Nessus Vulnerability Lab
By Pranav Rao

Overview

This project focuses on the pivotal steps of vulnerability scanning and verification within the Vulnerability Management Lifecycle. With a keen eye on efficiency and accuracy, utilizing Nessus Essentials as the primary tool for vulnerability scanning. Operating within a dynamic environment, local VMs hosted on Digital Ocean's Ubuntu Server are employed as the testing ground for the scanning process.

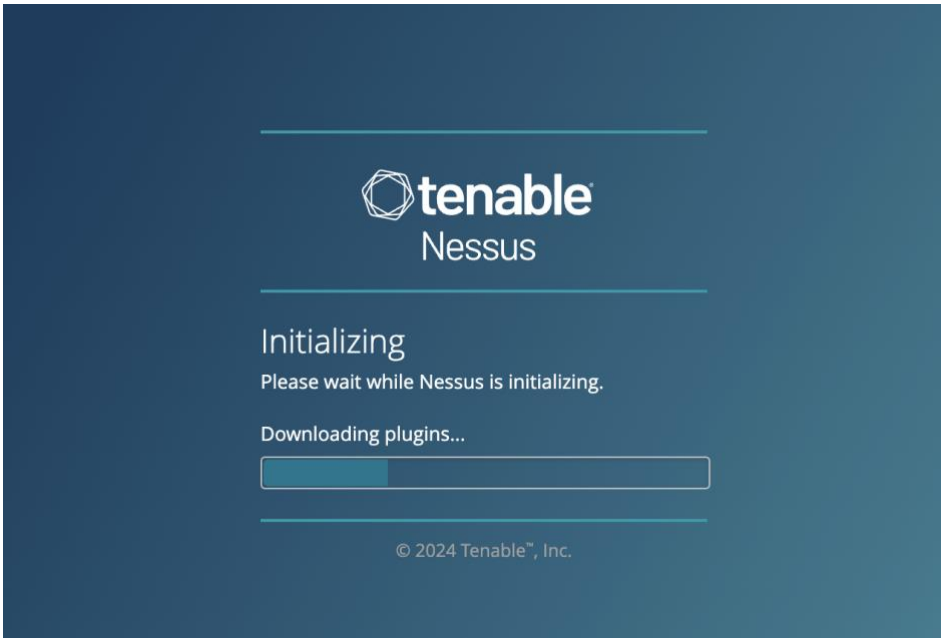
Nessus Essentials in uncovering vulnerabilities within the system's architecture. The scanning process is conducted with precision, providing comprehensive insights into potential areas of weakness and exposure. Following the scanning phase, emphasis is placed on the verification of vulnerabilities. A thorough rescan is performed to validate the accuracy of the initial scan results and ensure the reliability of the identified vulnerabilities. This verification step serves as a crucial checkpoint, affirming the integrity of the scanning process and the efficacy of the vulnerability assessment.

By focusing on vulnerability scanning and verification, this project offered me practical insights into bolstering an organization's cybersecurity defenses. Through a step-by-step approach, I have listed the process for the proactive vulnerability management and scans using Nessus essential

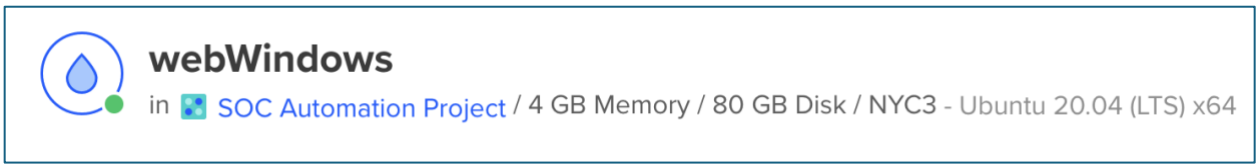
Tools

- **Windows ISO 2019 Server:** Utilized as the operating system for the virtual machines hosting the vulnerable systems.
- **Digital Ocean:** Cloud hosting provider used for hosting the virtual machines to simulate real-world environments.
- **Nessus Essentials:** Employed for conducting vulnerability scanning of the systems to identify potential security weaknesses.
- **Firefox 3.6.12:** Used as an example application to demonstrate vulnerabilities and the effectiveness of the scanning process.
- **Termius**: Used as a remote SSH client for accessing and managing the virtual machines.
- **VNC Viewer:** Utilized for remote desktop access to the virtual machines, enabling graphical user interface (GUI).

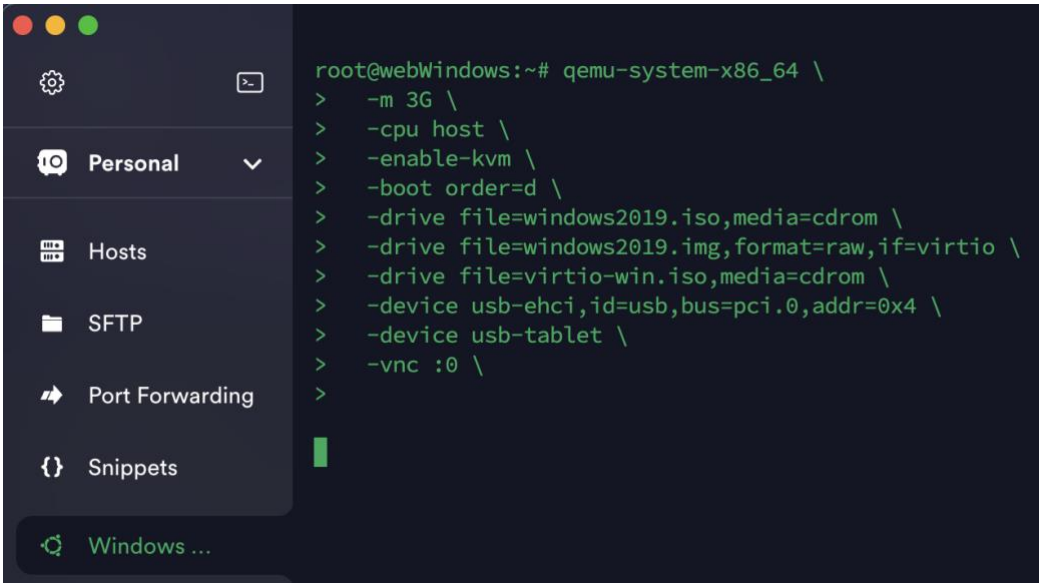
Installing Nessus



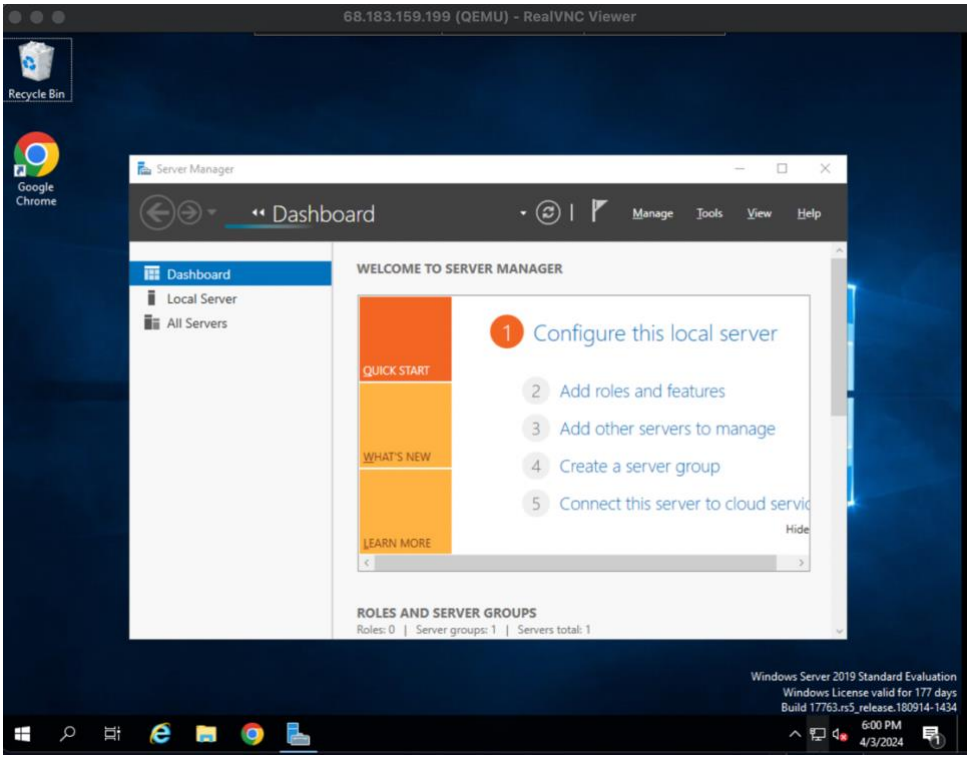
Creating a Droplet/Instance in Digital Ocean to hosting the Windows VM



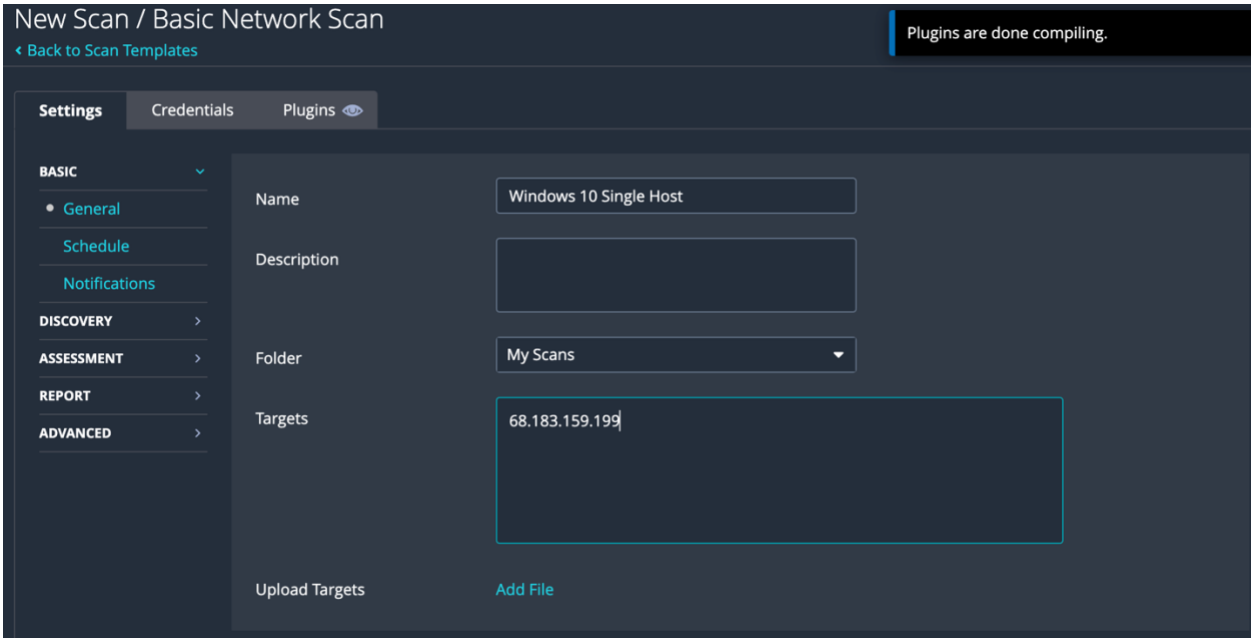
Using SSH Termius to access and manage the Virtual Machines



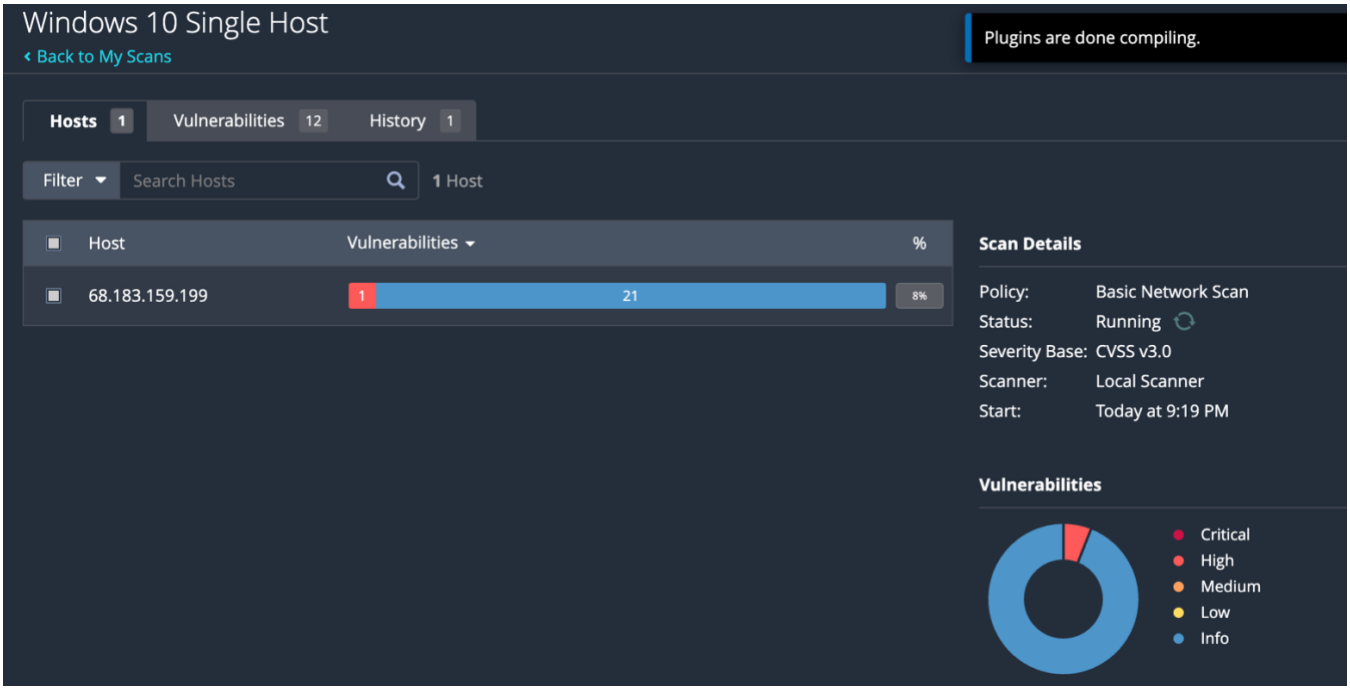
Using the VNC Viewer to graphically display the VM



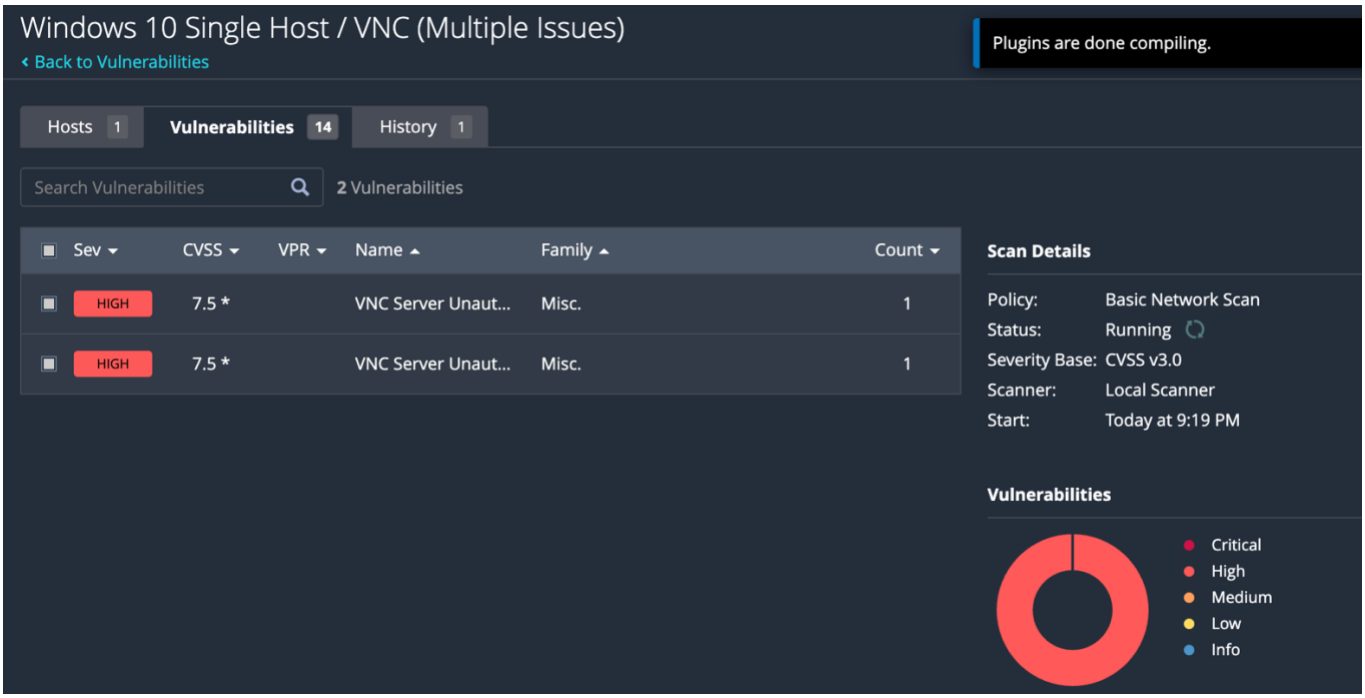
Conducting a Basic Network Scan



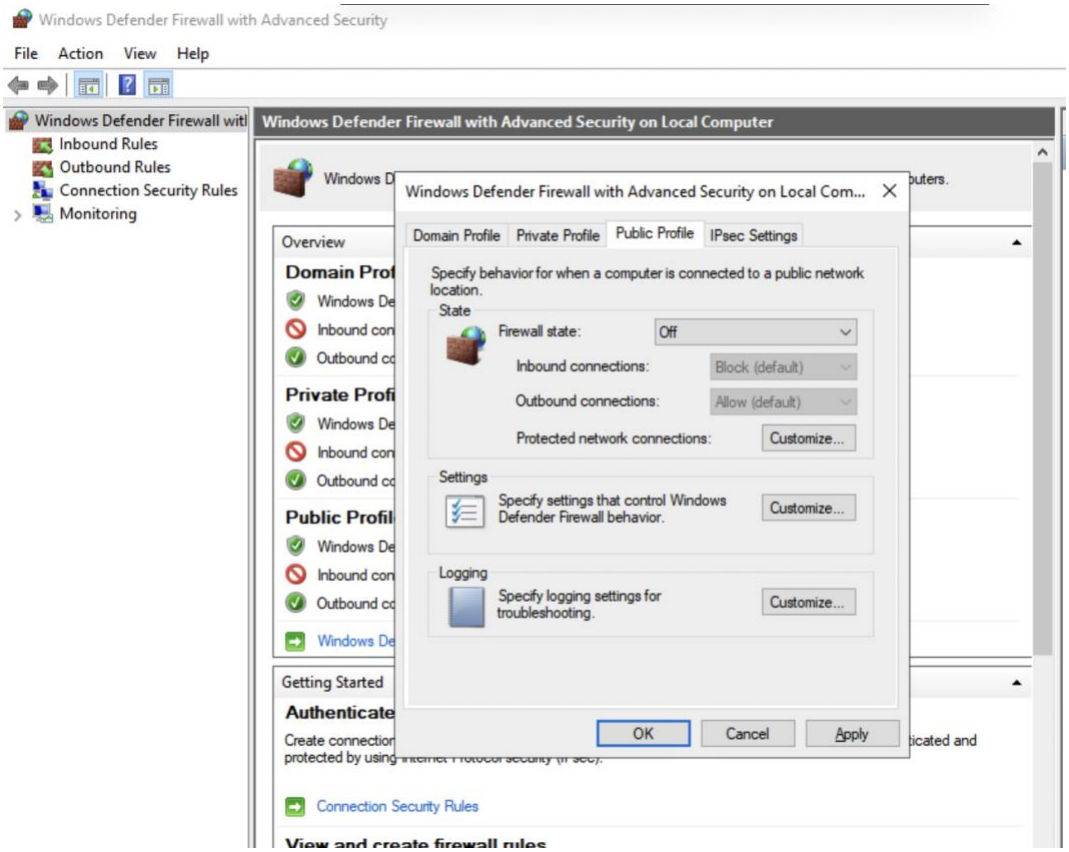
Result with basic window's 2019 configuration



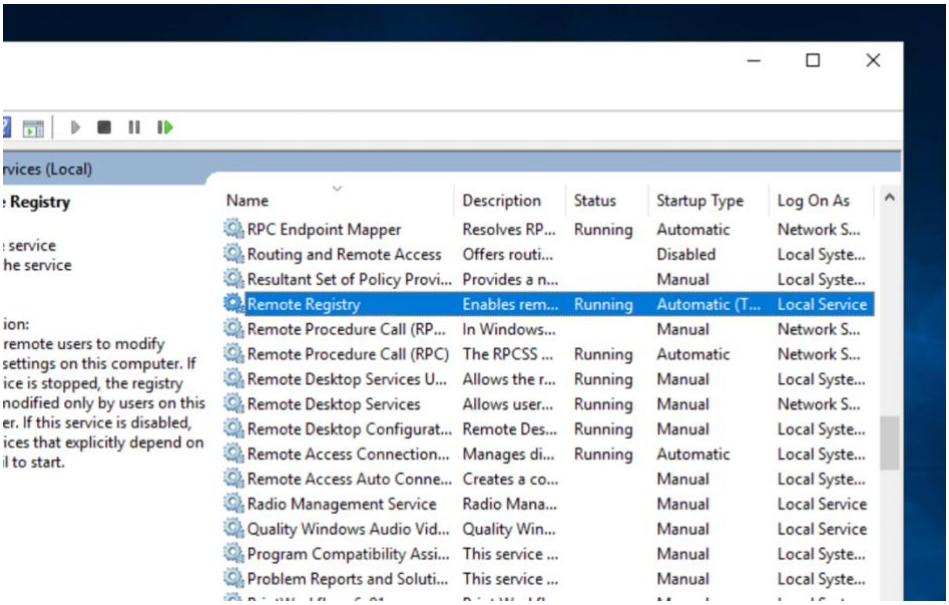
The VNC viewer is creating a higher vulnerability alert.



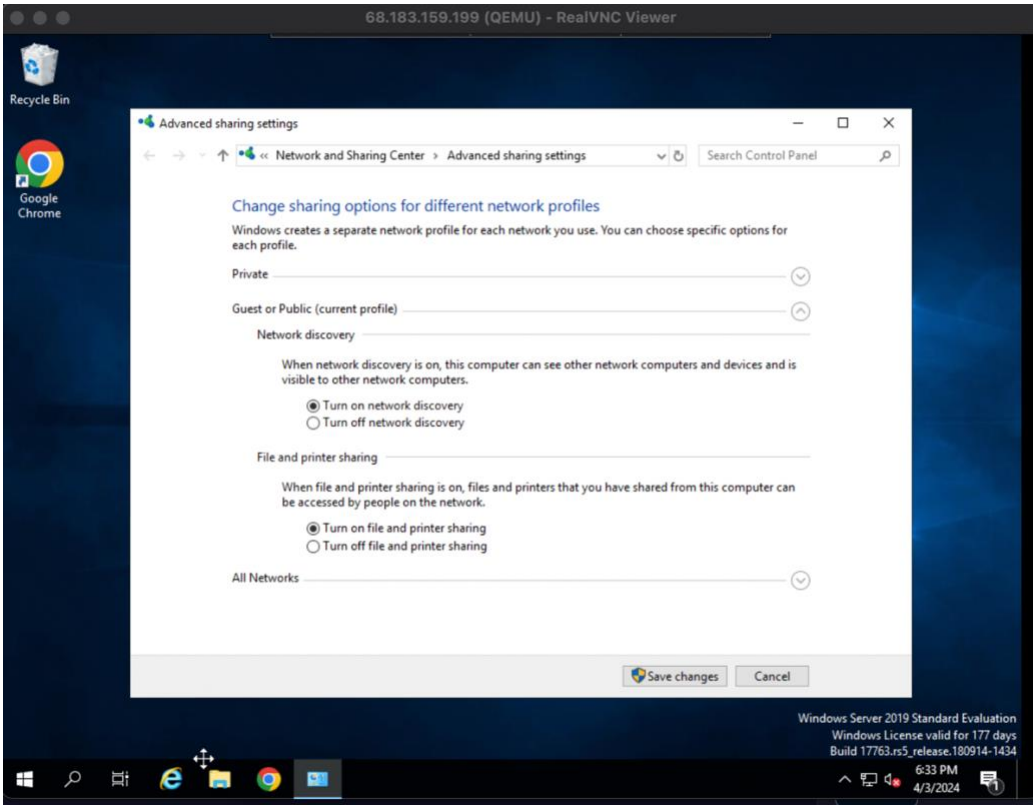
Making the Window Server more vulnerable by removing the firewall Status



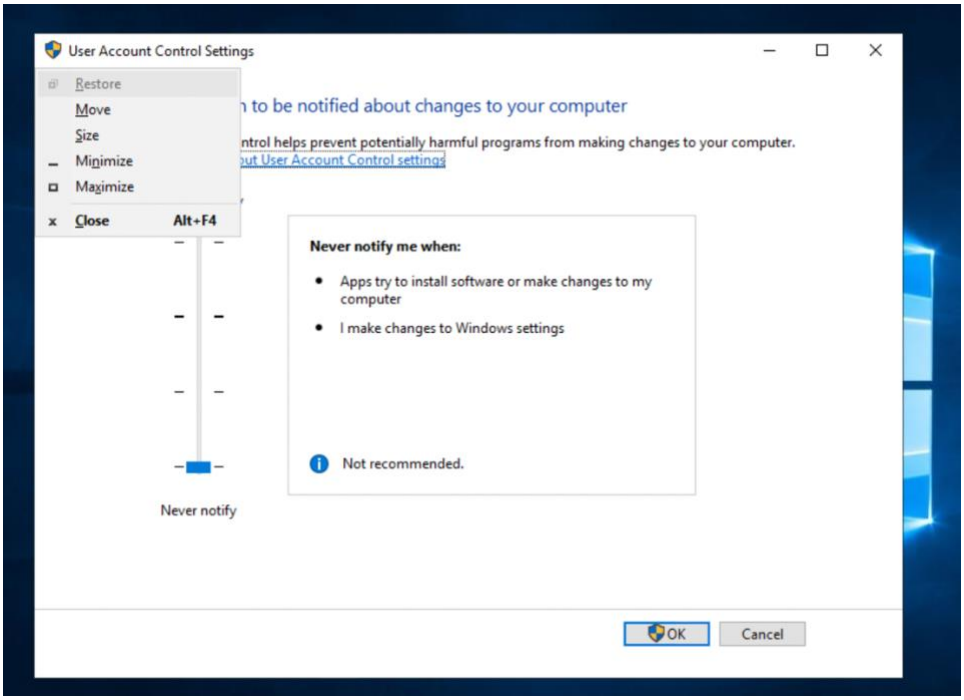
Enabling Remote Registry



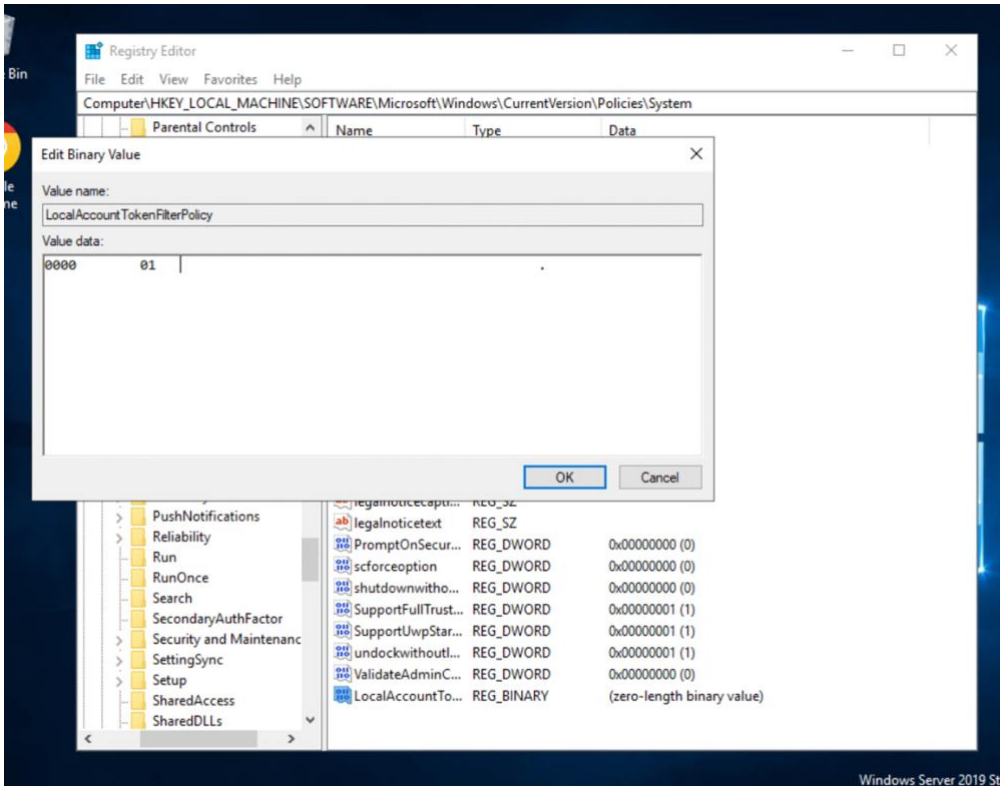
Turning on Automatic Network Sharing Settings



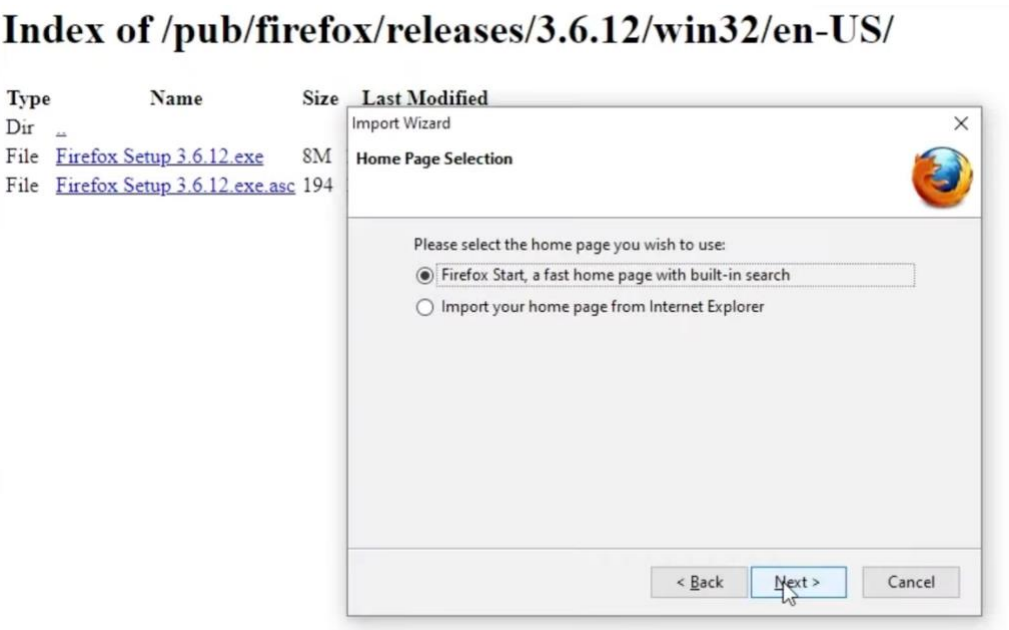
Applying Never Notifying on User Control Settings



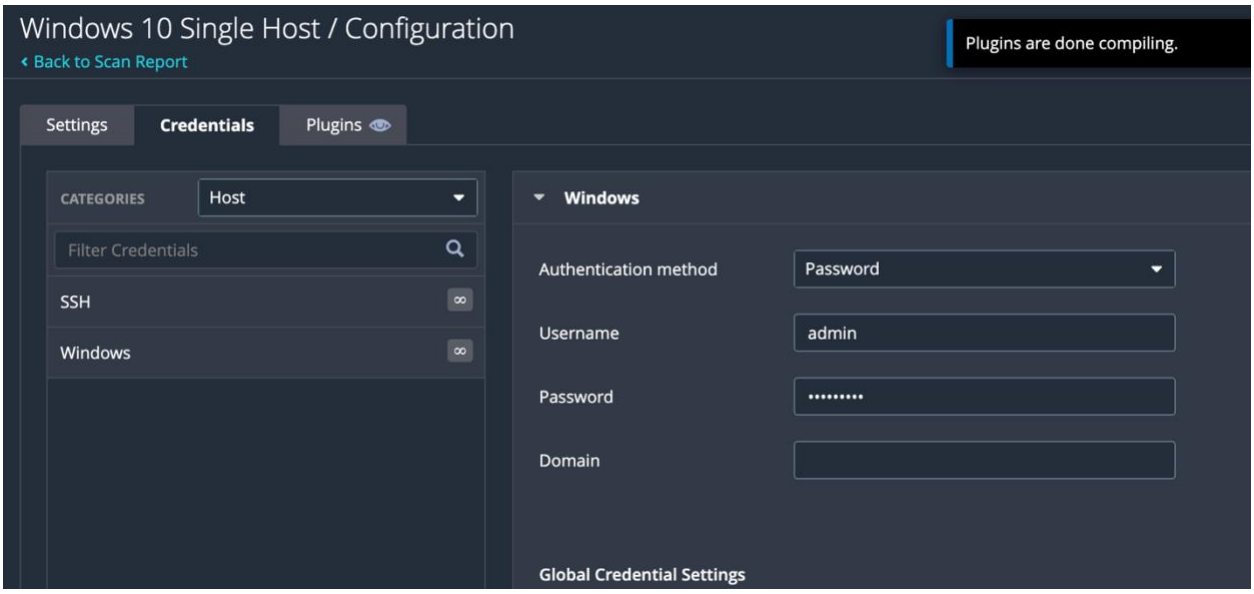
Creating a new Filter token Policy with binary value of 1



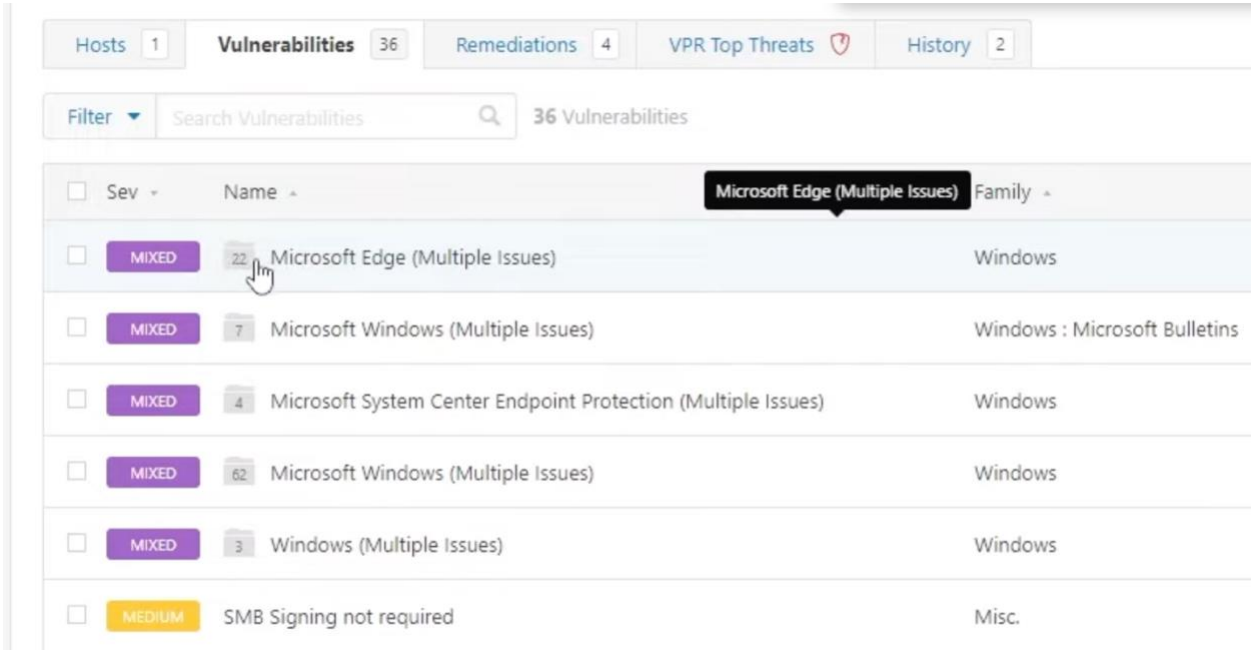
Installing Deprecated Mozella Firework



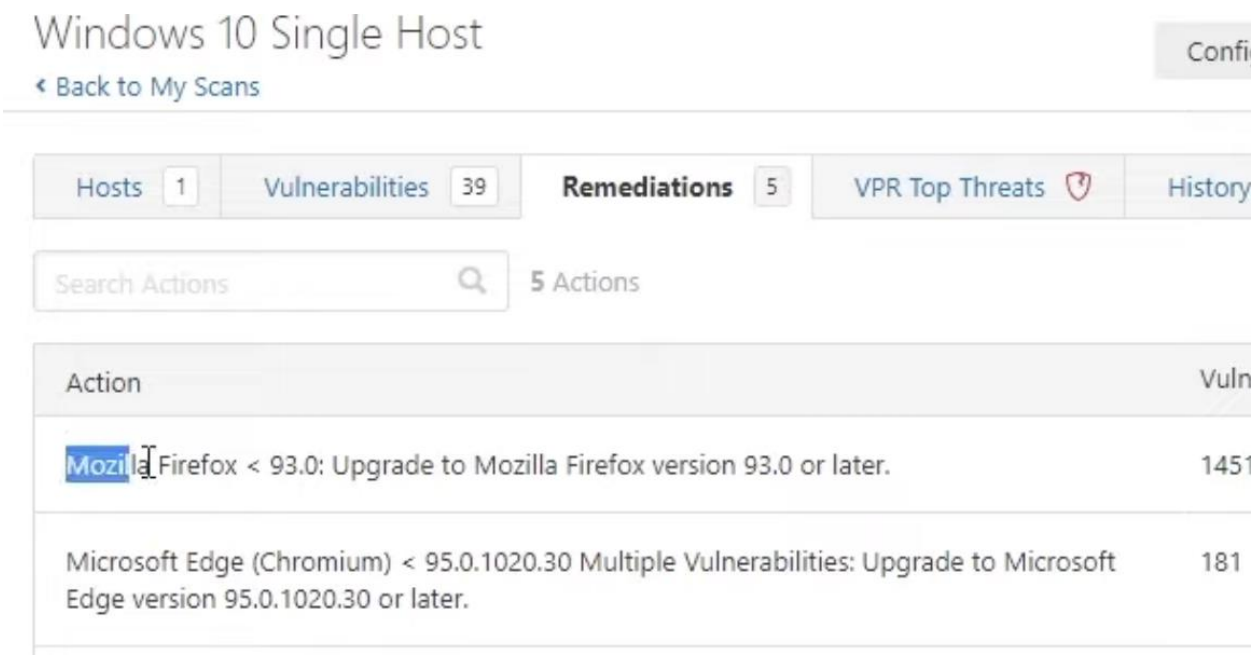
Performing a credential scan after the misconfigurations above



36 Vulnerabilities have been identified.



A you can see Nessus notifies that the Mozilla Firefox needs to be upgraded.



Conclusion

Through the integration of various tools and platforms, this project has provided a comprehensive exploration of vulnerability management, emphasizing the significance of proactive security measures in safeguarding digital assets. By leveraging the Windows ISO 2019 Server, Digital Ocean's cloud infrastructure, and a suite of tools including Nessus Essentials, Firefox 3.6.12, Termius, and VNC Viewer, we have embarked on a journey to fortify system defenses and enhance cybersecurity resilience. One of the key takeaways from this project is the refinement of skills in utilizing Nessus Essentials for vulnerability scanning. By conducting credentialed scans and meticulously analyzing the results, we have gained insights into the vulnerabilities present within our systems. Additionally, the project has underscored the importance of verification in the vulnerability management process, ensuring the reliability and accuracy of scan results.

Overall, this project serves as a testament to the efficacy of proactive vulnerability management practices. By embracing tools such as Nessus Essentials and adopting a systematic approach to vulnerability scanning and verification, we have fortified our understanding of cybersecurity best practices and are better equipped to mitigate potential threats in our digital environments.