Università degli Studi di Salerno

Dipartimento di Informatica

Penetration Testing & Ethical Hacking

Vulnerability Mapping
Parte 3

Arcangelo Castiglione
arcastiglione@unisa.it

Outline

- Concetti Preliminari
- Caratterizzazione delle Vulnerabilità
- Tassonomia delle Vulnerabilità
- Analisi Manuale delle Vulnerabilità
- **Analisi Automatizzata delle Vulnerabilità**
- Analisi delle Vulnerabilità nelle Applicazioni Web
- Analisi delle Vulnerabilità nei Database

Analisi Automatica delle Vulnerabilità

- **Osservazione:** Un processo di **penetration testing** deve essere tipicamente condotto in una **quantità di tempo limitata**

- Gli **strumenti** per la **rilevazione automatica delle vulnerabilità** possono risultare determinanti per condurre tale processo entro i tempi prestabiliti
  - Permettendo di ottenere in poco tempo una grande quantità di informazioni sull'asset in esame

- Tali strumenti consentono di condurre su determinato asset, in maniera del tutto automatica, le seguenti fasi di un tipico processo di penetration testing
  - *Target Discovery*
  - *Target Enumeration*
  - *Vulnerability Mapping*

Analisi Automatica delle Vulnerabilità

- Due tra i principali strumenti per la scansione automatizzata delle vulnerabilità (*Scanner*) sono

Analisi Automatica delle Vulnerabilità

Nessus

- Software proprietario (anche se nato Open Source)
  - Prodotto dall'azienda *Tenable Inc.*

- Strumento estremamente potente per l'analisi automatica delle vulnerabilità

Analisi Automatica delle Vulnerabilità
Nessus

- Consente di identificare e correggere, in maniera facile e veloce, vulnerabilità su una vasta gamma di Sistemi Operativi, dispositivi ed applicazioni

- Si occupa di rilevare
  - Difetti del software
  - Patch mancanti
  - Malware
  - Configurazioni errate
  - Etc

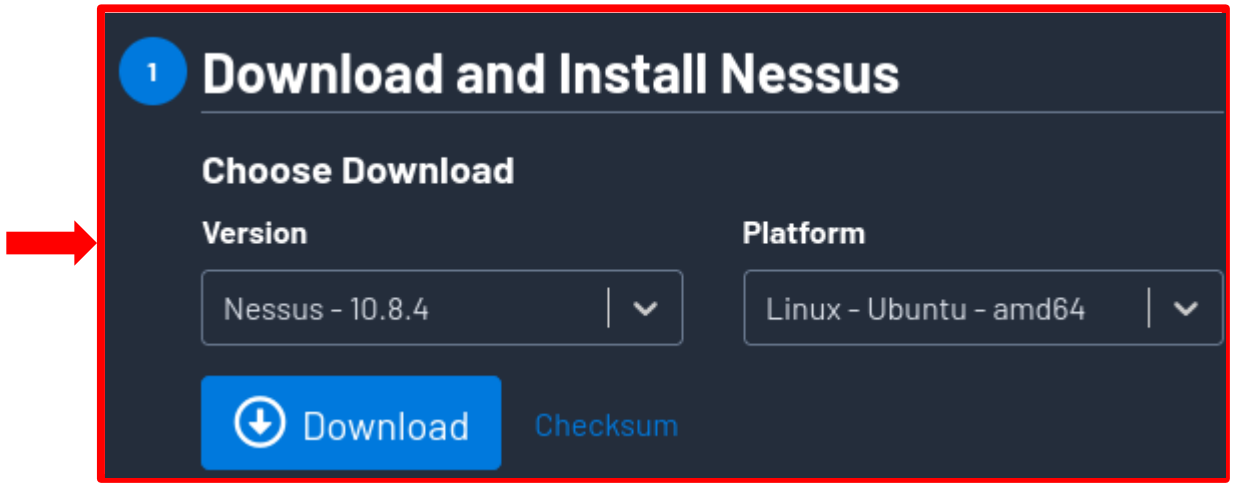
Analisi Automatica delle Vulnerabilità
Nessus

- Nessus non è installato di default in Kali Linux

- Utilizzeremo la versione *Essentials* di Nessus
  - Liberamente scaricabile, anche se la sua attivazione richiede una registrazione
  - Fornisce un sottoinsieme limitato delle funzionalità offerte dalla versione *Pro*, ad esempio
    - Permette di effettuare scansioni su un massimo di 16 indirizzi IP
    - Fornisce accesso assai limitato al supporto (*Help*)
    - Etc

Analisi Automatica delle Vulnerabilità
Nessus – Download

- https://www.tenable.com/downloads/nessus



Analisi Automatica delle Vulnerabilità

Nessus – Installazione

- Installiamo Nessus-10.8.4-ubuntu1604_amd64.deb
  - **dpkg -i Nessus-10.8.4-ubuntu1604_amd64.deb**

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# dpkg -i Nessus-10.8.4-ubuntu1604_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 416329 files and directories currently installed.)
Preparing to unpack Nessus-10.8.4-ubuntu1604_amd64.deb ...
Unpacking nessus (10.8.4) ...
Setting up nessus (10.8.4) ...
```

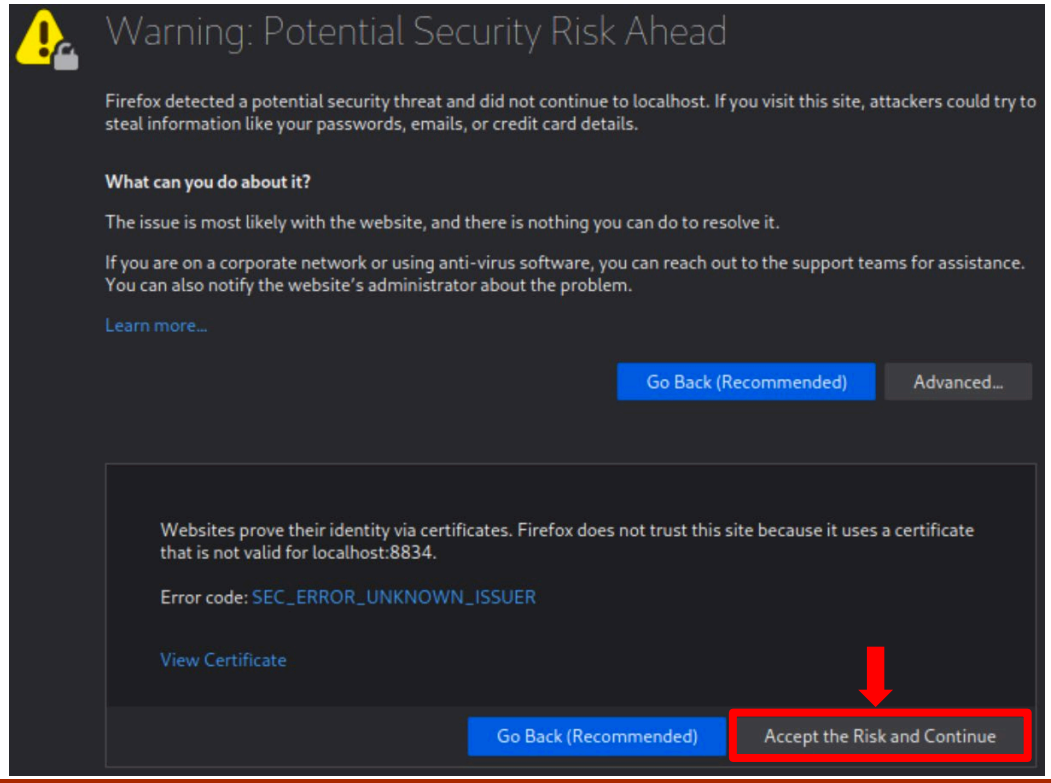
Analisi Automatica delle Vulnerabilità
Nessus – Avvio

- Una volta installato è possibile avviare Nessus
  - Da Terminale, tramite il comando
    - `/bin/systemctl start nessusd.service`

- Sarà necessario invocare tale comando ogni volta che si vorrà avviare Nessus

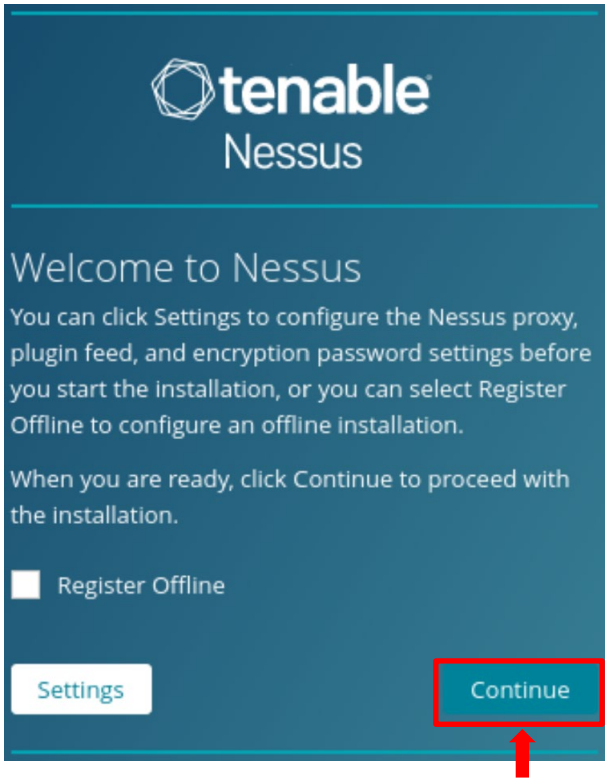
Analisi Automatica delle Vulnerabilità
Nessus – Avvio

- Accediamo a Nessus tramite un Web Browser
  - `https://localhost:8834`



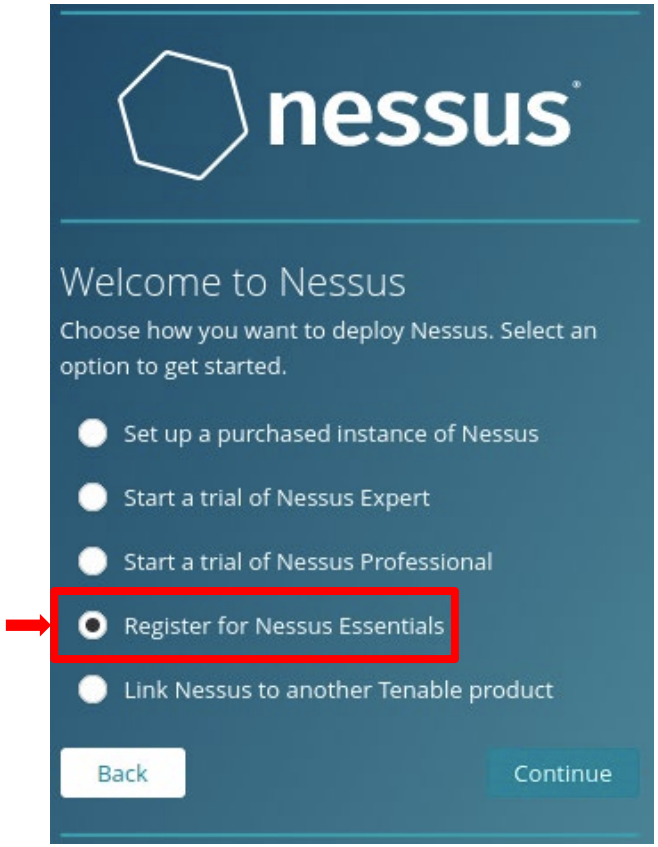
Analisi Automatica delle Vulnerabilità
Nessus – Avvio

- Registrazione ed attivazione



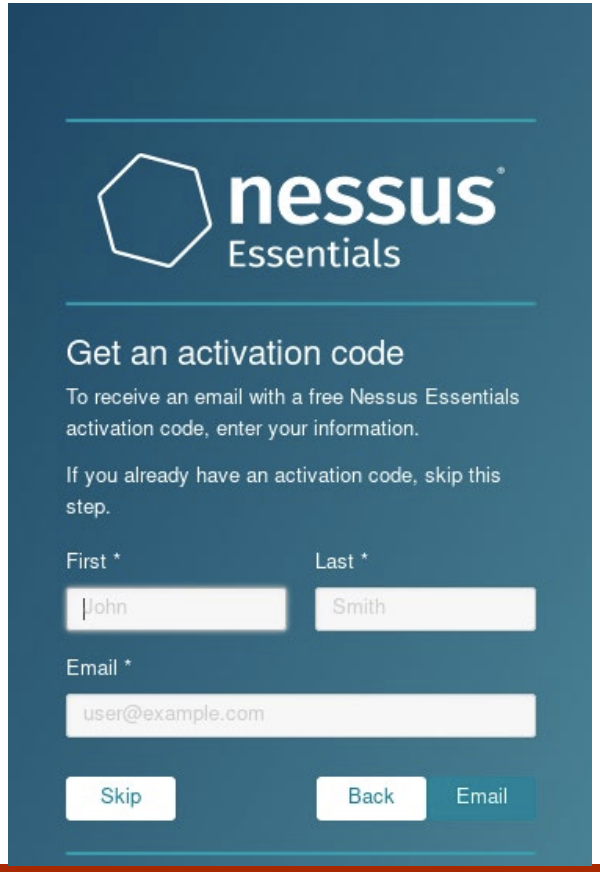
Analisi Automatica delle Vulnerabilità
Nessus – Avvio

- Registrazione ed attivazione



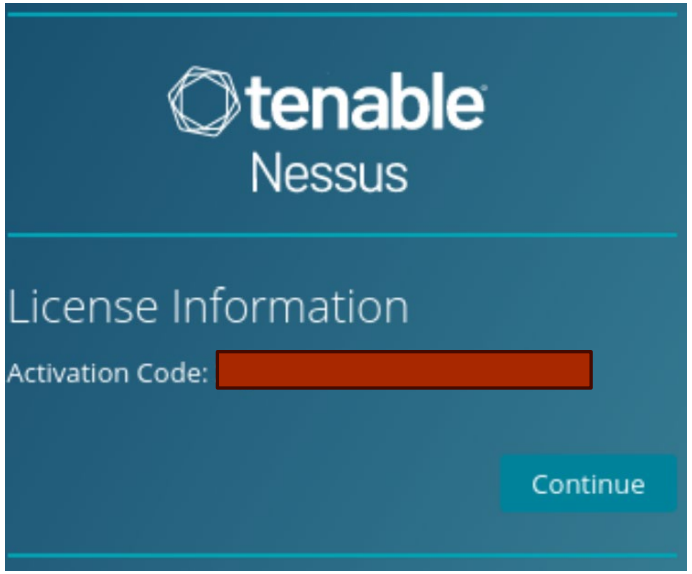
Analisi Automatica delle Vulnerabilità
Nessus – Avvio

- Registrazione ed attivazione



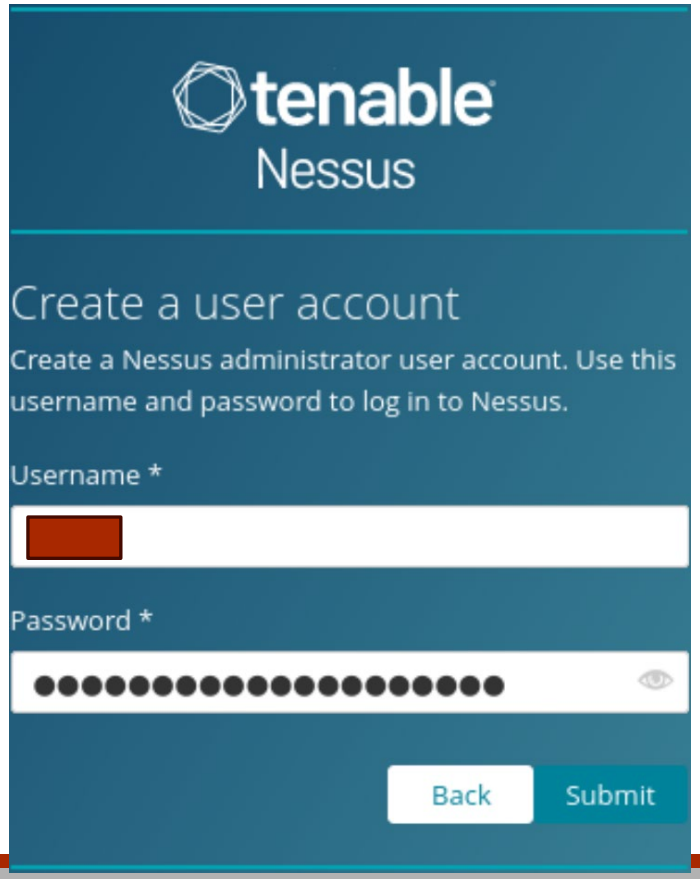
Analisi Automatica delle Vulnerabilità
Nessus – Avvio

- Registrazione ed attivazione



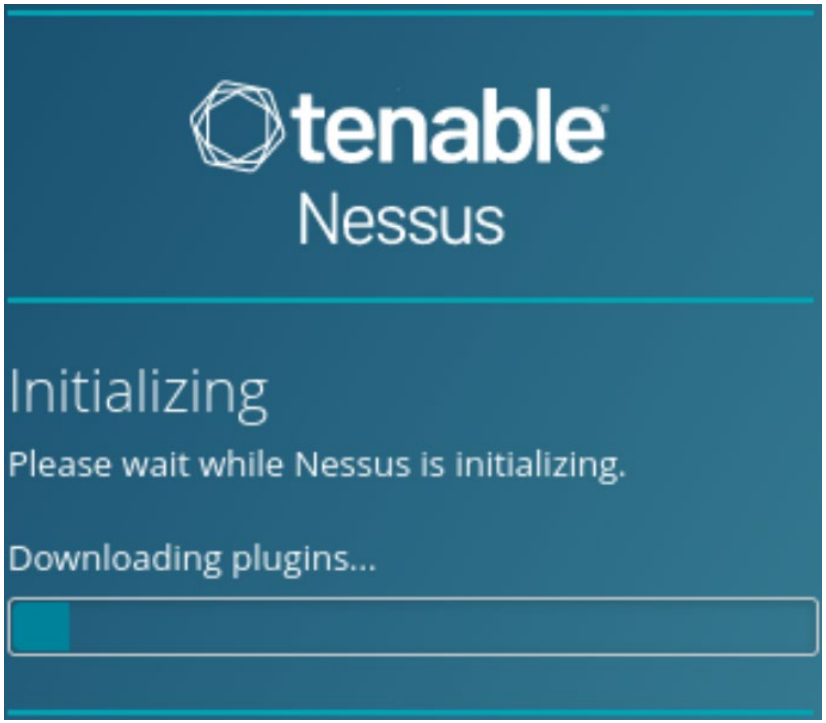
Analisi Automatica delle Vulnerabilità
Nessus – Avvio

- Registrazione ed attivazione



Analisi Automatica delle Vulnerabilità
Nessus – Avvio

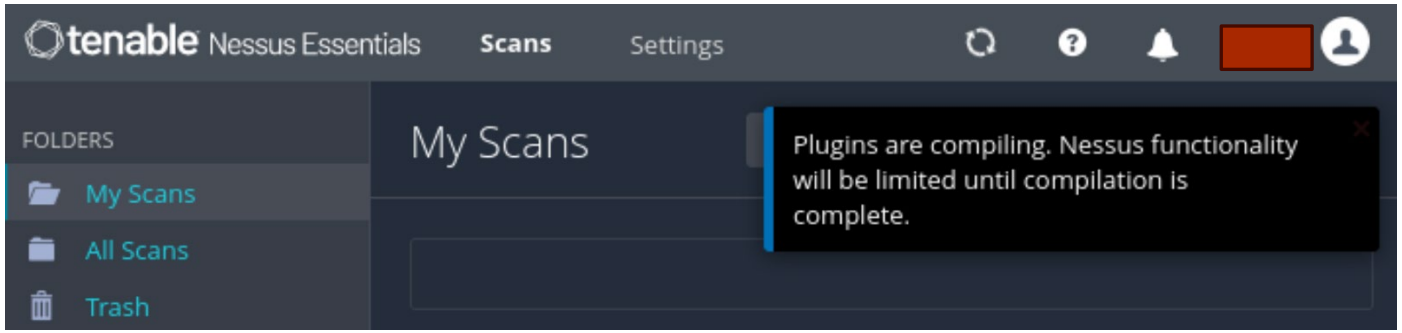
- Inizializzazione di Nessus



N.B. La prima inizializzazione di Nessun potrebbe richiedere molto tempo…

Analisi Automatica delle Vulnerabilità
Nessus – Avvio

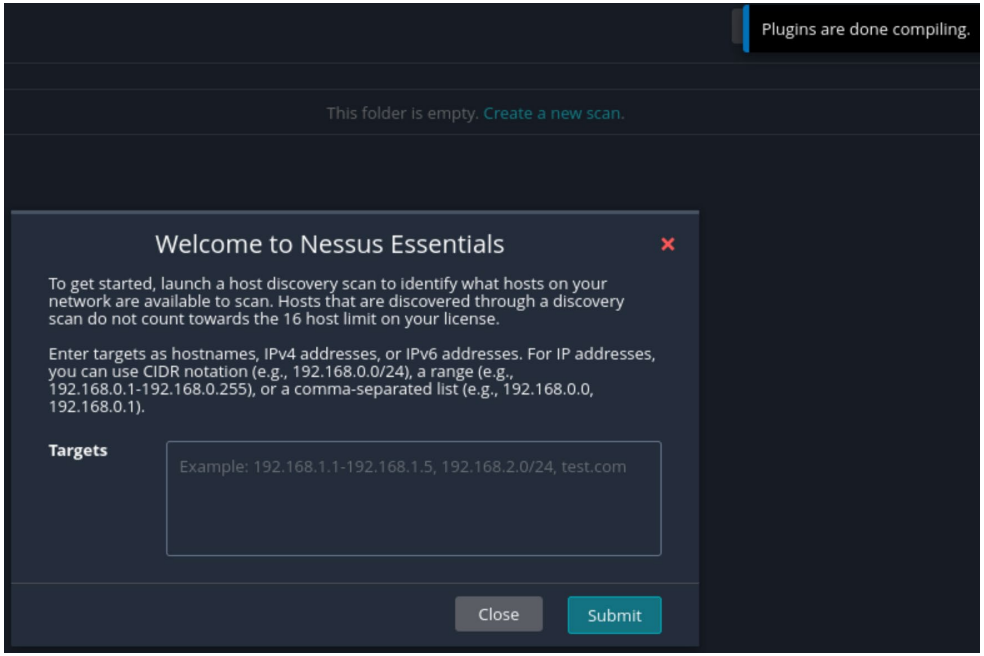
- Inizializzazione di Nessus



N.B. La prima inizializzazione di Nessun potrebbe richiedere molto tempo…

Analisi Automatica delle Vulnerabilità
Nessus – Avvio

- Attendere il download e la compilazione dei plugin, al termine della quale sarà mostrato un messaggio di benvenuto e diventerà selezionabile l'opzione «**`New Scan`**»

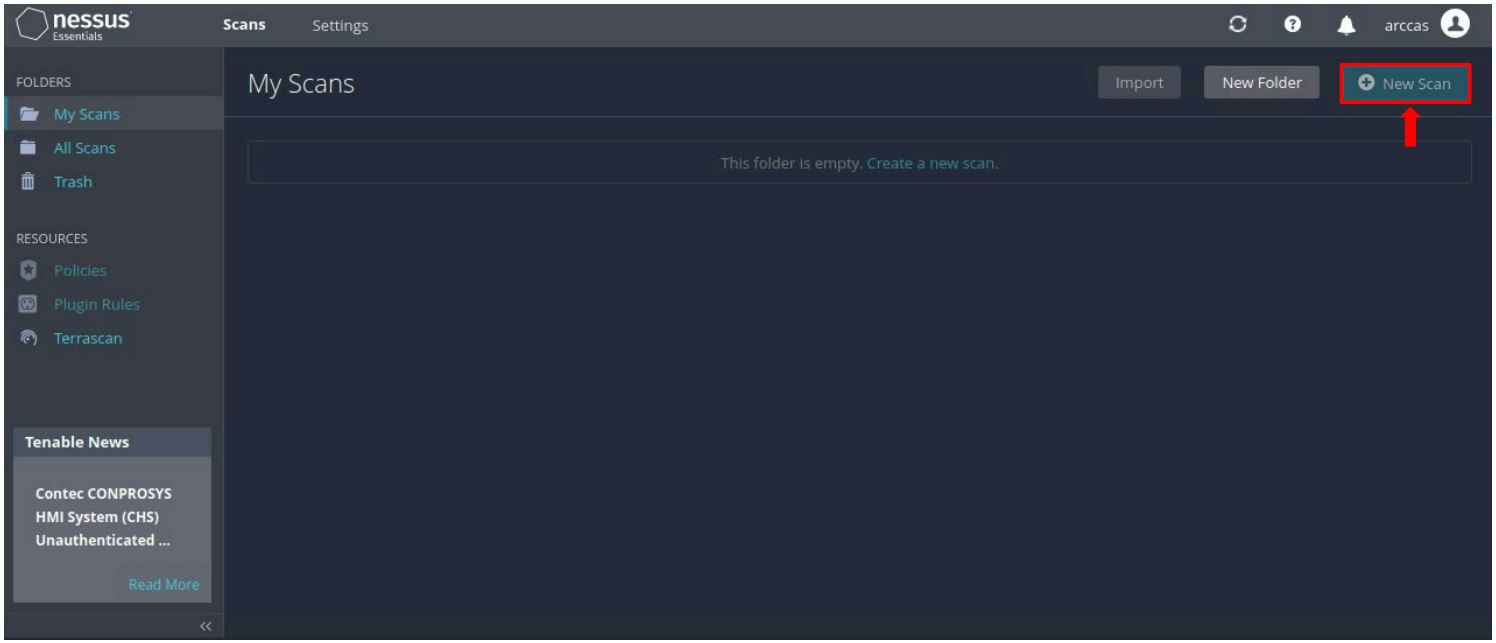


<u>N.B.</u> La prima inizializzazione di Nessun potrebbe richiedere molto tempo…

Analisi Automatica delle Vulnerabilità

Nessus – Avvio

- Attendere il download e la compilazione dei plugin, al termine della quale sarà selezionabile l'opzione «**`New Scan`**»

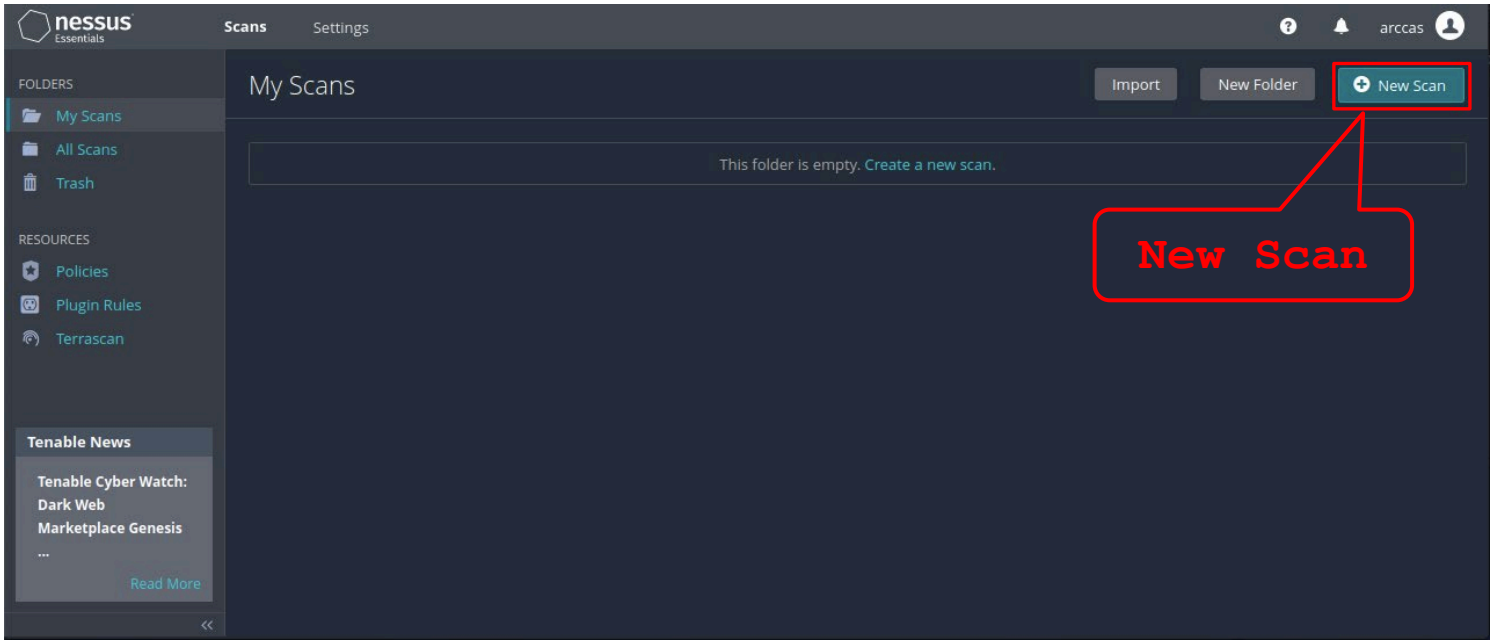


N.B. La prima inizializzazione di Nessun potrebbe richiedere molto tempo…

Analisi Automatica delle Vulnerabilità

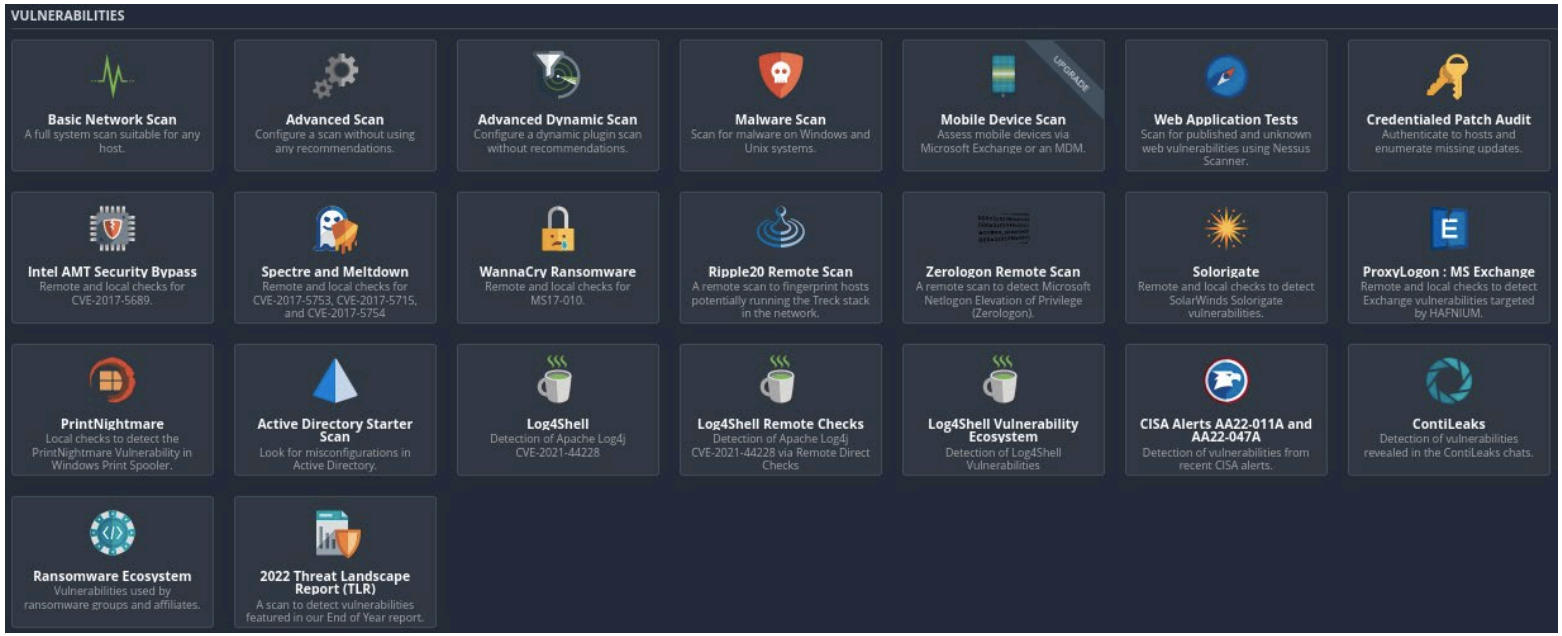
Nessus – Avvio

- Selezionare l'opzione «**`New Scan`**»



Analisi Automatica delle Vulnerabilità

Nessus – Configurazione di una Scansione



Nessus fornisce varie tipologie di scansione per la rilevazione delle vulnerabilità.
Alcune tipologie sono utilizzabili solo con la versione a pagamento di Nessus

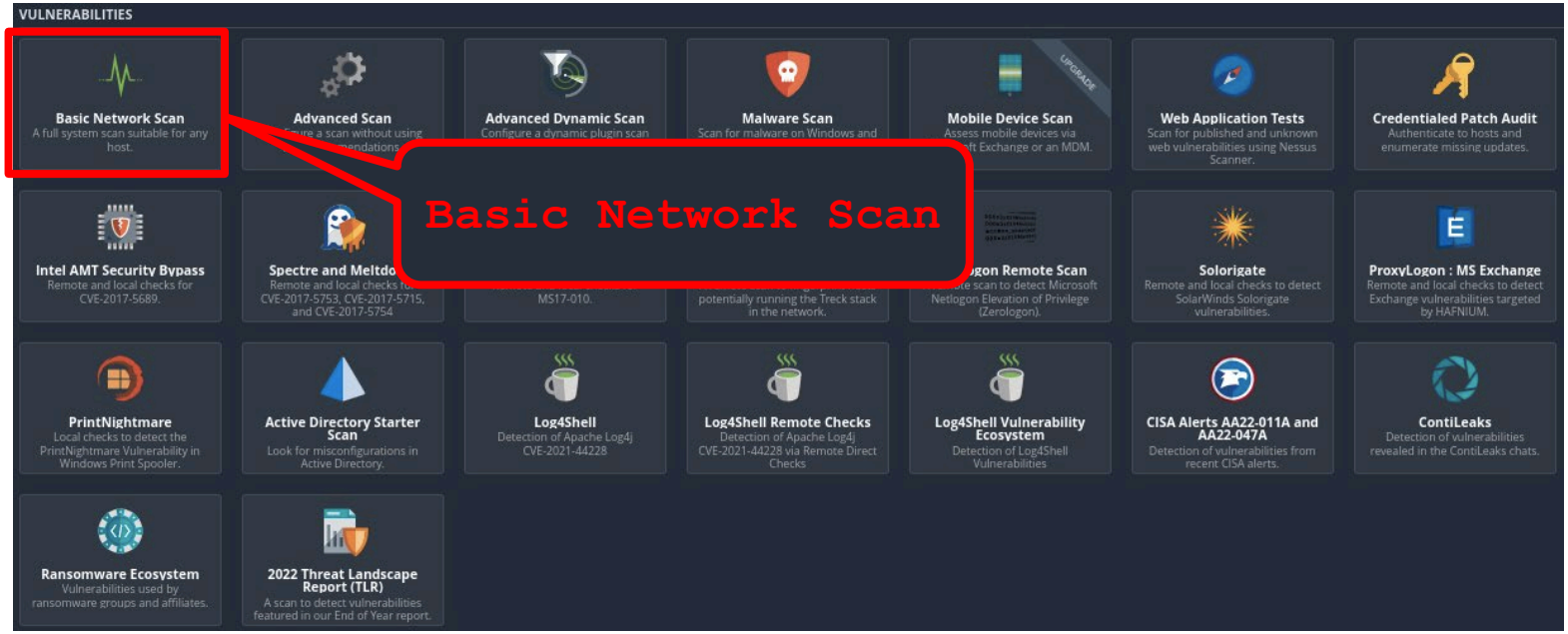
Analisi Automatica delle Vulnerabilità

Nessus – Configurazione di una Scansione

Nessus consente anche di effettuare operazioni di «Security Audit»

Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan



Utilizzeremo un «**`Basic Network Scan`**»

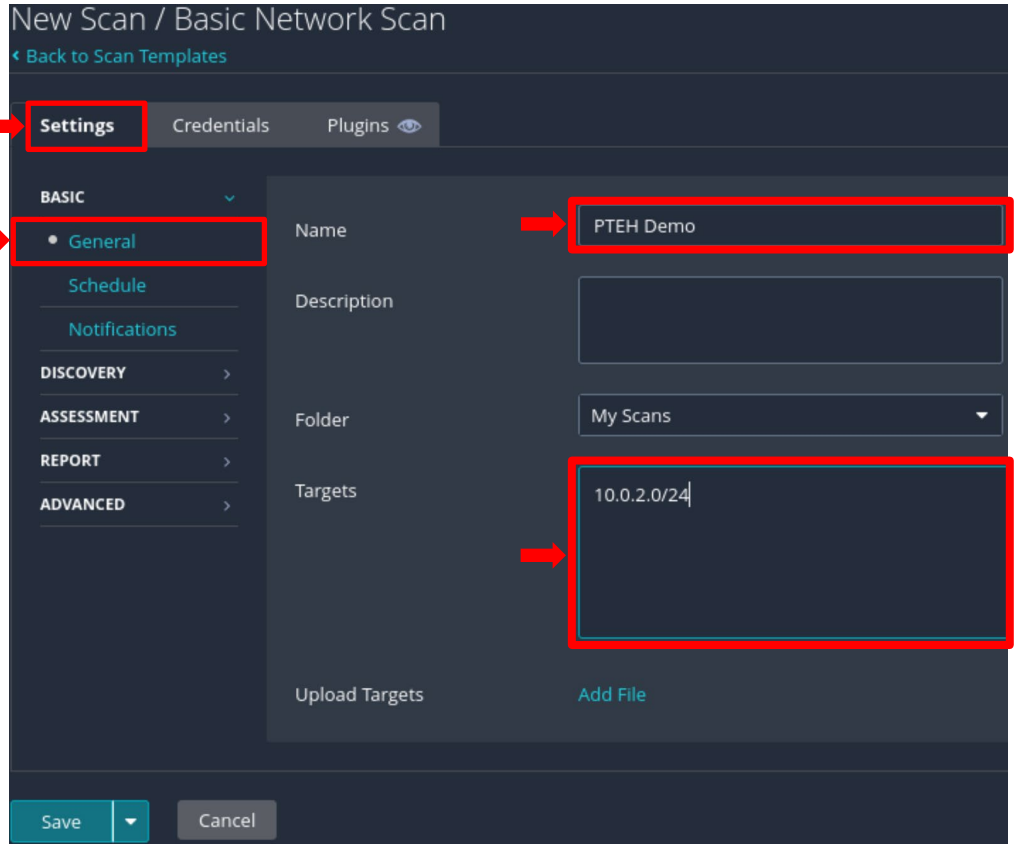
Analisi Automatica delle Vulnerabilità
Nessus – Basic Network Scan

- Nessus fornisce numerose opzioni (**`Settings`**) per la creazione e la configurazione di una scansione
  - **`Basic`**
    - **`General`**
    - **`Schedule`**
    - **`Notifications`**
  - **`Discovery`**
  - **`Assessment`**
  - **`Report`**
  - **`Advanced`**

Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Configurazione

- **`General`:** informazioni di base relative alla scansione

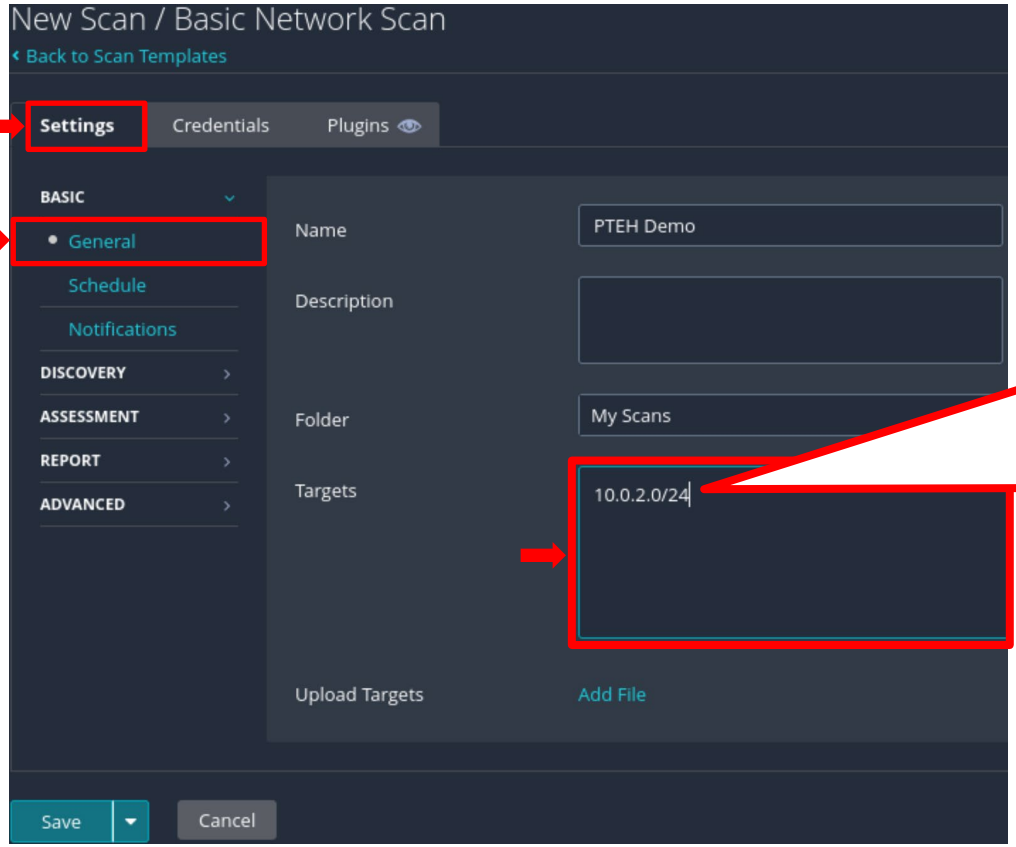


- **Inserire i dati relativi a `Name` e `Targets`**
  - **Unici parametri necessari per avviare una scansione**

Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Configurazione

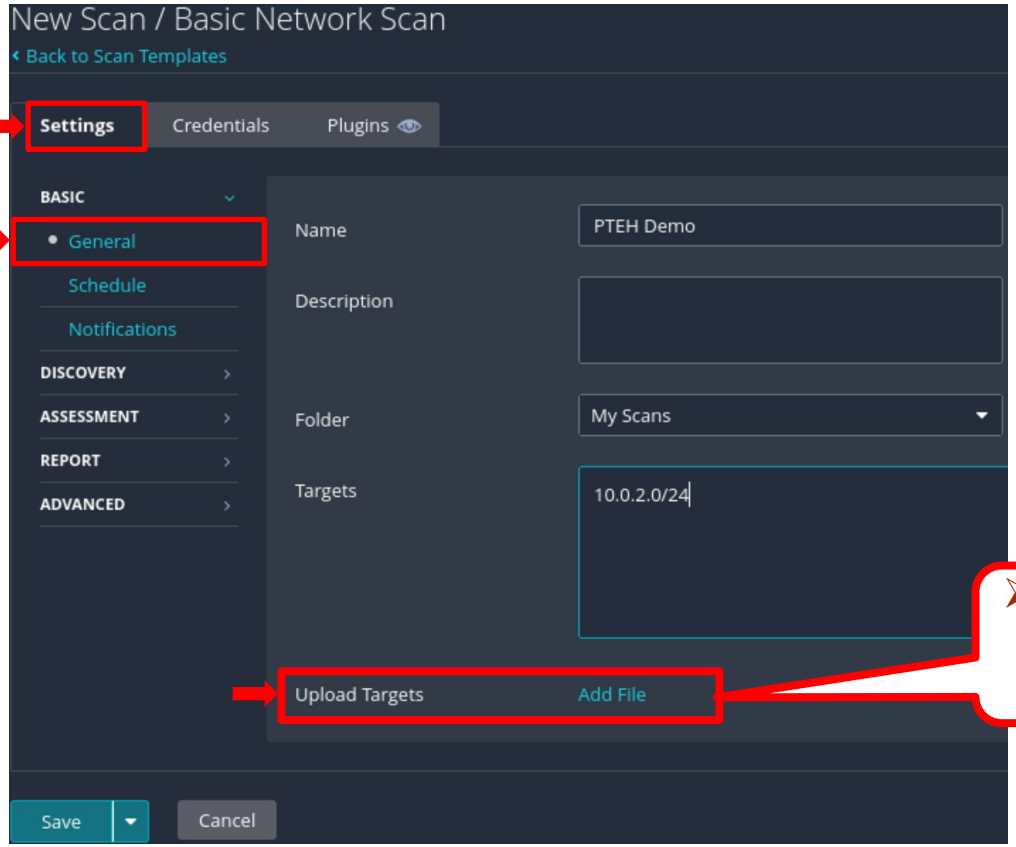
- **`General`:** informazioni di base relative alla scansione



- **È possibile specificare il target tramite**
  - **Singolo indirizzo IP**
  - **Indirizzi IP multipli**
    - **Lista**
    - **Notazione CIDR**
    - **Etc**

Analisi Automatica delle Vulnerabilità
Nessus – Basic Network Scan – Configurazione

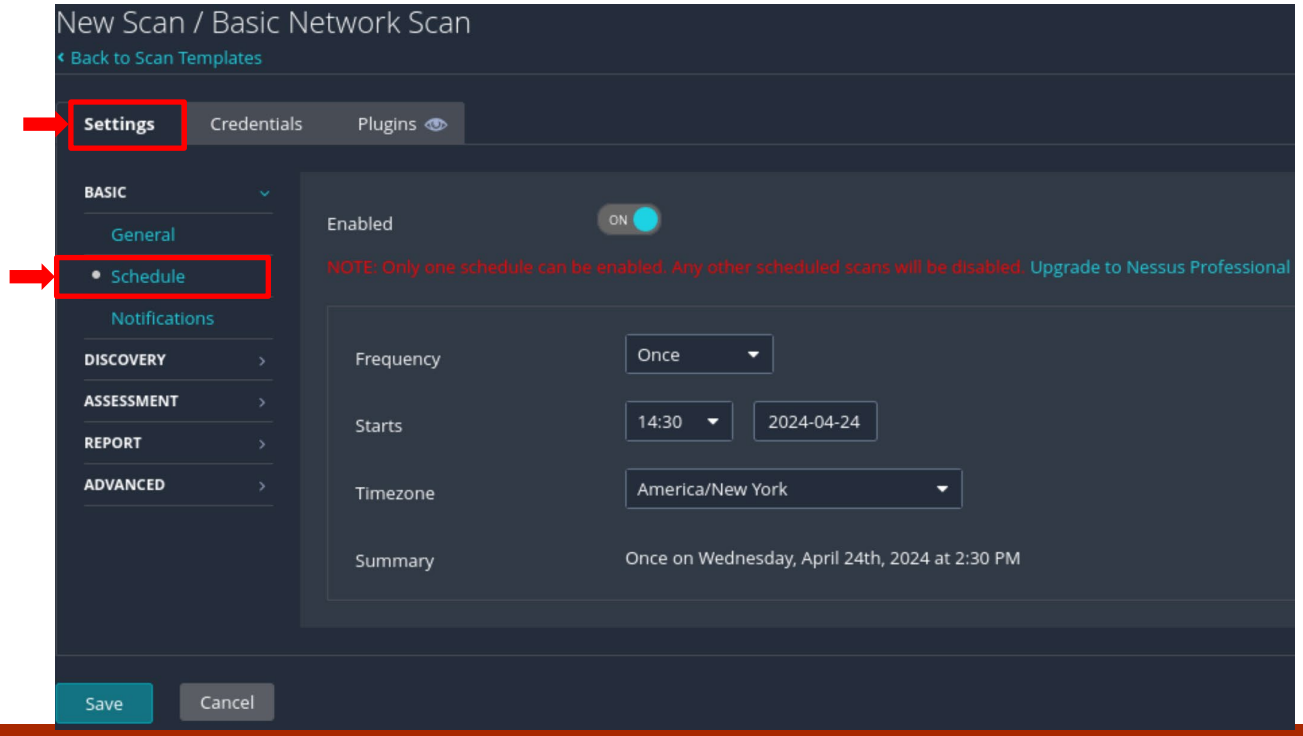
- **`General`:** informazioni di base relative alla scansione



- **È anche possibile specificare il target tramite file**

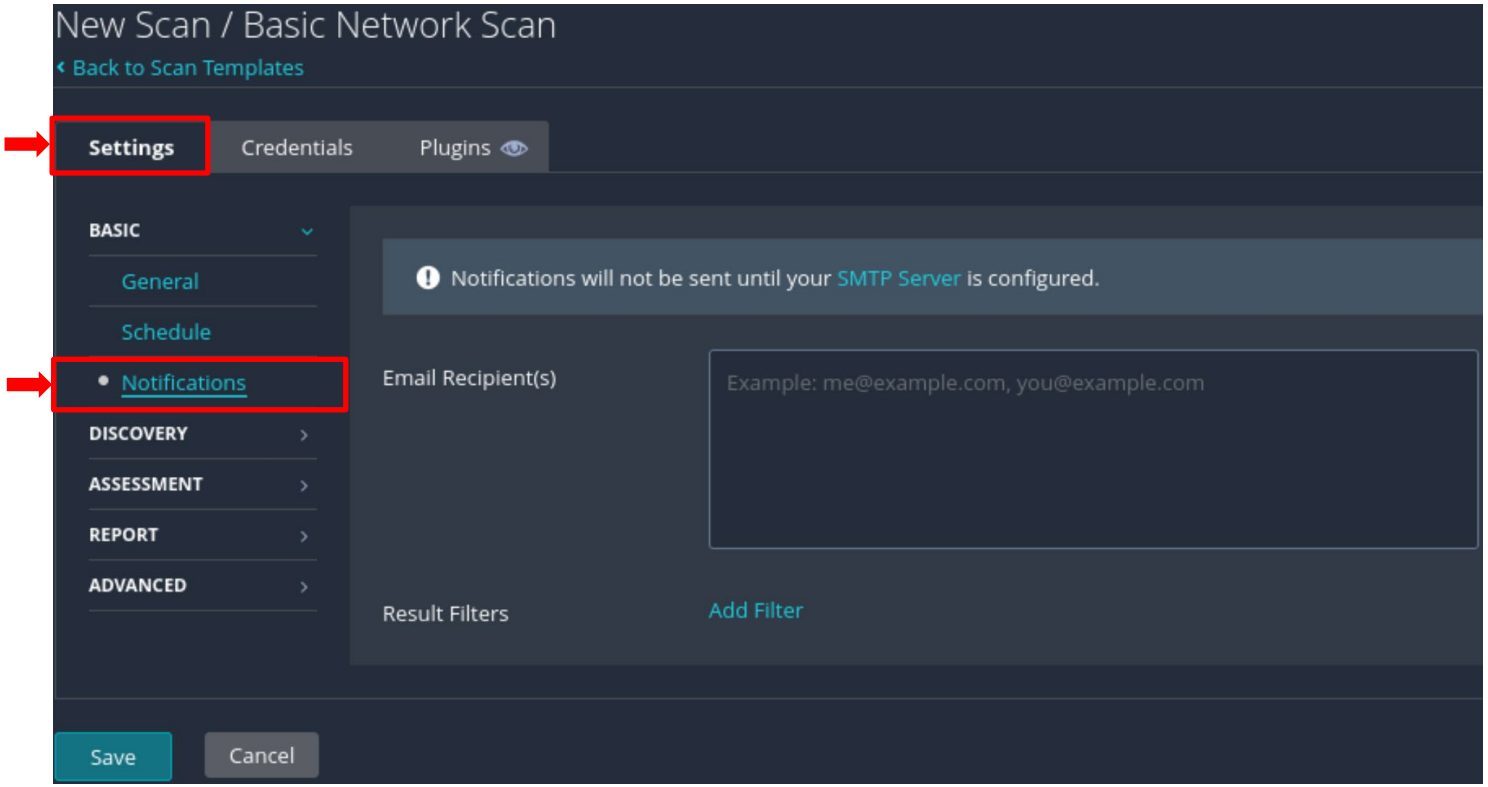
Analisi Automatica delle Vulnerabilità
Nessus – Basic Network Scan – Configurazione

- **`Schedule`:** consente di eseguire una scansione in un momento specifico
  - Utile, ad esempio, quando è necessario eseguire i test dopo l'orario di ufficio



Analisi Automatica delle Vulnerabilità
Nessus – Basic Network Scan – Configurazione

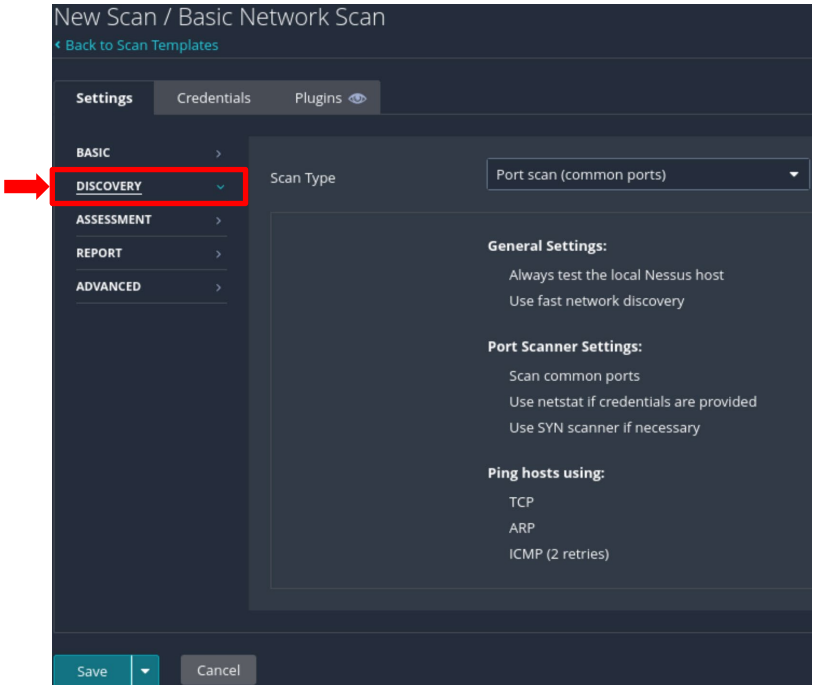
- **`Notifications`:** Nessus può essere configurato per inviare notifiche via e-mail al termine di una scansione



Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Configurazione

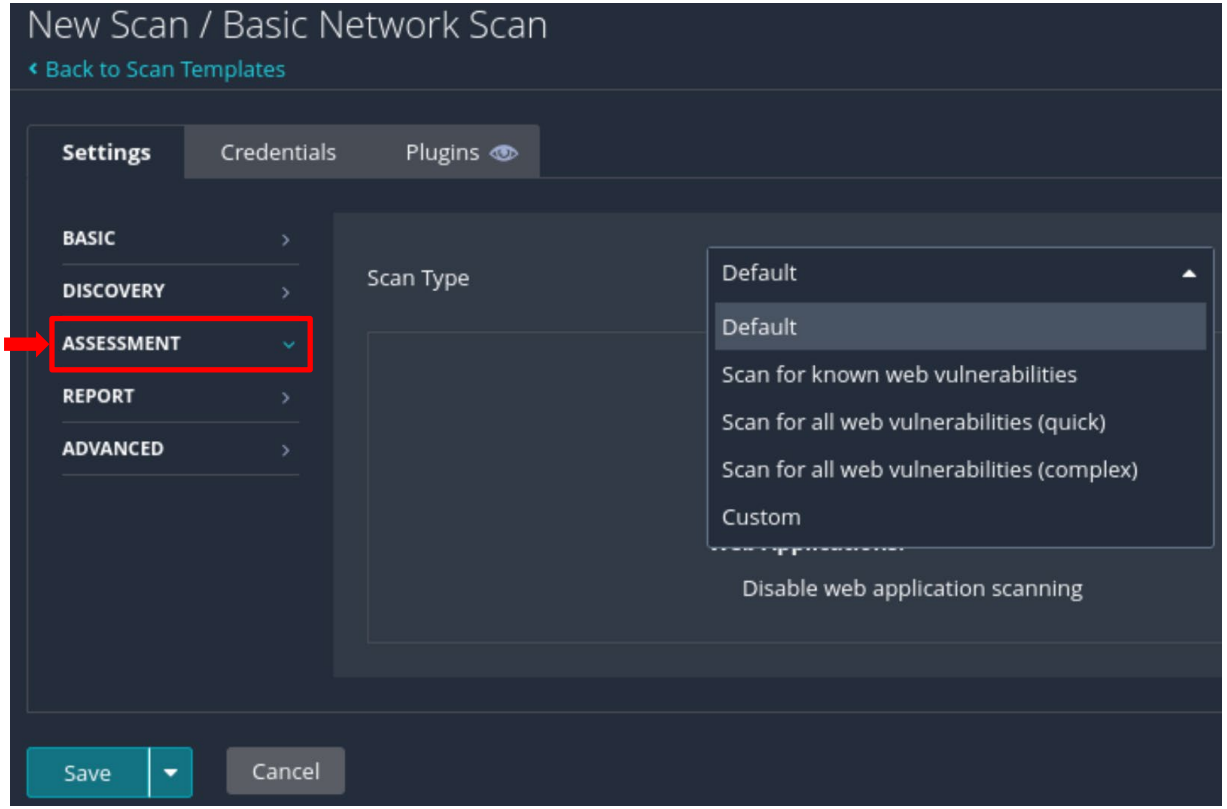
- **`Discovery`:** Nessus utilizza diversi metodi per scoprire gli host attivi ed i relativi servizi
  - In questa sezione possono essere impostati i parametri per il *Target Discovery*



Analisi Automatica delle Vulnerabilità

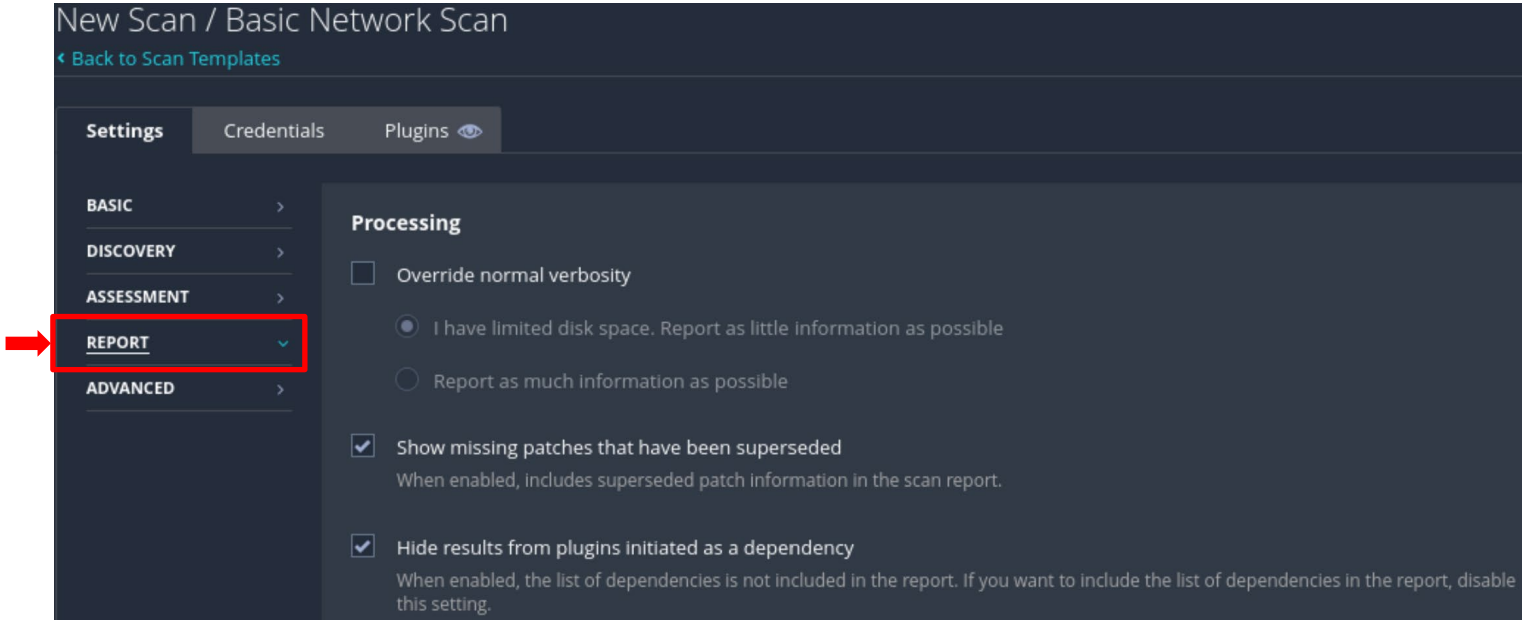
Nessus – Basic Network Scan – Configurazione

- **`Assessment:`** Consente di impostare il tipo di scansione



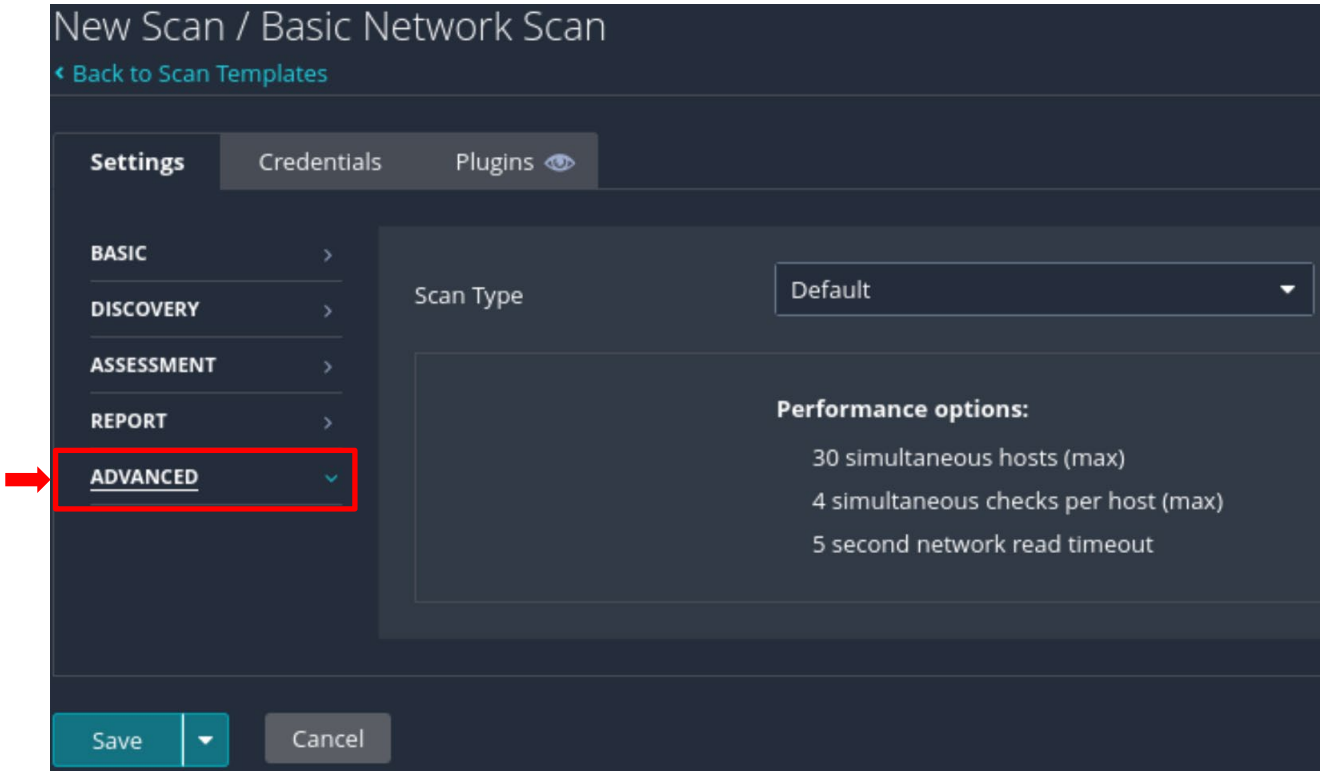
Analisi Automatica delle Vulnerabilità
Nessus – Basic Network Scan – Configurazione

- **`Report:`** Consente di personalizzare il modo in cui Nessus genera il report della scansione



Analisi Automatica delle Vulnerabilità
Nessus – Basic Network Scan – Configurazione

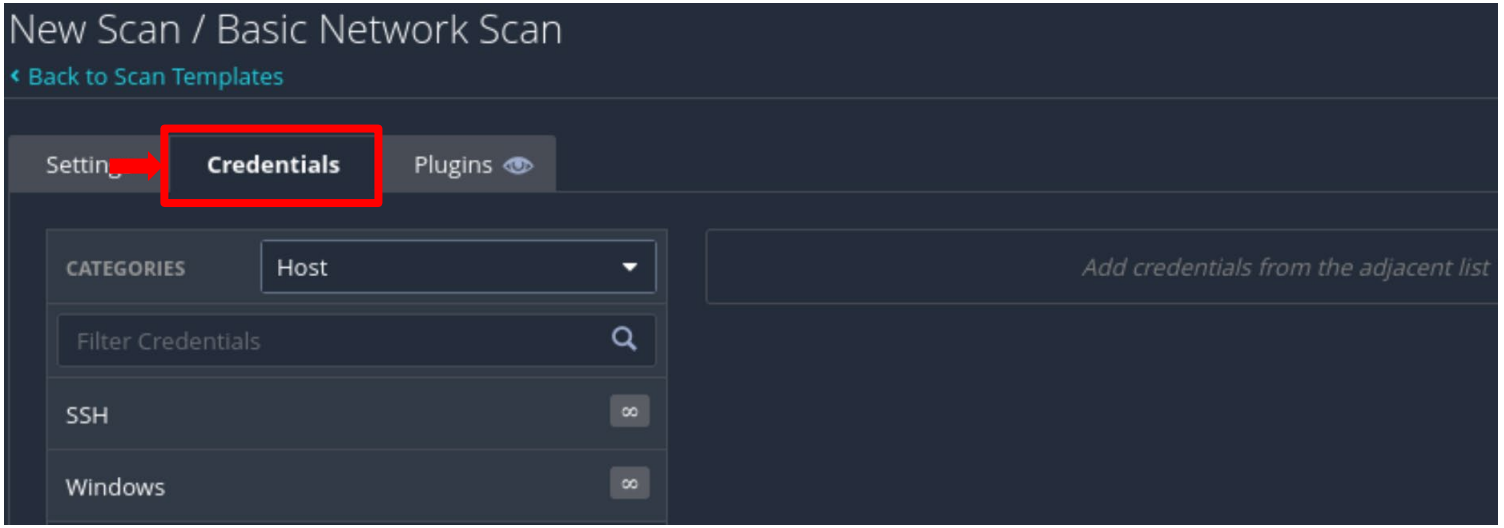
- **Advanced:** Consente di impostare il numero di host scansionati simultaneamente ed altri parametri di temporizzazione



Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Configurazione

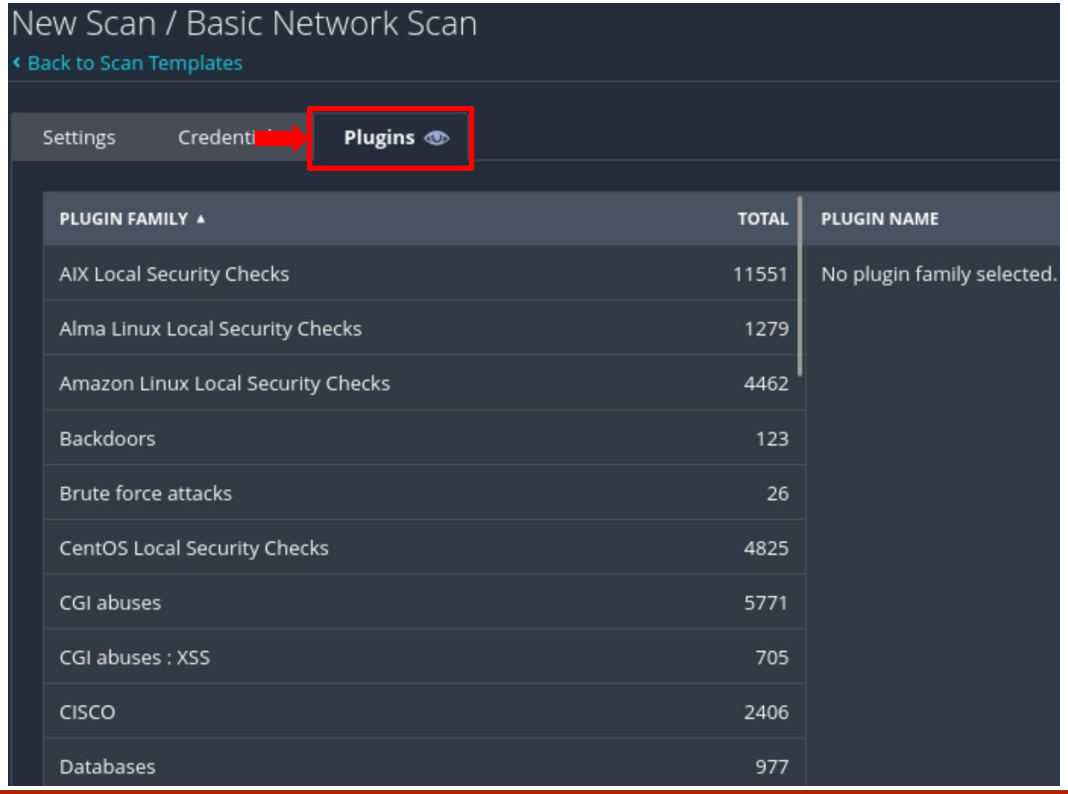
- **`Credentials:`** Prima di avviare la scansione, possono essere impostate le credenziali di autenticazione per vari servizi



Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Configurazione

- **`Plugins:`** Possono essere visualizzati i plugin usati dal template di scansione selezionato



Analisi Automatica delle Vulnerabilità

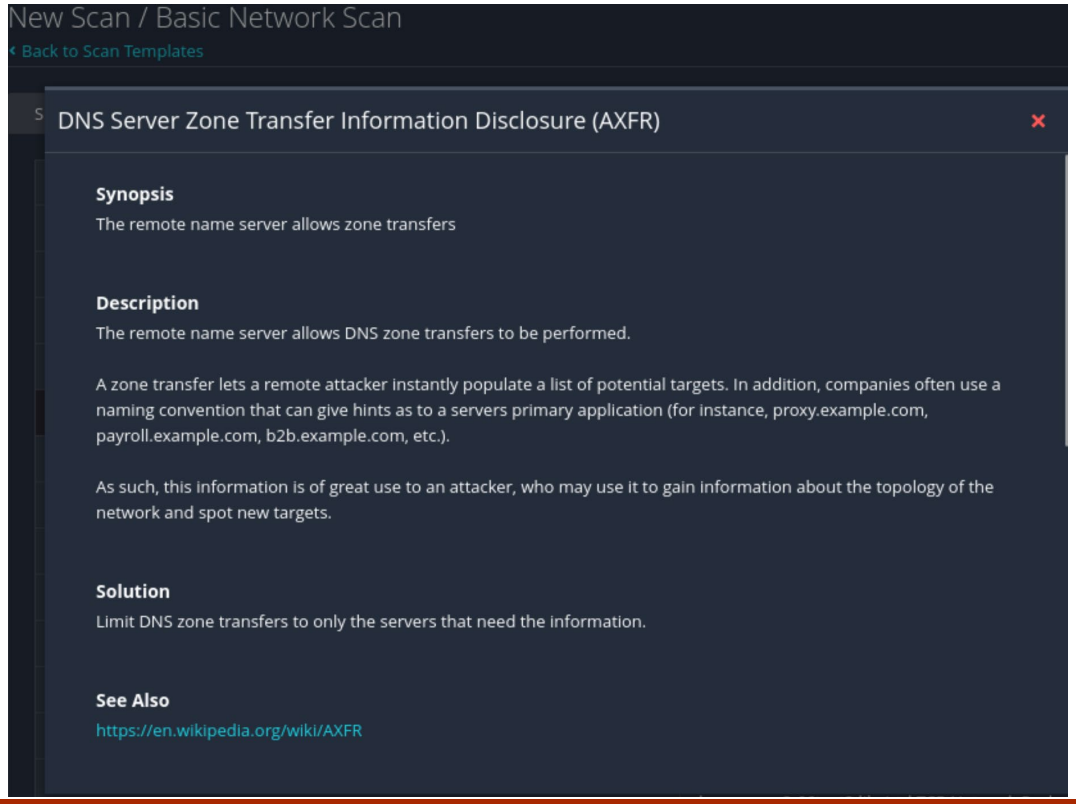
Nessus – Basic Network Scan – Configurazione

- **`Plugins`:** Possono essere visualizzati i plugin usati dal template di scansione selezionato

- **N.B. Un «`Basic Network Scan`» consente solo di visualizzare i plugin utilizzati, mentre un «`Advanced Scan`» consente anche di scegliere in maniera arbitraria quali plugin utilizzare per una scansione**

Analisi Automatica delle Vulnerabilità
Nessus – Basic Network Scan – Configurazione

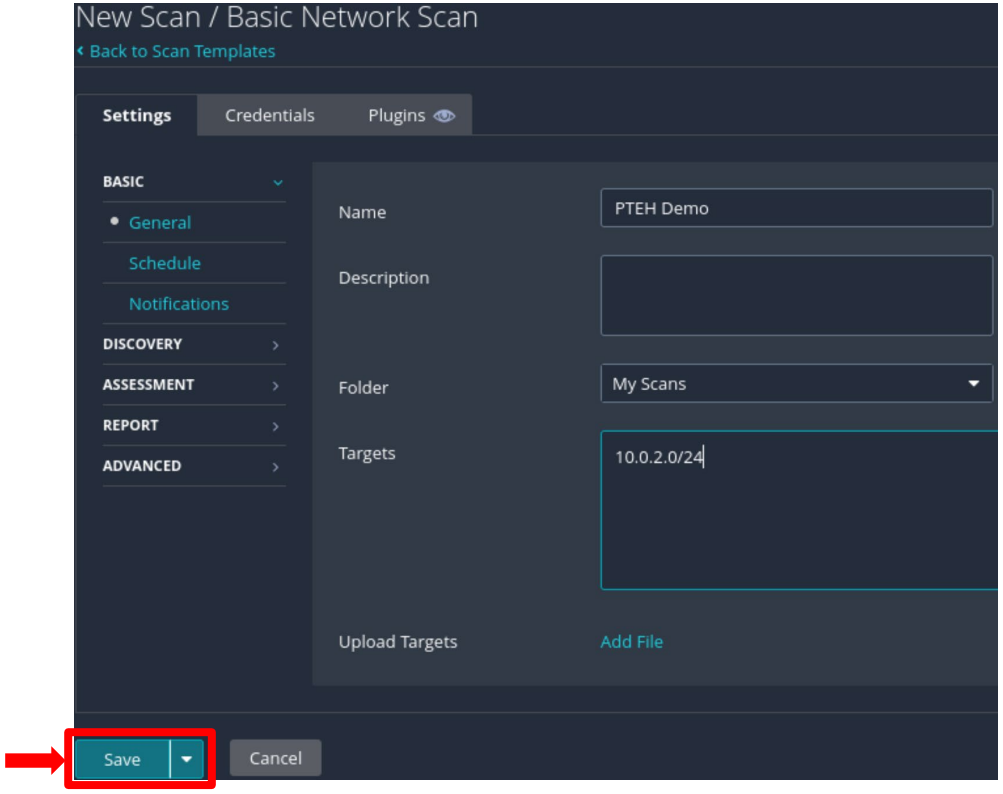
- **`Plugins`:** Possono essere visualizzati i plugin usati dal template di scansione selezionato



Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Configurazione

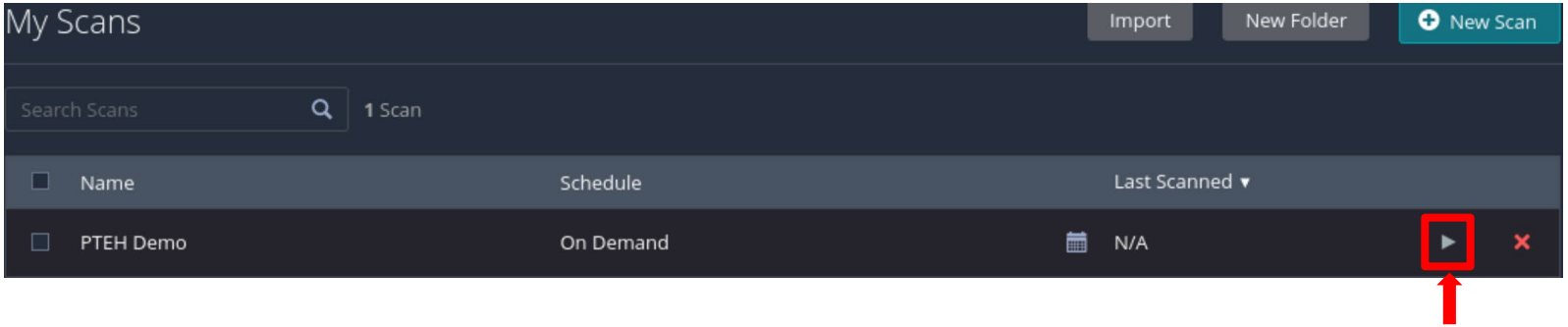
- Dopo aver configurato tutte le opzioni di scansione (*profilo di scansione*) è possibile memorizzare tale profilo



Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Scansione

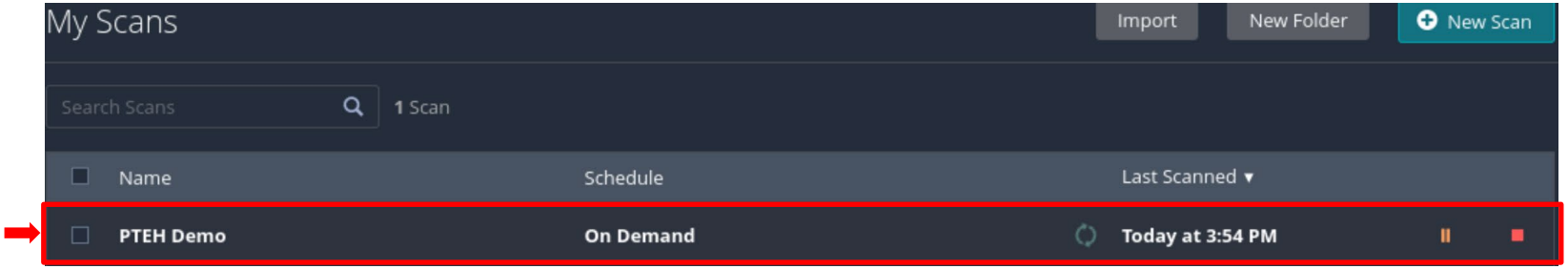
- Avvio della scansione



Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Scansione

- Avvio della scansione

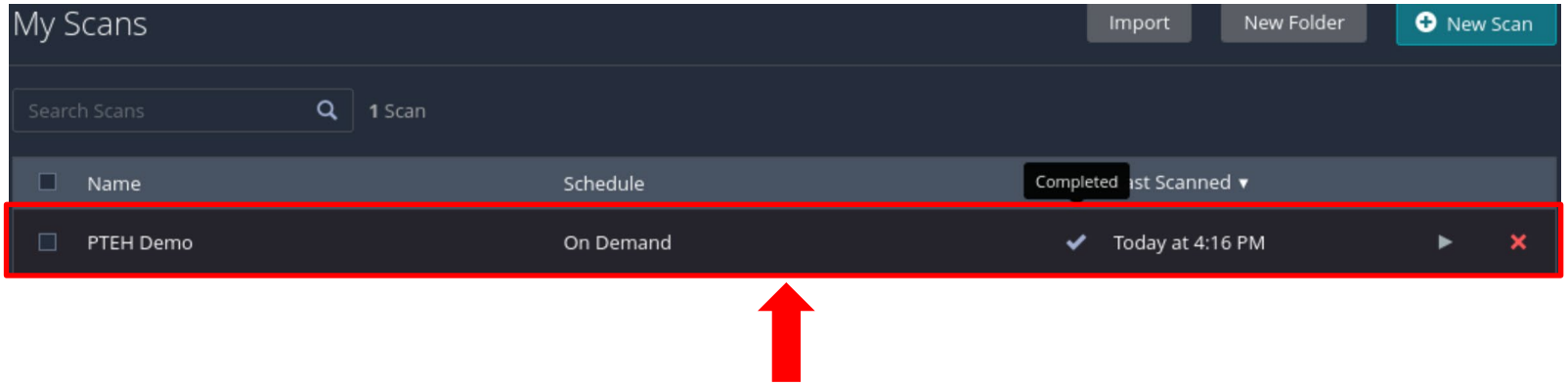


N.B. La scansione richiede un tempo variabile in base alla tipologia di scansione selezionata, al numero ed alla tipologia degli host da analizzare

Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Scansione

- Visualizzazione dei risultati della scansione



Terminata una scansione è possibile visualizzarne i risultati cliccando sulla riga relativa alla scansione di interesse

Analisi Automatica delle Vulnerabilità

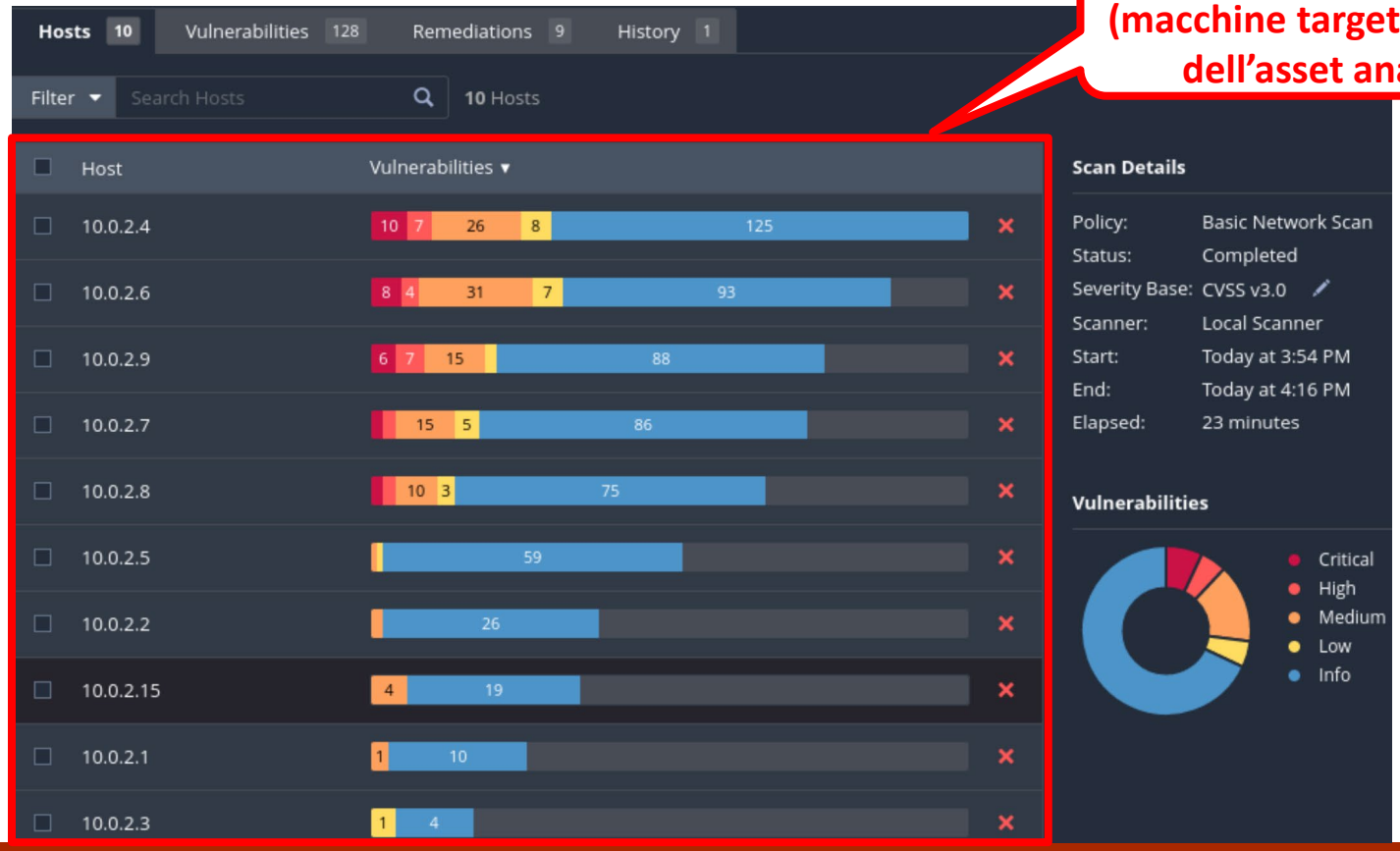
Nessus – Basic Network Scan – Scansione

- Risultati generali della scansione

Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Scansione

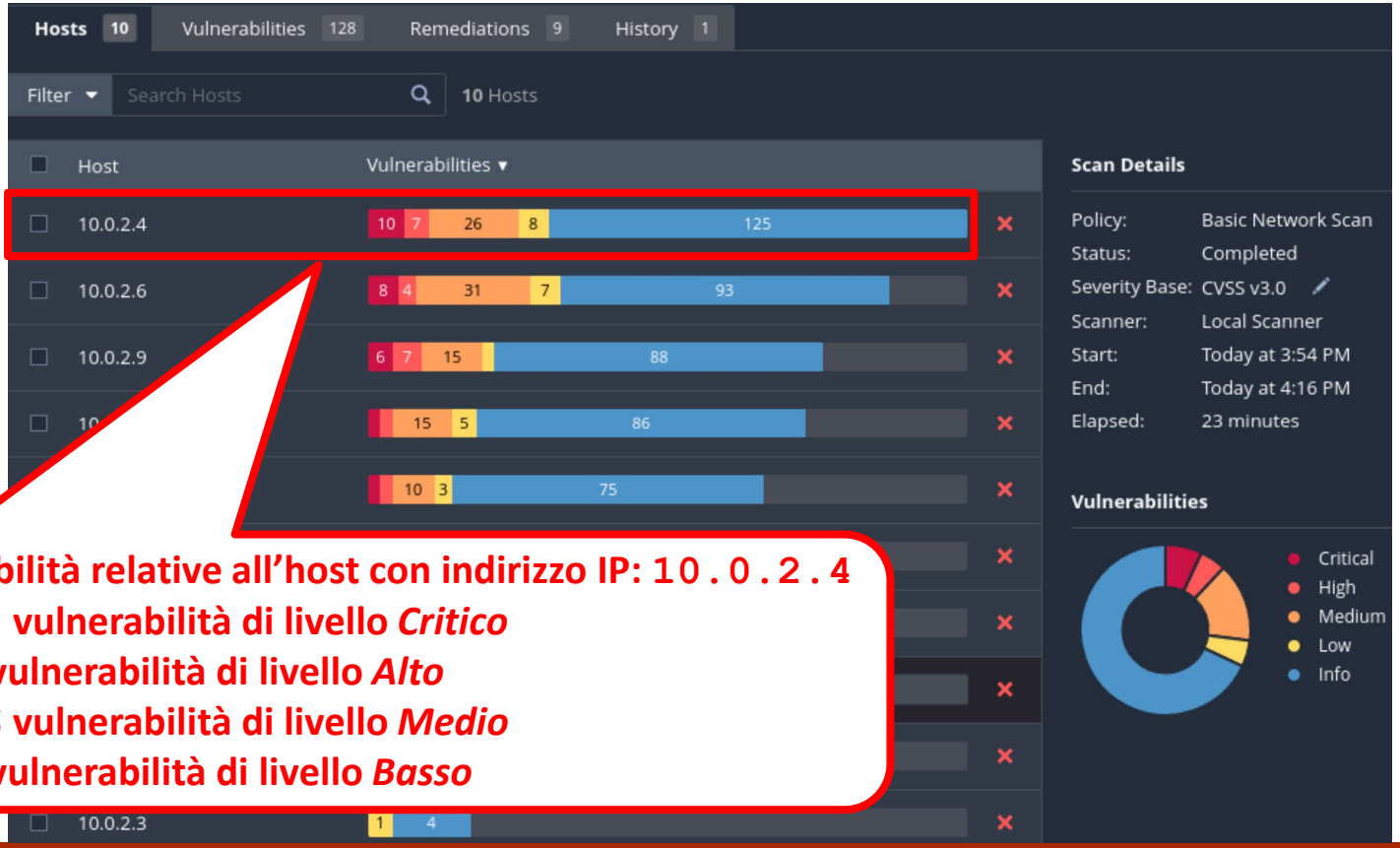
- Risultati generali della scansione



Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Scansione

- Risultati generali della scansione



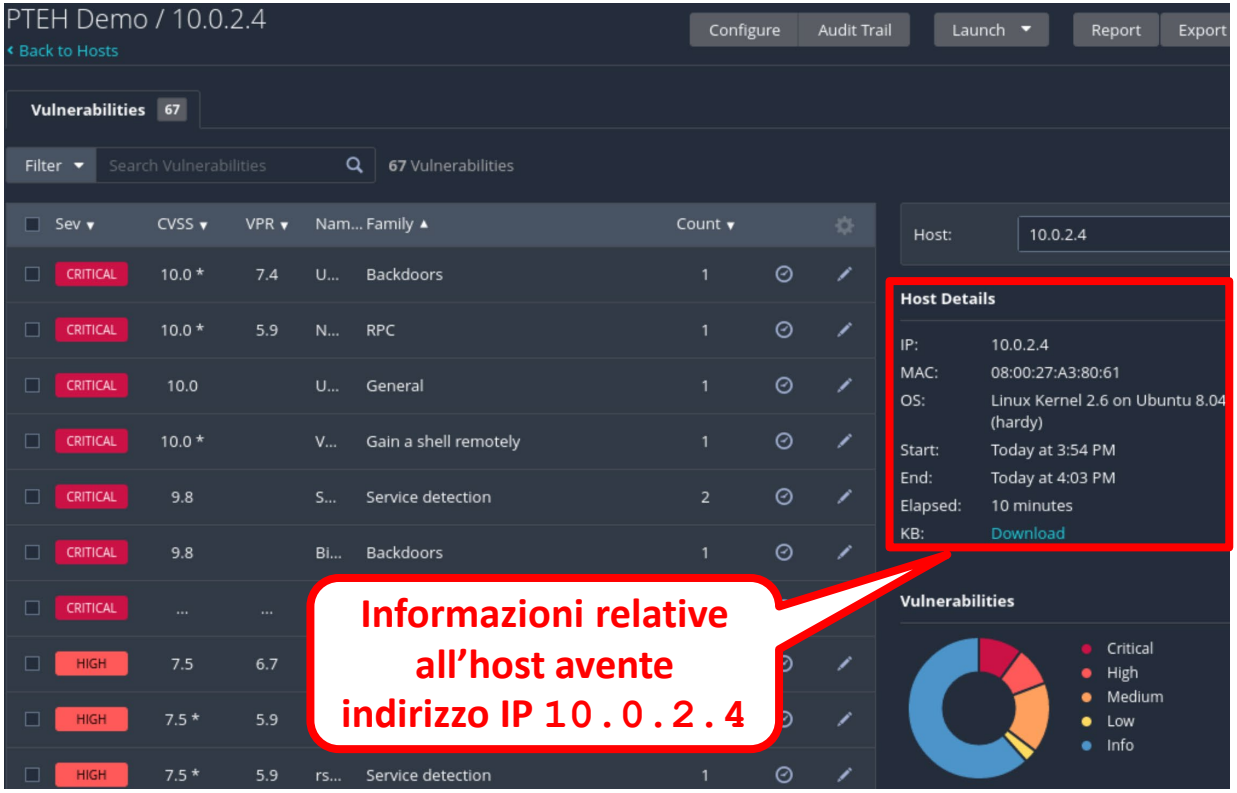
- **Vulnerabilità relative all'host con indirizzo IP: 10.0.2.4**
  - **10 vulnerabilità di livello *Critico***
  - **7 vulnerabilità di livello *Alto***
  - **26 vulnerabilità di livello *Medio***
  - **8 vulnerabilità di livello *Basso***

Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Scansione (MS 2)

- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - Dati riguardanti la macchina target (Metasploitable 2 - MS2)

Output parziale

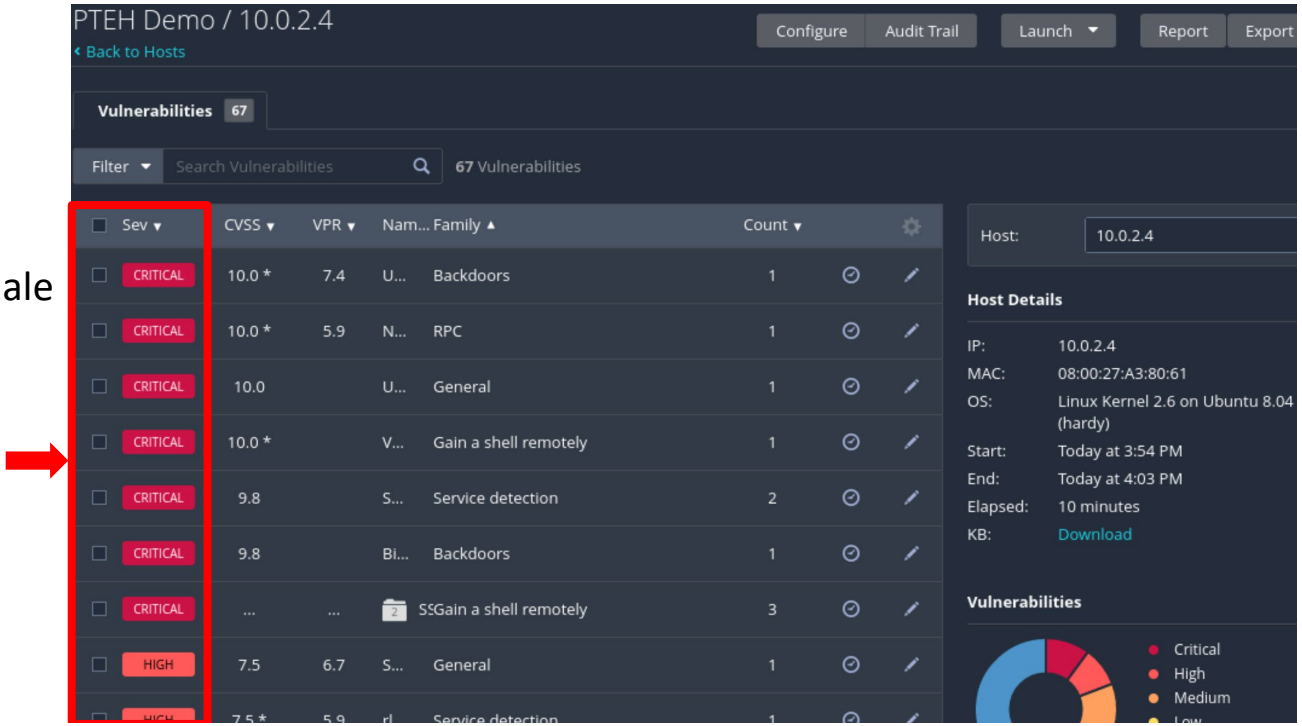


Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Scansione (MS 2)

- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`Severity`**

Output parziale



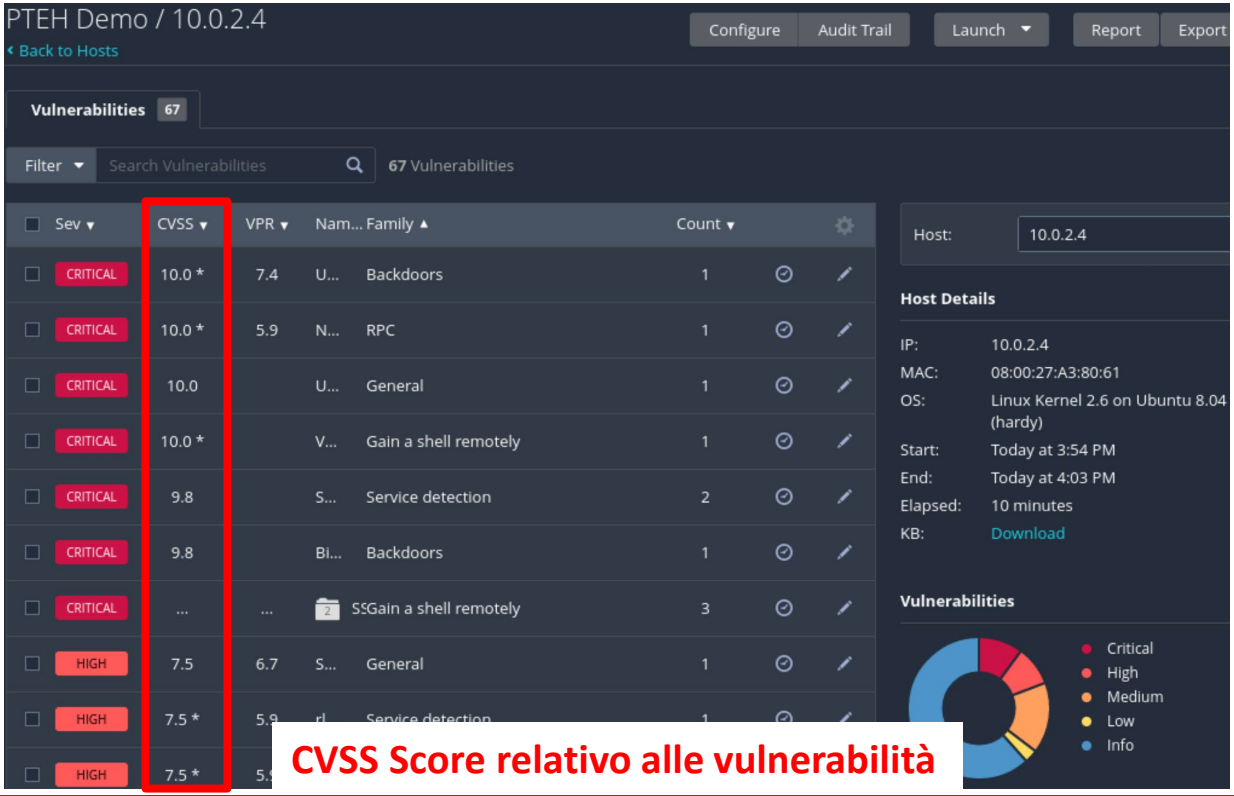
Le vulnerabilità sono ordinate di default in ordine decrescente di «`Severity`»

Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Scansione (MS 2)

- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **CVSS**

Output parziale

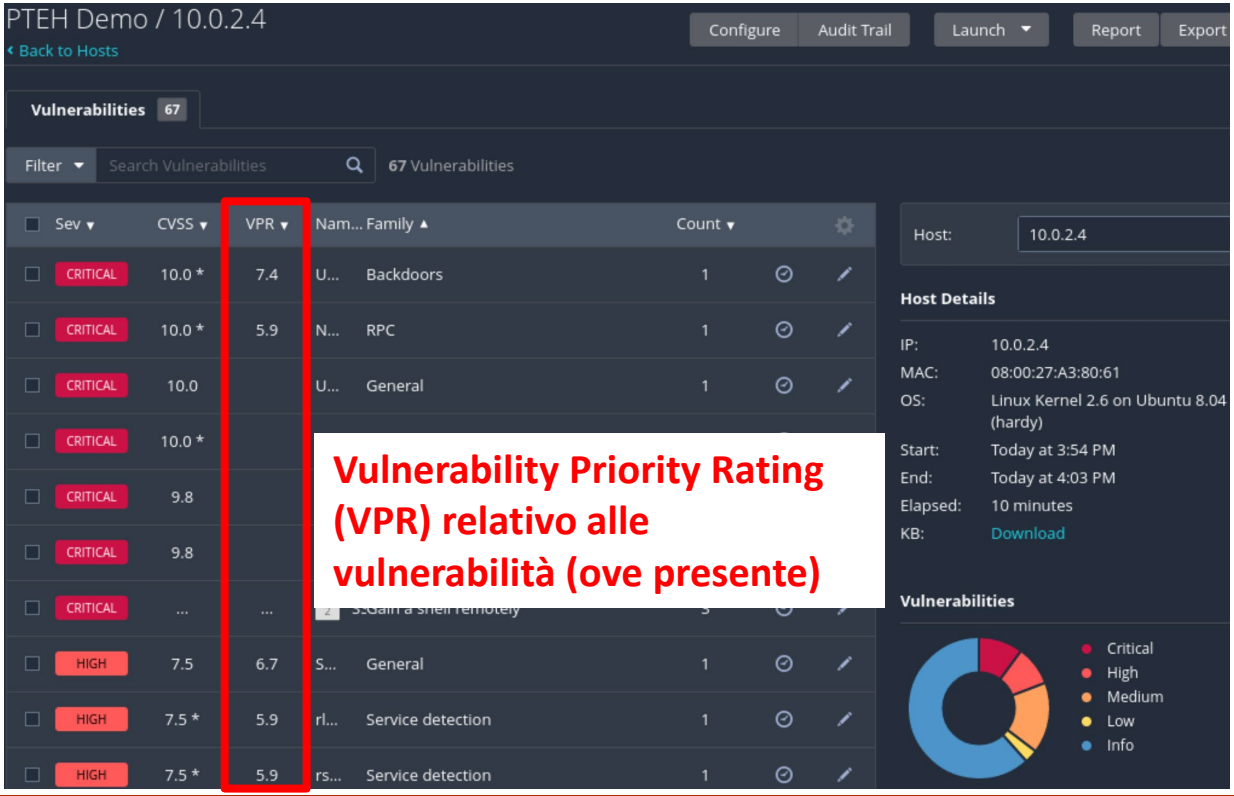


Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Scansione (MS 2)

- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`VPR`** (Per maggiori info, cliccare qui)

Output parziale

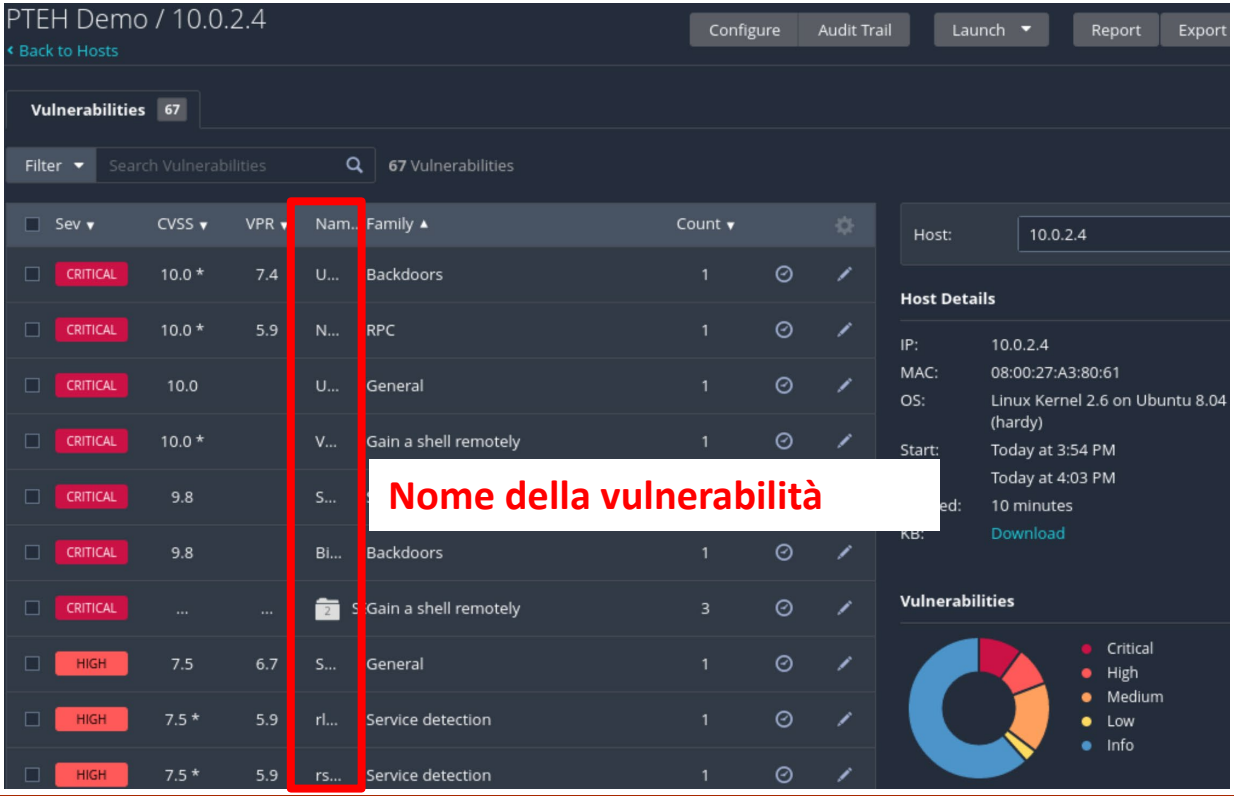


Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Scansione (MS 2)

- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`Name`**

Output parziale

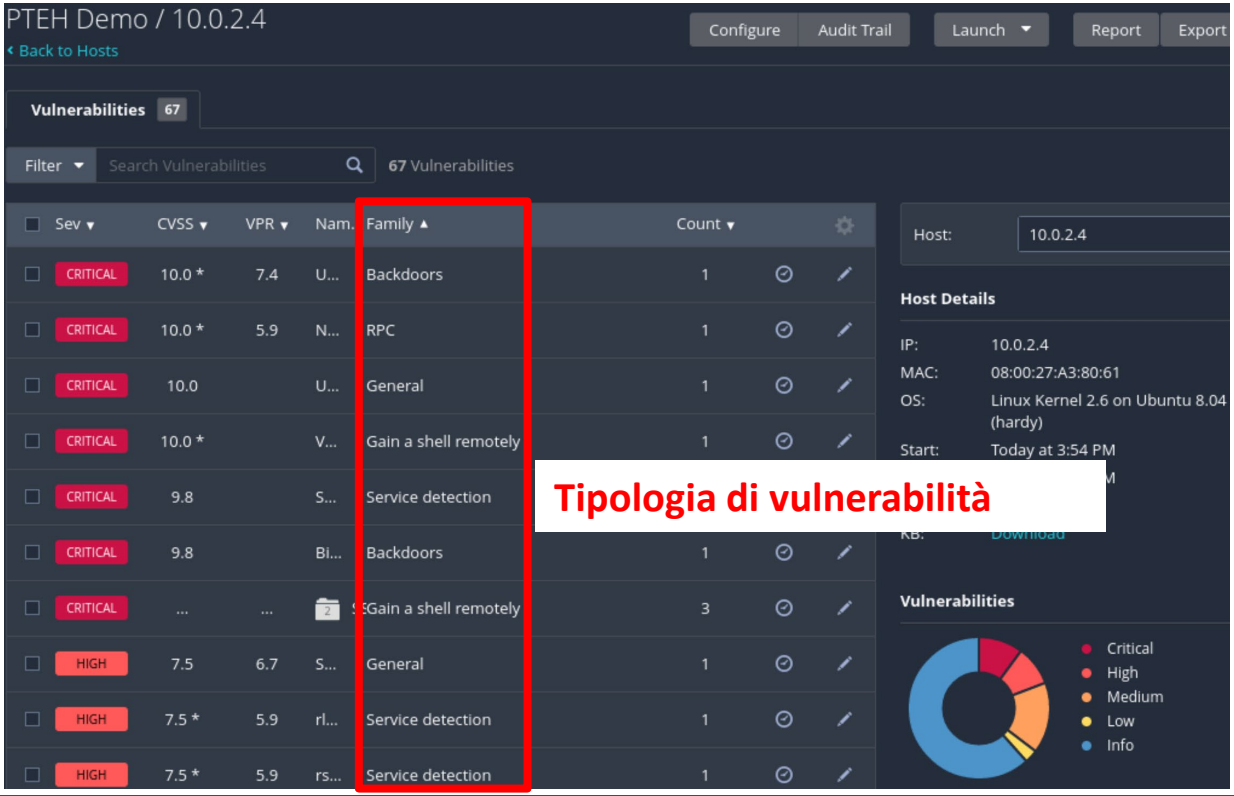


Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Scansione (MS 2)

- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`Family`**

Output parziale

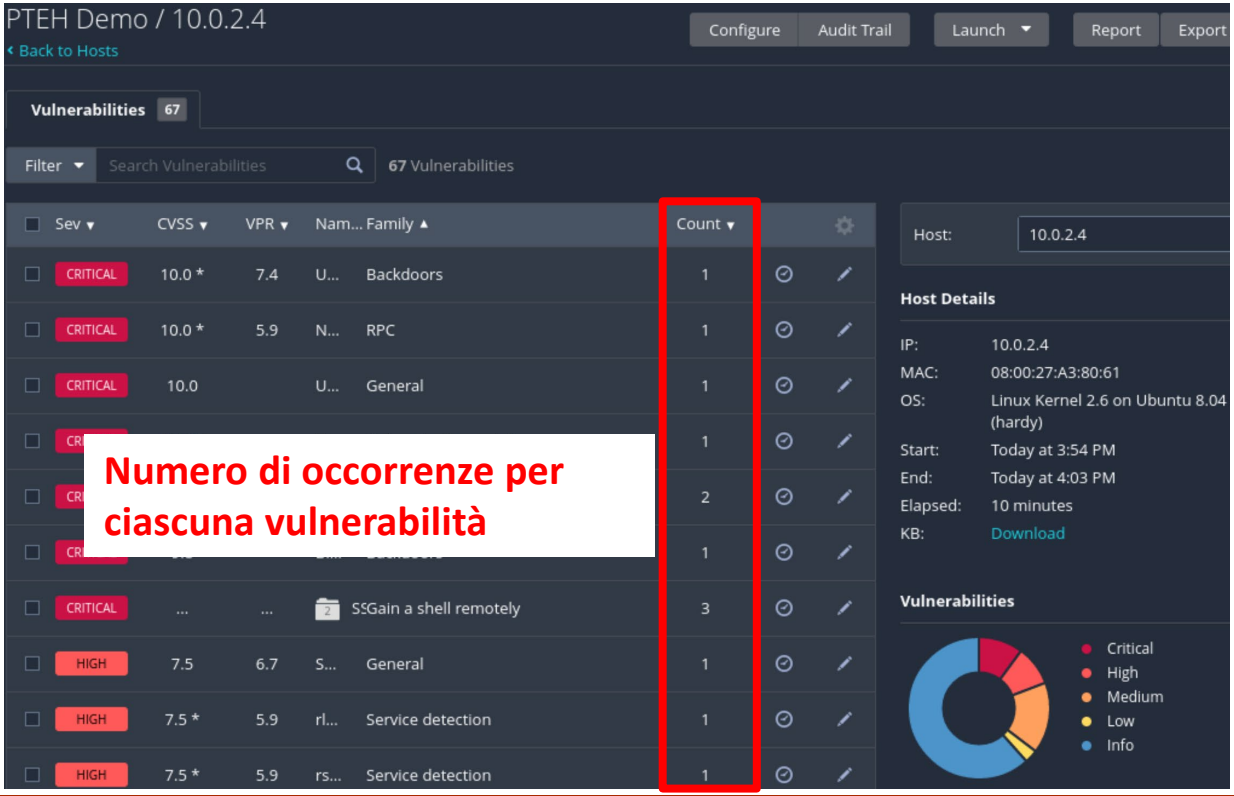


Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Scansione (MS 2)

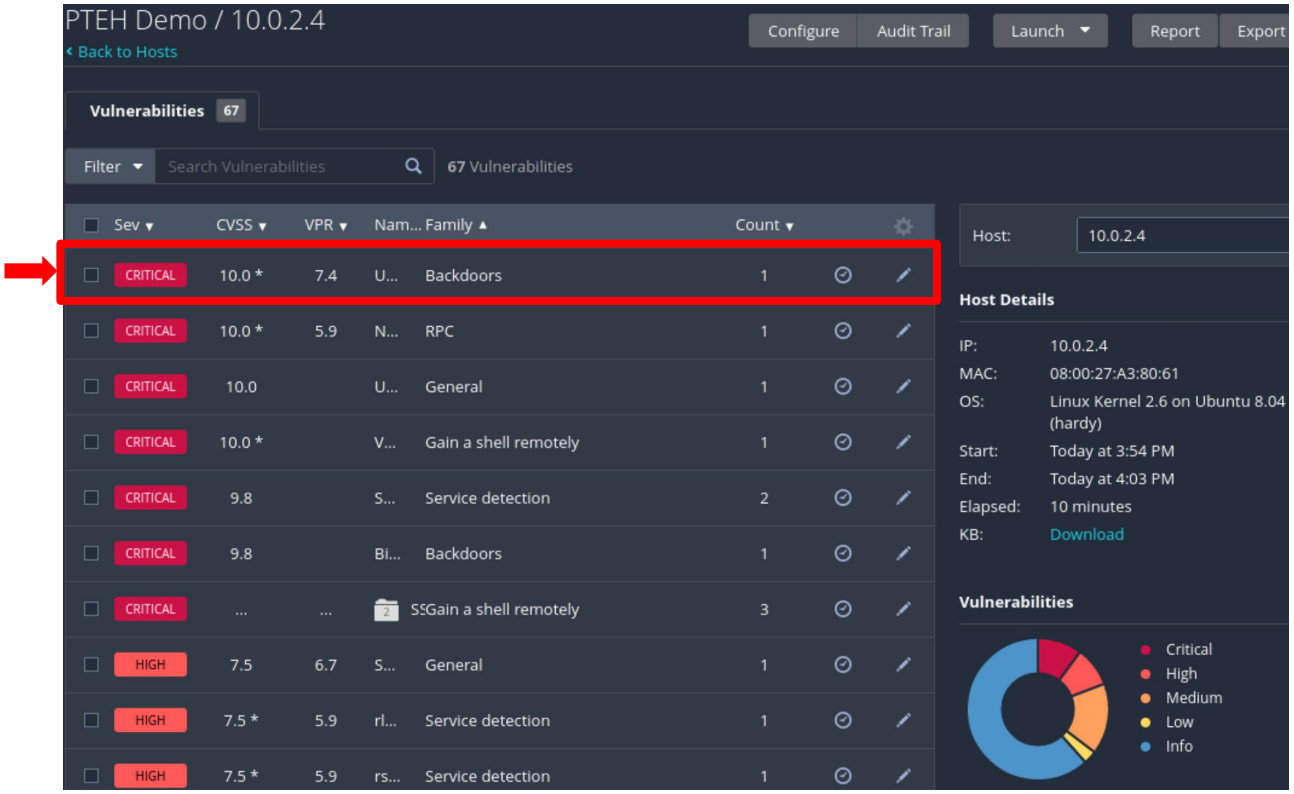
- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`Count`**

Output parziale



Analisi Automatica delle Vulnerabilità
Nessus – Basic Network Scan – Esempio 1 (MS 2)

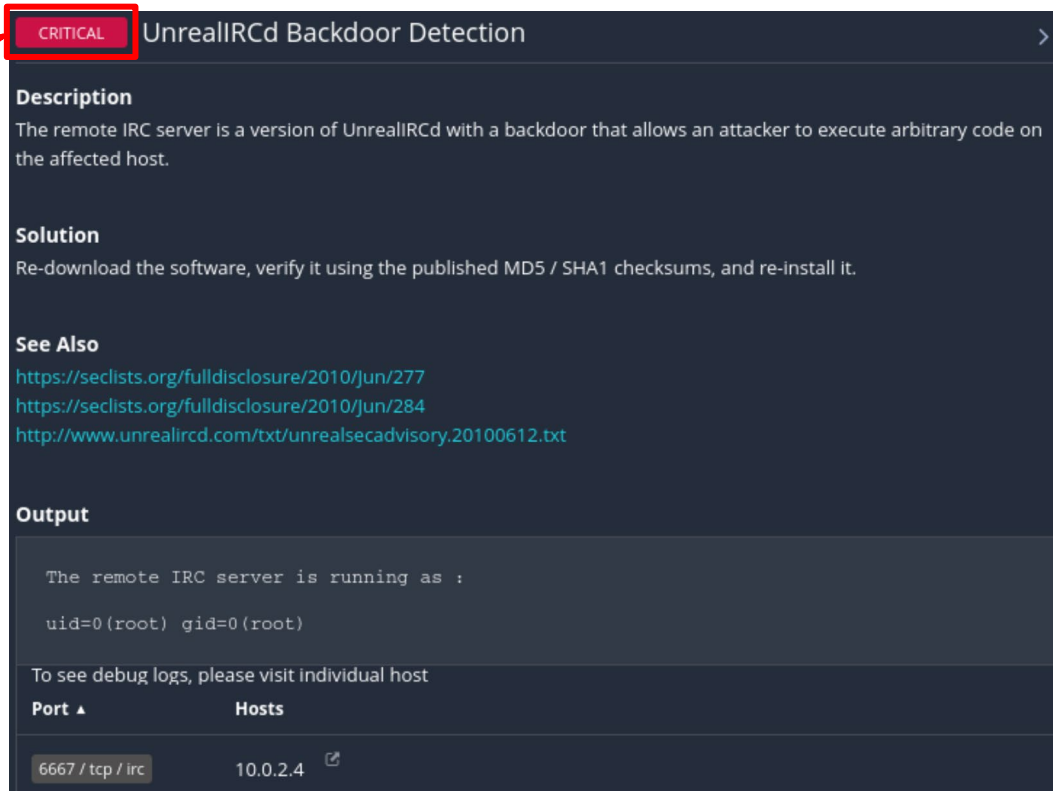
- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`UnrealIRCd Backdoor Detection`** (**`Backdoor`**)



Analisi Automatica delle Vulnerabilità
Nessus – Basic Network Scan – Esempio 1 (MS 2)

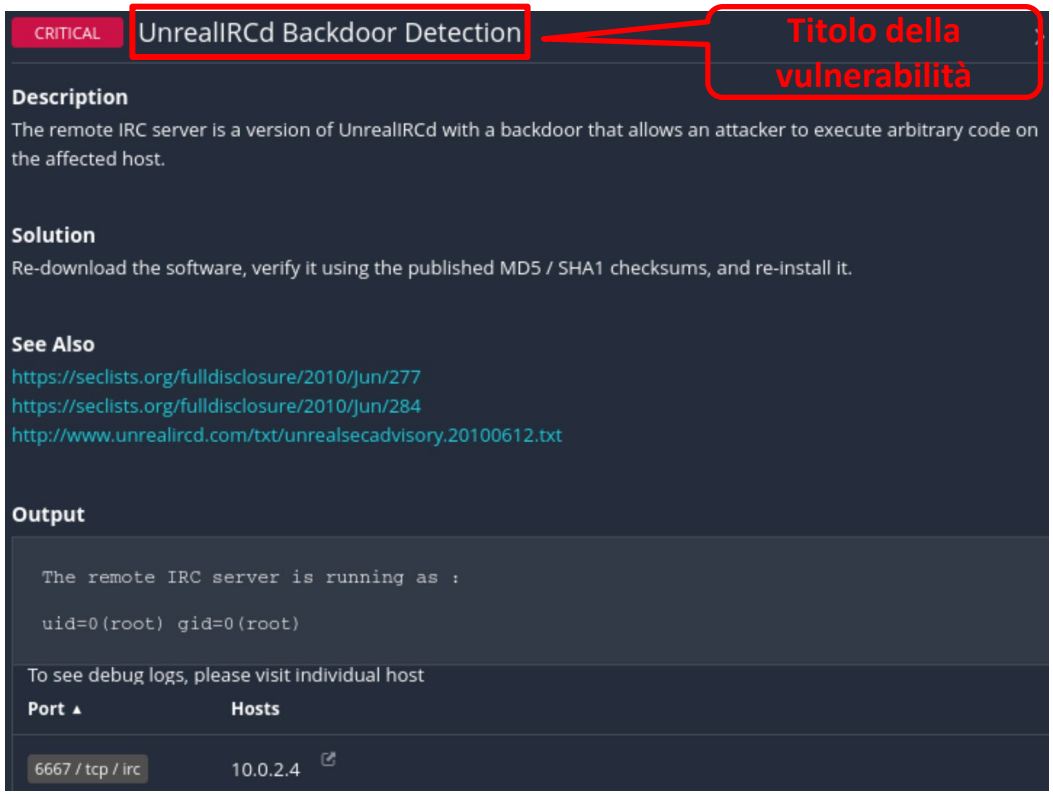
- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`UnrealIRCd Backdoor Detection`** (**`Backdoor`**)

Livello di Severity dalla vulnerabilità



Analisi Automatica delle Vulnerabilità
Nessus – Basic Network Scan – Esempio 1 (MS 2)

- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`UnrealIRCd Backdoor Detection`** (**`Backdoor`**)

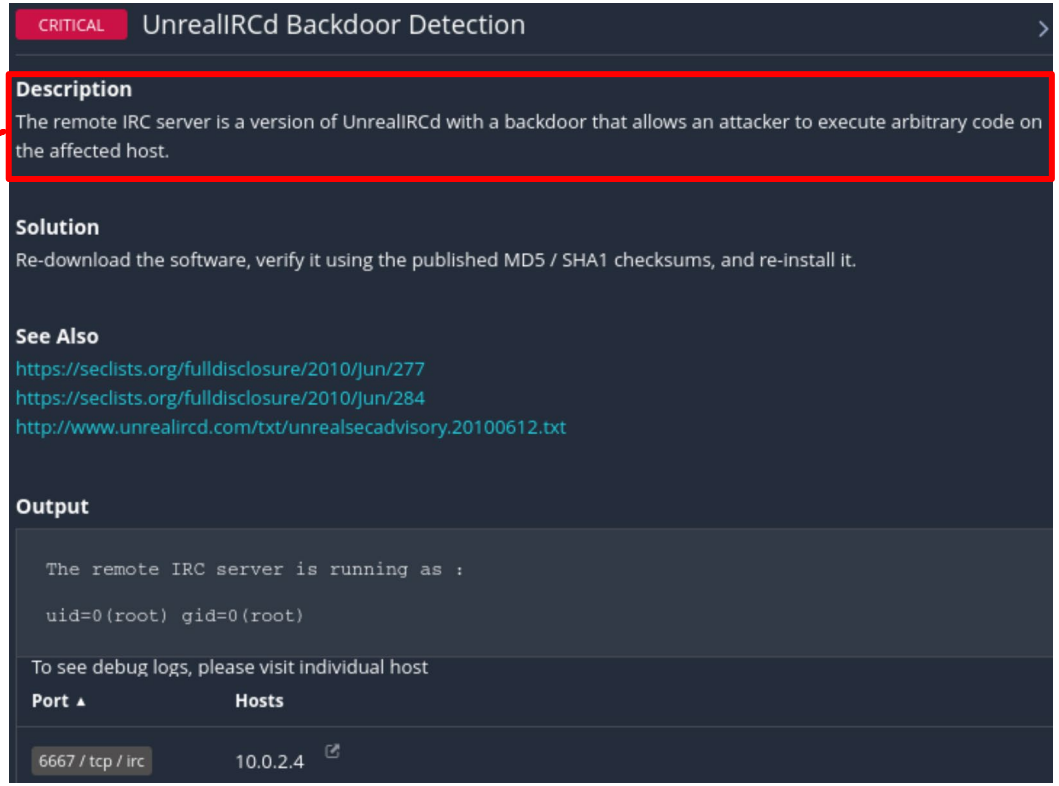


Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Esempio 1 (MS 2)

- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`UnrealIRCd Backdoor Detection`** (**`Backdoor`**)

Descrizione della vulnerabilità

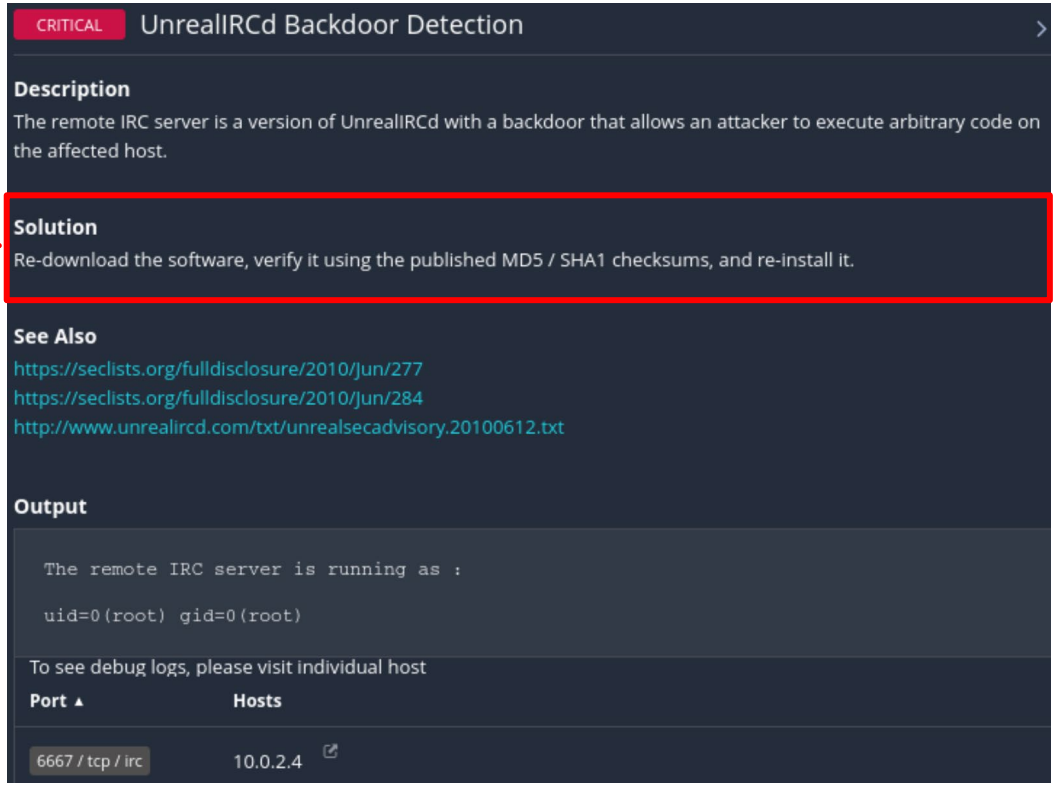


Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Esempio 1 (MS 2)

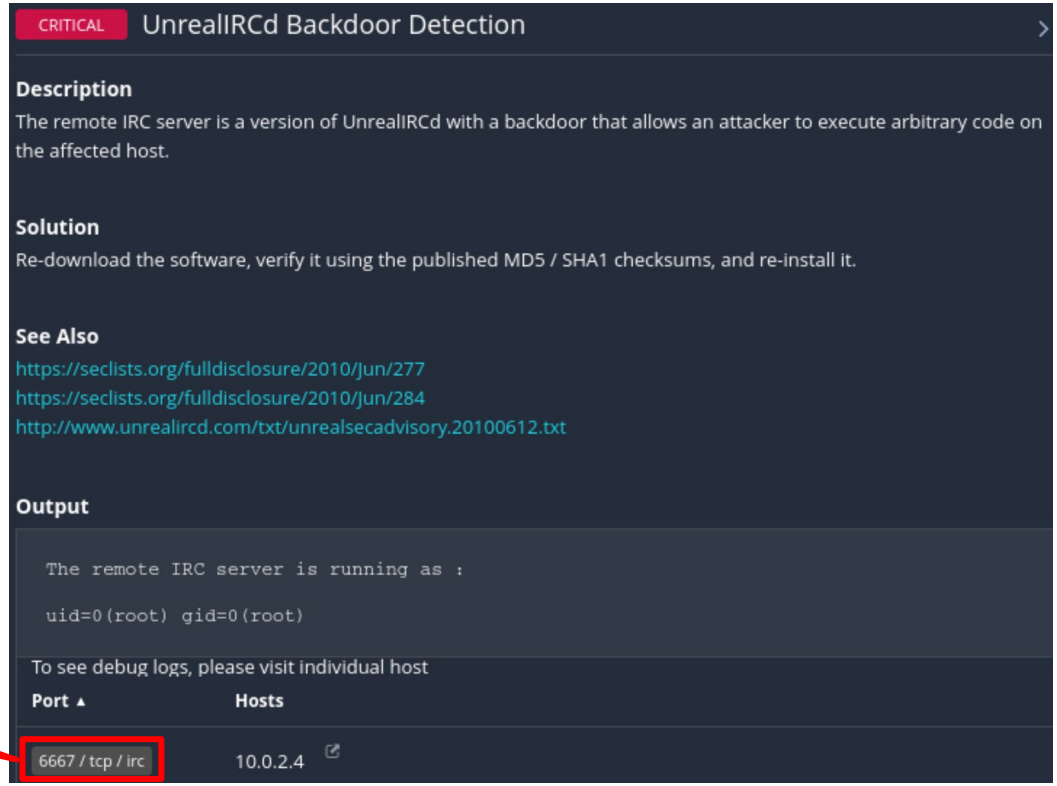
- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`UnrealIRCd Backdoor Detection`** (**`Backdoor`**)

Soluzione o mitigazione della vulnerabilità



Analisi Automatica delle Vulnerabilità
Nessus – Basic Network Scan – Esempio 1 (MS 2)

- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`UnrealIRCd Backdoor Detection`** (**`Backdoor`**)



Porta impattata dalla vulnerabilità

Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Esempio 1 (MS 2)

- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`UnrealIRCd Backdoor Detection`** (**`Backdoor`**)

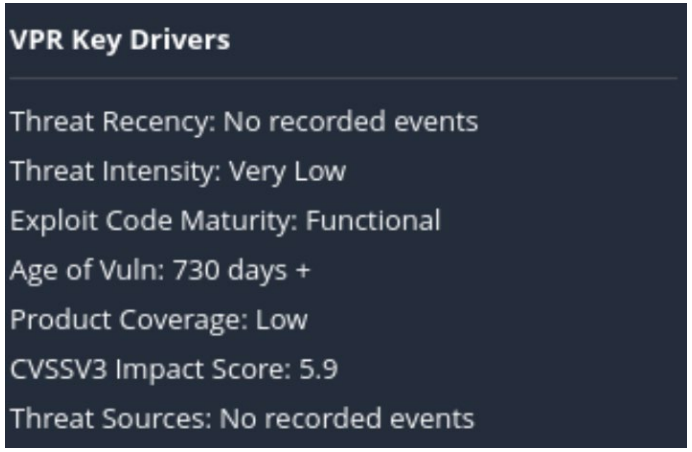
Plugin Details

Severity:	Critical
ID:	46882
Version:	1.16
Type:	remote
Family:	Backdoors
Published:	June 14, 2010
Modified:	April 11, 2022

Plugin che ha rilevato la vulnerabilità

Analisi Automatica delle Vulnerabilità
Nessus – Basic Network Scan – Esempio 1 (MS 2)

- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`UnrealIRCd Backdoor Detection`** (**`Backdoor`**)



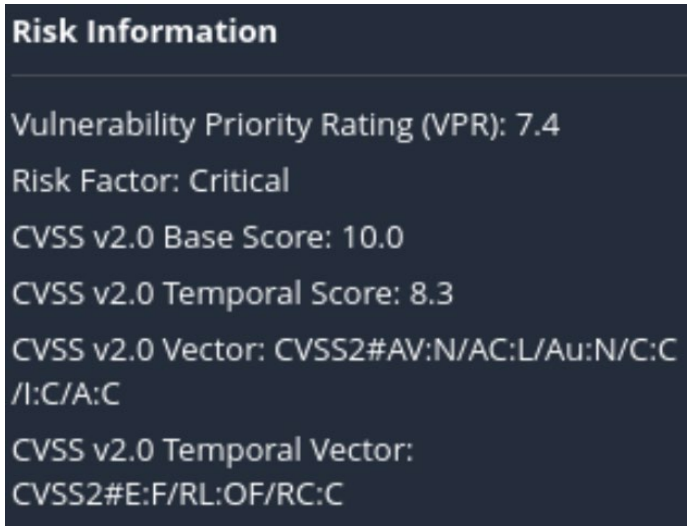
- **Il `Vulnerability Priority Rating` (`VPR`) determina con quanta urgenza si deve porre rimedio alla vulnerabilità**
- **I `VPR Key Drivers` sono gli elementi su cui si basa il livello di prioritizzazione della vulnerabilità**

`https://developer.tenable.com/docs/vpr-drivers-tio`

Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Esempio 1 (MS 2)

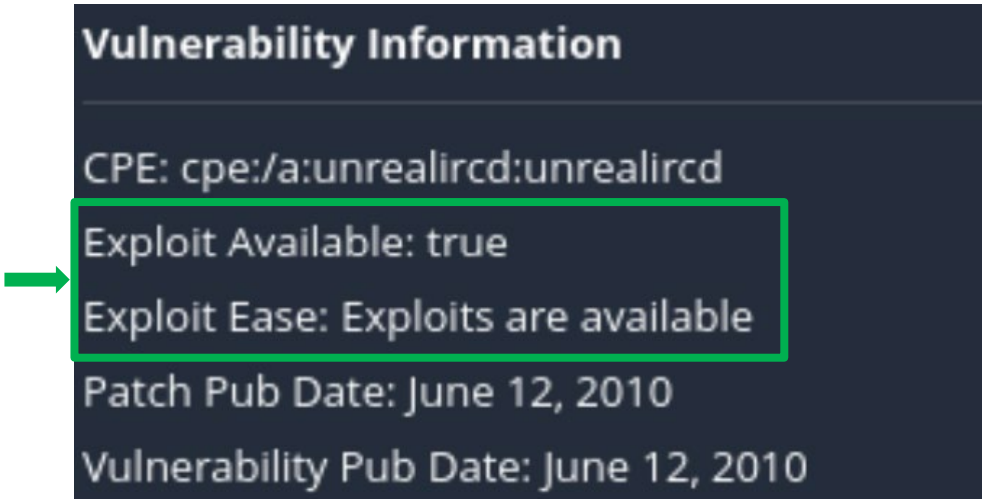
- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`UnrealIRCd Backdoor Detection`** (**`Backdoor`**)



Rischio relativo alla vulnerabilità

Analisi Automatica delle Vulnerabilità
Nessus – Basic Network Scan – Esempio 1 (MS 2)

- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`UnrealIRCd Backdoor Detection`** (**`Backdoor`**)

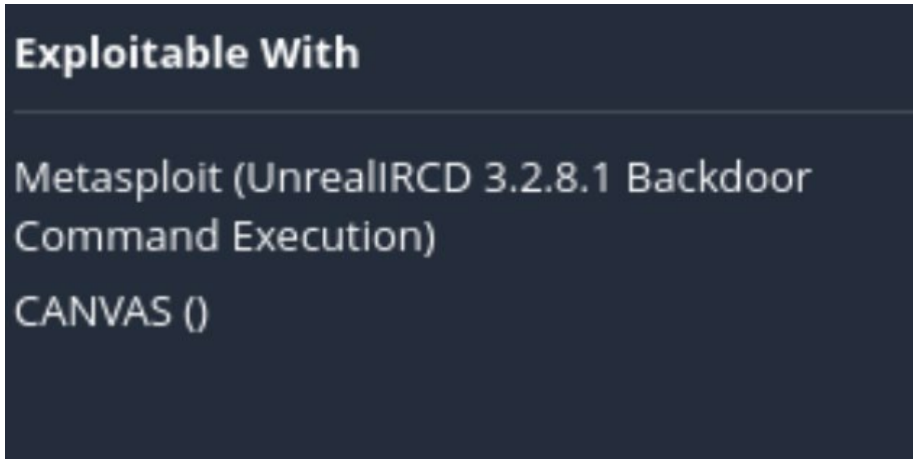


Ulteriori informazioni relative alla vulnerabilità ed alla sua «sfruttabilità»

Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Esempio 1 (MS 2)

- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`UnrealIRCd Backdoor Detection`** (**`Backdoor`**)



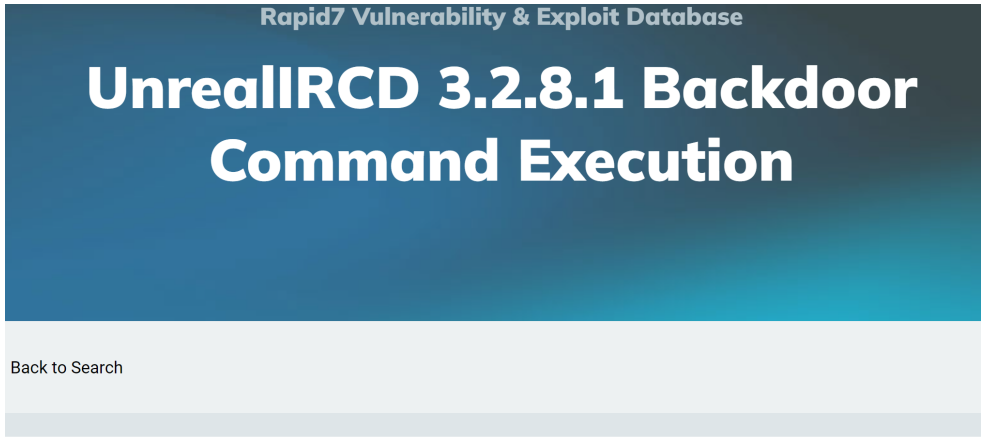
Strumento (e modulo) per sfruttare la vulnerabilità

Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Esempio 1 (MS 2)

- https://www.rapid7.com/db/modules/exploit/unix/irc/unreal_ircd_3281_backdoor/

Modulo Metasploit per sfruttare la vulnerabilità



UnrealIRCD 3.2.8.1 Backdoor Command Execution

Disclosed	Created
06/12/2010	05/30/2018

Description

This module exploits a malicious backdoor that was added to the Unreal IRCD 3.2.8.1 download archive. This backdoor was present in the Unreal3.2.8.1.tar.gz archive between November 2009 and June 12th 2010.

Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Esempio 1 (MS 2)

- https://www.rapid7.com/db/modules/exploit/unix/irc/unreal_ircd_3281_backdoor/

Development

- Source Code
- History

Modulo Metasploit per sfruttare la vulnerabilità

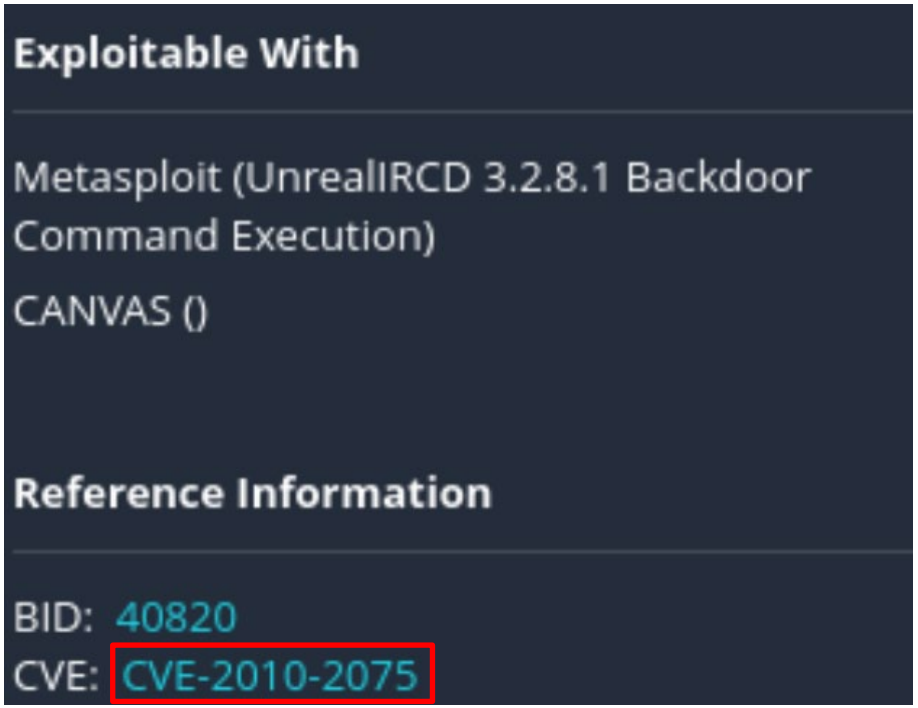
Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unreal_ircd_3281_backdoor) > show targets
    ...targets...
msf exploit(unreal_ircd_3281_backdoor) > set TARGET < target-id >
msf exploit(unreal_ircd_3281_backdoor) > show options
    ...show and set options...
msf exploit(unreal_ircd_3281_backdoor) > exploit
```

Analisi Automatica delle Vulnerabilità
Nessus – Basic Network Scan – Esempio 1 (MS 2)

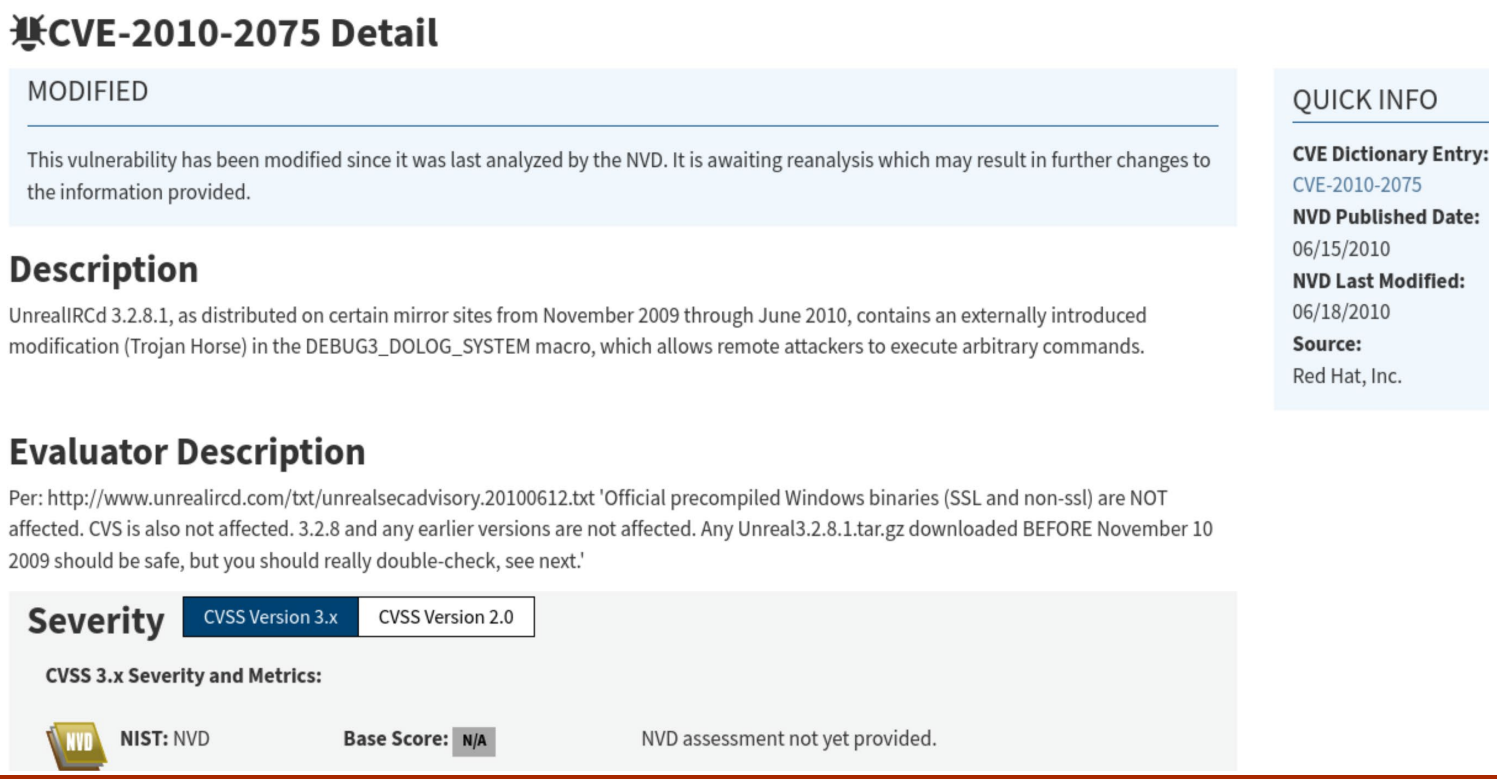
- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`UnrealIRCd Backdoor Detection`** (**`Backdoor`**)



Eventuali riferimenti a tassonomie

Analisi Automatica delle Vulnerabilità
Nessus – Basic Network Scan – Esempio 1 (MS 2)

- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`UnrealIRCd Backdoor Detection`** (**`Backdoor`**)



CVE-2010-2075 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

UnrealIRCd 3.2.8.1, as distributed on certain mirror sites from November 2009 through June 2010, contains an externally introduced modification (Trojan Horse) in the DEBUG3_DOLOG_SYSTEM macro, which allows remote attackers to execute arbitrary commands.

Evaluator Description

Per: http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt 'Official precompiled Windows binaries (SSL and non-ssl) are NOT affected. CVS is also not affected. 3.2.8 and any earlier versions are not affected. Any Unreal3.2.8.1.tar.gz downloaded BEFORE November 10 2009 should be safe, but you should really double-check, see next.'

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NVD **NIST:** NVD **Base Score:** N/A NVD assessment not yet provided.

QUICK INFO

CVE Dictionary Entry: CVE-2010-2075
NVD Published Date: 06/15/2010
NVD Last Modified: 06/18/2010
Source: Red Hat, Inc.

Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Esempio 1 (MS 2)

- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`UnrealIRCd Backdoor Detection`** (**`Backdoor`**)

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
http://seclists.org/fulldisclosure/2010/Jun/277	
http://seclists.org/fulldisclosure/2010/Jun/284	
http://security.gentoo.org/glsa/glsa-201006-21.xml	
http://www.exploit-db.com/exploits/13853	
http://www.openwall.com/lists/oss-security/2010/06/14/11	
http://www.securityfocus.com/bid/40820	Exploit
http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt	Vendor Advisory
http://www.vupen.com/english/advisories/2010/1437	Vendor Advisory

Analisi Automatica delle Vulnerabilità
Nessus – Basic Network Scan – Esempio 1 (MS 2)

- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`UnrealIRCd Backdoor Detection`** (**`Backdoor`**)

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-20	Improper Input Validation	NIST

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:a:unrealircd:unrealircd:3.2.8.1:*:*:*:*:*:*:*

Show Matching CPE(s)

Denotes Vulnerable Software

Are we missing a CPE here? Please let us know.

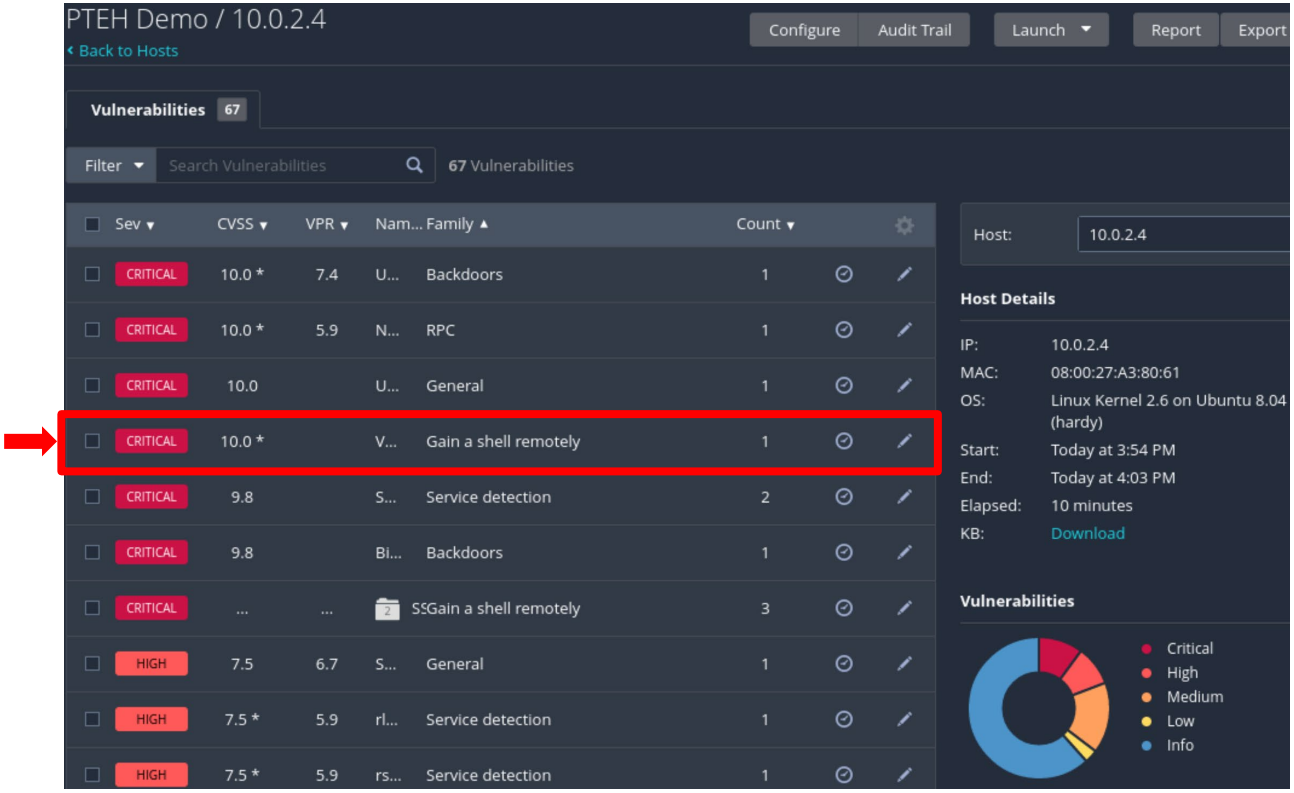
Change History

1 change records found show changes

Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Esempio 2 (MS 2)

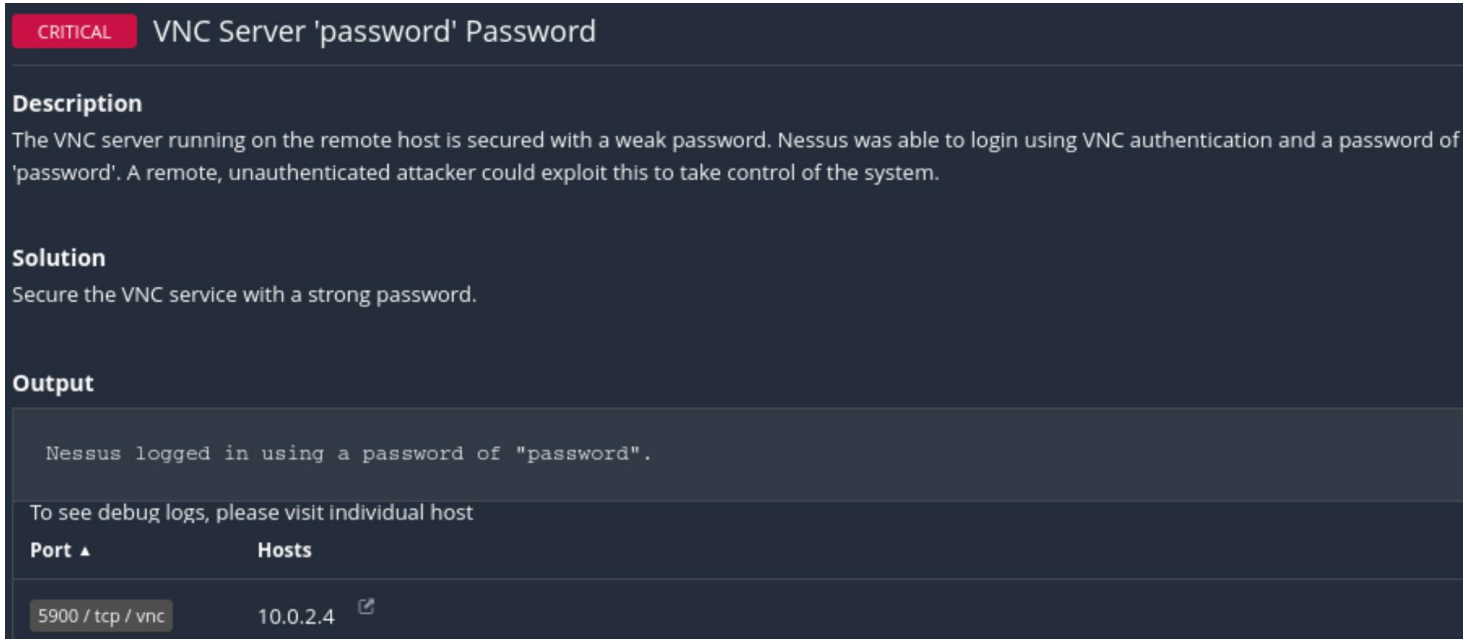
- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`VNC Server 'password' Password`**(**`Gain a shell remotely`**)



Analisi Automatica delle Vulnerabilità

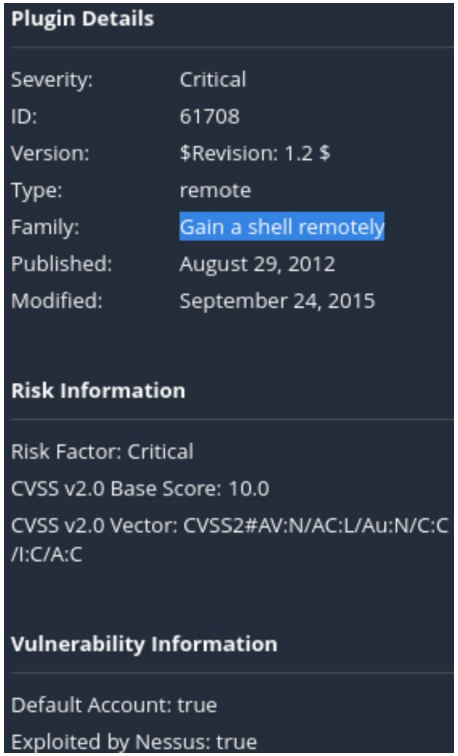
Nessus – Basic Network Scan – Esempio 2 (MS 2)

- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`VNC Server 'password' Password`**(**`Gain a shell remotely`**)



Analisi Automatica delle Vulnerabilità
Nessus – Basic Network Scan – Esempio 2 (MS 2)

- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`VNC Server 'password' Password`**(**`Gain a shell remotely`**)



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

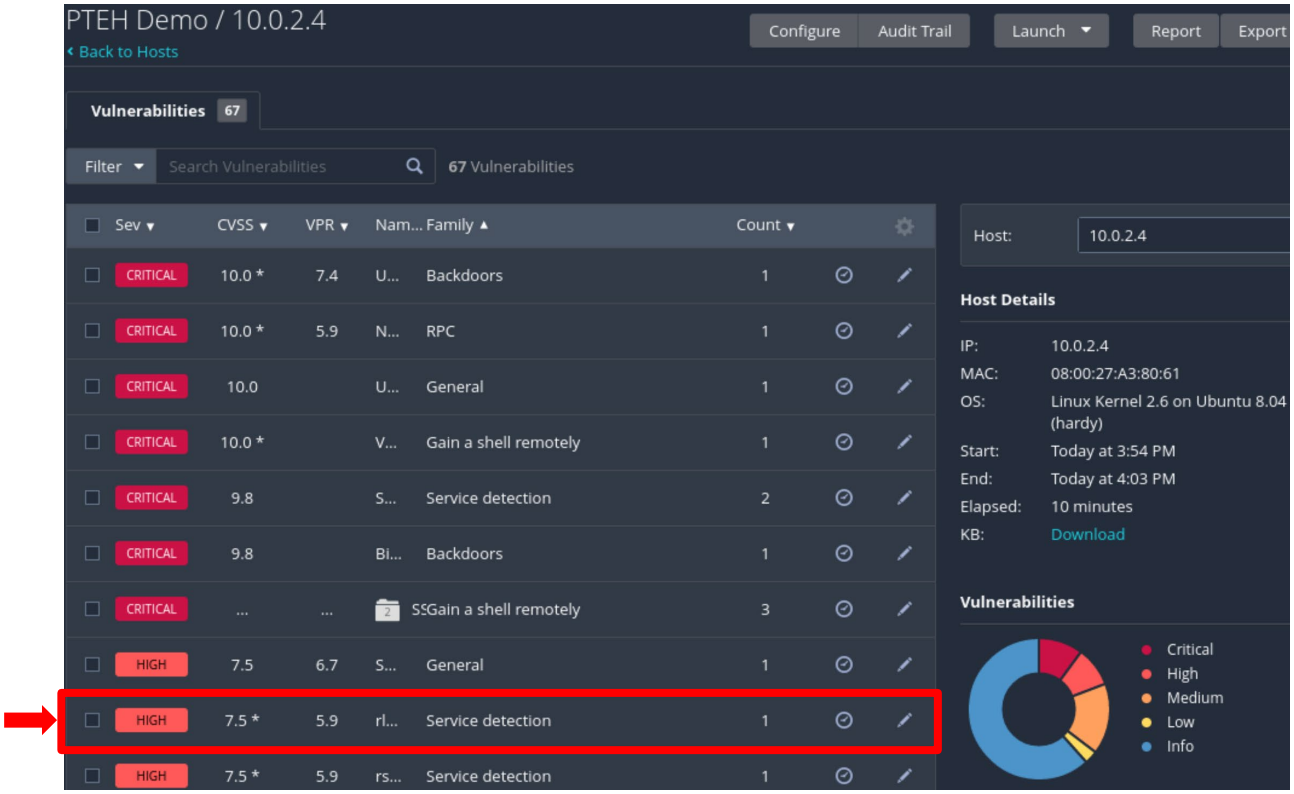
Vulnerability Information

Default Account: true

Exploited by Nessus: true

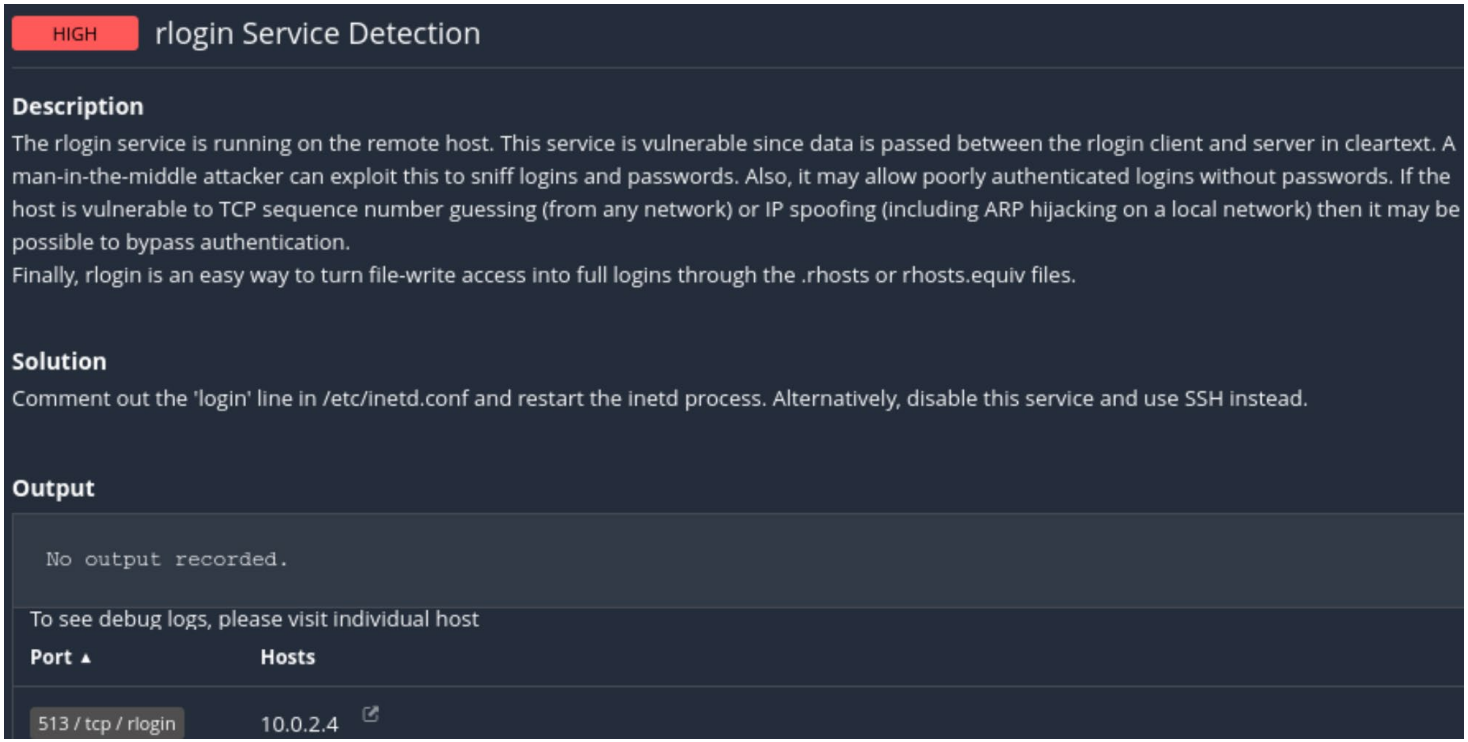
Analisi Automatica delle Vulnerabilità
Nessus – Basic Network Scan – Esempio 3 (MS 2)

- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`rlogin Service Detection`**(**`Service detection`**)



Analisi Automatica delle Vulnerabilità
Nessus – Basic Network Scan – Esempio 3 (MS 2)

- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`rlogin Service Detection`**(**`Service detection`**)



Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Esempio 3 (MS 2)

- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`rlogin Service Detection`**(**`Service detection`**)

Plugin Details

Severity:	High
ID:	10205
Version:	1.36
Type:	remote
Family:	Service detection
Published:	August 30, 1999
Modified:	April 11, 2022

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: Low
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 5.9
Risk Factor: High
CVSS v2.0 Base Score: 7.5
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

Vulnerability Information

Exploit Available: true
Exploit Ease: Exploits are available
Vulnerability Pub Date: January 1, 1990

Exploitable With

Metasploit (rlogin Authentication Scanner)

Reference Information

CVE: CVE-1999-0651

Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Esempio 3 (MS 2)

- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`rlogin Service Detection`**(**`Service detection`**)

rlogin Authentication Scanner

Created
05/30/2018

Description

This module will test an rlogin service on a range of machines and report successful logins. NOTE: This module requires access to bind to privileged ports (below 1024).

Author(s)

- jduck <jduck@metasploit.com>

Modulo Metasploit per sfruttare la vulnerabilità

Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Esempio 3 (MS 2)

- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`rlogin Service Detection (Service detection)`**

Development

- Source Code
- History

Modulo Metasploit per sfruttare la vulnerabilità

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use auxiliary/scanner/rservices/rlogin_login
msf auxiliary(rlogin_login) > show actions
    ...actions...
msf auxiliary(rlogin_login) > set ACTION < action-name >
msf auxiliary(rlogin_login) > show options
    ...show and set options...
msf auxiliary(rlogin_login) > run
```

Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Esempio 3 (MS 2)

- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`rlogin Service Detection`**(**`Service detection`**)

Plugin Details

Severity:	High
ID:	10205
Version:	1.36
Type:	remote
Family:	Service detection
Published:	August 30, 1999
Modified:	April 11, 2022

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: Low
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 5.9
Risk Factor: High
CVSS v2.0 Base Score: 7.5
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

Vulnerability Information

Exploit Available: true
Exploit Ease: Exploits are available
Vulnerability Pub Date: January 1, 1990

Exploitable With

Metasploit (rlogin Authentication Scanner)

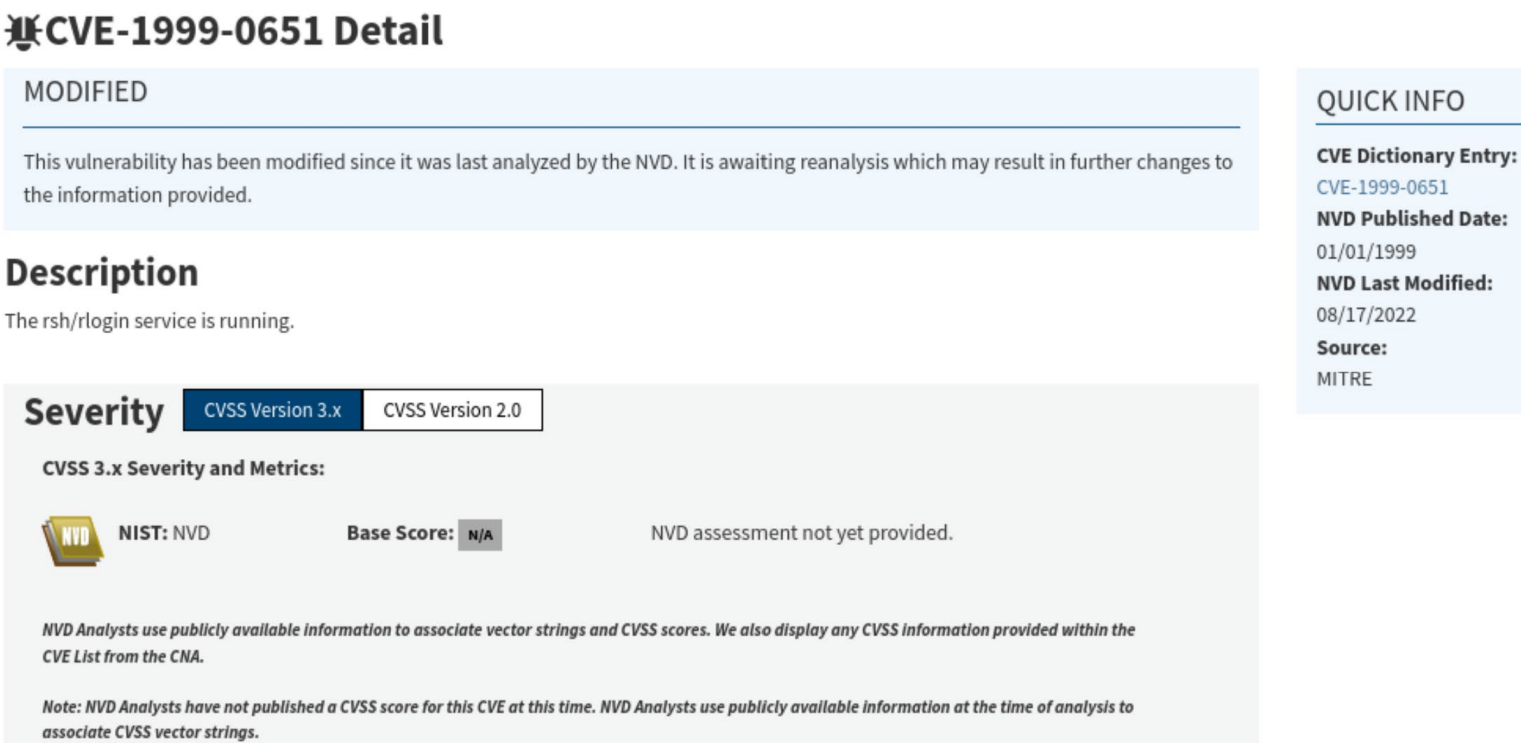
Reference Information

CVE: CVE-1999-0651

Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Esempio 3 (MS 2)

- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`rlogin Service Detection`**(**`Service detection`**)



CVE-1999-0651 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

The rsh/rlogin service is running.

Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** N/A NVD assessment not yet provided.

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have not published a CVSS score for this CVE at this time. NVD Analysts use publicly available information at the time of analysis to associate CVSS vector strings.

QUICK INFO

CVE Dictionary Entry: CVE-1999-0651
NVD Published Date: 01/01/1999
NVD Last Modified: 08/17/2022
Source: MITRE

Analisi Automatica delle Vulnerabilità
Nessus – Basic Network Scan – Esempio 3 (MS 2)

- Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.4`**
  - **`rlogin Service Detection`**(**`Service detection`**)

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://exchange.xforce.ibmcloud.com/vulnerabilities/2995	

Weakness Enumeration

CWE-ID	CWE Name	Source
NVD-CWE-Other	Other	NIST

Change History

2 change records found show changes

Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Scansione (MS 3)

- Risultati della scansione relativi all'host con indirizzo IP **10.0.2.9**
  - Dati riguardanti la macchina target (Metasploitable 3 – MS3)

- **Vulnerabilità relative all'host con indirizzo IP: 10.0.2.9**
  - **6 vulnerabilità di livello *Critico***
  - **7 vulnerabilità di livello *Alto***
  - **15 vulnerabilità di livello *Medio***
  - **2 vulnerabilità di livello *Basso***

Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Esempio (MS 3)

- Vulnerabilità **`Zohocorp Manageengine Desktop Central (Multiple Issues)`**

In questo caso saranno presenti varie vulnerabilità relative a `Zohocorp Manageengine Desktop Central` e ciascuna vulnerabilità potrebbe avere un livello di `Severity` diverso

Analisi Automatica delle Vulnerabilità

Nessus – Basic Network Scan – Esempio (MS 3)

- **Zohocorp Manageengine Desktop Central (Multiple Issues)**

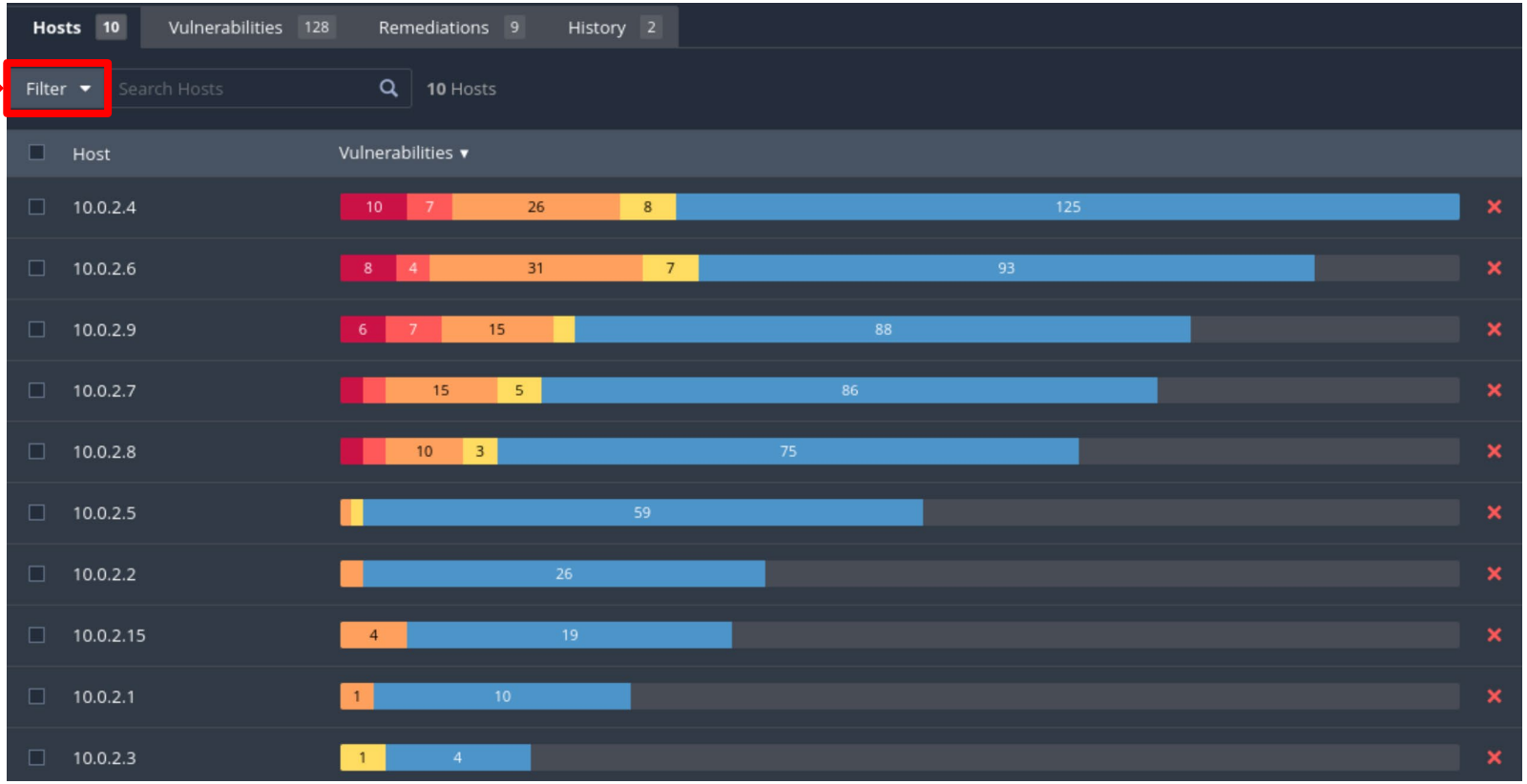
Search Vulnerabilities | 5 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	7.3	ManageEngine Desktop Central 8 / 9 < Build 91100 Multiple RCE	CGI abuses	2
CRITICAL	9.8	5.9	ManageEngine Desktop Central < 10 Build 10.0.533 Integer Overflow	CGI abuses	2
HIGH	8.8	6.7	ManageEngine Desktop Central 10 < Build 100282 Remote Privilege Esc...	CGI abuses	2
MEDIUM	6.1	3.0	ManageEngine Desktop Central 9 < Build 92027 Multiple Vulnerabilities	CGI abuses	2
INFO			ManageEngine Endpoint Central Detection	CGI abuses	2

Analisi Automatica delle Vulnerabilità

Nessus – Risultati di una Scansione (Filtri)

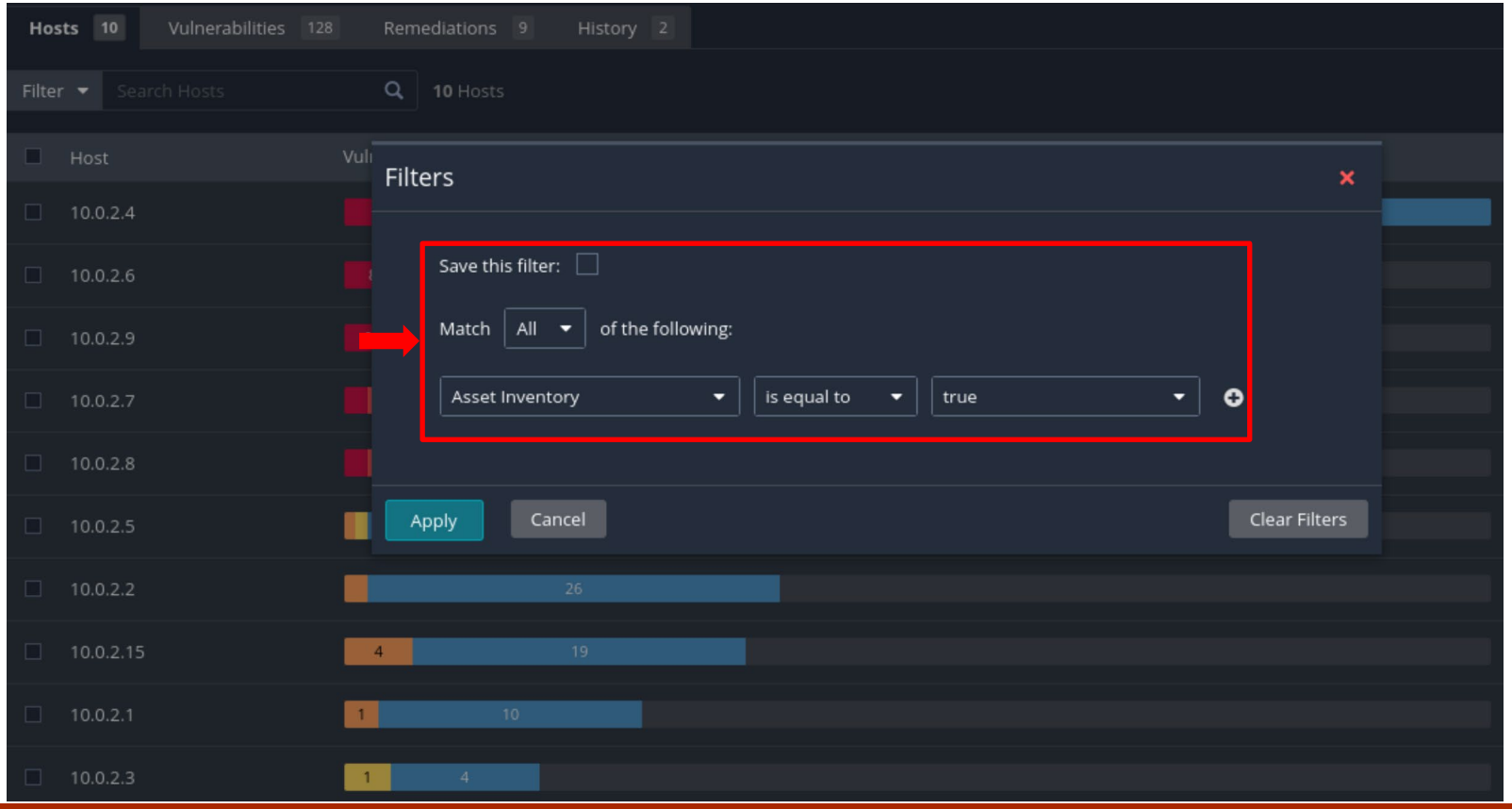
- È possibile «filtrare» i risultati prodotti da una scansione



Analisi Automatica delle Vulnerabilità

Nessus – Risultati di una Scansione (Filtri)

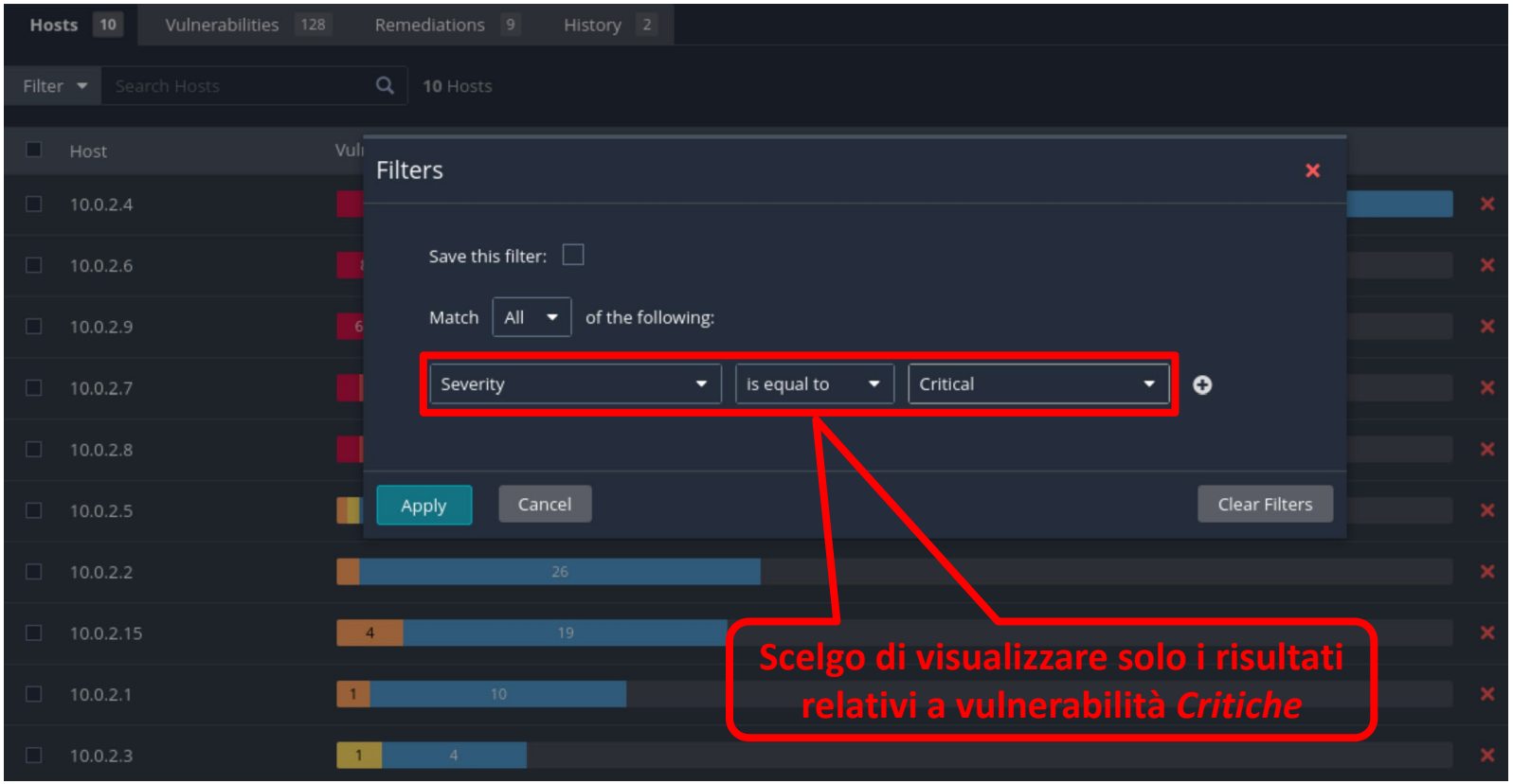
- È possibile «filtrare» i risultati prodotti da una scansione



Analisi Automatica delle Vulnerabilità

Nessus – Risultati di una Scansione (Filtri) – Esempio 1

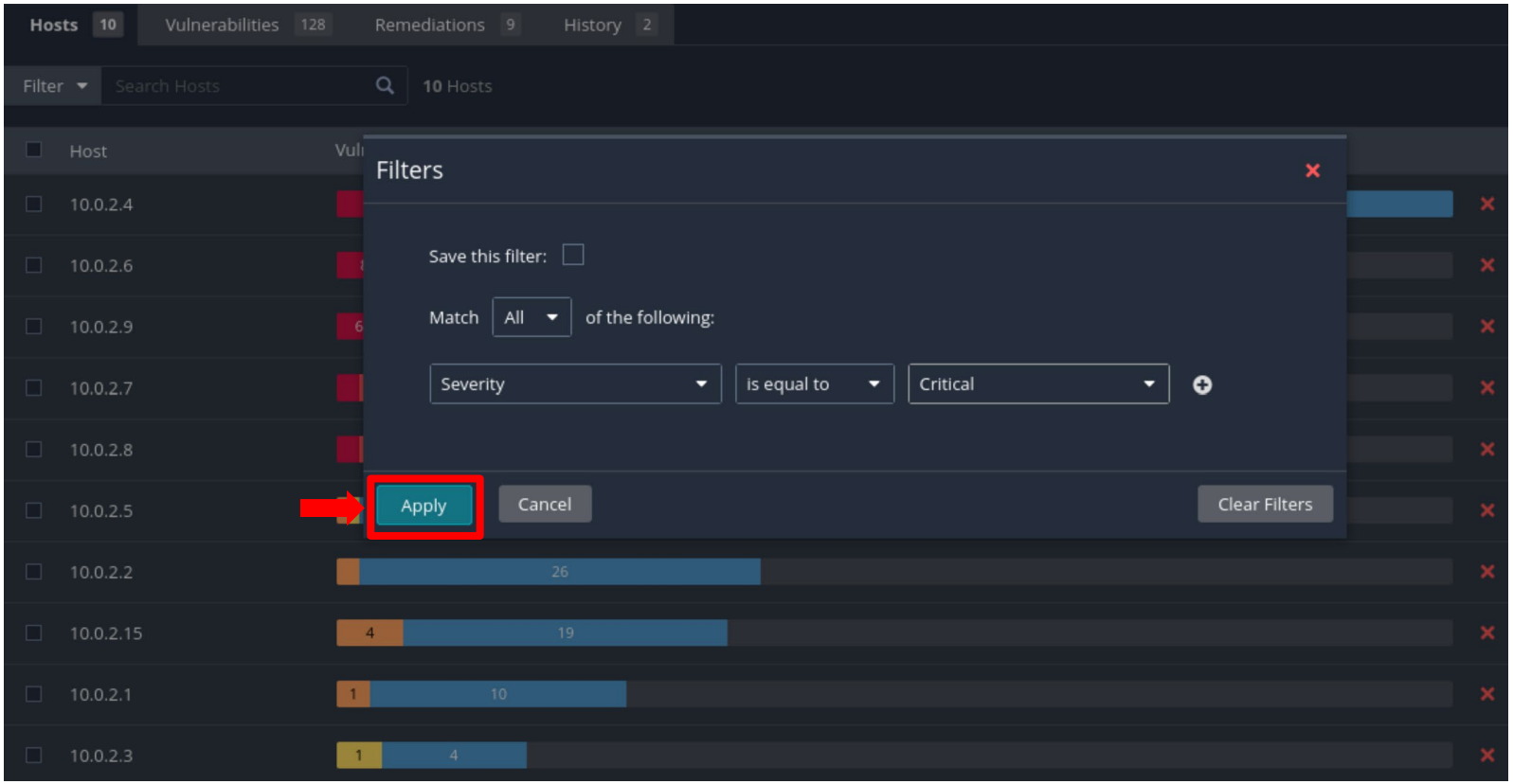
- È possibile «filtrare» i risultati prodotti da una scansione



Analisi Automatica delle Vulnerabilità

Nessus – Risultati di una Scansione (Filtri) – Esempio 1

- È possibile «filtrare» i risultati prodotti da una scansione



Analisi Automatica delle Vulnerabilità

Nessus – Risultati di una Scansione (Filtri) – Esempio 1

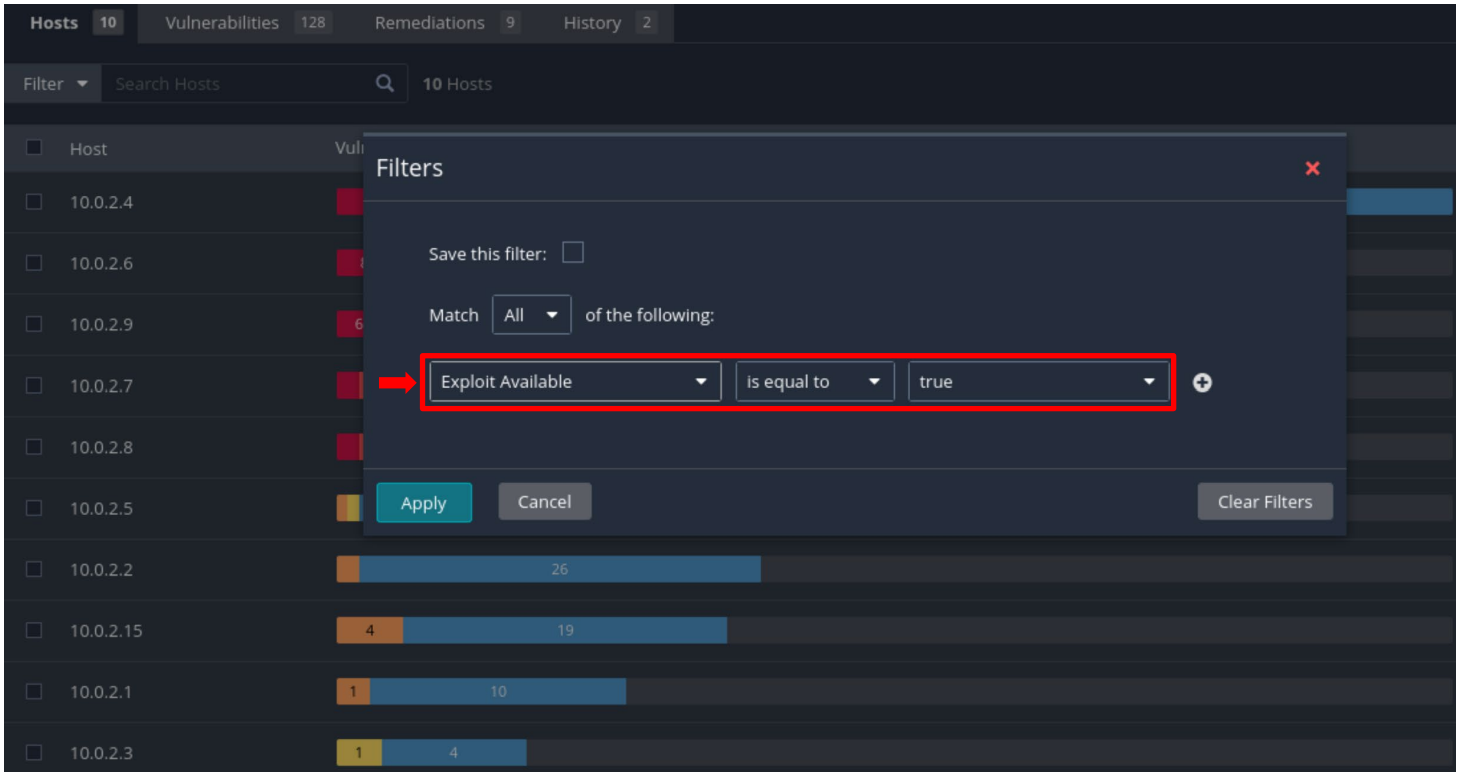
- È possibile «filtrare» i risultati prodotti da una scansione

Vulnerabilità *Critiche* relative a tutti gli host scansionati

Analisi Automatica delle Vulnerabilità

Nessus – Risultati di una Scansione (Filtri) – Esempio 2

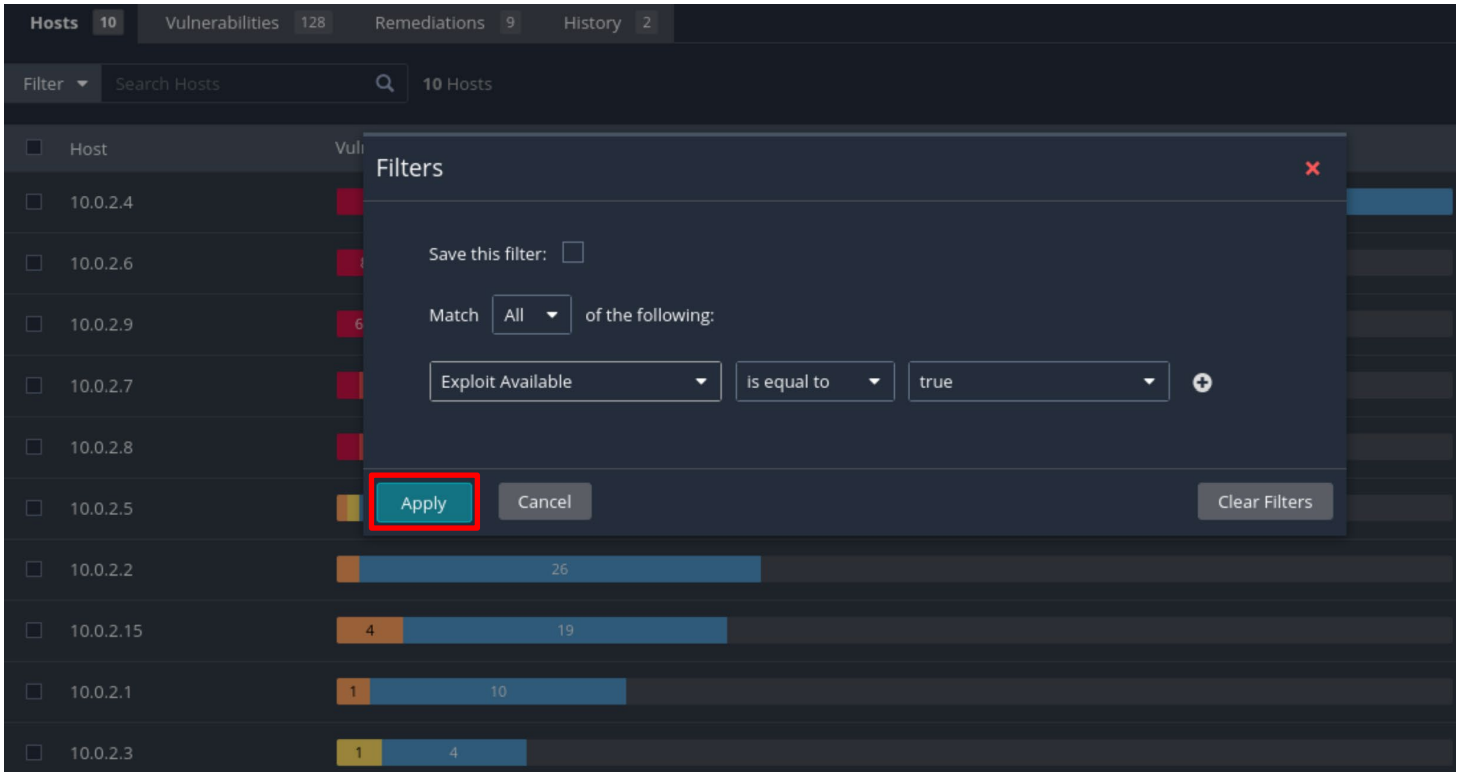
- Ad esempio, Nessus permette di mostrare solo le vulnerabilità per le quali esistono i relativi exploit



Analisi Automatica delle Vulnerabilità

Nessus – Risultati di una Scansione (Filtri) – Esempio 2

- Ad esempio, Nessus permette di mostrare solo le vulnerabilità per le quali esistono i relativi exploit



Analisi Automatica delle Vulnerabilità

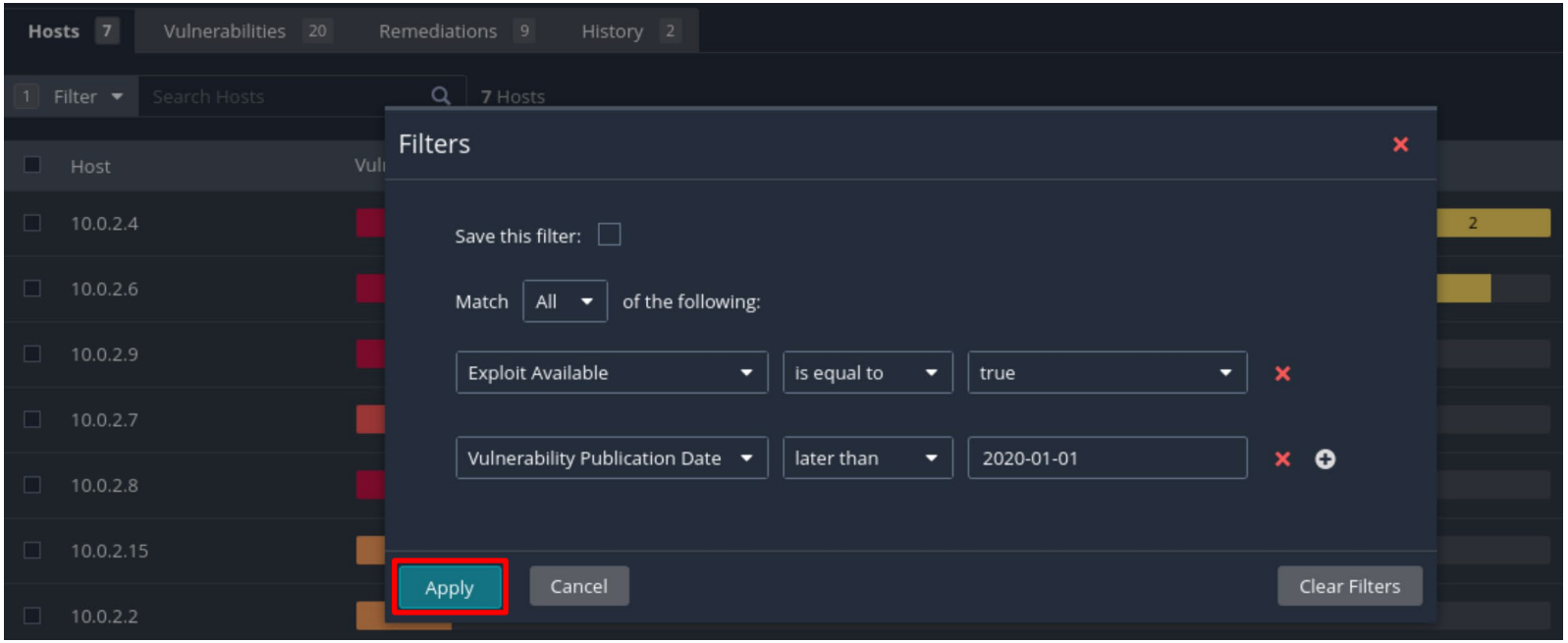
Nessus – Risultati di una Scansione (Filtri) – Esempio 2

- Ad esempio, Nessus permette di mostrare solo le vulnerabilità per le quali esistono i relativi exploit

Analisi Automatica delle Vulnerabilità

Nessus – Risultati di una Scansione (Filtri) – Esempio 3

- Ad esempio, Nessus permette di mostrare solo le vulnerabilità per le quali esistono i relativi exploit



Analisi Automatica delle Vulnerabilità

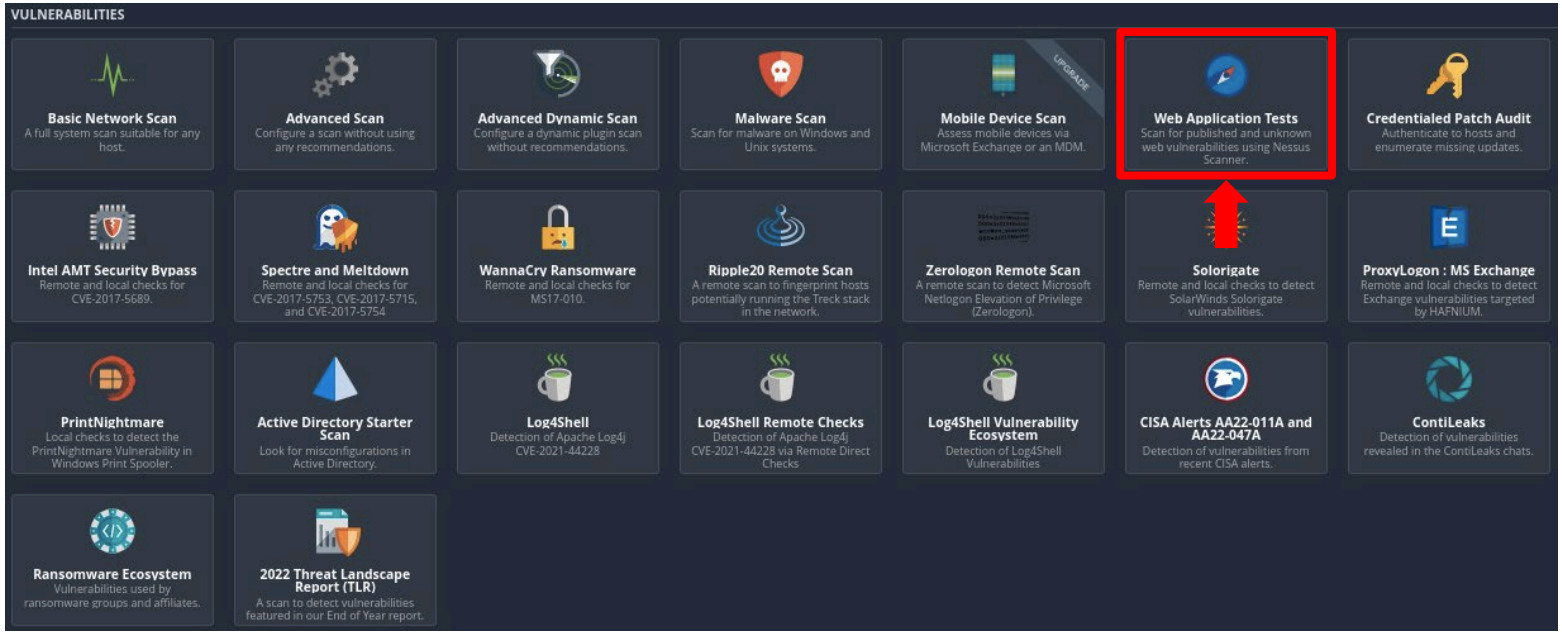
Nessus – Risultati di una Scansione (Filtri) – Esempio 3

- Ad esempio, Nessus permette di mostrare solo le vulnerabilità per le quali esistono i relativi exploit

Analisi Automatica delle Vulnerabilità

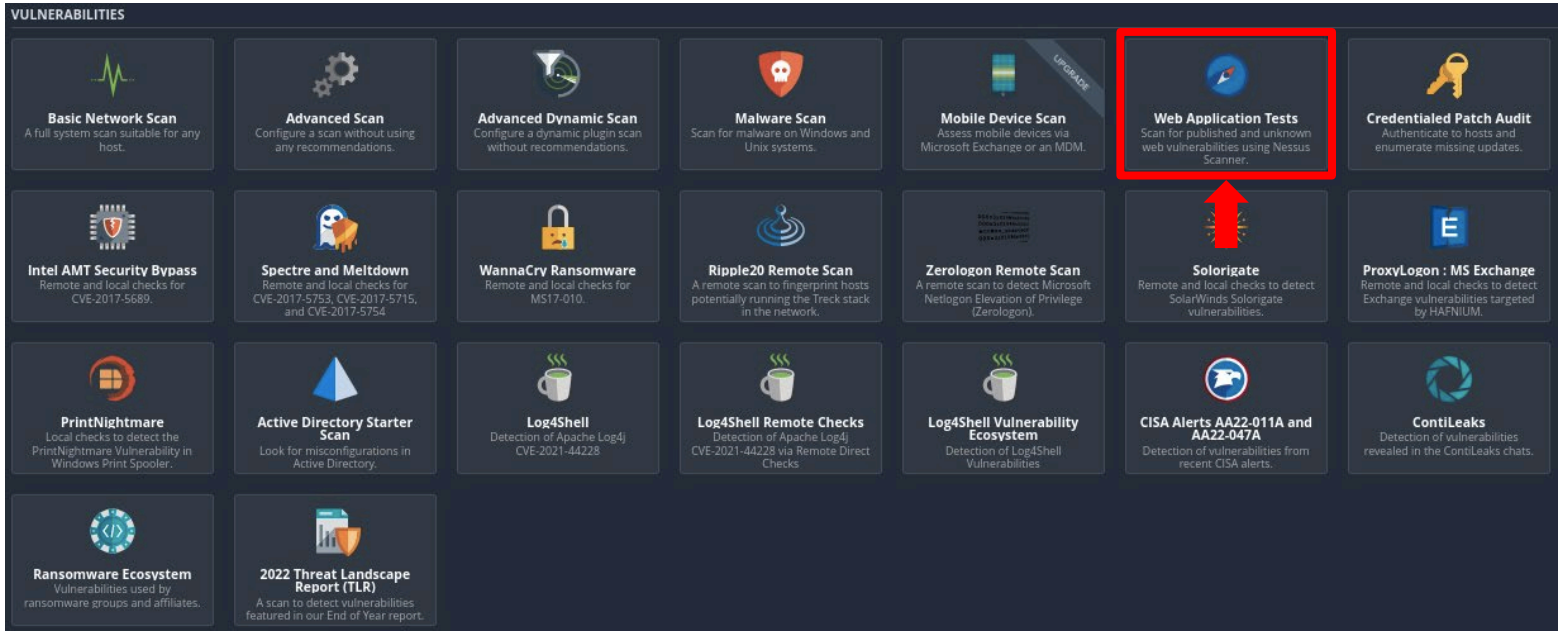
Nessus – Web Application Tests

- Scansione di Applicazioni Web



Analisi Automatica delle Vulnerabilità
Nessus – Web Application Tests

- Scansione di Applicazioni Web

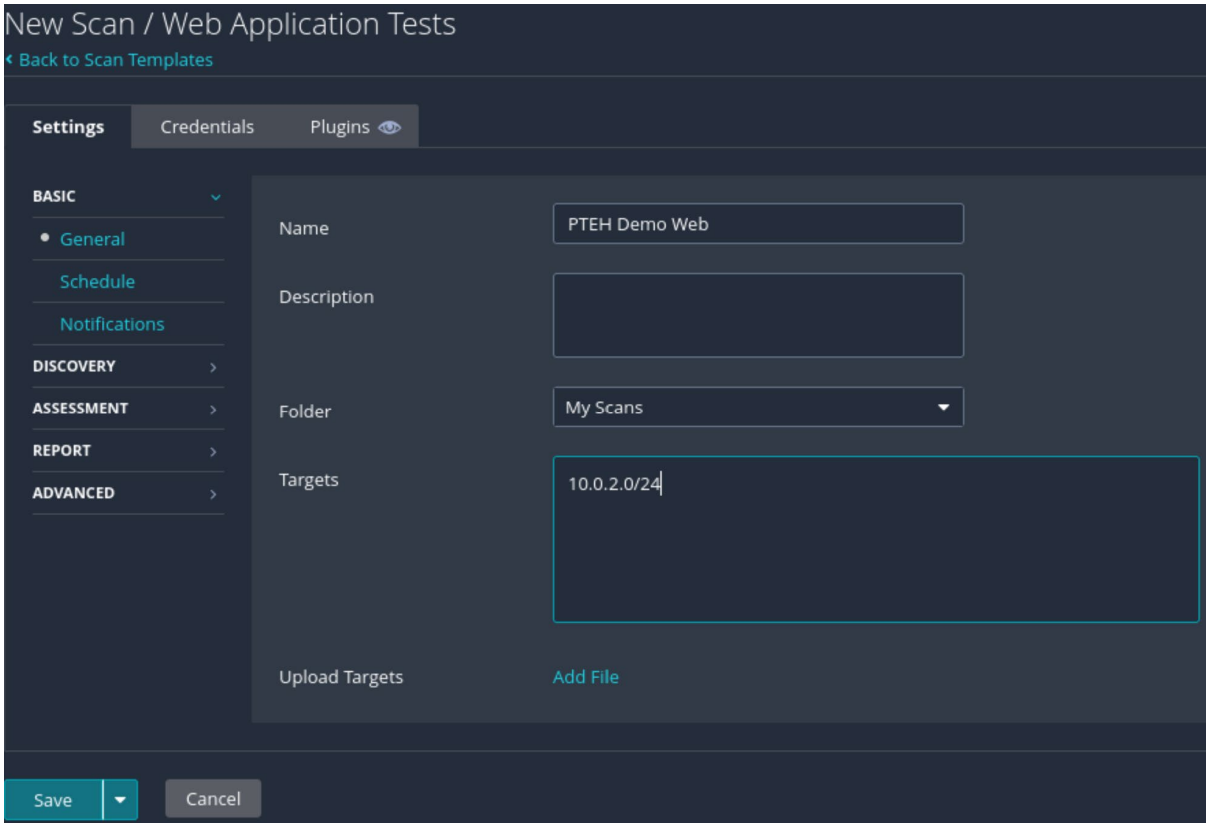


N.B. Tale tipologia di **scansione** dovrebbe essere **sempre utilizzata** quando l'asset utilizza **tecnologie Web-based**

Analisi Automatica delle Vulnerabilità

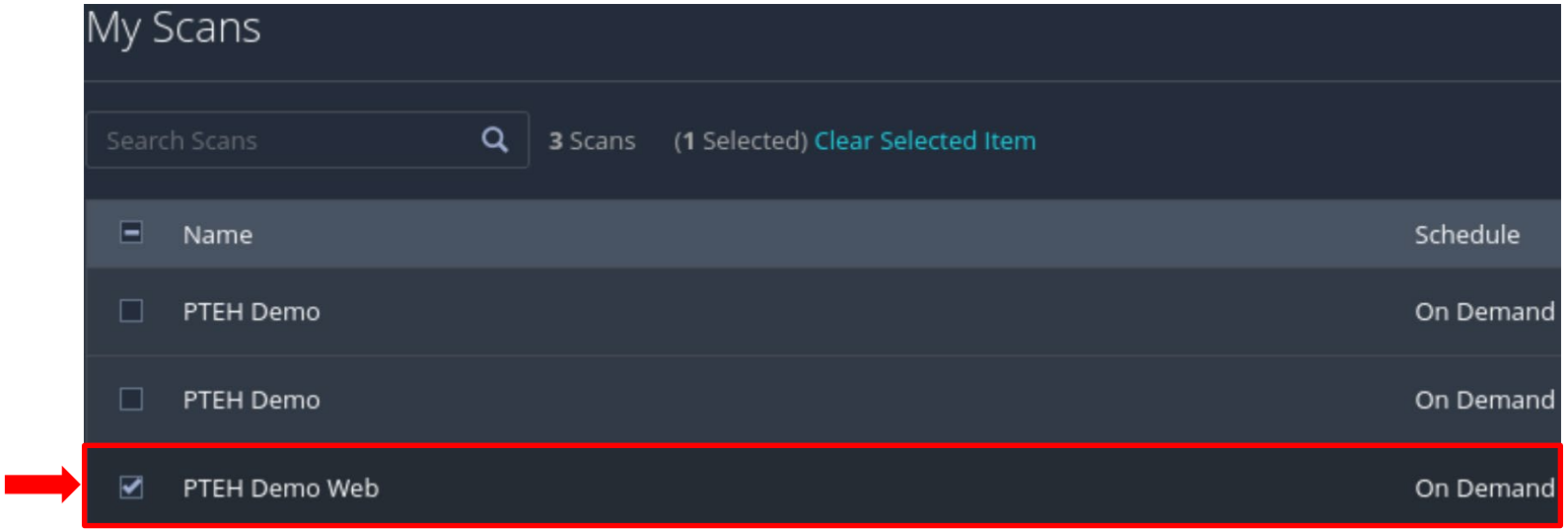
Nessus – Web Application Tests

- Scansione di Applicazioni Web



Analisi Automatica delle Vulnerabilità
Nessus – Web Application Tests

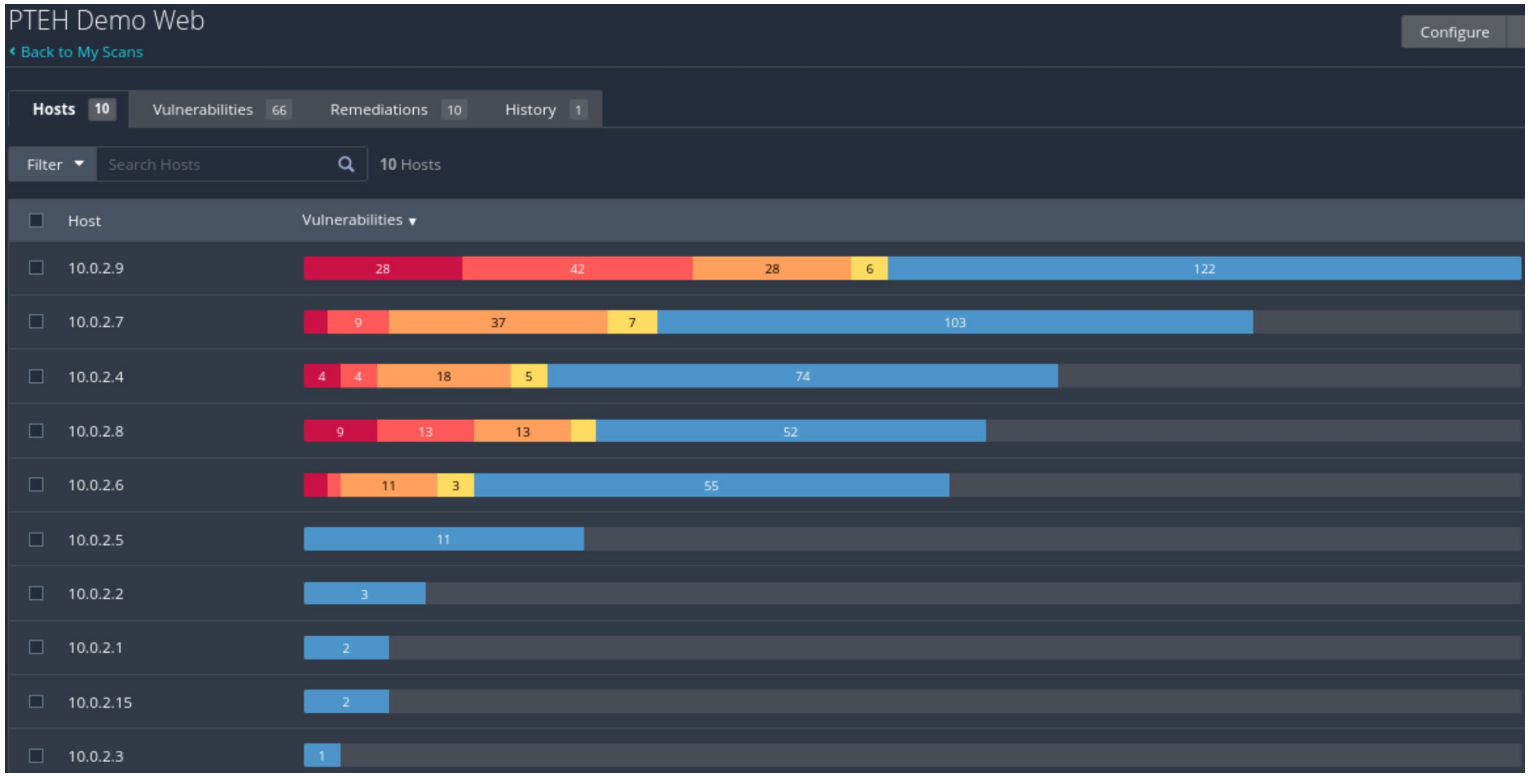
- Scansione di Applicazioni Web



Analisi Automatica delle Vulnerabilità

Nessus – Web Application Tests – Esempio

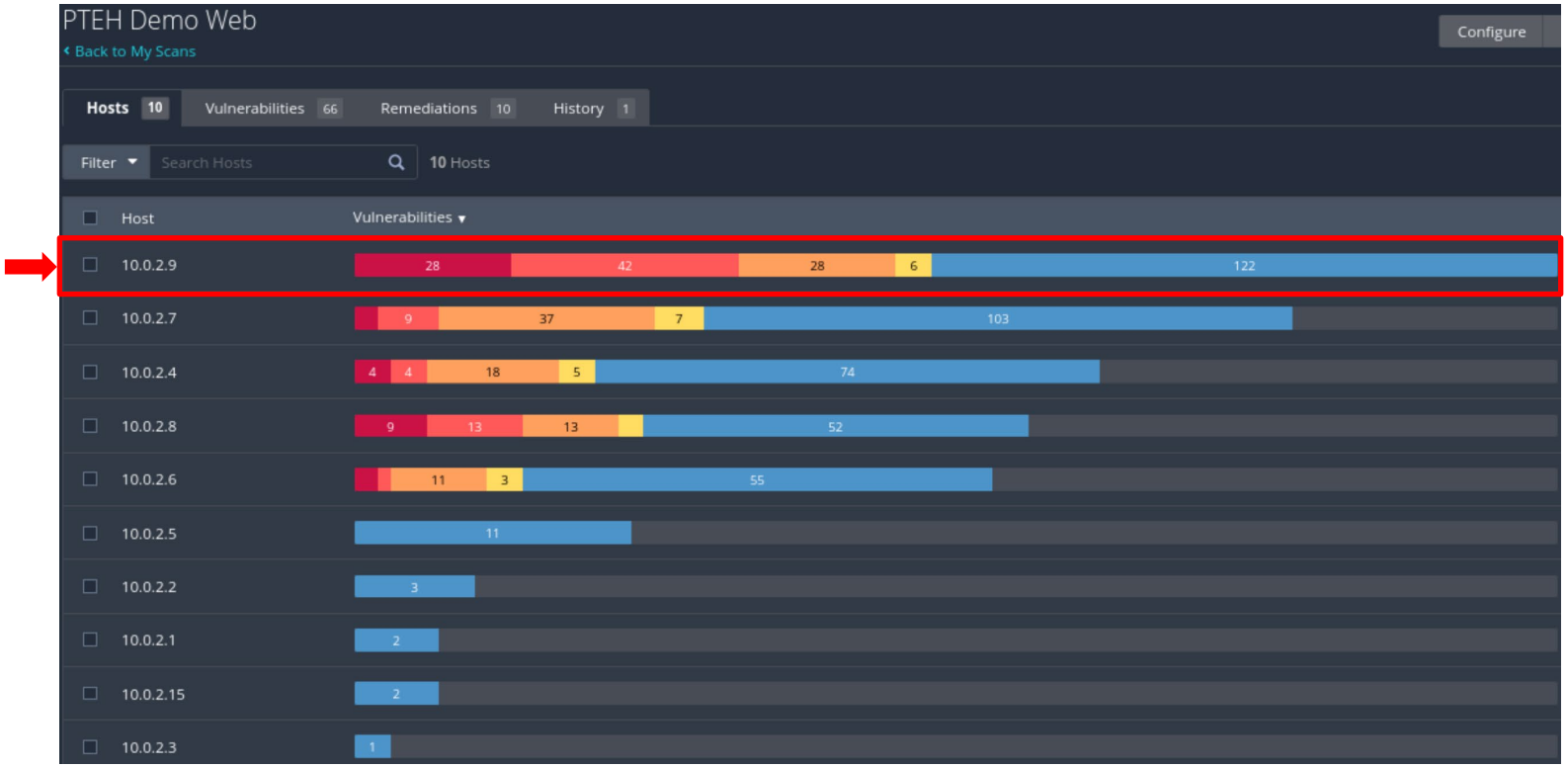
- Scansione di Applicazioni Web
  - Risultati generali della scansione



Analisi Automatica delle Vulnerabilità

Nessus – Web Application Tests – Esempio

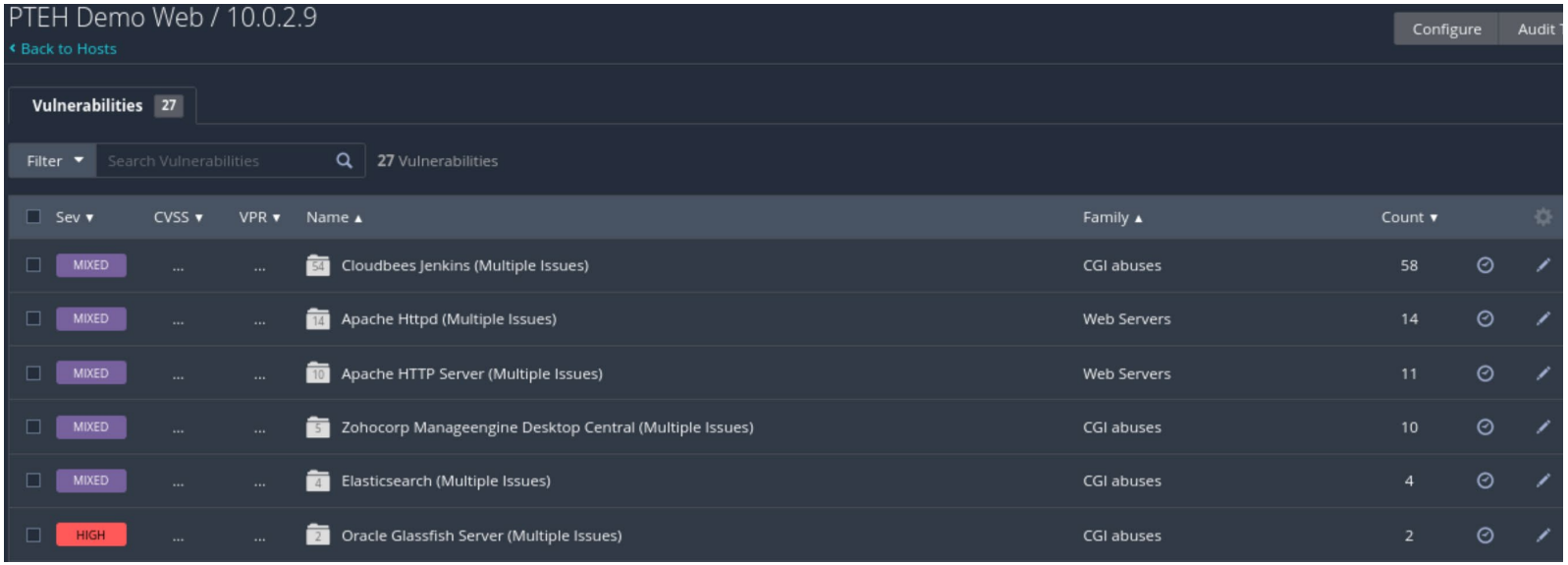
- Scansione di Applicazioni Web
  - Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.9`**



Analisi Automatica delle Vulnerabilità

Nessus – Web Application Tests – Esempio

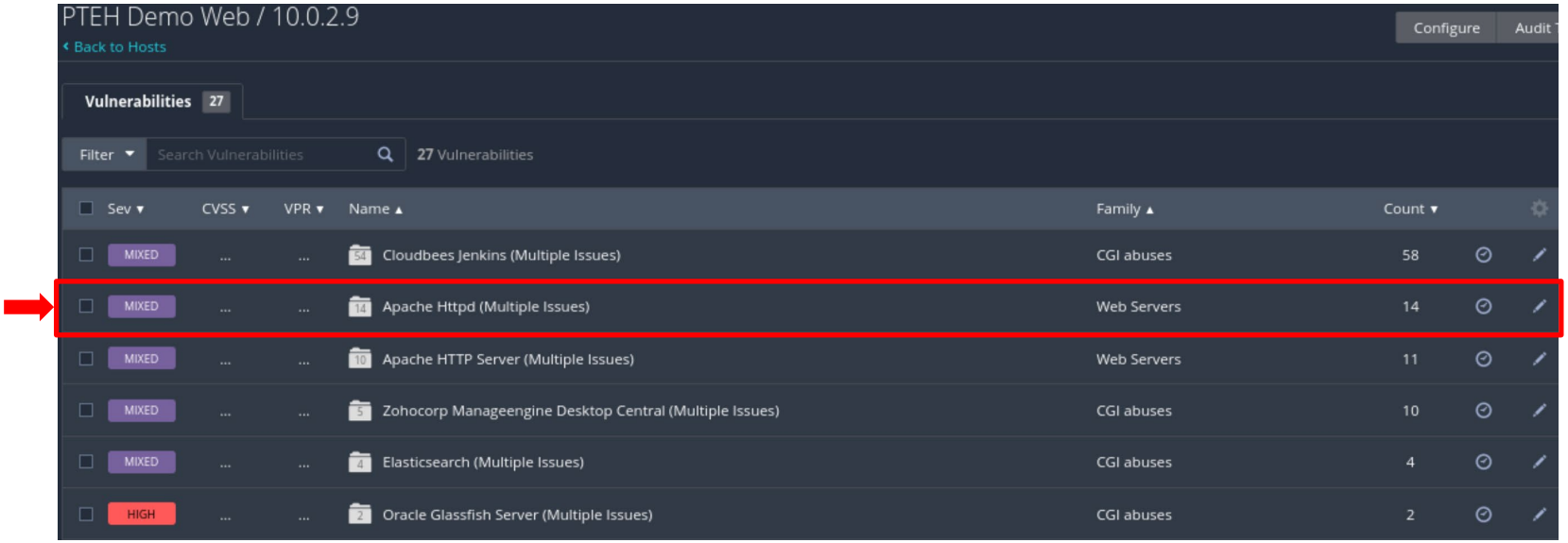
- Scansione di Applicazioni Web
  - Risultati della scansione relativi all'host con indirizzo IP **`10.0.2.9`**



Analisi Automatica delle Vulnerabilità

Nessus – Web Application Tests – Esempio

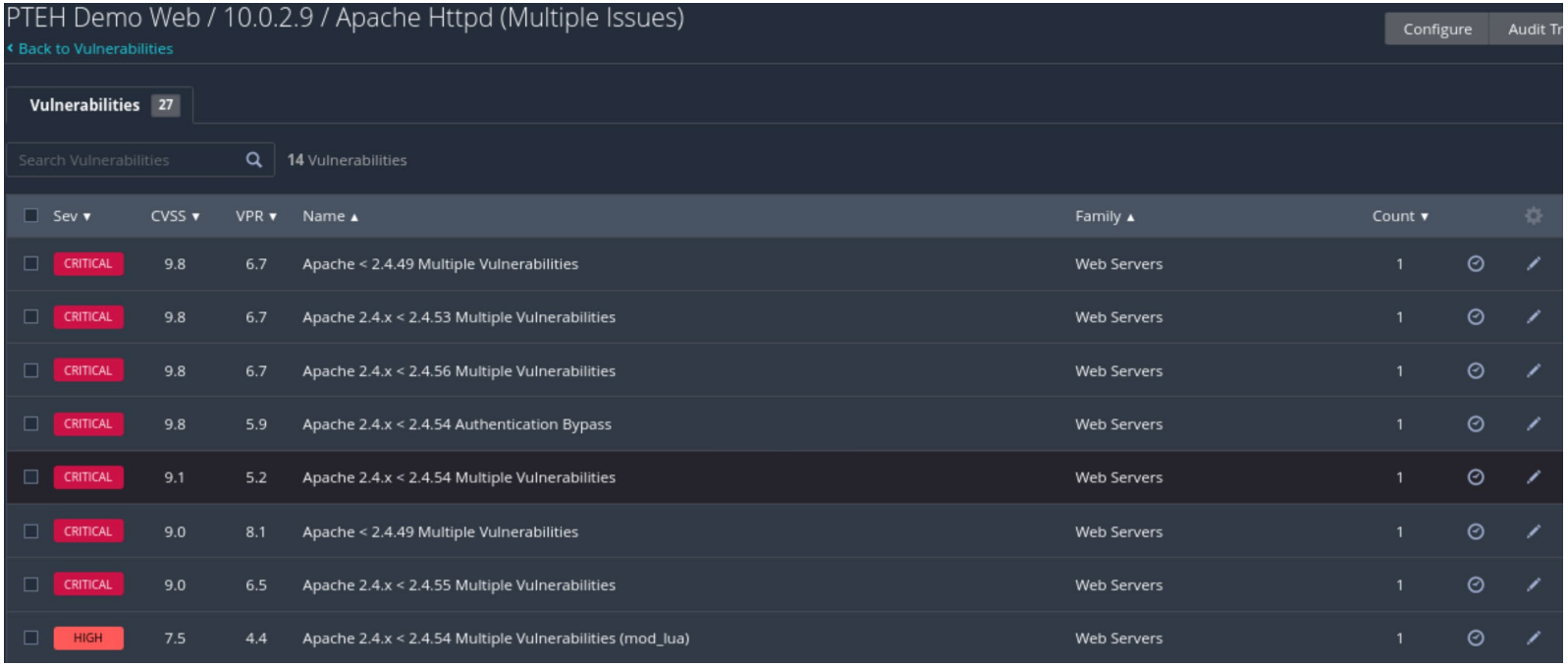
- Scansione di Applicazioni Web
  - Vulnerabilità **`Apache Httpd (Multiple Issues)`**



Analisi Automatica delle Vulnerabilità

Nessus – Web Application Tests – Esempio

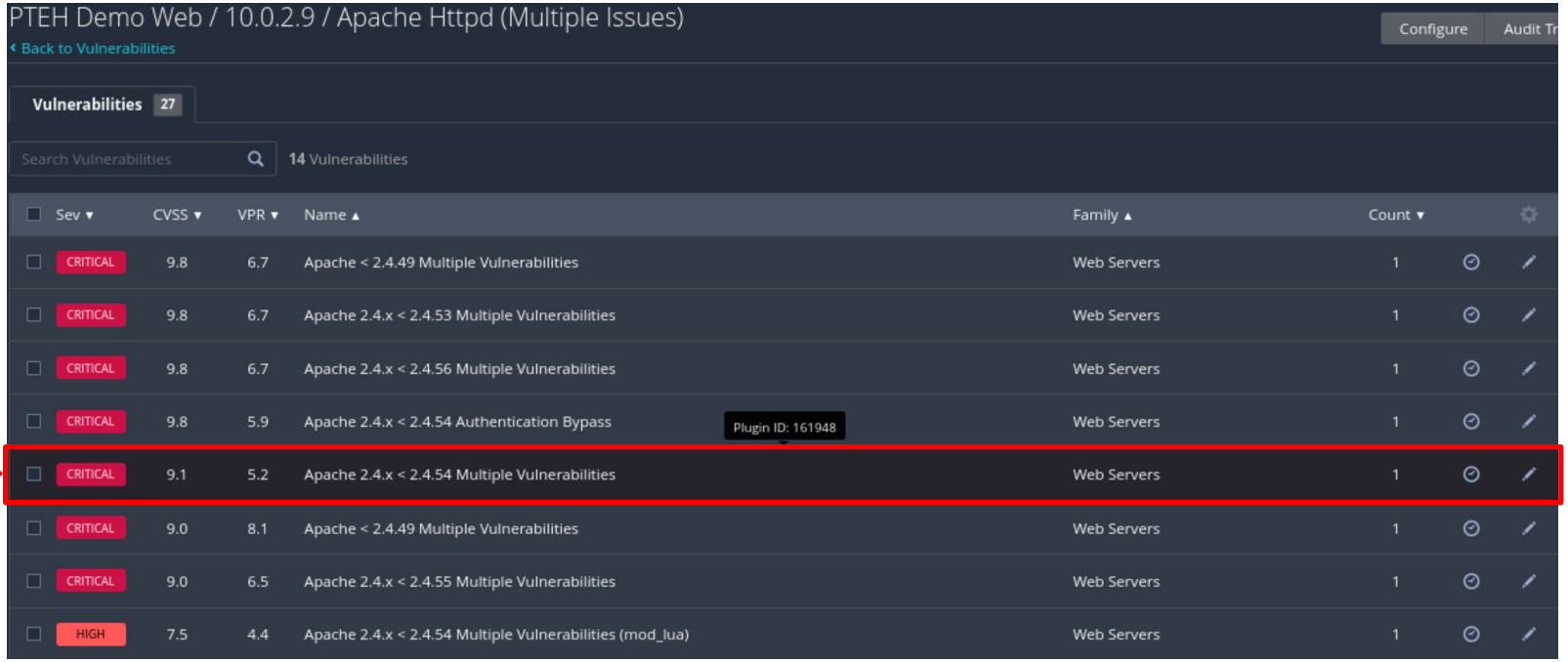
- Scansione di Applicazioni Web
  - Vulnerabilità appartenenti ad **`Apache Httpd (Multiple Issues)`**



Analisi Automatica delle Vulnerabilità

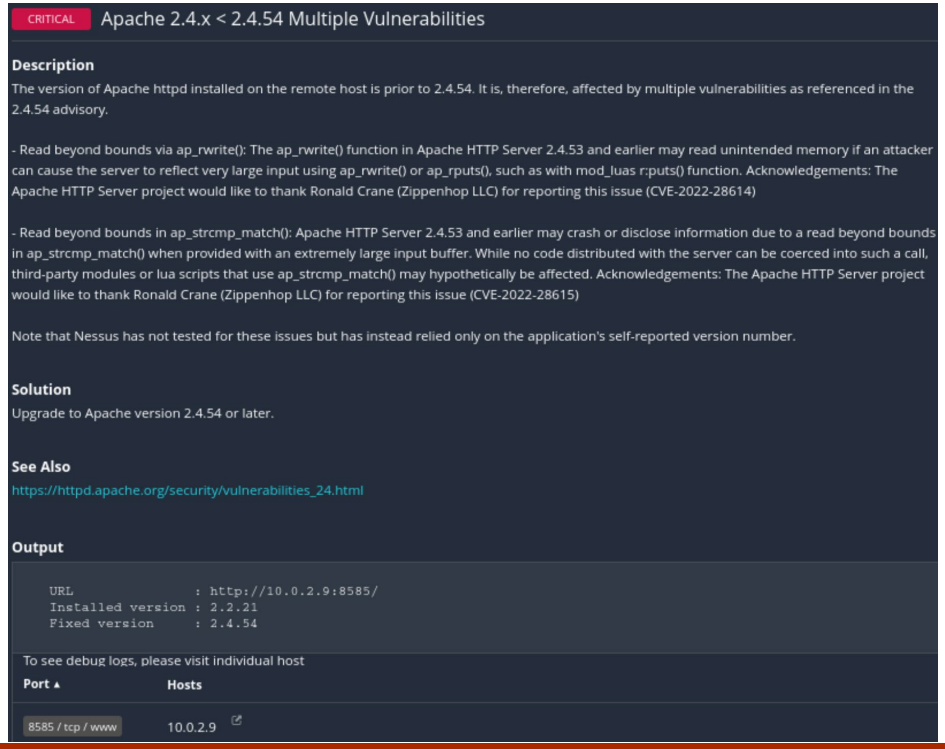
Nessus – Web Application Tests – Esempio

- Scansione di Applicazioni Web
  - Vulnerabilità **`Apache 2.4.x < 2.4.54 Multiple Vulnerabilities`**



Analisi Automatica delle Vulnerabilità
Nessus – Web Application Tests – Esempio

- Scansione di Applicazioni Web
  - Dettagli relativi alla vulnerabilità **`Apache 2.4.x < 2.4.54 Multiple Vulnerabilities`**



CRITICAL Apache 2.4.x < 2.4.54 Multiple Vulnerabilities

Description

The version of Apache httpd installed on the remote host is prior to 2.4.54. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.54 advisory.

- Read beyond bounds via ap_rwrite(): The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-28614)

- Read beyond bounds in ap_strcmp_match(): Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-28615)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.54 or later.

See Also

https://httpd.apache.org/security/vulnerabilities_24.html

Output

```
URL              : http://10.0.2.9:8585/
Installed version : 2.2.21
Fixed version     : 2.4.54
```

To see debug logs, please visit individual host

Port ▲	Hosts
8585 / tcp / www	10.0.2.9

Analisi Automatica delle Vulnerabilità

Nessus – Basic Scan vs. Web Application Tests

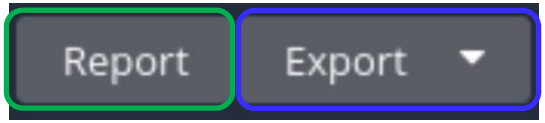
Basic Scan

Web Application Tests

Analisi Automatica delle Vulnerabilità

Nessus – Gestione Reporting

- Nessus consente di
  1. **Generare in vari formati il report relativo ad una scansione**
  2. **Esportare, in formato Nessus, i risultati relativi ad una scansione**

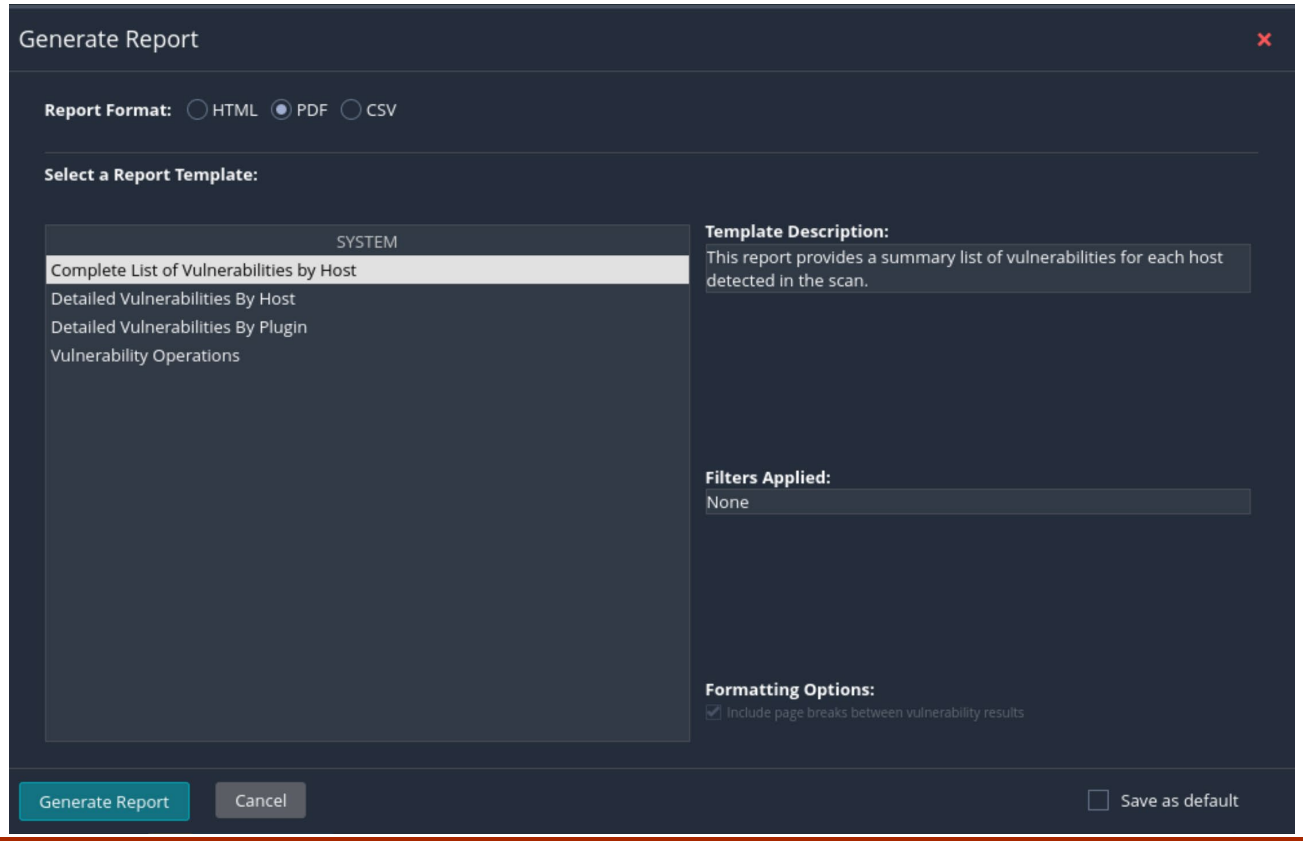


1. 2.

Analisi Automatica delle Vulnerabilità

Nessus – Gestione Reporting

- Generare il report di una scansione



Analisi Automatica delle Vulnerabilità

Nessus – Gestione Reporting

- Report di una scansione

Analisi Automatica delle Vulnerabilità

Nessus – Gestione Reporting

- Report di una scansione

TABLE OF CONTENTS

Analisi Automatica delle Vulnerabilità

Nessus – Gestione Reporting

- Report di una scansione

10.0.2.1

Vulnerabilities Total: 10

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	5.3	-	12217	DNS Server Cache Snooping Remote Information Disclosure
INFO	N/A	-	11002	DNS Server Detection
INFO	N/A	-	54615	Device Type
INFO	N/A	-	86420	Ethernet MAC Addresses

Analisi Automatica delle Vulnerabilità
OpenVAS e GVM

- **Open V**ulnerability **A**ssessment **S**ystem (**OpenVAS**)
  - Ha origine da una fork Open Source del progetto Nessus
  - Nato come uno scanner stand-alone, è stato poi inglobato nel framework **G**reenbone **V**ulnerability **M**anagement (**GVM**)
  - **GVM** offre diversi servizi e strumenti per la scansione e la gestione delle vulnerabilità

- Soluzione Open Source tra le più diffuse per la scansione e la gestione automatica delle vulnerabilità

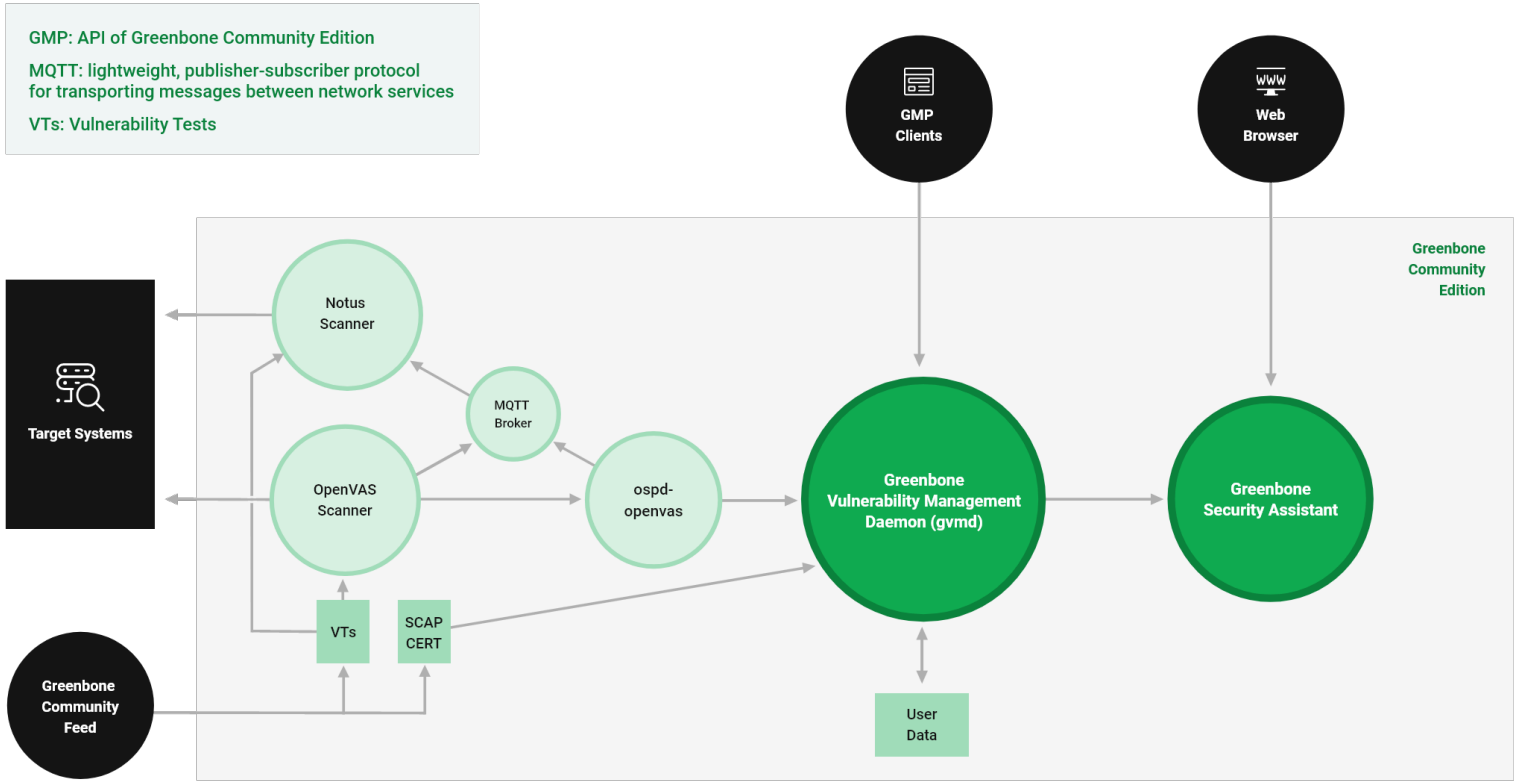
- Scanner appartenente alle soluzioni di sicurezza fornite dall'azienda tedesca *Greenbone Networks GmbH*

https://greenbone.github.io/docs/latest/history.html

Greenbone

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Architettura



https://greenbone.github.io/docs/latest/architecture.html

Greenbone

Analisi Automatica delle Vulnerabilità
OpenVAS e GVM – Installazione

- Non fa parte degli strumenti installati di default in Kali Linux

- Per l'installazione sono fortemente consigliati i seguenti passi
  - `apt install gvm*`
  - `apt install greenbone-feed-sync`
  - `gvm-setup`
  - `greenbone-feed-sync --type scap`
  - `gvm-check-setup`

N.B. In caso di errori nel corso dell'installazione, seguire di volta in volta i vari **FIX** suggeriti dal comando `gvm-check-setup`

Greenbone

Analisi Automatica delle Vulnerabilità
OpenVAS e GVM – Avvio

- Una volta installato è possibile avviare OpenVAS
  - Da Terminale mediante il seguente comando **`gvm-start`** oppure
  - Dal menu **«02 - Vulnerability Analysis»**

- Dopo alcuni secondi verrà avviato in automatico il Web Browser

Nel caso in cui il Web Browser non venga aperto automaticamente, digitare nuovamente `gvm-start` ed eventualmente collegarsi all'URL `https://127.0.0.1:9392`

Greenbone

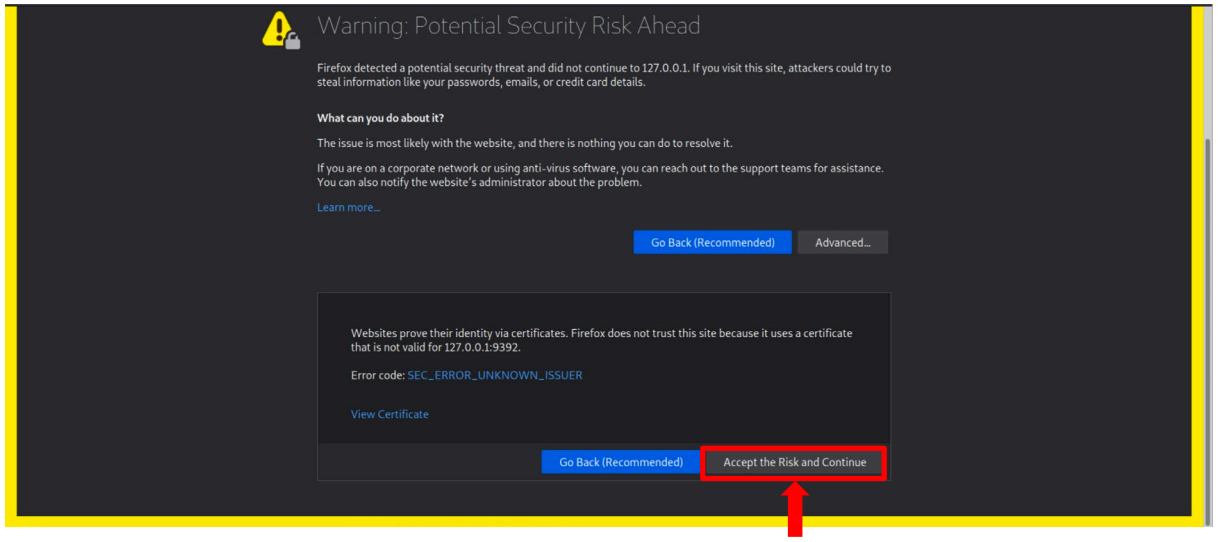
Analisi Automatica delle Vulnerabilità
OpenVAS e GVM – Avvio

- Una volta installato è possibile avviare OpenVAS
  - Da Terminale mediante il seguente comando **`gvm-start`** oppure
  - Dal menu **«02 - Vulnerability Analysis»**

Greenbone

Analisi Automatica delle Vulnerabilità
OpenVAS e GVM – Avvio

- Una volta installato è possibile avviare OpenVAS
  - Da Terminale mediante il seguente comando **`gvm-start`** oppure
  - Dal menu **«02 - Vulnerability Analysis»**



Greenbone

Analisi Automatica delle Vulnerabilità
OpenVAS e GVM – Avvio

- Una volta installato è possibile avviare OpenVAS
  - Da Terminale mediante il seguente comando **`gvm-start`** oppure
  - Dal menu **«02 - Vulnerability Analysis»**

- **N.B.** Prima degli avvii successivi di OpenVAS è opportuno aggiornare i relativi *feed*
  - **`gvm-feed-update`**

Greenbone

Analisi Automatica delle Vulnerabilità
Greenbone OS

- Virtual Machine basata sul framework Greenbone Vulnerability Management (GVM)
  - https://www.greenbone.net/en/testnow/

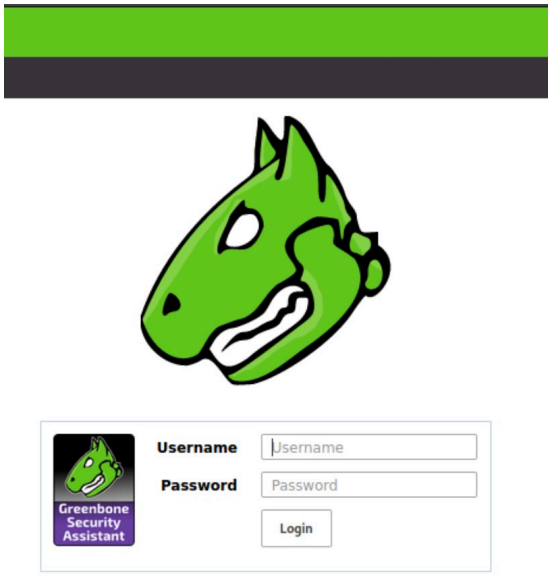
- Per l'installazione e la configurazione di Greenbone OS è fortemente consigliata la seguente guida
  - https://www.acunetix.com/support/docs/wvs/installing-network-scanning/

- Strumento molto ben documentato
  - https://docs.greenbone.net/

Greenbone

Analisi Automatica delle Vulnerabilità
OpenVAS e GVM – Login

- Schermata di login che consente di inserire le credenziali di accesso
  - Di default, lo Username è **`admin`** mentre la Password è quella generata da OpenVAS al termine del comando **`gvm-setup`**



- OpenVAS consente comunque una completa gestione dell'accounting
  - https://docs.greenbone.net/

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Interfaccia

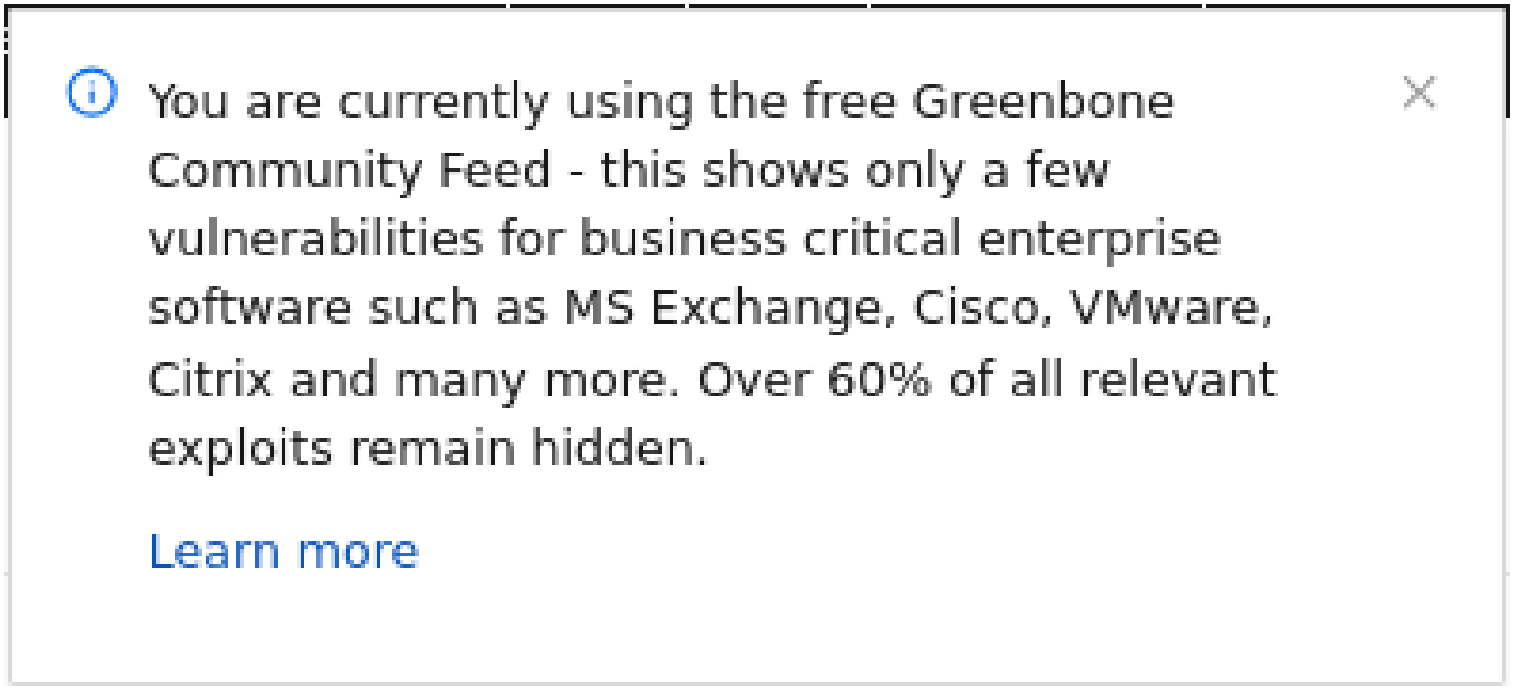
- *Dashboard* iniziale

Analisi Automatica delle Vulnerabilità
OpenVAS e GVM – Interfaccia

- *Dashboard* iniziale

Analisi Automatica delle Vulnerabilità
OpenVAS e GVM – Interfaccia

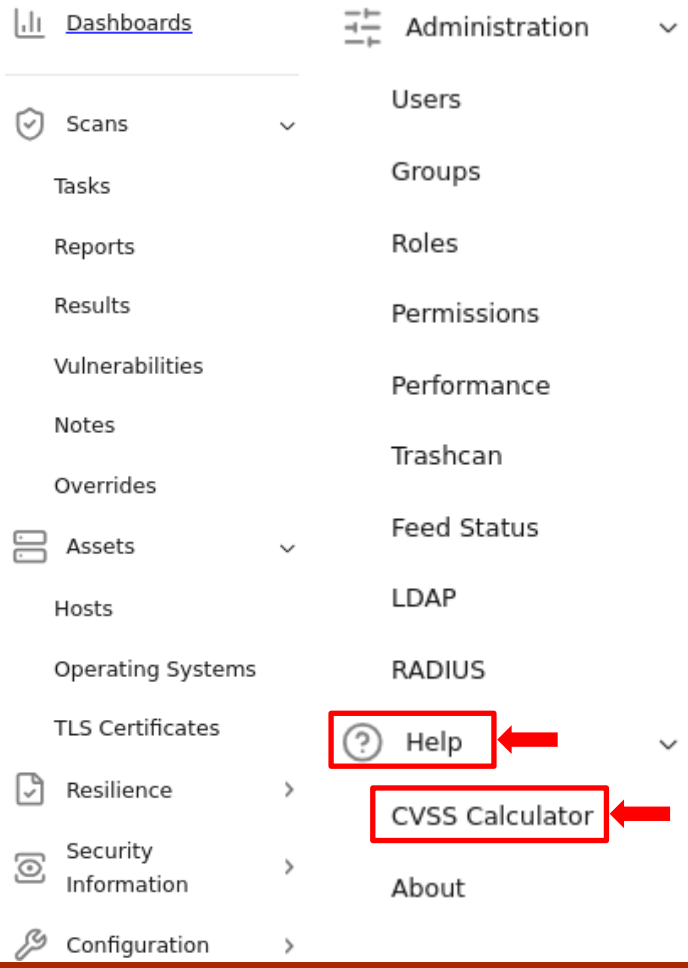
- *Dashboard* iniziale



Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Interfaccia – Funzionalità di Help

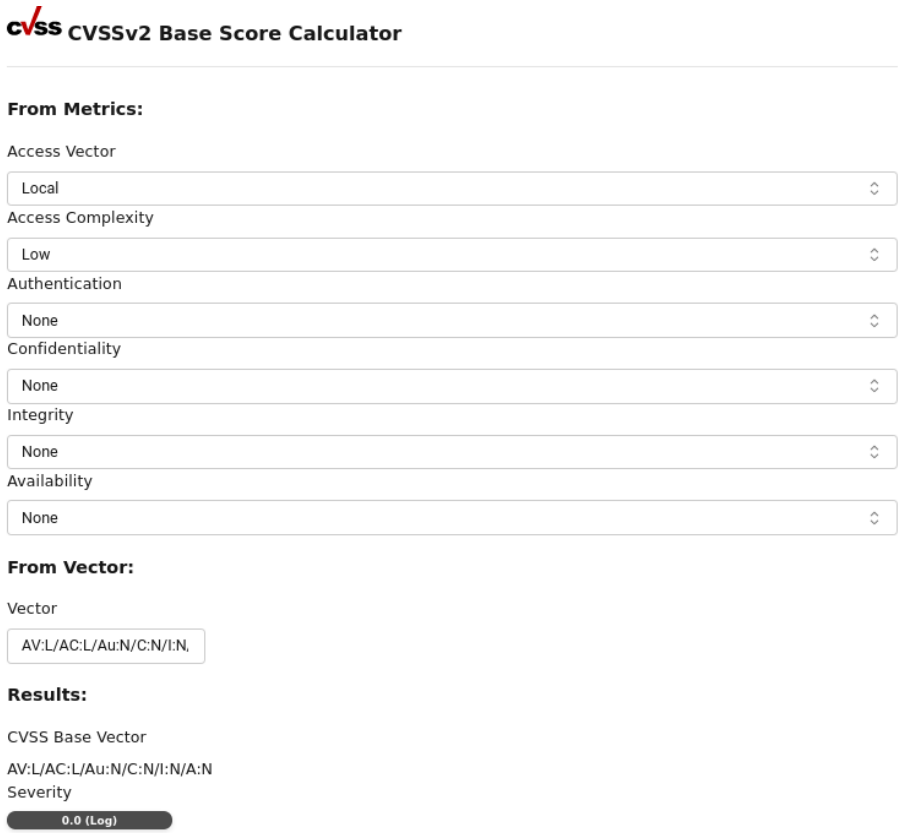
- *Dashboard* iniziale



Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Interfaccia – Funzionalità di Help

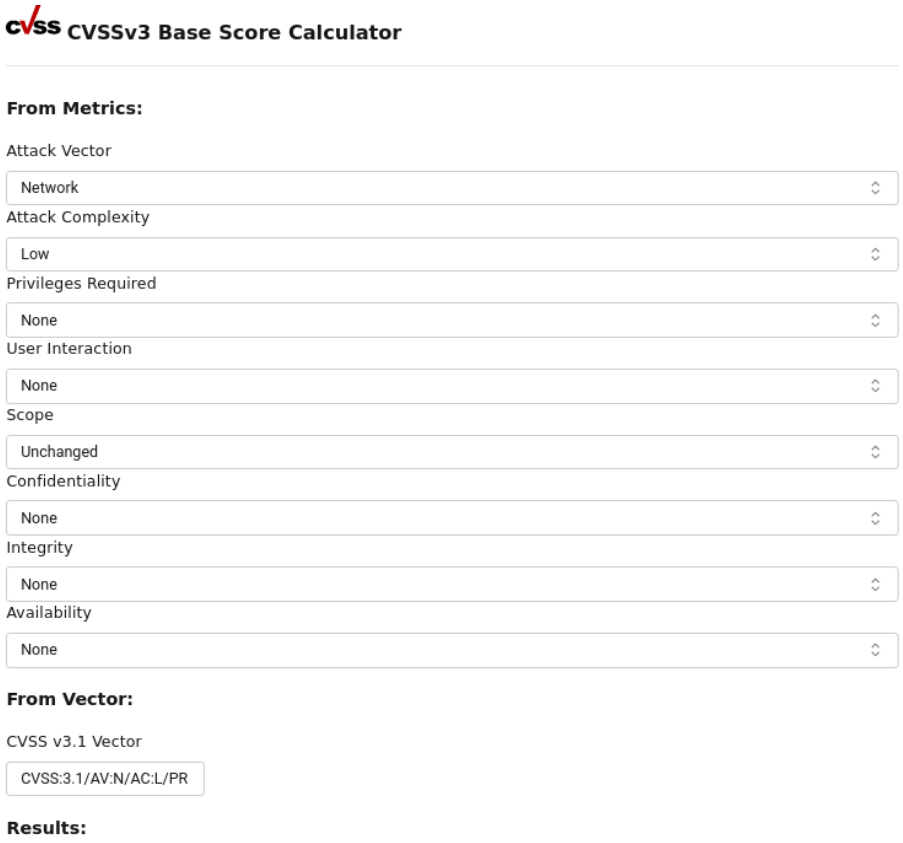
- *Dashboard* iniziale (CVSSv2 Base Score Calculator)



Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Interfaccia – Funzionalità di Help

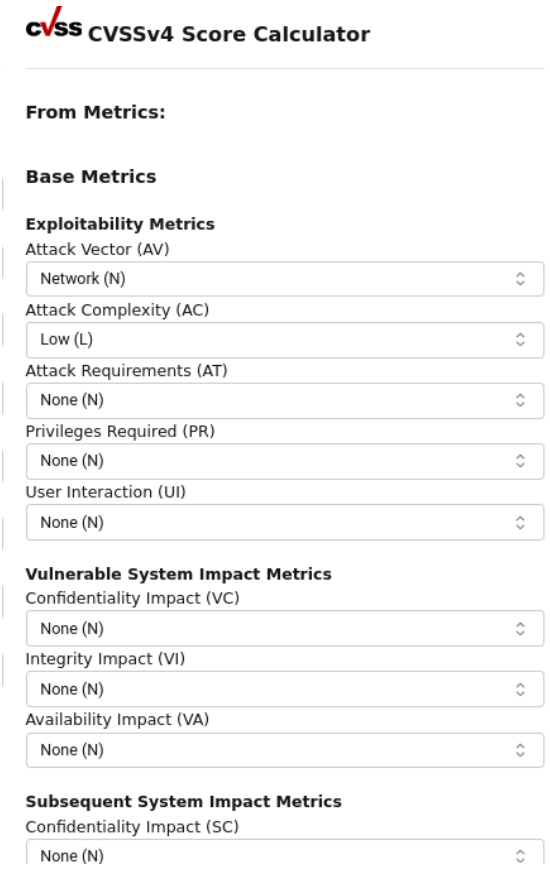
- *Dashboard* iniziale (CVSSv3 Base Score Calculator)



Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Interfaccia – Funzionalità di Help

- *Dashboard* iniziale (CVSSv4 Base Score Calculator)



Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Interfaccia – Funzionalità di Help

- **IMPORTANTE:** Dopo il login è NECESSARIO ATTENDERE la fine dell'aggiornamento completo dei Feed (Administration -> Feed Status)
  - **N.B.** Questa operazione potrebbe richiedere varie iterazioni e molto tempo

Feed Status

Type	Content	Version	Status
NVT	NVTs	20250507T0651	**Current**
SCAP	CVEs CPEs	20250507T0506	**Update in progress...**
CERT	CERT-Bund Advisories DFN-CERT Advisories	20250507T0409	**Update in progress...**

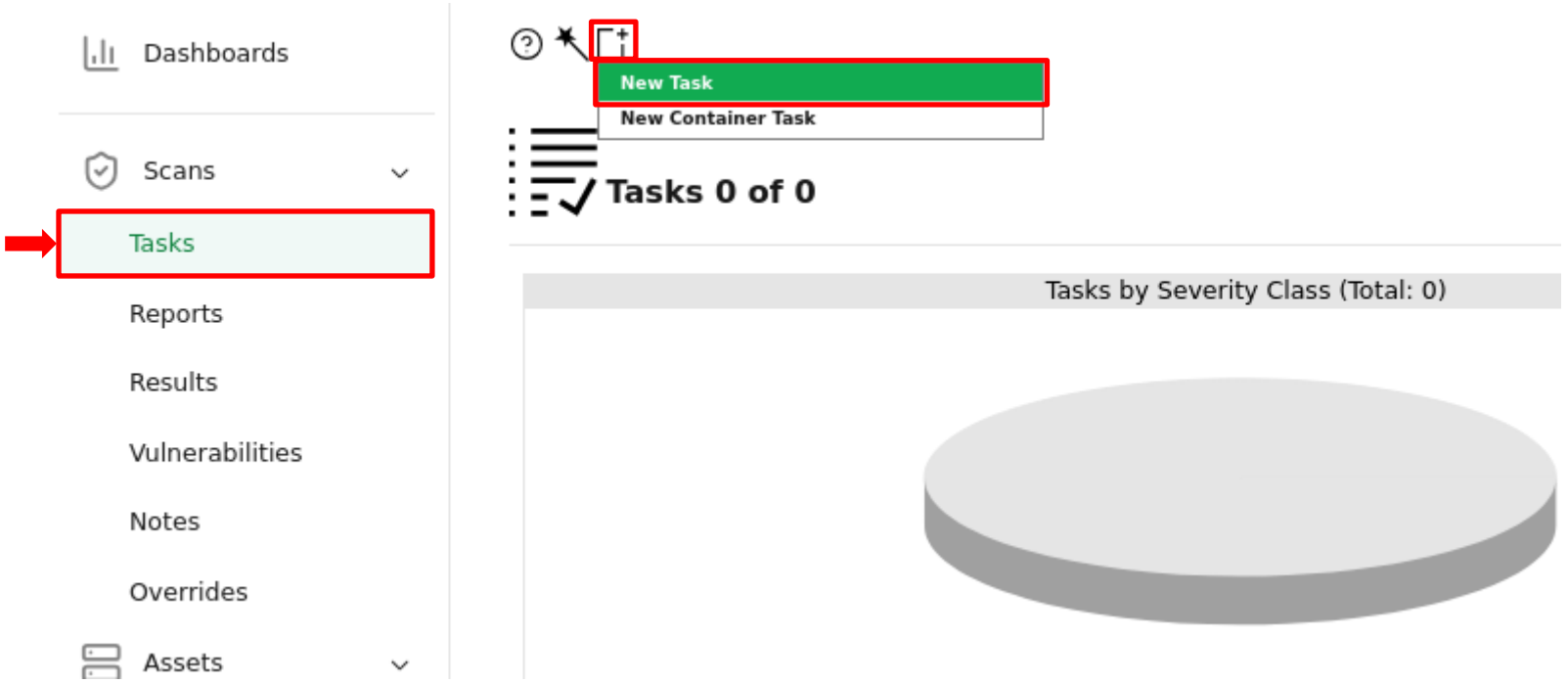
Feed Status

Type	Content	Version	Status
NVT	NVTs	20250507T0651	**Current**
SCAP	CVEs CPEs	20250507T0506	**Current**
CERT	CERT-Bund Advisories DFN-CERT Advisories	20250507T0409	**Current**

Analisi Automatica delle Vulnerabilità

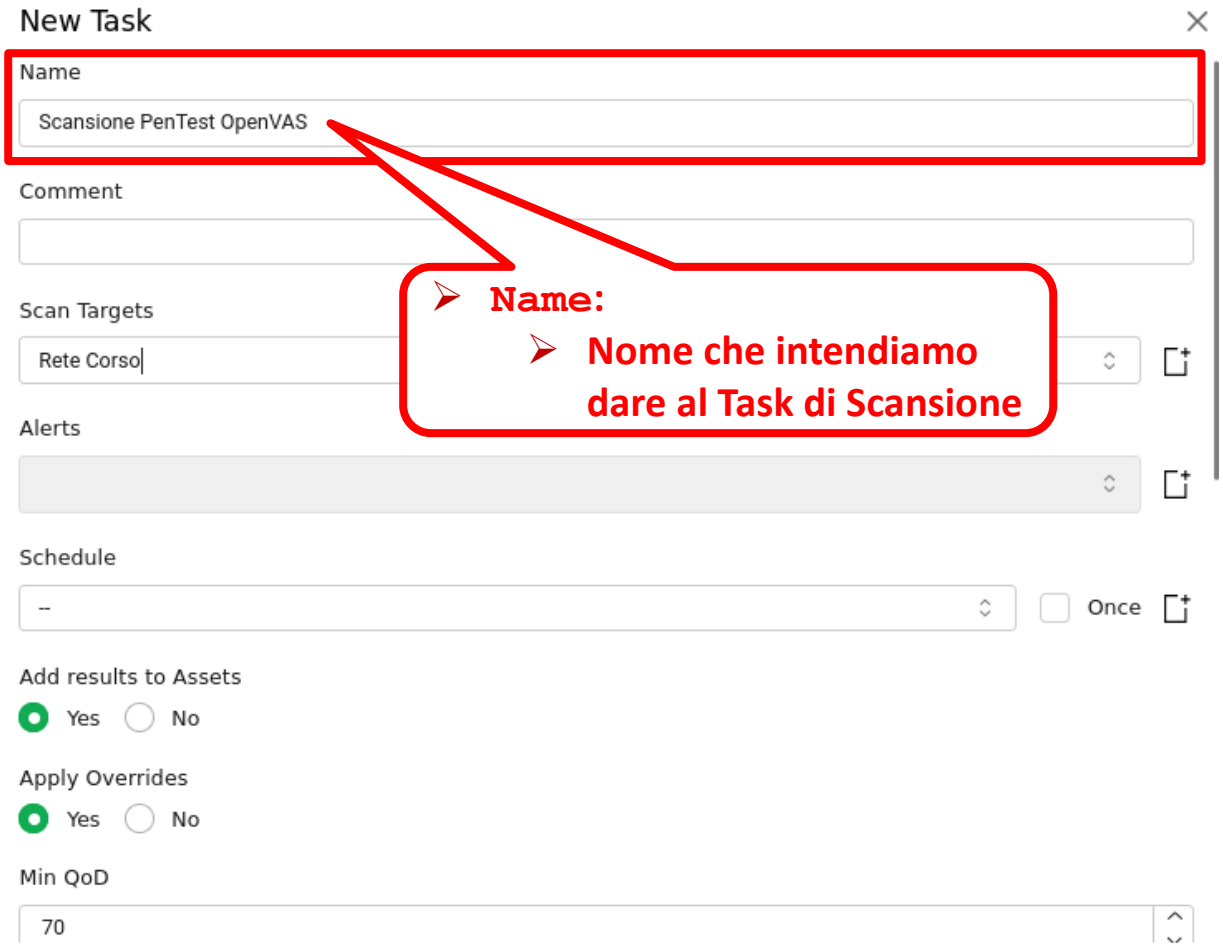
OpenVAS e GVM – Configurazione di una Scansione

- Creazione di un nuovo *Task di Scansione* (**`New Task`**)



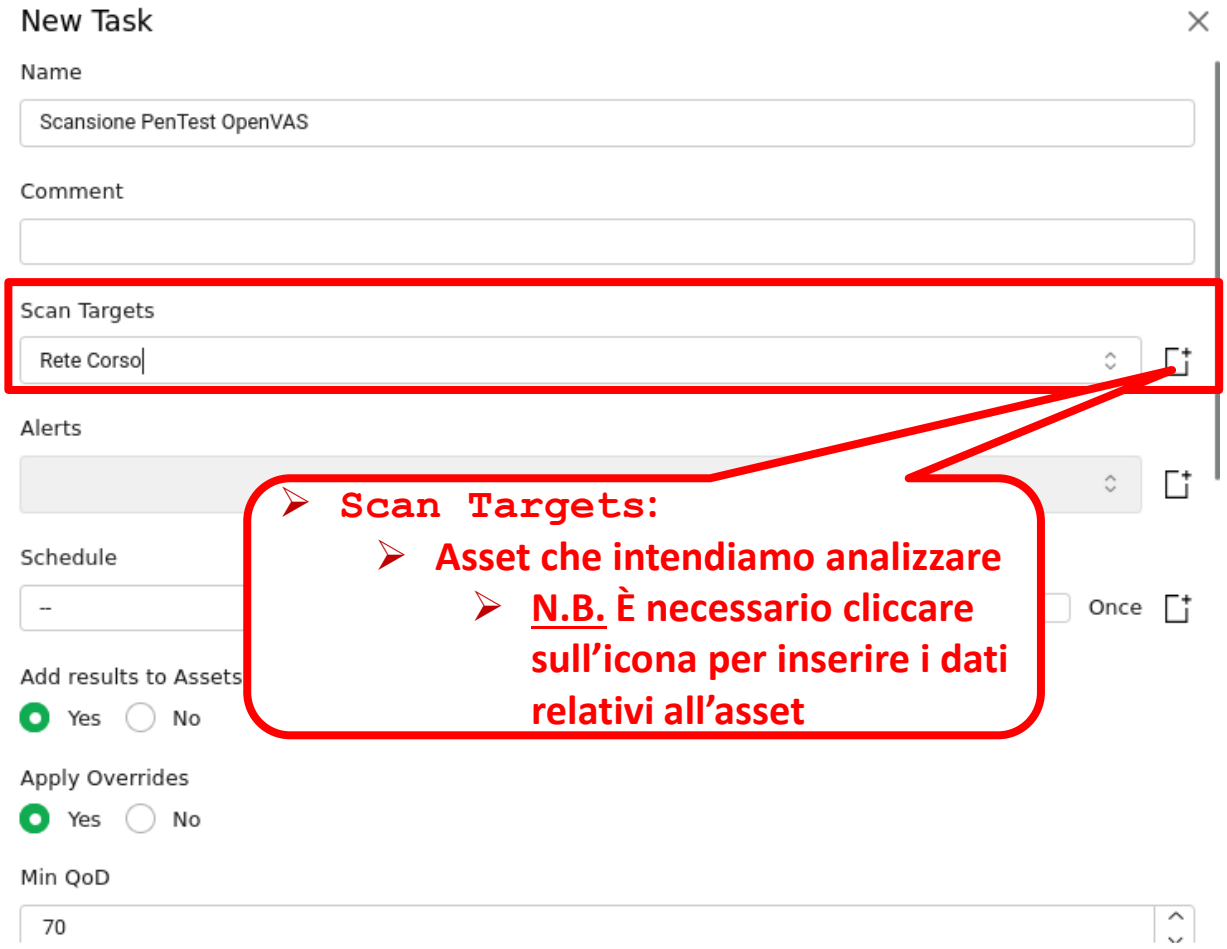
Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Configurazione di una Scansione



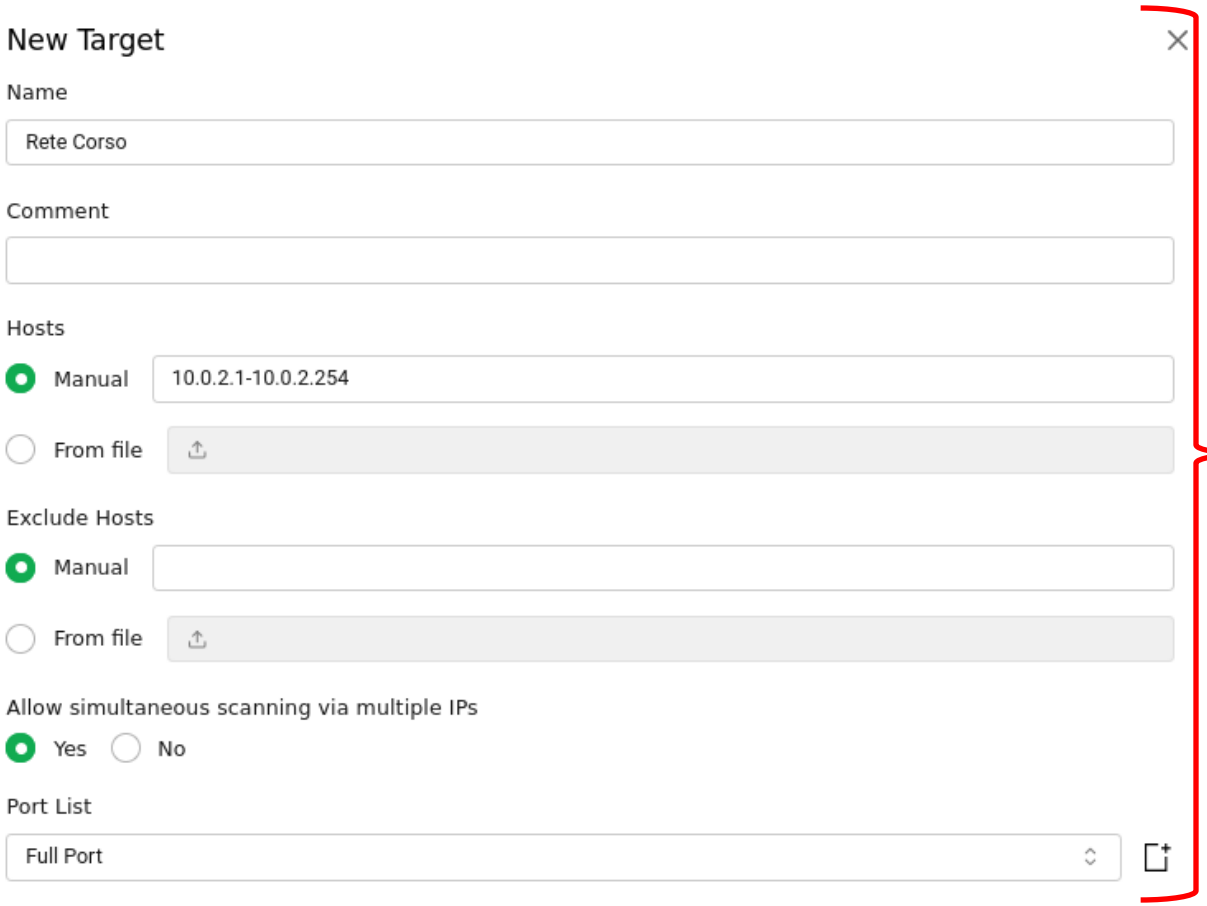
Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Configurazione di una Scansione



Analisi Automatica delle Vulnerabilità

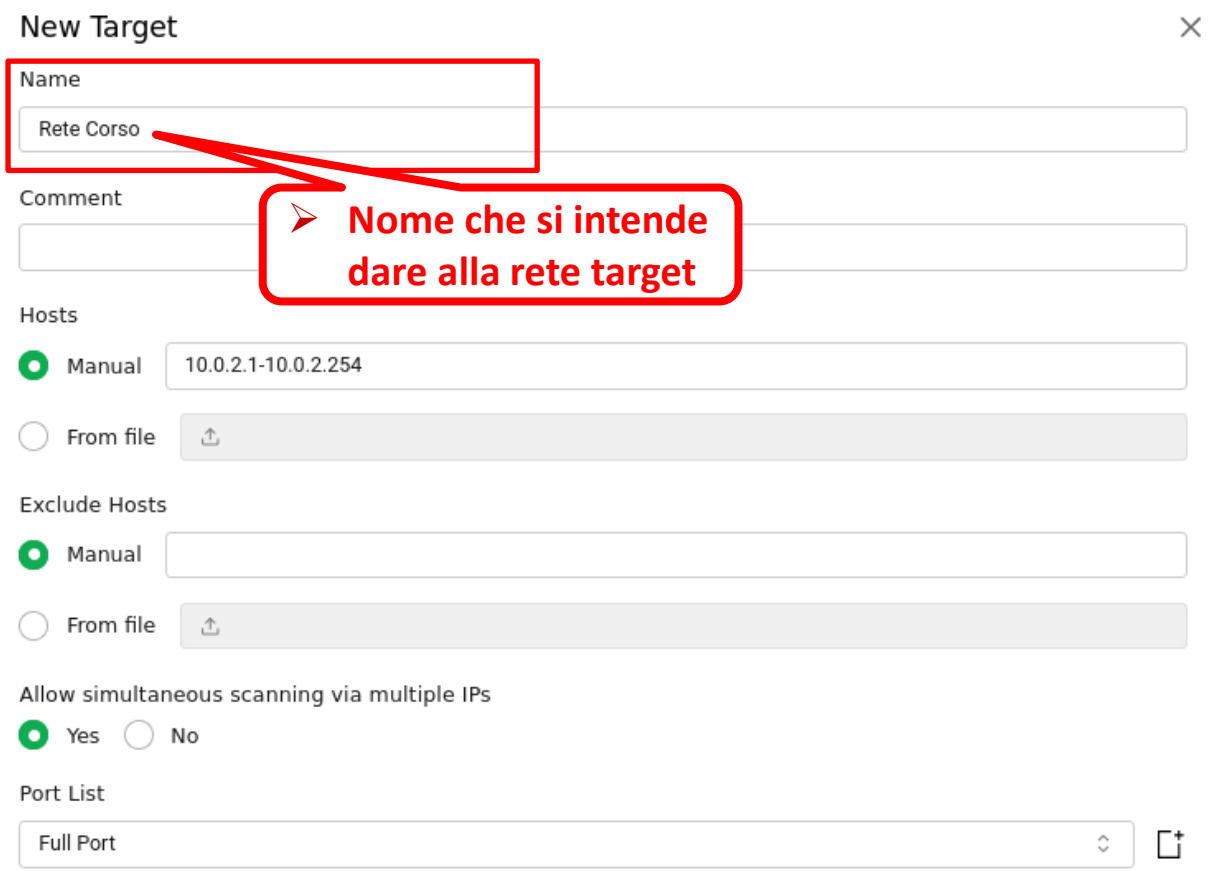
OpenVAS e GVM – Configurazione di una Scansione



Informazioni sull'asset da analizzare

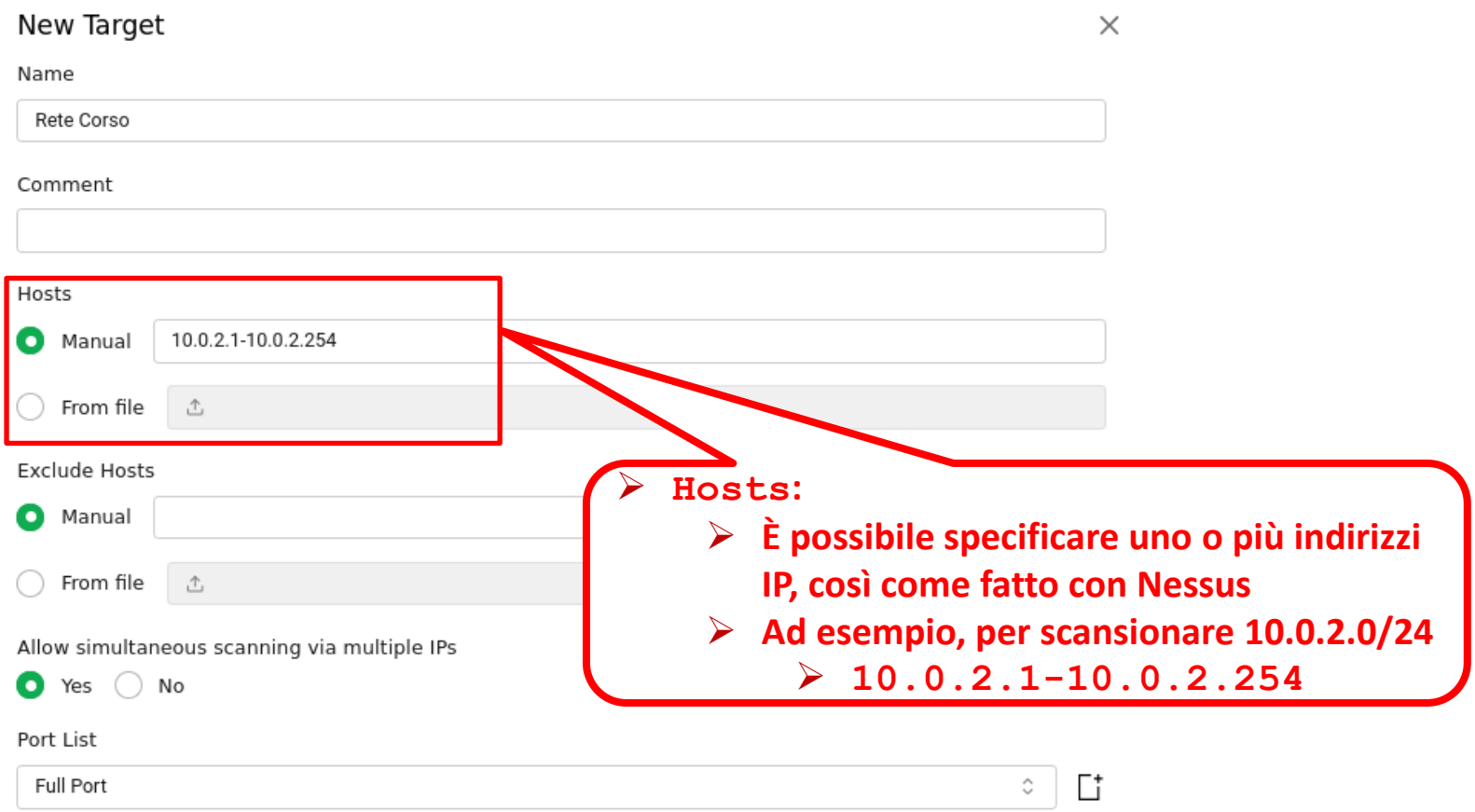
Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Configurazione di una Scansione



Analisi Automatica delle Vulnerabilità

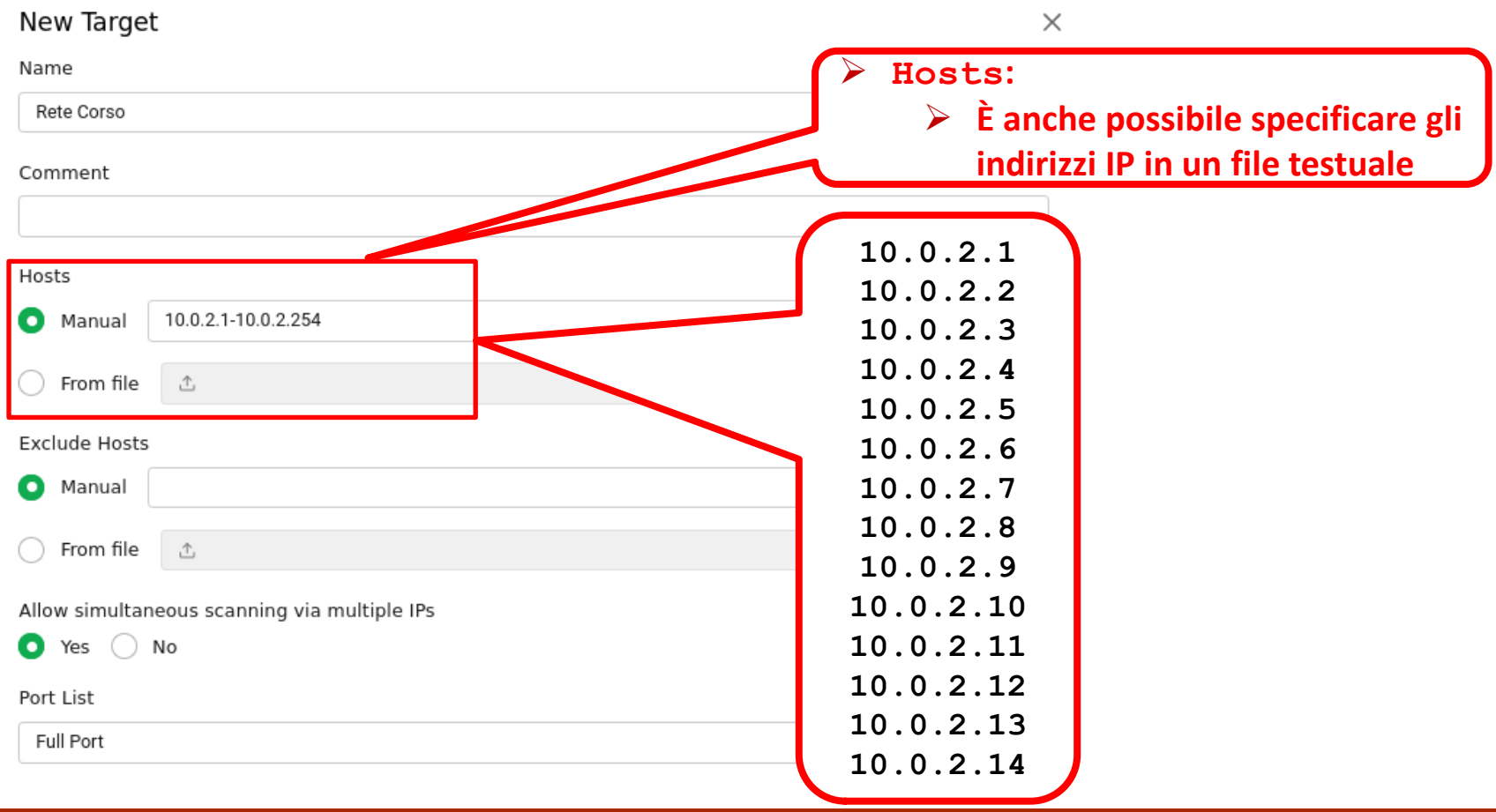
OpenVAS e GVM – Configurazione di una Scansione



- **Hosts:**
  - **È possibile specificare uno o più indirizzi IP, così come fatto con Nessus**
  - **Ad esempio, per scansionare 10.0.2.0/24**
    - `10.0.2.1-10.0.2.254`

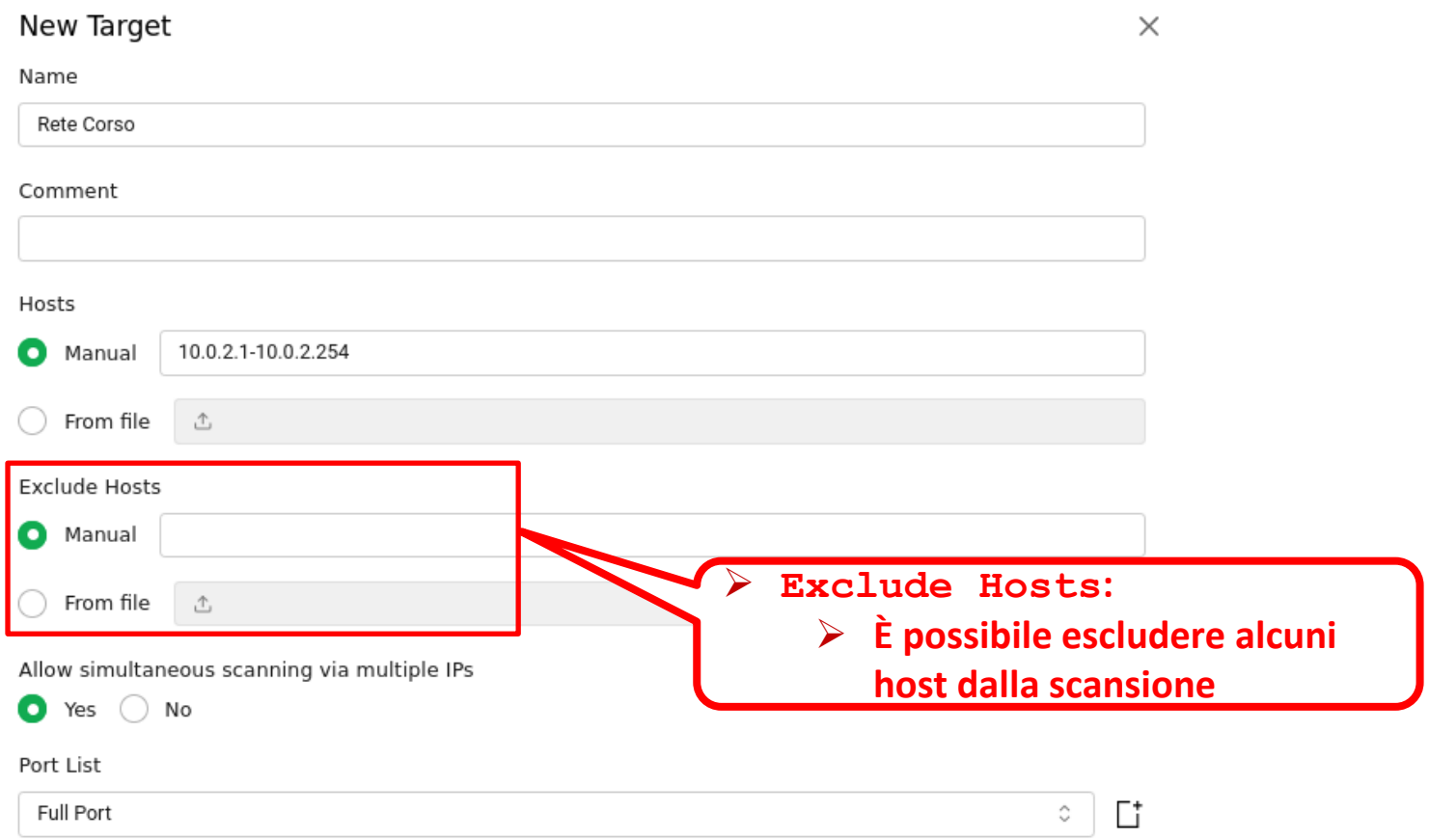
Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Configurazione di una Scansione



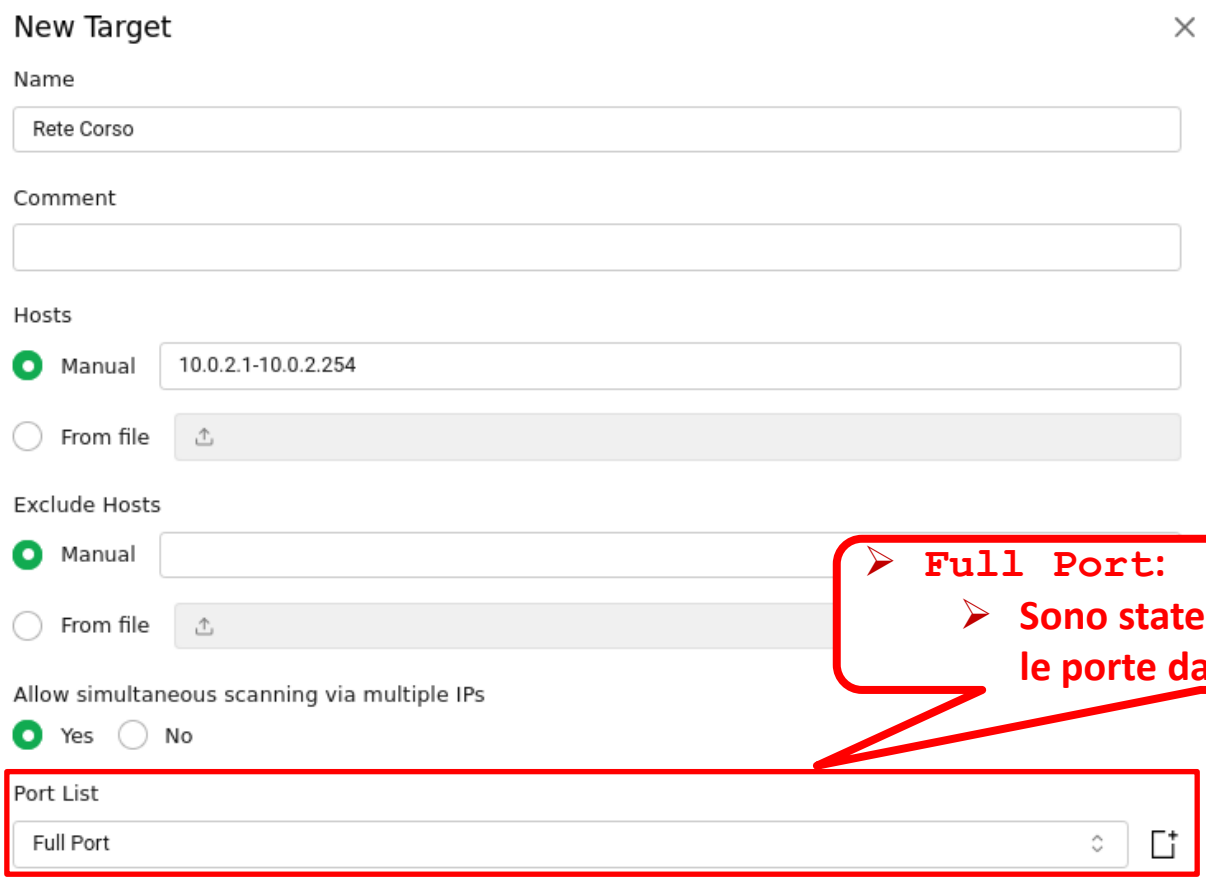
Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Configurazione di una Scansione



Analisi Automatica delle Vulnerabilità

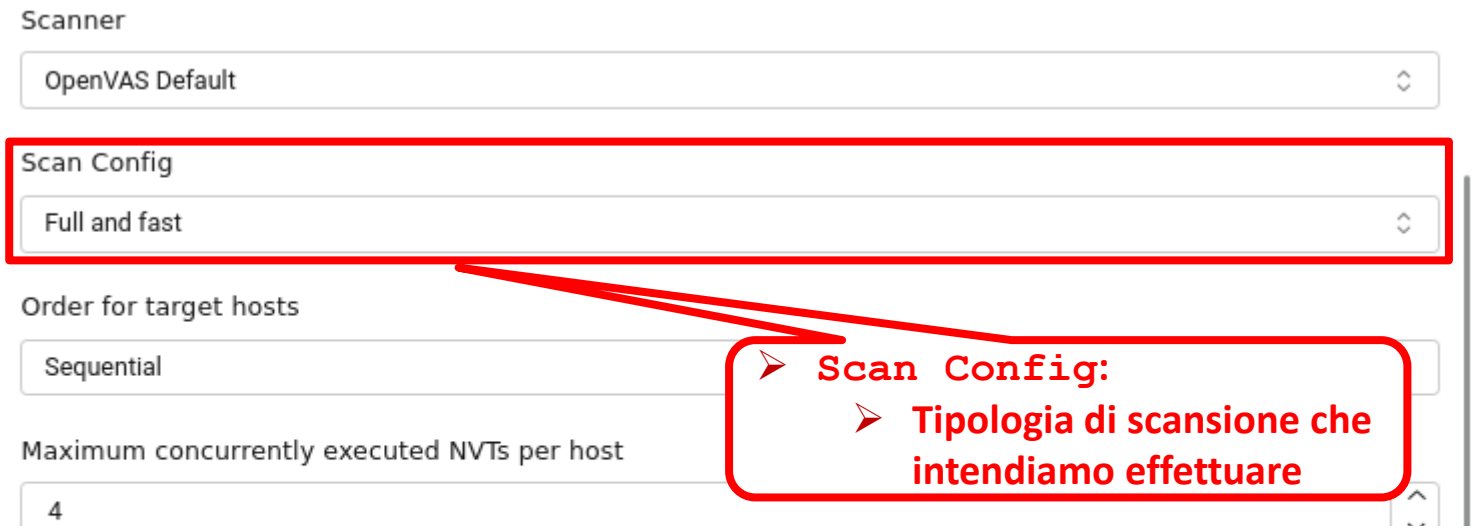
OpenVAS e GVM – Configurazione di una Scansione



- **Full Port:**
  - **Sono state manualmente impostate le porte dalla 1 alla 65535**

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Configurazione di una Scansione



N.B. Nel caso in cui «**Scan Config**» risulti bloccato, è possibile tentare i seguenti passi:

- **sudo greenbone-feed-sync --type SCAP**
- **sudo greenbone-feed-sync --type CERT**
- **sudo greenbone-feed-sync --type GVMD_DATA**
- **sudo gvm-stop**
- **sudo gvm-start**

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Configurazione di una Scansione

Analisi Automatica delle Vulnerabilità

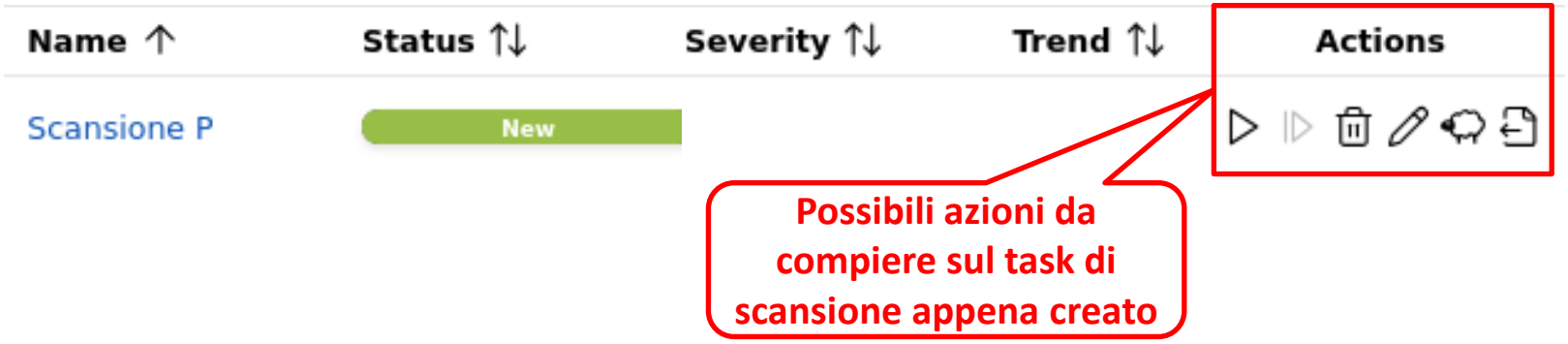
OpenVAS e GVM – Configurazione di una Scansione

- Task di scansione appena creato

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Configurazione di una Scansione

- Task di scansione appena creato



Analisi Automatica delle Vulnerabilità
OpenVAS e GVM – Esecuzione di una Scansione

- Avviamo il task di scansione appena creato

Non appena viene avviato un task di scansione, il suo Status diventa «Requested»

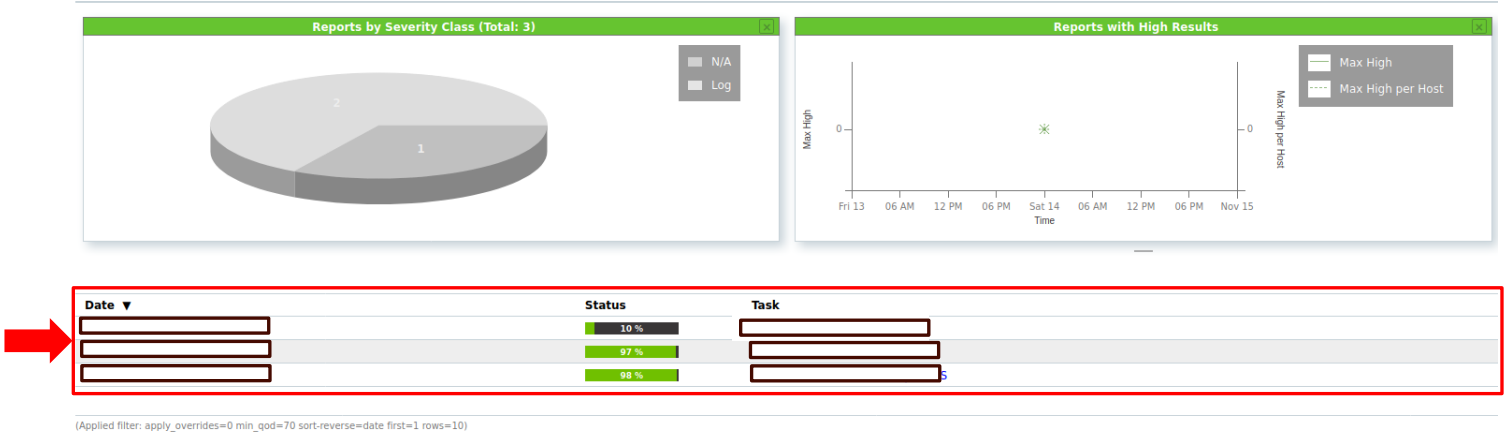
Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Esecuzione di una Scansione

- Avviamo il task di scansione appena creato

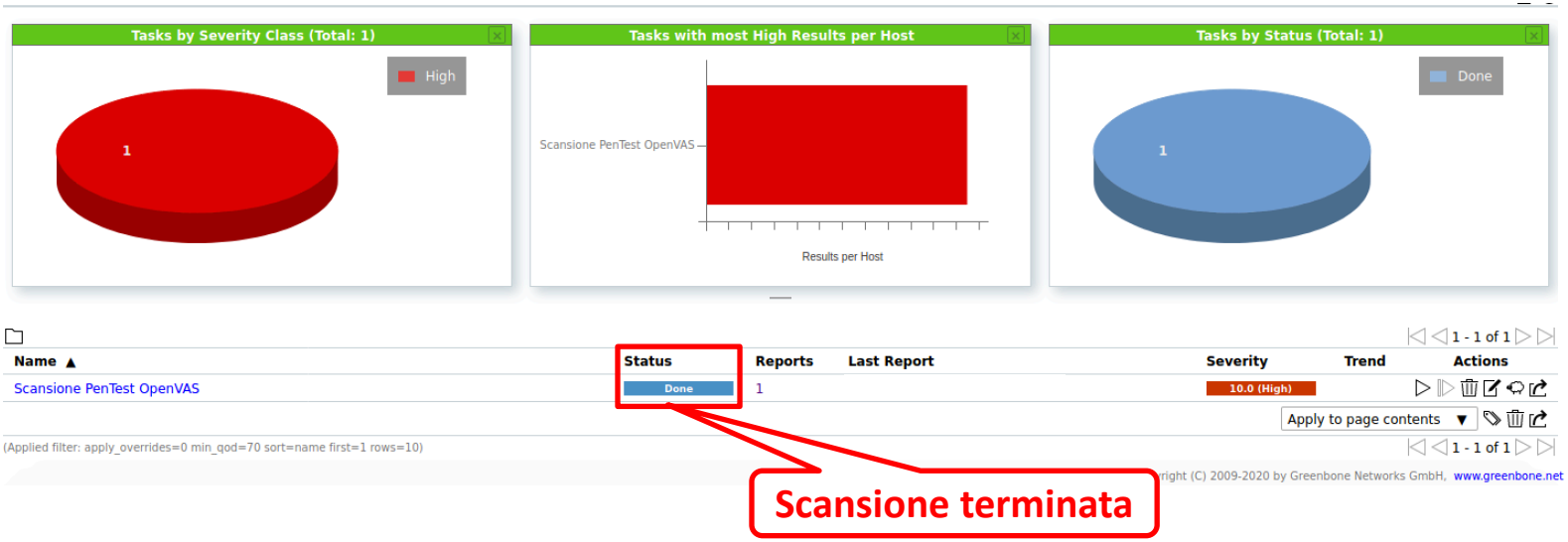
Analisi Automatica delle Vulnerabilità
OpenVAS e GVM – Scansioni Multiple

- OpenVAS permette l'esecuzione parallela di più task di scansione



Analisi Automatica delle Vulnerabilità
OpenVAS e GVM – Risultati di una Scansione

- Nella *Dashboard* vengono mostrati i risultati generali delle scansioni

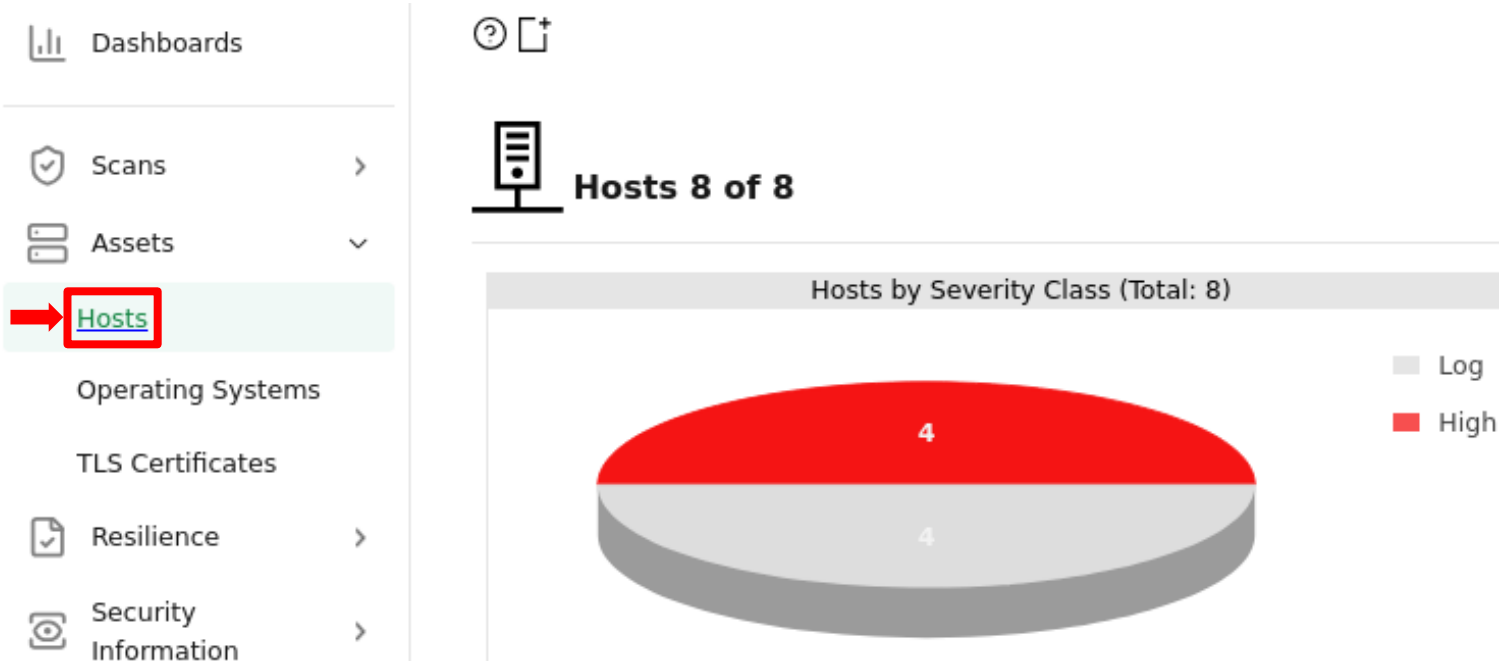


Quando un task di scansione termina, il suo Status passa da «**`Running`**» a «**`Done`**»

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare i risultati generali relativi ai vari host target



Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare i risultati generali relativi ai vari host target

Name	IP Address	OS	Severity
10.0.2.12	10.0.2.12		10.0 (High)
10.0.2.10	10.0.2.10		10.0 (High)
10.0.2.11	10.0.2.11		10.0 (High)
10.0.2.2	10.0.2.2		9.8 (High)
10.0.2.18	10.0.2.18		0.0 (Log)
10.0.2.15	10.0.2.15		0.0 (Log)
10.0.2.3	10.0.2.3		0.0 (Log)
10.0.2.1	10.0.2.1		0.0 (Log)

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare i risultati generali relativi ai vari host target

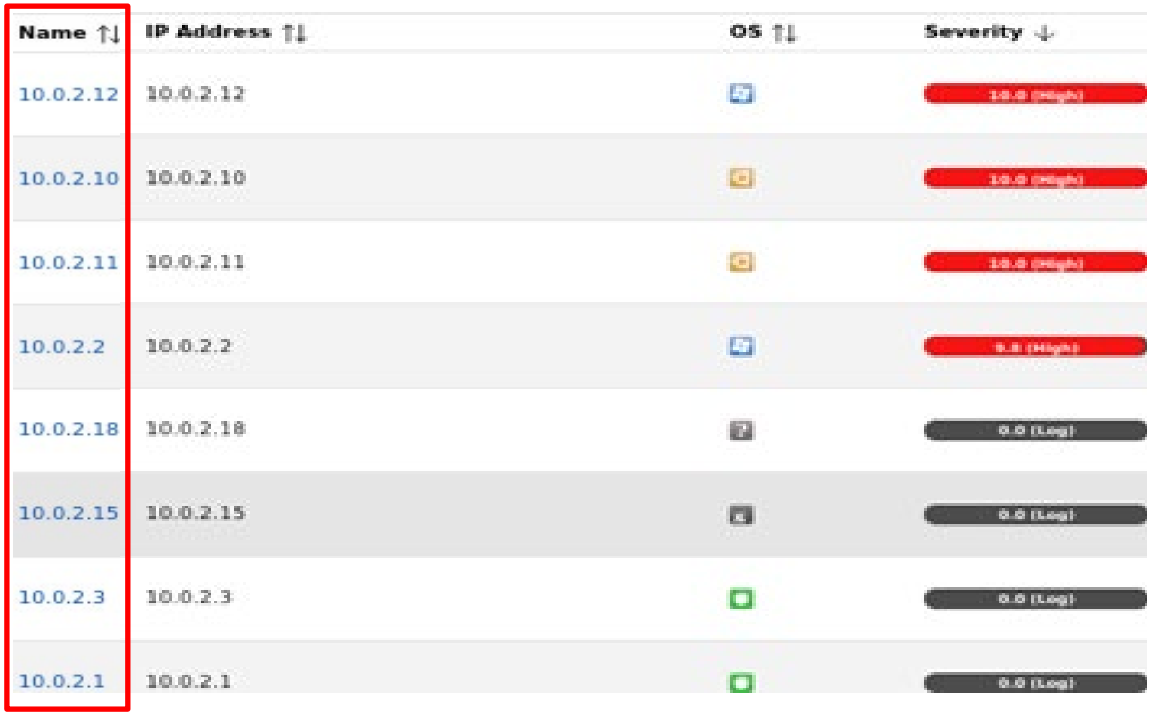
Name	IP Address	OS	Severity
10.0.2.12	10.0.2.12		10.0 (High)
10.0.2.10	10.0.2.10		10.0 (High)
10.0.2.11	10.0.2.11		10.0 (High)
10.0.2.2	10.0.2.2		9.8 (High)
10.0.2.18	10.0.2.18		0.0 (Log)
10.0.2.15	10.0.2.15		0.0 (Log)
10.0.2.3	10.0.2.3		0.0 (Log)
10.0.2.1	10.0.2.1		0.0 (Log)

Host target appartenenti all'asset analizzato

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare i risultati generali relativi ai vari host target

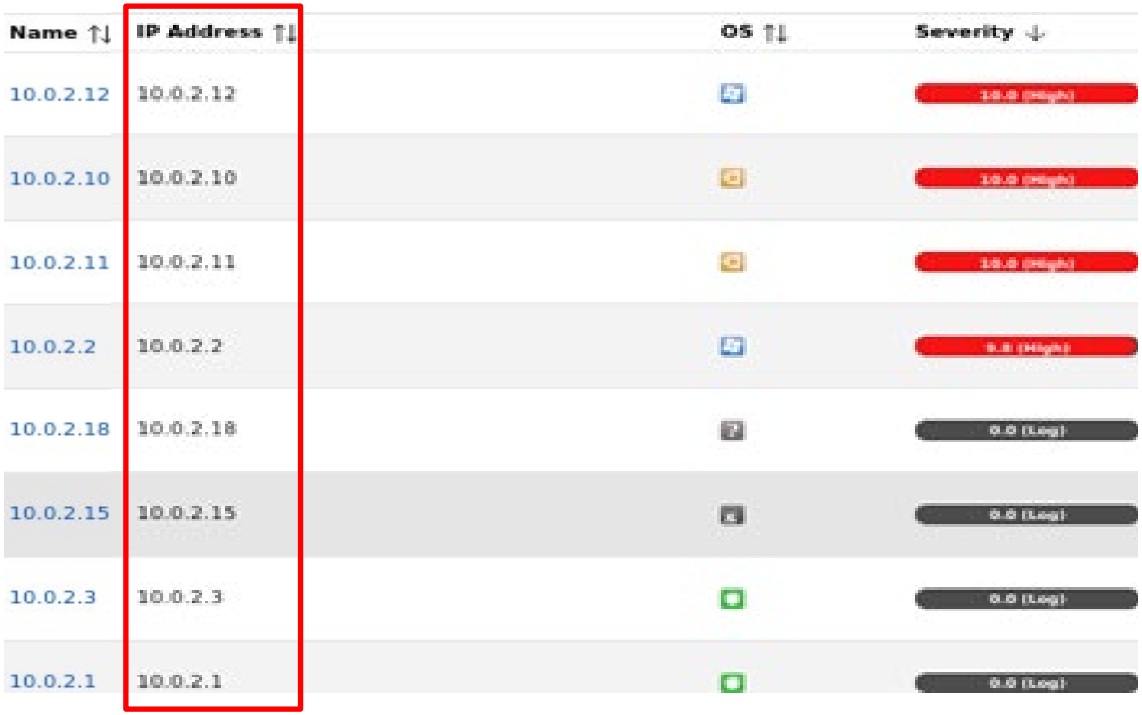


Nomi degli host target

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare i risultati generali relativi ai vari host target



Name	IP Address	OS	Severity
10.0.2.12	10.0.2.12		10.0 (High)
10.0.2.10	10.0.2.10		10.0 (High)
10.0.2.11	10.0.2.11		10.0 (High)
10.0.2.2	10.0.2.2		9.8 (High)
10.0.2.18	10.0.2.18		0.0 (Log)
10.0.2.15	10.0.2.15		0.0 (Log)
10.0.2.3	10.0.2.3		0.0 (Log)
10.0.2.1	10.0.2.1		0.0 (Log)

Indirizzi IP degli host target

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare i risultati generali relativi ai vari host target

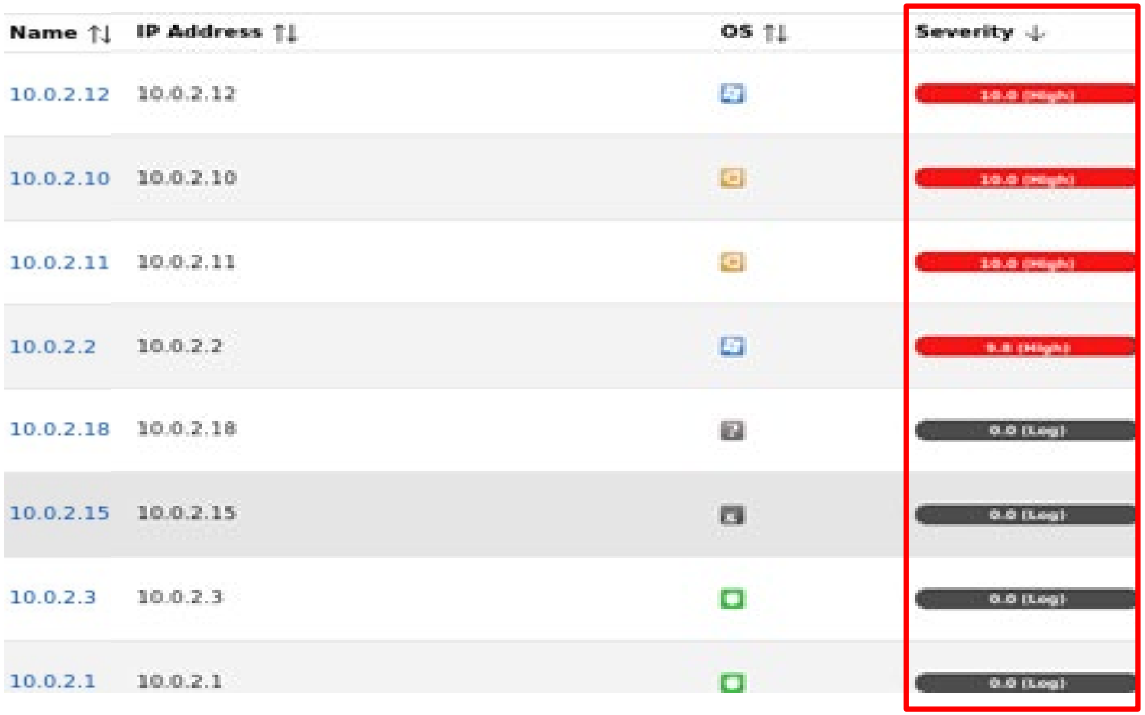
Name	IP Address	OS	Severity
10.0.2.12	10.0.2.12		10.0 (High)
10.0.2.10	10.0.2.10		10.0 (High)
10.0.2.11	10.0.2.11		10.0 (High)
10.0.2.2	10.0.2.2		9.8 (High)
10.0.2.18	10.0.2.18		0.0 (Log)
10.0.2.15	10.0.2.15		0.0 (Log)
10.0.2.3	10.0.2.3		0.0 (Log)
10.0.2.1	10.0.2.1		0.0 (Log)

Sistemi Operativi degli host target

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare i risultati generali relativi ai vari host target



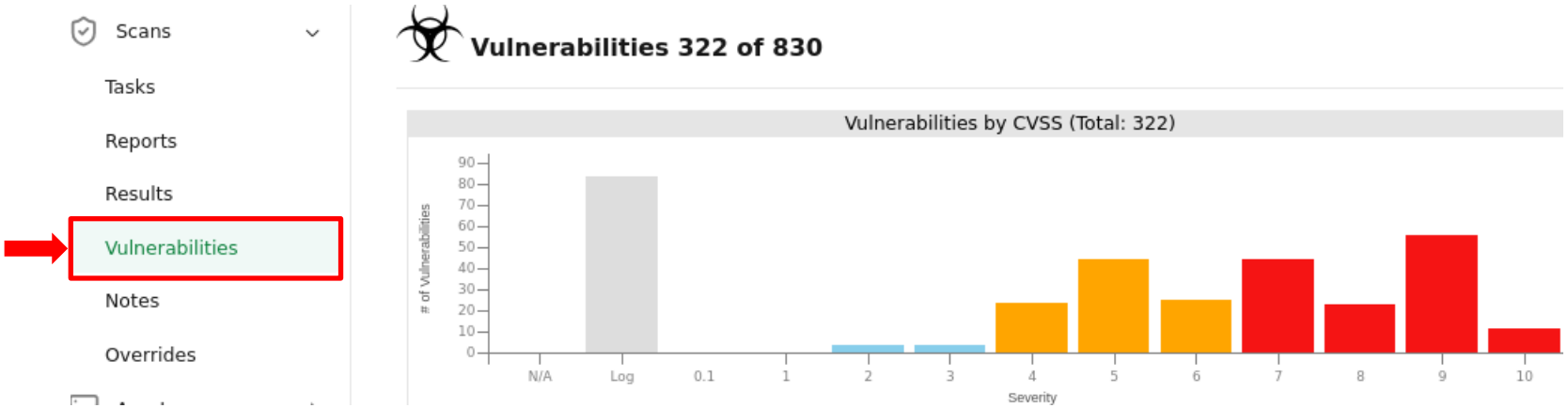
Name	IP Address	OS	Severity
10.0.2.12	10.0.2.12		10.0 (High)
10.0.2.10	10.0.2.10		10.0 (High)
10.0.2.11	10.0.2.11		10.0 (High)
10.0.2.2	10.0.2.2		9.8 (High)
10.0.2.18	10.0.2.18		0.0 (Log)
10.0.2.15	10.0.2.15		0.0 (Log)
10.0.2.3	10.0.2.3		0.0 (Log)
10.0.2.1	10.0.2.1		0.0 (Log)

Livello di Severity massima rilevata per ciascun host target

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione

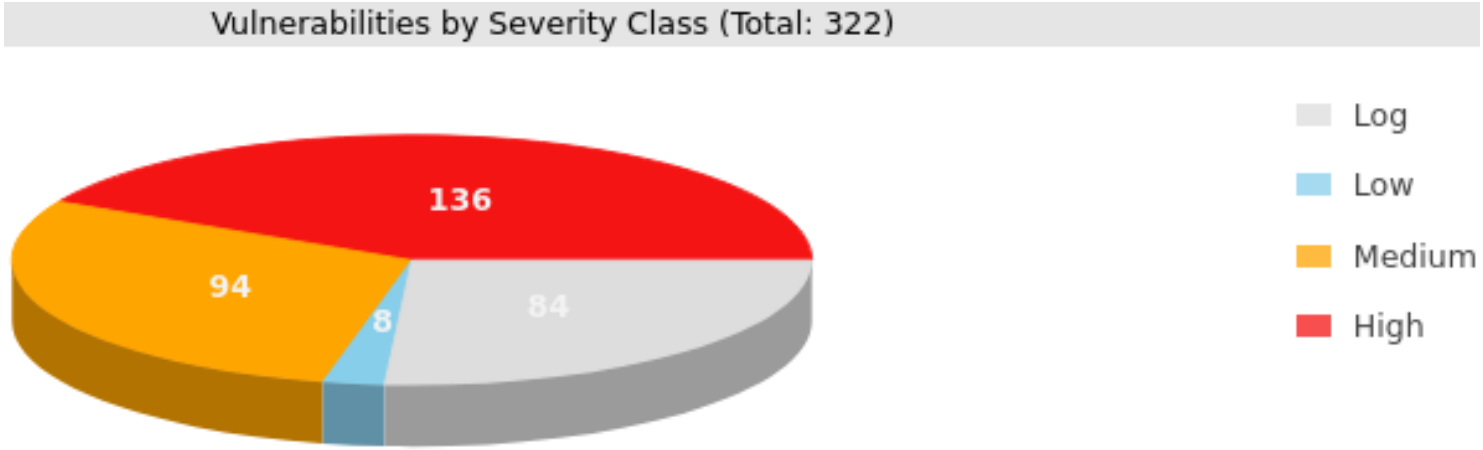
- È possibile visualizzare i risultati generali relativi alle varie vulnerabilità



Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare i risultati generali relativi alle varie vulnerabilità



Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare i risultati generali relativi alle varie vulnerabilità

Name ↑↓	Severity ↓	QoD ↑↓	Results ↑↓	Hosts ↑↓
Elasticsearch End of Life (EOL) Detection	10.0 (High)	80 %	1	1
rlogin Passwordless Login	10.0 (High)	80 %	1	1
Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities	10.0 (High)	99 %	1	1
Tiki Wiki CMS Groupware End of Life (EOL) Detection	10.0 (High)	80 %	1	1
Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Credentials (HTTP)	10.0 (High)	98 %	1	1
PHP End of Life (EOL) Detection - Windows	10.0 (High)	80 %	1	1
The rexec service is running	10.0 (High)	80 %	1	1
Operating System (OS) End of Life (EOL) Detection	10.0 (High)	80 %	2	2
Possible Backdoor: Ingreslock	10.0 (High)	99 %	1	1
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80 %	2	2

Nome Vulnerabilità

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare i risultati generali relativi alle varie vulnerabilità

Name ↑↓	Severity ↓	QoD ↑↓	Results ↑↓	Hosts ↑↓
Elasticsearch End of Life (EOL) Detection	10.0 (High)	80 %	1	1
rlogin Passwordless Login	10.0 (High)	80 %	1	1
Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities	10.0 (High)	99 %	1	1
Tiki Wiki CMS Groupware End of Life (EOL) Detection	10.0 (High)	80 %	1	1
Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Credentials (HTTP)	10.0 (High)	98 %	1	1
PHP End of Life (EOL) Detection - Windows	10.0 (High)	80 %	1	1
The rexec service is running	10.0 (High)	80 %	1	1
Operating System (OS) End of Life (EOL) Detection	10.0 (High)	80 %	2	2
Possible Backdoor: Ingreslock	10.0 (High)	99 %	1	1
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80 %	2	2

Livello di Severity

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare i risultati generali relativi alle varie vulnerabilità

Name ↑↓	Severity ↓	QoD ↑↓	Results ↑↓	Hosts ↑↓
Elasticsearch End of Life (EOL) Detection	10.0 (High)	80 %	1	1
rlogin Passwordless Login	10.0 (High)	80 %	1	1
Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities	10.0 (High)	99 %	1	1
Tiki Wiki CMS Groupware End of Life (EOL) Detection	10.0 (High)	80 %	1	1
Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Credentials (HTTP)	10.0 (High)	98 %	1	1
PHP End of Life (EOL) Detection - Windows	10.0 (High)	80 %	1	1
The rexec service is running	10.0 (High)	80 %	1	1
Operating System (OS) End of Life (EOL) Detection	10.0 (High)	80 %	2	2
Possible Backdoor: Ingreslock	10.0 (High)	99 %	1	1
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80 %	2	2

Percentuale di Quality of Detection (QoD)

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare i risultati generali relativi alle varie vulnerabilità

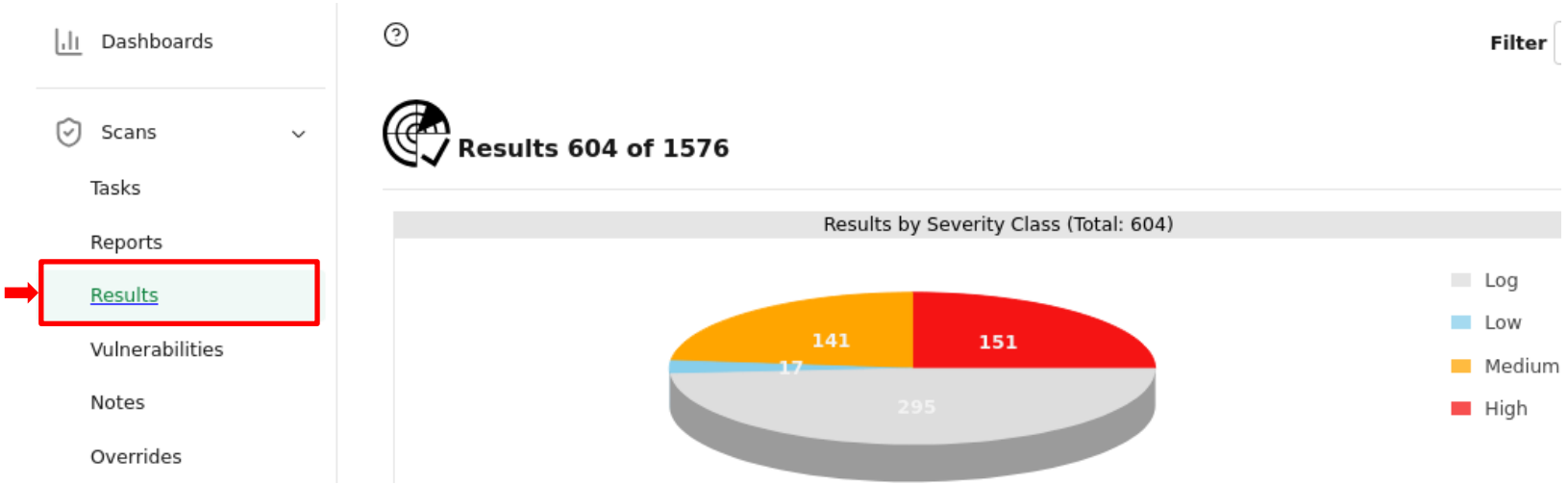
Name ↑↓	Severity ↓	QoD ↑↓	Results ↑↓	Hosts ↑↓
Elasticsearch End of Life (EOL) Detection	10.0 (High)	80 %	1	1
rlogin Passwordless Login	10.0 (High)	80 %	1	1
Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities	10.0 (High)	99 %	1	1
Tiki Wiki CMS Groupware End of Life (EOL) Detection	10.0 (High)	80 %	1	1
Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Credentials (HTTP)	10.0 (High)	98 %	1	1
PHP End of Life (EOL) Detection - Windows	10.0 (High)	80 %	1	1
The rexec service is running	10.0 (High)	80 %	1	1
Operating System (OS) End of Life (EOL) Detection	10.0 (High)	80 %	2	2
Possible Backdoor: Ingreslock	10.0 (High)	99 %	1	1
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80 %	2	2

Numero di Host affetti dalla vulnerabilità

Analisi Automatica delle Vulnerabilità

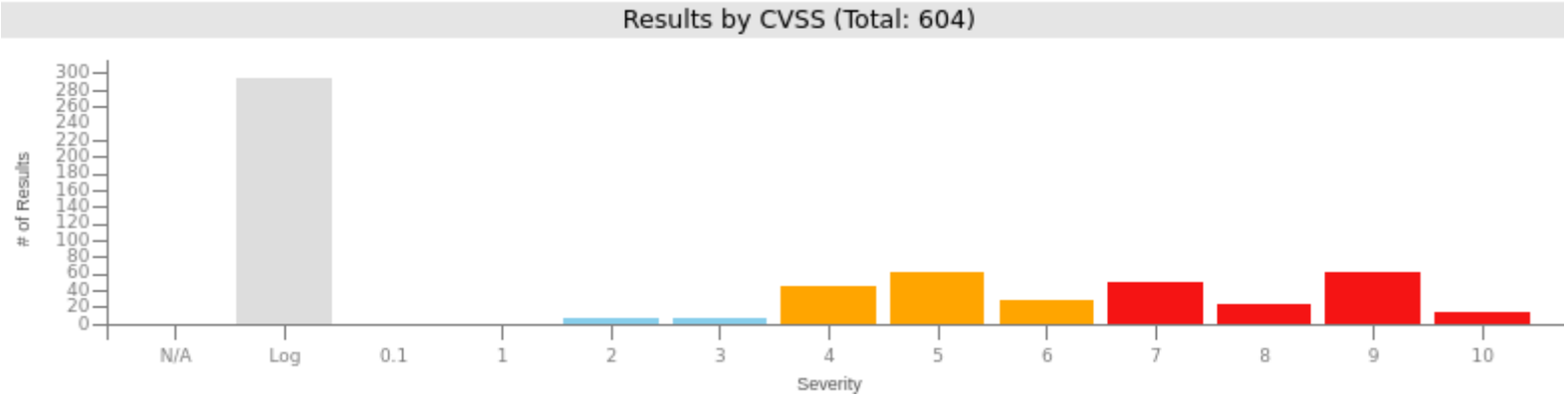
OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare tutte le vulnerabilità presenti nell'asset



Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione



Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare tutte le vulnerabilità presenti nell'asset

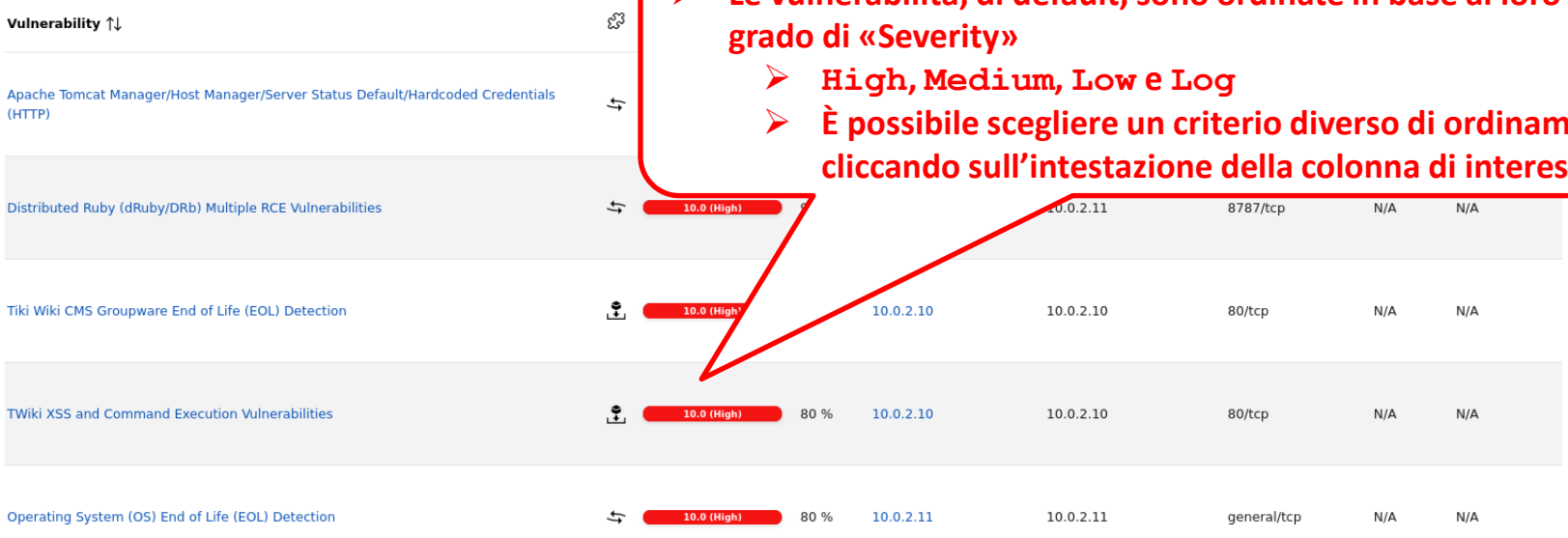
Vulnerability	Severity	QoD	Host		Location	EPSS	
			IP	Name		Score	Percentage
Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Credentials (HTTP)	10.0 (High)	98 %	10.0.2.10	10.0.2.10	8180/tcp	N/A	N/A
Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities	10.0 (High)	99 %	10.0.2.11	10.0.2.11	8787/tcp	N/A	N/A
Tiki Wiki CMS Groupware End of Life (EOL) Detection	10.0 (High)	80 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A
Operating System (OS) End of Life (EOL) Detection	10.0 (High)	80 %	10.0.2.11	10.0.2.11	general/tcp	N/A	N/A

Di default vengono mostrate, in ordine decrescente di gravità, tutte le vulnerabilità rilevate sull'asset (per tutti gli host) dal task di scansione

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare tutte le vulnerabilità presenti nell'asset



Vulnerability ↑↓								
Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Credentials (HTTP)								
Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities		10.0 (High)			10.0.2.11	8787/tcp	N/A	N/A
Tiki Wiki CMS Groupware End of Life (EOL) Detection		10.0 (High)		10.0.2.10	10.0.2.10	80/tcp	N/A	N/A
TWiki XSS and Command Execution Vulnerabilities		10.0 (High)	80 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A
Operating System (OS) End of Life (EOL) Detection		10.0 (High)	80 %	10.0.2.11	10.0.2.11	general/tcp	N/A	N/A

- **Le vulnerabilità, di default, sono ordinate in base al loro grado di «Severity»**
  - **`High`, `Medium`, `Low` e `Log`**
  - **È possibile scegliere un criterio diverso di ordinamento, cliccando sull'intestazione della colonna di interesse**

Di default vengono mostrate, in ordine decrescente di gravità, tutte le vulnerabilità rilevate sull'asset (per tutti gli host) dal task di scansione

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare tutte le vulnerabilità presenti nell'asset

Vulnerability	Severity	QoD	Host IP	Host Name	Location	EPSS Score	EPSS Percentage
Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Credentials (HTTP)	10.0 (High)	98 %	10.0.2.10	10.0.2.10	8180/tcp	N/A	N/A
Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities	10.0 (High)	99 %	10.0.2.11	10.0.2.11	8787/tcp	N/A	N/A
Tiki Wiki CMS Groupware End of Life (EOL) Detection	10.0 (High)	80 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A
Operating System (OS) End of Life (EOL) Detection	10.0 (High)	80 %	10.0.2.11	10.0.2.11	general/tcp	N/A	N/A

Nomi delle vulnerabilità

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare tutte le vulnerabilità presenti nell'asset

Vulnerability		Severity	QoD	Host		Location	EPSS	
				IP	Name		Score	Percentage
Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Credentials (HTTP)		10.0 (High)	98 %	10.0.2.10	10.0.2.10	8180/tcp	N/A	N/A
Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities		10.0 (High)	99 %	10.0.2.11	10.0.2.11	8787/tcp	N/A	N/A
Tiki Wiki CMS Groupware End of Life (EOL) Detection		10.0 (High)	80 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A
TWiki XSS and Command Execution Vulnerabilities		10.0 (High)	80 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A
Operating System (OS) End of Life (EOL) Detection		10.0 (High)	80 %	10.0.2.11	10.0.2.11	general/tcp	N/A	N/A

Tipo di soluzione per eliminare/mitigare le vulnerabilità

Analisi Automatica delle Vulnerabilità
OpenVAS e GVM – Risultati di una Scansione

- **Tipi di Soluzione**

Workaround: Sono disponibili informazioni che possono essere utilizzate per evitare l'esposizione alla vulnerabilità

Mitigation: Sono disponibili informazioni che aiutano a ridurre il rischio della vulnerabilità ma che non la risolvono/eliminano

Vendor-Fix: Sono disponibili informazioni su un *fix* ufficiale rilasciato dall'autore del prodotto (o piattaforma) coinvolto

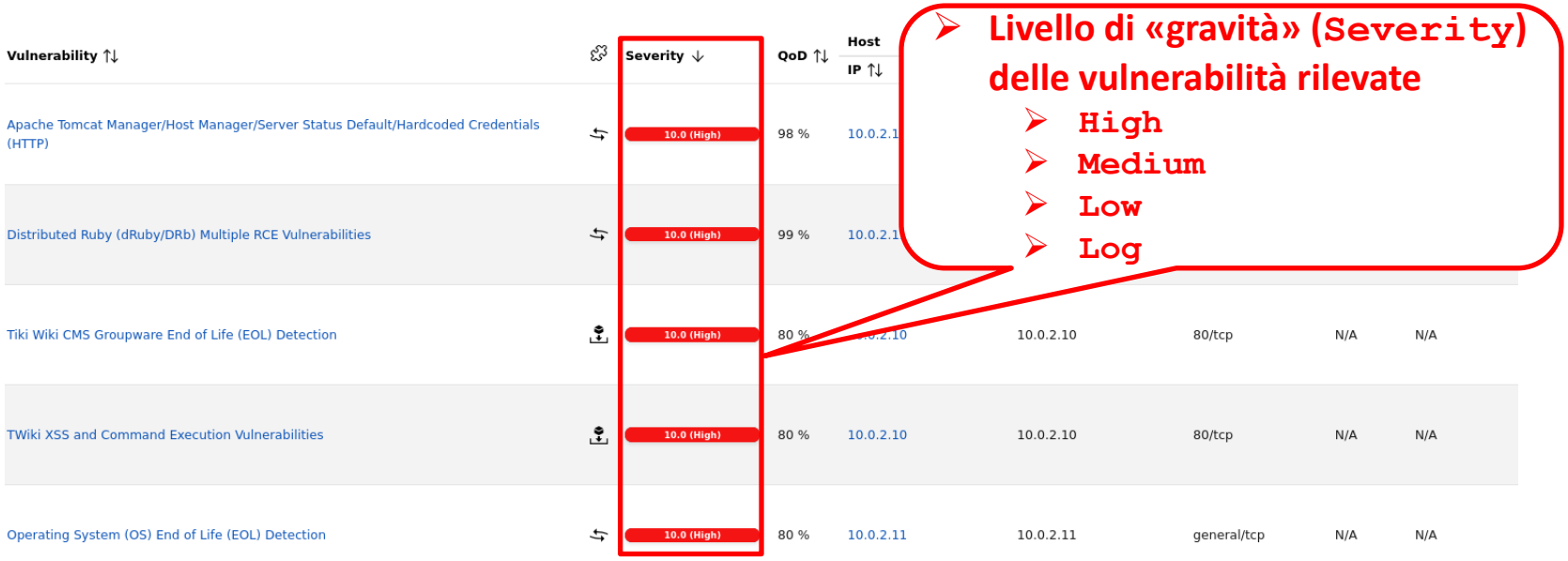
None-Available: Attualmente non è disponibile alcun *fix*

WillNotFix: Non esiste un *fix* per la vulnerabilità e non ce ne sarà mai uno. Questo è spesso il caso in cui un prodotto è rimasto «orfano», a fine vita o deprecato

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare tutte le vulnerabilità presenti nell'asset



Vulnerability ↑↓	Severity ↓	QoD ↑↓	Host IP ↑↓				
Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Credentials (HTTP)	10.0 (High)	98 %	10.0.2.1				
Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities	10.0 (High)	99 %	10.0.2.1				
Tiki Wiki CMS Groupware End of Life (EOL) Detection	10.0 (High)	80 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A
Operating System (OS) End of Life (EOL) Detection	10.0 (High)	80 %	10.0.2.11	10.0.2.11	general/tcp	N/A	N/A

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare tutte le vulnerabilità presenti nell'asset

Vulnerability	Severity	QoD	Host IP	Host Name	Location	EPSS Score	EPSS Percentage
Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Credentials (HTTP)	10.0 (High)	98 %	10.0.2.10				
Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities	10.0 (High)	99 %	10.0.2.11				
Tiki Wiki CMS Groupware End of Life (EOL) Detection	10.0 (High)	80 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A
Operating System (OS) End of Life (EOL) Detection	10.0 (High)	80 %	10.0.2.11	10.0.2.11	general/tcp	N/A	N/A

- **Quality of Detection (QoD)**
  - **Valore compreso tra 0% e 100% che descrive l'affidabilità del rilevamento delle vulnerabilità o del prodotto**

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare tutte le vulnerabilità presenti nell'asset

Vulnerability	Severity	QoD	Host		Location	EPSS	
			IP	Name		Score	Percentage
Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Credentials (HTTP)	10.0 (High)	98 %	10.0.2.10	10.0.2.10	8180/tcp	N/A	N/A
Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities	10.0 (High)	99 %	10.0.2.11	10.0.2.11	8787/tcp	N/A	N/A
Tiki Wiki CMS Groupware End of Life (EOL) Detection	10.0 (High)	80 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A
Operating System (OS) End of Life (EOL) Detection	10.0 (High)	80 %	10.0.2.11	10.0.2.11	general/tcp	N/A	N/A

- **Macchine (host) target appartenenti all'asset**

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare tutte le vulnerabilità presenti nell'asset

Vulnerability	Severity	QoD	Host		Location	EPSS	
			IP	Name		Score	Percentage
Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Credentials (HTTP)	10.0 (High)	98 %	10.0.2.10	10.0.2.10	8180/tcp	N/A	N/A
Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities	10.0 (High)	99 %	10.0.2.11	10.0.2.11	8787/tcp	N/A	N/A
Tiki Wiki CMS Groupware End of Life (EOL) Detection	10.0 (High)	80 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A
Operating System (OS) End of Life (EOL) Detection	10.0 (High)	80 %	10.0.2.11	10.0.2.11	general/tcp	N/A	N/A

- **Porte/protocolli affetti dalle vulnerabilità**

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare tutte le vulnerabilità presenti nell'asset

Vulnerability	Severity	QoD	Host		Location	EPSS	
			IP	Name		Score	Percentage
Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Credentials (HTTP)	10.0 (High)	98 %	10.0.2.10	10.0.2.10	8180/tcp	N/A	N/A
Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities	10.0 (High)	99 %	10.0.2.11	10.0.2.11	8787/tcp	N/A	N/A
Tiki Wiki CMS Groupware End of Life (EOL) Detection	10.0 (High)	80 %	10.0.2.10		80/tcp	N/A	N/A
TWiki XSS and Command Execution Vulnerabilities					80/tcp	N/A	N/A
Operating System (OS) End of Life (EOL) Detection					general/tcp	N/A	N/A

- **EPSS (Exploit Prediction Scoring System): consente la prioritizzazione delle vulnerabilità, prevedendo la probabilità che una vulnerabilità venga sfruttata**

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare le informazioni su una singola vulnerabilità

Vulnerability	Severity	QoD	Host IP	Host Name	Location	EPSS Score	EPSS Percentage
Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Credentials (HTTP)	10.0 (High)	98 %	10.0.2.10	10.0.2.10	8180/tcp	N/A	N/A
Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities	10.0 (High)	99 %	10.0.2.11	10.0.2.11	8787/tcp	N/A	N/A
Tiki Wiki CMS Groupware End of Life (EOL) Detection	10.0 (High)	80 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A
Operating System (OS) End of Life (EOL) Detection	10.0 (High)	80 %	10.0.2.11	10.0.2.11	general/tcp	N/A	N/A

Vulnerabilità «Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Credentials (HTTP)»

Analisi Automatica delle Vulnerabilità
OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare le informazioni su una singola vulnerabilità

Summary

The Apache Tomcat Manager/Host Manager/Server Status is using default or known hardcoded credentials.

Detection Result

```
It was possible to login into the Tomcat Manager at http://10.0.2.10:8180/manager/html using user "tomcat" with password
"tomcat"

It was possible to login into the Tomcat Server Status at http://10.0.2.10:8180/manager/status using user "tomcat" with password
"tomcat"
```

Product Detection Result

Product	cpe:/a:apache:tomcat:5.5.25
Method	Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.107652)
Log	View details of product detection

Vulnerabilità «Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Credentials (HTTP)»

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare le informazioni su una singola vulnerabilità

Detection Method

Details: Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Cre...OID: 1.3.6.1.4.1.25623.1.0.103550

Version used: 2023-07-25T05:05:58Z

Impact

An attacker can exploit this issue to upload and execute arbitrary
code, which will facilitate a complete compromise of the affected computer.

Solution

Solution Type: ⇆ Mitigation
Change the password to a strong one or remove the user from tomcat-users.xml.

Vulnerabilità «Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Credentials (HTTP)»

Analisi Automatica delle Vulnerabilità
OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare le informazioni su una singola vulnerabilità

References

CVE	CVE-2010-4094 CVE-2009-3548 CVE-2009-4189 CVE-2009-3099 CVE-2009-3843 CVE-2009-4188 CVE-2010-0557
CERT	DFN-CERT-2012-1832 DFN-CERT-2011-0185 DFN-CERT-2010-0801 DFN-CERT-2010-0690 DFN-CERT-2009-1640
Other	https://www.zerodayinitiative.com/advisories/ZDI-10-214/ http://www.securityfocus.com/bid/36258 http://www.securityfocus.com/bid/36954 http://www.securityfocus.com/bid/37086 http://www.securityfocus.com/bid/38084 http://www.securityfocus.com/bid/44172 http://www.securityfocus.com/bid/79264 http://www.securityfocus.com/bid/79351 https://www.zerodayinitiative.com/advisories/ZDI-09-085/

Vulnerabilità «Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Credentials (HTTP)»

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare le informazioni su una singola vulnerabilità

Vulnerability	Severity	QoD	Host IP	Host Name	Location	EPSS Score	EPSS Percentage
Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Credentials (HTTP)	10.0 (High)	98 %	10.0.2.10	10.0.2.10	8180/tcp	N/A	N/A
Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities	10.0 (High)	99 %	10.0.2.11	10.0.2.11	8787/tcp	N/A	N/A
Tiki Wiki CMS Groupware End of Life (EOL) Detection	10.0 (High)	80 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A
Operating System (OS) End of Life (EOL) Detection	10.0 (High)	80 %	10.0.2.11	10.0.2.11	general/tcp	N/A	N/A

Vulnerabilità «Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities»

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare le informazioni su una singola vulnerabilità

Summary

Systems using Distributed Ruby (dRuby/DRb), which is available in Ruby versions 1.6 and later, may permit unauthorized systems to execute distributed commands.

Detection Result

The service is running in $SAFE >= 1 mode. However it is still possible to run arbitrary syscall commands on the remote host. Sending an invalid syscall the service returned the following response:

Flo:Errno::ENOSYS:bt["3/usr/lib/ruby/1.8/drb/drb.rb:1555:in `syscall'"0/usr/lib/ruby/1.8/drb/drb.rb:1555:in `send'"4/usr/lib/ruby/1.8/drb/drb.rb:1555:in `__send__'"A/usr/lib/ruby/1.8/drb/drb.rb:1555:in `perform_without_block'"3/usr/lib/ruby/1.8/drb/drb.rb:1515:in `perform'"5/usr/lib/ruby/1.8/drb/drb.rb:1589:in `main_loop'"0/usr/lib/ruby/1.8/drb/drb.rb:1585:in `loop'"5/usr/lib/ruby/1.8/drb/drb.rb:1585:in `main_loop'"1/usr/lib/ruby/1.8/drb/drb.rb:1581:in `start'"5/usr/lib/ruby/1.8/drb/drb.rb:1581:in `main_loop'"//usr/lib/ruby/1.8/drb/drb.rb:1430:in `run'"1/usr/lib/ruby/1.8/drb/drb.rb:1427:in `start'"//usr/lib/ruby/1.8/drb/drb.rb:1427:in `run'"6/usr/lib/ruby/1.8/drb/drb.rb:1347:in `initialize'"//usr/lib/ruby/1.8/drb/drb.rb:1627:in `new'"9/usr/lib/ruby/1.8/drb/drb.rb:1627:in `start_service'"%/usr/sbin/druby_timeserver.rb:12:errnoi+:mesg"Function not implemented

Vulnerabilità «Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities»

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare le informazioni su una singola vulnerabilità

Detection Method

Send a crafted command to the service and check for a remote command execution via the instance_eval or syscall requests.

Details: Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities OID: 1.3.6.1.4.1.25623.1.0.108010

Version used: 2024-06-28T05:05:33Z

Impact

By default, Distributed Ruby does not impose restrictions on allowed hosts or set the $SAFE environment variable to prevent privileged activities. If other controls are not in place, especially if the Distributed Ruby process runs with elevated privileges, an attacker could execute arbitrary system commands or Ruby scripts on the Distributed Ruby server. An attacker may need to know only the URI of the listening Distributed Ruby server to submit Ruby commands.

Vulnerabilità «`Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities`»

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione

- È possibile visualizzare le informazioni su una singola vulnerabilità

Solution

Solution Type: ⇆ Mitigation
Administrators of environments that rely on Distributed Ruby should ensure that appropriate controls are in place. Code-level controls may include:

- Implementing taint on untrusted input

- Setting $SAFE levels appropriately (>=2 is recommended if untrusted hosts are allowed to submit Ruby commands, and >=3 may be appropriate)

- Including drb/acl.rb to set ACLEntry to restrict access to trusted hosts

References

Other
https://tools.cisco.com/security/center/viewAlert.x?alertId=22750
http://www.securityfocus.com/bid/47071
http://blog.recurity-labs.com/archives/2011/05/12/druby_for_penetration_testers/
http://www.ruby-doc.org/stdlib-1.9.3/libdoc/drb/rdoc/DRb.html

Vulnerabilità «`Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities`»

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione (Singolo Host)

- È possibile visualizzare le vulnerabilità relative ad un singolo host target

Selezioniamo l'host target di interesse

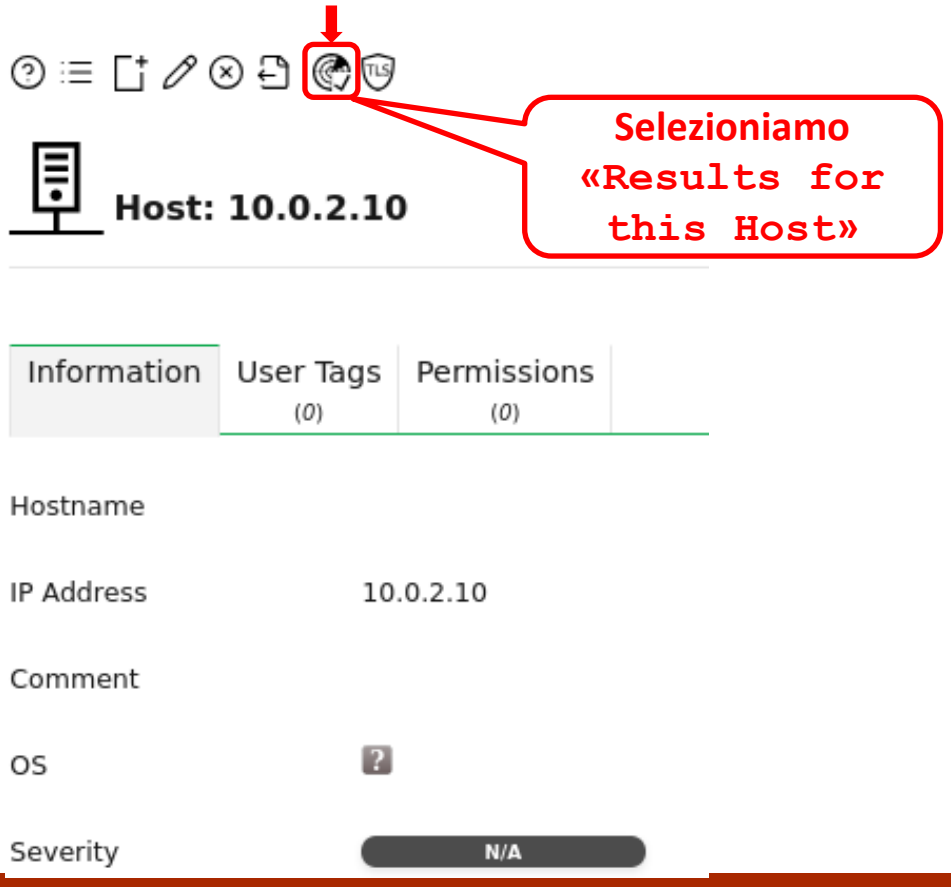
Vulnerability	Severity	QoD	Host IP				Percentage
Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Credentials (HTTP)	10.0 (High)	98 %	10.0.2.10	10.0.2.10	8180/tcp	N/A	N/A
Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities	10.0 (High)	99 %	10.0.2.11	10.0.2.11	8787/tcp	N/A	N/A
Tiki Wiki CMS Groupware End of Life (EOL) Detection	10.0 (High)	80 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A
Operating System (OS) End of Life (EOL) Detection	10.0 (High)	80 %	10.0.2.11	10.0.2.11	general/tcp	N/A	N/A

Host target: indirizzo IP `10.0.2.10`

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione (Singolo Host)

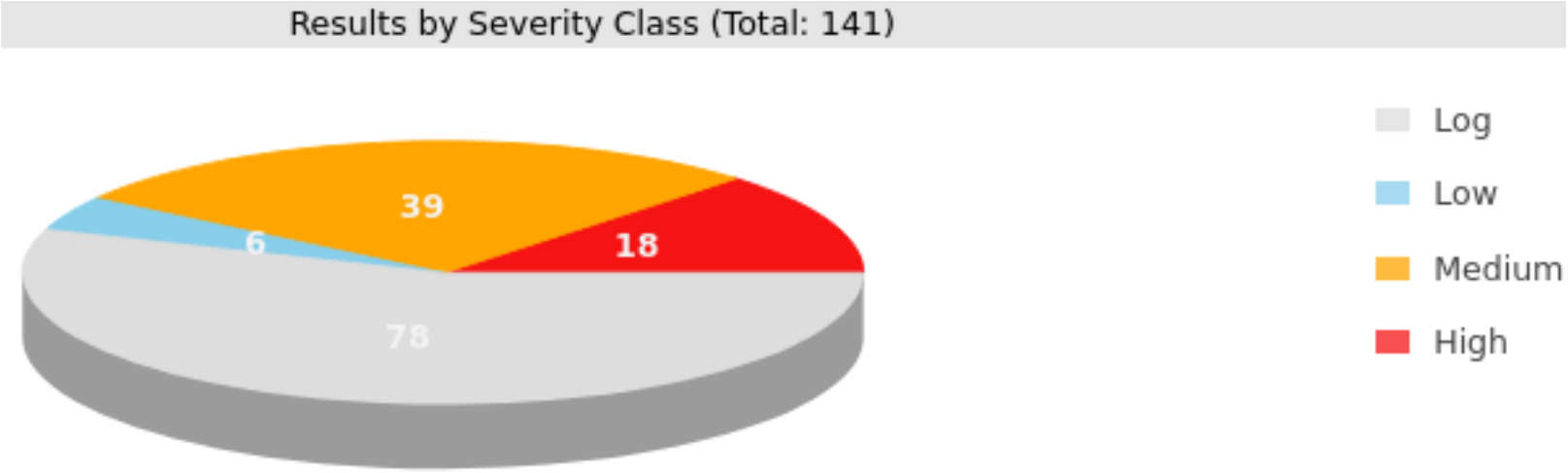
- È possibile visualizzare le vulnerabilità relative ad un singolo host target



Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione (Singolo Host)

- È possibile visualizzare le vulnerabilità relative ad un singolo host target

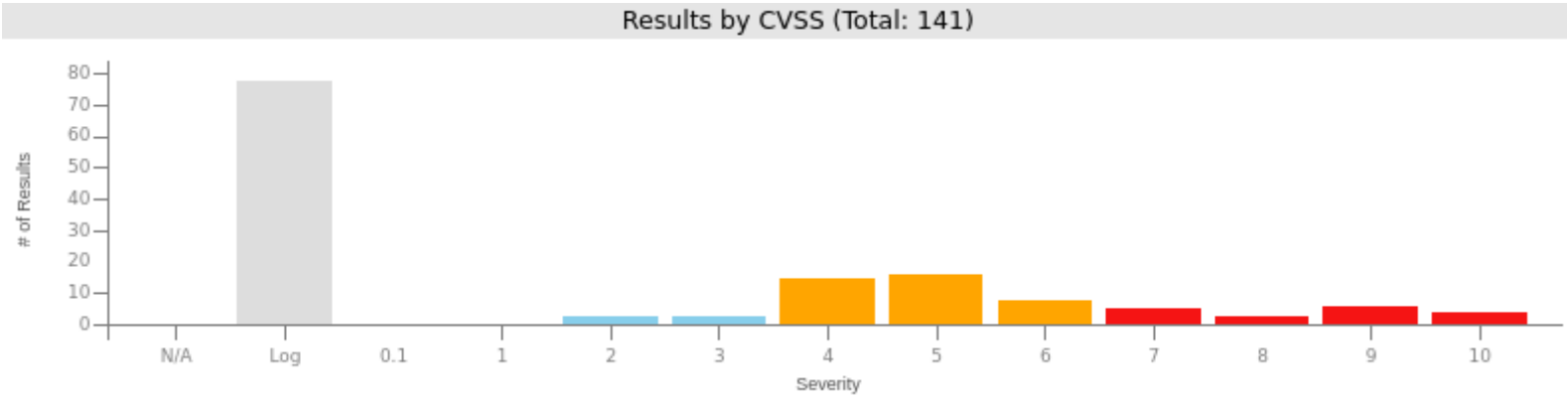


Host target: indirizzo IP `10.0.2.10`

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione (Singolo Host)

- È possibile visualizzare le vulnerabilità relative ad un singolo host target



Host target: indirizzo IP `10.0.2.10`

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione (Singolo Host)

- È possibile visualizzare le vulnerabilità relative ad un singolo host target

Vulnerability ↑	Severity ↑↓	QoD ↑↓	Host		Location ↑↓	EPSS	
			IP ↑↓	Name ↑↓		Score ↑↓	Percentage ↑↓
Allowed HTTP Methods Enumeration	0.0 (Log)	70 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A
Apache HTTP Server Detection Consolidation	0.0 (Log)	80 %	10.0.2.10	10.0.2.10	general/tcp	N/A	N/A
Apache HTTP Server ETag Header Information Disclosure Weakness	4.3 (Medium)	80 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A
Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	4.3 (Medium)	99 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A
Apache JServ Protocol (AJP) v1.3 Detection	0.0 (Log)	80 %	10.0.2.10	10.0.2.10	8009/tcp	N/A	N/A
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	9.8 (High)	99 %	10.0.2.10	10.0.2.10	8009/tcp	N/A	N/A
Apache Tomcat 'cal2.jsp' XSS Vulnerability - Active Check	4.3 (Medium)	70 %	10.0.2.10	10.0.2.10	8180/tcp	N/A	N/A

Di default le vulnerabilità vengono mostrate in ordine alfabetico

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione (Singolo Host)

- È possibile visualizzare le vulnerabilità relative ad un singolo host target

- **È possibile ordinare in base a vari criteri le vulnerabilità rilevate**
  - **Ad es., in base al livello di «`Severity`»**

Vulnerability	Severity	QoD	IP	Name	Location	Score	Percentage
Allowed HTTP Methods Enumeration	0.0 (Log)	70 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A
Apache HTTP Server Detection Consolidation	0.0 (Log)	80 %	10.0.2.10	10.0.2.10	general/tcp	N/A	N/A
Apache HTTP Server ETag Header Information Disclosure Weakness	4.3 (Medium)	80 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A
Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	4.3 (Medium)	99 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A
Apache JServ Protocol (AJP) v1.3 Detection	0.0 (Log)	80 %	10.0.2.10	10.0.2.10	8009/tcp	N/A	N/A
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	9.8 (High)	99 %	10.0.2.10	10.0.2.10	8009/tcp	N/A	N/A
Apache Tomcat 'cal2.jsp' XSS Vulnerability - Active Check	4.3 (Medium)	70 %	10.0.2.10	10.0.2.10	8180/tcp	N/A	N/A

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione (Singolo Host)

- È possibile visualizzare le vulnerabilità relative ad un singolo host target

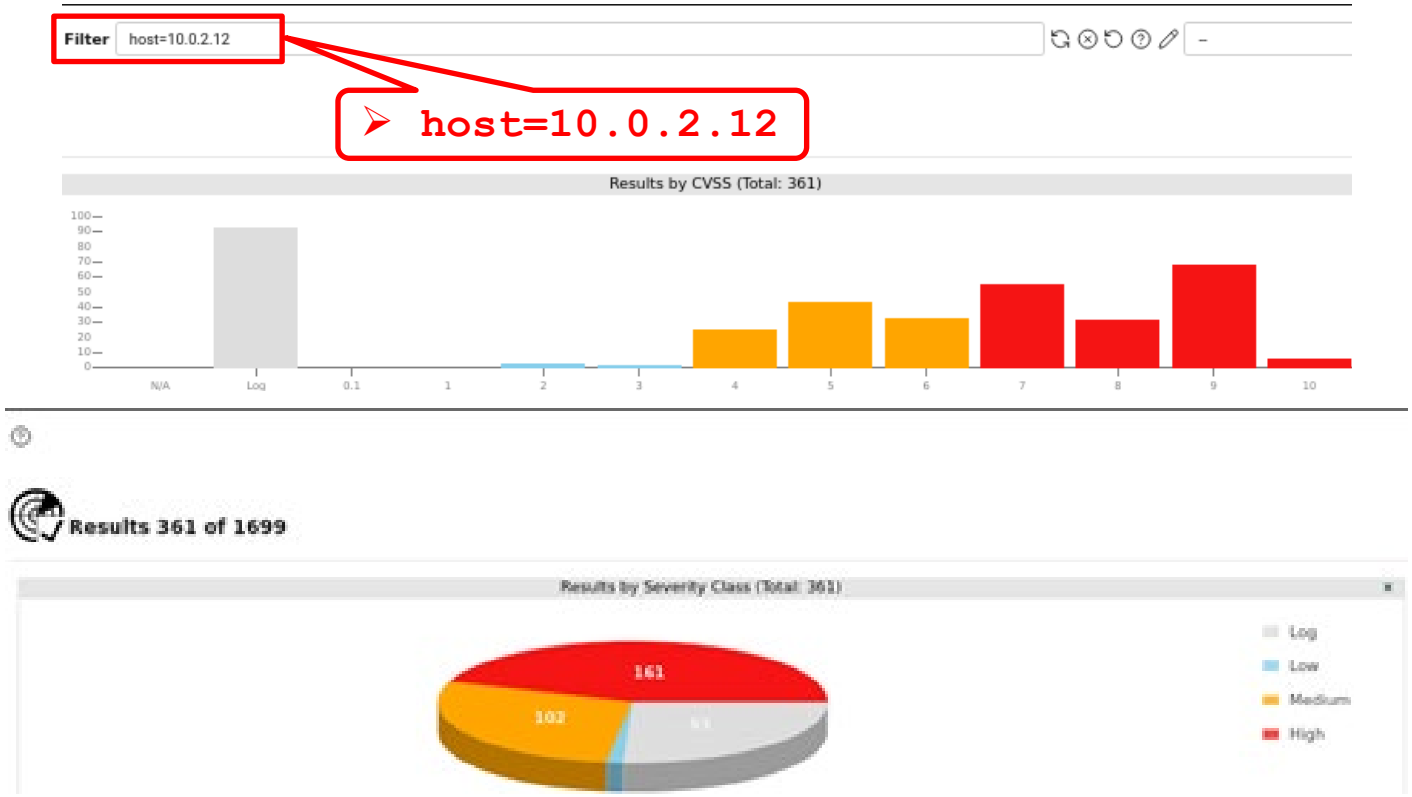
Vulnerability ↑↓	Severity ↓	QoD ↑↓	Host		Location ↑↓	EPSS		Created ↑↓
			IP ↑↓	Name ↑↓		Score ↑↓	Percentage ↑↓	
Tiki Wiki CMS Groupware End of Life (EOL) Detection	10.0 (High)	80 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A	Wed, May 7, 2025 4:29 PM
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80 %	10.0.2.10	10.0.2.10	80/tcp	N/A	N/A	Wed, May 7, 2025 4:29 PM
Operating System (OS) End of Life (EOL) Detection	10.0 (High)	80 %	10.0.2.10	10.0.2.10	general/tcp	N/A	N/A	Wed, May 7, 2025 4:16 PM
Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Credentials (HTTP)	10.0 (High)	98 %	10.0.2.10	10.0.2.10	8180/tcp	N/A	N/A	Wed, May 7, 2025 4:32 PM
HTTP Brute Force Logins With Default Credentials Reporting	9.8 (High)	95 %	10.0.2.10	10.0.2.10	8180/tcp	N/A	N/A	Wed, May 7, 2025 4:32 PM
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	9.8 (High)	99 %	10.0.2.10	10.0.2.10	8009/tcp	N/A	N/A	Wed, May 7, 2025 4:36 PM

Vulnerabilità ordinate in base al loro livello di «gravità» (`Severity`)

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione (Singolo Host)

- È possibile visualizzare le vulnerabilità relative ad altri host target, utilizzando il filtro «**`host`**»



Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione (Singolo Host)

- È possibile visualizzare le vulnerabilità relative ad altri host target, utilizzando il filtro «**`host`**»

Vulnerability ↑↓		Severity ↓	QoD ↑↓
Apache Tomcat End of Life (EOL) Detection - Windows		10.0 (High)	80 %
Elasticsearch End of Life (EOL) Detection		10.0 (High)	80 %
PHP End of Life (EOL) Detection - Windows		10.0 (High)	80 %
Apache HTTP Server End of Life (EOL) Detection - Windows		10.0 (High)	80 %
PHP '_php_stream_scandir()' Buffer Overflow Vulnerability - Windows		10.0 (High)	80 %
PHP 'com_print_typeinfo()' Remote Code Execution Vulnerability - Windows		10.0 (High)	80 %
PHP 'type confusion' Denial of Service Vulnerability - Windows		9.8 (High)	80 %
PHP < 5.6.29, 7.0.x < 7.0.14 DoS Vulnerability - Windows		9.8 (High)	80 %
PHP < 8.1.31, 8.2.x < 8.2.26, 8.3.x < 8.3.14 Multiple Vulnerabilities - Windows		9.8 (High)	80 %
PHP < 8.0.30, 8.1.x < 8.1.22, 8.2.x < 8.2.9 Security Update - Windows		9.8 (High)	80 %

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione (Singolo Host)

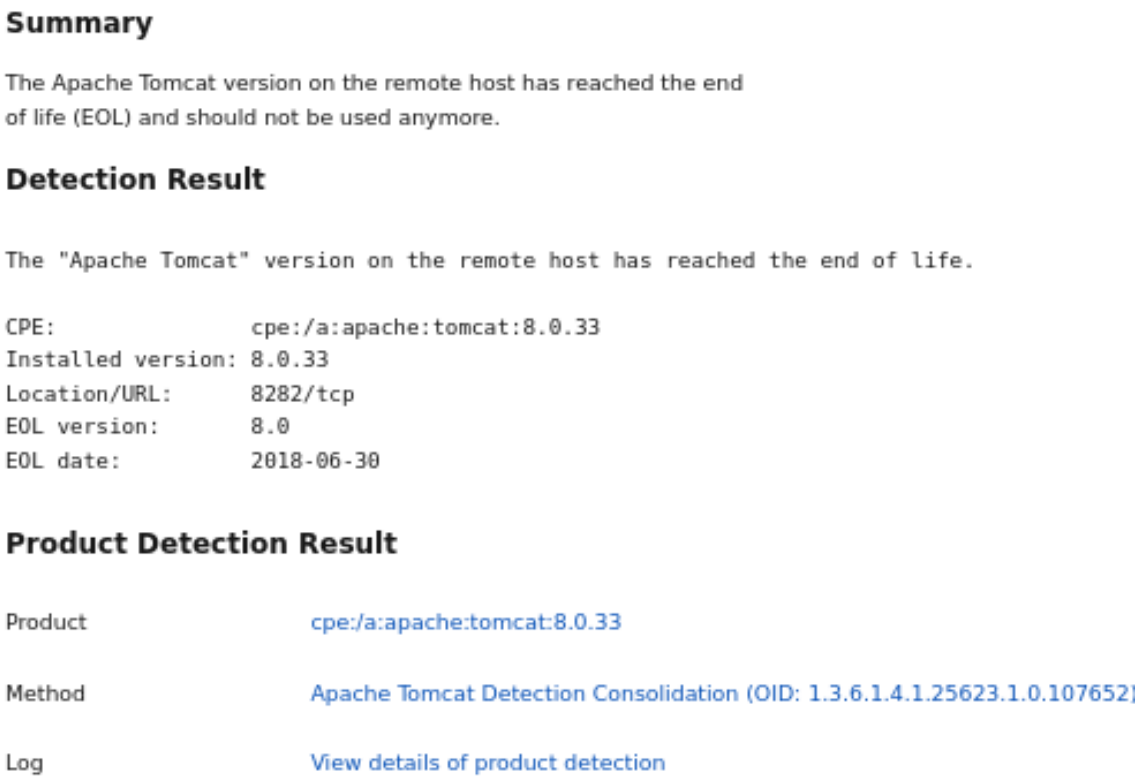
- È possibile visualizzare le vulnerabilità relative ad altri host target, utilizzando il filtro «**`host`**»

Vulnerability ↑↓		Severity ↓	QoD ↑↓
Apache Tomcat End of Life (EOL) Detection - Windows		10.0 (High)	80 %
Elasticsearch End of Life (EOL) Detection		10.0 (High)	80 %
PHP End of Life (EOL) Detection - Windows		10.0 (High)	80 %
Apache HTTP Server End of Life (EOL) Detection - Windows		10.0 (High)	80 %
PHP '_php_stream_scandir()' Buffer Overflow Vulnerability - Windows		10.0 (High)	80 %
PHP 'com_print_typeinfo()' Remote Code Execution Vulnerability - Windows		10.0 (High)	80 %
PHP 'type confusion' Denial of Service Vulnerability - Windows		9.8 (High)	80 %
PHP < 5.6.29, 7.0.x < 7.0.14 DoS Vulnerability - Windows		9.8 (High)	80 %
PHP < 8.1.31, 8.2.x < 8.2.26, 8.3.x < 8.3.14 Multiple Vulnerabilities - Windows		9.8 (High)	80 %
PHP < 8.0.30, 8.1.x < 8.1.22, 8.2.x < 8.2.9 Security Update - Windows		9.8 (High)	80 %

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione (Singolo Host)

- È possibile visualizzare le vulnerabilità relative ad altri host target, utilizzando il filtro «**`host`**»



Summary

The Apache Tomcat version on the remote host has reached the end of life (EOL) and should not be used anymore.

Detection Result

The "Apache Tomcat" version on the remote host has reached the end of life.

CPE: cpe:/a:apache:tomcat:8.0.33
Installed version: 8.0.33
Location/URL: 8282/tcp
EOL version: 8.0
EOL date: 2018-06-30

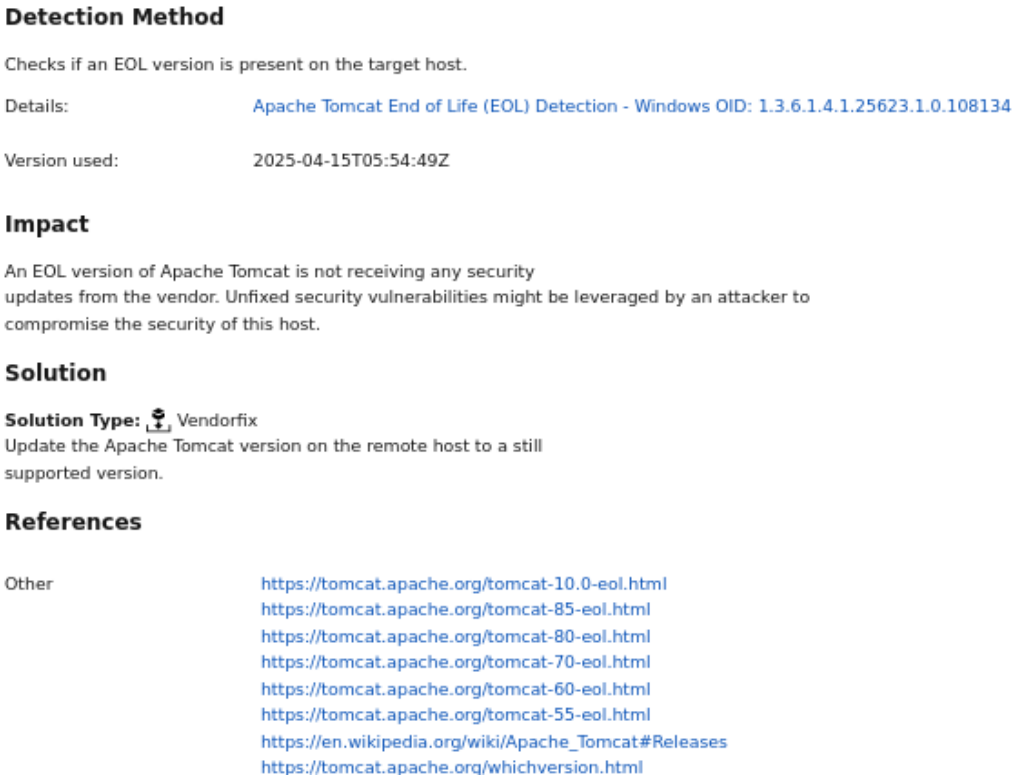
Product Detection Result

Product	cpe:/a:apache:tomcat:8.0.33
Method	Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.107652)
Log	View details of product detection

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Risultati di una Scansione (Singolo Host)

- È possibile visualizzare le vulnerabilità relative ad altri host target, utilizzando il filtro «**`host`**»



Detection Method

Checks if an EOL version is present on the target host.

Details: Apache Tomcat End of Life (EOL) Detection - Windows OID: 1.3.6.1.4.1.25623.1.0.108134

Version used: 2025-04-15T05:54:49Z

Impact

An EOL version of Apache Tomcat is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution

Solution Type: Vendorfix
Update the Apache Tomcat version on the remote host to a still supported version.

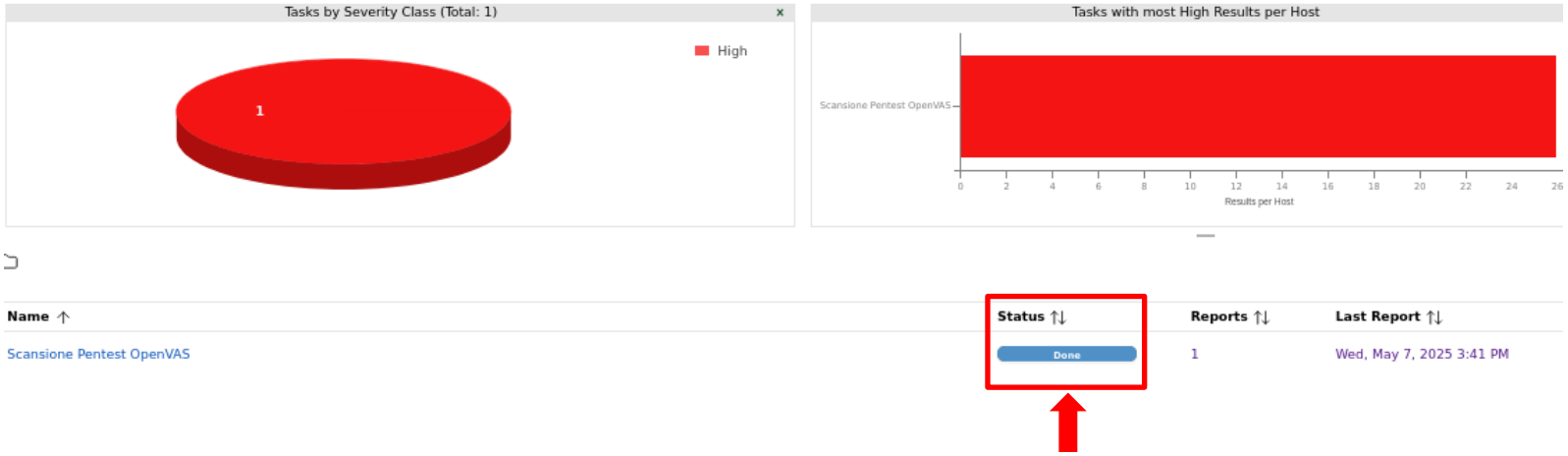
References

Other
https://tomcat.apache.org/tomcat-10.0-eol.html
https://tomcat.apache.org/tomcat-85-eol.html
https://tomcat.apache.org/tomcat-80-eol.html
https://tomcat.apache.org/tomcat-70-eol.html
https://tomcat.apache.org/tomcat-60-eol.html
https://tomcat.apache.org/tomcat-55-eol.html
https://en.wikipedia.org/wiki/Apache_Tomcat#Releases
https://tomcat.apache.org/whichversion.html

Analisi Automatica delle Vulnerabilità

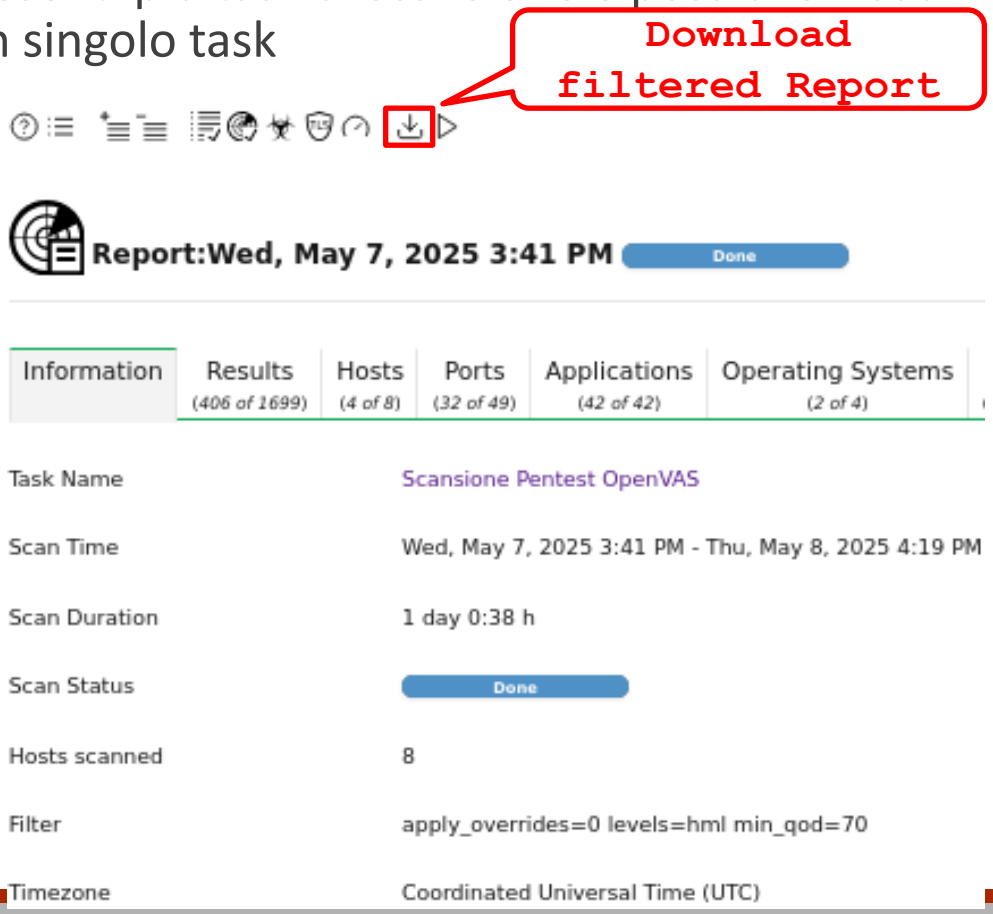
OpenVAS e GVM – Generazione Report

- Se sono presenti più task di scansione è possibile visualizzare i risultati relativi ad un singolo task



Analisi Automatica delle Vulnerabilità
OpenVAS e GVM – Generazione Report

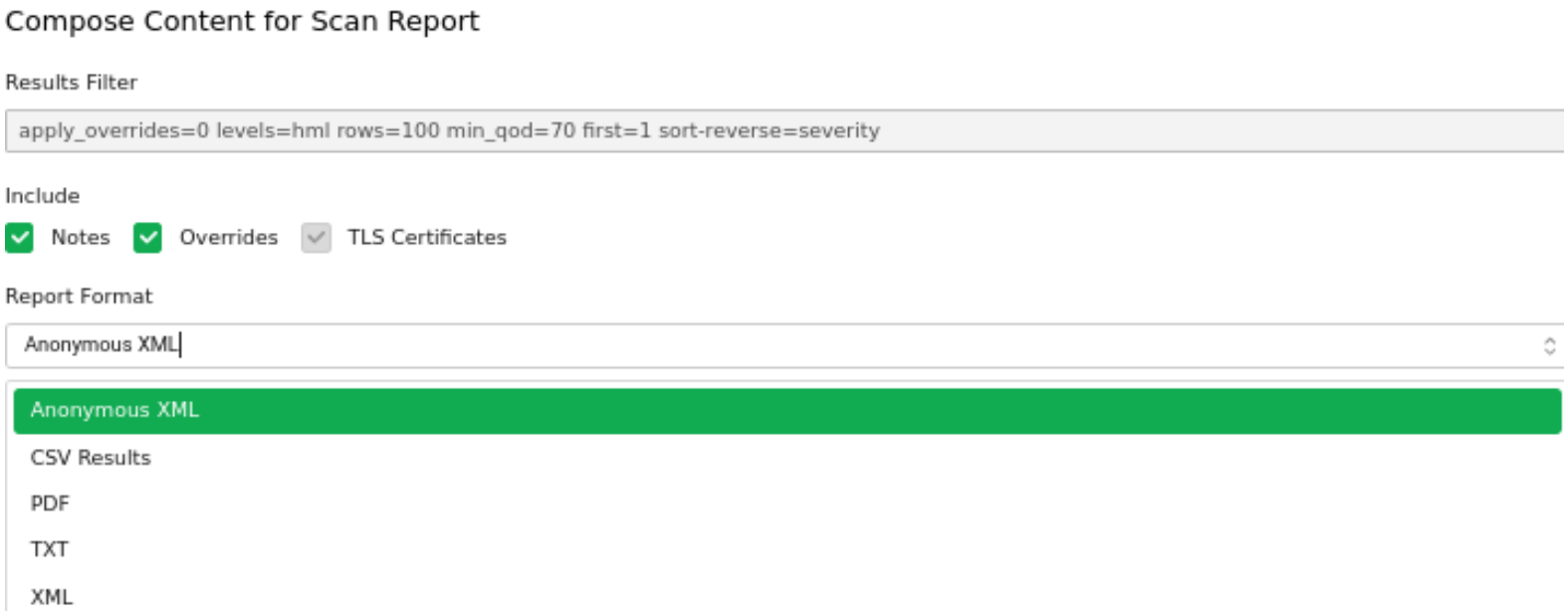
- Se sono presenti più task di scansione è possibile visualizzare i risultati relativi ad un singolo task



Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Generazione Report

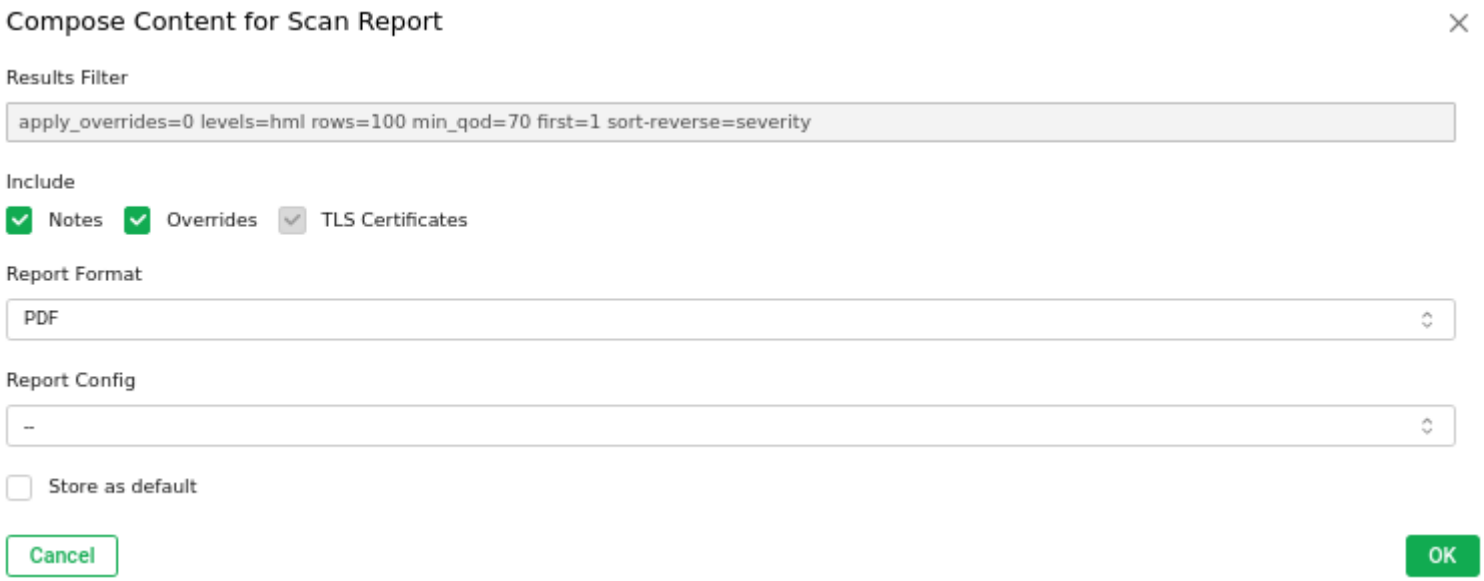
- OpenVAS consente di generare ed esportare in vari formati (*CSV*, *XML*, *PDF*, etc) i report relativi alle scansioni effettuate



Analisi Automatica delle Vulnerabilità

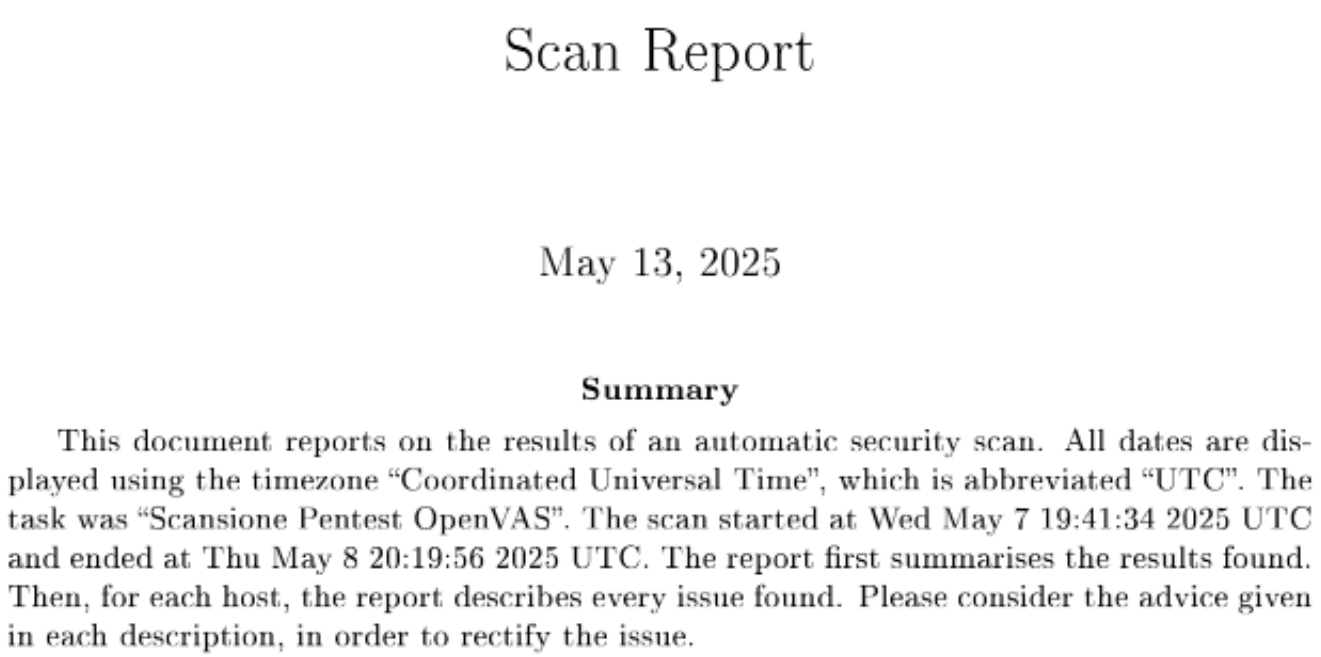
OpenVAS e GVM – Generazione Report

- OpenVAS consente di generare ed esportare in vari formati (*CSV*, XML, *PDF*, etc) i report relativi alle scansioni effettuate



Analisi Automatica delle Vulnerabilità
OpenVAS e GVM – Generazione Report

- OpenVAS consente di generare ed esportare in vari formati (*CSV*, *XML*, *PDF*, etc) i report relativi alle scansioni effettuate



Scan Report

May 13, 2025

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Scansione Pentest OpenVAS". The scan started at Wed May 7 19:41:34 2025 UTC and ended at Thu May 8 20:19:56 2025 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Generazione Report

- OpenVAS consente di generare ed esportare in vari formati (*CSV*, *XML*, *PDF*, etc) i report relativi alle scansioni effettuate

Contents

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Generazione Report

- OpenVAS consente di generare ed esportare in vari formati (*CSV*, *XML*, *PDF*, etc) i report relativi alle scansioni effettuate

1 Result Overview

Host	High	Medium	Low	Log	False Positive
10.0.2.12	161	102	5	0	0
10.0.2.10	18	39	6	0	0
10.0.2.11	26	40	6	0	0
10.0.2.2	2	1	0	0	0
Total: 4	207	182	17	0	0

Analisi Automatica delle Vulnerabilità

OpenVAS e GVM – Generazione Report

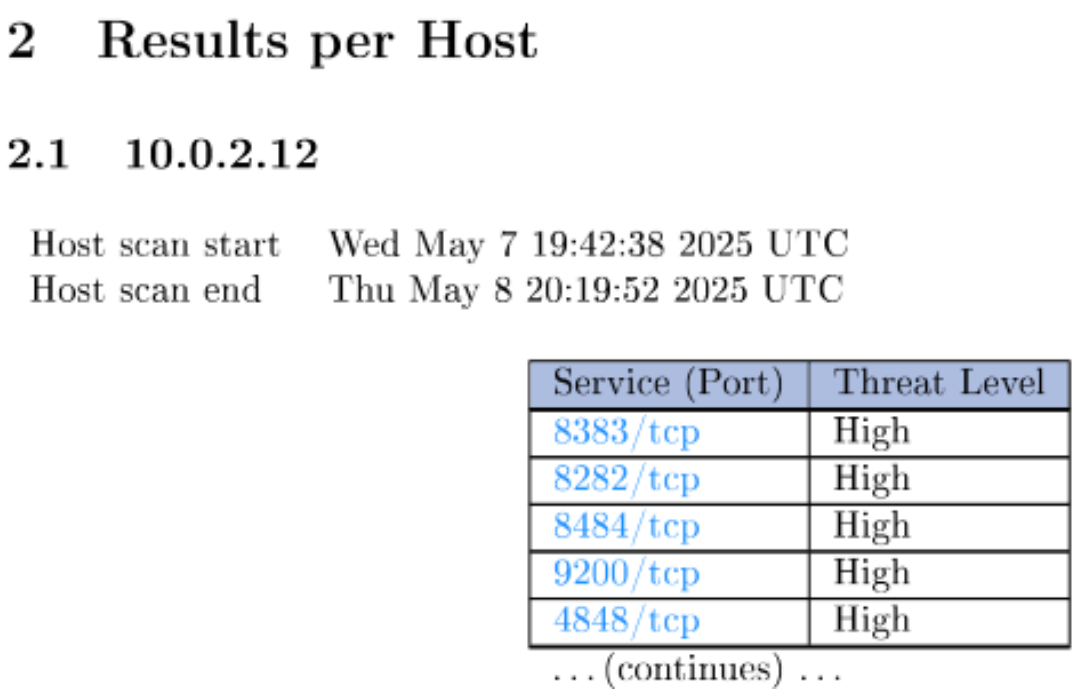
- OpenVAS consente di generare ed esportare in vari formati (*CSV*, *XML*, *PDF*, etc) i report relativi alle scansioni effettuate

1.1 Host Authentications

Host	Protocol	Result	Port/User
10.0.2.10	SMB	Success	Protocol SMB, Port 445, User
10.0.2.11	SMB	Success	Protocol SMB, Port 445, User

Analisi Automatica delle Vulnerabilità
OpenVAS e GVM – Generazione Report

- OpenVAS consente di generare ed esportare in vari formati (*CSV*, *XML*, *PDF*, etc) i report relativi alle scansioni effettuate



2 Results per Host

2.1 10.0.2.12

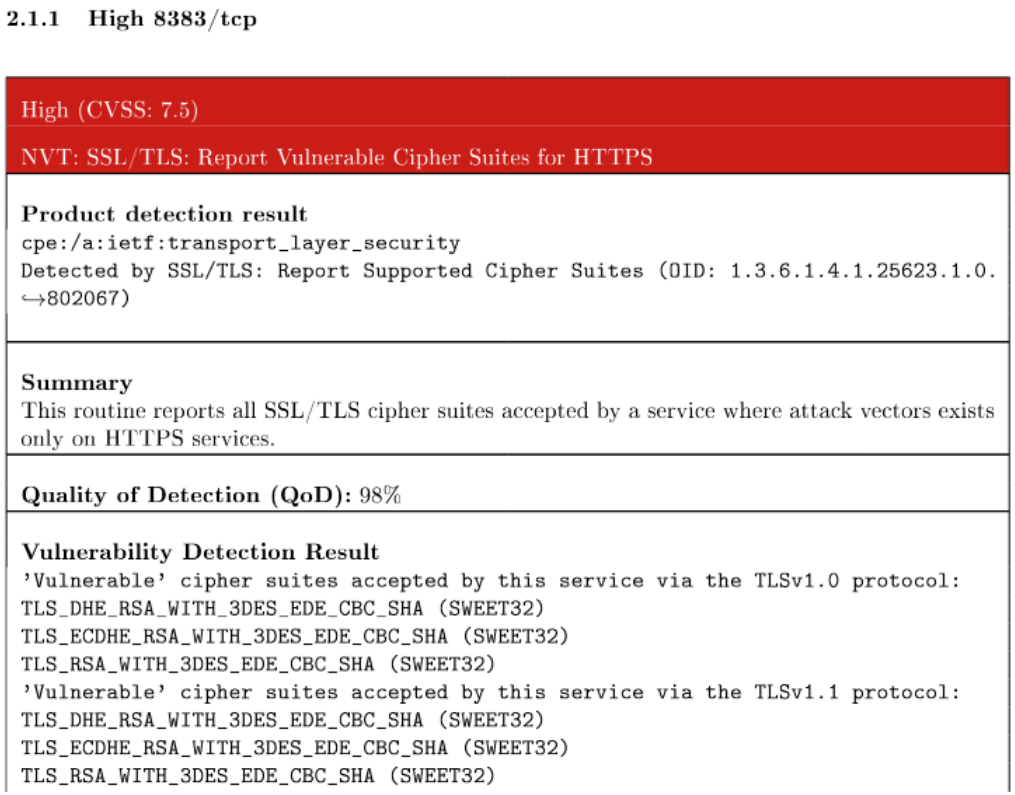
Host scan start	Wed May 7 19:42:38 2025 UTC
Host scan end	Thu May 8 20:19:52 2025 UTC

Service (Port)	Threat Level
8383/tcp	High
8282/tcp	High
8484/tcp	High
9200/tcp	High
4848/tcp	High

. . . (continues) . . .

Analisi Automatica delle Vulnerabilità
OpenVAS e GVM – Generazione Report

- OpenVAS consente di generare ed esportare in vari formati (*CSV*, *XML*, *PDF*, etc) i report relativi alle scansioni effettuate



2.1.1 High 8383/tcp

High (CVSS: 7.5)

NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

Summary
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

Quality of Detection (QoD): 98%

Vulnerability Detection Result
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

Analisi Automatica delle Vulnerabilità
OpenVAS e GVM – Generazione Report

- OpenVAS consente di generare ed esportare in vari formati (*CSV*, *XML*, *PDF*, etc) i report relativi alle scansioni effettuate

Impact
This could allow remote attackers to obtain sensitive information or have other, unspecified impacts.

Solution:
Solution type: Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

Affected Software/OS
All services accepting vulnerable SSL/TLS cipher suites via HTTPS.

Vulnerability Insight
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Vulnerability Detection Method
Checks previous collected cipher suites.
Details: `SSL/TLS: Report Vulnerable Cipher Suites for HTTPS`
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: `2025-03-27T05:38:50Z`

Analisi Automatica delle Vulnerabilità
OpenVAS e GVM – Generazione Report

- OpenVAS consente di generare ed esportare in vari formati (*CSV*, *XML*, *PDF*, etc) i report relativi alle scansioni effettuate

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

References
cve: CVE-2016-2183
cve: CVE-2016-6329
cve: CVE-2020-12872
url: https://ssl-config.mozilla.org
url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidel
↪ines/TG02102/BSI-TR-02102-1.html
url: https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/
↪TLS-Protokoll/TLS-Protokoll_node.html
url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Technisch
↪eRichtlinien/TR03116/BSI-TR-03116-4.html
url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindes
↪tstandard_BSI_TLS_Version_2_4.html