Penetration Testing Report: SMTP Service Enumeration on Port 9001

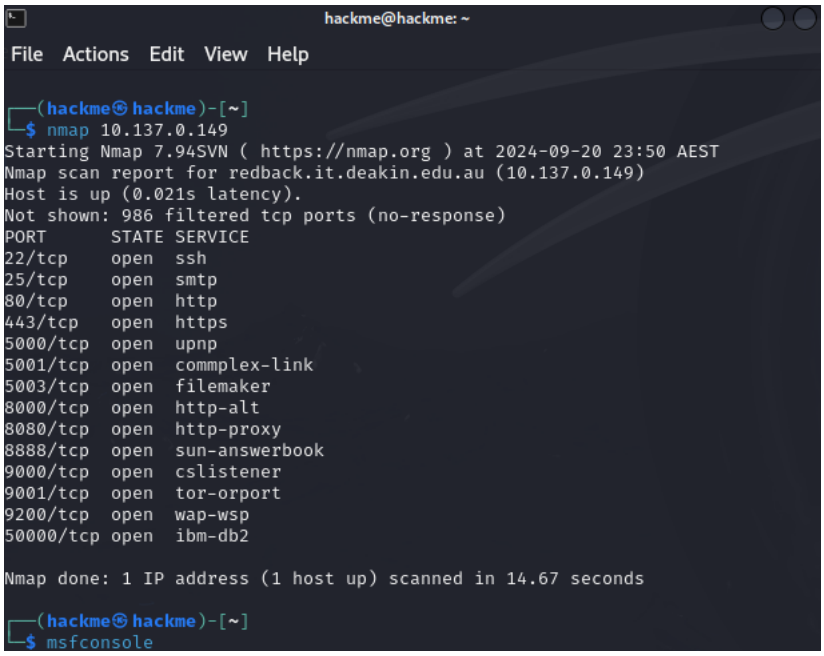
Target: 10.137.0.149

Test Conducted By: MD SAMSUL KABIR

Date:21/09/2024

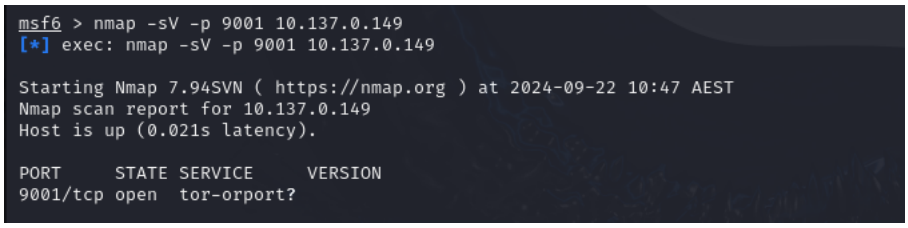
Test Scope: Authorized penetration testing on the Port 9001.

The penetration test was conducted on the MinIO service running on port 9001 of the target IP address 10.137.0.149. The test aimed to identify vulnerabilities associated with the service, particularly focusing on default credential usage and access controls.



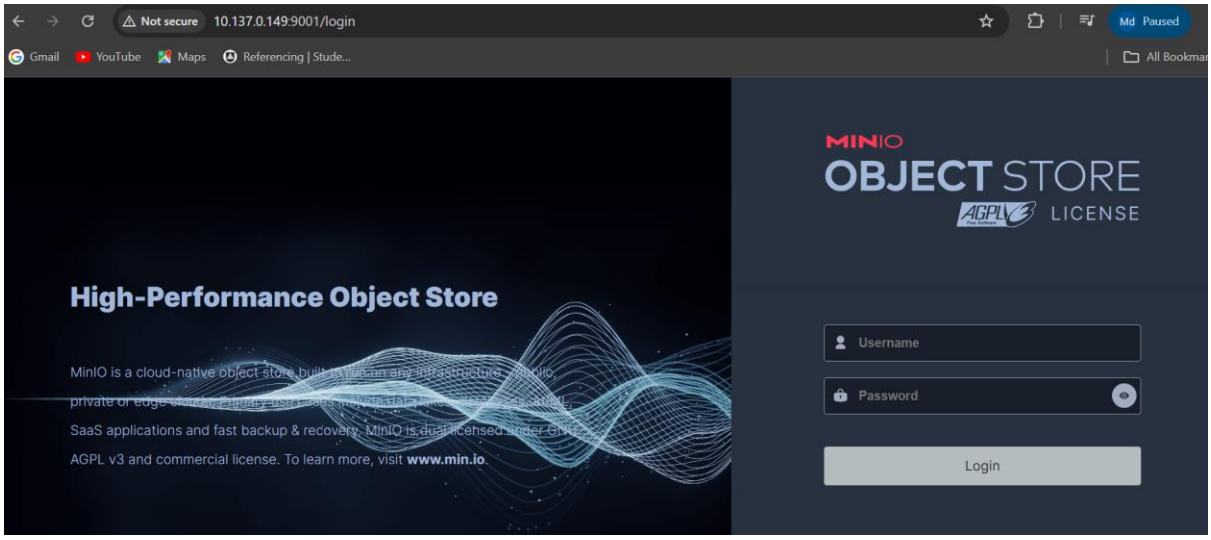
Open Ports

Service Detection



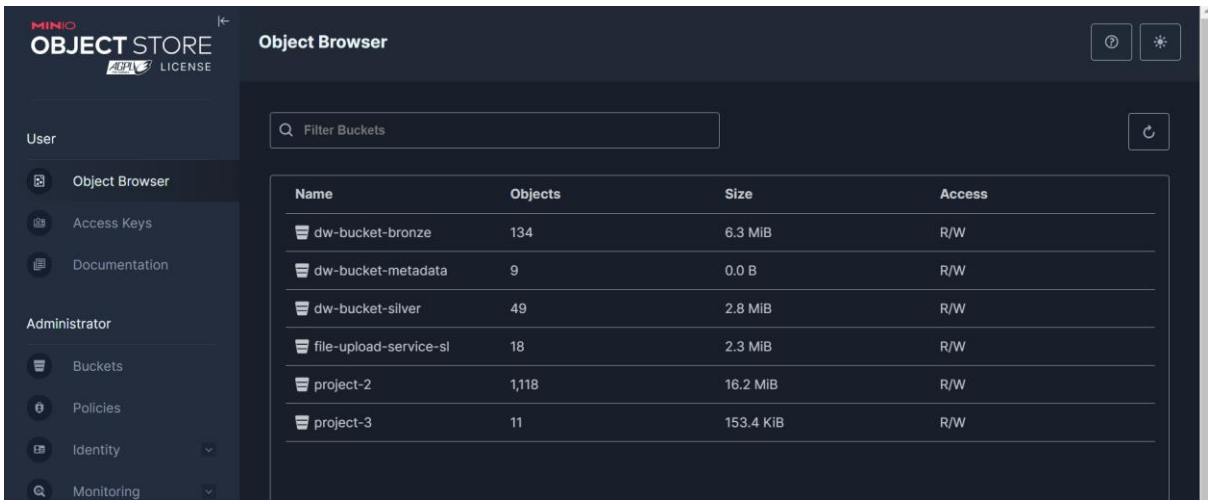
Service Detection

We can navigate to http://10.137.0.149:9001.

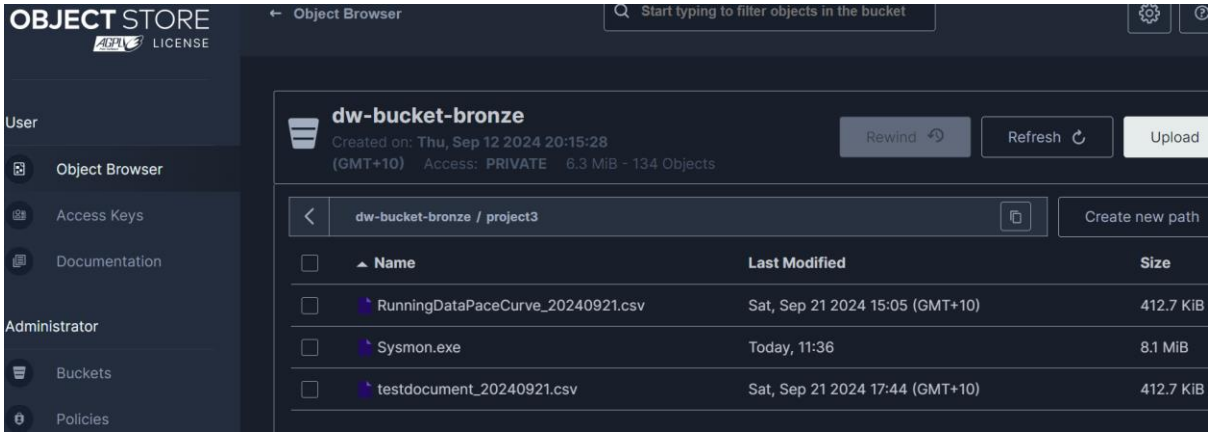


Minio Log in page

I always try default credentials during penetration testing because many organizations overlook changing them, which leaves their services vulnerable. This step allows me to gain quick access if defaults are still in use, highlighting significant security oversights. It also helps me assess the overall security posture of the environment. Demonstrating successful logins with default credentials provides clear evidence of vulnerabilities that need to be addressed in my final report. In this case default credentials actually works.

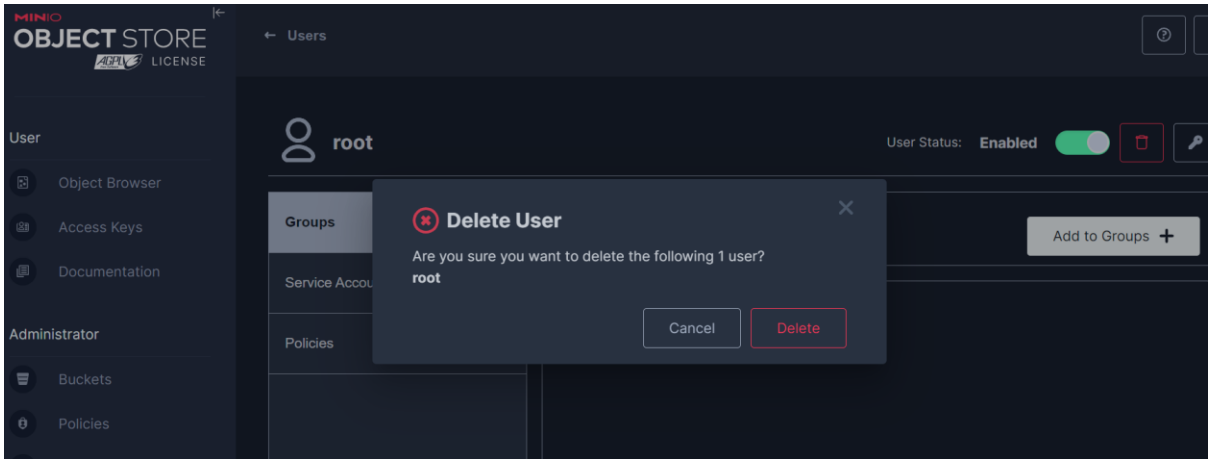


Logged in with default credentials



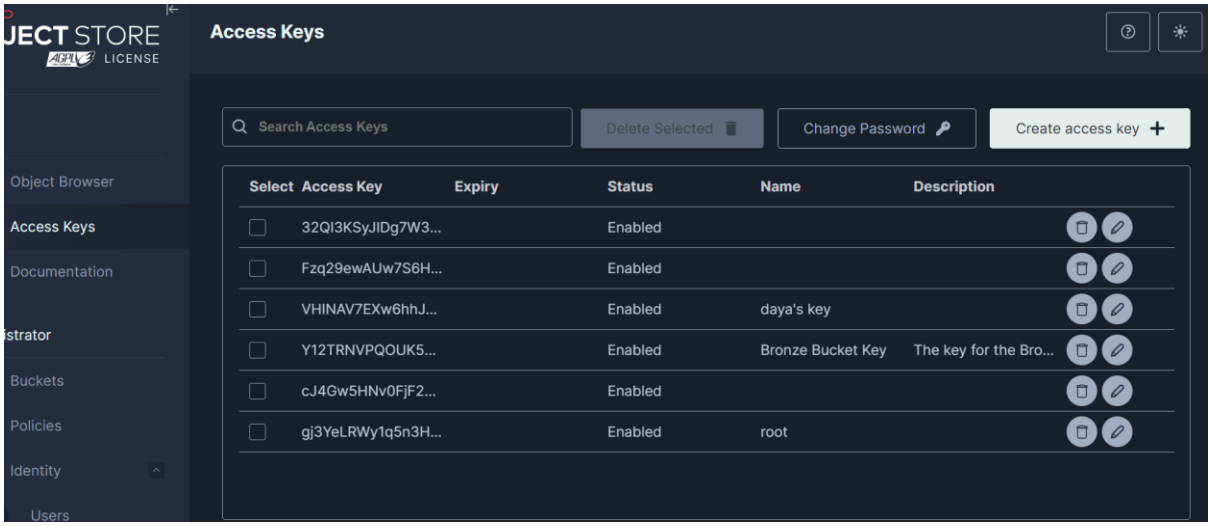
In the project-2 we was able to upload a ".exe" file which is a clear indication anyone can upload a malware.

We can also delete the users root privileges.



User can be deleted

We also can create and delete access keys.



Access keys Accessing

Findings

Access Granted with Default Credentials: Successfully logged in using default credentials.

File Upload Capability: The ability to upload a .exe file was confirmed. This presents a severe risk, as it allows for the potential upload of malware or malicious files.

User Management: It was possible to delete users and modify access privileges, including:

Deleting root user privileges and creating and deleting access keys.

Vulnerabilities Identified

Use of Default Credentials: The use of default login credentials is a critical vulnerability, allowing unauthorized access.

Insecure File Upload: The ability to upload executable files poses a risk for malicious exploitation.

Poor User Access Management: Inadequate controls over user privileges can lead to unauthorized actions within the MinIO service.

Recommendations

Change Default Credentials: Immediately change the default credentials to strong, unique passwords to enhance security.

Implement File Type Restrictions: Restrict file uploads to prevent executable files unless necessary. Consider validating file types before allowing uploads.

Review User Privileges: Establish strict access controls and regularly review user permissions to mitigate risks associated with privilege escalation.

Conduct Regular Security Audits: Regularly assess the security posture of the environment to identify and remediate vulnerabilities.

Conclusion

The penetration test on port 9001 revealed significant vulnerabilities associated with the MinIO service, primarily stemming from the use of default credentials and insecure configurations. Immediate actions are recommended to mitigate identified risks and strengthen the overall security posture.