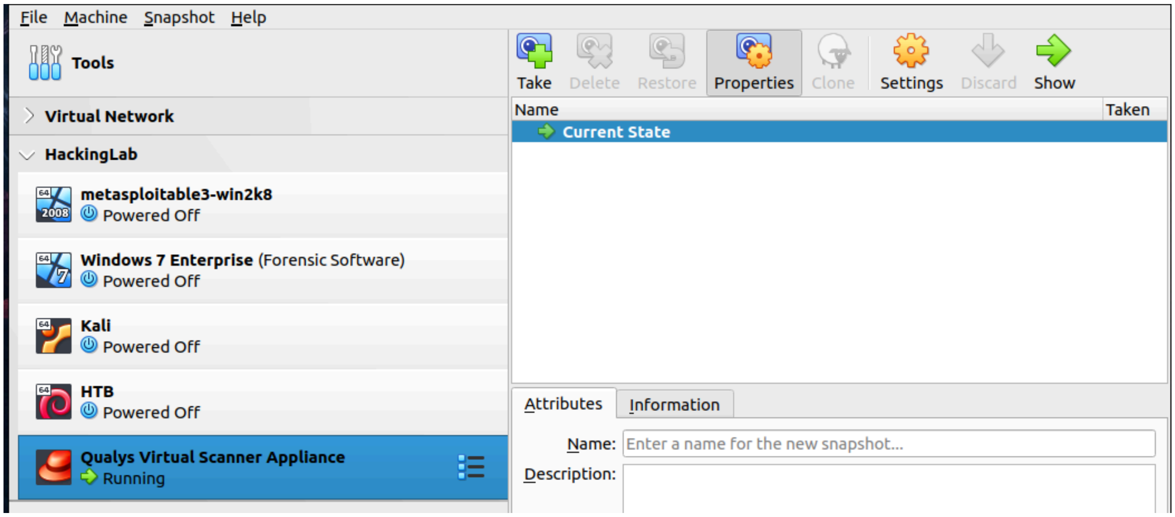
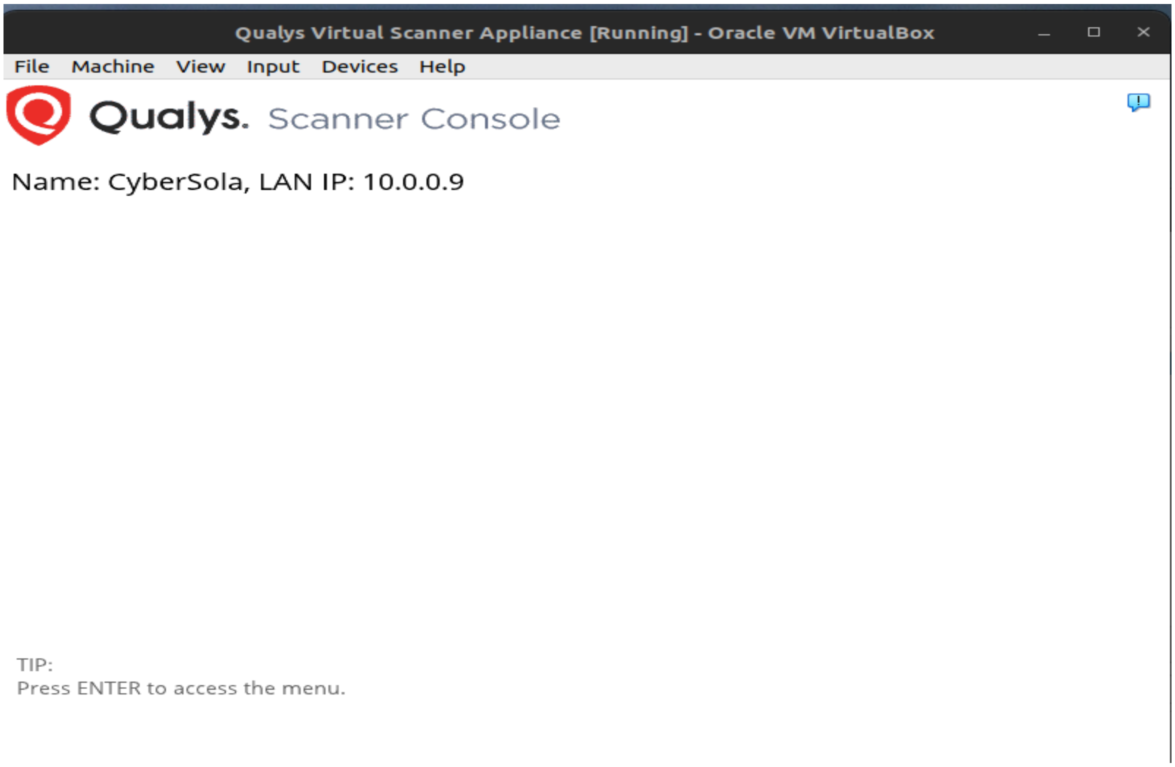
Vulnerability Management-Qualys

Project Description

Install and deploy Qualys Virtual scanner appliance, and execute vulnerability management lifecycle on target systems.

Qualys Virtual Scanner Appliance

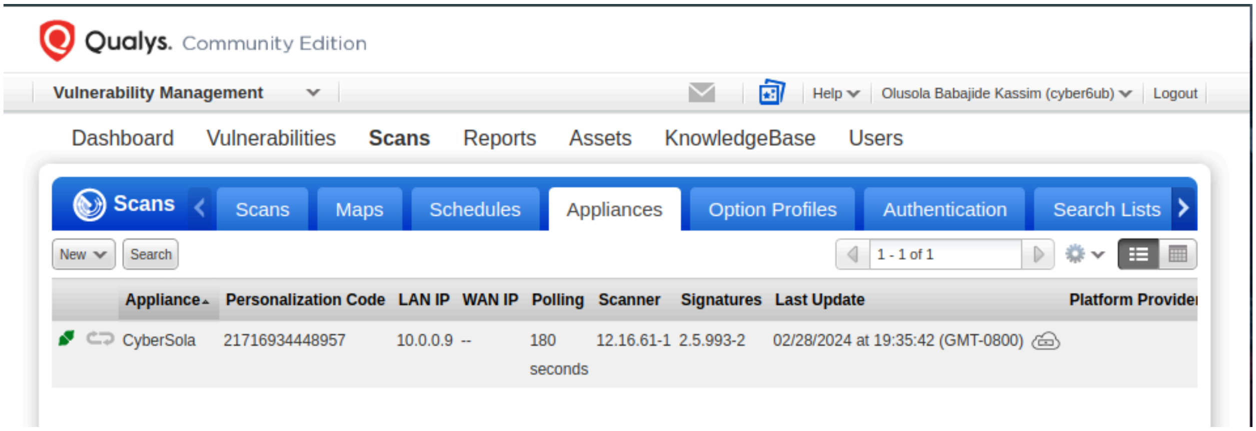



Qualys Virtual Scanner Appliance [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Qualys. Scanner Console

Name: CyberSola, LAN IP: 10.0.0.9

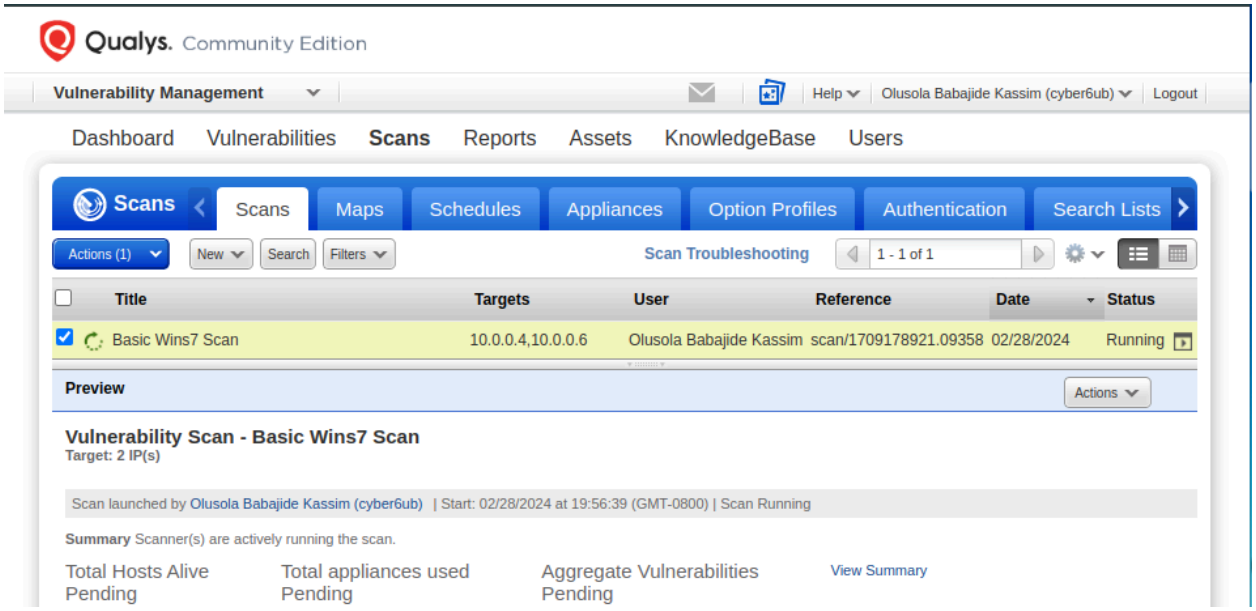
TIP:
Press ENTER to access the menu.

Virtual Scanner access on Qualys Cloud Platform



Appliance	Personalization Code	LAN IP	WAN IP	Polling	Scanner	Signatures	Last Update	Platform Provide
CyberSola	21716934448957	10.0.0.9	--	180 seconds	12.16.61-1	2.5.993-2	02/28/2024 at 19:35:42 (GMT-0800)	

Scan in progress



☐	Title	Targets	User	Reference	Date	Status
☑	Basic Wins7 Scan	10.0.0.4,10.0.0.6	Olusola Babajide Kassim	scan/1709178921.09358	02/28/2024	Running

Preview

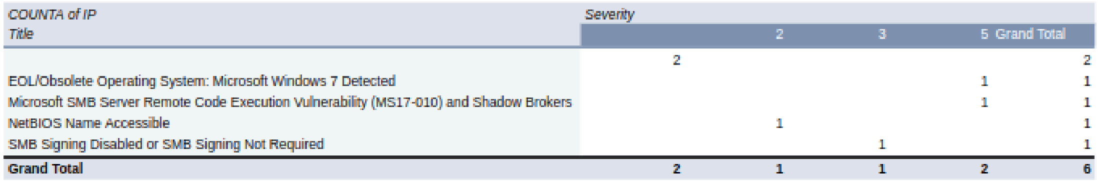
Vulnerability Scan - Basic Wins7 Scan
Target: 2 IP(s)

Scan launched by Olusola Babajide Kassim (cyber6ub) | Start: 02/28/2024 at 19:56:39 (GMT-0800) | Scan Running

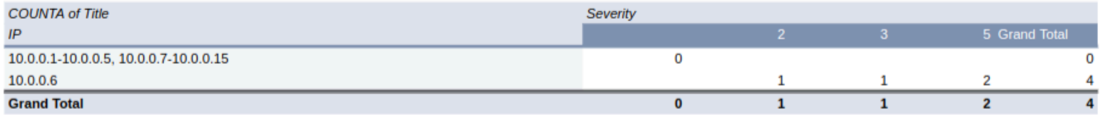
Summary Scanner(s) are actively running the scan.

Total Hosts Alive: Pending
Total appliances used: Pending
Aggregate Vulnerabilities: Pending

Quick view of scan result



COUNTA of IP	*Severity*				
Title		2	3	5	Grand Total
	2				2
EOL/Obsolete Operating System: Microsoft Windows 7 Detected				1	1
Microsoft SMB Server Remote Code Execution Vulnerability (MS17-010) and Shadow Brokers				1	1
NetBIOS Name Accessible		1			1
SMB Signing Disabled or SMB Signing Not Required			1		1
Grand Total	**2**	**1**	**1**	**2**	**6**



COUNTA of Title	*Severity*				
IP		2	3	5	Grand Total
10.0.0.1-10.0.0.5, 10.0.0.7-10.0.0.15	0				0
10.0.0.6		1	1	2	4
Grand Total	**0**	**1**	**1**	**2**	**4**

Summary

Qualys has identified the device “Window-7” is affected by the vulnerability - Microsoft SMB Server Remote Code Execution Vulnerability (MS17-010) and Shadow Brokers; providing information on impact and solution.

- Impact: A remote attacker could gain the ability to execute code by sending crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server. The latest version of the Petya ransomware is spreading over Windows SMB and is reportedly using the ETERNALBLUE exploit.
- Solution: Customers are advised to refer to Microsoft Advisory MS17-010 (https://technet.microsoft.com/en-us/security/bulletin/MS17-010) or How to verify that MS17-010 is installed (https://support.microsoft.com/eu-es/help/4023262/how-to-verify-that-ms17-010-is-installed) for more details. Workaround:Disable SMBv1

A detailed version of the report is attached.