

Agent Based Monitoring in a Remote Device Utilizing a Windows 11 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 Windows 11 Virtual Machine using Microsoft Azure.

Virtual machine		Networking	
Computer name	Win11VMBruce	Public IP address ⓘ	-
Operating system	Windows (Windows 11 Pro)	Public IP address (IPv6)	-
VM generation	V2	Private IP address	10.1.0.170
VM architecture	x64	Private IP address (IPv6)	-
Agent status	Ready	Virtual network/subnet	Cyber-Range-2-VNet/Cyber-Range-2-Subnet

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

Windows10-Basic agent Scan					See All Details	×
Activity	Created	Vulnerabilities by Severity		Scan Duration	Type	Template
	07/29/2025 at 5:31 PM	CRITICAL 0	HIGH 0	12hr	N/A	Basic Agent Scan
	Started	MEDIUM 0	LOW 0	Targets	Schedule	
	10/16/2025 at 7:00 PM			N/A	Triggered	
	Running					
	10/17/2025 at 7:00 AM					

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 PowerShell ISE on the Virtual Machine and then run the command:

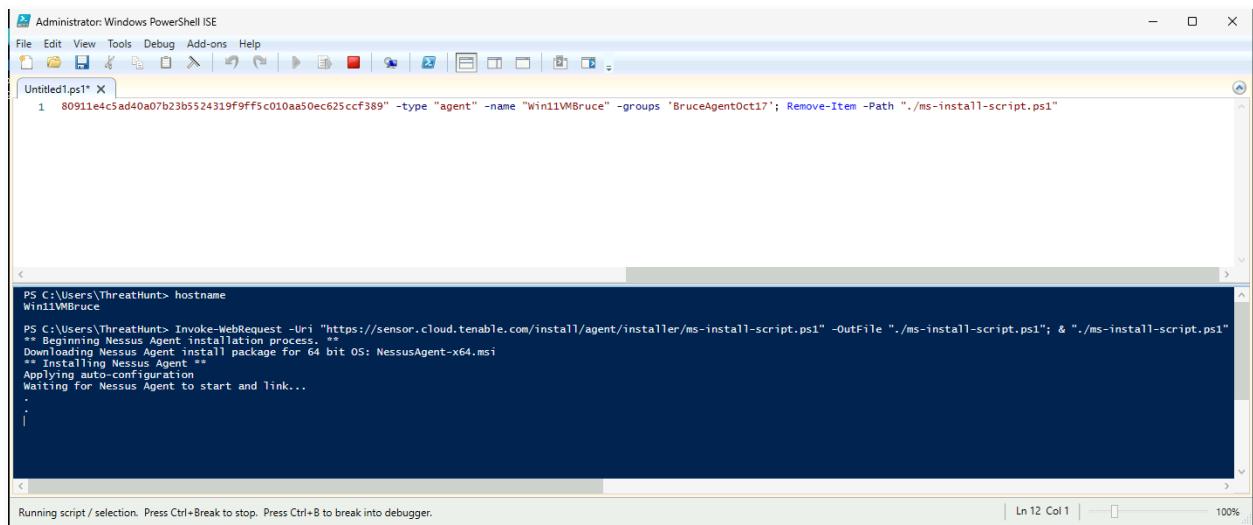
Invoke-WebRequest -Uri

"https://sensor.cloud.tenable.com/install/agent/installer/ms-install-script.ps1"

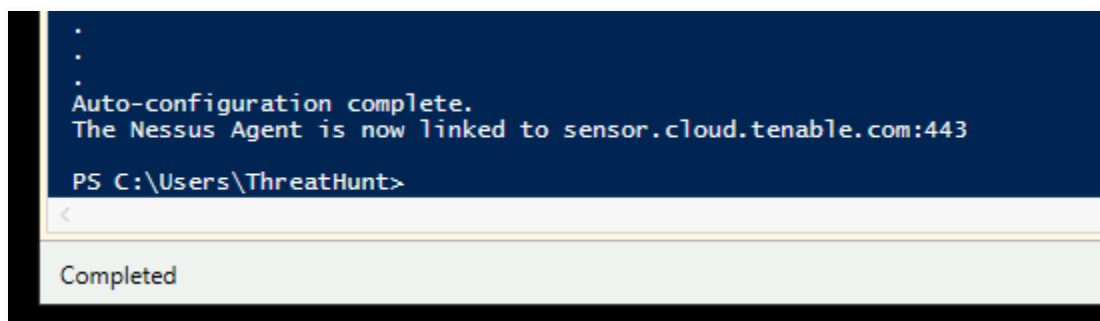
-OutFile ".\ms-install-script.ps1"; & ".\ms-install-script.ps1" -key

"58aab372289ac80911e4c5ad40a07b23b5524319f9ff5c010aa50ec625ccf389"

-type "agent" -name "Win11VMBruce" -groups 'BruceAgentOct17'; Remove-Item -Path ".\ms-install-script.ps1"



The screenshot shows the Windows PowerShell ISE interface. The top pane displays the command: `1 80911e4c5ad40a07b23b5524319f9ff5c010aa50ec625ccf389" -type "agent" -name "Win11VMBruce" -groups 'BruceAgentOct17'; Remove-Item -Path ".\ms-install-script.ps1"`. The bottom pane shows the output: `PS C:\Users\ThreatHunt> hostname
Win11VMBruce
PS C:\Users\ThreatHunt> Invoke-WebRequest -Uri "https://sensor.cloud.tenable.com/install/agent/installer/ms-install-script.ps1" -OutFile ".\ms-install-script.ps1"; & ".\ms-install-script.ps1"
** Beginning Nessus Agent installation process. **
Downloading Nessus Agent install package for 64 bit OS: NessusAgent-x64.msi
** Installing Nessus Agent **
Applying auto-configuration
Waiting for Nessus Agent to start and link...
. .
|`



The screenshot shows the final output of the PowerShell command: `.
. .
Auto-configuration complete.
The Nessus Agent is now linked to sensor.cloud.tenable.com:443
PS C:\Users\ThreatHunt>`

The Agent is now properly installed on my Virtual Machine. Now I will give the Agent the file: "start.txt" to trigger the scan and initiate the process of removing the file "start.txt."


I will demonstrate the file path taken and the commands to install the file: "start.txt" here:

```
PS C:\Users\ThreatHunt> cd \
PS C:\> cd ProgramData
PS C:\ProgramData> cd Tenable
PS C:\ProgramData\Tenable> cd '.\Nessus Agent\'
PS C:\ProgramData\Tenable\Nessus Agent> cd nessus
PS C:\ProgramData\Tenable\Nessus Agent\nessus> cd triggers
PS C:\ProgramData\Tenable\Nessus Agent\nessus\triggers> New-Item -Name start.txt

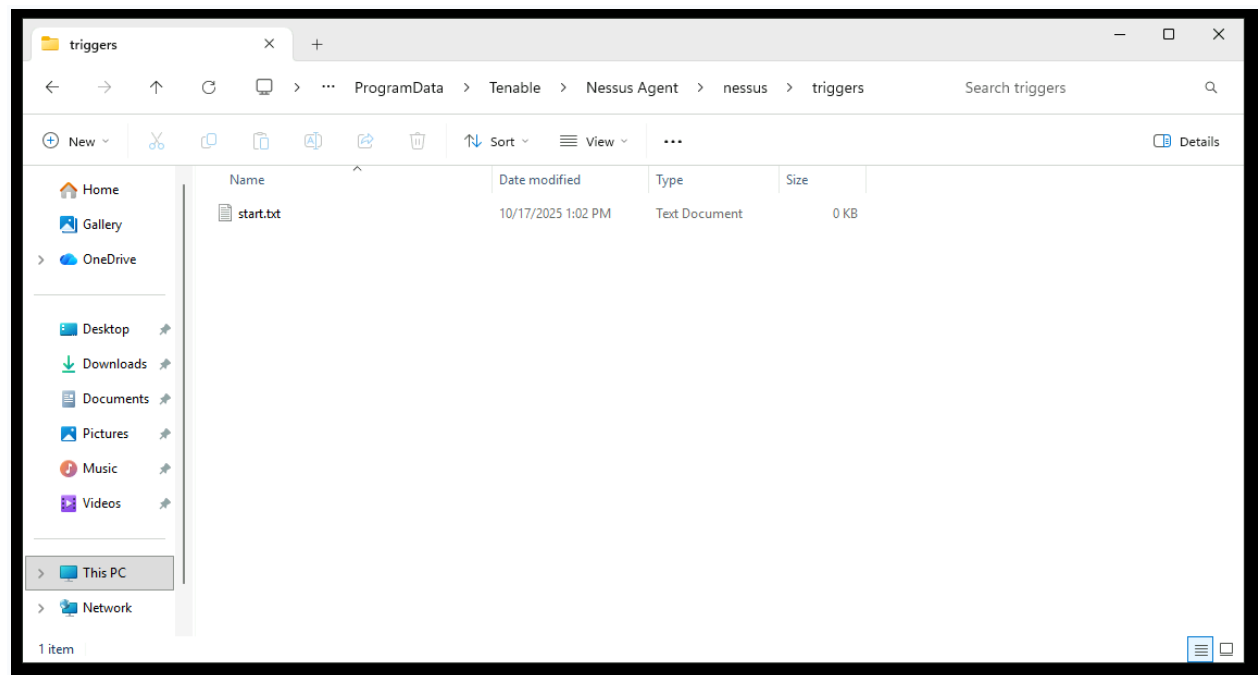
Directory: C:\ProgramData\Tenable\Nessus Agent\nessus\triggers

Mode                LastWriteTime         Length Name
----                -
-a-----         10/17/2025   1:02 PM             0 start.txt

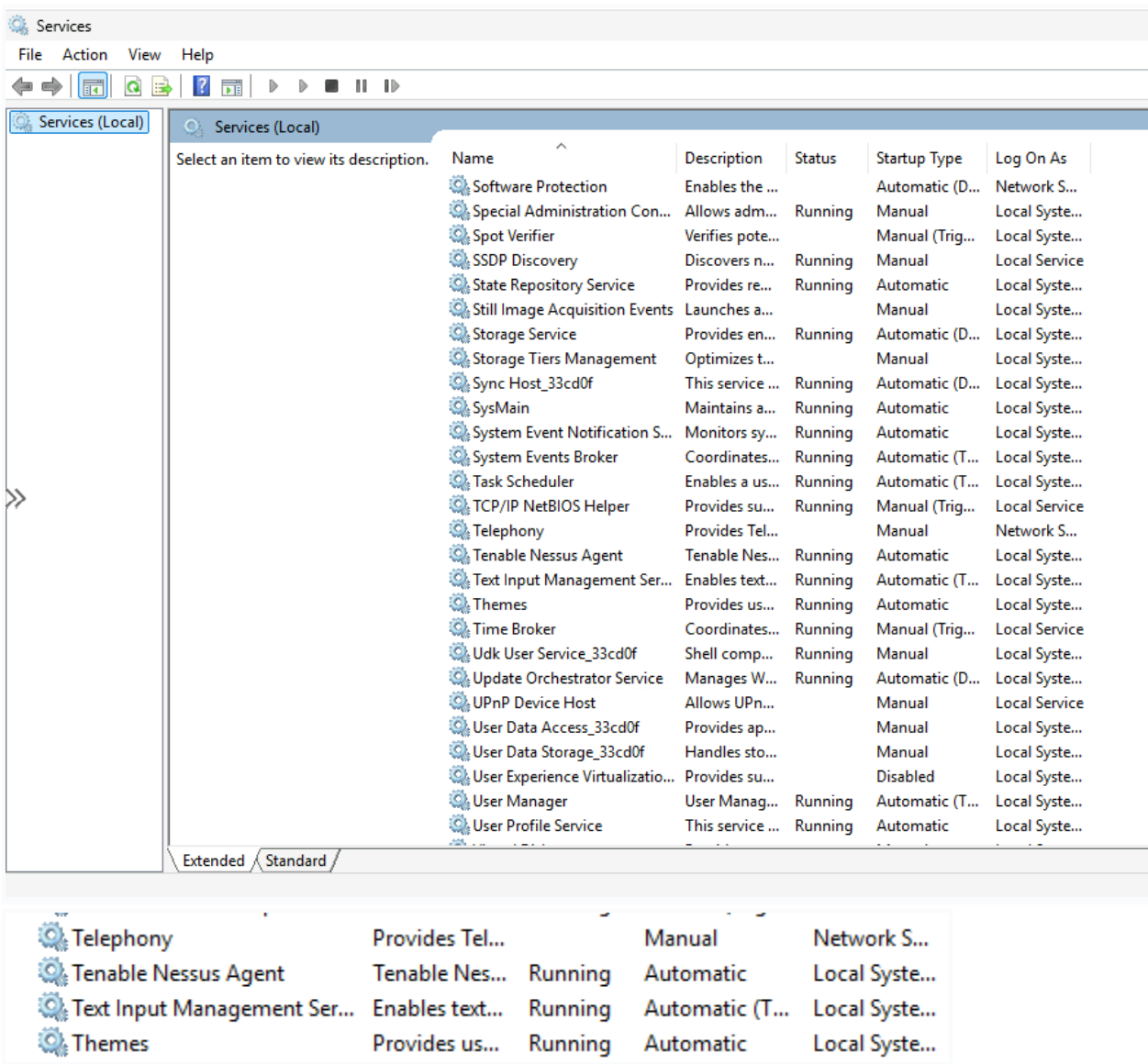
PS C:\ProgramData\Tenable\Nessus Agent\nessus\triggers> |
```



I have successfully created the file to trigger the scan Agent.

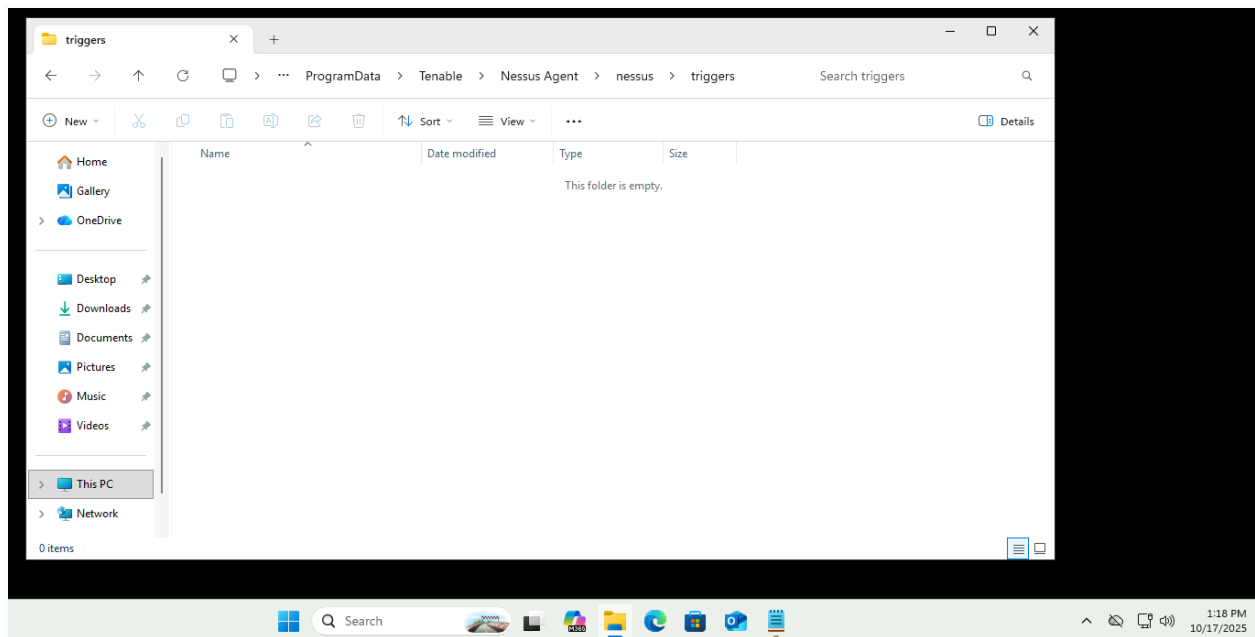


I check to ensure that Tenable is running by opening the Command Line and running: `services.msc`

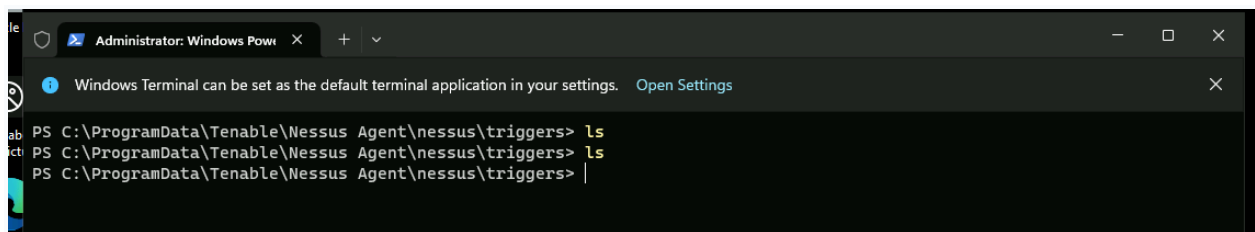


The Tenable Nessus Agent is confirmed in these screenshots as running within our Virtual Machine.

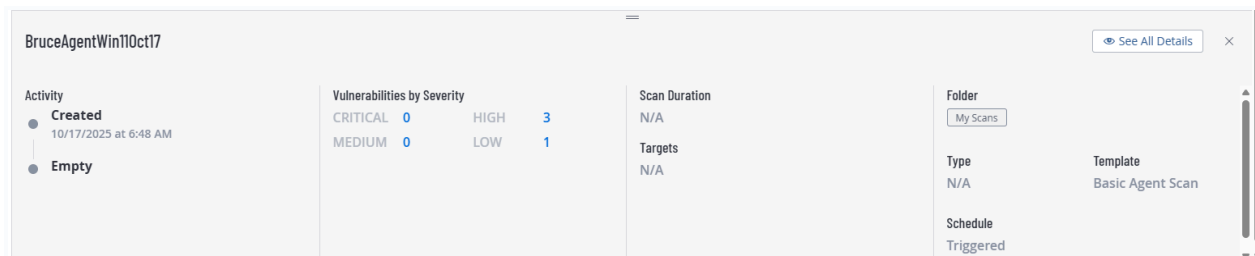
The Agent has been triggered, and the file has been removed:



Confirming this in the Command Line:



Confirming that Tenable has discovered the file “start.txt” and has performed the necessary actions and discovered “Vulnerabilities by Severity”:



In the following screenshots Tenable shows that the Asset has been discovered in the bottom right under Asset Details and also within the “Vulns by Asset” tab:

tenable

Vulnerability Management

Scans > Scan Details

Quick Actions

BR

BruceAgentWin11Oct17

VULNERABILITY MANAGEMENT SCANS

Edit

Trash

Summary

Vulns by Plugin

Vulns by Asset

History

This is a Rule-based Agent scan configuration, and is launched by the Agent based on a set of triggers. Rule-based scans do not have a scan time window, and Agents can upload results at any time. You can view an aggregate of all vulnerabilities found in 12 hour windows here; visit [Findings](#) to view and export all vulnerability and audit results.

Description

No description found

Triggers

FILE NAME

start.txt

0

CRITICAL VULNERABILITIES

3

HIGH VULNERABILITIES

0

MEDIUM VULNERABILITIES

1

LOW VULNERABILITIES

Scan Details

STATUS

Enabled

MODIFIED TIME

10/17/2025 at 6:48 AM

CREATED TIME

10/17/2025 at 6:48 AM

TEMPLATE

Basic Agent Scan

Agent Details

GROUPS

BruceAgentOct17

Asset Details

ASSETS SEEN

1

tenable

Vulnerability Management

Scans > Scan Details

Quick Actions

BR

BruceAgentWin11Oct17

VULNERABILITY MANAGEMENT SCANS

Edit

Trash

Summary

Vulns by Plugin

Vulns by Asset

History

Filters

Search

1 Asset

Saved Searches

1 Asset

1 to 1 of 1

Page 1 of 1

NAME	IPV4 ADDRESS	VULNERABILITIES	VULNERABILITIES	CRITICAL	HIGH
win11vmbruce	10.1.0.170	<div></div>	116	0	3

Scan Details

STATUS

Enabled

MODIFIED TIME

10/17/2025 at 6:48 AM

CREATED TIME

10/17/2025 at 6:48 AM

TEMPLATE

Basic Agent Scan

Agent Details

GROUPS

BruceAgentOct17

Asset Details

ASSETS SEEN

1

tenable

Vulnerability Management

Settings > Sensors > Details

Quick Actions

WinT1VMBruce

Edit SettingsExportAdd to GroupsUnlink

OverviewLogsAgent Health Events

Agent Detail

STATUS

Online

LINKED ON

Today at 07:49 AM

NETWORK

Default

AGENT UUID

dfff1303-5bf6-43a1-a12d-5306af19bed7

IP ADDRESS

10.1.0.170

VERSION

11.0.1

PLATFORM

Windows (win-x86-64)

LAST CONNECTION

Today at 08:30 AM

TYPE

Agent

PROFILE

Default

Groups

BruceAgentOct17

Plugins

LAST UPDATED

October 16, 2025

PLUGIN SET

202510162351

I have included this screenshot of the output for the Agent through Tenable as well.

I have also included this list of vulnerabilities that were found by this Agent:

tenable

Vulnerability Management

Scans > Scan Details

Quick Actions

BruceAgentWin11Oct17

EditTrash

SummaryVulns by PluginVulns by AssetHistory

FiltersSearch116 Results

116 items

1 to 50 of 116Page 1 of 3

SEVERITY	NAME	FAMILY	INSTANCES
High	WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPadding...	Windows : Microsoft Bulletins	1
High	Security Updates Outlook for Windows (April 2024)	Windows : Microsoft Bulletins	1
High	Microsoft Teams for Desktop < 25122.1415.3698.6812 Remote Code Execution (Au...	Windows	1
Low	Microsoft Teams for Desktop < 25163.3611.3774.6315 Elevation of Privilege (July 2...	Windows	1
Info	Microsoft Windows SMB Shares Enumeration	Windows	1
Info	Microsoft Windows SMB Shares Access	Windows	1
Info	Microsoft Windows SMB Registry Remotely Accessible	Windows	1
Info	Microsoft Windows SMB Service Enumeration	Windows	1
Info	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration	Windows	1
Info	SMB Use Host SID to Enumerate Local Users	Windows : User management	1
Info	Microsoft Windows 'Administrators' Group User List	Windows : User management	1
Info	Microsoft Windows - Local Users Information : Can't Change Password	Windows : User management	1
Info	Microsoft Windows - Local Users Information : Disabled Accounts	Windows : User manaeement	1

0 CRITICAL VULNERABILITIES

3 HIGH VULNERABILITIES

0 MEDIUM VULNERABILITIES

1 LOW VULNERABILITIES

Scan Details

STATUSEnabled

MODIFIED TIME10/17/2025 at 6:48 AM

CREATED TIME10/17/2025 at 6:48 AM

TEMPLATEBasic Agent Scan

Agent Details

GROUPSBruceAgentOct17

Asset Details

ASSETS SEEN1

Concluding this Lab and moving forward, the 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.