Vulnerability Scanner Deployment Project

Introduction

Here is a comprehensive tutorial on how to install and run Nessus, a program that the cybersecurity industry highly values. This lesson covers the procedures for installing Nessus in the environment, setting it up to search for vulnerabilities, and effectively interpreting the scan findings.

Nessus is an acronym for an attack point designed to identify weak points and possible threats in your system, applications, and network architecture. You may strengthen your cybersecurity posture by proactively identifying and fixing vulnerabilities through the regular use of individual vulnerability scanning and the staffed deployment of Nessus.

I will walk through each stage of the configuration procedure for Nessus and explain how this scanner works during my presentation. Nessus is an indispensable resource for individuals seeking to enhance their understanding of cybersecurity, as well as for IT administrators tasked with fortifying their organisation's network security. You will acquire the skills and information needed to utilise this potent instrument efficiently after completing our training.

Let's examine the tutorial's structure and the topics that will be addressed at each stage.

Preparing for Deployment

Understanding Nessus

Before deploying Nessus, ensure that you understand everything you need to know about it, including how it works with vulnerability management. Info security teams may identify and categorise security flaws in the network infrastructure, apps, and systems of the entire company by using Tenable's highly effective vulnerability scanner, Nessus. By using Nessus to scan for known vulnerabilities, misconfigurations, and potential security threats, companies can identify and close gaps in their systems before attackers can exploit any security signals or weak points. Additionally, Nessus produces thorough reports and recommendations to support the security team in taking prompt, effective commercial action to eradicate the danger and strengthen the security industry position.

Assessing System Requirements

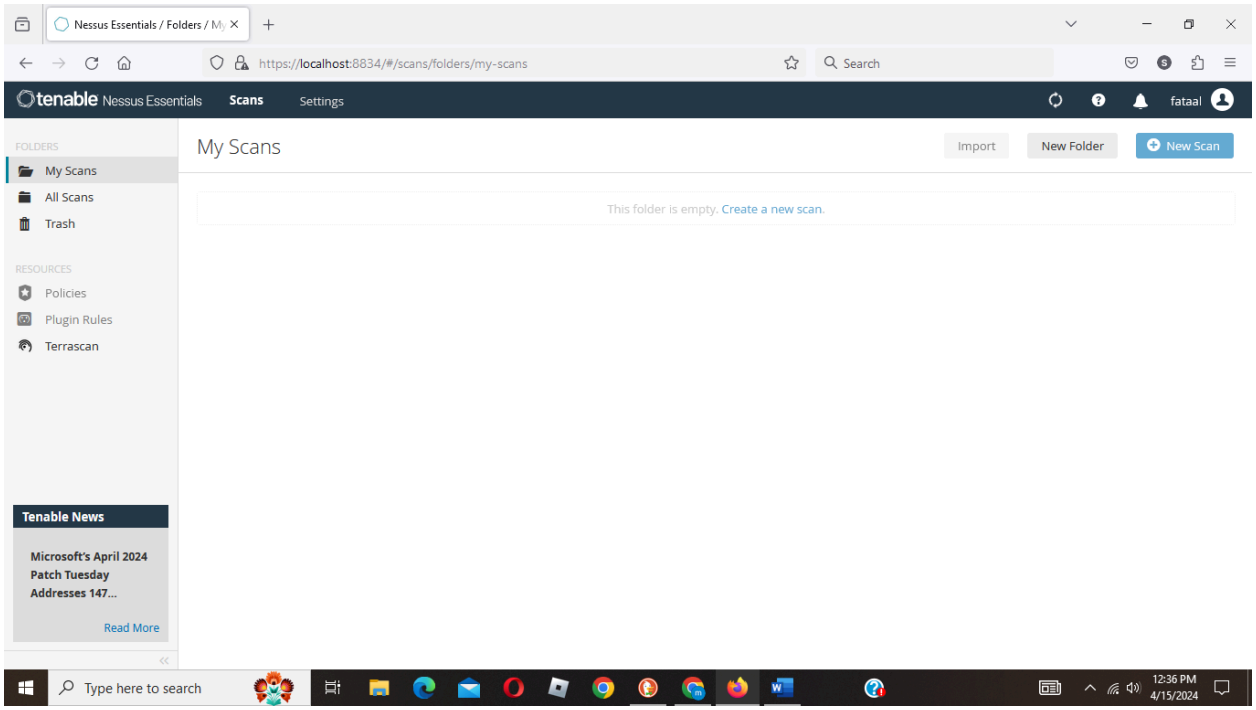
System requirements are evaluated prior to Nessus's final deployment, allowing you to quickly determine whether your infrastructure is capable of supporting this service. The size of your network, the number of assets to be examined at once, and the frequency of the scans are only a few of the numerous variables that might affect the minimal requirements for the Nessus program. Hard memory tracker Nessus, by default, needs a server or virtual machine (VM) with a specific amount of RAM, CPU, and storage space. Nessus implementation may also require initial software dependencies or other compatibility requirements to be met. By assessing the system needs in advance, you can ensure that Nessus will operate constantly at peak efficiency and identify any potential issues during deployment.

Nessus Installation

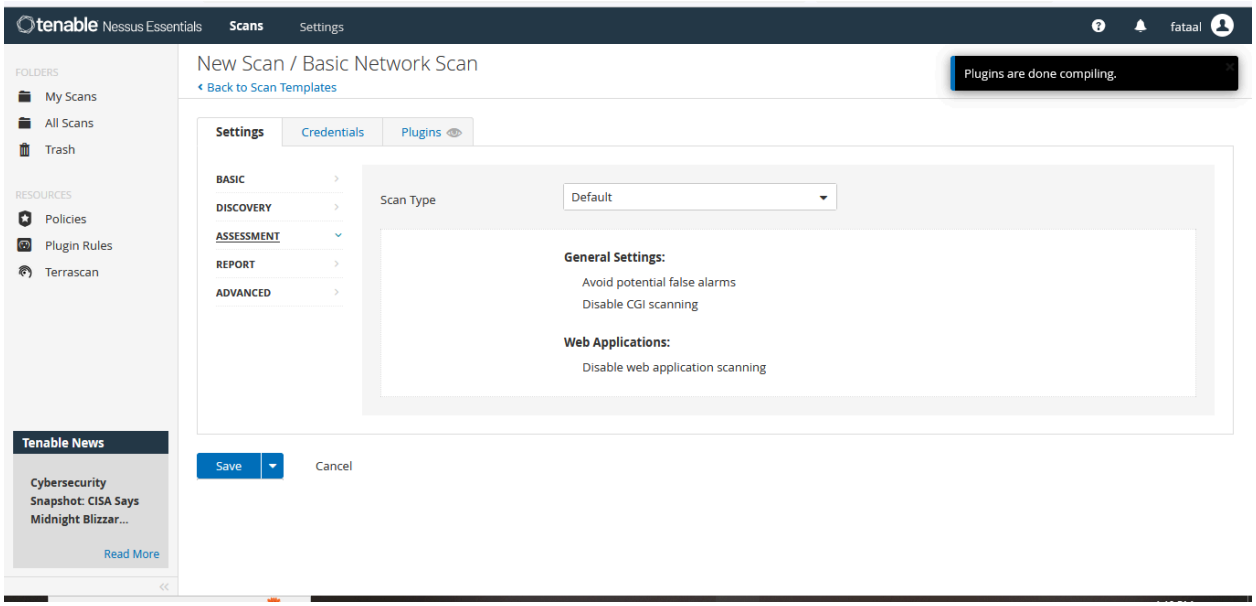
You can then obtain the Nessus software and install it on the target platform to see if it is operating efficiently after you have completed that and verified that the system satisfies the system requirements. The Tenable website offers a download for Execution Nessus. If your company is tiny, you can choose Nessus Essentials, which is free, or Nessus Professional, which is chargeable, if it is huge. The Tenable software's installation instructions will walk you through installing Nessus on a server or virtual machine, if necessary after you've downloaded it. I got the software from their official website, which is accessible from this link: Nessus.

Configuration Phase

After installing Nessus, I accessed the web interface to configure it. It had a nice appearance, and I had no trouble using the features and functions. My next assignment, among many other things, involved creating new scanning policies that would satisfy our organisational requirements and unquestionably increase the effectiveness of vulnerability scanning by guaranteeing in-depth investigations and concurrently reducing false positives. After the previous phase, which preceded the identification of the target asset, I was eager to fine-tune the IP addresses and domain names in order to serve as the ransomware scan for Nessus and produce a targeted exposure to vulnerability assessment. In order to streamline the scanning process, I ultimately introduced sets for scans as recurring jobs and schedules that can significantly increase vulnerability assessment accuracy in order to guarantee regular assessments and be ahead of new hazards.



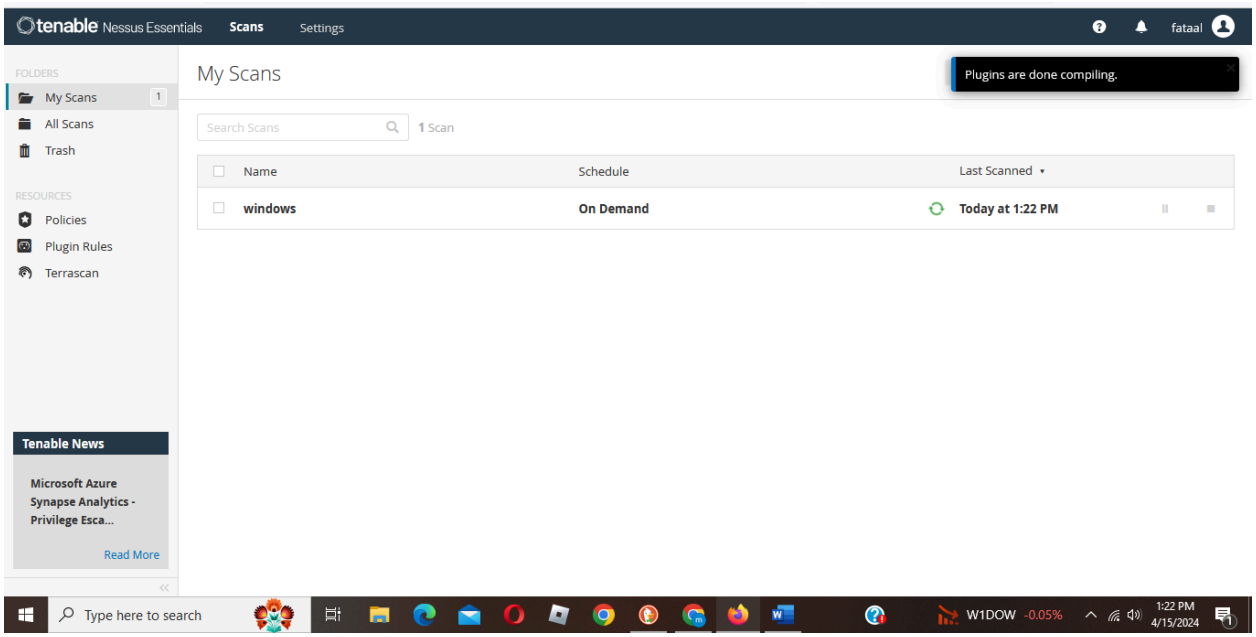
Configure Nessus for Scanning

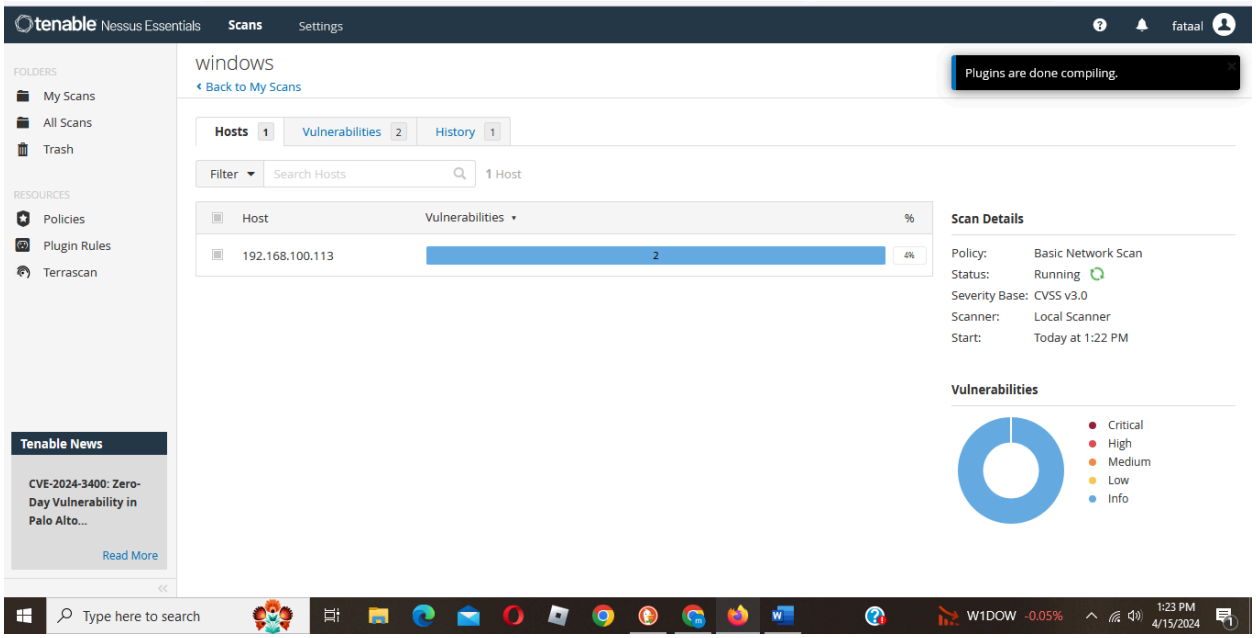


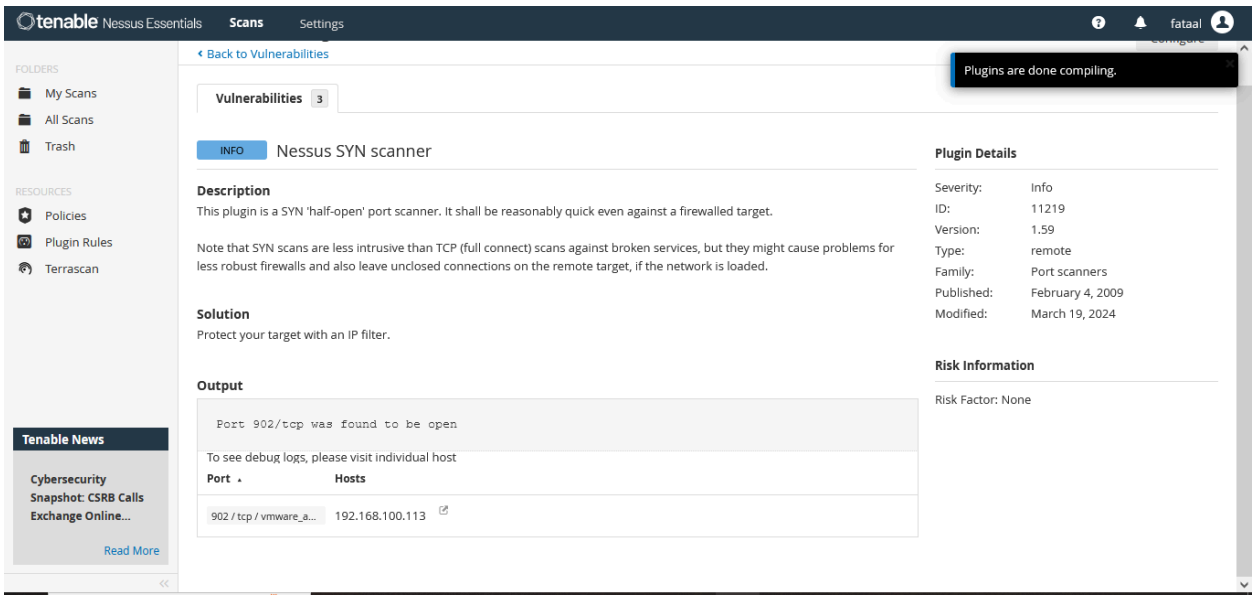
Conducting Scans and analysing results

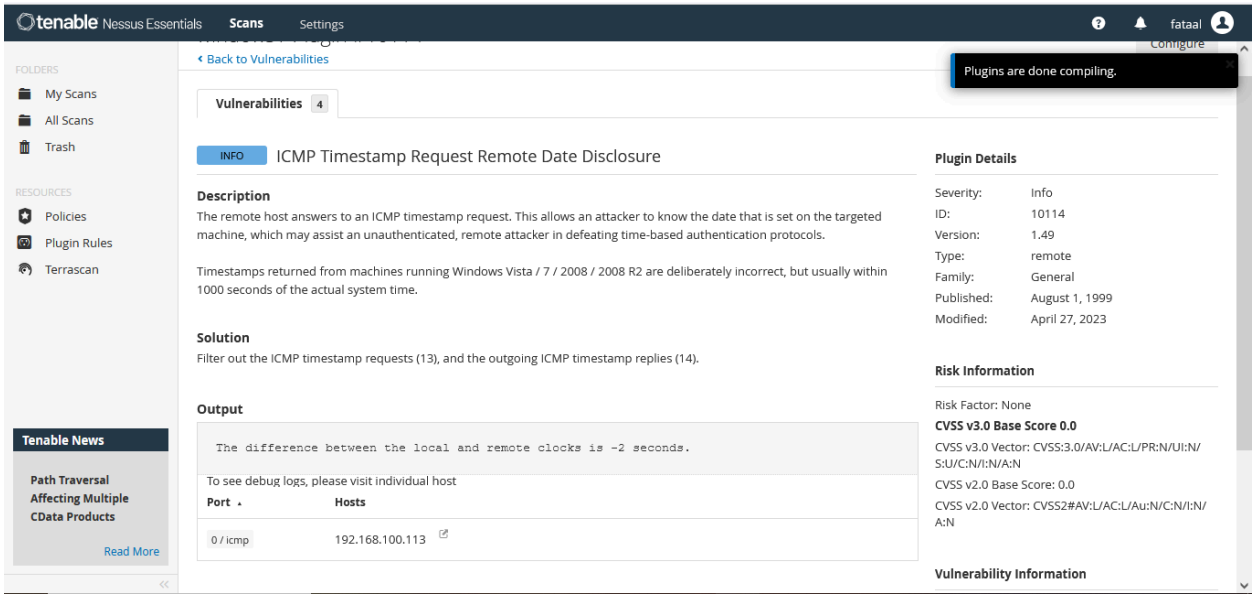
The scanning and analysis process constitutes the second part of the transition; I examined events in real time while doing task vulnerability scans using the default parameters and designated targets. The scan findings evaluation was my favourite task since it allowed me to carefully identify the vulnerabilities and prioritise them based on secession and priority. We were able to prioritise the remediation efforts and communicate with stakeholders more effectively because of the comprehensive reports, cybersecurity scan results, and security recommendations that helped us better understand the security posture of our network.

Nessus initial scan

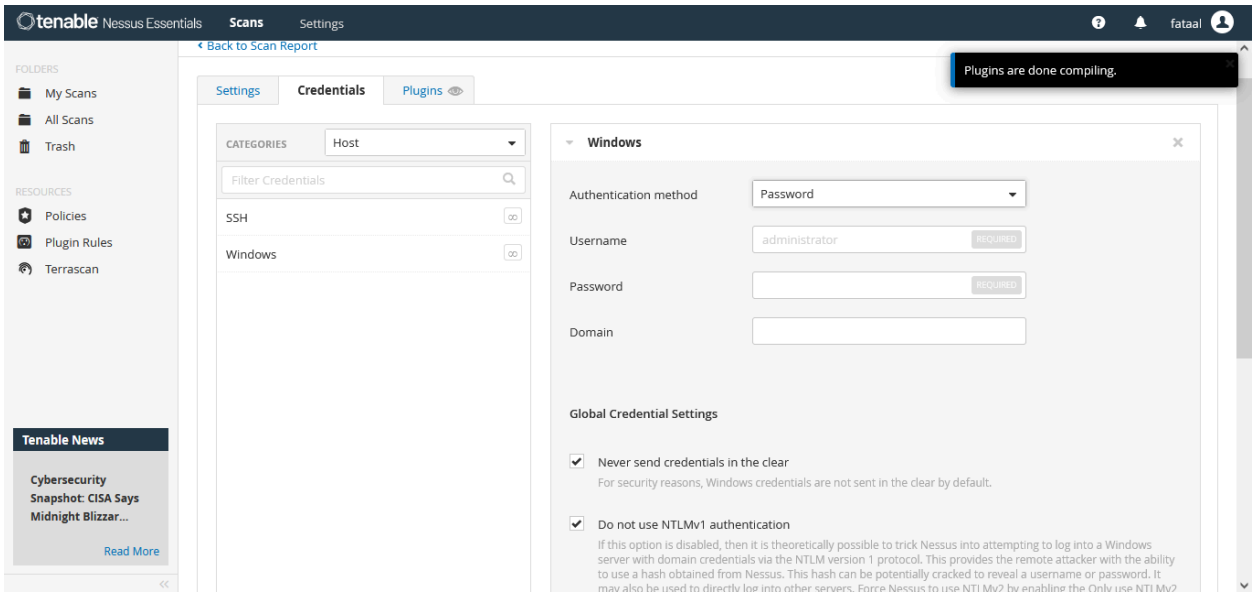



tenable Nessus Essentials
Scans
Settings
fataal
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
CVE-2024-3400: Zero-Day Vulnerability in Palo Alto...
Read More
windows
Back to My Scans
Plugins are done compiling.
Hosts 1
Vulnerabilities 2
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
%
192.168.100.113
2
4%
Scan Details
Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 1:22 PM
Vulnerabilities
Critical
High
Medium
Low
Info
Type here to search
W1DOW -0.05%
1:23 PM
4/15/2024

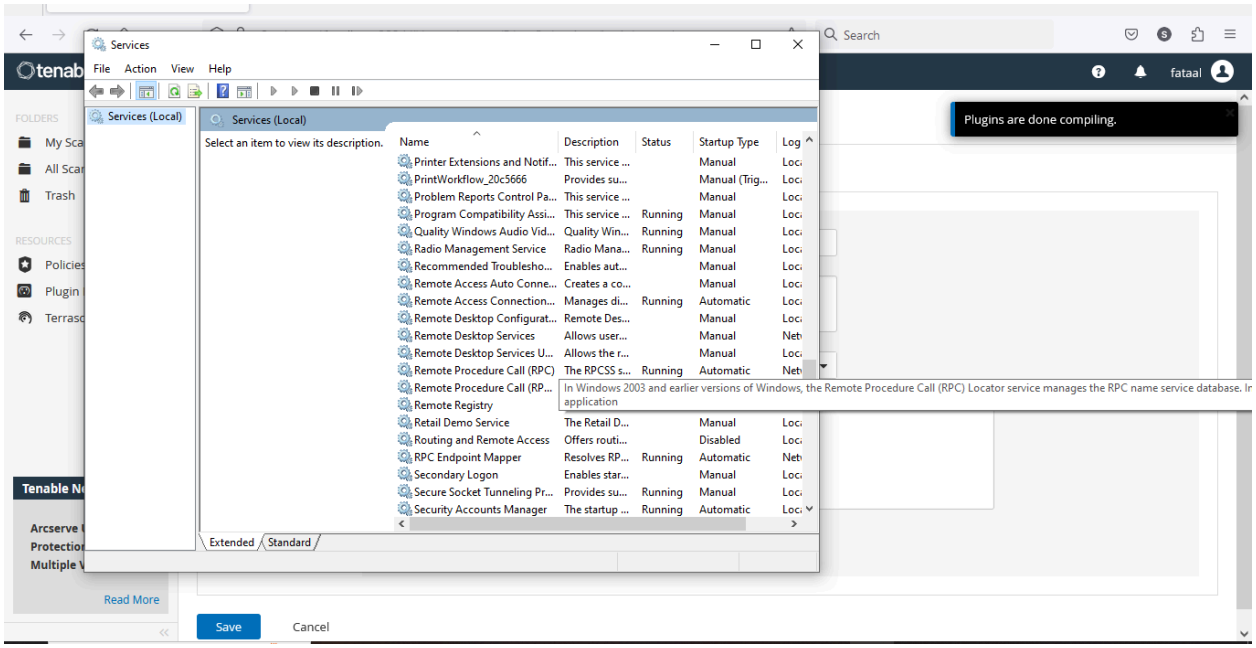

tenable Nessus Essentials
Scans
Settings
fataal
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Cybersecurity Snapshot: CSRB Calls Exchange Online...
Read More
Back to Vulnerabilities
Plugins are done compiling.
Vulnerabilities 3
INFO
Nessus SYN scanner
Description
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.
Solution
Protect your target with an IP filter.
Output
Port 902/tcp was found to be open
To see debug logs, please visit individual host
Port
Hosts
902 / tcp / vmware_a...
192.168.100.113
Plugin Details
Severity: Info
ID: 11219
Version: 1.59
Type: remote
Family: Port scanners
Published: February 4, 2009
Modified: March 19, 2024
Risk Information
Risk Factor: None



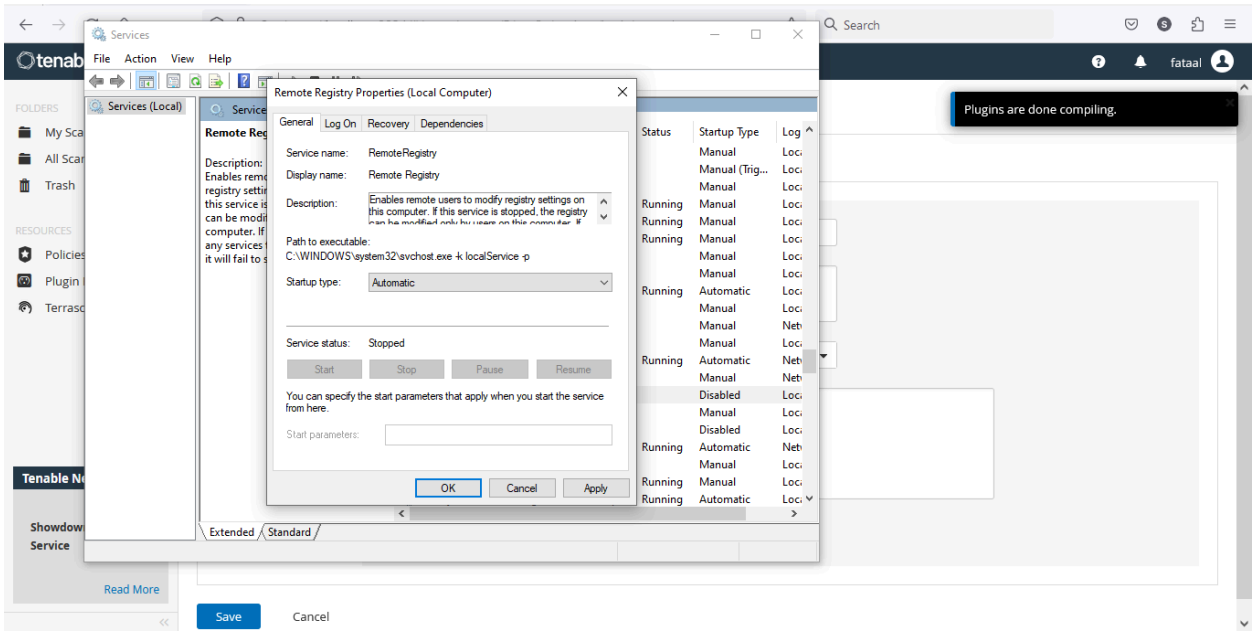
Configuration of Credentials for Credential scan



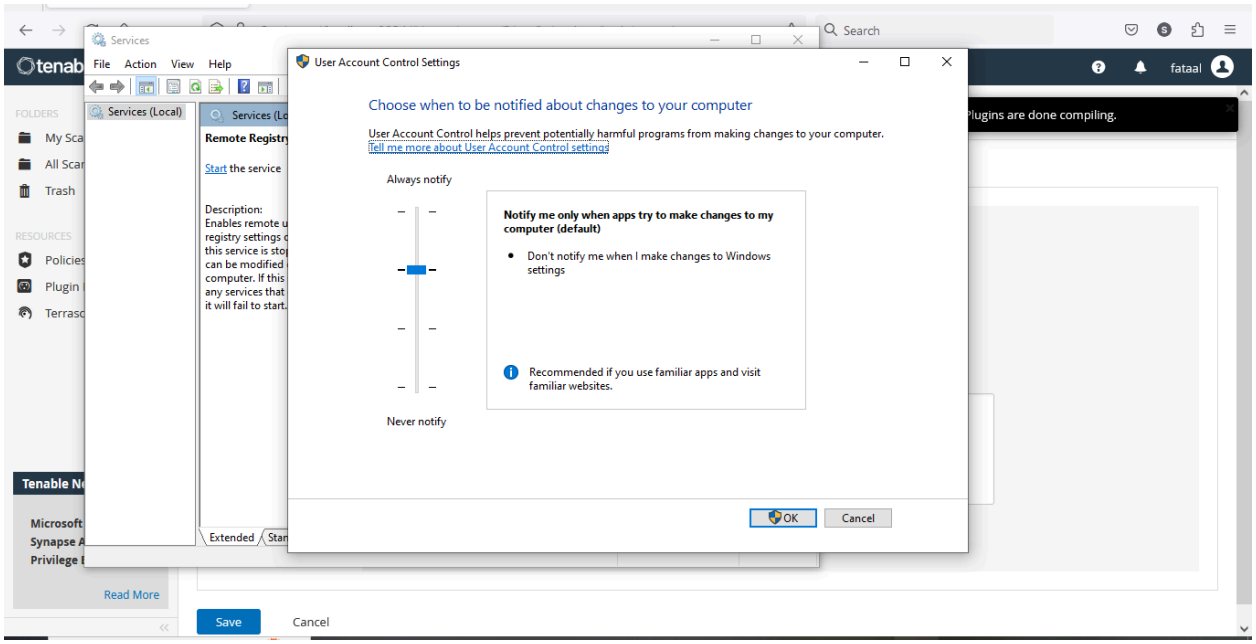
Remote registry

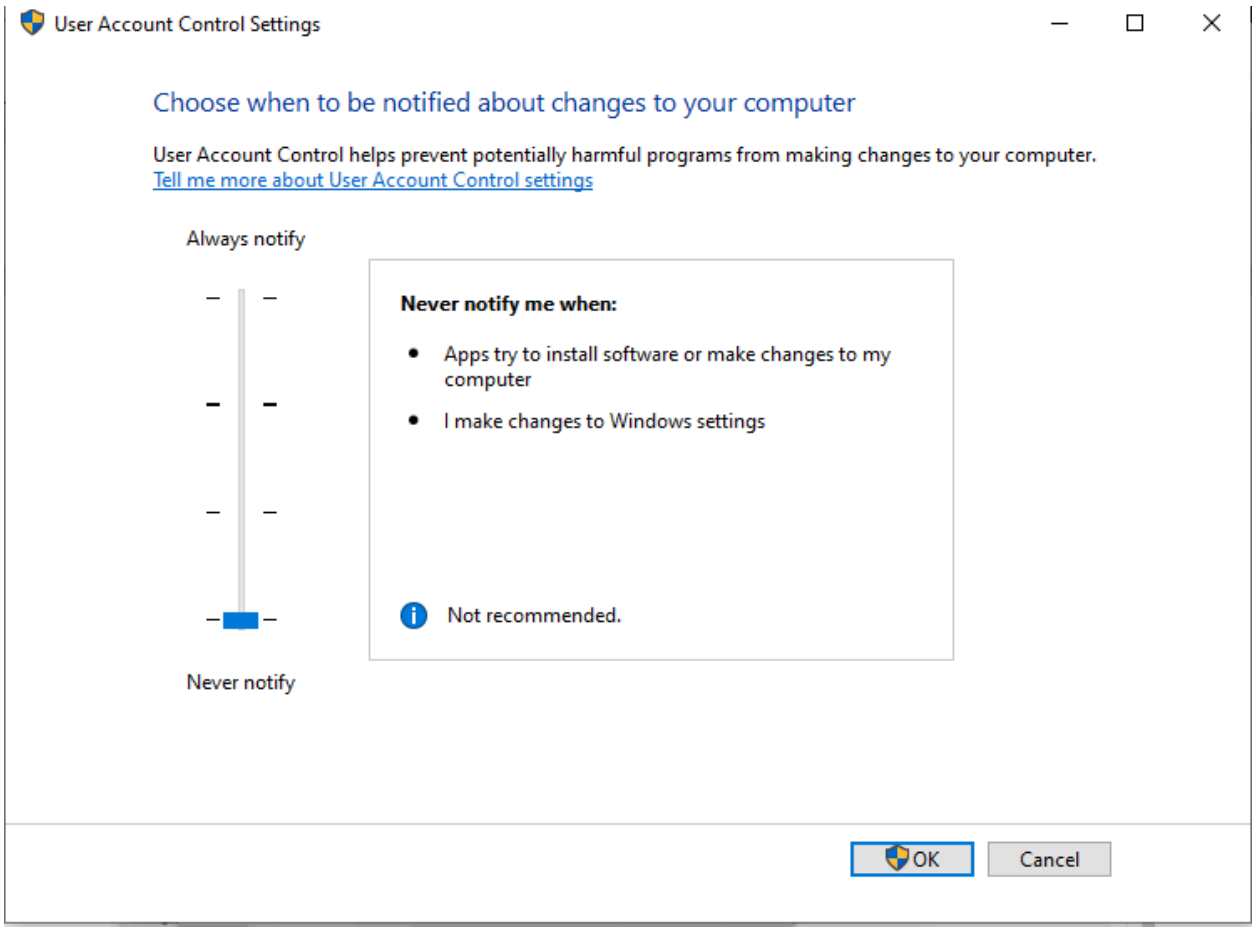


I changed the status type to automatic, which allows you to connect remotely to the system registry database to perform different operations.



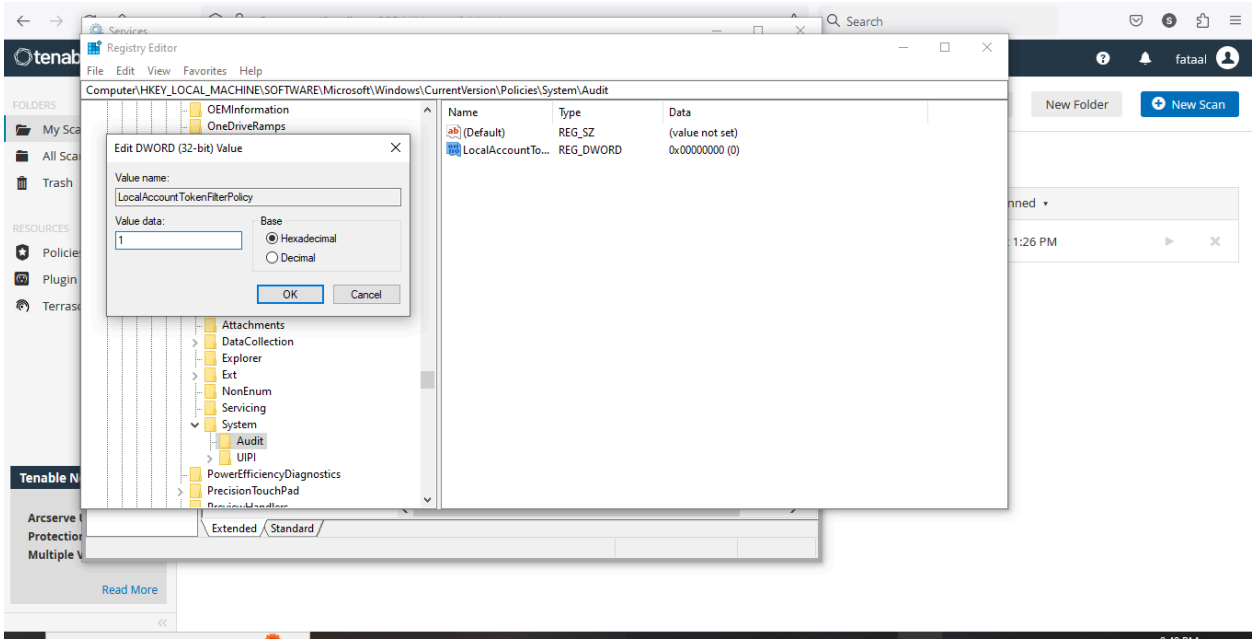
User account control settings is dragged to the bottom to disable notifications from disrupting the scans being conducted.



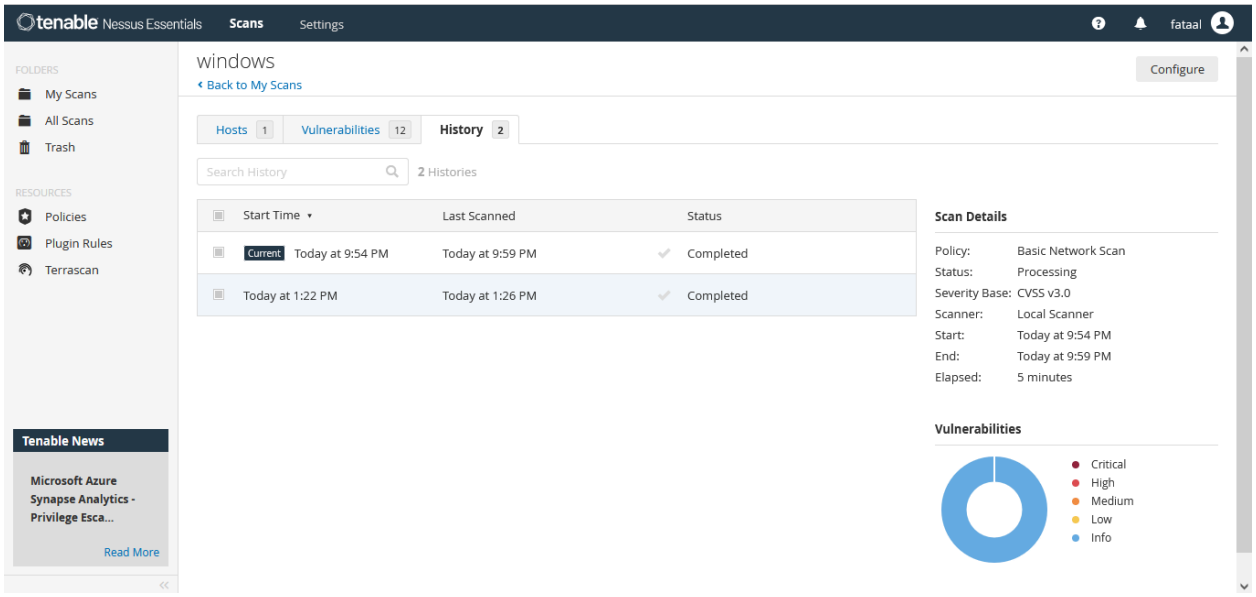


For the next exercise, I open the registry editor by clicking on the "HKEY_LOCAL_MACCHINE" key, then I go to "SOFTWARE," then "Microsoft," and lastly, I

get to the "Windows" directory. The Local Account Token Filter Policy is reviewed and modified here, and exceptions are made for free administrator accounts that are not subject to the restrictions on distant procedure core cognitive access. As a result, the improvements enable Nessus to perform more complex system scans, increasing its capacity to find an excessive number of vulnerabilities.



Nessus Credential and Advanced Nessus Scan



Remediation

In the course of the repair and follow-up service, I updated software patches, reset network settings, and performed any other necessary modifications right away to make sure that all of the system vulnerabilities were closed. Following our implementation, these issues were fixed, and additional research helped us determine which ones still required attention. Continuous monitoring and maintenance solutions became our ultimate goal as we strived to preserve a healthy state of cyber health. They assisted us in early threat detection and maintained a high degree of cybersecurity vigilance over the monitoring period.

Conclusion

In conclusion, Nessus has given us a possible way to fortify our system and is now an essential part of our cybersecurity. We have obtained the appropriate cues and inputs that enable us to identify network vulnerabilities and insecurities through meticulous coordination, astute design, and thorough inspection. Custom scanning policies, asset personalisation, and automated scanning schedules have all greatly aided in our ability to identify, rank, and promptly address any security threats that may be lurking around the corner. I managed to clearly convey results and prioritise remediation based on the severity of the security incident by using Nessus's report creation feature. From now on, we will establish our routine maintenance and monitoring to keep our ever-expanding cyberthreats from ever making us too susceptible. In general, we have strengthened our defence, improved the security of our communications, and shielded our company data systems from online attacks.