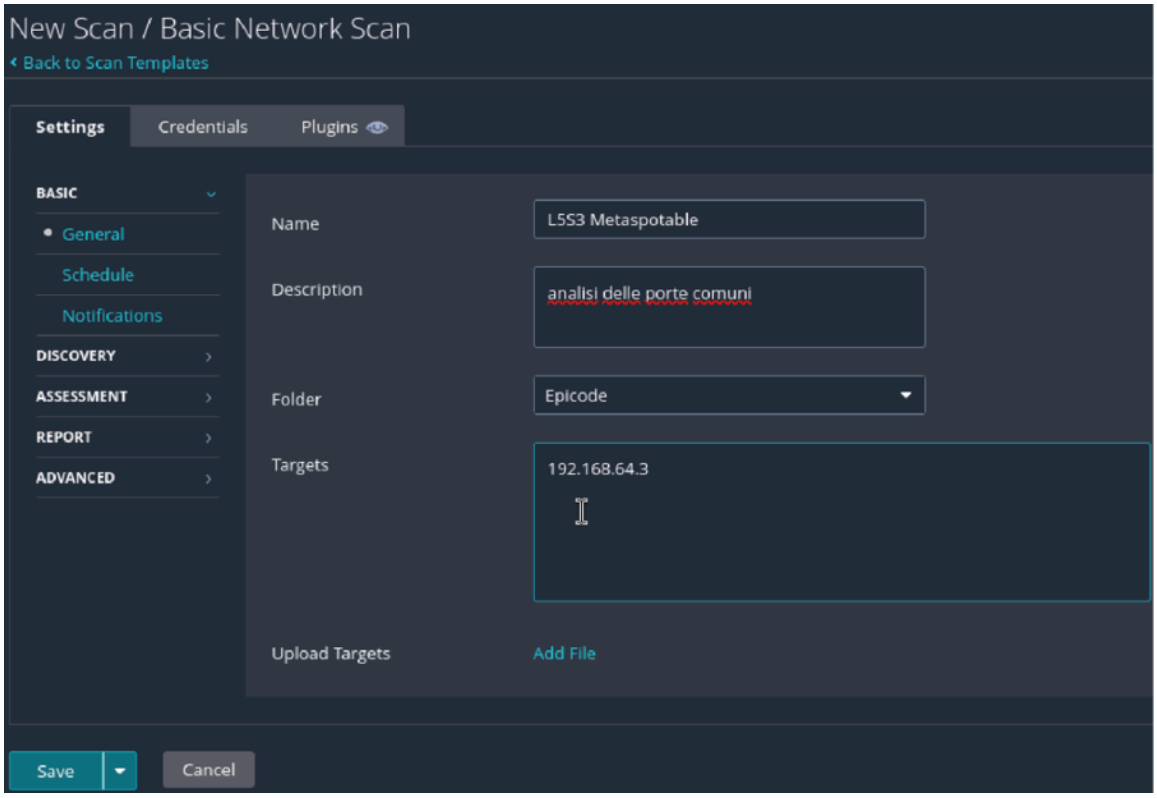
S5L3

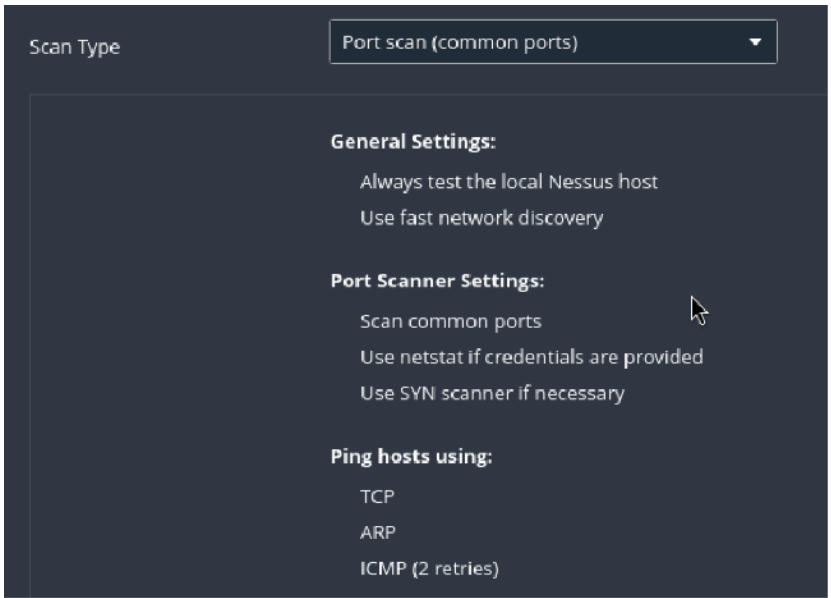
Obiettivo: Esercizio Traccia Lo studente effettuerà un Vulnerability Scanning sulla macchina Metasploitable utilizzando Nessus, concentrandosi sulle porte comuni. Questo esercizio ha lo scopo di fare pratica con lo strumento Nessus, la configurazione delle scansioni, e di familiarizzare con alcune delle vulnerabilità note.

Step1. Configurazione della scansione

Come primo step sono andato su Nessus basic network Scan per poi impostare il target che in questo caso è la mia Metaspotable con ip 192.168.64.3.

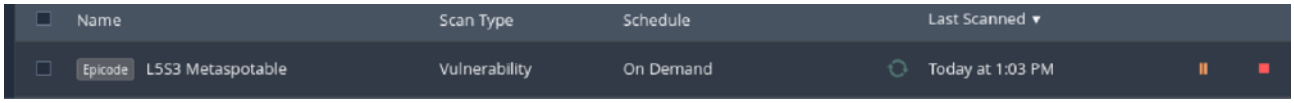


Nella finestra Discovery ho impostato le porte che mi interessavano ovvero quelle comuni.



Step2. Esecuzione della scansione.

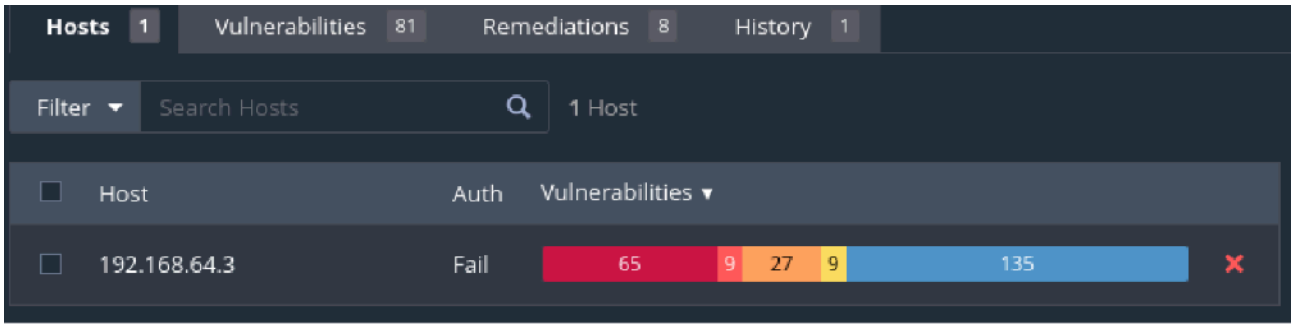
Una volta configurata la scansione e premendo su salva mi appare nel reparto scansioni questa barra:



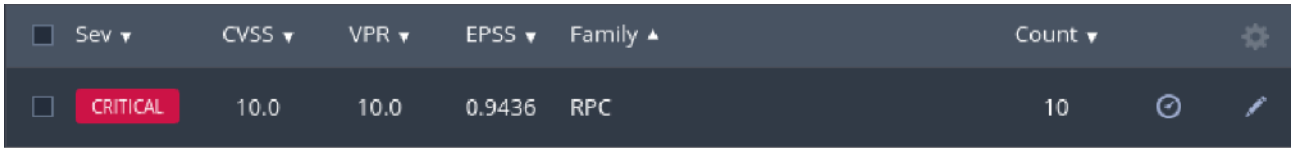
A questo punto ho la possibilità di avviare la scansione e il programma mi segnalerà il tempo di attesa e le vulnerabilità che troverà in tempo reale.

Step3. Analisi del report

Una volta completata la scansione mi apparirà una una barra tipo questa:

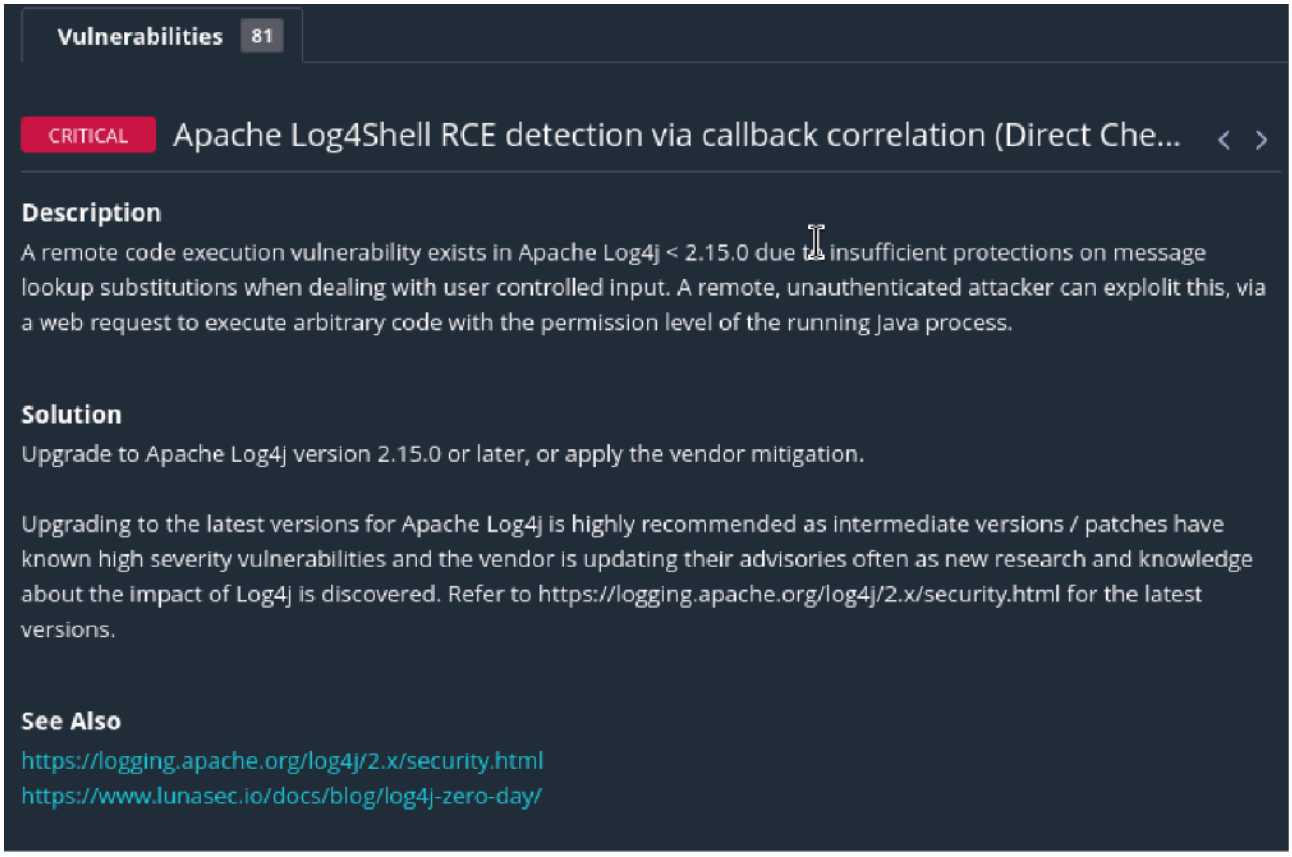


Cliccandoci sopra avrò la possibilità di analizzare le varie vulnerabilità Prenderò come esempio una delle più gravi ovvero:



Step4. Possibile risoluzione del problema

Cliccando sopra ad una delle vulnerabilità segnalate mi dara tutte le informazioni al riguardo.



In questo caso posso vedere che questa vulnerabilità viene segnalata come “ Log4Shell RCE”.

Il programma mi da anche una descrizione del problema dicendomi che una vulnerabilità di esecuzione di codice da remoto (RCE) è presente in Apache Log4j versione inferiore a 2.15.0.
L'attacco sfrutta input controllati dall'utente che vengono usati nelle lookup di messaggi (JNDIlookup), permettendo a un attaccante remoto (senza autenticazione) di eseguire comandi arbitrari con i permessi del processo Java.

Pericolosità:

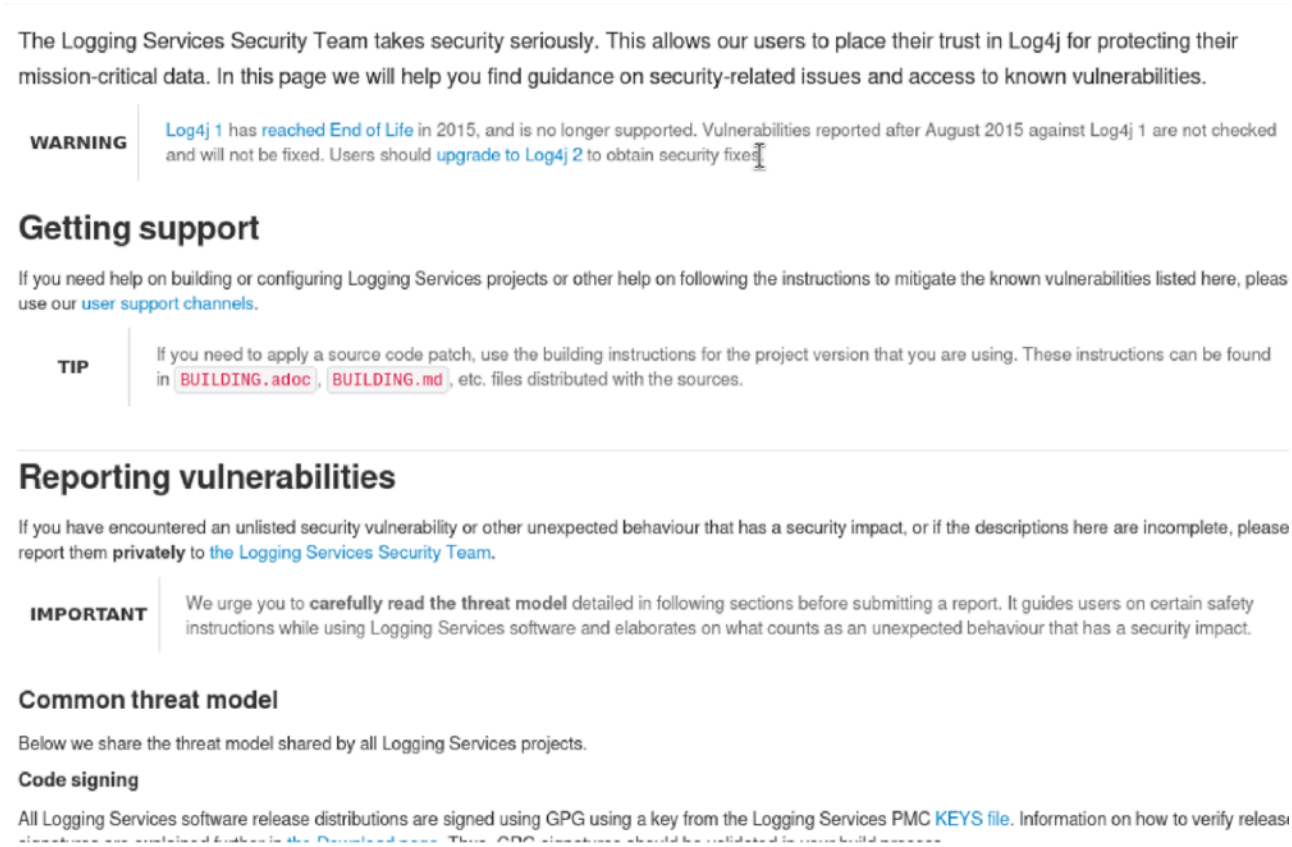
Impatto: L’attaccante può eseguire comandi come se fosse il servizio Java stesso, quindi potenzialmente ottenere controllo completo del sistema.

Diffusione: È stato uno degli zero-day più devastanti degli ultimi anni, usato in attacchi reali su larga scala.

Oltre alla descrizione mi da anche delle soluzioni possibili ovvero:

1. Aggiornare la versione del Apache
2. Applicare la mitigazione fornita dal fornitore

Nessus ci da anche dei siti per consultare il problema e trovare la soluzione come questo:



The Logging Services Security Team takes security seriously. This allows our users to place their trust in Log4j for protecting their mission-critical data. In this page we will help you find guidance on security-related issues and access to known vulnerabilities.

WARNING Log4j 1 has reached End of Life in 2015, and is no longer supported. Vulnerabilities reported after August 2015 against Log4j 1 are not checked and will not be fixed. Users should upgrade to Log4j 2 to obtain security fixes

Getting support

If you need help on building or configuring Logging Services projects or other help on following the instructions to mitigate the known vulnerabilities listed here, pleas use our user support channels.

TIP If you need to apply a source code patch, use the building instructions for the project version that you are using. These instructions can be found in `BUILDING.adoc`, `BUILDING.md`, etc. files distributed with the sources.

Reporting vulnerabilities

If you have encountered an unlisted security vulnerability or other unexpected behaviour that has a security impact, or if the descriptions here are incomplete, please report them **privately** to the Logging Services Security Team.

IMPORTANT We urge you to **carefully read the threat model** detailed in following sections before submitting a report. It guides users on certain safety instructions while using Logging Services software and elaborates on what counts as an unexpected behaviour that has a security impact.

Common threat model

Below we share the threat model shared by all Logging Services projects.

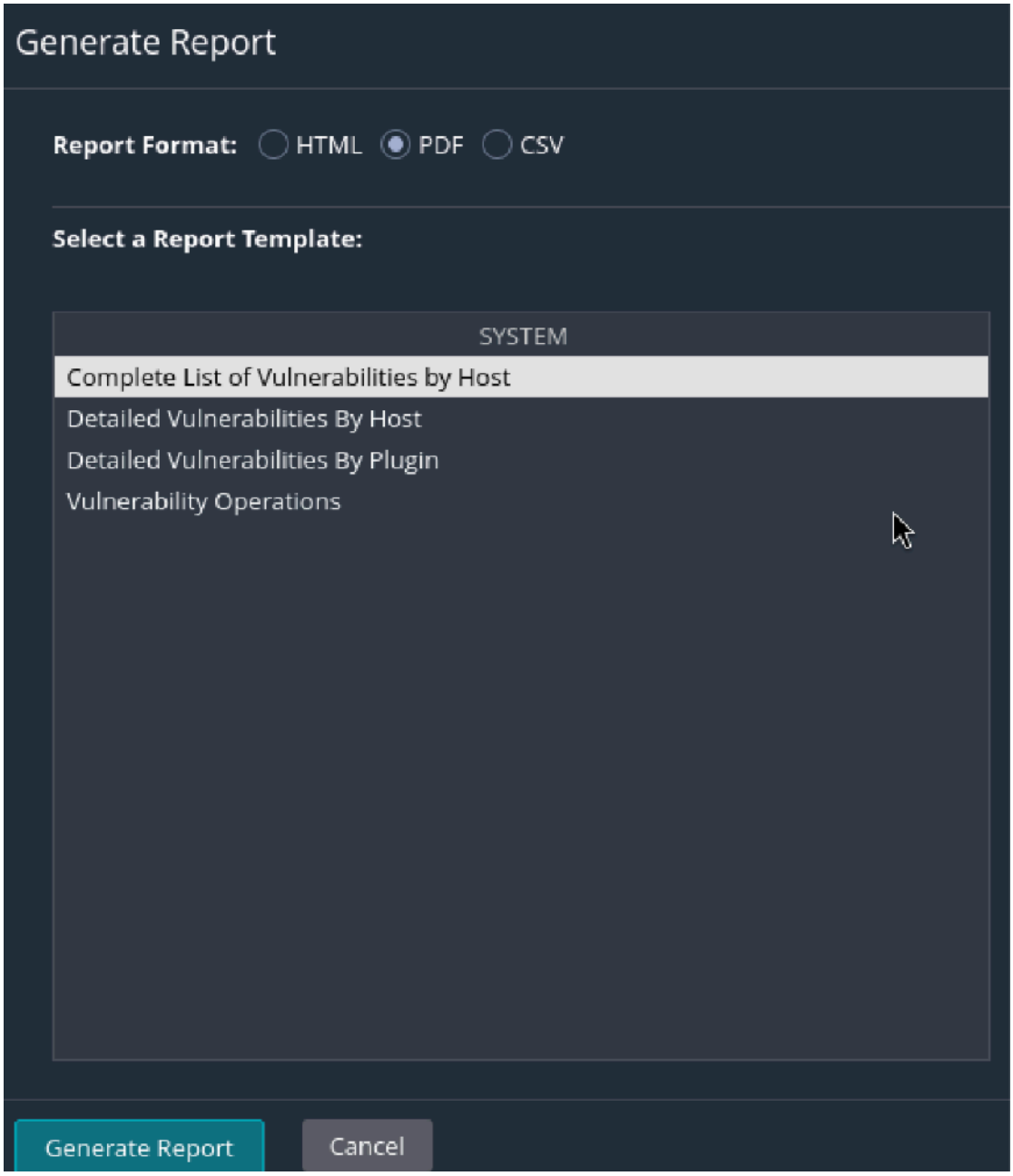
Code signing

All Logging Services software release distributions are signed using GPG using a key from the Logging Services PMC KEYS file. Information on how to verify releas

Una delle possibili soluzioni che ho trovato ricercando sul web è quella di

1. Verifica quale applicazione sulla tua Metasploitable usa Log4j
2. Andare a cambiare il `.jar` Log4j nella directory `/lib` del progetto.
3. Usare un container Docker sicuro o una VM aggiornata per sostituire quella vulnerabile.

Extra: Abbiamo anche la possibilità di creare un report per agevolare e facilitare future analisi.
Basta andare su Report in alto a destra e potremmo selezionare il tipo di report che vogliamo (consigliato Detailed Vulnerabilities by host) e il formato desiderato (HTML, PDF, CSV)



Conclusioni:

Nessus è un programma che permette di individuare, tramite scansioni sul target richiesto , le varie vulnerabilità spiegando come poterle risolvere e segnalandole in base alla loro pericolosità. Estremamente utile per capire se una rete o dispositivo è al sicuro da attacchi esterni.