**Name:** Hemant Jain

**Lab Progress Report Due Date:** 04/05/2021

**Current Week Since Start Date:** Week 11 (04/07/2021– 04/13/2021)

**Reporting Week:** From Mar 30, 2021 to Apr 05, 2021

**Summary about the Test Out Module-11 Learning:**

From the Test Out LabSim, I learnt about Security Assessments. The module initially started with the discussion on Penetration Testing: Types of Penetration Tests, Security Teams, Documentation/Contracts, Penetration Testing Life Cycle. The four different types of penetration test types discussed were White Box, Black Box, Gray box, Bug bounties. The security team’s brief description and detailing out the Red Team, Blue Team, Purple Team, and White team. There were various documentation and contract types are discussed which outline the goals and guidelines of the tests and the scope of work and rules.

Documentation Types like Scope of work is a very detailed document that defines exactly what is going to be included in the penetration test and the Rules of Engagement document defines exactly how the penetration test will be carried out. Penetration Testing Life Cycle starts with Performing Reconnaissance, Scan/Enumerate, Gain Access, Maintain Access, Report.

In the Monitoring and reconnaissance lessons learnt how to perform the port and ping scans on the virtual machines. Performed Reconnaissance with Nmap and Harvester tool. Discussed some tools which are important to monitor the health of a network. Defining Reconnaissance also known as foot printing , is the process of gathering as much information about a target before beginning in any penetration test or security audit. Passive and Active Reconnaissance exists; with each one including some 4-5 methods to gather information on the target with no direct interaction with that target.

Continuing further learnt how to implement intrusion monitoring and intrusion prevention and using **squil** and **squert**. Read about the difference between IDSs and IPSs. Detection methods like Signature-based and Heuristic-based and the host-based and network-based device implementation of IDS/IPS. Performed lab on Scanning for Windows, Linux, Domain Controller, Security Appliance, Web Application Protection (WAP) vulnerabilities.

Threat hunting which is the human-based, proactive and methodical searching and monitoring of the network, includes three steps: Trigger, Investigation and Resolution.

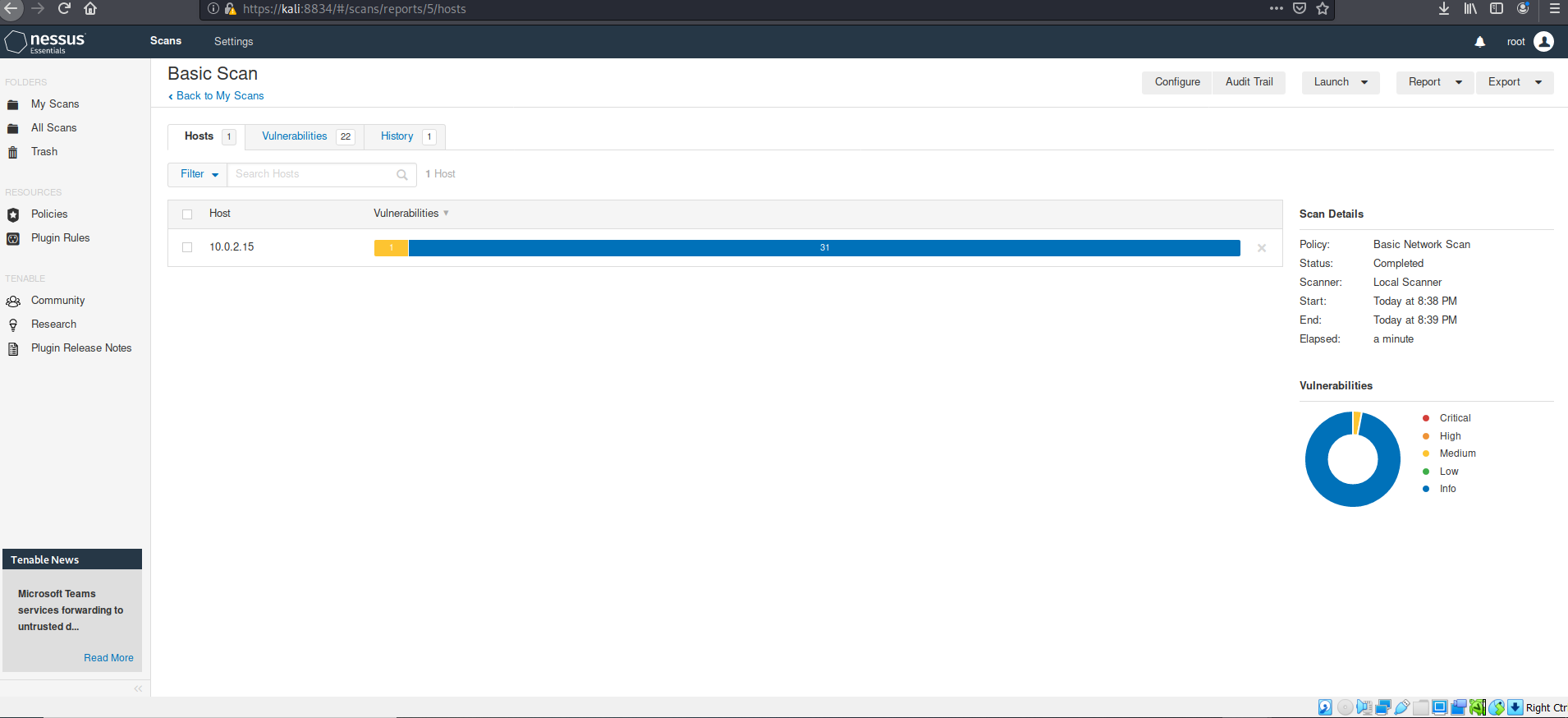
Read in detail about the Security Information and Event Management (SIEM) systems and Security Orchestration, Automation and Responses (SOAR) systems. Reading about how the protocol analyzers work and uses of protocol analyzers was one of my favorite topic to read in detail while going through the coursework. And in the end, learnt about the Poison ARP and analyses with Wireshark, Poison DNS, and Perform and analyze a SYN flood. Malicious Code Facts with Python, Command Shells, Macros.

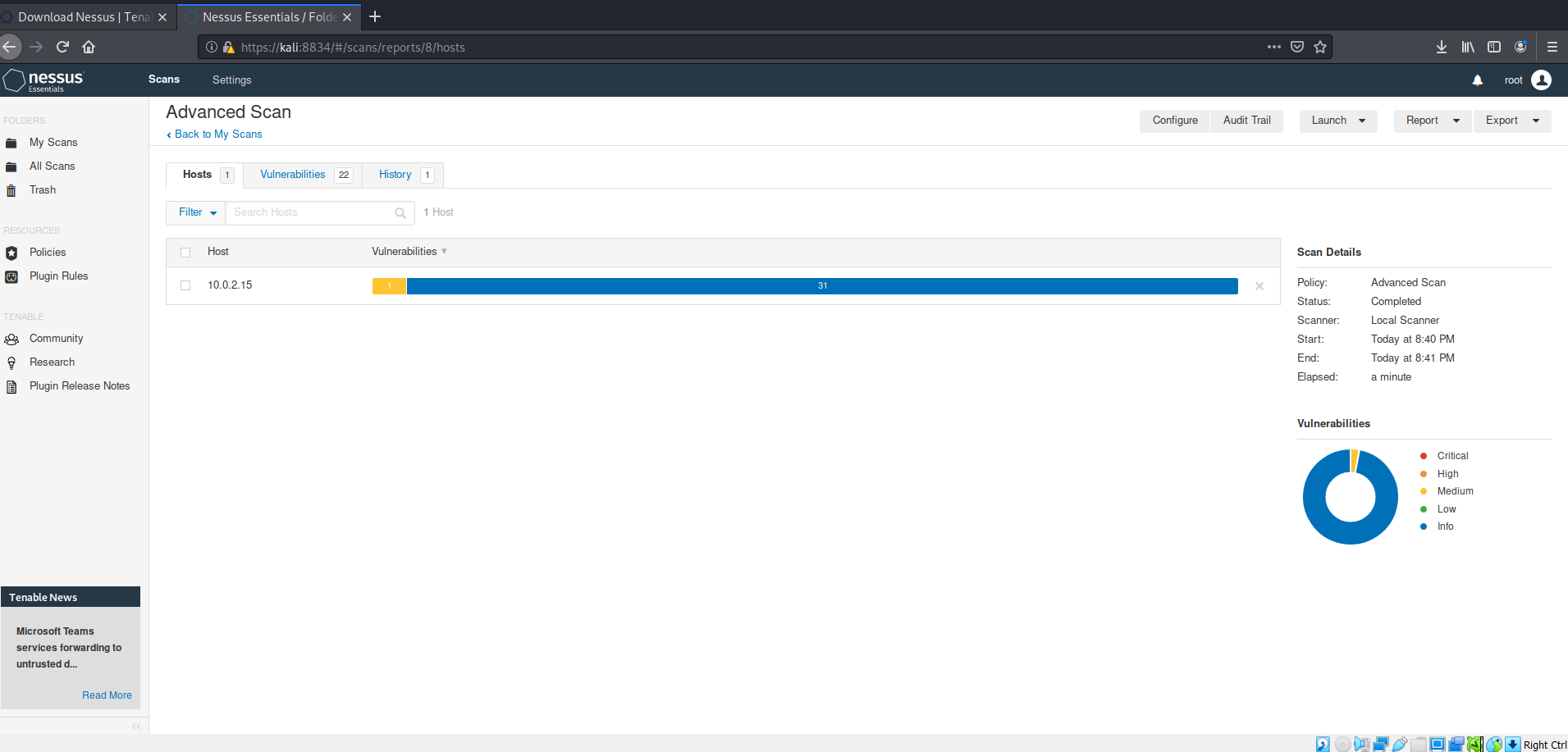
Lab on cracking a password using rainbow tables and with John the Ripper was a repetitive task of our previous lab which already performed in our curriculum in past.

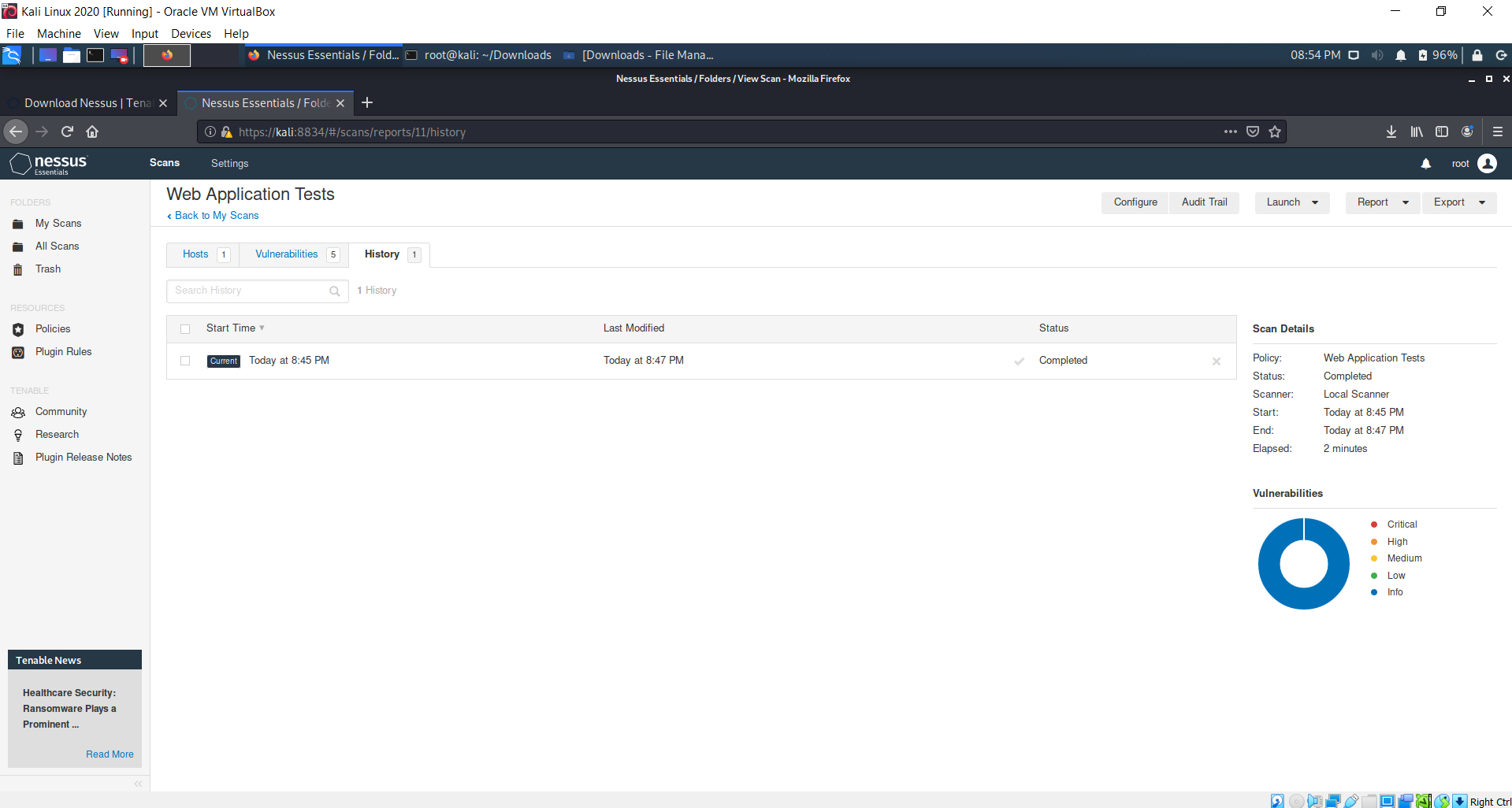
**Class Labs Screenshots:**

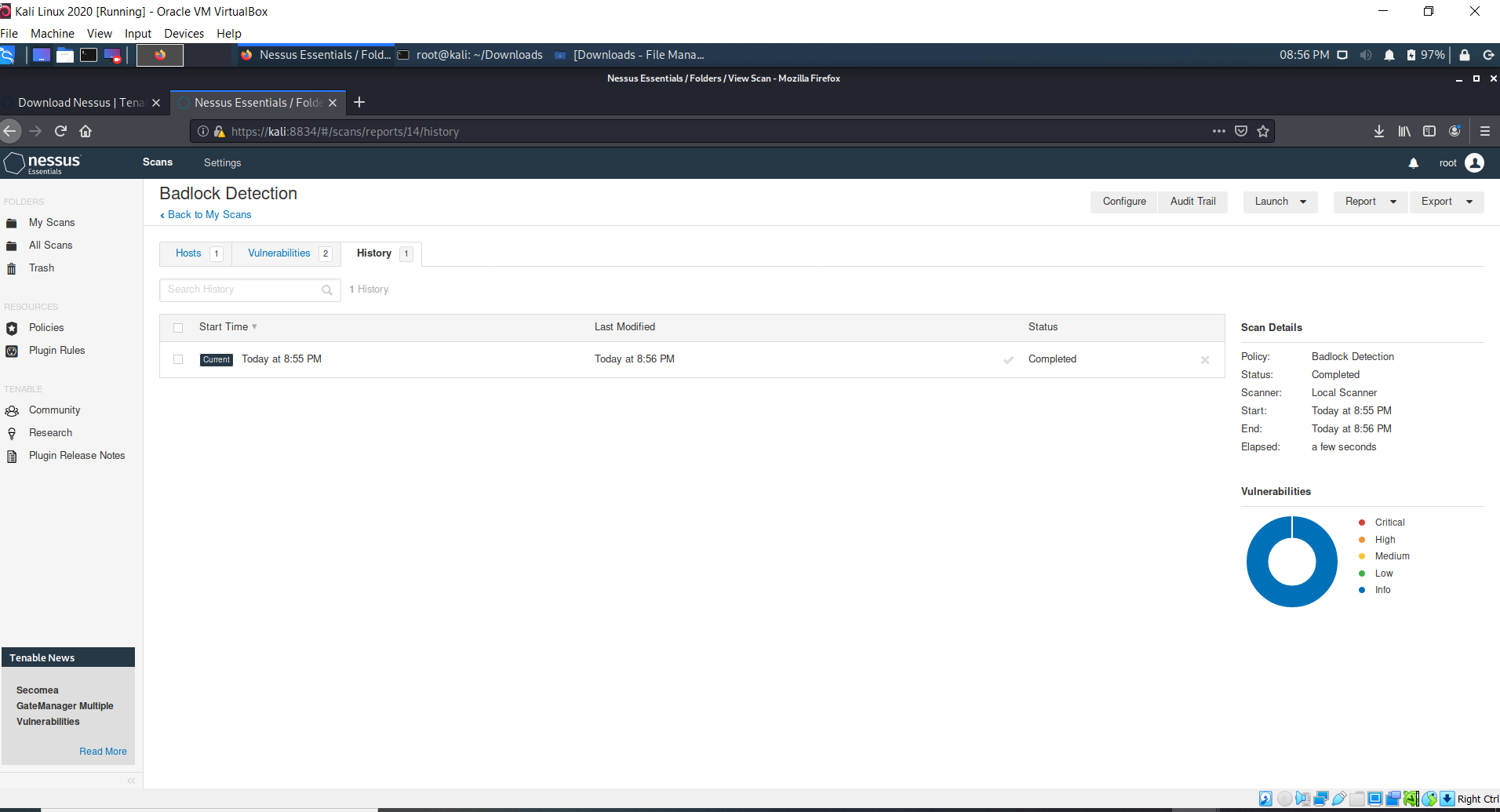
**Nessus Tool Diagnosis Results:**

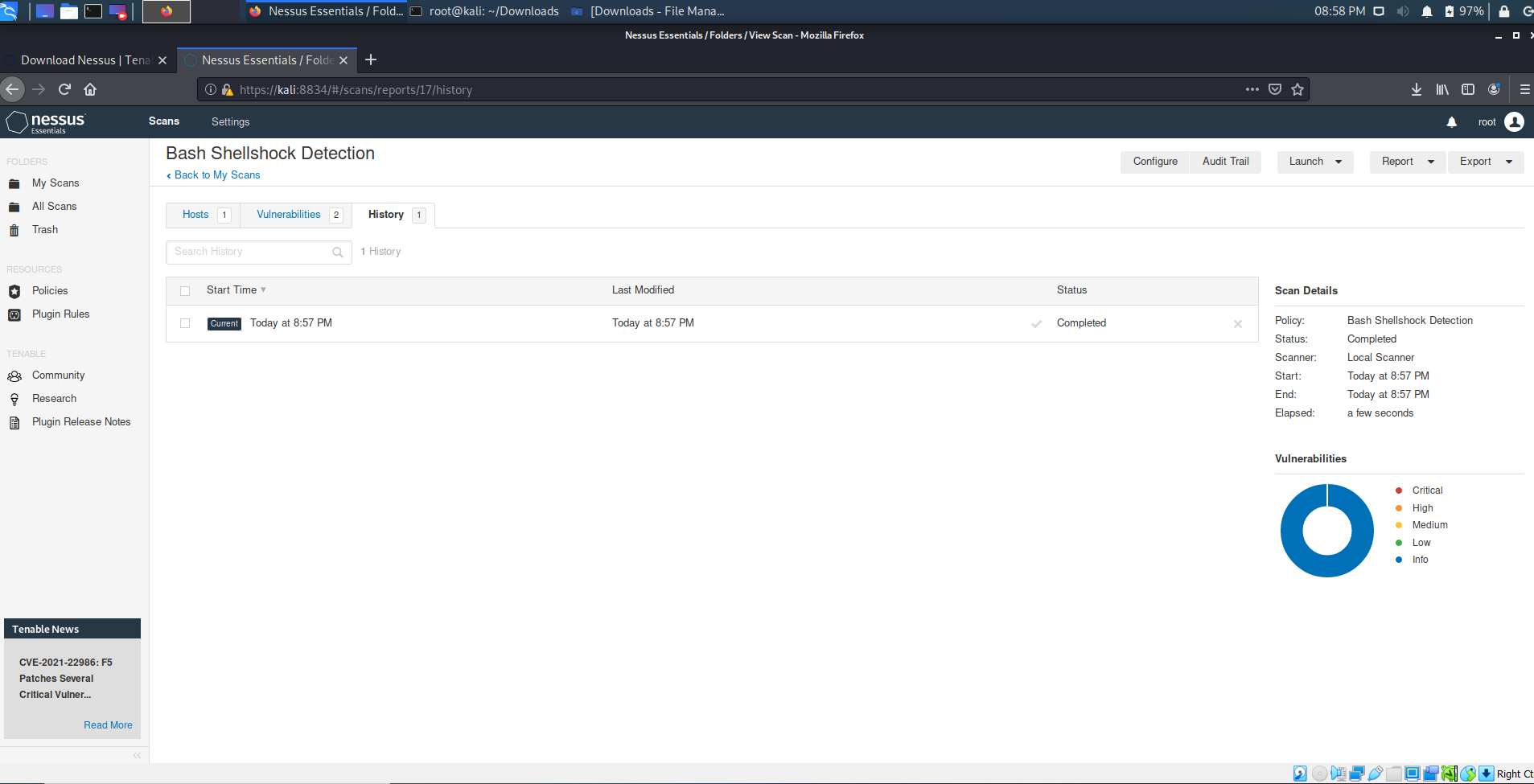
**Metasploitable Virtual Machine ---- 10.0.2.15 IP**

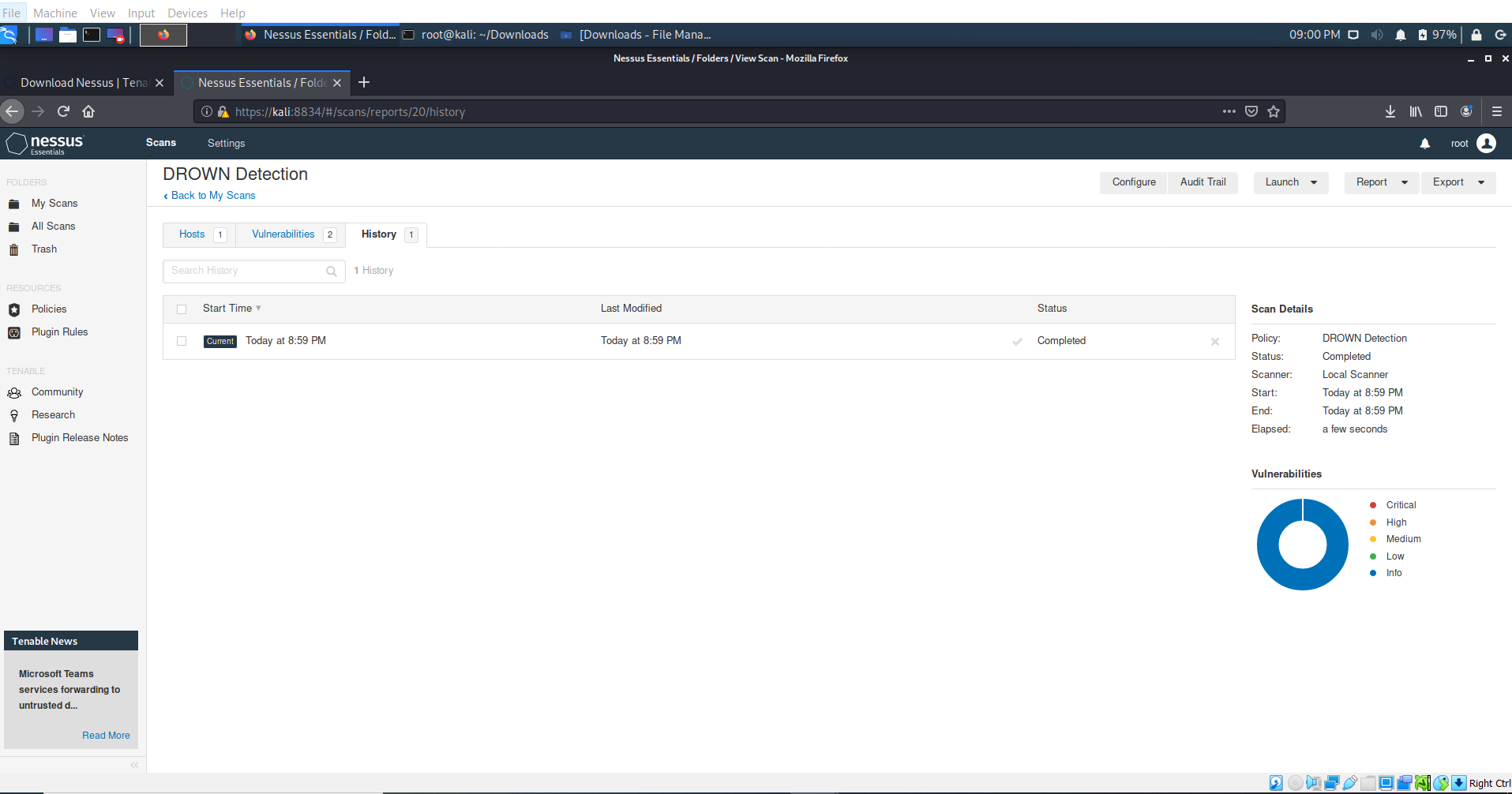


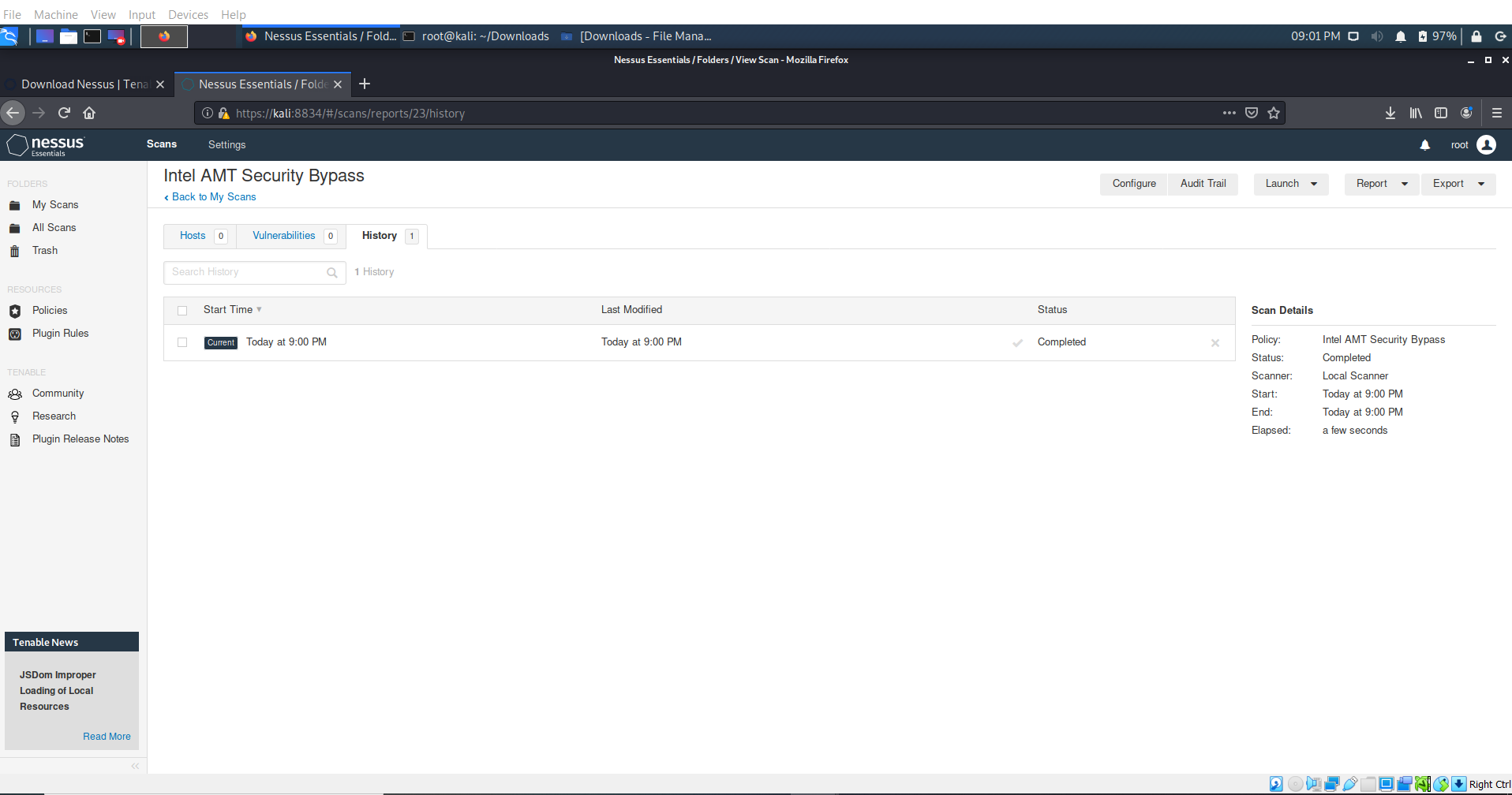


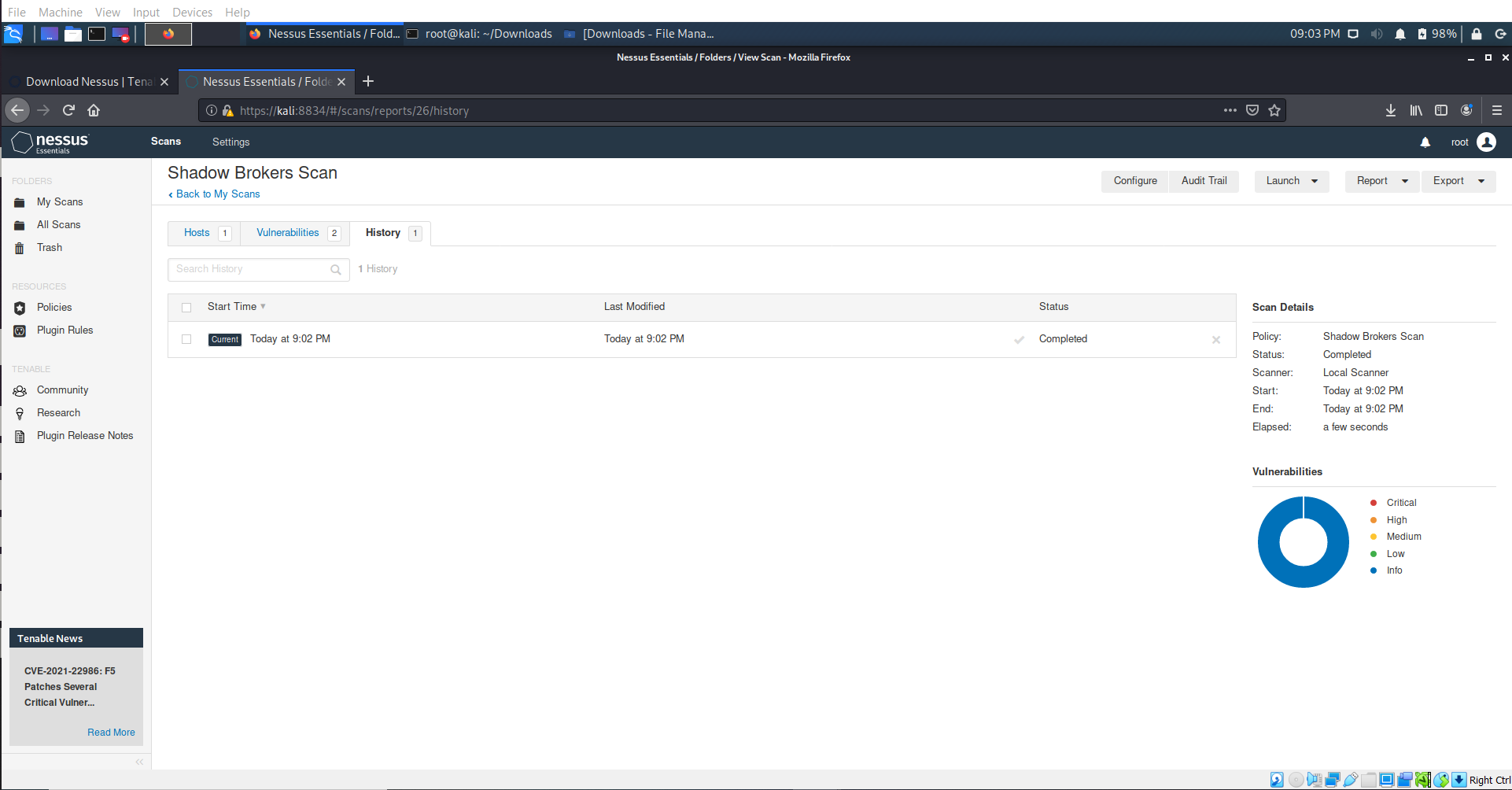


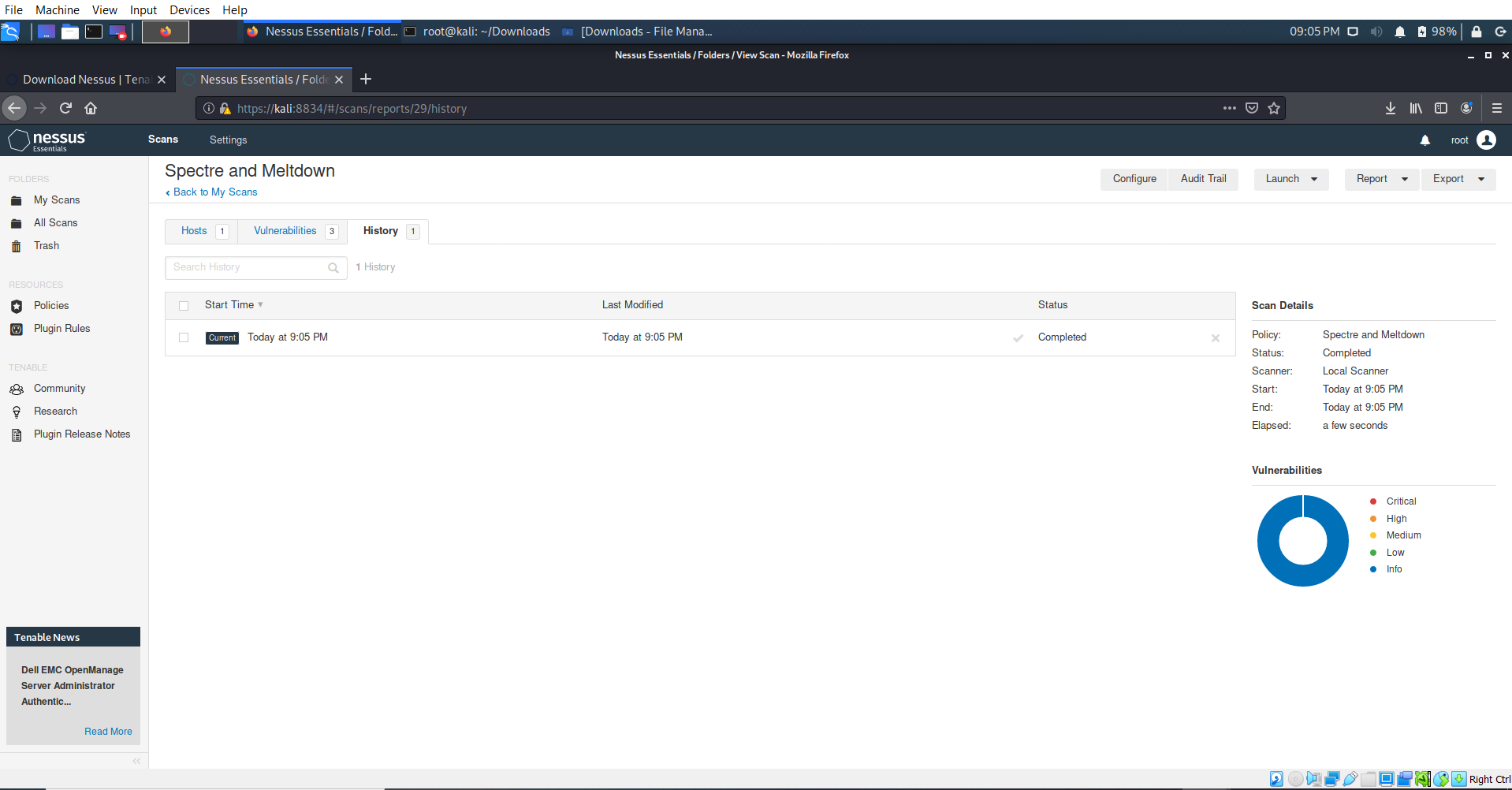


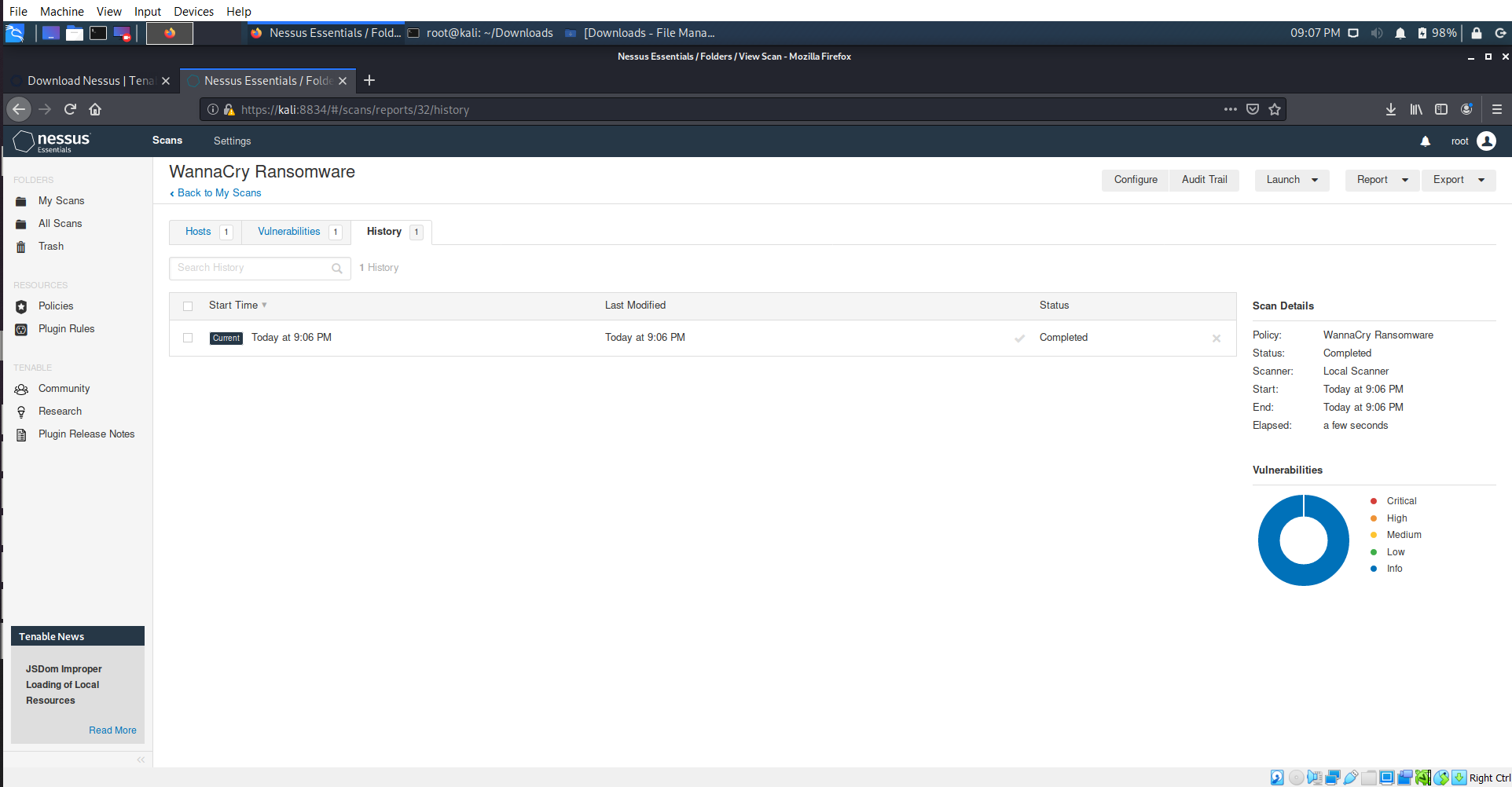


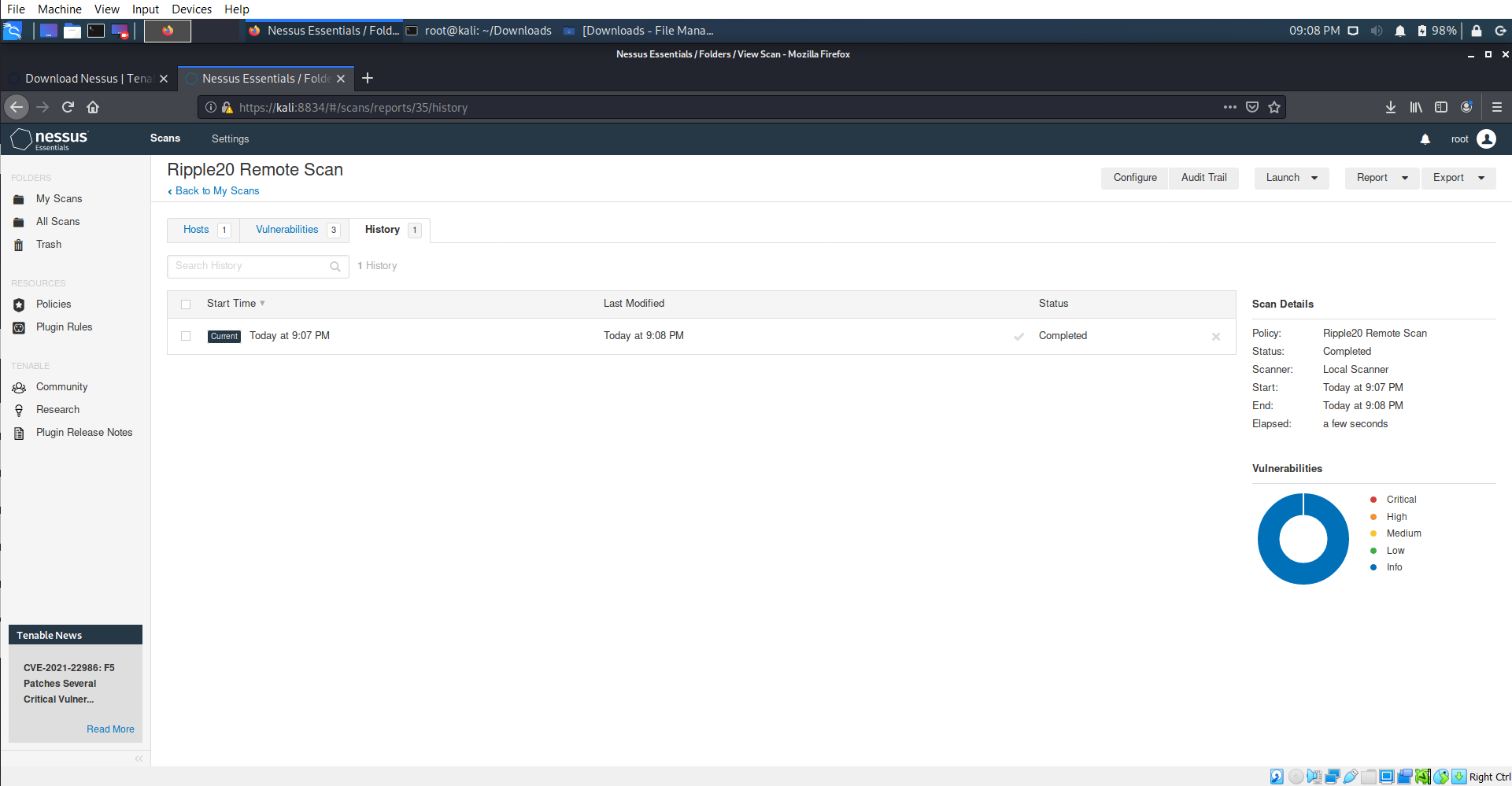


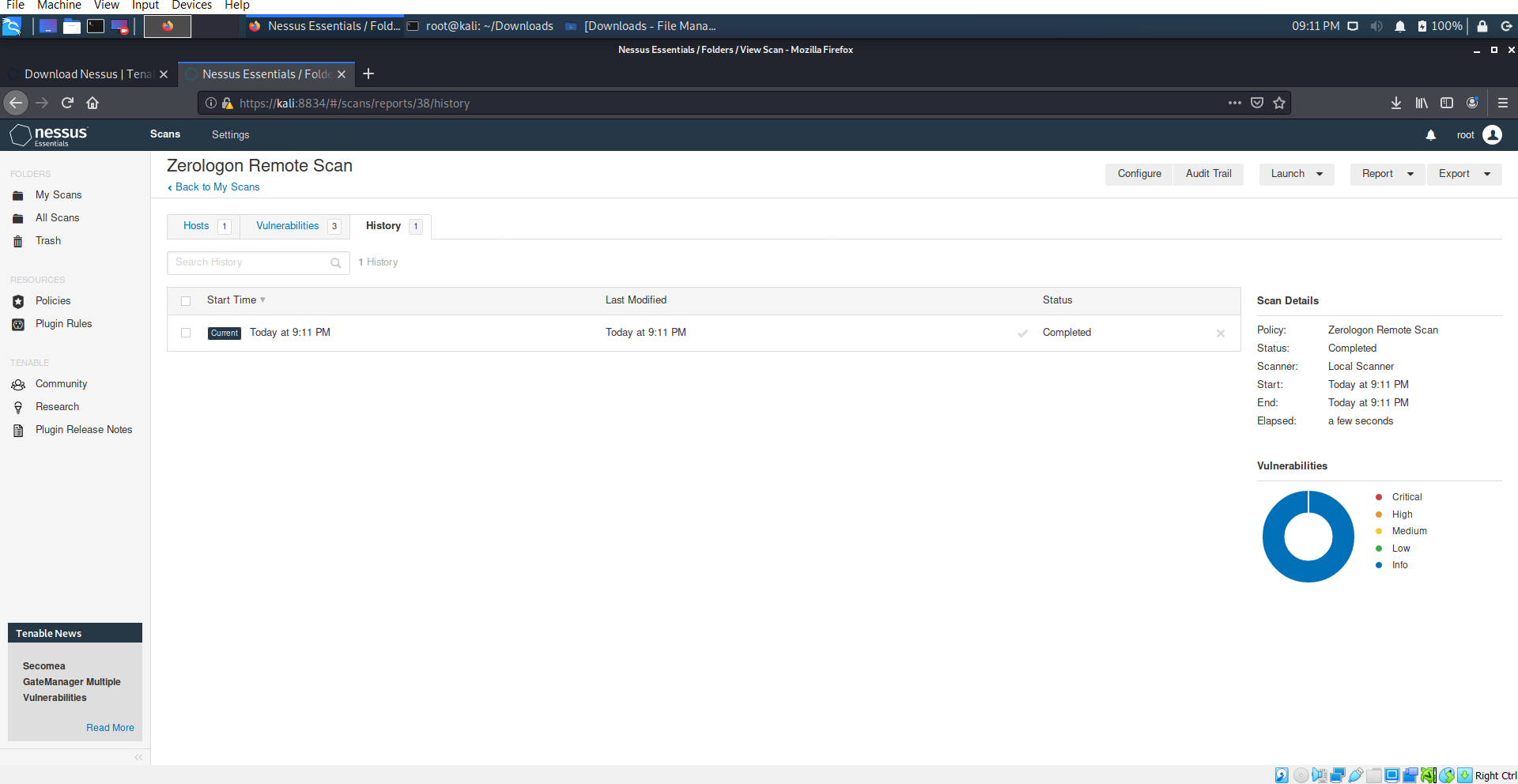


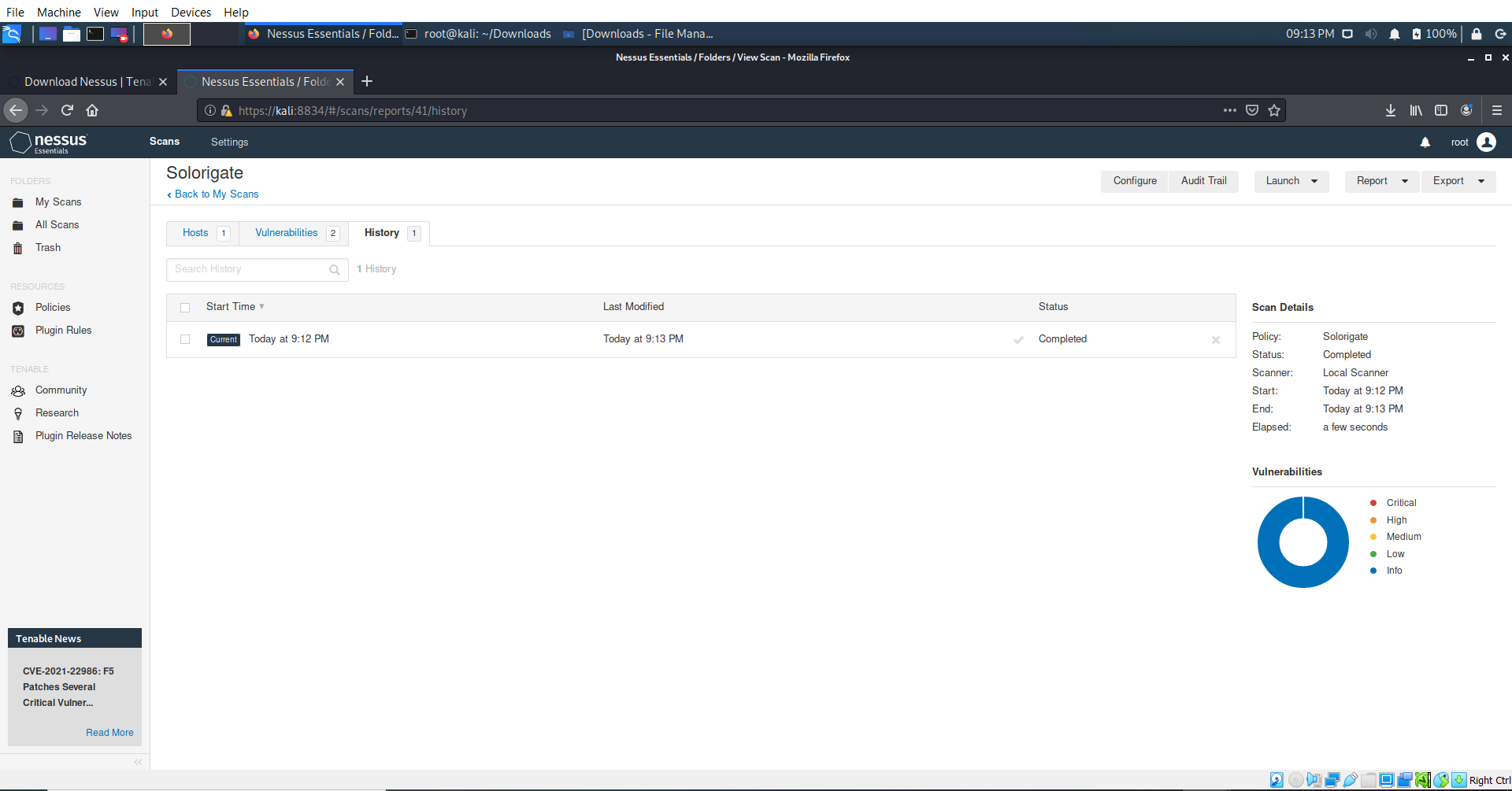


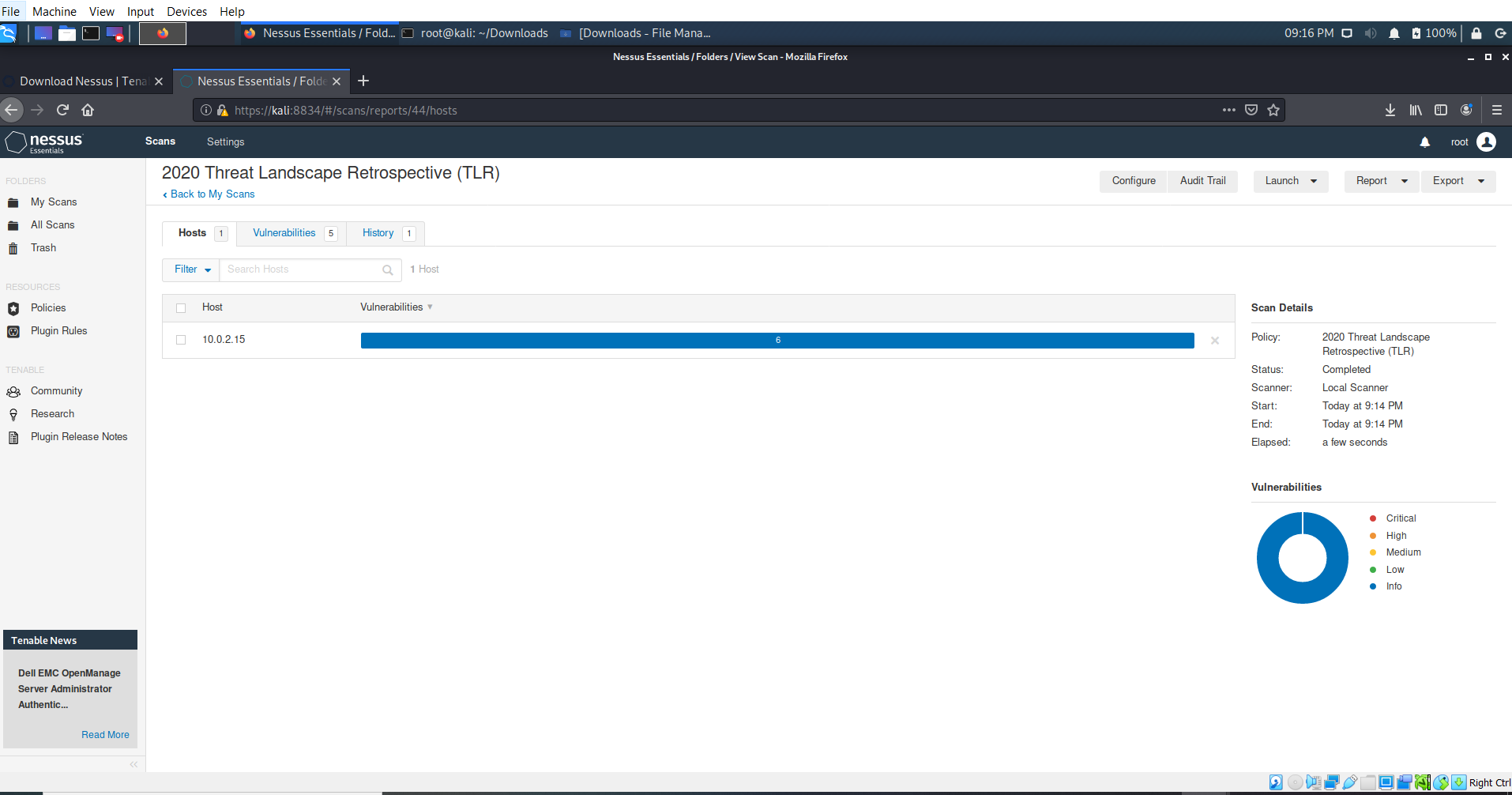


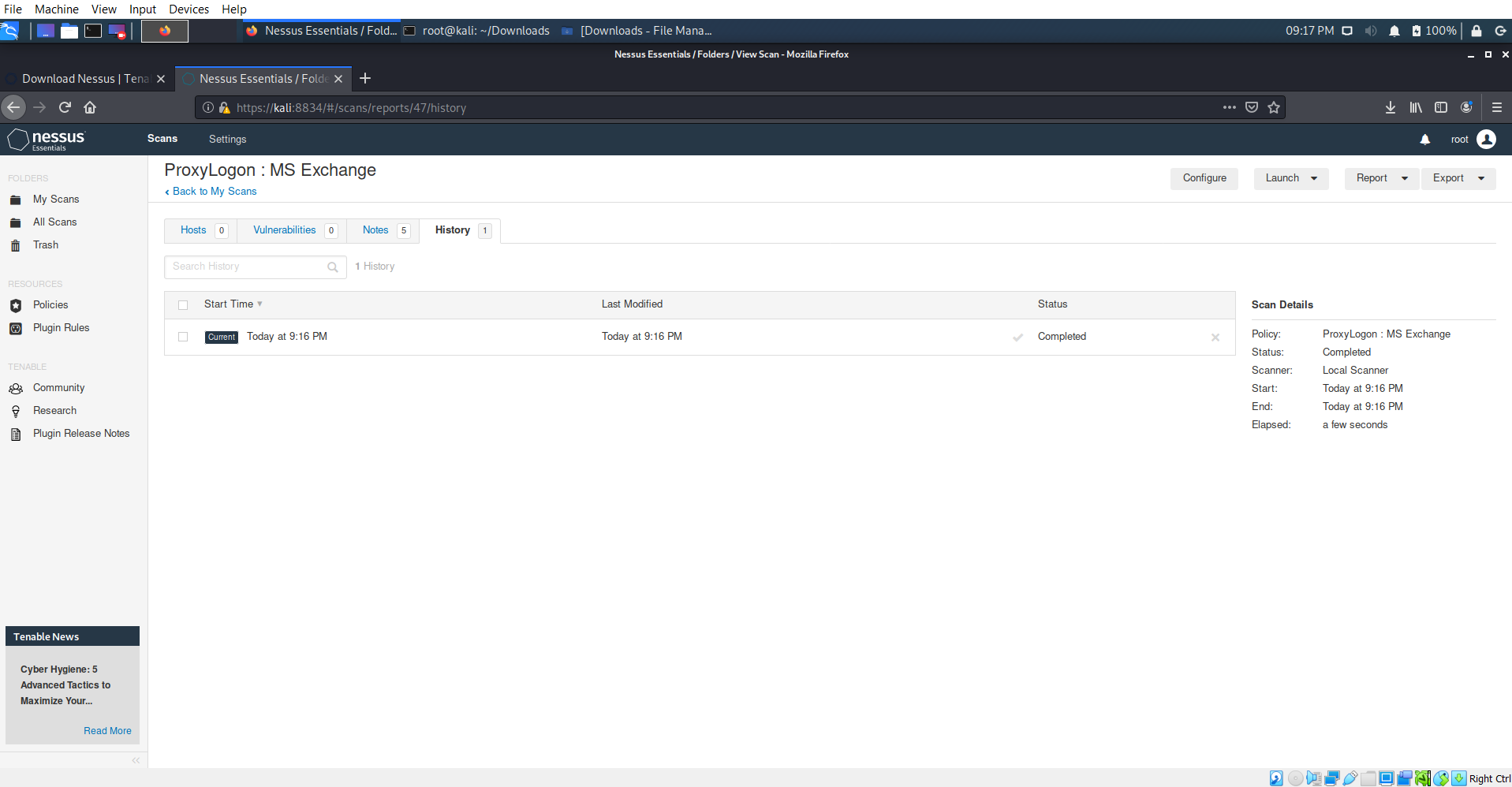


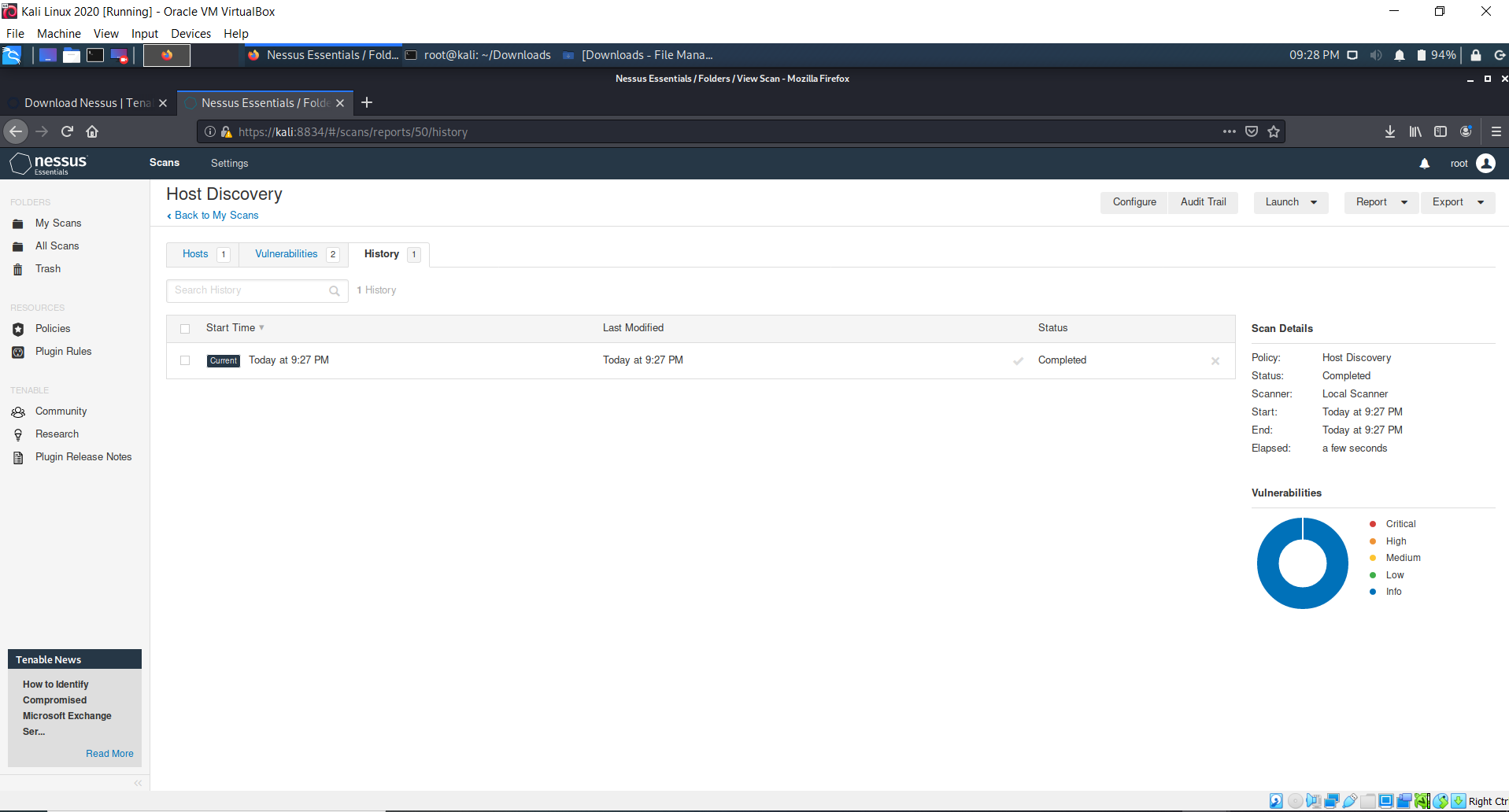


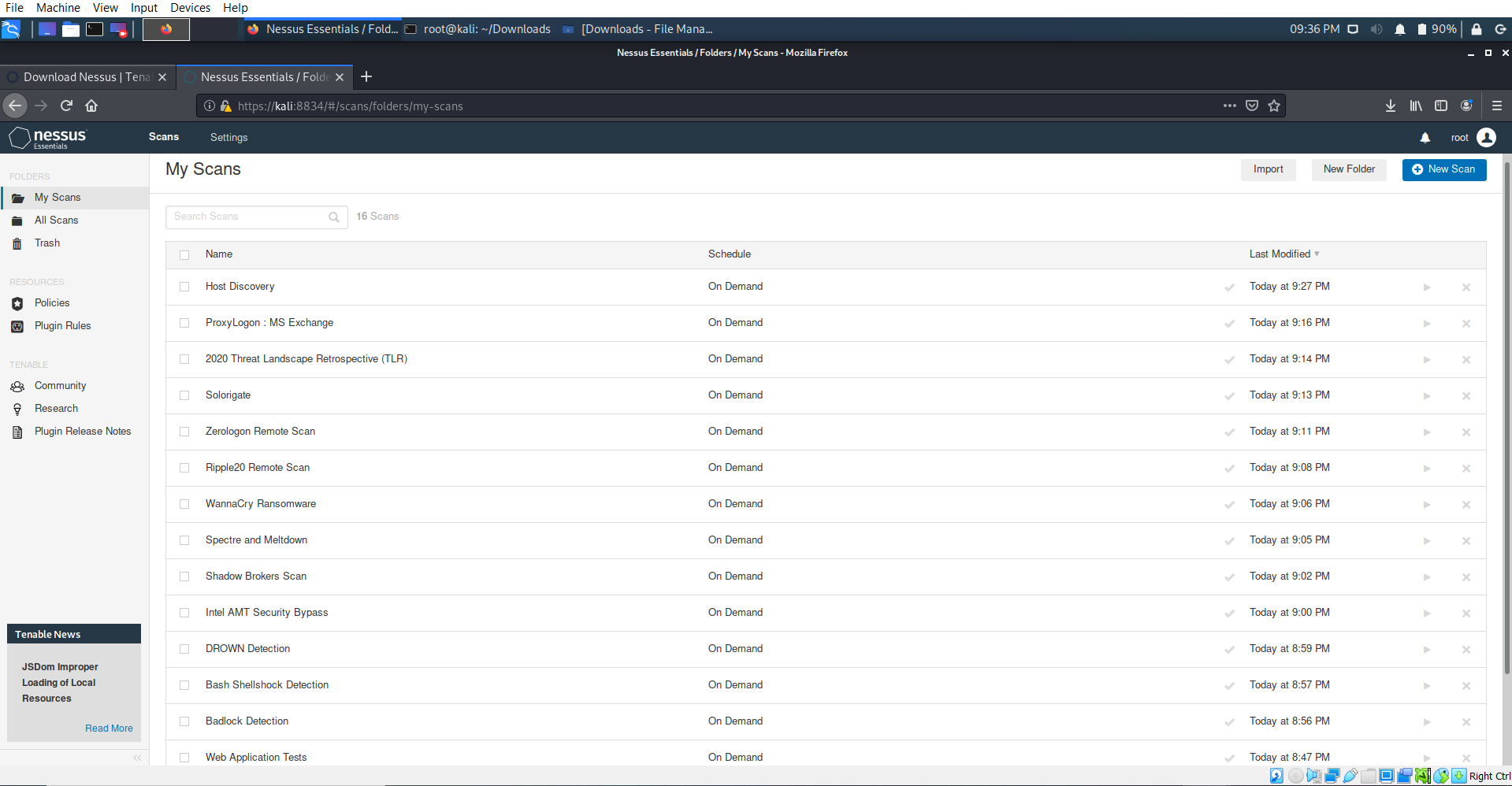




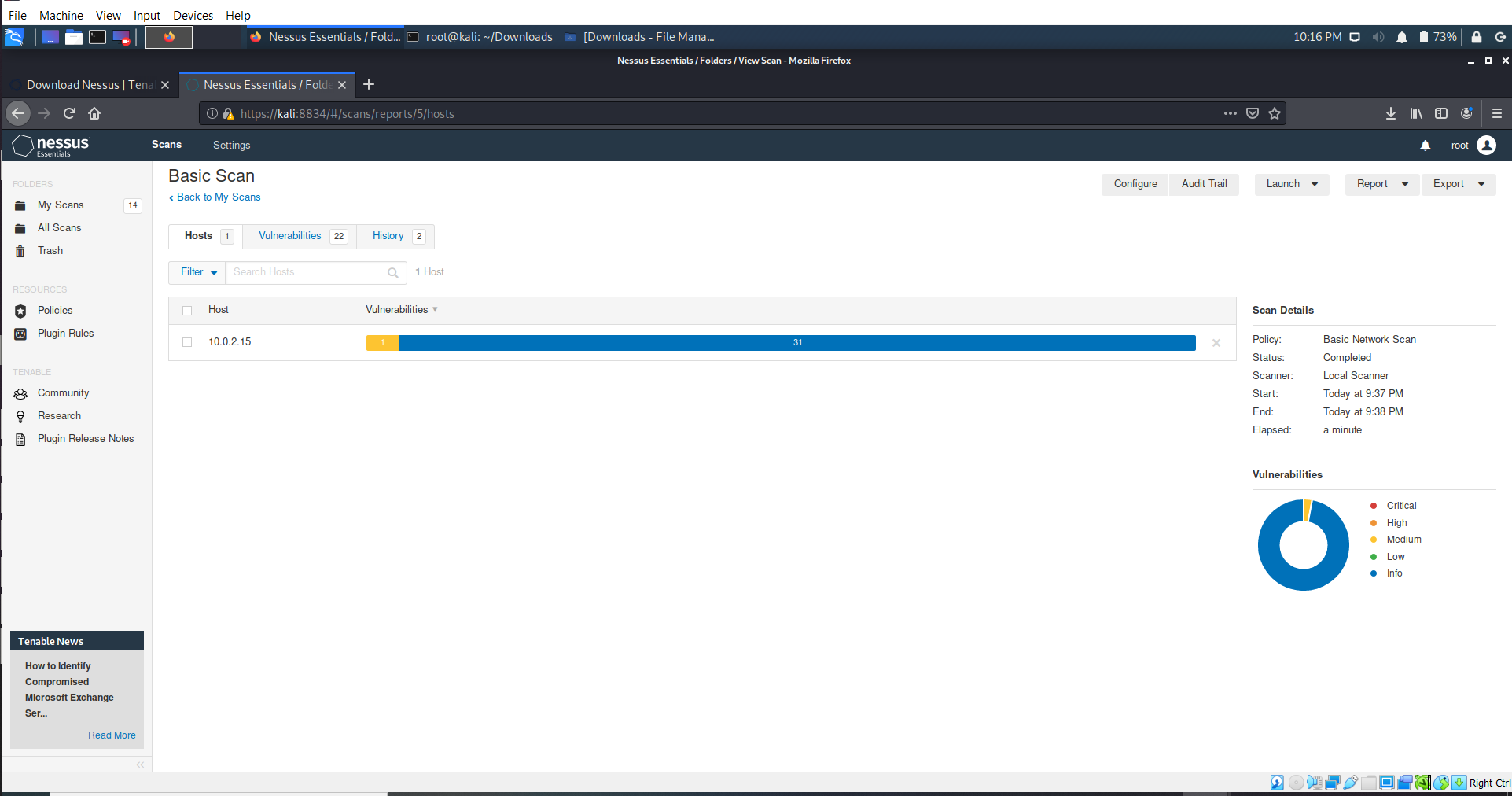


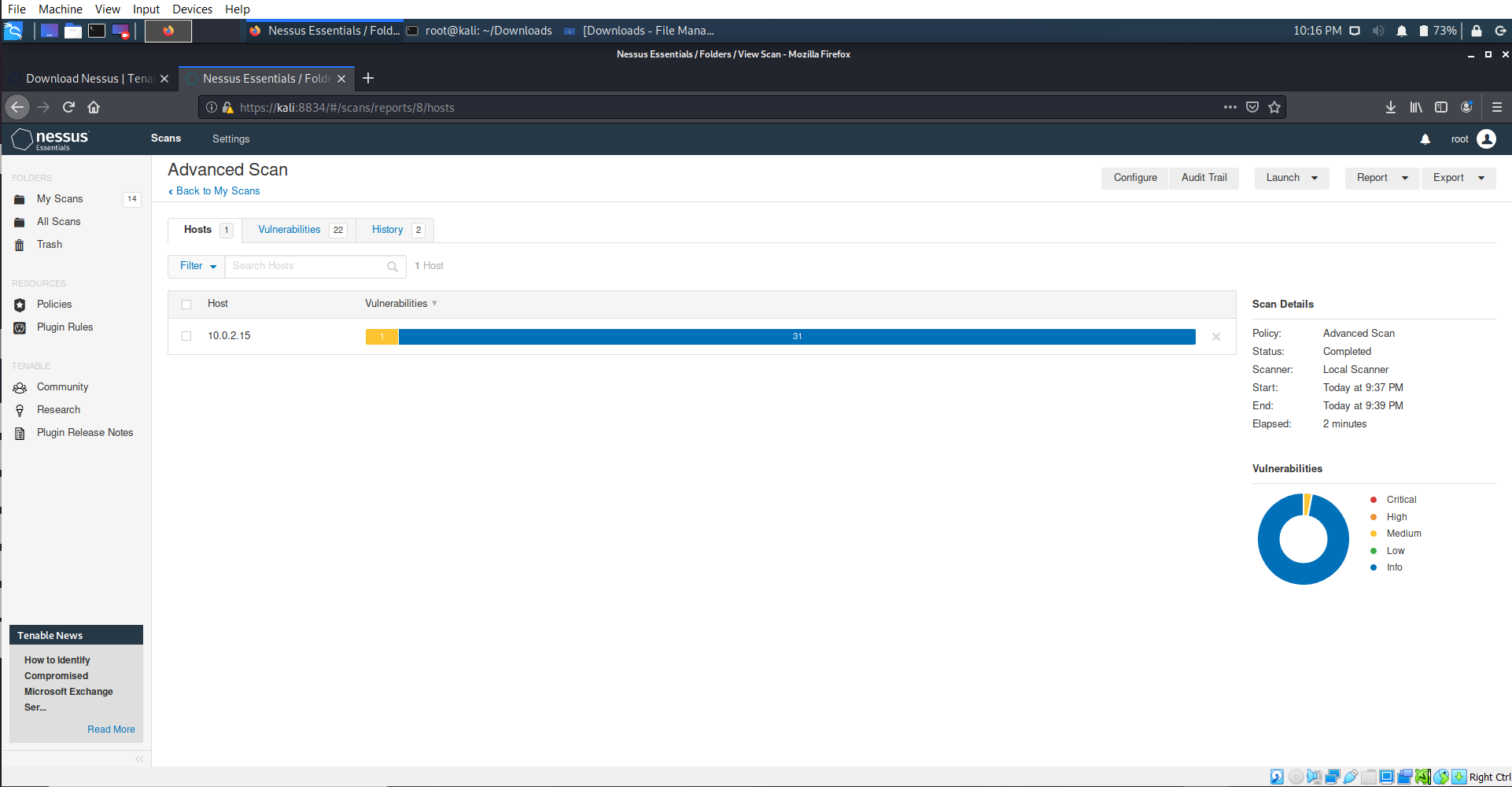


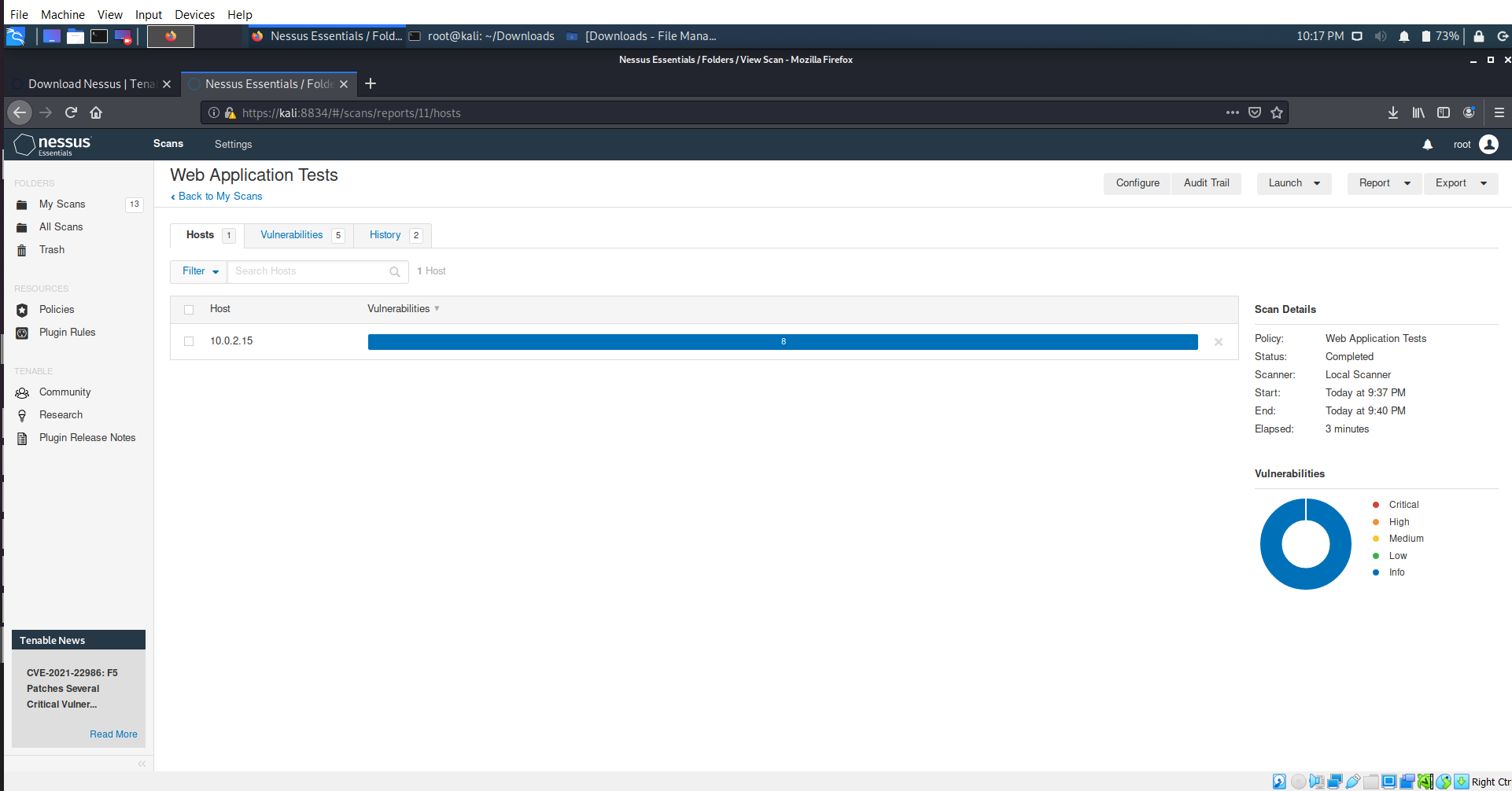


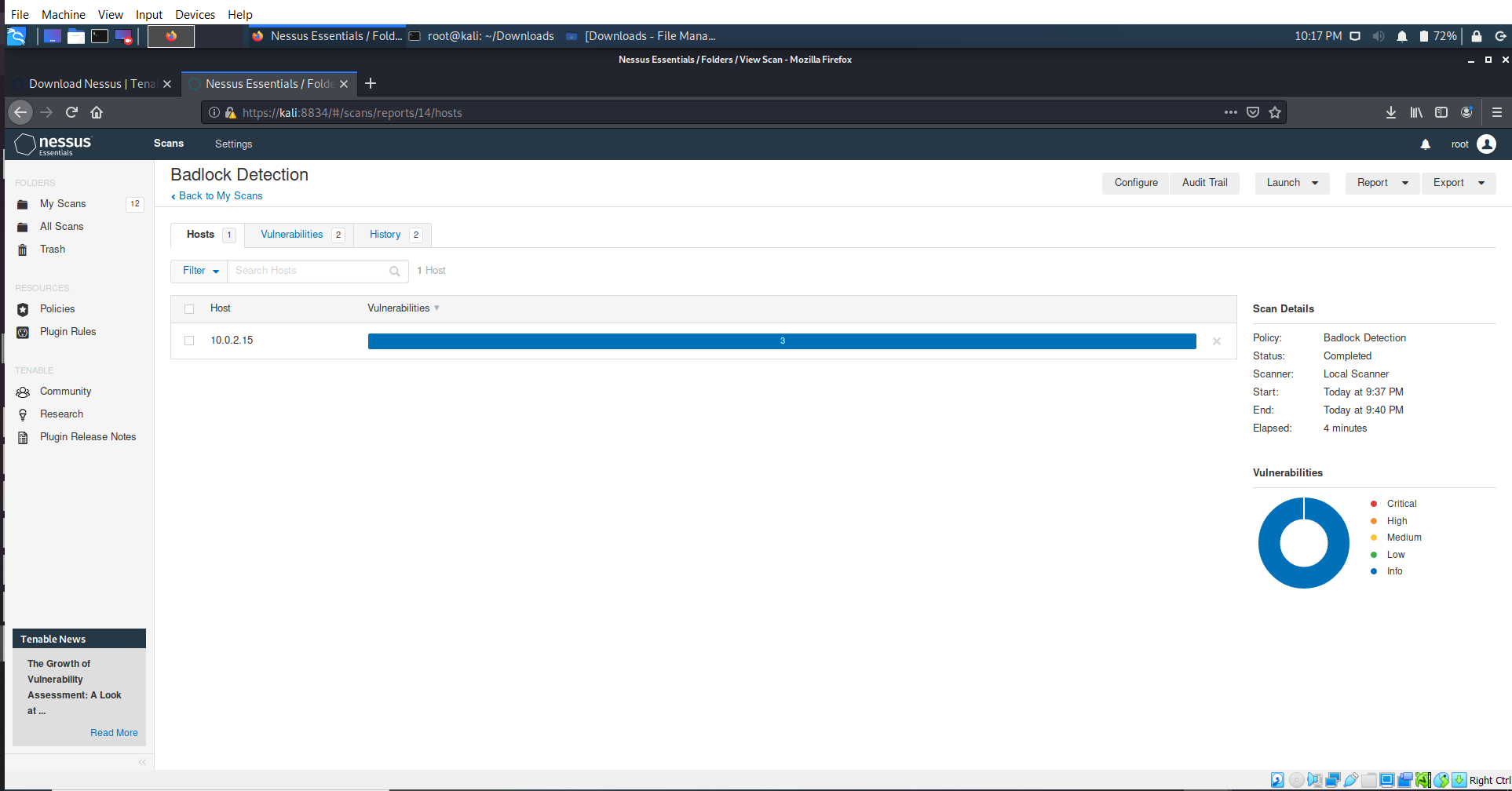


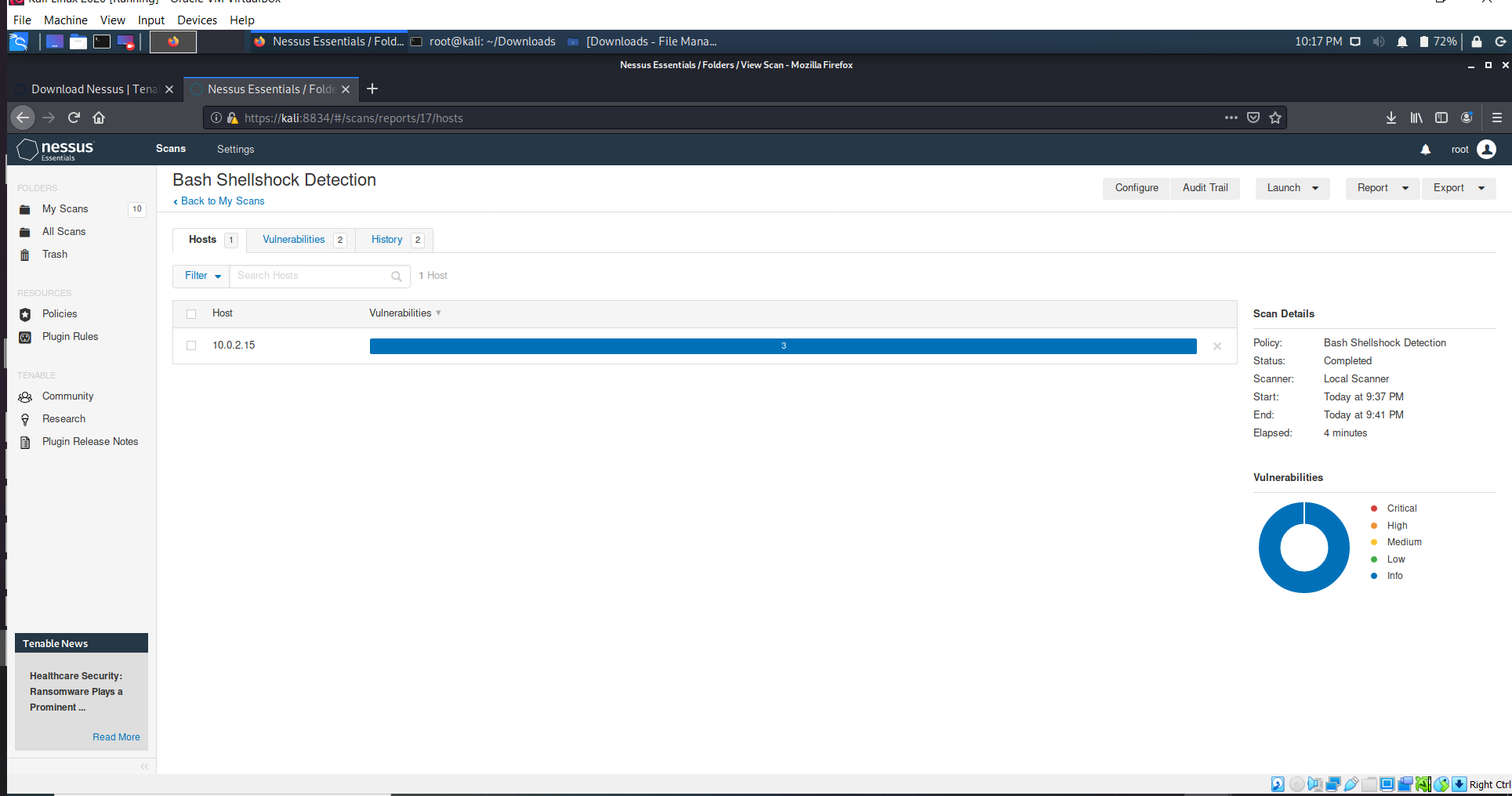
**SEED Ubuntu Virtual Machine ---- 10.0.2.15 IP**

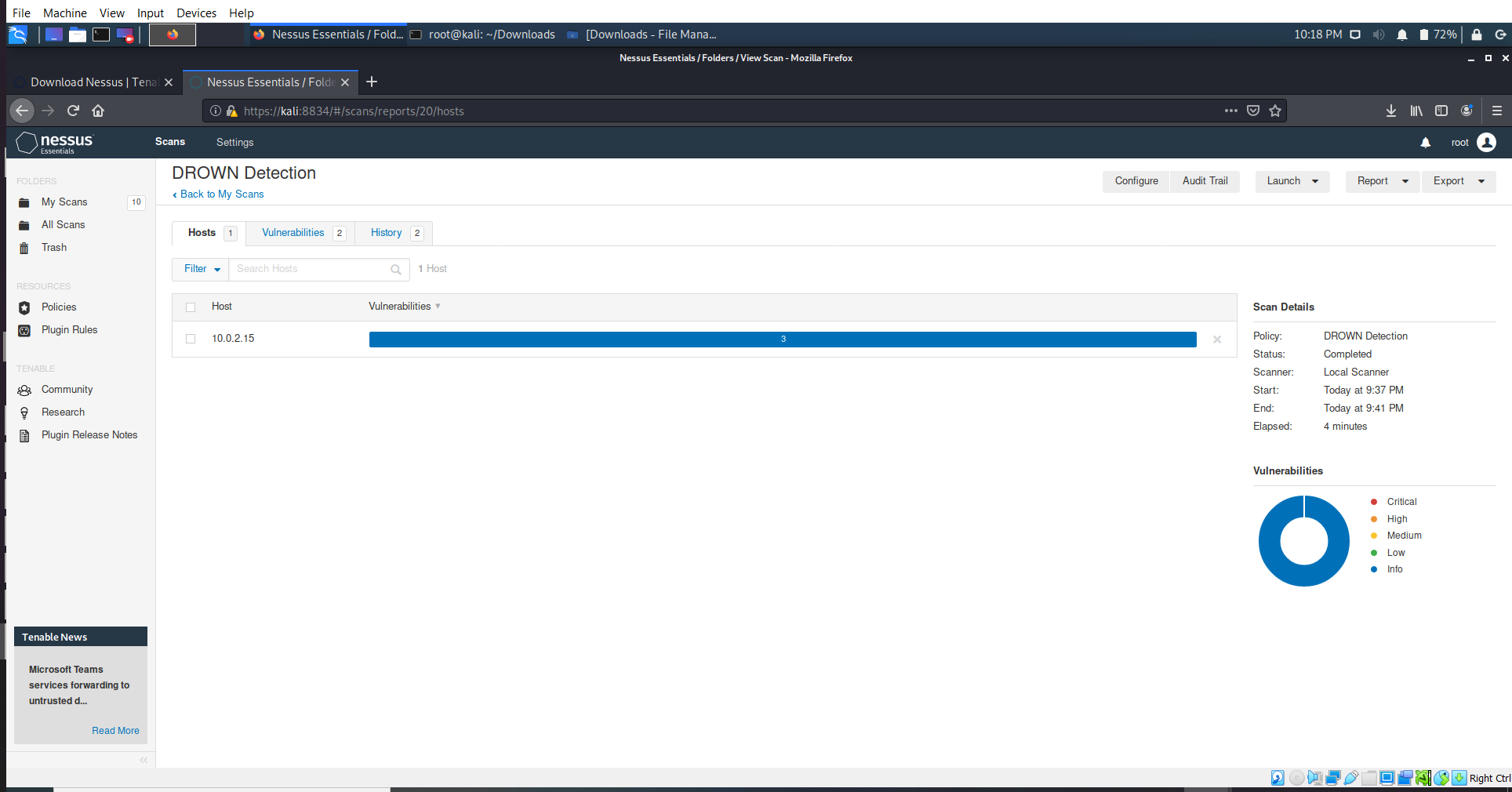


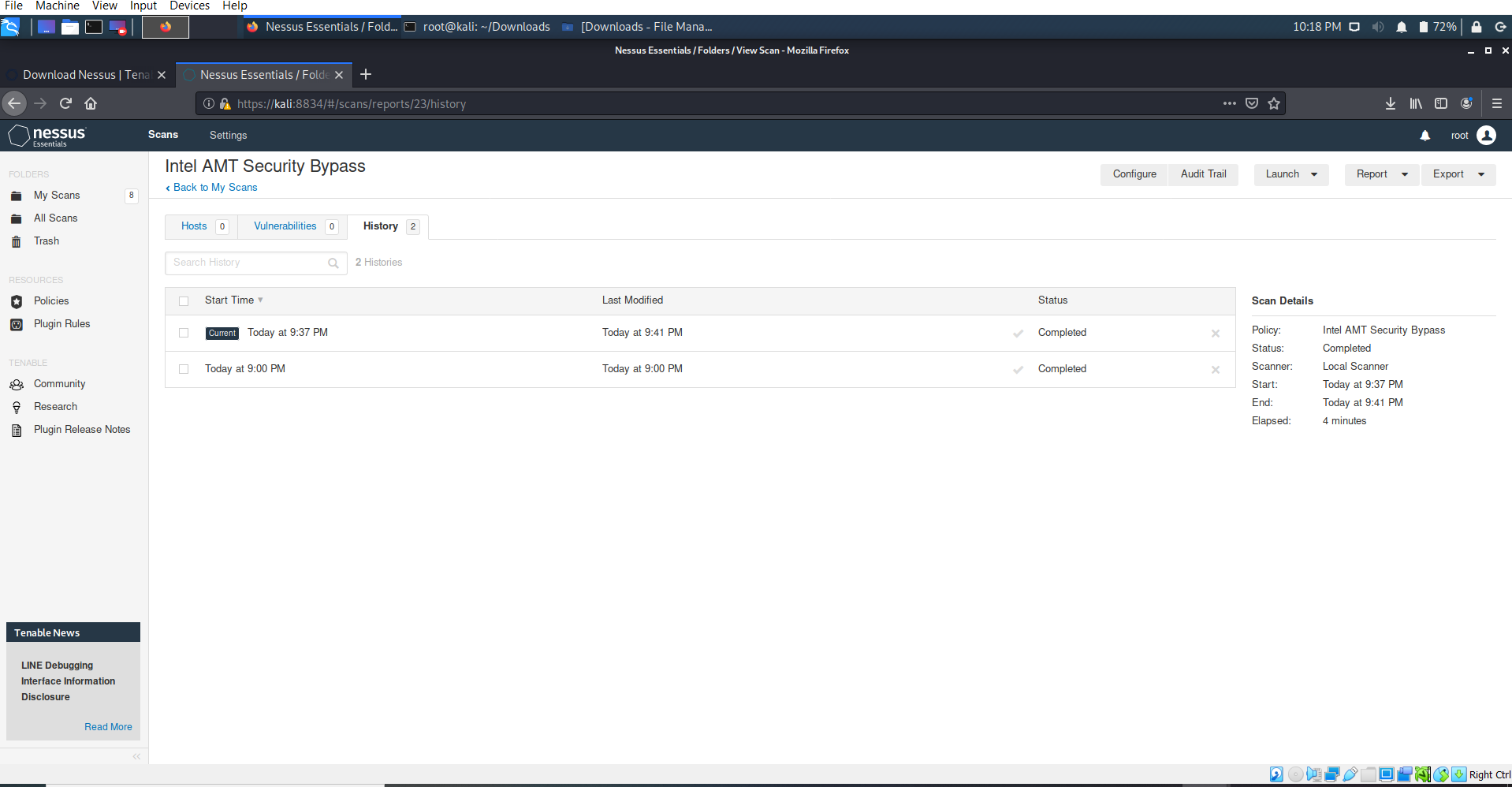


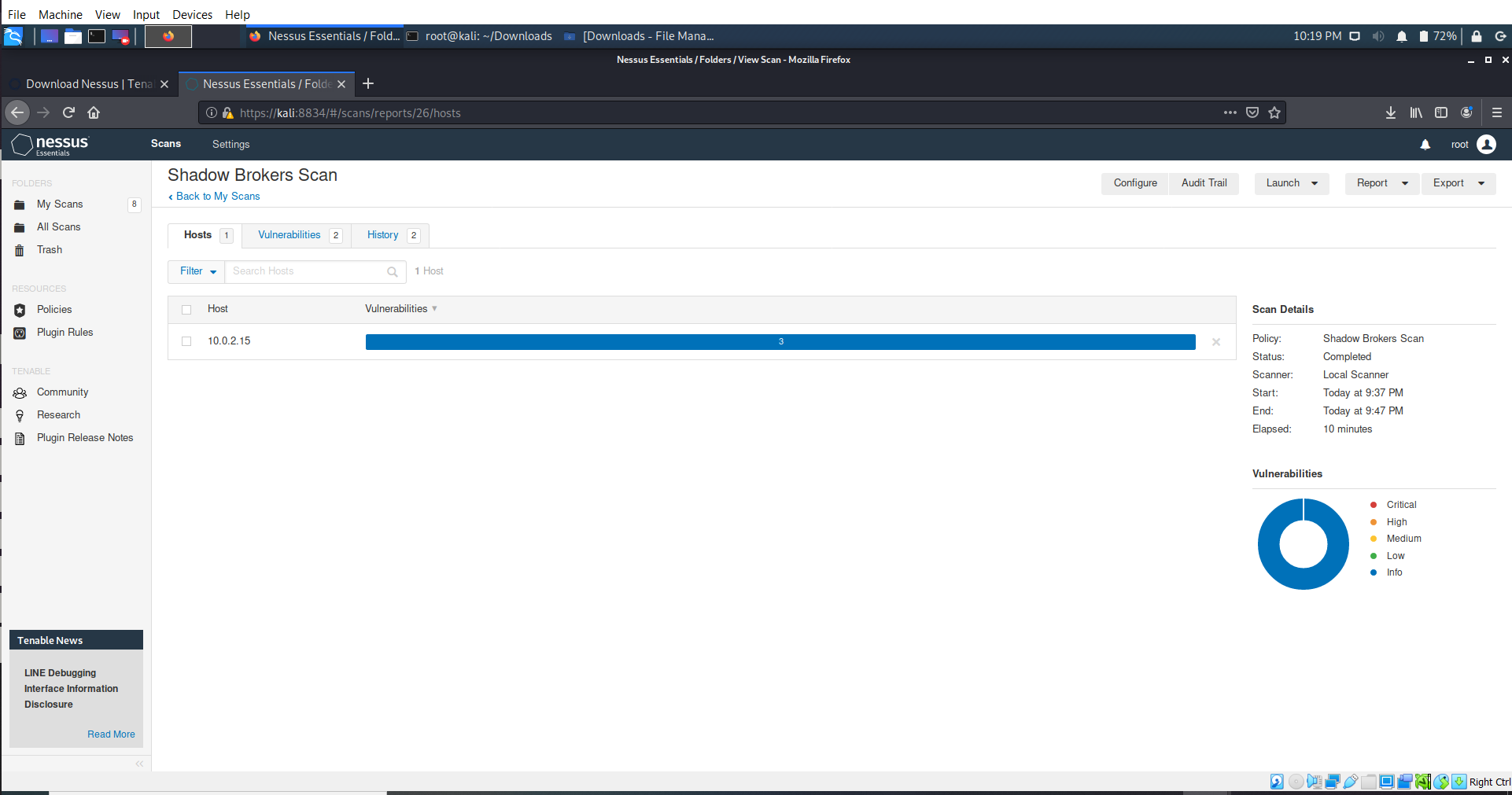


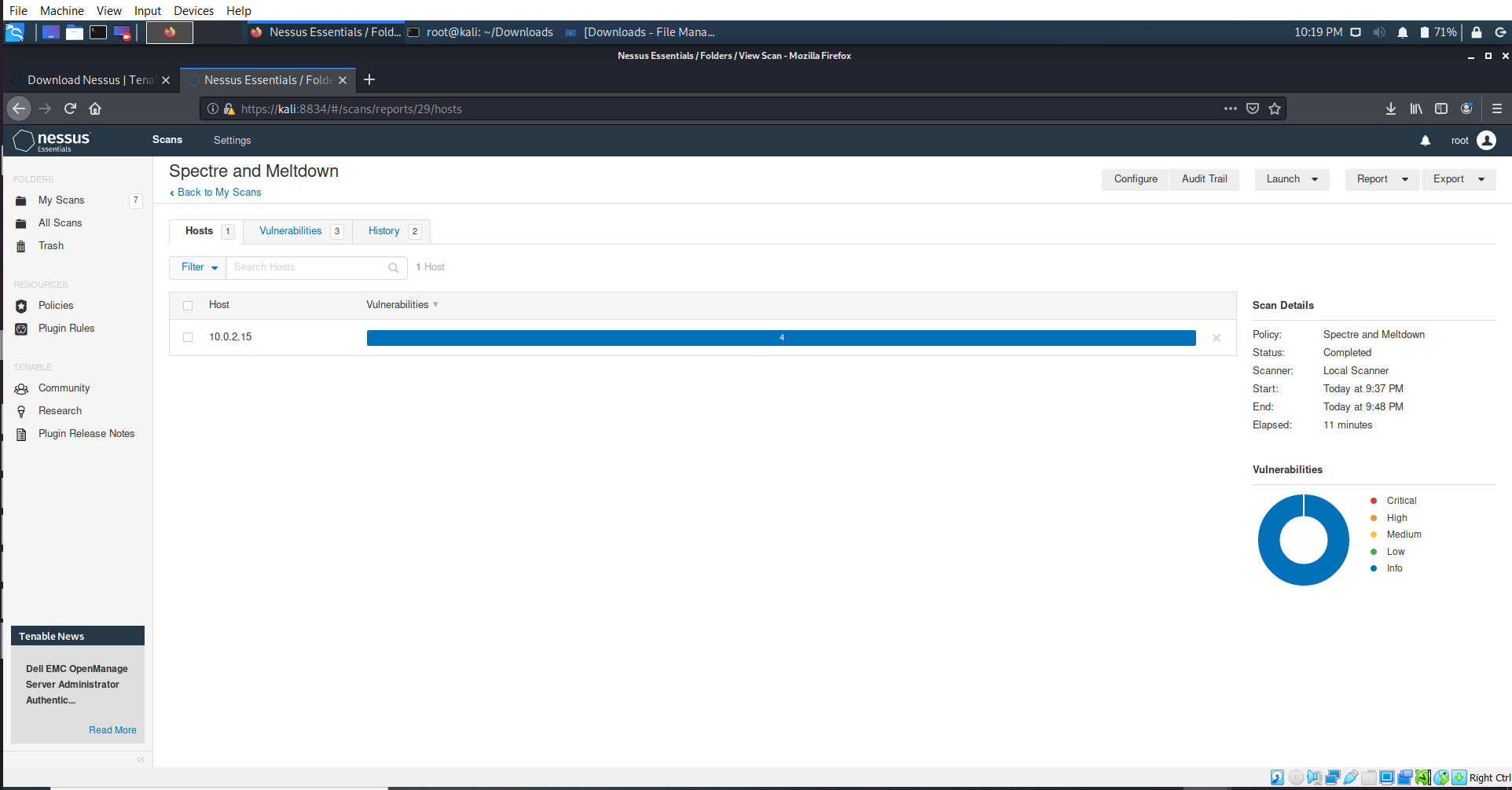


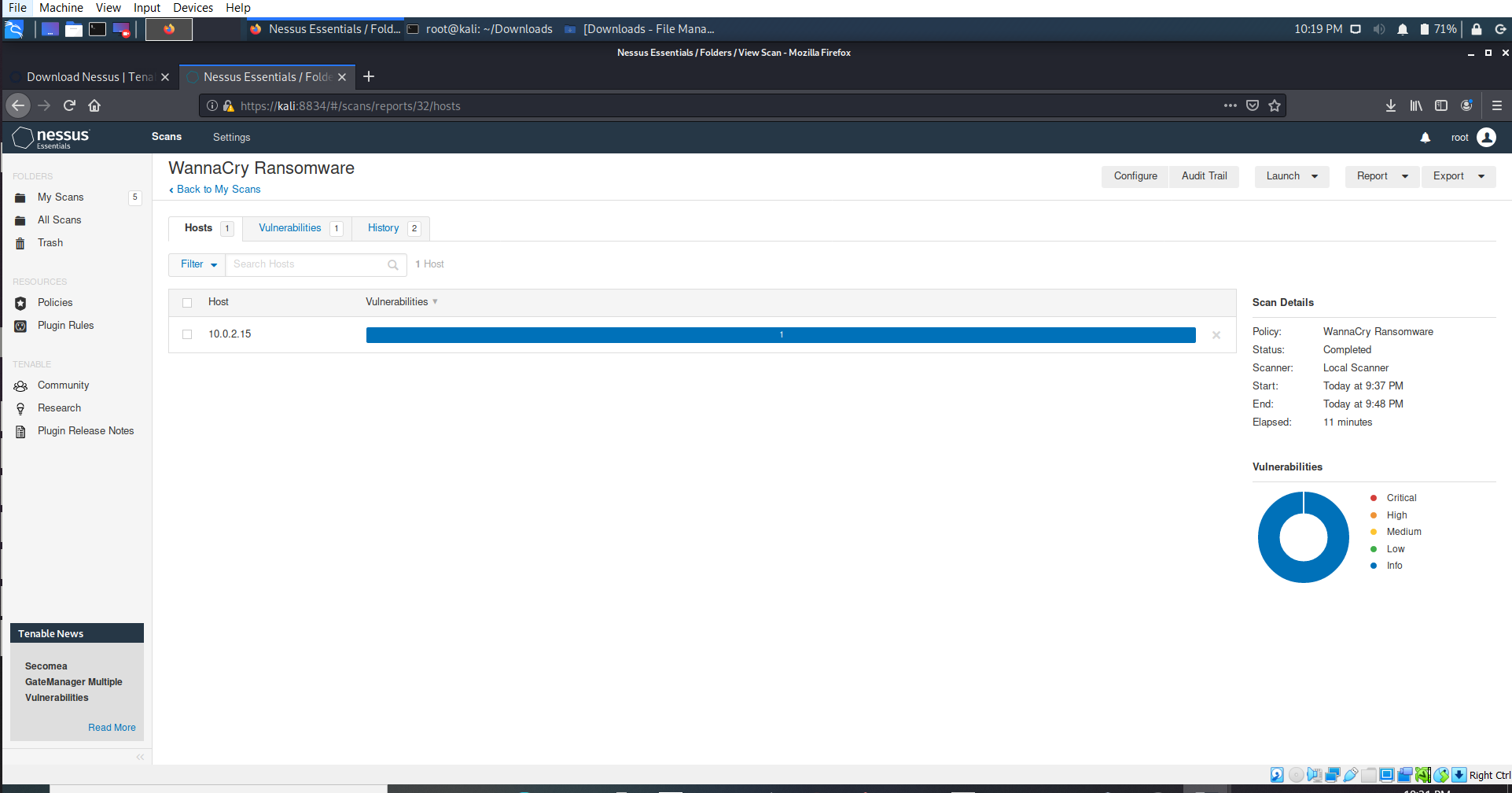


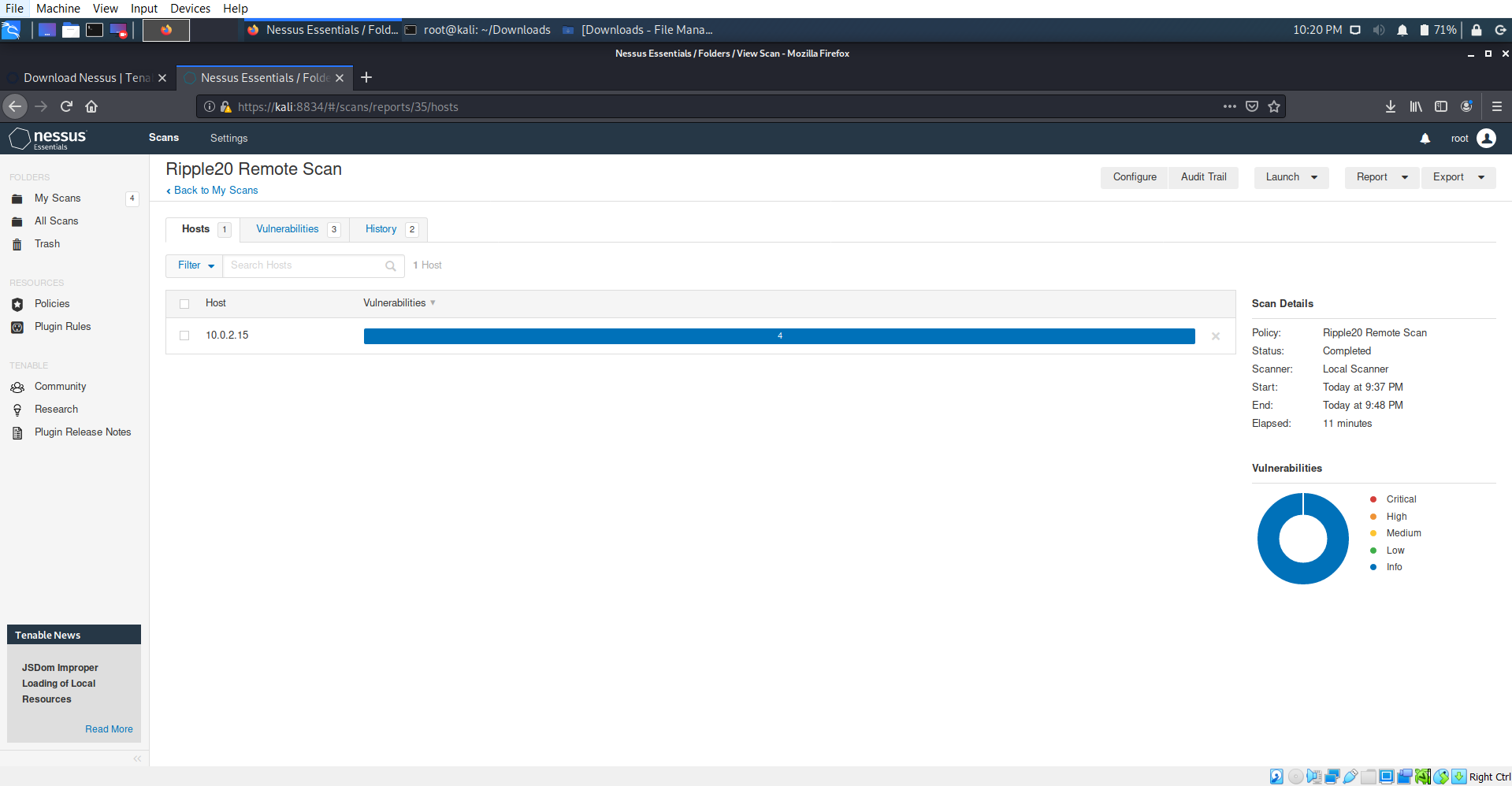


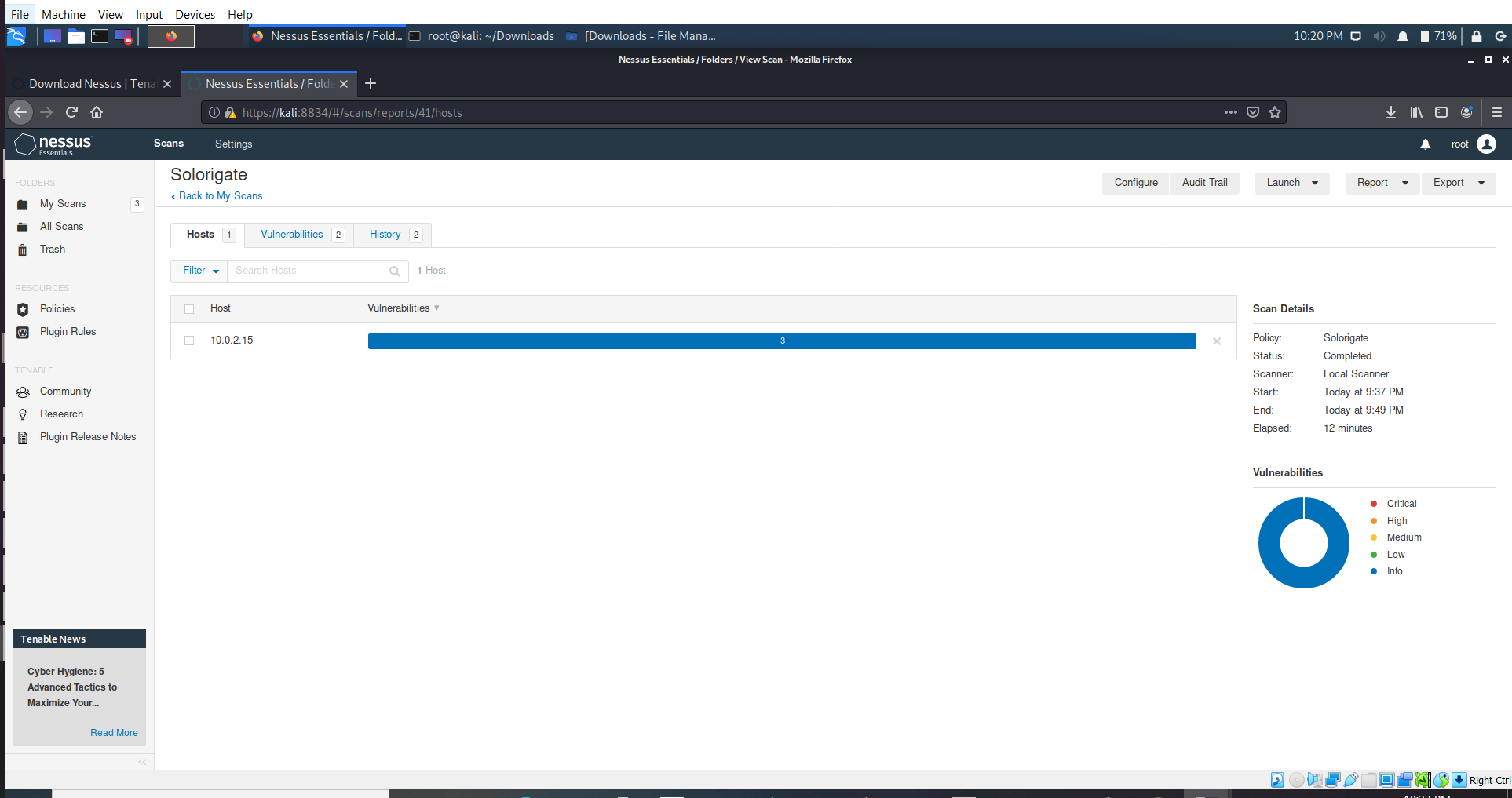


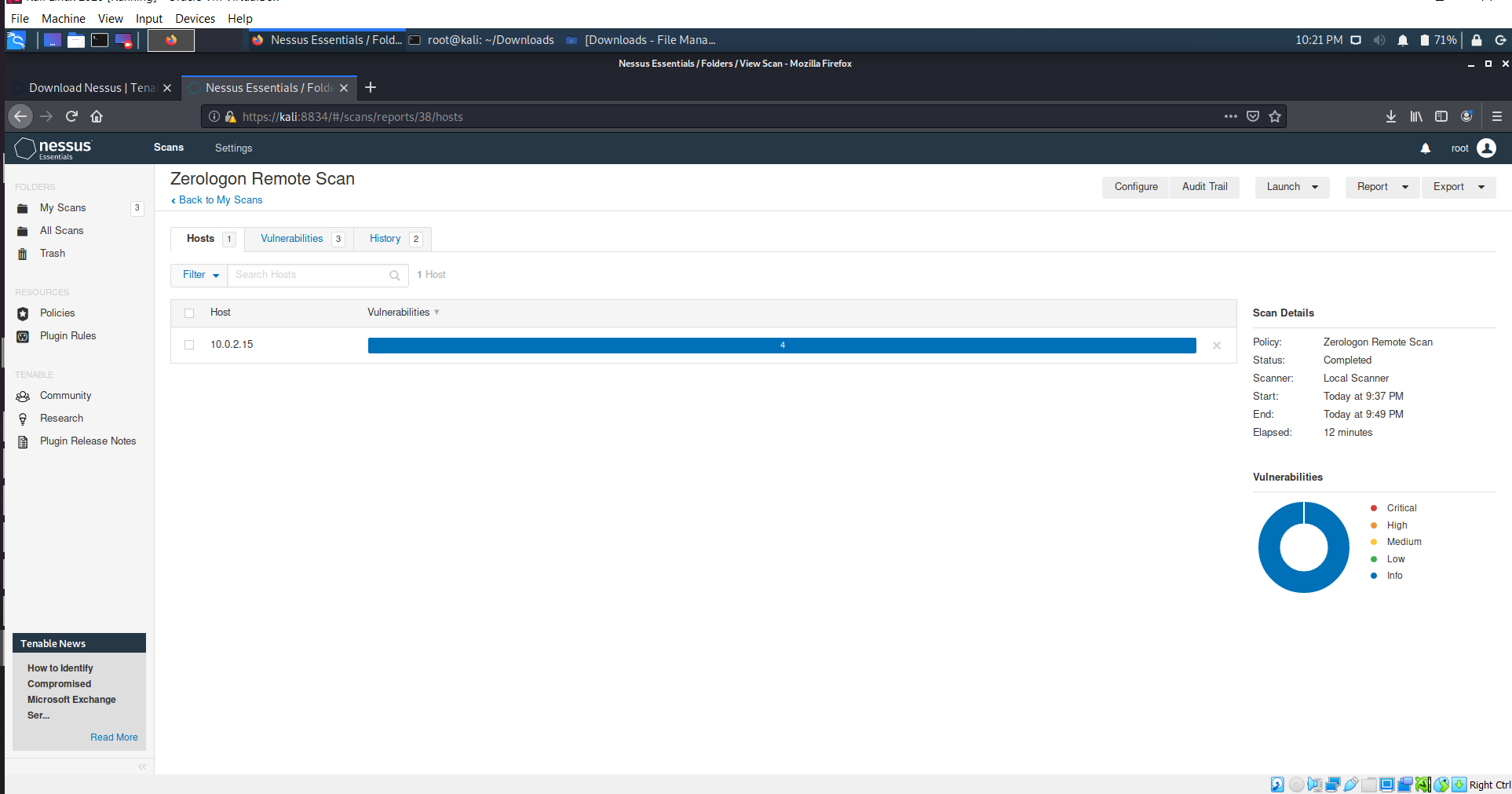


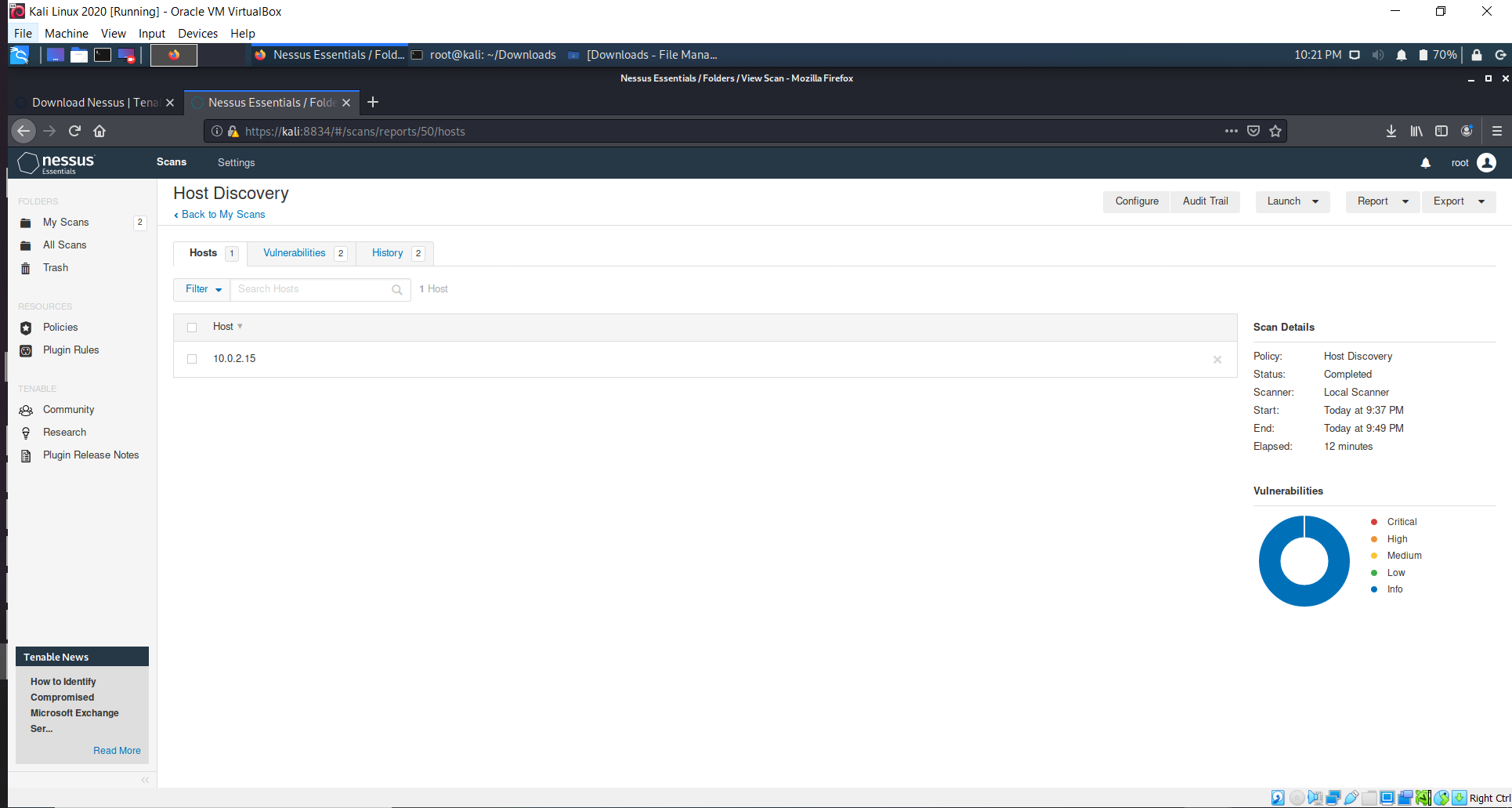


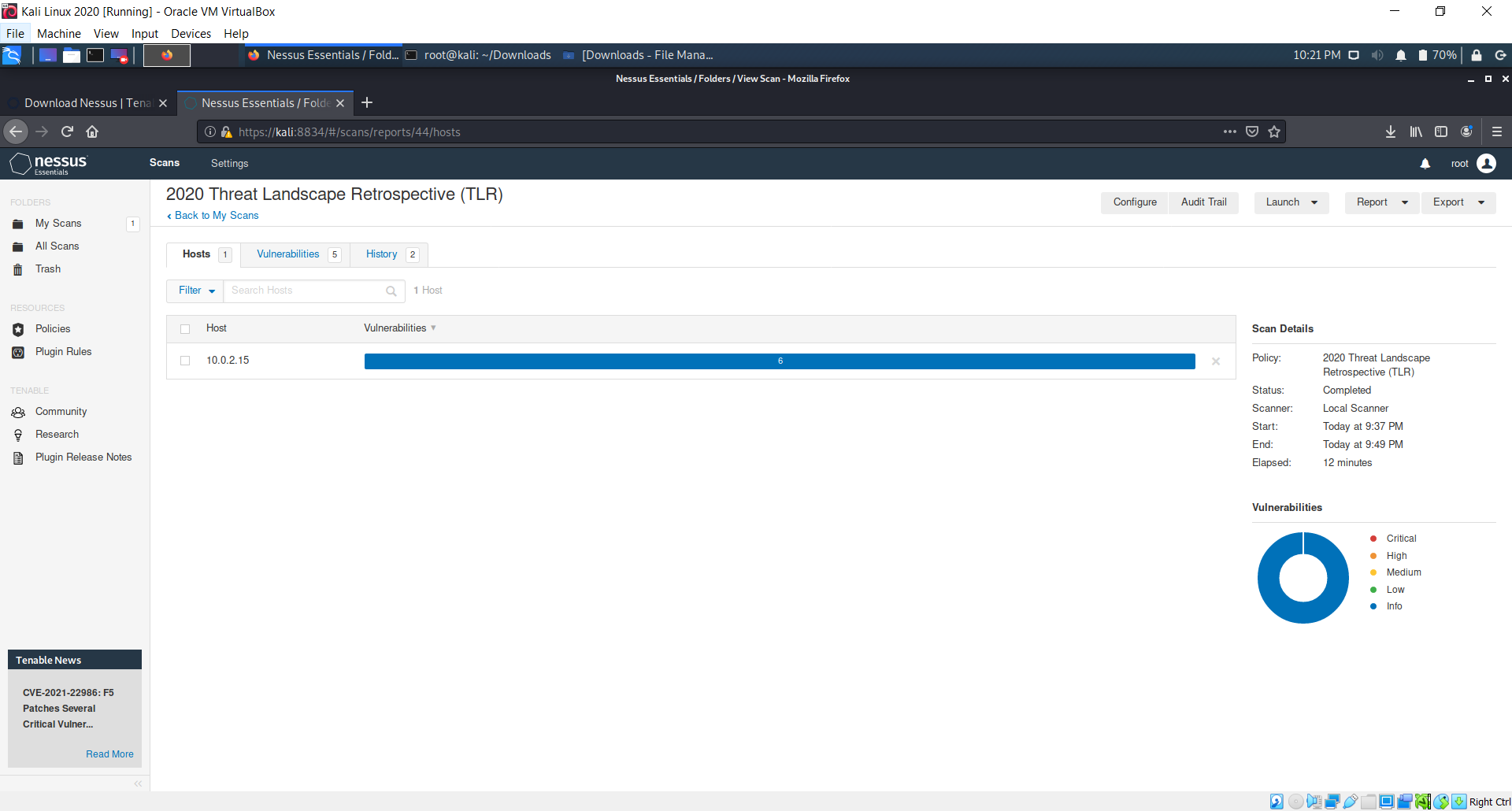












**Progress Embedded Image of Progress Report from LabSim:**

