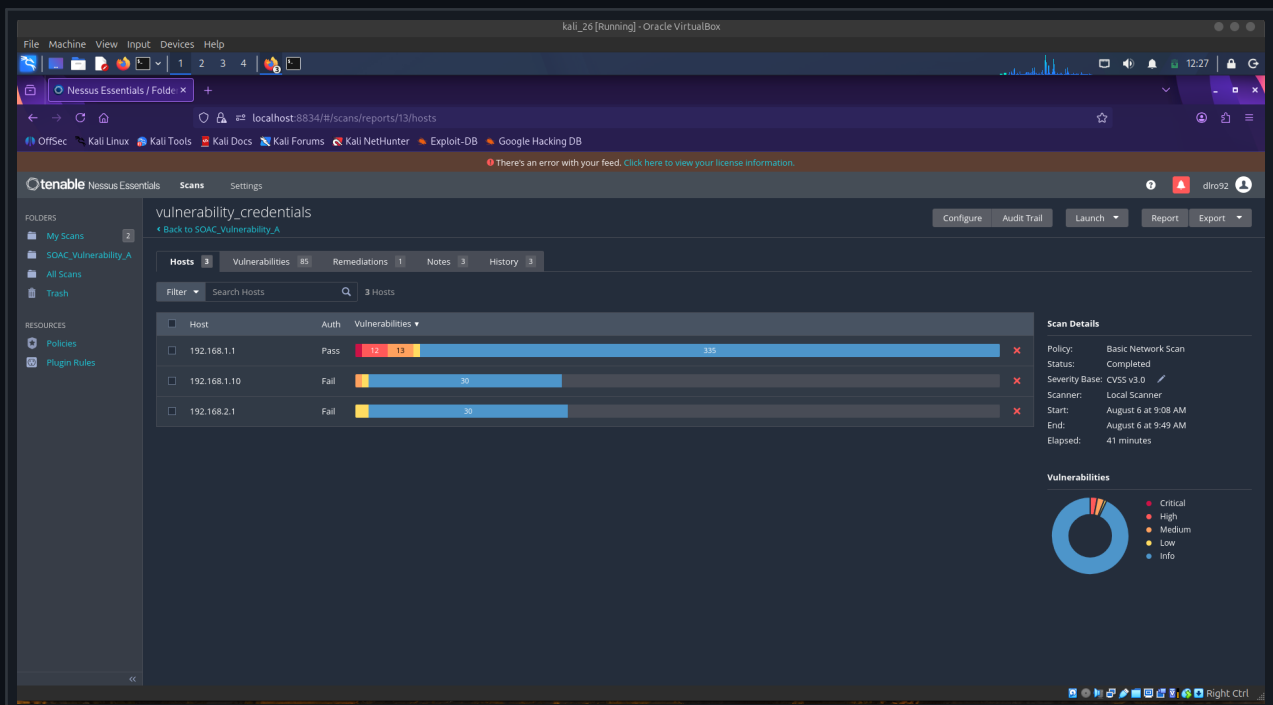


Figure 2.2 Authenticated scan 75 vulnerabilities S-DC1 Auth: Pass

Authenticated Scan S-DC1 Vulnerability List

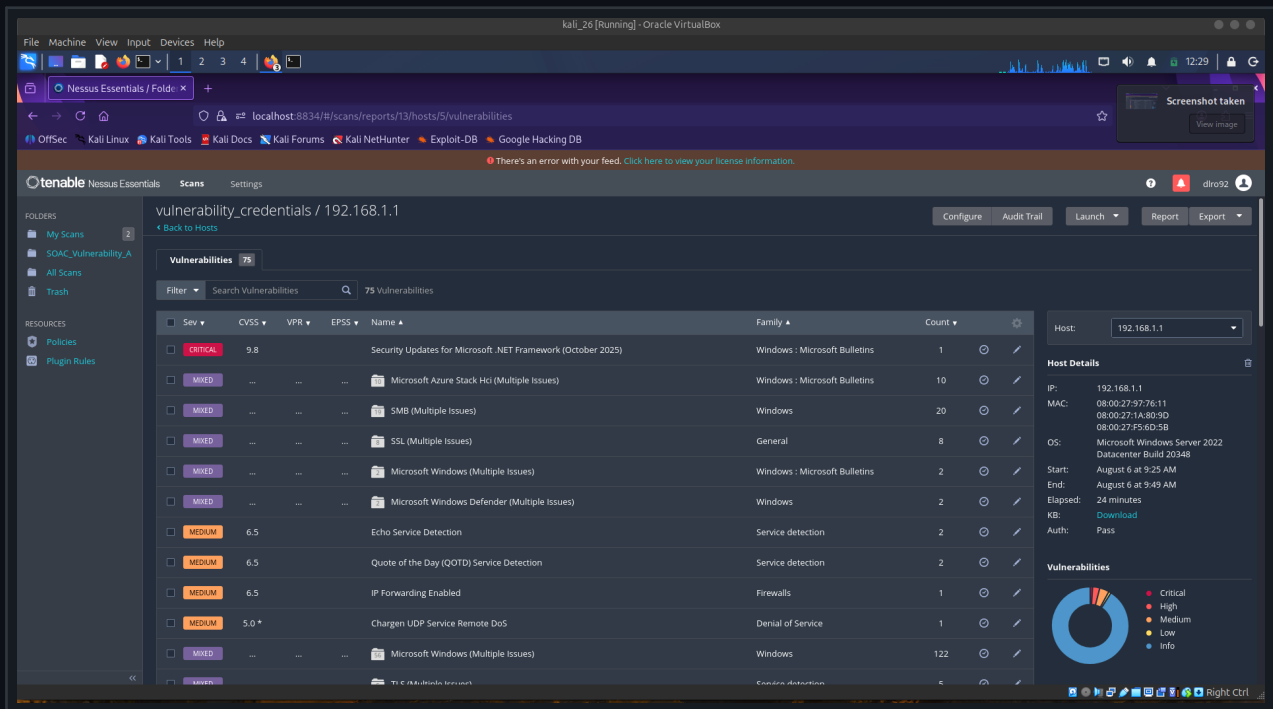


Figure 2.3 Authenticated scan vulnerability list S-DC1 (192.168.1.1) 75 total

Unauthenticated Scan S-DC1 Vulnerability List

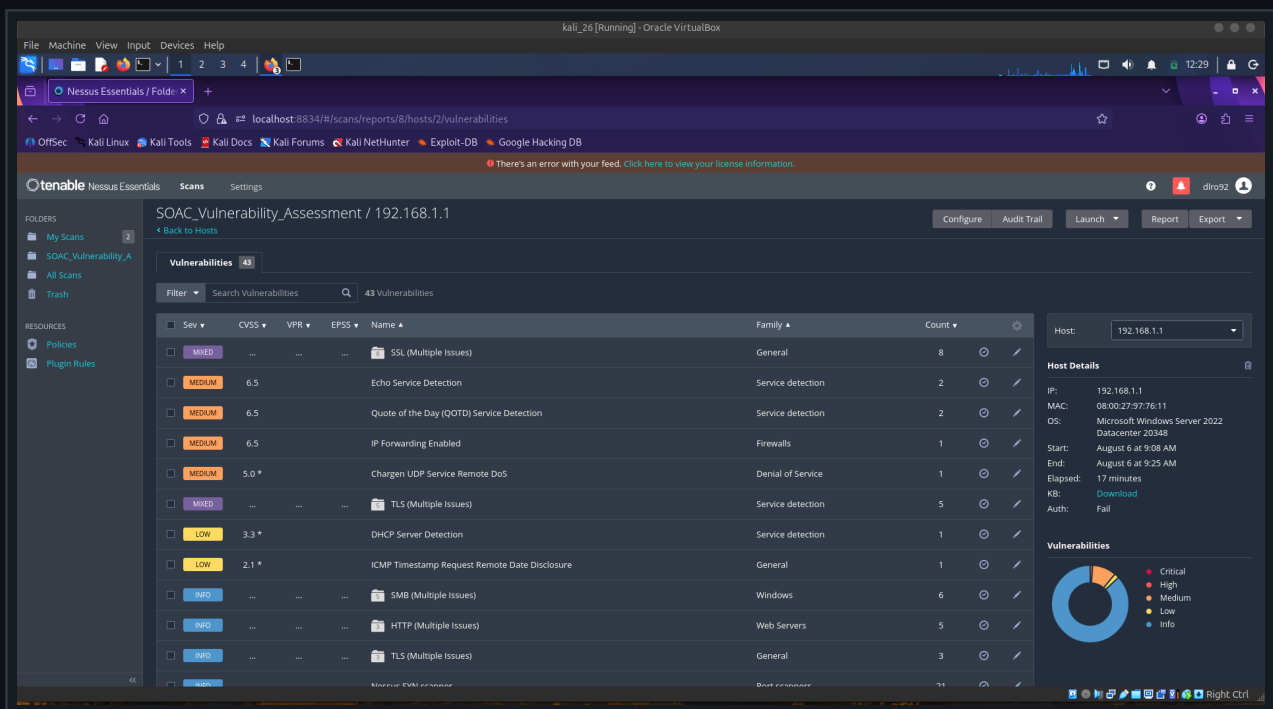


Figure 2.4 Unauthenticated scan vulnerability list S-DC1 (192.168.1.1) 43 total

Selected Vulnerabilities

Six vulnerabilities were selected from the scan results representing Critical, High, Medium and Low severity categories across two hosts. Severity classification follows CVSS v3.1 [5].

#	Vulnerability	Severity	CVSS	CVE	Host
1	Missing .NET Framework Update	CRITICAL	9.8	CVE-2025-55248	S-DC1
2	SWEET32 SSL Ciphers	HIGH	7.5	CVE-2016-2183	S-DC1
3	IP Forwarding Enabled	MEDIUM	6.5	CVE-1999-0511	S-DC1
4	SMB Signing Not Required	MEDIUM	5.3	N/A	ClientS1
5	DHCP Server Detection	LOW	3.3	N/A	S-DC1
6	ICMP Timestamp Disclosure	LOW	2.1	CVE-1999-0524	S-DC1

Vulnerability 1

Security Updates for Microsoft .NET Framework (October 2025)

CRITICAL

CVSS	CVE	Host	Port	Tool
9.8	CVE-2025-55248	S-DC1 (192.168.1.1)	445 / tcp	Nessus Essentials Plus

Description

The .NET Framework 4.8 installation on S-DC1 is missing the October 2025 security update (installed: 4.8.4770.0, required: 4.8.4797.0). This exposes the host to an information disclosure vulnerability exploitable remotely without user interaction [1].

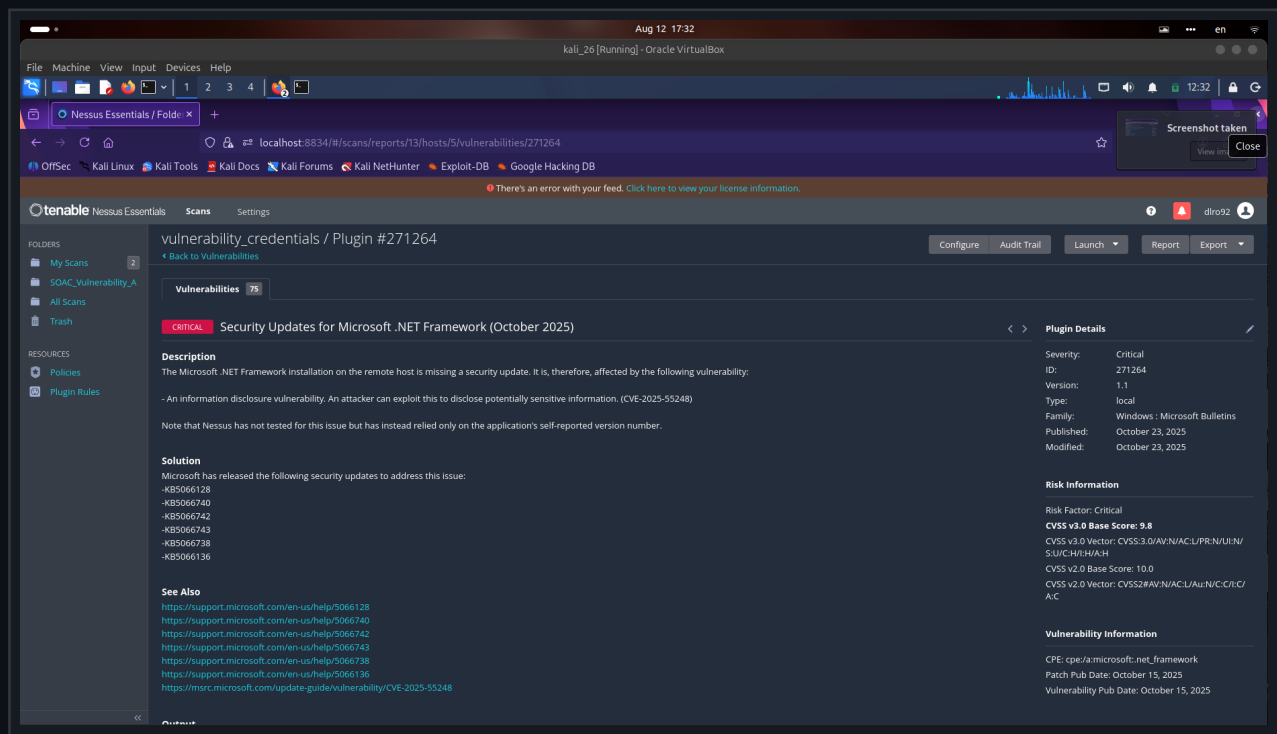


Figure 3.1 Nessus Plugin 271264: .NET Framework Missing Update (CRITICAL, CVSS 9.8) CVE-2025-55248

Vulnerability 2

SSL Medium Strength Cipher Suites Supported (SWEET32)

HIGH

CVSS	CVE	Host	Port	Tool
7.5	CVE-2016-2183	S-DC1 (192.168.1.1)	443 / tcp	Nessus Essentials Plus

Description

The IIS web server accepts 3DES cipher suites with a 64-bit block size across TLS 1.0, 1.1 and 1.2. An attacker on the same network can exploit the SWEET32 birthday collision to partially recover plaintext from encrypted HTTPS sessions [2].

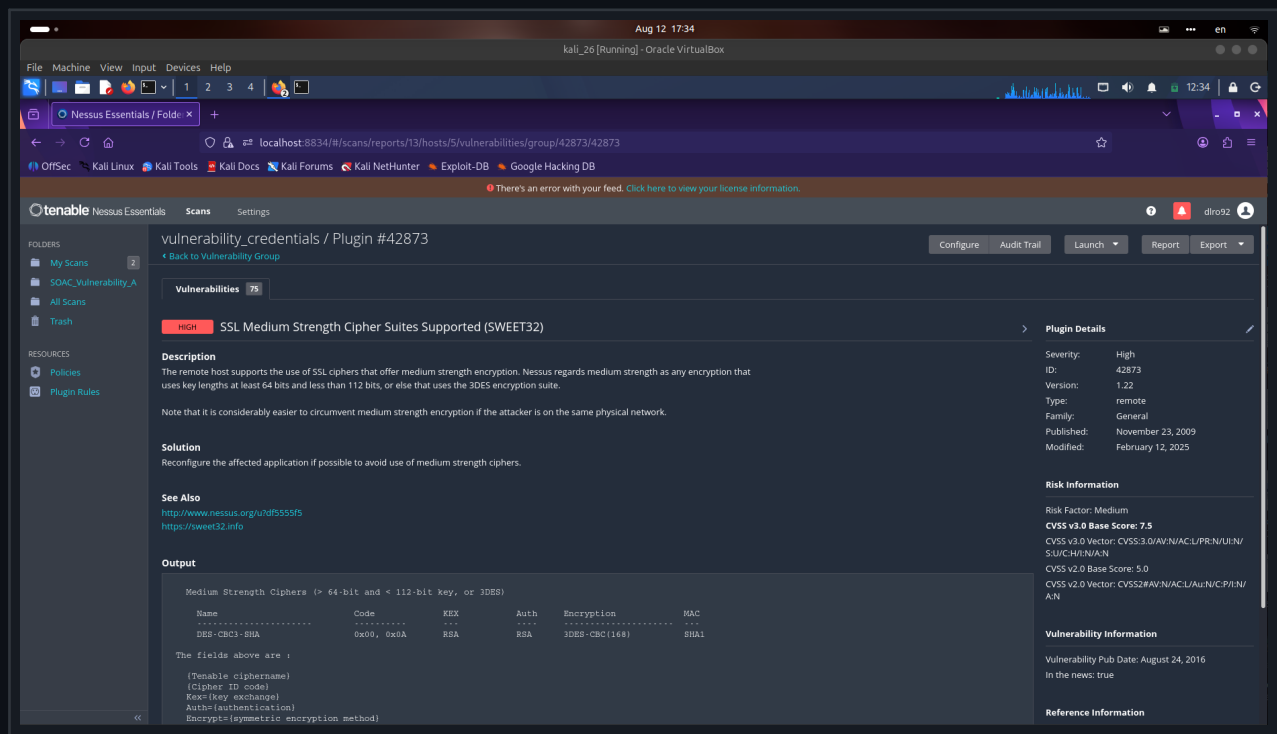


Figure 3.2 Nessus Plugin 42873: SWEET32 SSL Medium Strength Ciphers (HIGH, CVSS 7.5) CVE-2016-2183

Vulnerability 3

IP Forwarding Enabled

MEDIUM

CVSS	CVE	Host	Port	Tool
6.5	CVE-1999-0511	S-DC1 (192.168.1.1)	N/A	Nessus Essentials Plus

Description

S-DC1 forwards packets between its network interfaces, behaving as a router. On a Domain Controller this is a security risk, as an attacker could use it as a pivot point to route traffic between the Swansea and London subnets, bypassing firewall segmentation controls.

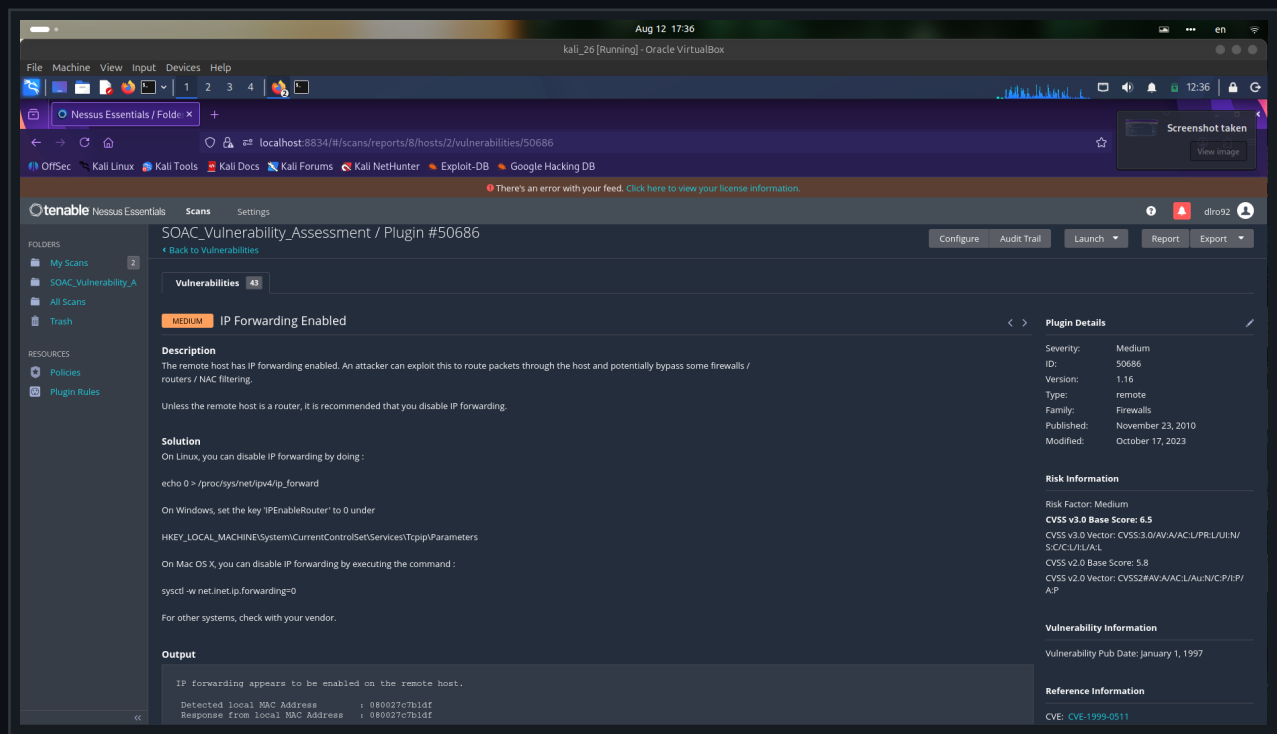


Figure 3.3 Nessus Plugin 50686: IP Forwarding Enabled (MEDIUM, CVSS 6.5) 192.168.1.1

Vulnerability 4

SMB Signing Not Required

MEDIUM

CVSS	CVE	Host	Port	Tool
5.3	N/A	ClientS1 (192.168.1.10)	445 / tcp	Nessus Essentials Plus

Description

SMB message signing is optional on ClientS1. Without mandatory signing, an attacker on the network can intercept SMB sessions and perform NTLM relay attacks, authenticating to other systems using captured credentials without knowing the plaintext password [3].

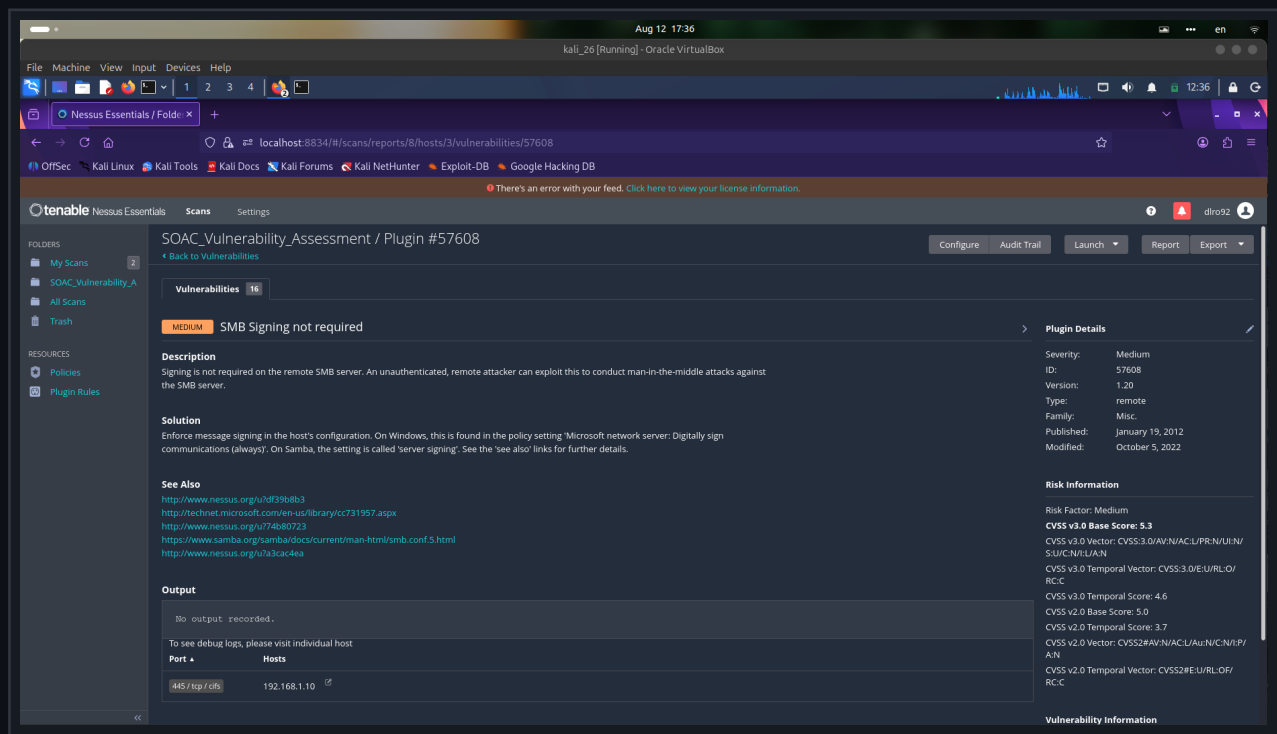


Figure 3.4 Nessus Plugin 57608: SMB Signing Not Required (MEDIUM, CVSS 5.3) 192.168.1.10

Vulnerability 5

DHCP Server Detection

LOW

CVSS	CVE	Host	Port	Tool
3.3	N/A	S-DC1 (192.168.1.1)	67 / udp	Nessus Essentials Plus

Description

The DHCP server on S-DC1 discloses network topology details including subnet mask, server identifier and lease parameters to any unauthenticated host that sends a broadcast discovery request, facilitating network reconnaissance.

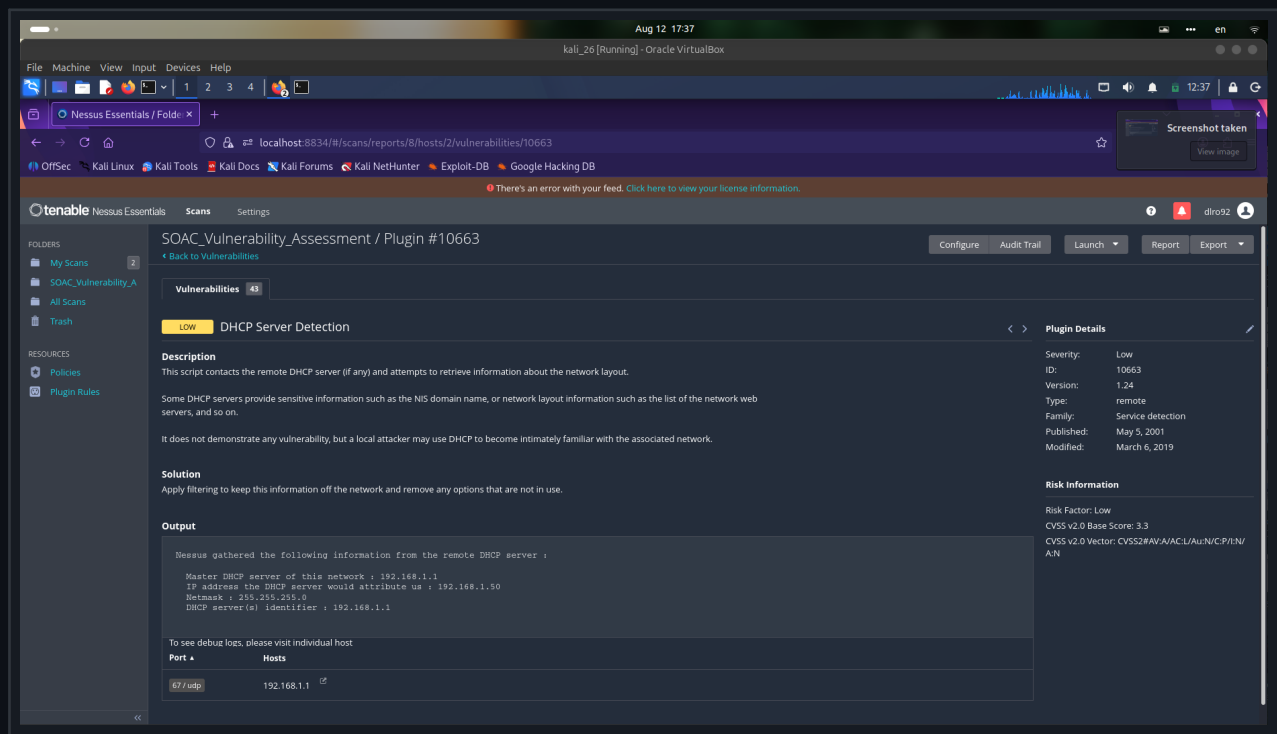


Figure 3.5 Nessus Plugin 10663: DHCP Server Detection (LOW, CVSS 3.3) 192.168.1.1 port 67/udp

Vulnerability 6

ICMP Timestamp Request Remote Date Disclosure

LOW

CVSS	CVE	Host	Port	Tool
2.1	CVE-1999-0524	S-DC1 (192.168.1.1)	0 / icmp	Nessus Essentials Plus

Description

S-DC1 responds to ICMP Timestamp Requests, disclosing its system clock to any remote host. On a Domain Controller using Kerberos, which enforces a maximum five-minute clock skew, this information could assist time-based attacks against authentication tokens.

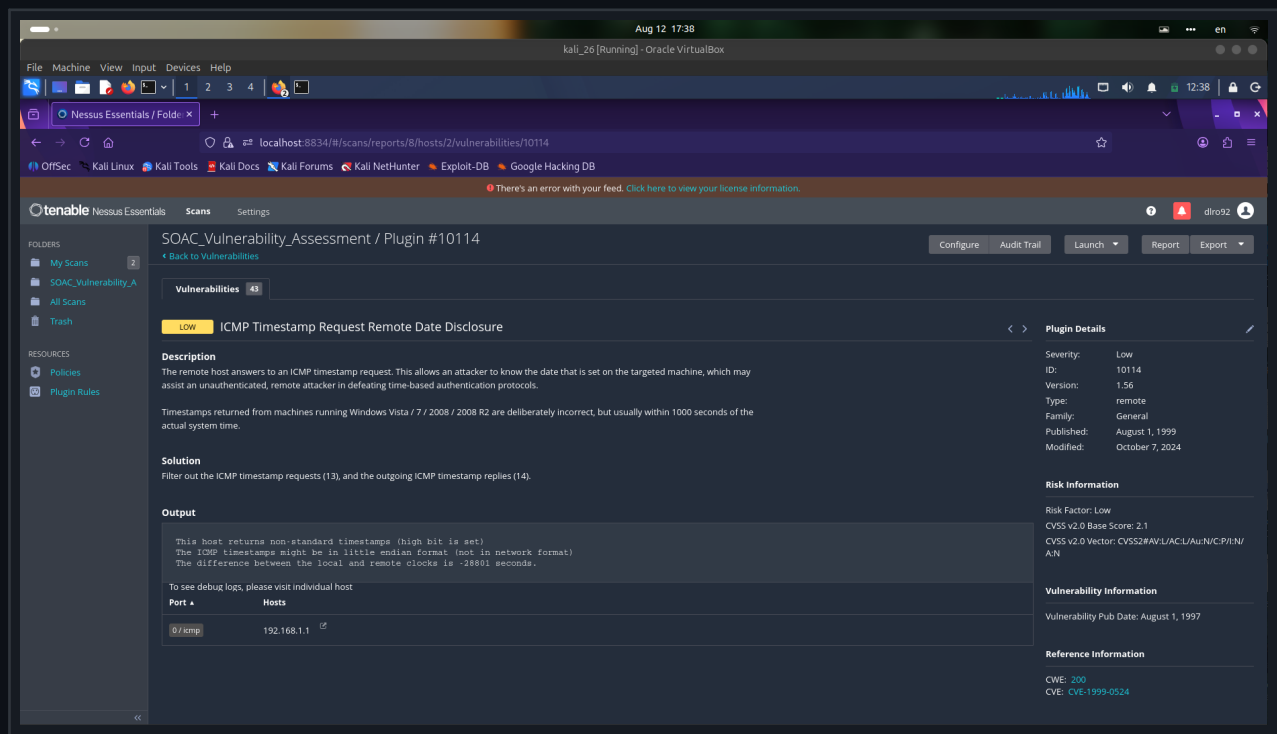


Figure 3.6 Nessus Plugin 10114: ICMP Timestamp Disclosure (LOW, CVSS 2.1) CVE-1999-0524

References

[1] National Institute of Standards and Technology, "NIST Cybersecurity Framework 2.0," NIST CSWP 29, Feb. 2024. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>

[2] National Vulnerability Database, "CVE-2016-2183: Birthday attacks against TLS ciphers with 64-bit block size (SWEET32)," NIST, 2016. [Online]. Available: <https://nvd.nist.gov/vuln/detail/CVE-2016-2183>

[3] Microsoft Corporation, "Control SMB signing behaviour," Microsoft Learn, 2025. [Online]. Available: <https://learn.microsoft.com/en-us/windows-server/storage/file-server/smb-signing>

[4] MITRE ATT&CK;, "OS Credential Dumping: NTDS (T1003.003)," MITRE Corporation, 2024. [Online]. Available: <https://attack.mitre.org/techniques/T1003/003/>

[5] Forum of Incident Response and Security Teams, "Common Vulnerability Scoring System v3.1: Specification Document," FIRST, 2023. [Online]. Available: <https://www.first.org/cvss/specification-document>