Hybrid Vulnerability Scanning Lab Report

Author: Alan  
Date: May 2025  
Version: 1.0

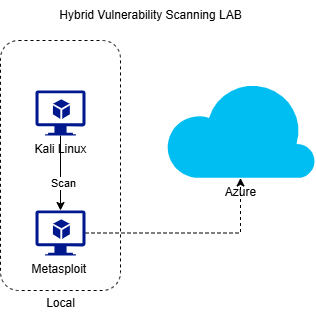
# Executive summary

This project demonstrates how vulnerability management practices can be adapted in hybrid environments by combining local scanning tools with cloud-based methodologies. While Azure restricts deploying intentionally vulnerable machines, this lab simulates real-world risk analysis by using a local setup (Nessus + Metasploitable) and documenting findings as if they were part of an Azure security program. It serves as a learning bridge between on-prem scanning and cloud-native protection tools like Microsoft Defender for Cloud.

# Objective

The goal of this lab is to simulate vulnerability management in a hybrid environment by combining on-premises scanning with cloud-based security management concepts using Azure.

**Diagram**



# Limitation

Azure does not allow deploying intentionally vulnerable virtual machines (such as Metasploitable) due to security and compliance policies.

# Workaround: Local Vulnerable Lab

To overcome this limitation, a local lab was built to safely perform network-based vulnerability scanning.

## Local Lab Setup

Scanning Machine: Linux VM running Nessus Essentials

Vulnerable Target: Metasploitable VM

Environment: Isolated Virtual Network on VirtualBox

# Azure Connection (Hybrid Simulation)

Although the vulnerable machine runs locally, the lab simulates a real-world hybrid environment by:  
- Treating the local VM as an on-premises asset managed together with Azure resources.  
- Documenting findings as if this VM were part of an Azure subscription.  
- Applying risk management workflows similar to those used with Azure Defender for Cloud.

# Tools Used

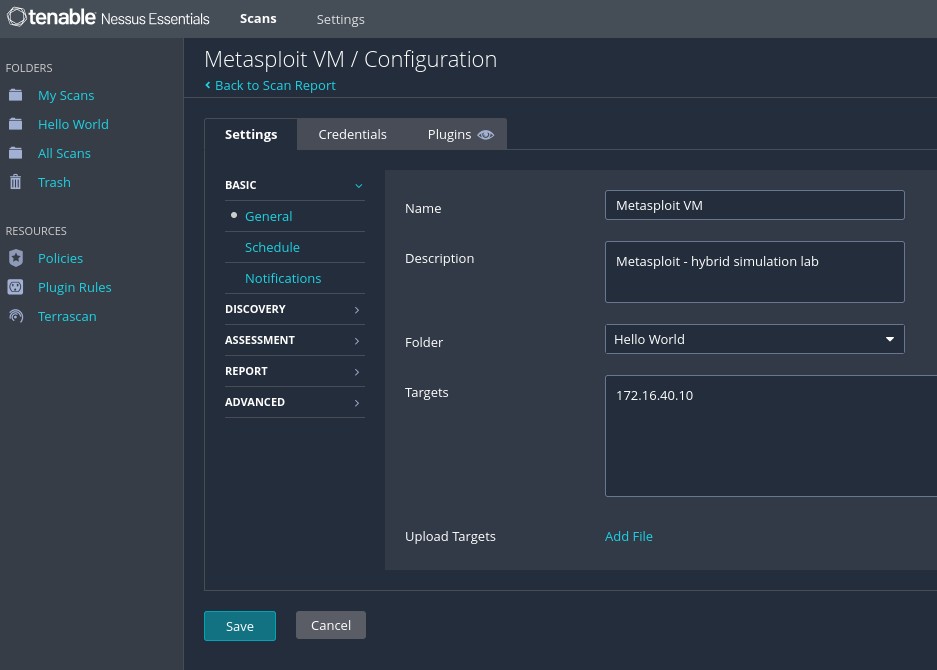
- Nessus Essentials (Free Vulnerability Scanner)  
- Metasploitable (Intentionally Vulnerable VM)  
- VirtualBox / VMware / Hyper-V (Hypervisor)  
- Azure Portal (For process comparison and future implementation)

# What Was Covered

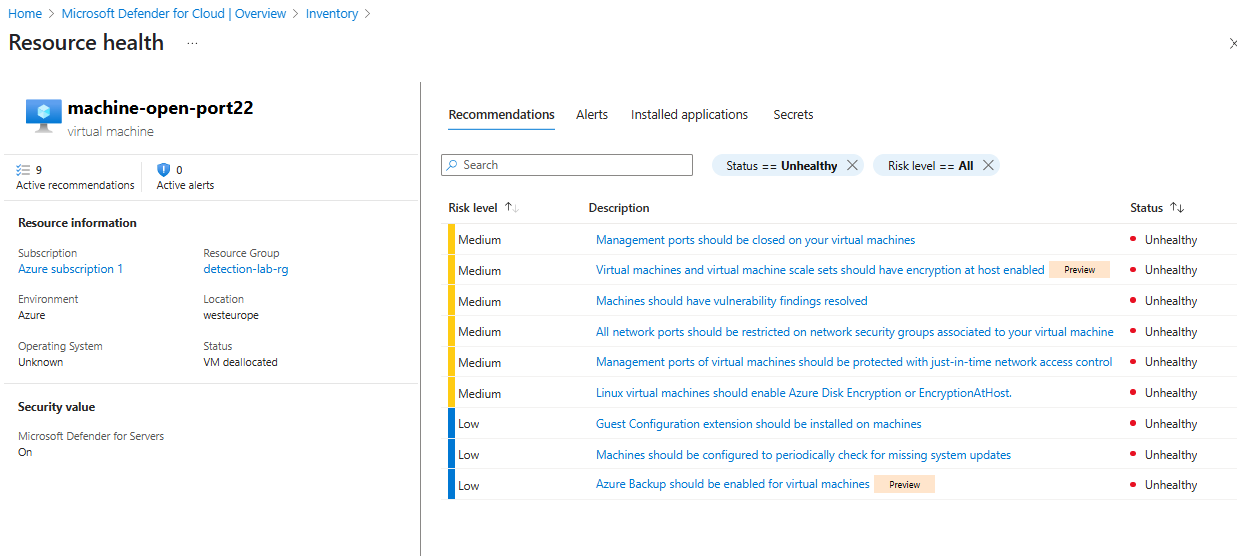
- Vulnerability scanning using Nessus Essentials  
- Identification of critical and high-risk vulnerabilities  
- Documentation of findings using Azure-like reporting structure  
- Preparing for agent-based vulnerability scanning with Azure Defender for Cloud

# Next Steps

- Repeat the process with Azure VMs using Defender for Cloud's Vulnerability Management (powered by Qualys)  
- Compare agent-based scanning vs network-based scanning  
- Document the differences in detection, coverage, and risk management



Findings comparation. Nessus’s Network scan vs Azure agent-based detection



Vulnerable machine created in Azure VM

A screenshot of a computer

AI-generated content may be incorrect.

Metasploit VM running in local environment

Report with

A table with numbers and letters

AI-generated content may be incorrect.

# Security Consideration

* Isolated virtual network
* No internet exposure
* No real or sensitive data used
* Compliant with Azure usage policies
* Controlled and safe lab environment

# Findings / Results Using Nessus, I scanned the Metasploitable VM and quickly found several high and critical vulnerabilities, like outdated services and remote code execution flaws. It was a great hands-on way to understand how attackers can find weak spots — and how security teams prioritize what to fix first..

# Conclusion

Even though I couldn’t use Azure directly for this part, building a local setup helped me simulate a hybrid environment and apply real-world security workflows. It reminded me that creativity matters in cybersecurity — you don’t need the perfect lab, just the right mindset to learn and improve.