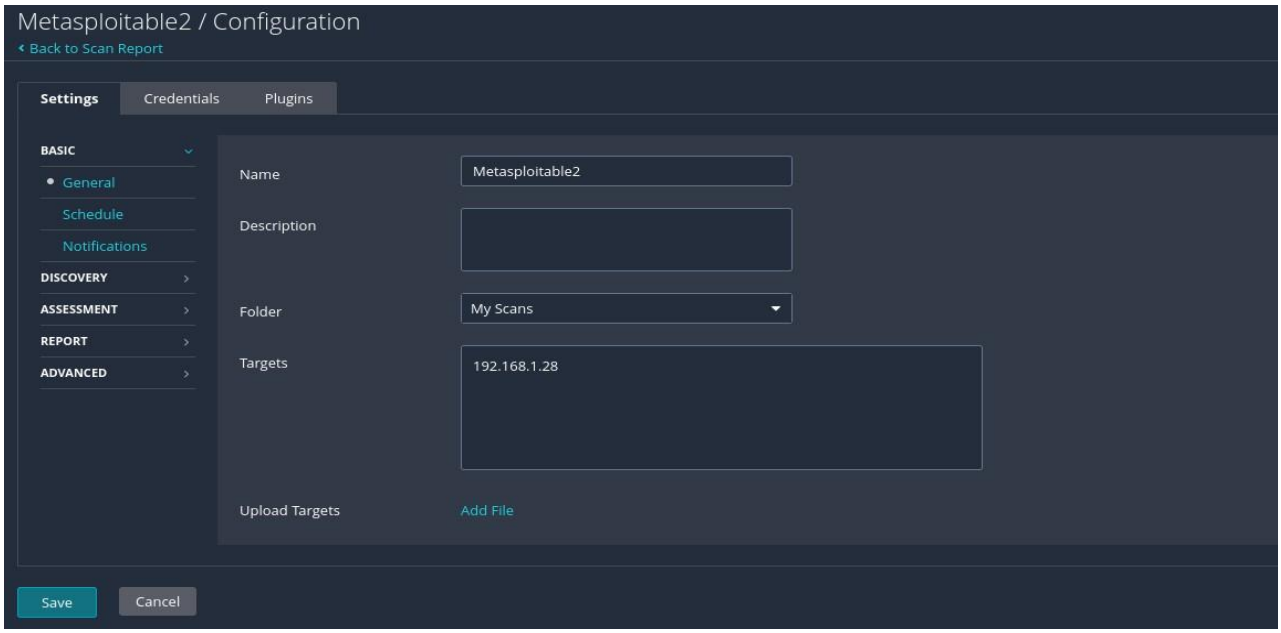
Relazione Scan Target Metasploitable e Scan Ports tramite il Software Nessus Essentials

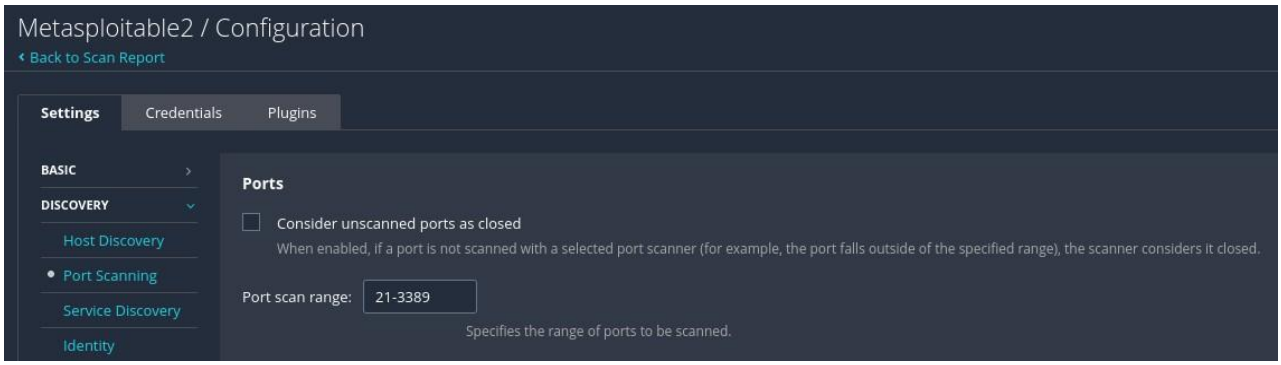
Nessus Essentials: è un Software Scanner semplice da utilizzare, ma allo stesso tempo potente, usato per coprire reti estese

- Utilizziamo Nessus per la scansione avanzata sul **Target METASPLOITABLE2**:
- Nella seguente immagine andremo a nominare il target: **Metasploitable2**
- Scrivo nella scheda **Targets** l'indirizzo IP della VM Matasploitable2: **192.168.1.28**



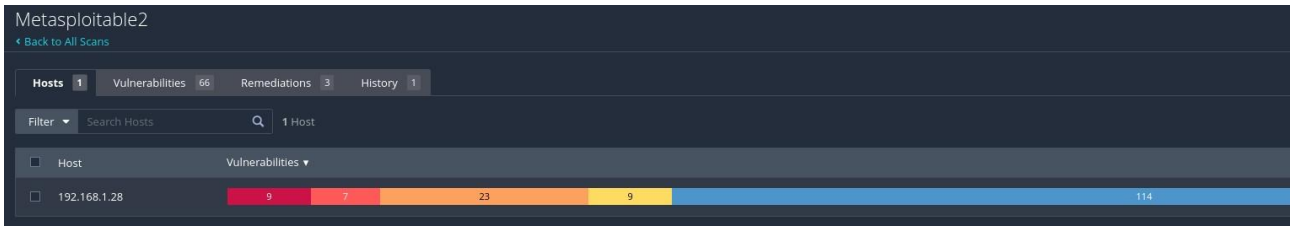
Nel seguente passaggio ed immagine, vado ad inserire le porte da scansionare, in TCP, come ad esempio: **range 21-3389**:

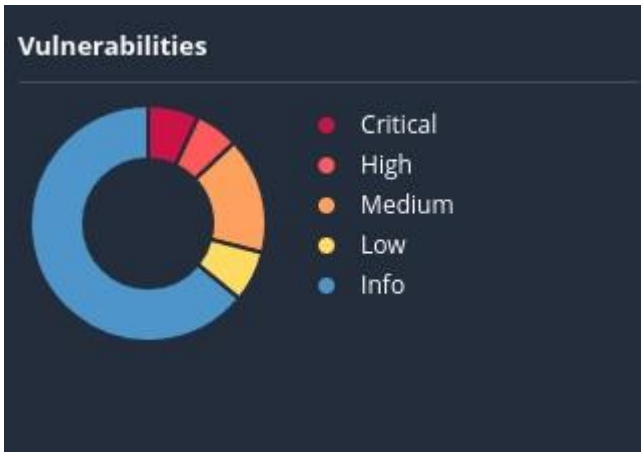
- Scrivo nella scheda **Port scan range: 21-3389**, così che Nessus effettui lo scan tra la porta 21 e la porta 3389



Nel seguente passaggio ed immagine, possiamo vedere il risultato finale della scansione con i relativi colori che identificano i livelli di vulnerabilità:

- **Critical**
- **High**
- **Medium**
- **Low**
- **Info**





Nel seguente passaggio, dopo aver illustrato precedentemente i vari livelli di vulnerabilità, identificati con i vari colori, in ultimo, potremmo vedere i consigli che ci illustra **Nessus Essentials**, chiamate **Actions** per riparare e correggere le vulnerabilità:

Analisi dei livelli di vulnerabilità

Per l'analisi dei vari livelli di vulnerabilità, tramite il Report finale creato da **Nessus Essentials**, come da seguente immagine, devo cliccare sul numero identificativo in blu (**PLUGIN**), dove, posso vedere successivamente, la descrizione della vulnerabilità:

- **CRITICAL**

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	0.9728	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)

- **HIGH**

HIGH	8.6	5.2	0.0234	136769	ISC BIND Service Downgrade / Reflected DoS

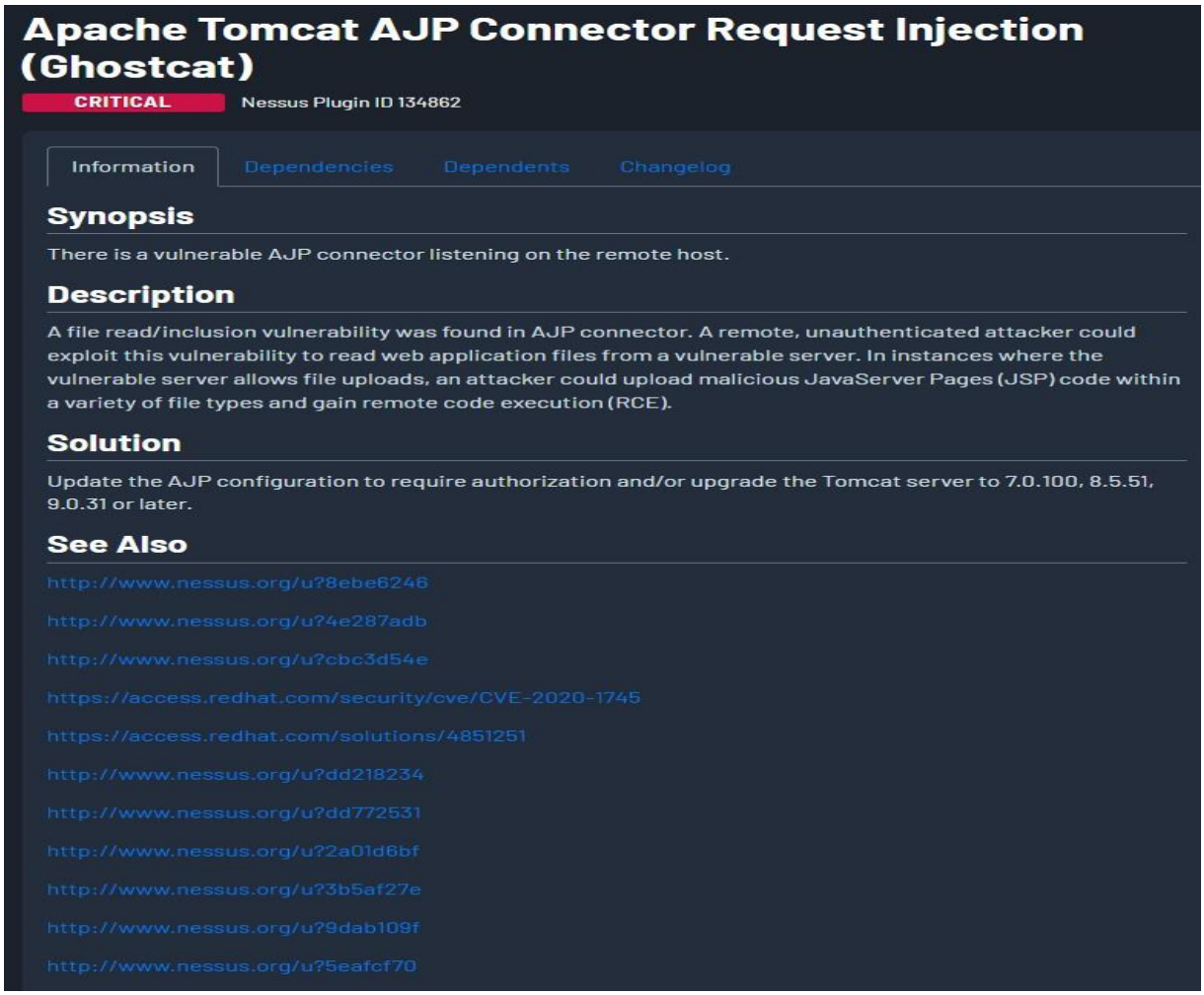
- **MEDIUM**

MEDIUM	6.5	3.6	0.0041	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS

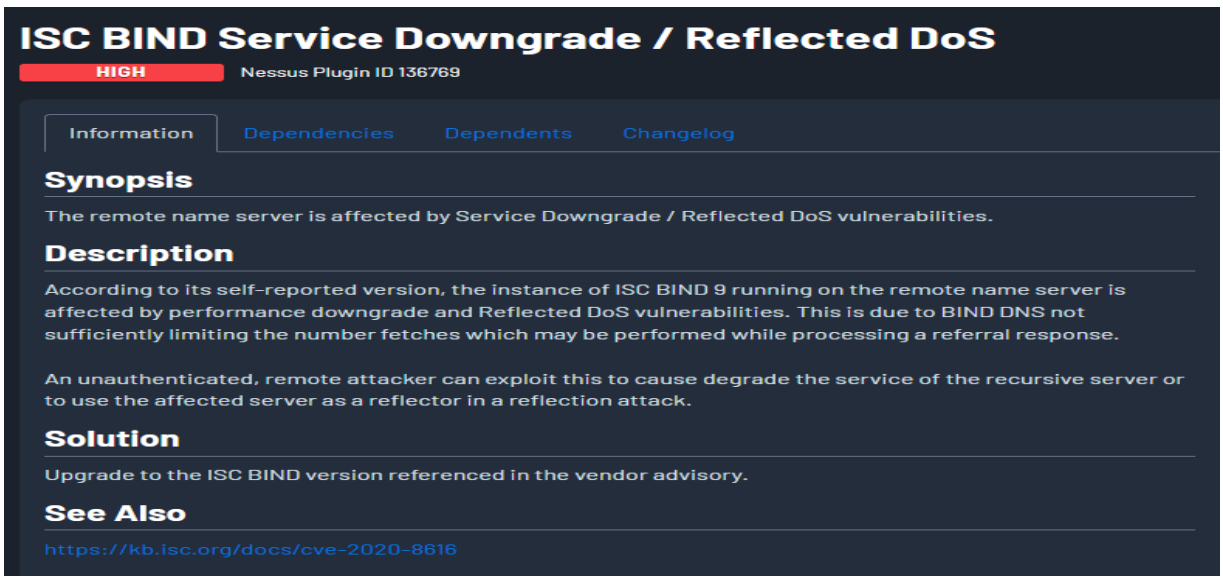
- **LOW**

LOW	3.7	3.6	0.5961	70658	SSH Server CBC Mode Ciphers Enabled

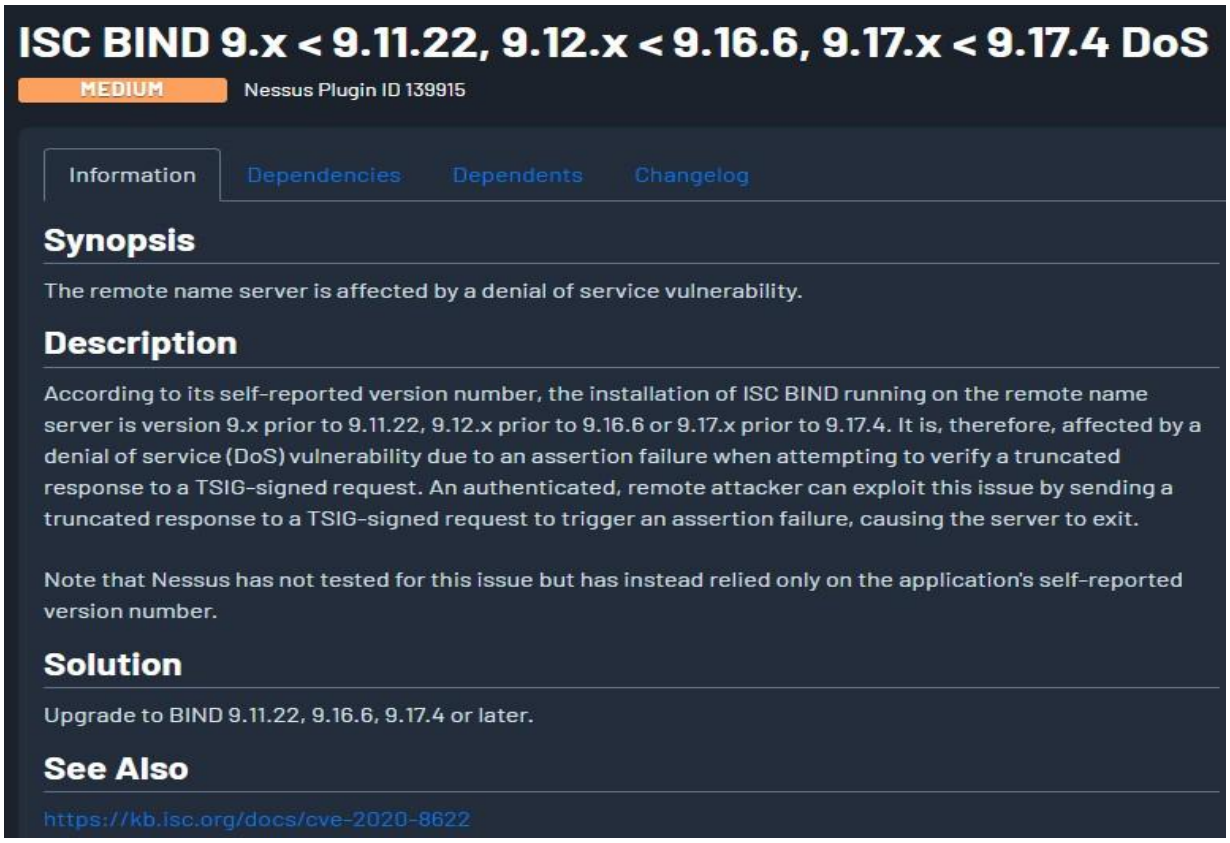
1. **Analisi del livello di vulnerabilità: Critical**



2. **Analisi del livello di vulnerabilità: High**



3. **Analisi del livello di vulnerabilità: Medium**



4. **Analisi del livello di vulnerabilità: Low**