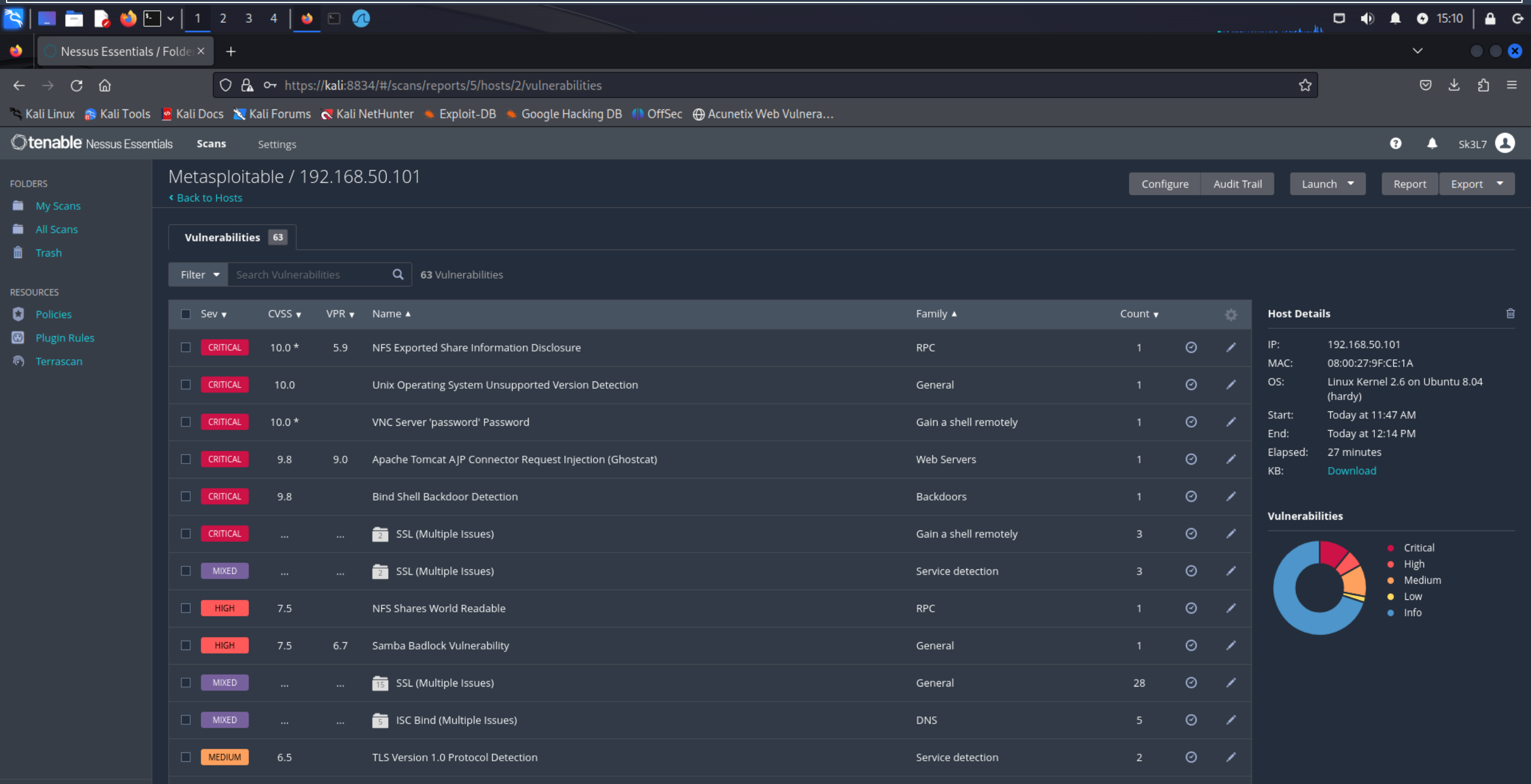
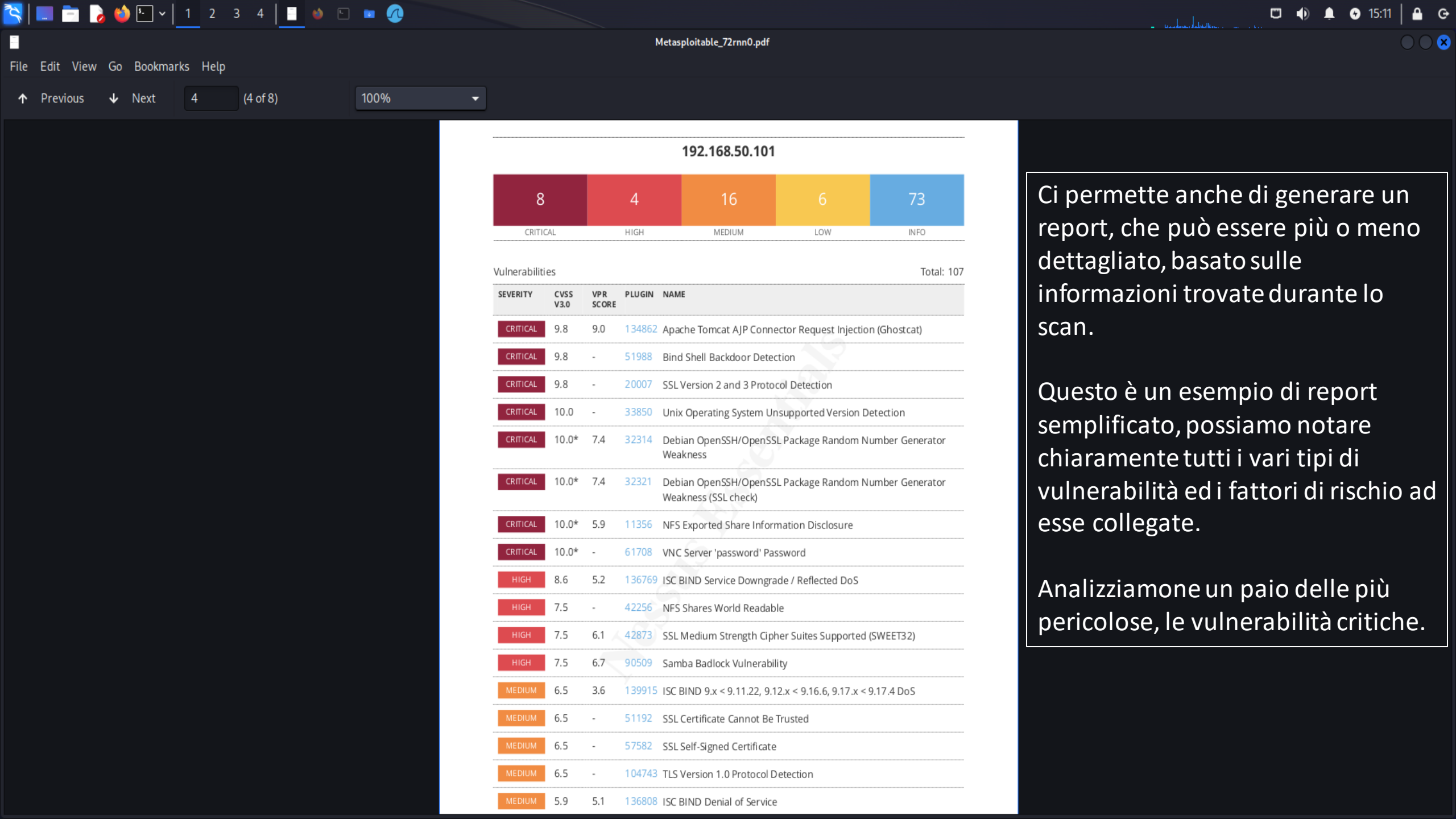
In questo esercizio, andremo a fare pratica con Nessus, un vulnerability scanner molto utile e molto potente.
Come vulnerability scanner, ci permette di visualizzare i rischi e le vulnerabilità della rete che stiamo scansionando (delle "informazioni).

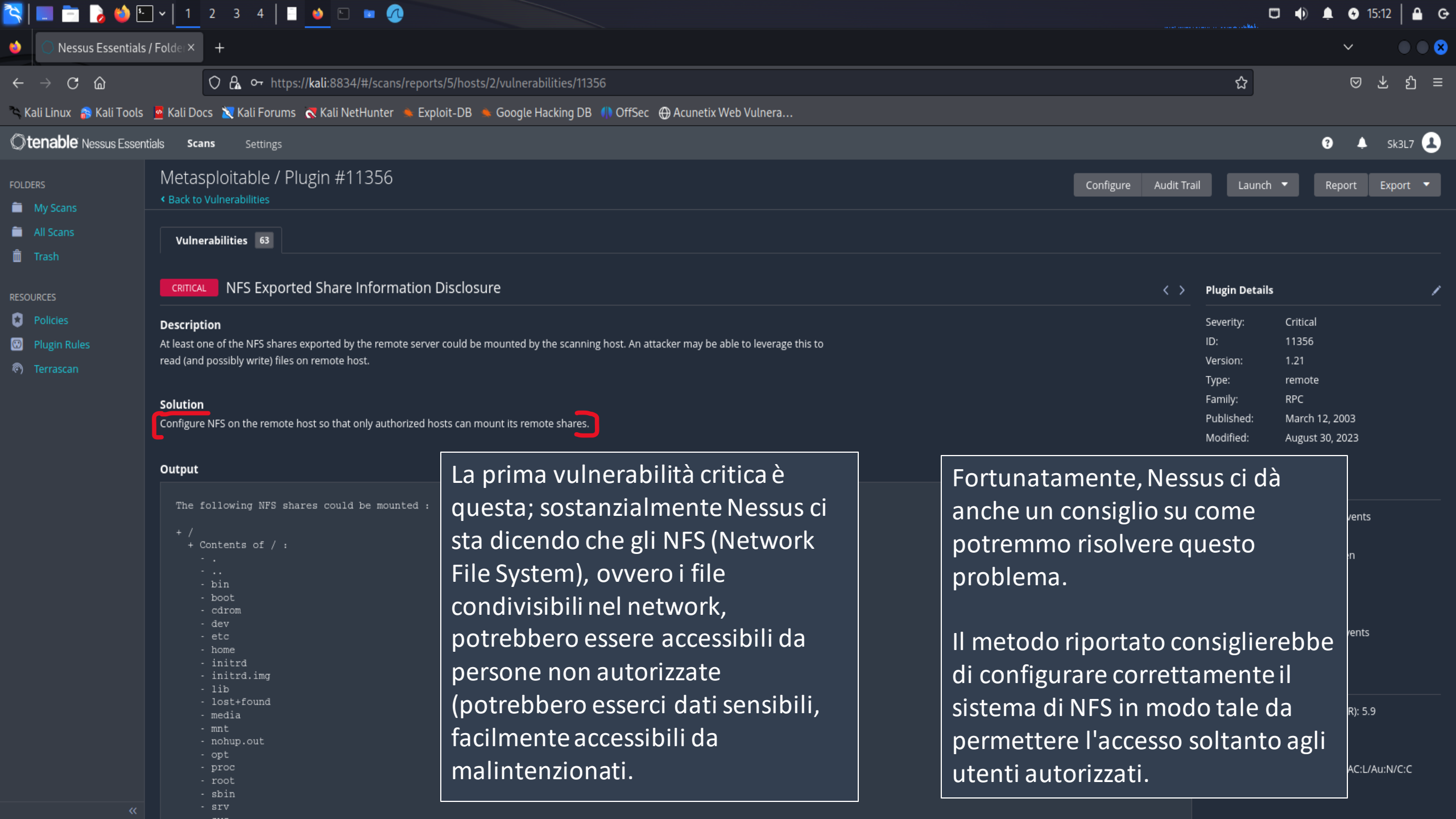




Ci permette anche di generare un report, che può essere più o meno dettagliato, basato sulle informazioni trovate durante lo scan.

Questo è un esempio di report semplificato, possiamo notare chiaramente tutti i vari tipi di vulnerabilità ed i fattori di rischio ad esse collegate.

Analizziamone un paio delle più pericolose, le vulnerabilità critiche.



La prima vulnerabilità critica è questa; sostanzialmente Nessus ci sta dicendo che gli NFS (Network File System), ovvero i file condivisibili nel network, potrebbero essere accessibili da persone non autorizzate (potrebbero esserci dati sensibili, facilmente accessibili da malintenzionati.

Fortunatamente, Nessus ci dà anche un consiglio su come potremmo risolvere questo problema.

Il metodo riportato consiglierebbe di configurare correttamente il sistema di NFS in modo tale da permettere l'accesso soltanto agli utenti autorizzati.

Nessus Essentials / Folde

https://kali:8834/#/scans/reports/5/hosts/2/vulnerabilities/33850

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec | Acunetix Web Vulnera...

tenable Nessus Essentials | Scans | Settings | Sk3L7

FOLDERS
- My Scans
- All Scans
- Trash

RESOURCES
- Policies
- Plugin Rules
- Terrascan

Metasploitable / Plugin #33850

‹ Back to Vulnerabilities

Configure | Audit Trail | Launch | Report | Export

Vulnerabilities 63

CRITICAL Unix Operating System Unsupported Version Detection

Description

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution

Upgrade to a version of the Unix operating system that is currently supported.

Output

```
Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09 (Server).
Upgrade to Ubuntu 23.04 / LTS 22.04 / LTS 20.04 .

For more information, see : https://wiki.ubuntu.com/Releases
```

To see debug logs, please visit individual host

Port ▲	Hosts
N/A	192.168.50.101

Plugin Details

Severity:	Critical
ID:	33850
Version:	1.289
Type:	combined
Family:	General
Published:	August 8, 2008
Modified:	October 18, 2023

Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score 10.0

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

Vulnerability Information

Unsupported by vendor: true

Reference Information

IAVA: 0001-A-0502, 0001-A-0648

Qui abbiamo un altro esempio, in questo caso la versione di Unix (il sistema operativo di Metasploitable è una variante, vulnerabile, di Linux, alla fin fine) è troppo datata, probabilmente obsoleta.
La soluzione secondo Nessus, sarebbe sicuramente di aggiornare ad una versione dell'OS più aggiornata.

Aggiornare i sistemi operativi infatti, può spesso aiutare a risolvere vulnerabilità delle versioni precedenti.

Nessus Essentials / Folde

https://kali:8834/#/scans/reports/5/hosts/2/vulnerabilities/61708

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec | Acunetix Web Vulnera...

tenable Nessus Essentials | Scans | Settings | Sk3L7

FOLDERS
- My Scans
- All Scans
- Trash

RESOURCES
- Policies
- Plugin Rules
- Terrascan

Metasploitable / Plugin #61708

‹ Back to Vulnerabilities

Configure | Audit Trail | Launch | Report | Export

Vulnerabilities 63

CRITICAL VNC Server 'password' Password

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

Output

```
Nessus logged in using a password of "password".
```

To see debug logs, please visit individual host

Port ▲	Hosts
5900 / tcp / vnc	192.168.50.101

Plugin Details

Severity:	Critical
ID:	61708
Version:	$Revision: 1.2 $
Type:	remote
Family:	Gain a shell remotely
Published:	August 29, 2012
Modified:	September 24, 2015

Risk Information

Risk Factor: Critical

CVSS v2.0 Base Score: 10.0

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

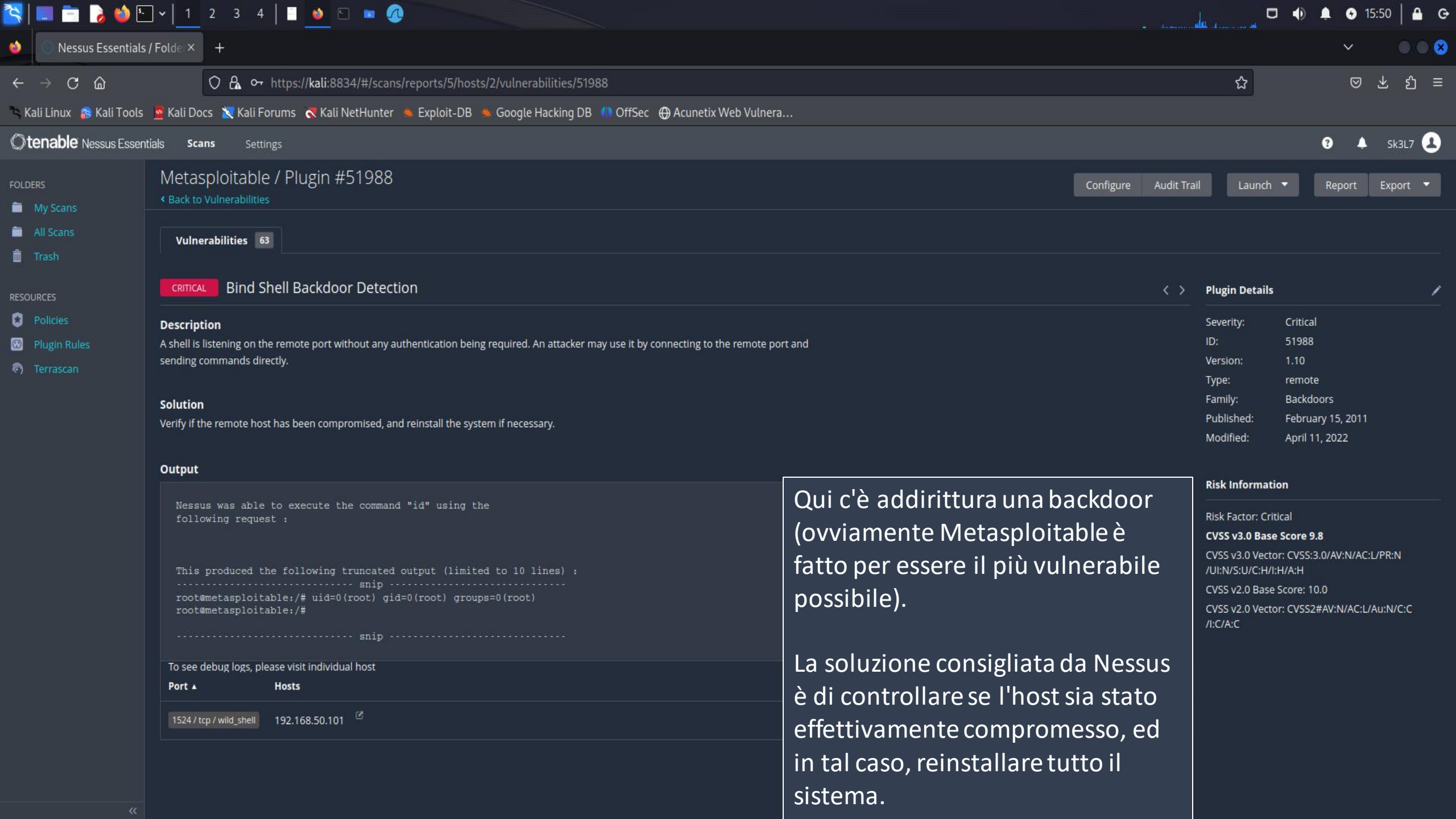
Vulnerability Information

Default Account: true

Exploited by Nessus: true

In quest'altro caso invece, il problema sembra essere riguardante il server VNC (Virtual Network Computing). Ovvero le credenziali utilizzate per accedervi sono molto scarse, Nessus è riuscito ad accedervi utilizzando semplicemente "password".

Di logica, dunque, la soluzione sarebbe di utilizzare delle credenziali migliori e più forti, più complesse.



Qui c'è addirittura una backdoor (ovviamente Metasploitable è fatto per essere il più vulnerabile possibile).

La soluzione consigliata da Nessus è di controllare se l'host sia stato effettivamente compromesso, ed in tal caso, reinstallare tutto il sistema.