Agent Based Monitoring in a Remote Device Utilizing a Linux/Ubuntu Virtual Machine

October 17, 2025

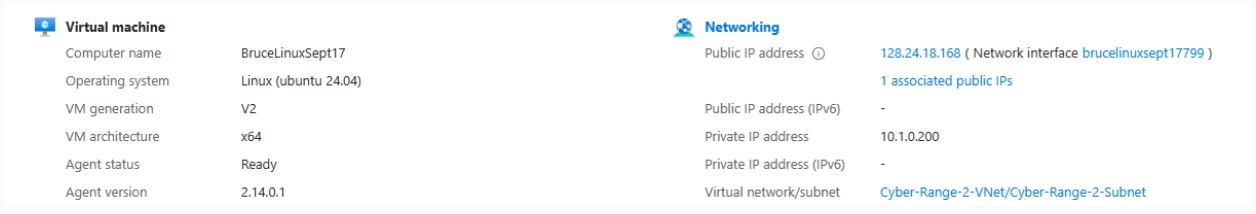
Bruce Thornton

In this Lab I am creating a virtual reality where an “Employee” is working at a workstation/computer/device “remotely.” I have created an “Agent” to be a “Local Agent” and installed it on the workstation/computer/device to perform an assessment of vulnerabilities, and observe the results in our Tenable portal. In order to facilitate this in this “virtual reality” I have placed the file “start.txt” on the workstation/computer/device (aka: Virtual Machine) to create a potential vulnerability to find and resolve. This file named “start.txt” will trigger the scan Agent and begin the process of allowing this scan Agent to remove this file “start.txt.” We will be able to watch the file be removed from this workstation/computer/device in real time.

Tools Used:

- Tenable.sc / Nessus
- Microsoft Azure Virtual Machine

In this Lab I have provisioned a Linux/Ubuntu Virtual Machine using Microsoft Azure.



Virtual machine

Computer name	BruceLinuxSept17
Operating system	Linux (ubuntu 24.04)
VM generation	V2
VM architecture	x64
Agent status	Ready
Agent version	2.14.0.1

Networking

Public IP address	128.24.18.168 (Network interface brucelinuxsept17799)
	1 associated public IPs
Public IP address (IPv6)	-
Private IP address	10.1.0.200
Private IP address (IPv6)	-
Virtual network/subnet	Cyber-Range-2-VNet/Cyber-Range-2-Subnet

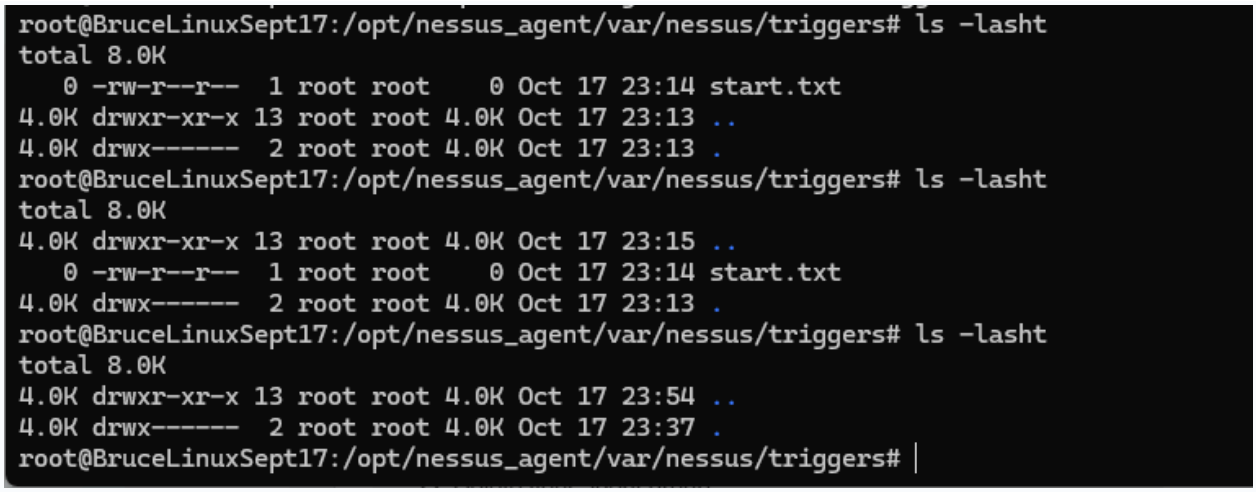
I have also utilized Tenable to create an Agent Based Scan.

This command is provided within Tenable under: settings -> Sensors -> Nessus Agents -> +Add Nessus Agent, on the right side of the screen I find the Windows command and highlight and copy it. I will open the Command Line on my own Computer and SSH into the Virtual Machine and the run the command:

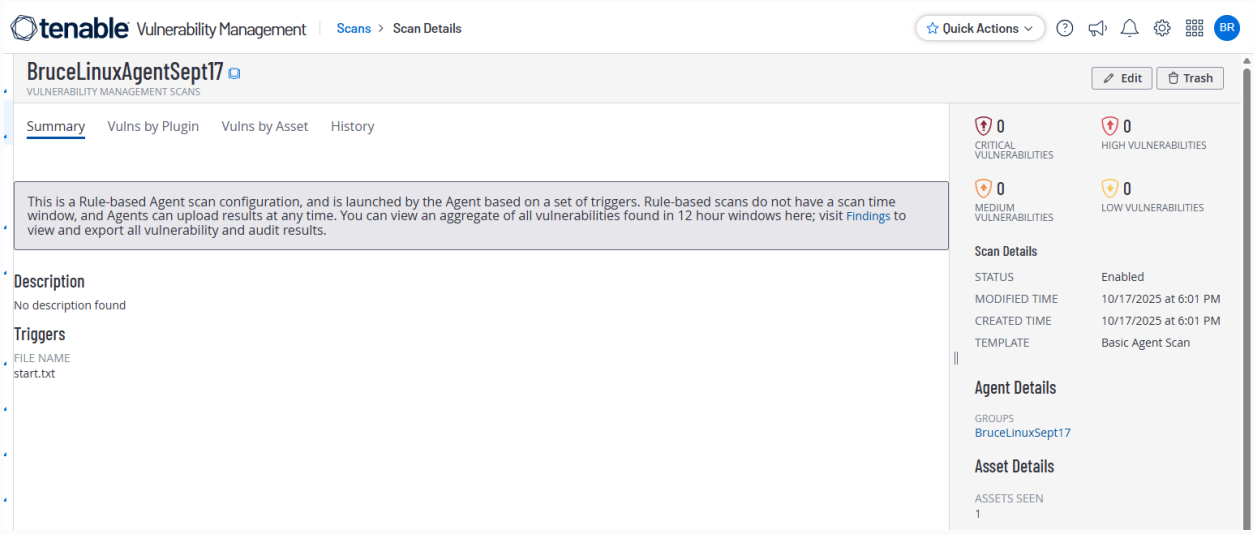
curl -H 'X-Key: 58aab372289ac80911e4c5ad40a07b23b5524319f9ff5c010aa50ec625ccf389' 'https://sensor.cloud.tenable.com/install/agent?name=agent-name&groups=agent-group' | bash

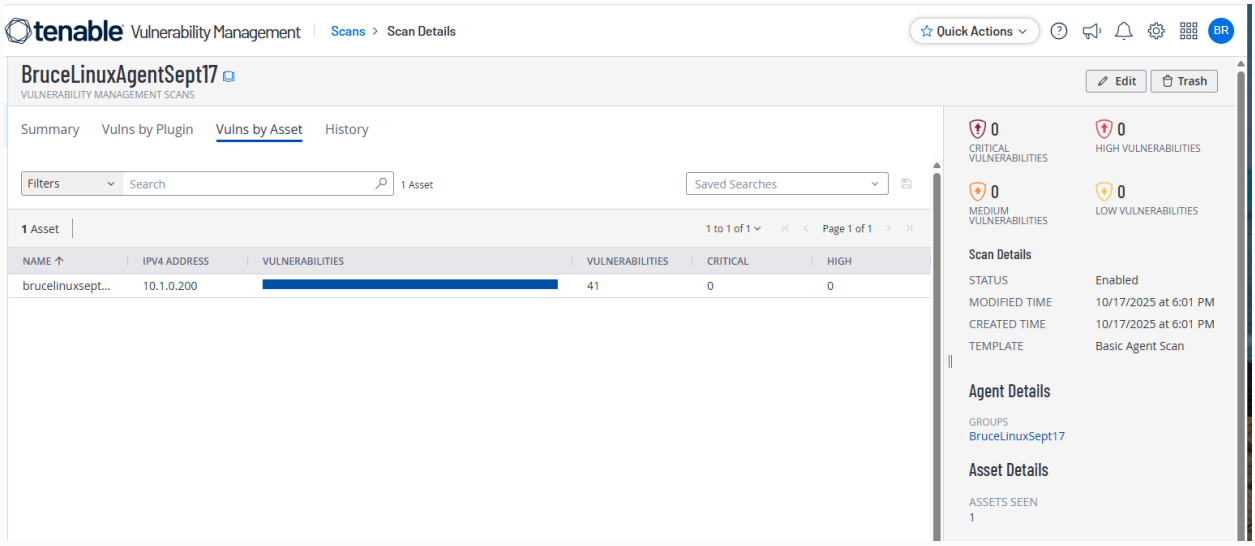
Configured and Agent is running as shown in this screenshot:

I have had the file “start.txt” installed into the “triggers” file. And now I can demonstrate the subtle process of watching the Agent pick up the “trigger” file, and remove it as shown in this screenshot:

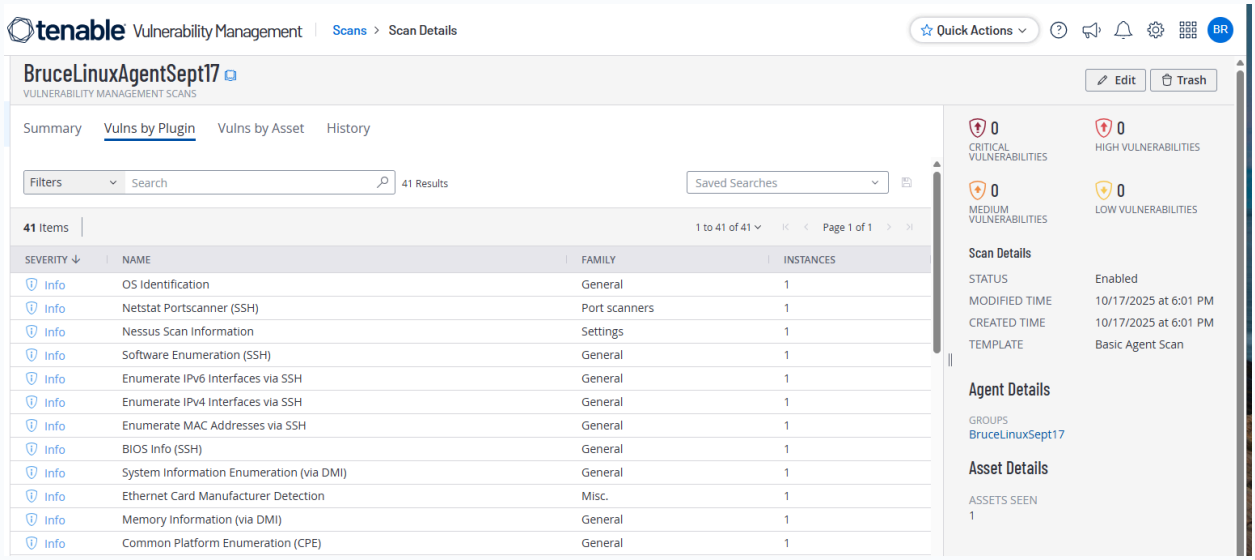


I have the evidence of the findings and the time that this scan and Agent have ran within this next screenshot. We see the Assets and findings listed as “start.txt.” Listed under “Assets seen.”





I can also demonstrate the success of this Agent deployment in the following screenshot, which shows the vulnerabilities that it was able to discover. Most of these vulnerabilities are not necessarily the most severe, however this definitely shows the success of this deployment.



Concluding this Lab and moving forward, these vulnerabilities can be remediated at this point. I can scan the results of my remediations by adjusting our scan criteria.

This Lab demonstrates my ability to work with Enterprise grade tools, setting up and utilizing real world tools and techniques to successfully create and deploy an Agent in Tenable for use with remote workstations/computers/devices for Vulnerability Management and Remediation.