

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		Networking	
Computer name	BruceLinuxSept17	Public IP address ⓘ	128.24.18.168 (Network interface brucelinuxsept17799)
Operating system	Linux (ubuntu 24.04)		1 associated public IPs
VM generation	V2	Public IP address (IPv6)	-
VM architecture	x64	Private IP address	10.1.0.200
Agent status	Ready	Private IP address (IPv6)	-
Agent version	2.14.0.1	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-g
roup' | bash
```

Configured and Agent is running as shown in this screenshot:

```
Applying auto-configuration.
Starting Nessus Agent.
Waiting for Nessus Agent to start and link...
.....
Auto-configuration complete.
The Nessus Agent is now linked to sensor.cloud.tenable.com:443
root@BruceLinuxSept17:~#
```

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:

```
root@BruceLinuxSept17:/opt/nessus_agent/var/nessus/triggers# ls -lasht
total 8.0K
 0 -rw-r--r--  1 root root    0 Oct 17 23:14 start.txt
4.0K drwxr-xr-x 13 root root 4.0K Oct 17 23:13 ..
4.0K drwx-----  2 root root 4.0K Oct 17 23:13 .
root@BruceLinuxSept17:/opt/nessus_agent/var/nessus/triggers# ls -lasht
total 8.0K
4.0K drwxr-xr-x 13 root root 4.0K Oct 17 23:15 ..
 0 -rw-r--r--  1 root root    0 Oct 17 23:14 start.txt
4.0K drwx-----  2 root root 4.0K Oct 17 23:13 .
root@BruceLinuxSept17:/opt/nessus_agent/var/nessus/triggers# ls -lasht
total 8.0K
4.0K drwxr-xr-x 13 root root 4.0K Oct 17 23:54 ..
4.0K drwx-----  2 root root 4.0K Oct 17 23:37 .
root@BruceLinuxSept17:/opt/nessus_agent/var/nessus/triggers# |
```

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."

tenable Vulnerability Management | Scans > Scan Details

BruceLinuxAgentSept17
VULNERABILITY MANAGEMENT SCANS

Summary **Vulns by Plugin** Vulns by Asset History

Filters Search 41 Results Saved Searches

41 Items 1 to 41 of 41 Page 1 of 1

SEVERITY	NAME	FAMILY	INSTANCES
Info	OS Identification	General	1
Info	Netstat Portscanner (SSH)	Port scanners	1
Info	Nessus Scan Information	Settings	1
Info	Software Enumeration (SSH)	General	1
Info	Enumerate IPv6 Interfaces via SSH	General	1
Info	Enumerate IPv4 Interfaces via SSH	General	1
Info	Enumerate MAC Addresses via SSH	General	1
Info	BIOS Info (SSH)	General	1
Info	System Information Enumeration (via DMI)	General	1
Info	Ethernet Card Manufacturer Detection	Misc.	1
Info	Memory Information (via DMI)	General	1
Info	Common Platform Enumeration (CPE)	General	1

0 CRITICAL VULNERABILITIES
0 HIGH VULNERABILITIES
0 MEDIUM VULNERABILITIES
0 LOW VULNERABILITIES

Scan Details
STATUS Enabled
MODIFIED TIME 10/17/2025 at 6:01 PM
CREATED TIME 10/17/2025 at 6:01 PM
TEMPLATE Basic Agent Scan

Agent Details
GROUPS BruceLinuxSept17

Asset Details
ASSETS SEEN 1

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.