Vulnerability Management and Asset Scanning Using Qualys on AWS: A Practical Implementation

BY
OLUWASEYI MAJEKODUNMI

Table of Contents

1. Introduction 3
2. Implementation and Environment Setup 4
3. Configuration on Qualys Web GUI 6
4. Basic Port Scanning 7
5. Advanced Scanning with Authentication 10
6. Vulnerabilities Dashboard 12
7. Conclusion 13

Introduction

Qualys is a leading cloud-based platform that provides security and compliance solutions for IT infrastructure. It enables organizations to identify, assess, and manage vulnerabilities across their digital assets, ensuring that potential security risks are identified and mitigated in a timely manner. The **Qualys Cloud Platform** integrates a wide range of security functions, including vulnerability scanning, compliance monitoring, and asset inventory, all accessible through a single web interface.

Implementation and Environment Setup

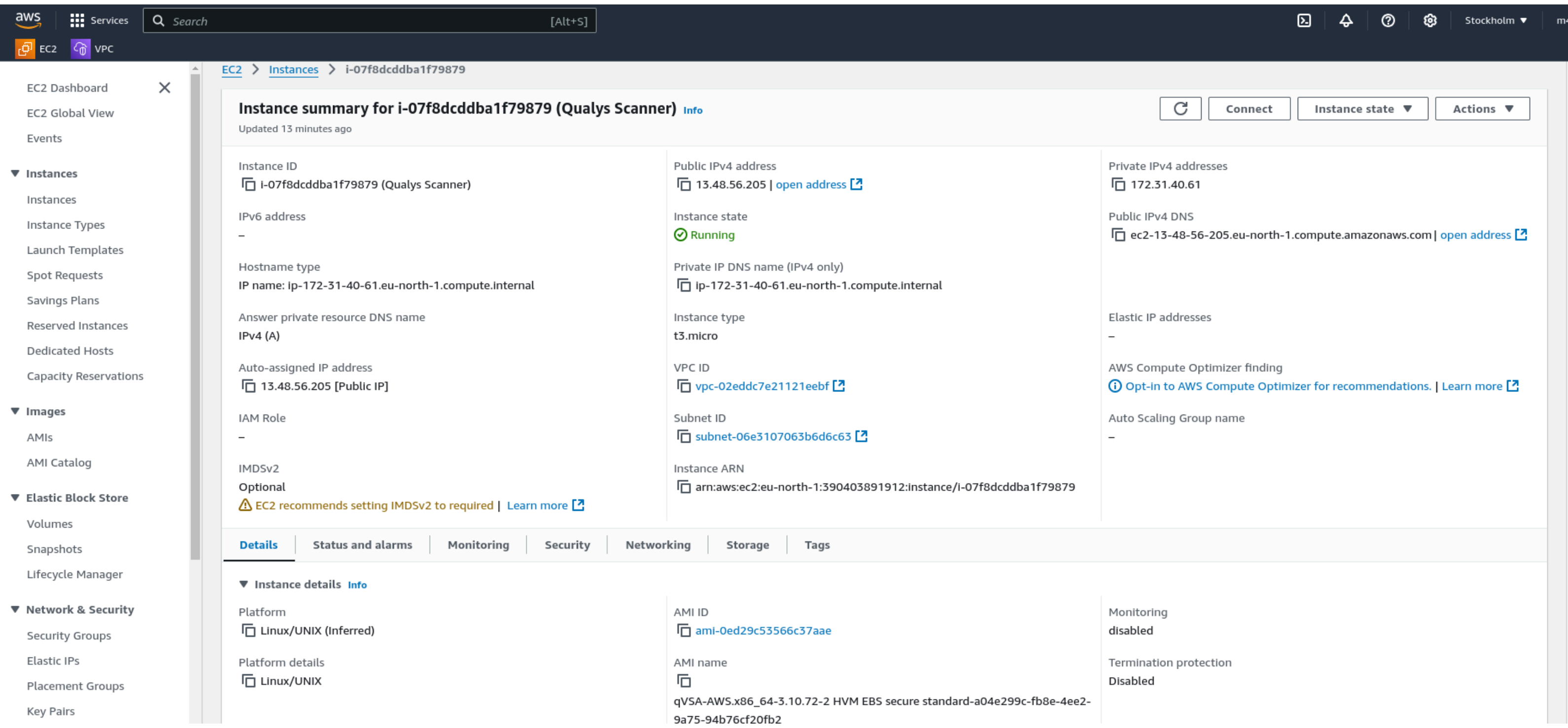
To begin, I set up a cloud environment on **Amazon Web Services (AWS)**,which involved deploying the following components:

- A **Qualys Virtual Scanner Appliance**, which I deployed using an AWS EC2 instance with the **Qualys-provided AMI**.
- Three client machines: **Two Windows instances** and **one Ubuntu instance**.

With these components in place, my primary objective was to ensure everything was configured correctly for continuous monitoring and scanning of the target systems.

Setting Up the Virtual Scanner Appliance

The first step was deploying the **Qualys Virtual Scanner**. I launched the scanner using the **Qualys Virtual Scanner (qVS) AMI** on an EC2 instance. During the setup, I added the **personalization code** provided by Qualys to ensure secure communication with my account. Once everything was running, I verified that the scanner was properly connected to the Qualys platform.



Instance summary for i-07f8dcddba1f79879 (Qualys Scanner) Info

Updated 13 minutes ago

Instance ID: i-07f8dcddba1f79879 (Qualys Scanner)

Public IPv4 address: 13.48.56.205 | open address

Private IPv4 addresses: 172.31.40.61

IPv6 address: –

Instance state: Running

Public IPv4 DNS: ec2-13-48-56-205.eu-north-1.compute.amazonaws.com | open address

Hostname type: IP name: ip-172-31-40-61.eu-north-1.compute.internal

Private IP DNS name (IPv4 only): ip-172-31-40-61.eu-north-1.compute.internal

Answer private resource DNS name: IPv4 (A)

Instance type: t3.micro

Elastic IP addresses: –

Auto-assigned IP address: 13.48.56.205 [Public IP]

VPC ID: vpc-02eddc7e21121eebf

AWS Compute Optimizer finding: Opt-in to AWS Compute Optimizer for recommendations. | Learn more

IAM Role: –

Subnet ID: subnet-06e3107063b6d6c63

Auto Scaling Group name: –

IMDSv2: Optional

⚠ EC2 recommends setting IMDSv2 to required | Learn more

Instance ARN: arn:aws:ec2:eu-north-1:390403891912:instance/i-07f8dcddba1f79879

▼ Instance details Info

Platform: Linux/UNIX (Inferred)

AMI ID: ami-0ed29c53566c37aae

Monitoring: disabled

Platform details: Linux/UNIX

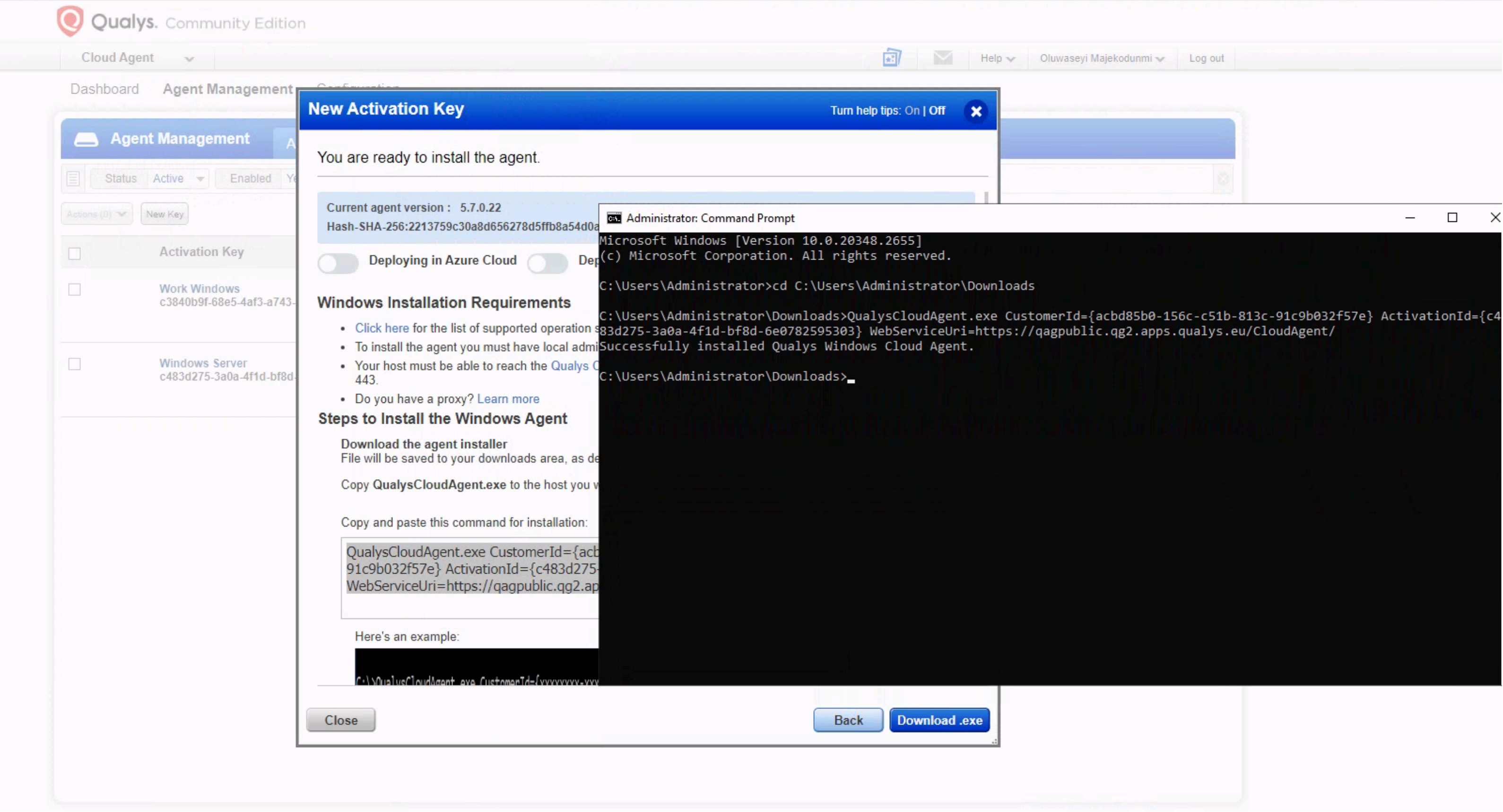
AMI name: qVSA-AWS.x86_64-3.10.72-2 HVM EBS secure standard-a04e299c-fb8e-4ee2-9a75-94b76cf20fb2

Termination protection: Disabled

Cloud Agent Installation

After the scanner was set up, I moved on to installing **Qualys Cloud Agents** on the three client machines. These agents monitor vulnerabilities in real-time, allowing me to get an up-to-date view of each asset's security posture. Here's how I installed the agents:

- For the **Windows instances**, I logged in via **RDP**, downloaded the agent installer, and followed the setup steps to connect them to my Qualys account.
- For the **Ubuntu instance**, I accessed it via **SSH**, downloaded the agent package using **wget**, and installed it with **dpkg**.



Work Windows
c3840b9f-68e5-4af3-a743-

Windows Server
c483d275-3a0a-4f1d-bf8d-

New Activation Key

You are ready to install the agent.

Current agent version : 5.7.0.22
Hash-SHA-256:2213759c30a8d656278d5ffb8a54d0a

Deploying in Azure Cloud

Windows Installation Requirements

- Click here for the list of supported operation s
- To install the agent you must have local admi
- Your host must be able to reach the Qualys C 443.
- Do you have a proxy? Learn more

Steps to Install the Windows Agent

Download the agent installer
File will be saved to your downloads area, as de

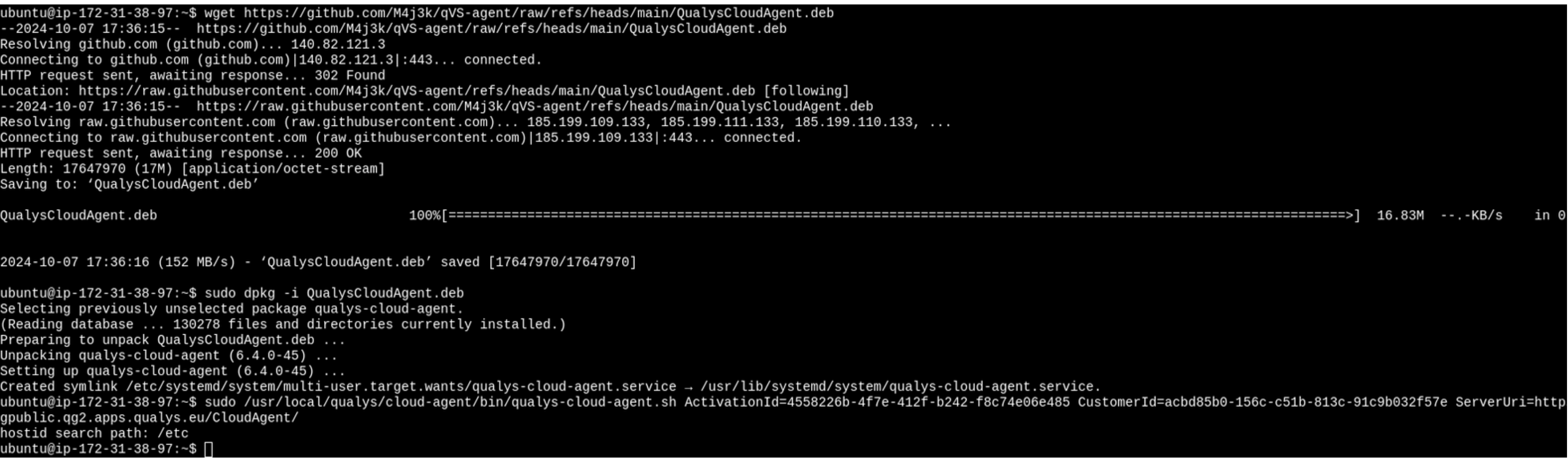
Copy **QualysCloudAgent.exe** to the host you w

Copy and paste this command for installation:

```
QualysCloudAgent.exe CustomerId={acb
91c9b032f57e} ActivationId={c483d275-
WebServiceUri=https://qagpublic.qg2.ap
```

Here's an example:

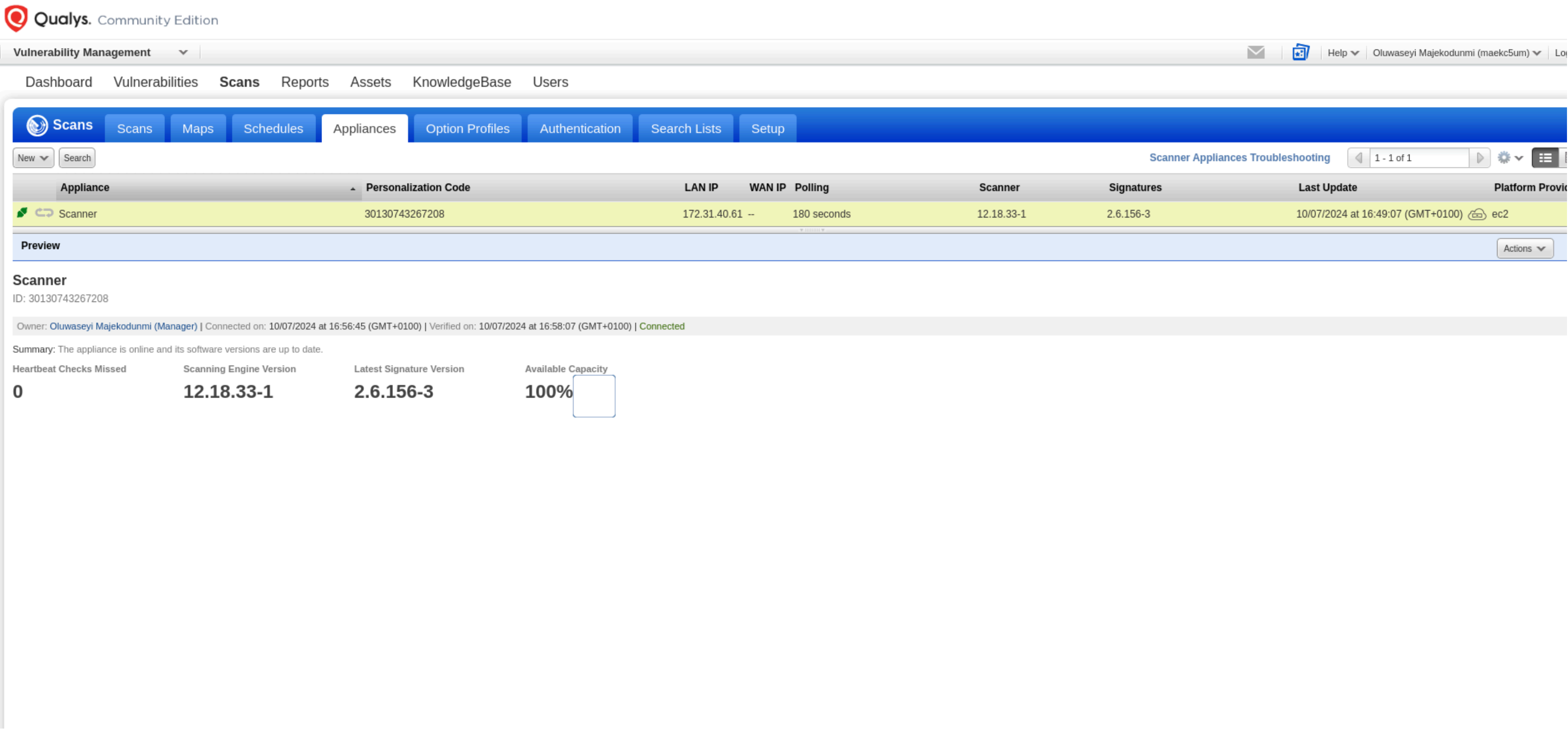
```
Microsoft Windows [Version 10.0.20348.2655]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\Users\Administrator\Downloads

C:\Users\Administrator\Downloads>QualysCloudAgent.exe CustomerId={acbd85b0-156c-c51b-813c-91c9b032f57e} ActivationId={c4
83d275-3a0a-4f1d-bf8d-6e0782595303} WebServiceUri=https://qagpublic.qg2.apps.qualys.eu/CloudAgent/
Successfully installed Qualys Windows Cloud Agent.

C:\Users\Administrator\Downloads>_
```



```
ubuntu@ip-172-31-38-97:~$ wget https://github.com/M4j3k/qVS-agent/raw/refs/heads/main/QualysCloudAgent.deb
--2024-10-07 17:36:15--  https://github.com/M4j3k/qVS-agent/raw/refs/heads/main/QualysCloudAgent.deb
Resolving github.com (github.com)... 140.82.121.3
Connecting to github.com (github.com)|140.82.121.3|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://raw.githubusercontent.com/M4j3k/qVS-agent/refs/heads/main/QualysCloudAgent.deb [following]
--2024-10-07 17:36:15--  https://raw.githubusercontent.com/M4j3k/qVS-agent/refs/heads/main/QualysCloudAgent.deb
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.109.133, 185.199.111.133, 185.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.109.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17647970 (17M) [application/octet-stream]
Saving to: ‘QualysCloudAgent.deb’

QualysCloudAgent.deb                          100%[==================================================================================================================>]  16.83M  --.-KB/s    in 0


2024-10-07 17:36:16 (152 MB/s) - ‘QualysCloudAgent.deb’ saved [17647970/17647970]

ubuntu@ip-172-31-38-97:~$ sudo dpkg -i QualysCloudAgent.deb
Selecting previously unselected package qualys-cloud-agent.
(Reading database ... 130278 files and directories currently installed.)
Preparing to unpack QualysCloudAgent.deb ...
Unpacking qualys-cloud-agent (6.4.0-45) ...
Setting up qualys-cloud-agent (6.4.0-45) ...
Created symlink /etc/systemd/system/multi-user.target.wants/qualys-cloud-agent.service → /usr/lib/systemd/system/qualys-cloud-agent.service.
ubuntu@ip-172-31-38-97:~$ sudo /usr/local/qualys/cloud-agent/bin/qualys-cloud-agent.sh ActivationId=4558226b-4f7e-412f-b242-f8c74e06e485 CustomerId=acbd85b0-156c-c51b-813c-91c9b032f57e ServerUri=http
gpublic.qg2.apps.qualys.eu/CloudAgent/
hostid search path: /etc
ubuntu@ip-172-31-38-97:~$ 
```

Configuration on Qualys Web GUI

Once the agents and the virtual scanner were set up, I made sure to verify on the **Qualys Web GUI** that the virtual scanner was active and correctly linked to the assets in my AWS environment and also the cloud agents were connected and reporting to the Qualys platform, ensuring that I had visibility into all target systems.



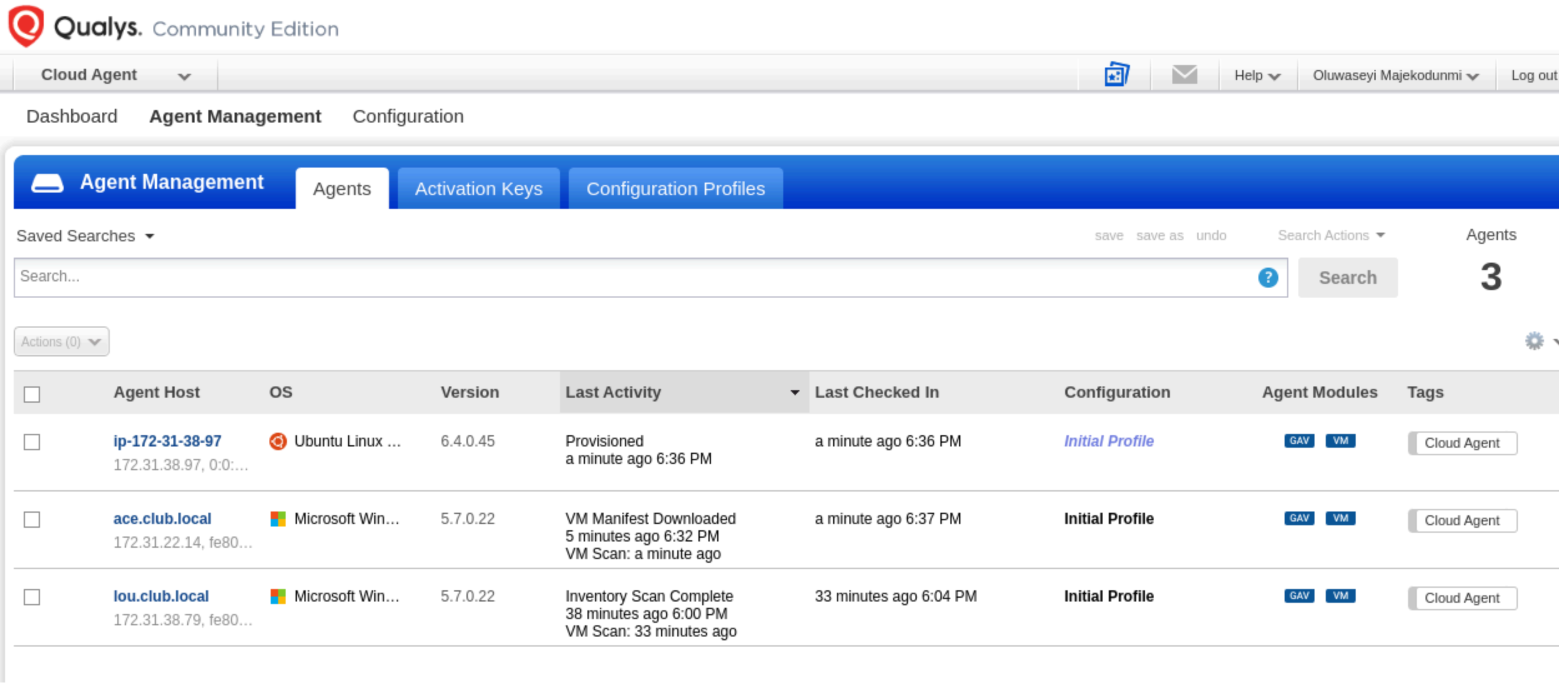
Appliance	Personalization Code	LAN IP	WAN IP	Polling	Scanner	Signatures	Last Update	Platform Provi
Scanner	30130743267208	172.31.40.61	--	180 seconds	12.18.33-1	2.6.156-3	10/07/2024 at 16:49:07 (GMT+0100)	ec2

Scanner
ID: 30130743267208

Owner: Oluwaseyi Majekodunmi (Manager) | Connected on: 10/07/2024 at 16:56:45 (GMT+0100) | Verified on: 10/07/2024 at 16:58:07 (GMT+0100) | Connected

Summary: The appliance is online and its software versions are up to date.

Heartbeat Checks Missed	Scanning Engine Version	Latest Signature Version	Available Capacity
0	12.18.33-1	2.6.156-3	100%



Agents
3

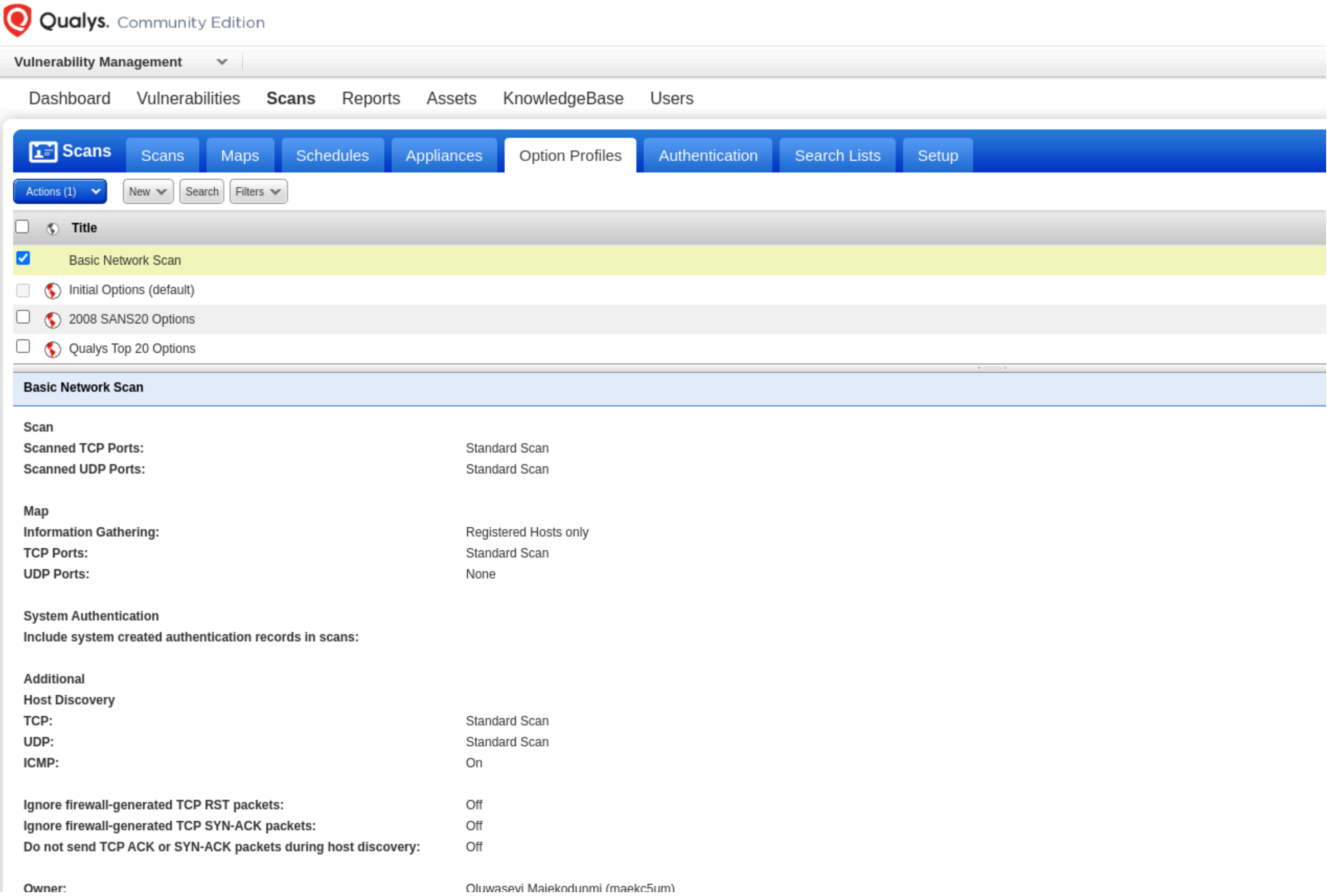
□	Agent Host	OS	Version	Last Activity	Last Checked In	Configuration	Agent Modules	Tags
□	ip-172-31-38-97 172.31.38.97, 0:0:...	Ubuntu Linux ...	6.4.0.45	Provisioned a minute ago 6:36 PM	a minute ago 6:36 PM	*Initial Profile*	GAV VM	Cloud Agent
□	ace.club.local 172.31.22.14, fe80...	Microsoft Win...	5.7.0.22	VM Manifest Downloaded 5 minutes ago 6:32 PM VM Scan: a minute ago	a minute ago 6:37 PM	Initial Profile	GAV VM	Cloud Agent
□	lou.club.local 172.31.38.79, fe80...	Microsoft Win...	5.7.0.22	Inventory Scan Complete 38 minutes ago 6:00 PM VM Scan: 33 minutes ago	33 minutes ago 6:04 PM	Initial Profile	GAV VM	Cloud Agent

With the environment properly configured, I was ready to start vulnerability scanning.

Basic Port Scanning

Set Up a New Option Profile

I began by creating a new option profile specifically configured for a basic port scan. This profile was designed to focus on identifying open ports on the client machines, allowing me to detect any exposed network services that could pose a security risk.



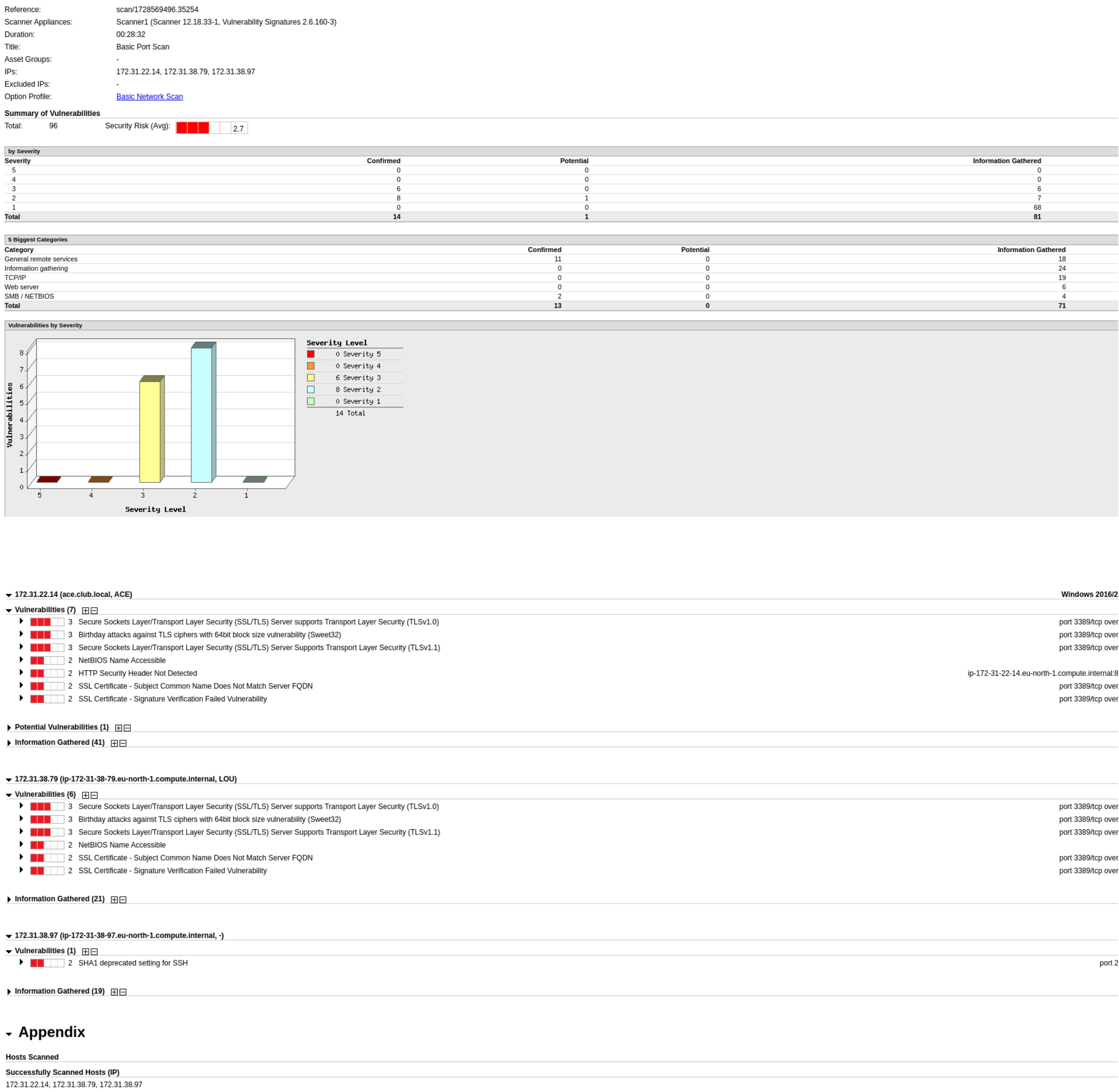
	Title
☑	Basic Network Scan
□	Initial Options (default)
□	2008 SANS20 Options
□	Qualys Top 20 Options

Basic Network Scan

Scan	
Scanned TCP Ports:	Standard Scan
Scanned UDP Ports:	Standard Scan
Map	
Information Gathering:	Registered Hosts only
TCP Ports:	Standard Scan
UDP Ports:	None
System Authentication	
Include system created authentication records in scans:	
Additional	
Host Discovery	
TCP:	Standard Scan
UDP:	Standard Scan
ICMP:	On
Ignore firewall-generated TCP RST packets:	Off
Ignore firewall-generated TCP SYN-ACK packets:	Off
Do not send TCP ACK or SYN-ACK packets during host discovery:	Off
Owner:	Oluwaseyi Majekodunmi (maekc5um)

Run the Basic Port Scan

After configuring the option profile, I initiated the scan across the client machines. This scan provided a preliminary overview of the network exposure, helping me assess the ports that were open and potentially vulnerable to exploitation.



Reference:	scan/1728569496.35254
Scanner Appliances:	Scanner1 (Scanner 12.18.33-1, Vulnerability Signatures 2.6.160-3)
Duration:	00:28:32
Title:	Basic Port Scan
Asset Groups:	-
IPs:	172.31.22.14, 172.31.38.79, 172.31.38.97
Excluded IPs:	-
Option Profile:	Basic Network Scan

Summary of Vulnerabilities

Total: 96 Security Risk (Avg): 🟥🟥🟥□□ 2.7

by Severity

Severity	Confirmed	Potential	Information Gathered
5	0	0	0
4	0	0	0
3	6	0	6
2	8	1	7
1	0	0	68
Total	**14**	**1**	**81**

5 Biggest Categories

Category	Confirmed	Potential	Information Gathered
General remote services	11	0	18
Information gathering	0	0	24
TCP/IP	0	0	19
Web server	0	0	6
SMB / NETBIOS	2	0	4
Total	**13**	**0**	**71**

Vulnerabilities by Severity

172.31.22.14 (ace.club.local, ACE) **Windows 2016/2**

Vulnerabilities (7) ⊞⊟

🟥🟥🟥□□	3	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)	port 3389/tcp over
🟥🟥🟥□□	3	Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)	port 3389/tcp over
🟥🟥🟥□□	3	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1)	port 3389/tcp over
🟥🟥□□□	2	NetBIOS Name Accessible	
🟥🟥□□□	2	HTTP Security Header Not Detected	ip-172-31-22-14.eu-north-1.compute.internal:8
🟥🟥□□□	2	SSL Certificate - Subject Common Name Does Not Match Server FQDN	port 3389/tcp over
🟥🟥□□□	2	SSL Certificate - Signature Verification Failed Vulnerability	port 3389/tcp over

Potential Vulnerabilities (1) ⊞⊟

Information Gathered (41) ⊞⊟

172.31.38.79 (ip-172-31-38-79.eu-north-1.compute.internal, LOU)

Vulnerabilities (6) ⊞⊟

🟥🟥🟥□□	3	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)	port 3389/tcp over
🟥🟥🟥□□	3	Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)	port 3389/tcp over
🟥🟥🟥□□	3	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1)	port 3389/tcp over
🟥🟥□□□	2	NetBIOS Name Accessible	
🟥🟥□□□	2	SSL Certificate - Subject Common Name Does Not Match Server FQDN	port 3389/tcp over
🟥🟥□□□	2	SSL Certificate - Signature Verification Failed Vulnerability	port 3389/tcp over

Information Gathered (21) ⊞⊟

172.31.38.97 (ip-172-31-38-97.eu-north-1.compute.internal, -)

Vulnerabilities (1) ⊞⊟

🟥🟥□□□	2	SHA1 deprecated setting for SSH	port 2

Information Gathered (19) ⊞⊟

Appendix

Hosts Scanned

Successfully Scanned Hosts (IP)

172.31.22.14, 172.31.38.79, 172.31.38.97

Analysis of the Scan Results

The results of the basic port scan highlighted several critical and moderate vulnerabilities that require immediate attention:

1. **TLS Vulnerabilities**: The use of outdated TLS versions (1.0 and 1.1) exposes the server to various attacks, including man-in-the-middle attacks and downgrade attacks. It is essential to configure the server to only support TLS 1.2 and above to mitigate these risks.
2. **Sweet32 Vulnerability**: The presence of the Sweet32 vulnerability suggests that sensitive data could be exposed through certain types of attacks. Remediation involves updating the cipher suites used for SSL/TLS connections to eliminate those with 64-bit block sizes.
3. **SSL Certificate Issues**: Misconfigured SSL certificates can undermine the trustworthiness of secure connections. Correcting the Subject Common Name to match the server's FQDN and ensuring proper signature verification are necessary steps to secure the SSL implementation.
4. **NetBIOS Exposure**: Accessible NetBIOS names can facilitate enumeration attacks and should be restricted to limit information disclosure.
5. **Weak SSH Configuration**: The use of SHA1 in SSH configurations indicates a need to enhance security measures. Upgrading to stronger algorithms will help protect against cryptographic vulnerabilities.

Next Steps

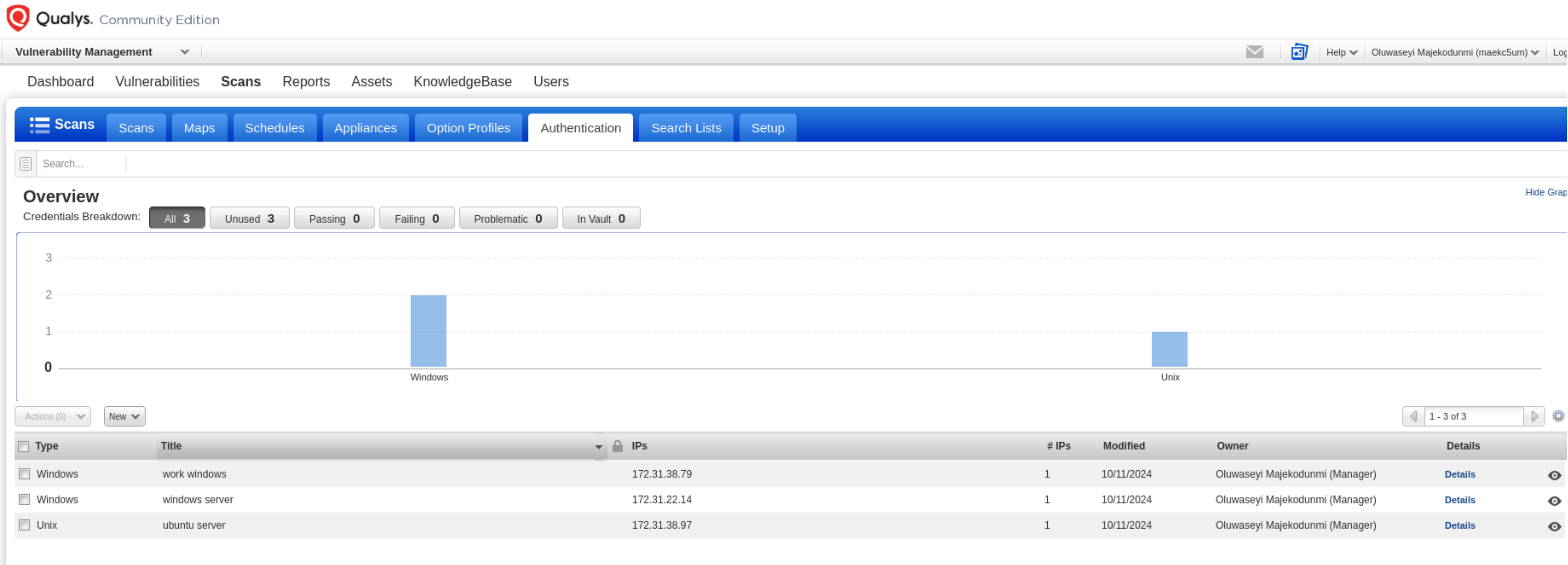
Based on the scan results, I prioritized the vulnerabilities for remediation. Immediate actions include:

- Updating the TLS configurations on the servers to support only secure protocols.
- Revisiting SSL certificate configurations to ensure they meet security standards.
- Restricting NetBIOS exposure and addressing the SHA1 usage in SSH.

Advanced Scanning with Authentication

Set Up Authentication

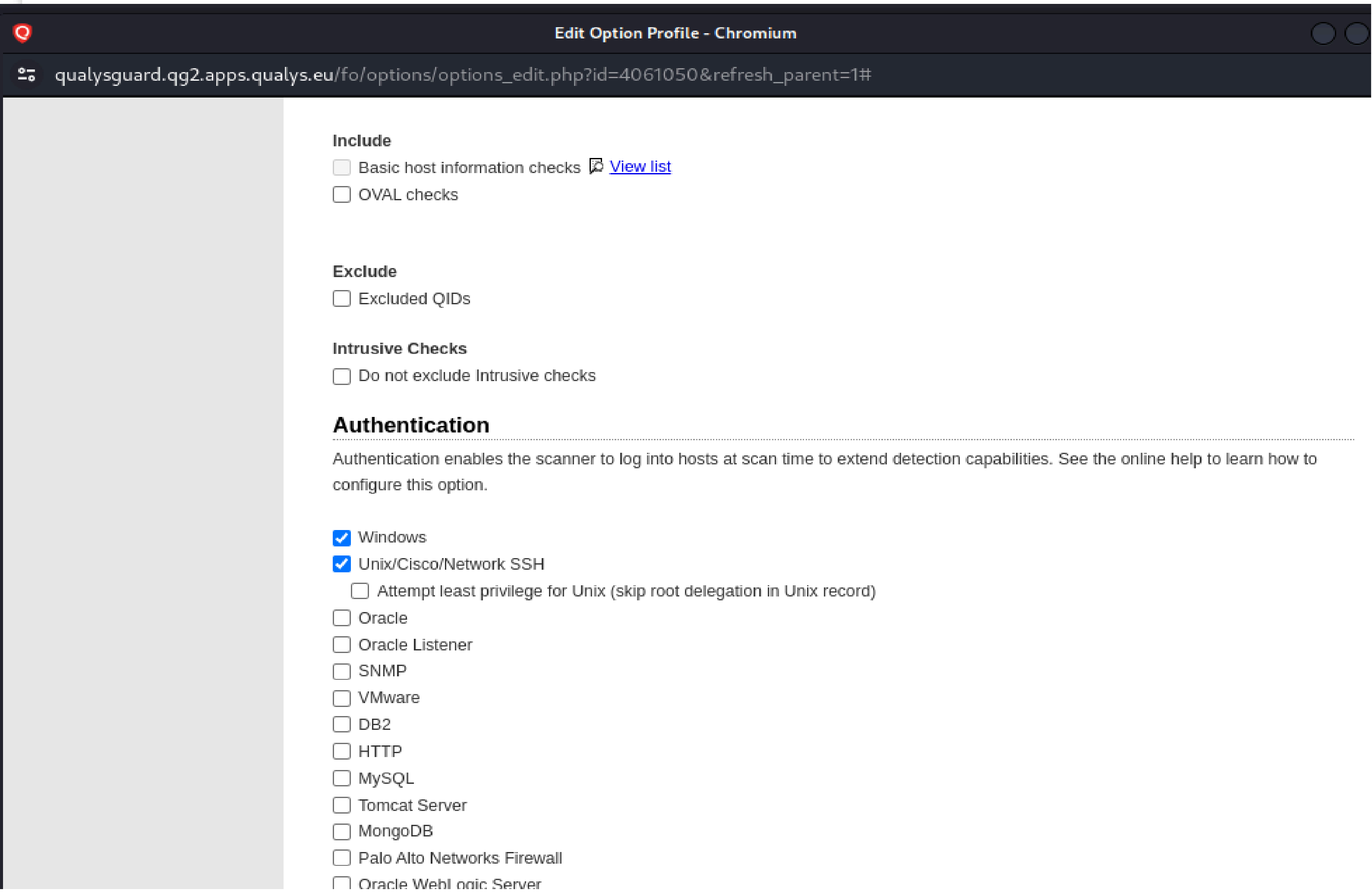
I added authentication credentials for both the Windows and Ubuntu systems on the **Qualys Web GUI.** After setting up the required credentials,I configured the authentication settings for both Windows and Unix within my scanning profile. These steps allowed me to access deeper system information, enabling the scans to retrieve detailed data from within the operating systems. This comprehensive access was essential for identifying vulnerabilities that might remain hidden during basic scans.



Overview

Credentials Breakdown: All 3 | Unused 3 | Passing 0 | Failing 0 | Problematic 0 | In Vault 0

Type	Title	IPs	# IPs	Modified	Owner	Details
Windows	work windows	172.31.38.79	1	10/11/2024	Oluwaseyi Majekodunmi (Manager)	Details
Windows	windows server	172.31.22.14	1	10/11/2024	Oluwaseyi Majekodunmi (Manager)	Details
Unix	ubuntu server	172.31.38.97	1	10/11/2024	Oluwaseyi Majekodunmi (Manager)	Details


Edit Option Profile - Chromium
qualysguard.qg2.apps.qualys.eu/fo/options/options_edit.php?id=4061050&refresh_parent=1#
View list

Include

□ Basic host information checks

□ OVAL checks

Exclude

□ Excluded QIDs

Intrusive Checks

□ Do not exclude Intrusive checks

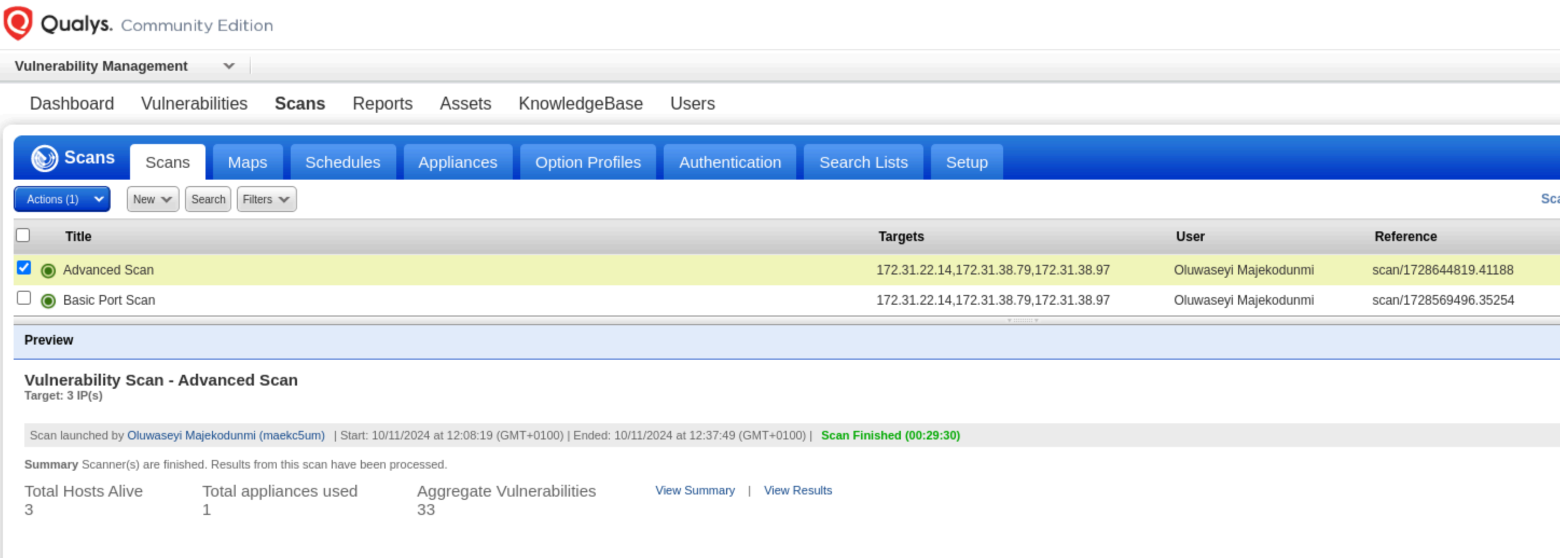
Authentication

Authentication enables the scanner to log into hosts at scan time to extend detection capabilities. See the online help to learn how to configure this option.

☑ Windows
☑ Unix/Cisco/Network SSH
  □ Attempt least privilege for Unix (skip root delegation in Unix record)
□ Oracle
□ Oracle Listener
□ SNMP
□ VMware
□ DB2
□ HTTP
□ MySQL
□ Tomcat Server
□ MongoDB
□ Palo Alto Networks Firewall
□ Oracle WebLogic Server

Run the Advanced Scan

With the authentication credentials in place, I initiated an advanced scan on the client machines. This scan was designed to delve deeper into the systems, leveraging the credentials to uncover vulnerabilities and configuration issues that might not be detectable during standard scans.



□	Title	Targets	User	Reference
☑	● Advanced Scan	172.31.22.14,172.31.38.79,172.31.38.97	Oluwaseyi Majekodunmi	scan/1728644819.41188
□	● Basic Port Scan	172.31.22.14,172.31.38.79,172.31.38.97	Oluwaseyi Majekodunmi	scan/1728569496.35254

Preview

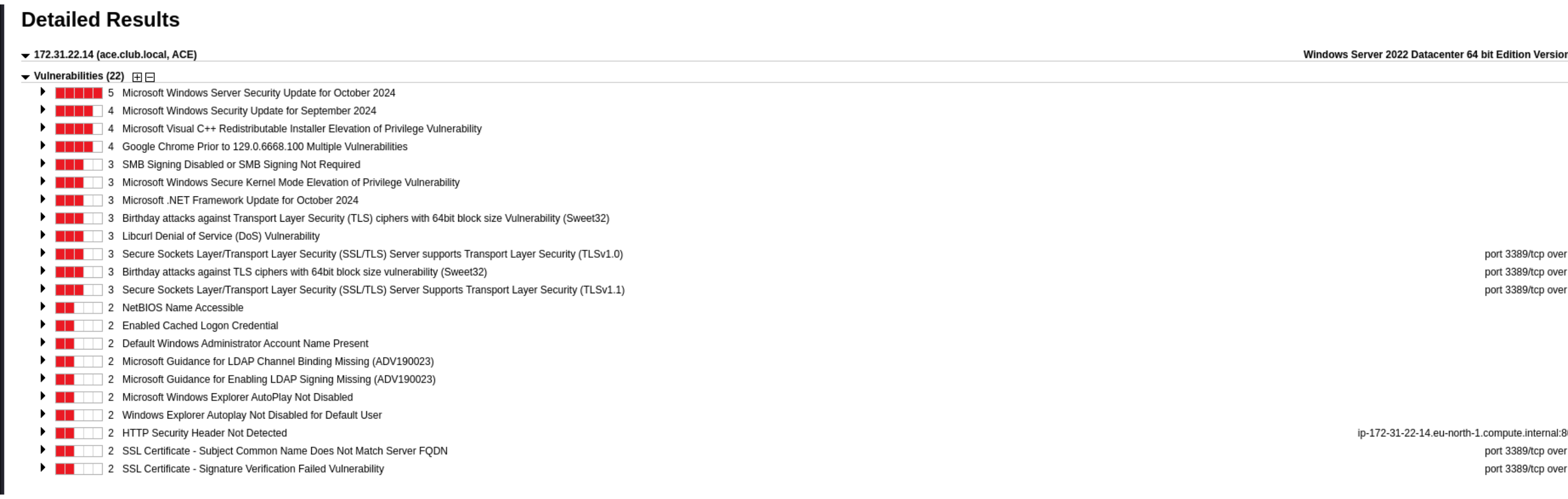
Vulnerability Scan - Advanced Scan
Target: 3 IP(s)

Scan launched by Oluwaseyi Majekodunmi (maekc5um) | Start: 10/11/2024 at 12:08:19 (GMT+0100) | Ended: 10/11/2024 at 12:37:49 (GMT+0100) | Scan Finished (00:29:30)

Summary Scanner(s) are finished. Results from this scan have been processed.

Total Hosts Alive	Total appliances used	Aggregate Vulnerabilities
3	1	33

View Summary | View Results



Detailed Results

172.31.22.14 (ace.club.local, ACE) Windows Server 2022 Datacenter 64 bit Edition Versior

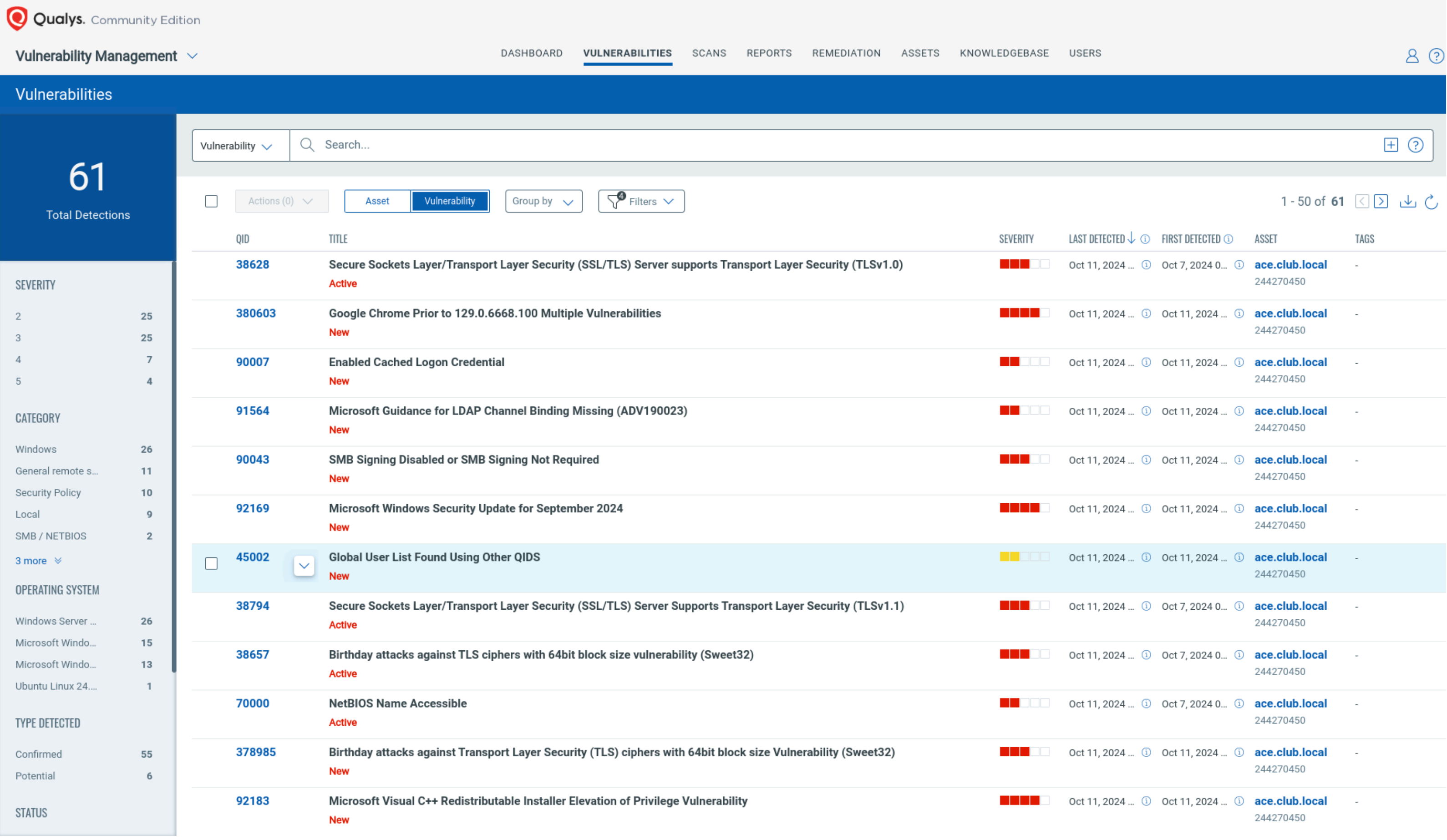
Vulnerabilities (22)

5	Microsoft Windows Server Security Update for October 2024	
4	Microsoft Windows Security Update for September 2024	
4	Microsoft Visual C++ Redistributable Installer Elevation of Privilege Vulnerability	
4	Google Chrome Prior to 129.0.6668.100 Multiple Vulnerabilities	
3	SMB Signing Disabled or SMB Signing Not Required	
3	Microsoft Windows Secure Kernel Mode Elevation of Privilege Vulnerability	
3	Microsoft .NET Framework Update for October 2024	
3	Birthday attacks against Transport Layer Security (TLS) ciphers with 64bit block size Vulnerability (Sweet32)	
3	Libcurl Denial of Service (DoS) Vulnerability	
3	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)	port 3389/tcp over
3	Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)	port 3389/tcp over
3	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1)	port 3389/tcp over
2	NetBIOS Name Accessible	
2	Enabled Cached Logon Credential	
2	Default Windows Administrator Account Name Present	
2	Microsoft Guidance for LDAP Channel Binding Missing (ADV190023)	
2	Microsoft Guidance for Enabling LDAP Signing Missing (ADV190023)	
2	Microsoft Windows Explorer AutoPlay Not Disabled	
2	Windows Explorer Autoplay Not Disabled for Default User	
2	HTTP Security Header Not Detected	ip-172-31-22-14.eu-north-1.compute.internal:8
2	SSL Certificate - Subject Common Name Does Not Match Server FQDN	port 3389/tcp over
2	SSL Certificate - Signature Verification Failed Vulnerability	port 3389/tcp over

Using advanced scanning with authentication enabled, I was able to dive deeper into the systems, uncovering not only network vulnerabilities but also those at the application level. This approach provided a more comprehensive view of the security posture, identifying critical software flaws, misconfigurations, and outdated applications that would have otherwise been missed during basic scans. By accessing internal system data, I could pinpoint weaknesses within the operating systems and applications themselves, enabling more precise vulnerability detection and remediation efforts.

Vulnerabilities Dashboard

In the Qualys dashboard, I reviewed the vulnerabilities associated with each asset. The dashboard provided a clear overview of the identified vulnerabilities, categorized by severity. Each asset was displayed alongside its associated risks, allowing me to prioritize remediation efforts effectively.



61

Total Detections

SEVERITY

2	25
3	25
4	7
5	4

CATEGORY

Windows	26
General remote s...	11
Security Policy	10
Local	9
SMB / NETBIOS	2

3 more

OPERATING SYSTEM

Windows Server ...	26
Microsoft Windo...	15
Microsoft Windo...	13
Ubuntu Linux 24....	1

TYPE DETECTED

Confirmed	55
Potential	6

STATUS

QID	TITLE	SEVERITY	LAST DETECTED	FIRST DETECTED	ASSET	TAGS
38628	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0) Active	🟥🟥🟥□□	Oct 11, 2024 ...	Oct 7, 2024 0...	ace.club.local 244270450	-
380603	Google Chrome Prior to 129.0.6668.100 Multiple Vulnerabilities New	🟥🟥🟥🟥□	Oct 11, 2024 ...	Oct 11, 2024 ...	ace.club.local 244270450	-
90007	Enabled Cached Logon Credential New	🟥🟥□□□	Oct 11, 2024 ...	Oct 11, 2024 ...	ace.club.local 244270450	-
91564	Microsoft Guidance for LDAP Channel Binding Missing (ADV190023) New	🟥🟥□□□	Oct 11, 2024 ...	Oct 11, 2024 ...	ace.club.local 244270450	-
90043	SMB Signing Disabled or SMB Signing Not Required New	🟥🟥🟥□□	Oct 11, 2024 ...	Oct 11, 2024 ...	ace.club.local 244270450	-
92169	Microsoft Windows Security Update for September 2024 New	🟥🟥🟥🟥□	Oct 11, 2024 ...	Oct 11, 2024 ...	ace.club.local 244270450	-
45002	Global User List Found Using Other QIDS New	🟨🟨□□□	Oct 11, 2024 ...	Oct 11, 2024 ...	ace.club.local 244270450	-
38794	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1) Active	🟥🟥🟥□□	Oct 11, 2024 ...	Oct 7, 2024 0...	ace.club.local 244270450	-
38657	Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) Active	🟥🟥🟥□□	Oct 11, 2024 ...	Oct 7, 2024 0...	ace.club.local 244270450	-
70000	NetBIOS Name Accessible Active	🟥🟥□□□	Oct 11, 2024 ...	Oct 7, 2024 0...	ace.club.local 244270450	-
378985	Birthday attacks against Transport Layer Security (TLS) ciphers with 64bit block size Vulnerability (Sweet32) New	🟥🟥🟥□□	Oct 11, 2024 ...	Oct 11, 2024 ...	ace.club.local 244270450	-
92183	Microsoft Visual C++ Redistributable Installer Elevation of Privilege Vulnerability New	🟥🟥🟥🟥□	Oct 11, 2024 ...	Oct 11, 2024 ...	ace.club.local 244270450	-

Conclusion

This project successfully demonstrated the use of the Qualys Cloud Platform to manage vulnerabilities in a variety of environments. The combination of Qualys Cloud Agents and the Virtual Scanner Appliance provided comprehensive vulnerability detection across a range of assets. While patching required manual intervention due to limitations in the Community Edition, the platform's detailed reports and guidance allowed for effective remediation of security risks.