TransferRoom –
Lead InfoSec Tech Assignment

Tasks:

- Recon & Vulnerability Assessment,
- Security Configuration Review

Overview

Two tasks selected from assignment:
1. Recon & Vulnerability Assessment
2. Security Configuration Review
Objective: Demonstrate practical InfoSec capabilities using Azure-based test servers

Environment Setup

- Platform: Microsoft Azure
- OS: Ubuntu Server (B1s tier)
- Tools/services: nmap, nikto, tenable, UFW, docker, Apache
- One VM provisioned for the two tasks

RDP login creds
Public IP: 20.84.67.45
username: infosecuser
password: Techtest123@

Task 1: Recon & Vulnerability Assessment

- Deployed Ubuntu VM on Azure
- Scanned open ports using Nmap
- Identified services and versions
- Conducted vulnerability scan using Nessus and Nikto
- Compiled prioritized list of findings

(Attached the full vulnerability scan report in the github repo)

Task 1: Findings Summary

Portscan:

- Nmap found two open scans: port 22 and 80

(Full Nmap scan submitted in the repo)

- Also identified the Apache service running on the server

Nmap scan command: *sudo nmap -T4 -sS -sV -A 20.84.67.45 > nmap.txt*

- **Vulnerability scan – Tenable (severity classified by criticality(CVSS)**
- A total number of 19 vulnerabilities
- 1 medium rated vulnerability – RDP MITM weakness
- The others were informational

Recommendations

- Restrict access to RDP/SSH only to authorized Ips/networks
- Enforce encryption in transit for RDP access

Task 2: Security Configuration Review

- Reviewed SSH configuration for secure settings
- Audited firewall rules UFW and Azure NSG rules
- User permissions review(both OS and Azure Entra ID)
- Inspected logs for anomalies(System, auth, Azure activity logs,etc)

Task 2: Findings & Recommendations

Findings

- Firewall had broad port access
- Firewall inactive at the OS level
- Some users “might have” unnecessary Sudo rights
- Privileged users do not have MFA enabled

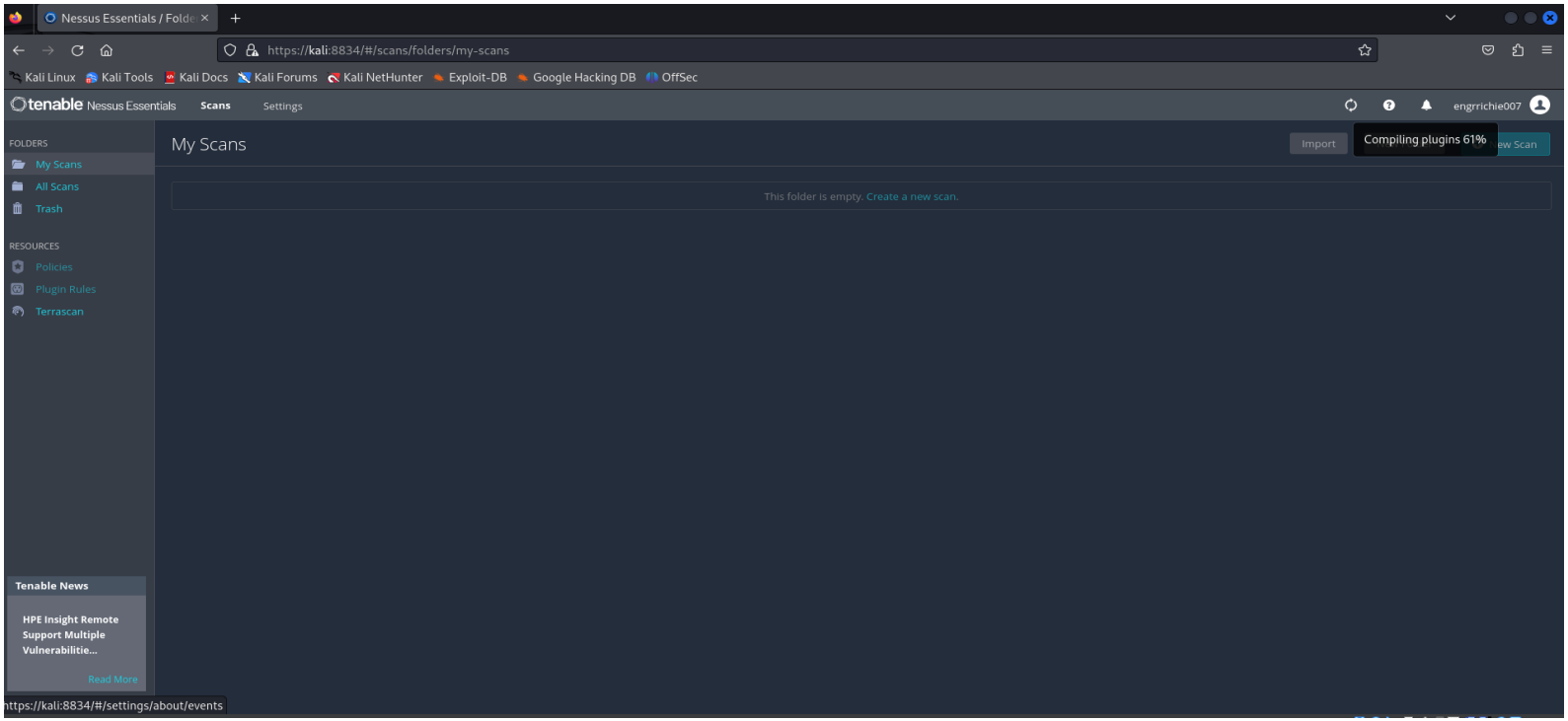
Recommendations:

Harden firewall rules(SSH, RDP, etc.) at the Azure NSG level
Enable and harden firewall at the OS level.
Enforce least privilege – only grant Sudo privileges to users that require it.
Enforce MFA for privileged users in Azure.

Technical Challenges

Nessus plugin installation took forever initially-
had to switch to Nikto vulnerability scan as a back up

Reason I had a separate video for Nessus scan.



Conclusion

Successfully completed both tasks
Ready to discuss findings and methodology in detail

Appendix & References

- Azure VM setup: https://learn.microsoft.com/en-us/azure/virtual-machines/
- CVSS Scoring System: https://www.first.org/cvss/
- nmap documentation: https://nmap.org/book/
- Nessus essential: https://www.tenable.com/products/nessus/nessus-essentials