Fundamentals of Information Security: Cybersecurity (88252)

Ana Herrera Flores'

Security Lab 4 - Nessus Scanning

Scan Types in Nessus and what they do:

Basic Network Scan: provides additional information about the network before carrying out deeper scans.

Advanced Scan: it provides the user with the ability to customize the settings of the scan as well as a detailed scan.

Advanced Dynamic Scan: it includes new filters that match certain criteria, and it does this automatically.

Malware Scan: it identifies vulnerabilities that can be exploited by malware.

Mobile device scan: identify vulnerabilities for a mobile device but requires a Mobile Device Managment (MDM) system.

Credentialed Path Audit scan: uses credentials that were provided to log in to the target system.

Intel AMT security bypass scan: it ensures accurate detection of the Intel AMT ports.

Spectre and Meltdown scan: it identifies hardware vulnerabilities.

WannaCry Ransomware scan: offer templates to detect vulnerabilities related to WannaCry, SMBv1, MS17-010 patch and others.

Ripple20 Remote scan: it scans vulnerabilities related to the Treck TCP/IP software library.

Solorigate: it identifies vulnerabilities, especially those related to SolarWinds Solorigate.

2020 Threat Landscape Retrospective (TLR) scan: report that identifies trends in vulnerabilities, ransomware, and others during COVID-19 pandemic.

ProxyLogon: MS Exchange scan: analyzes if an exchange server is vulnerable to the ProxyLogon exploit.

Host Discovery scan: it identifies active hosts on a network and provides information about these hosts.

Audit Cloud Infrastructure scan: it analyzes cloud environments.

Internal PCI Network scan: it identifies and helps organizations to organize vulnerabilities related to PCI DSS compliance requirements.

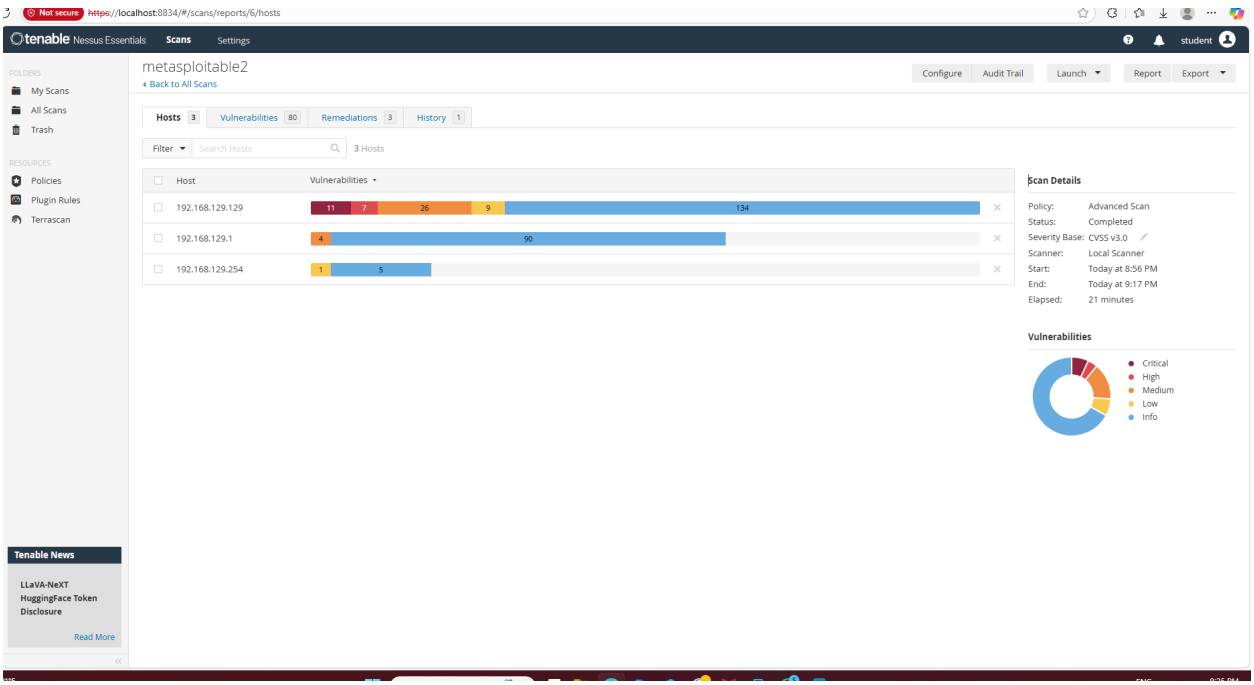
MDM Config Audit scan: detection and resolution of security configurations of MDM.

Offline Config Audit scan: it helps with the configuration of a system without internet connection.

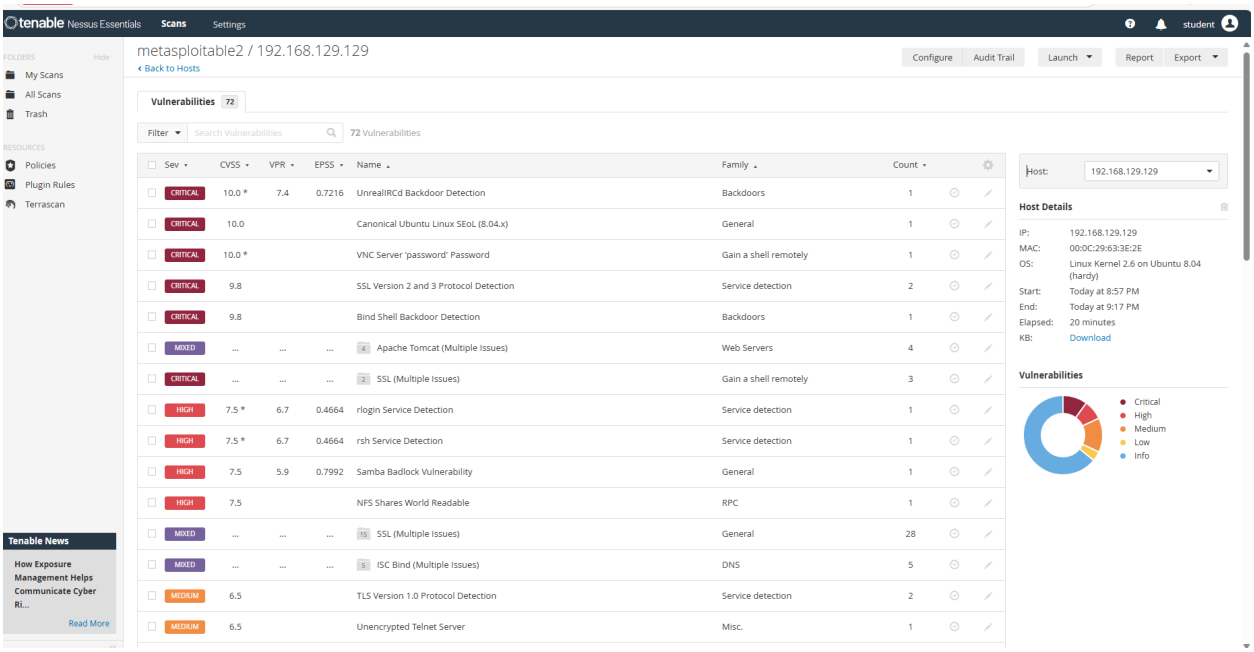
PCI Quarterly External scan: it is designed to assess and fulfil the requirements of the Payment Card Industry Data Security Standard (PCI DSS).

SCAP and OVAL Auditing scan: SCAP automates security policies and vulnerability management. OVAL is a language used in SCAP to know system states and vulnerabilities.

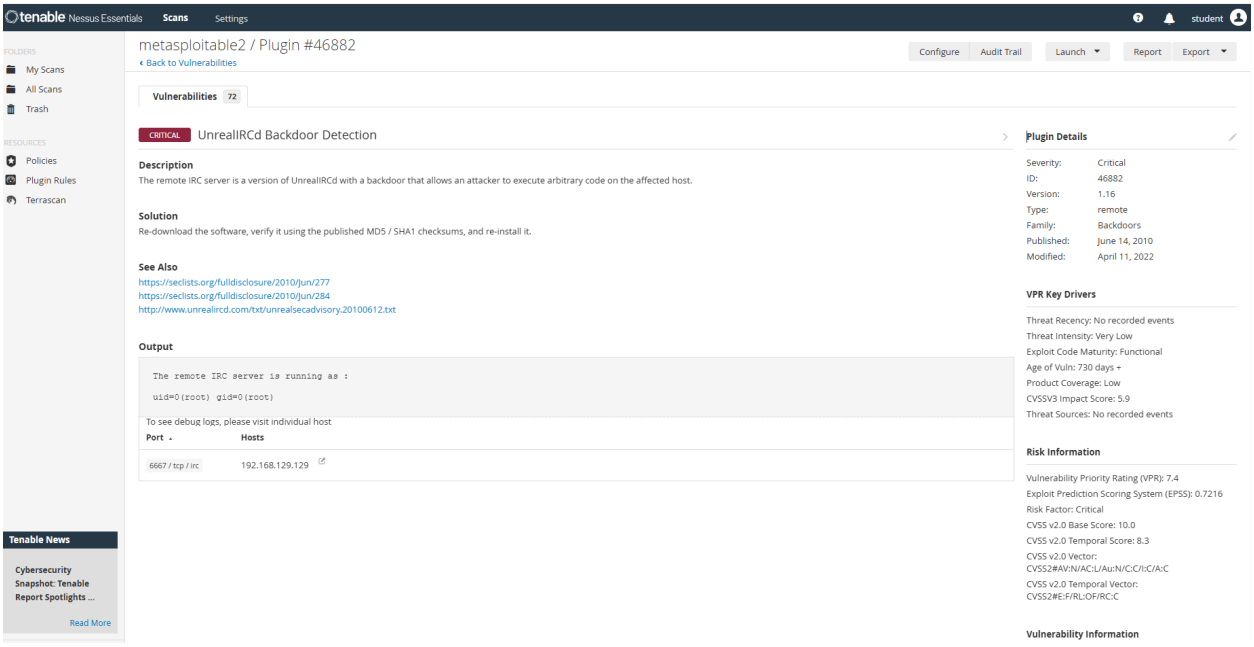
Scan MetaSploitable2:



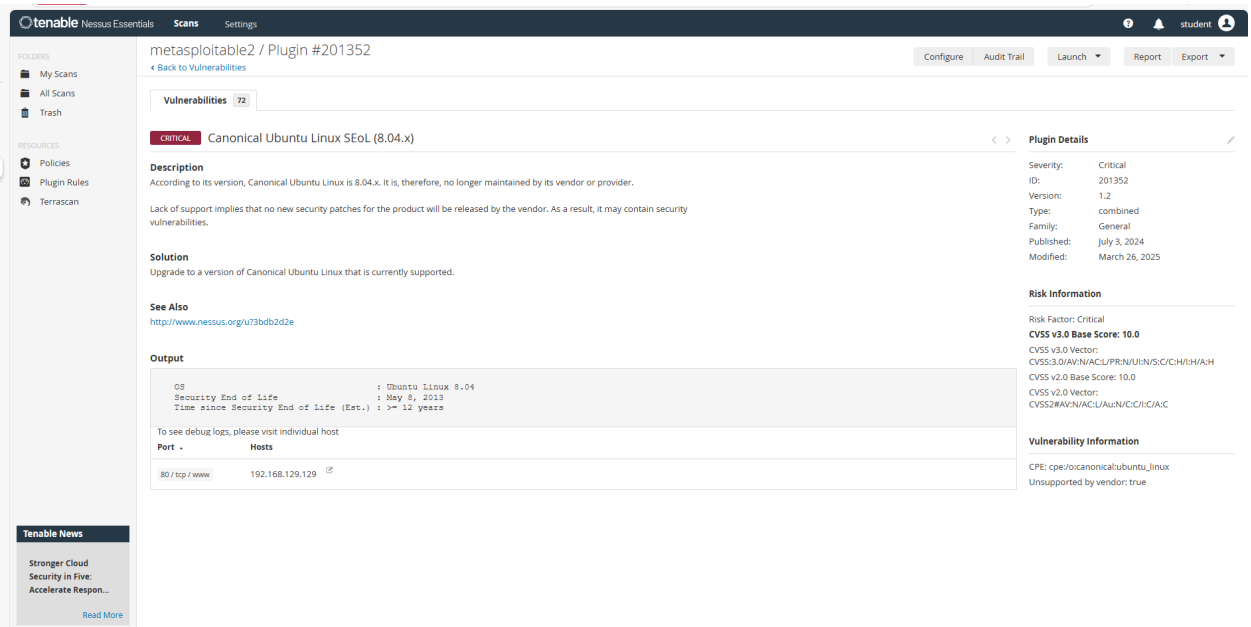
As we can see in this screenshot, this is how the main dashboard looks with the scanning of MetaSploitable2. IP: 192.168.129.129



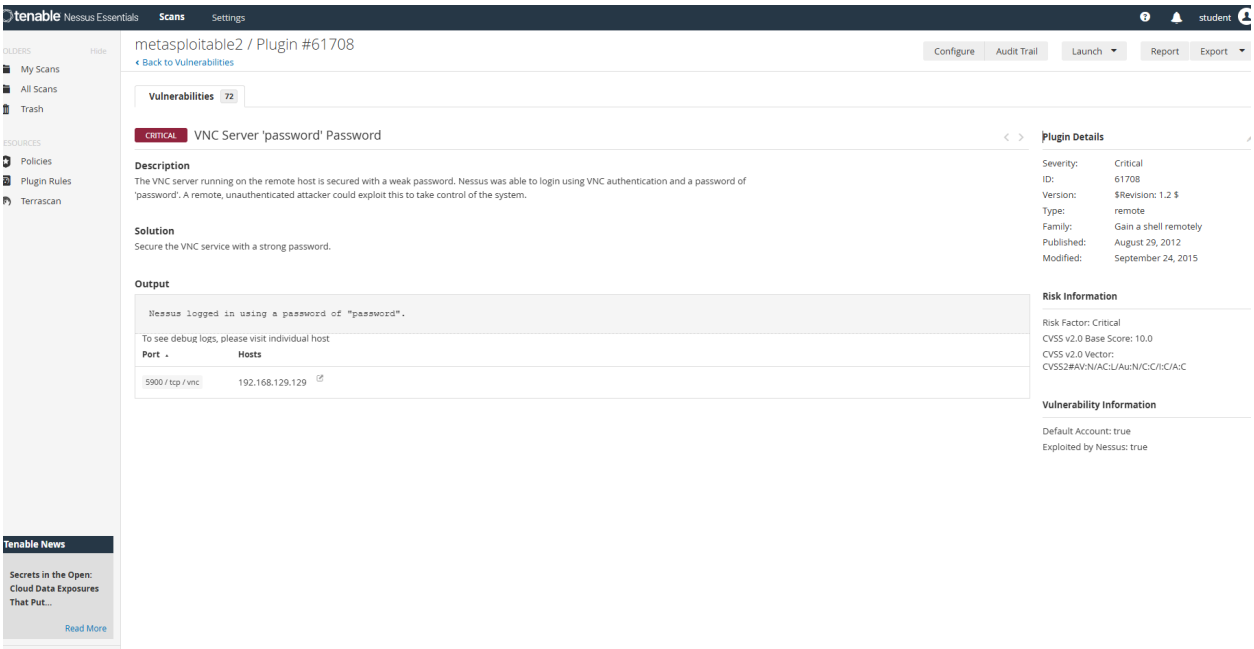
This second picture shows us in a little bit of detail the vulnerability scan.



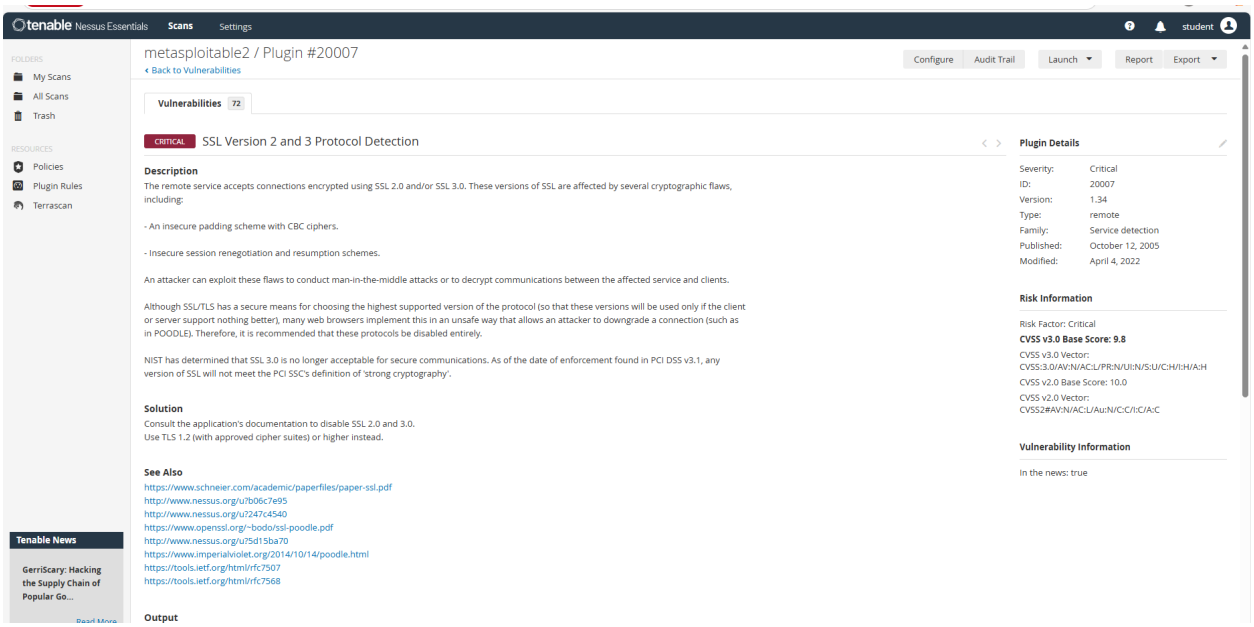
As we can see it is telling us that there is software that has an open backdoor that can allow a hacker to execute arbitrary code. The solution would be to re-download and re-install the software.



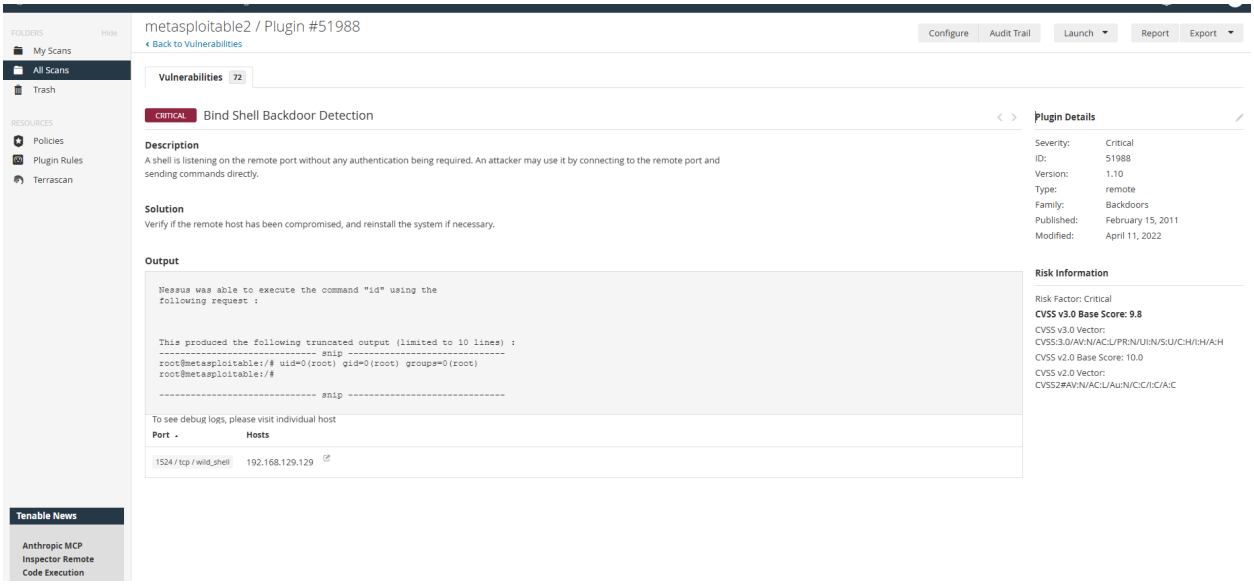
As we can see, the Canonical Ubuntu Linux version is not upgraded, so we no longer have the new security patches because this version is not maintained by the vendor. The solution will be to upgrade to a version that is currently supported.



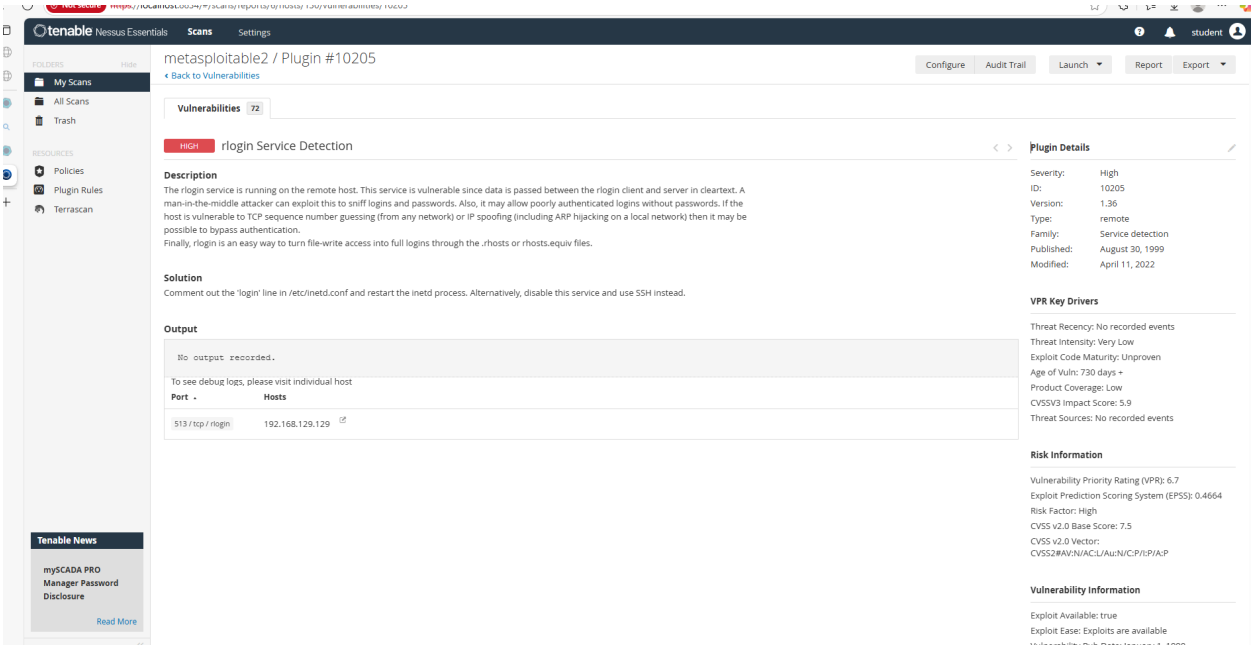
The VNC Server has a password of password which is weak, a hacker could exploit this vulnerability and take over the system. The solution is to set a stronger password.



Use of SSL Version 2 and 3 Protocol which is no longer considered secure. The solution is to disable these versions and use TLS 1.2.



A shell is open on a remote port without authentication; an attacker can use this and send commands. Verify if the host hasn't been compromised and reinstall the system.



We can see that the rlogin service is functioning in a remote host and data running between client and server can be exploited by a hacker. It also might be possible to login to the system without a password. The solution is to run the command ”login” and restart the process .