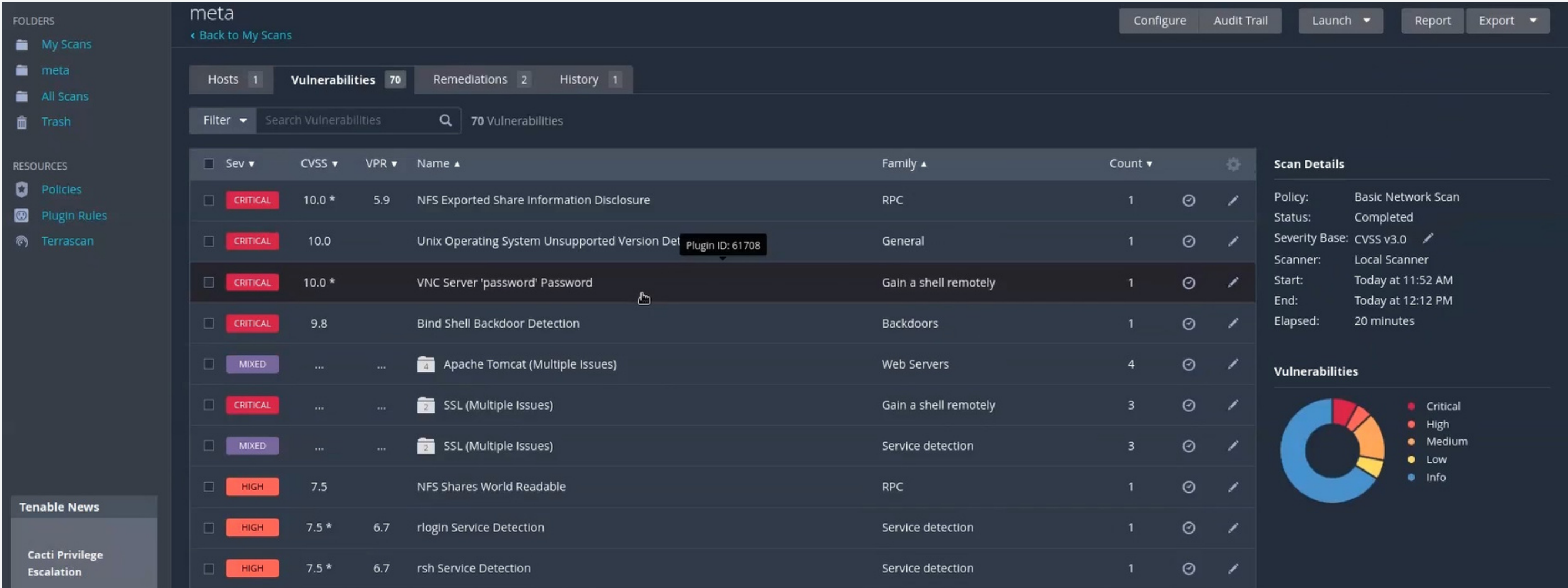





**S5L4**

# Una volta aperto Nessus e collegato a Metasploite abbiamo verificato le varie vulnerabilità



# Tra le vulnerabilità troviamo una Backdoor

Tenable

Nessus Essentials

Scans

Settings

?

🔔

Eindr...

FOLDERS

- My Scans
- meta
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Terrascan

meta / Plugin #51988

[Back to Vulnerabilities](#)

Configure

Audit Trail

Launch

Report

Export

Hosts1

Vulnerabilities70

Remediations2

History1

CRITICAL

Bind Shell Backdoor Detection

<>

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Output

Nessus was able to execute the command "id" using the following request :

This produced the following truncated output (limited to 10 lines) :

----- snip -----

root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)

root@metasploitable:/#

----- snip -----

To see debug logs, please visit individual host

Plugin Details

Severity:Critical

ID:51988

Version:1.10

Type:remote

Family:Backdoors

Published:February 15, 2011

Modified:April 11, 2022

Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score 9.8

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:/I:C/A:C