Discovery Scan: Entire Cyber Range Subnet

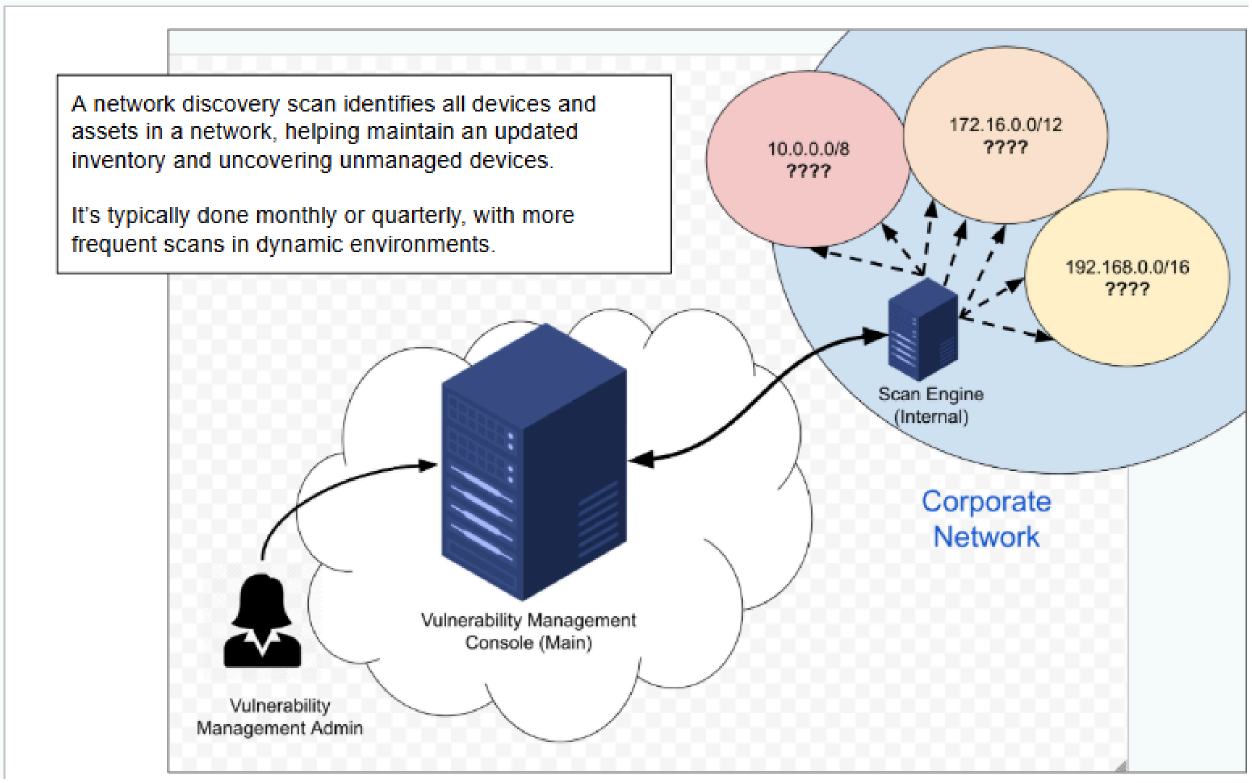
Lab created and performed by: Bruce Thornton

10/24/2025

Tools Used:

- Tenable.sc / Nessus
- Microsoft Azure https://portal.azure.com/

Introduction:



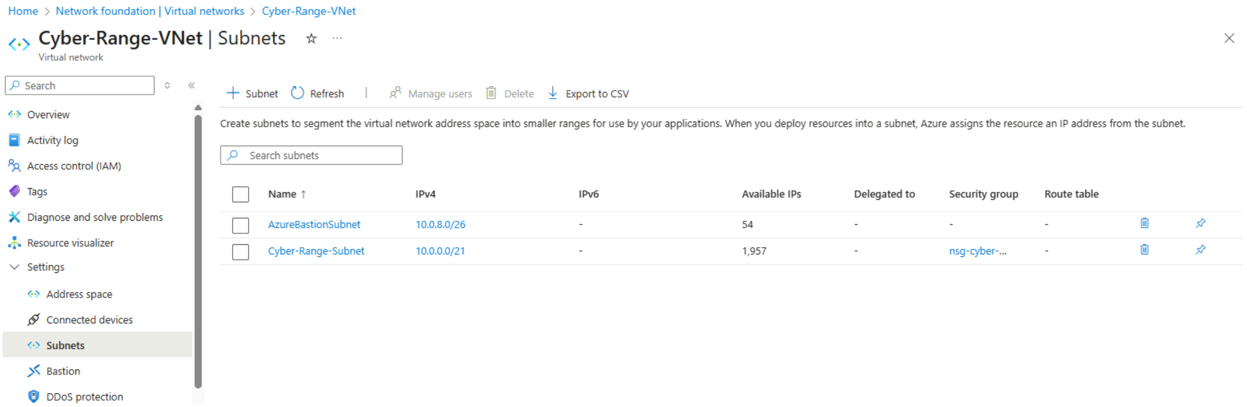
A network discovery scan identifies all devices and assets in a network, helping maintain an updated inventory and uncovering unmanaged devices.

It's typically done monthly or quarterly, with more frequent scans in dynamic environments.

Picture Courtesy of Josh Madakor and the Cyber Range

Logging into Microsoft Azure I have utilized the CIDR range for the entire subnet of the Cyber Range. I have plugged that into the Tenable Vulnerability Scanning tool, creating a Host/Network Discovery Scan.

Screenshots demonstrate this:

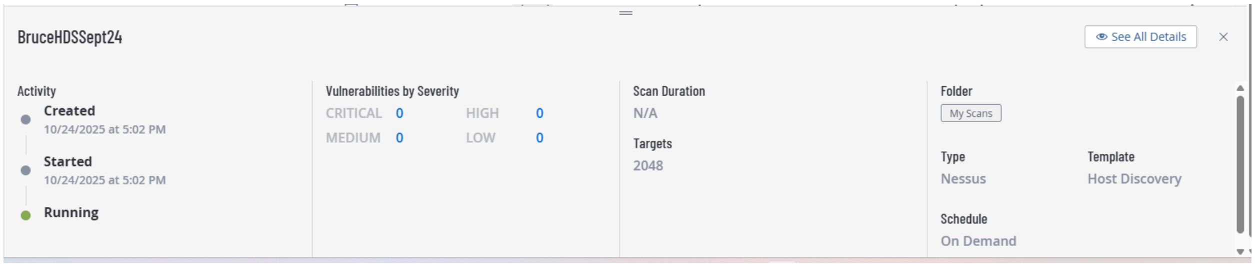


Cyber-Range-VNet | Subnets

Virtual network

Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet.

Name ↑	IPv4	IPv6	Available IPs	Delegated to	Security group	Route table
AzureBastionSubnet	10.0.8.0/26	-	54	-	-	-
Cyber-Range-Subnet	10.0.0.0/21	-	1,957	-	nsg-cyber-...	-



BruceHDSSept24

Activity
- Created 10/24/2025 at 5:02 PM
- Started 10/24/2025 at 5:02 PM
- Running

Vulnerabilities by Severity

CRITICAL 0 HIGH 0
MEDIUM 0 LOW 0

Scan Duration: N/A

Targets: 2048

Folder: My Scans

Type: Nessus

Template: Host Discovery

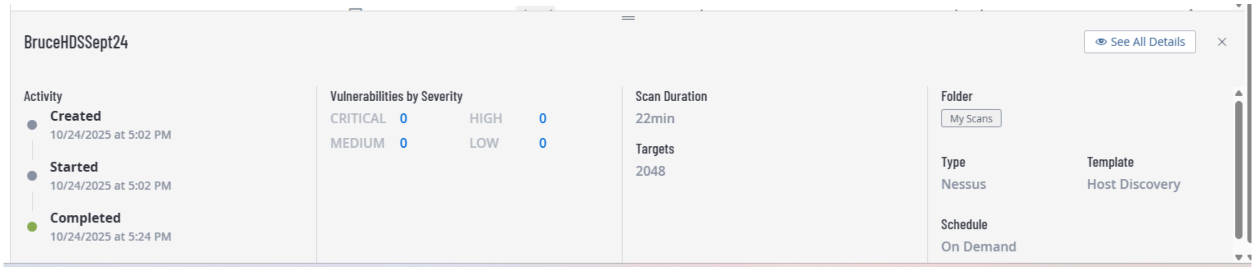
Schedule: On Demand

It should be noted that I have entered the subnet CIDR range into Tenable as:

<u>10.0.0.0/21</u>

This is needed during the creation of the scan.

The scan has completed.



BruceHDSSept24

Activity
- Created 10/24/2025 at 5:02 PM
- Started 10/24/2025 at 5:02 PM
- Completed 10/24/2025 at 5:24 PM

Vulnerabilities by Severity

CRITICAL 0 HIGH 0
MEDIUM 0 LOW 0

Scan Duration: 22min

Targets: 2048

Folder: My Scans

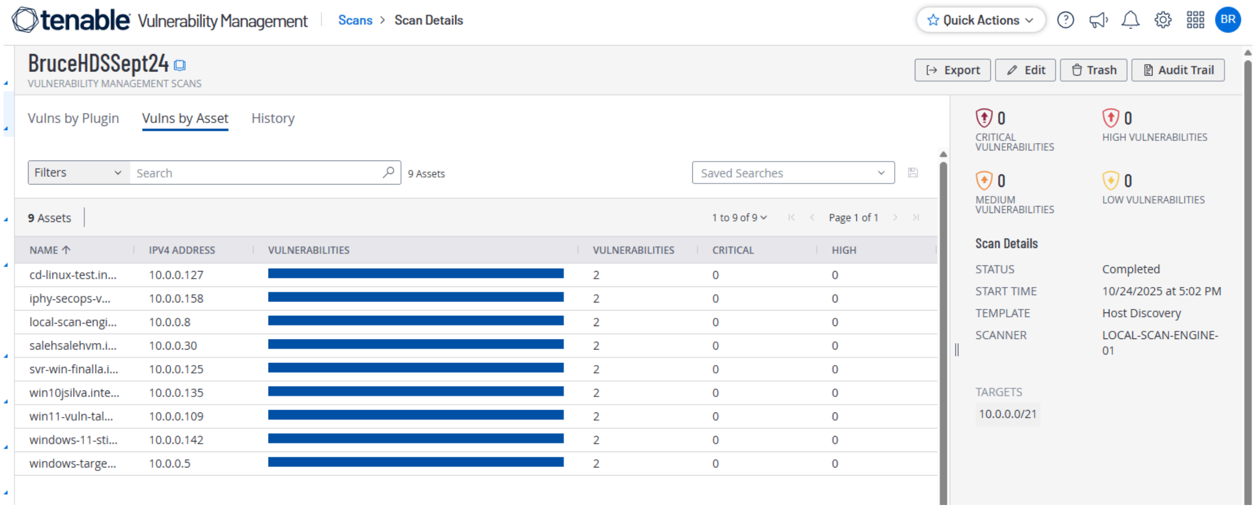
Type: Nessus

Template: Host Discovery

Schedule: On Demand

This screenshot is the information from the completed scan, I will now click on “See All Details”

Here I have located the Scan results under the “Vulns by Asset” tab:



BruceHDSSept24
VULNERABILITY MANAGEMENT SCANS

9 Assets

9 Assets — 1 to 9 of 9 — Page 1 of 1

NAME ↑	IPV4 ADDRESS	VULNERABILITIES	VULNERABILITIES	CRITICAL	HIGH
cd-linux-test.in...	10.0.0.127		2	0	0
iphy-secops-v...	10.0.0.158		2	0	0
local-scan-engi...	10.0.0.8		2	0	0
salehsalehvm.i...	10.0.0.30		2	0	0
svr-win-finalla.i...	10.0.0.125		2	0	0
win10jsilva.inte...	10.0.0.135		2	0	0
win11-vuln-tal...	10.0.0.109		2	0	0
windows-11-sti...	10.0.0.142		2	0	0
windows-targe...	10.0.0.5		2	0	0

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

Scan Details

STATUS	Completed
START TIME	10/24/2025 at 5:02 PM
TEMPLATE	Host Discovery
SCANNER	LOCAL-SCAN-ENGINE-01

TARGETS
10.0.0.0/21

The Scan results show that the Cyber Range at this specific time has: **9 total Assets**

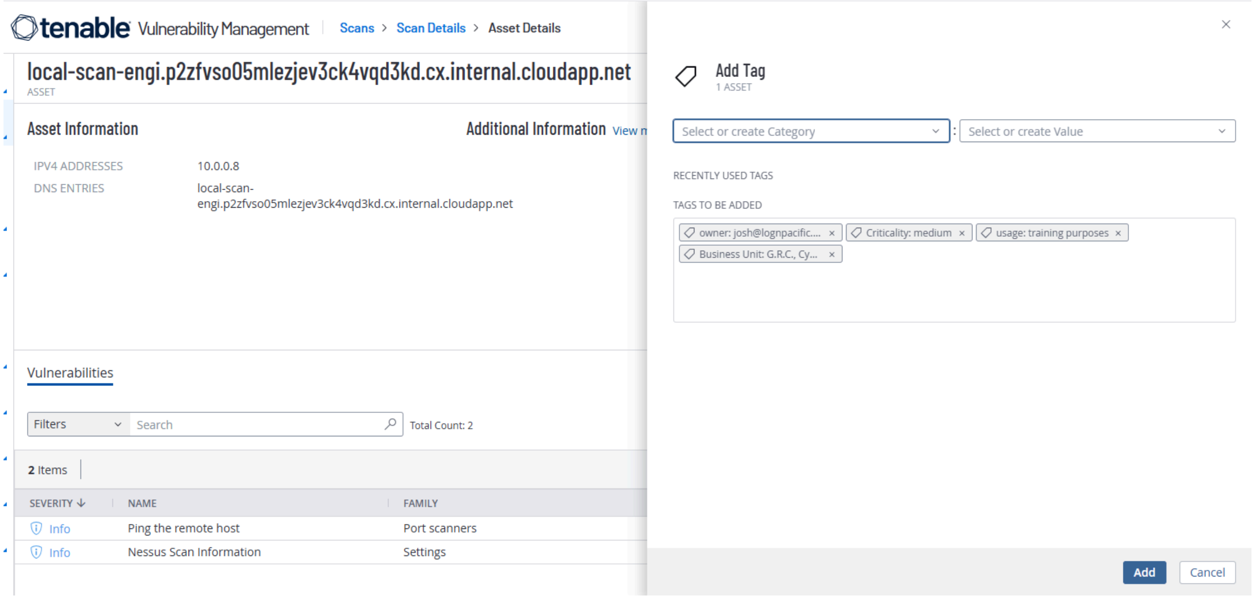
Two of these Assets are part of the structure of this Virtual Environment and can be seen in the screenshot as: Local-Scan-Engine which is internal, and windows-target-1 which is also internal.
The other Assets returned from this Discovery Scan are Cyber Range members Virtual Machines and Scans that are currently live at the time of this Scan.

Any of these listed Assets can be “Tagged” and identified using the Tenable “Add Tag” option. This is to assist in Asset Management, Classification, and Security.

For the purposes of this Lab we have chosen:

local-scan-engi.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net

Evidence:



tenable Vulnerability Management
Scans > Scan Details > Asset Details

local-scan-engi.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net
ASSET

Asset Information

IPV4 ADDRESSES	10.0.0.8
DNS ENTRIES	local-scan-engi.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net

Additional Information

View m
Vulnerabilities
Filters
Search

Total Count: 2

2 Items

SEVERITY	NAME	FAMILY
Info	Ping the remote host	Port scanners
Info	Nessus Scan Information	Settings

Add Tag
1 ASSET

TAGS TO BE ADDED

- owner: josh@lognpacific....
- Criticality: medium
- usage: training purposes
- Business Unit: G.R.C., Cy...

Now I can Identify and Classify the devices; determining the device type, owner (who is responsible for patching), and the device purpose.

This example Asset can not be removed, it is just an example, however…

These can also be grouped with similar assets and I can include an organization’s ongoing vulnerability scan schedule and remediation cycles. Utilizing the ability within Tenable to “Add Tag” all of this can be more organized, and it enables me to keep track of all Assets within the “Platform.”

Had any of the Assets that were found in the Scan been found as “Rogue Assets,” the following steps would have been taken:

Isolate: Disconnect the rogue device from your network to prevent any unauthorized access.

Investigate: Analyze the device to understand its purpose and security status using network scanning tools.

Decide: Follow your organization's security policies to either remove or secure and reintegrate the device.