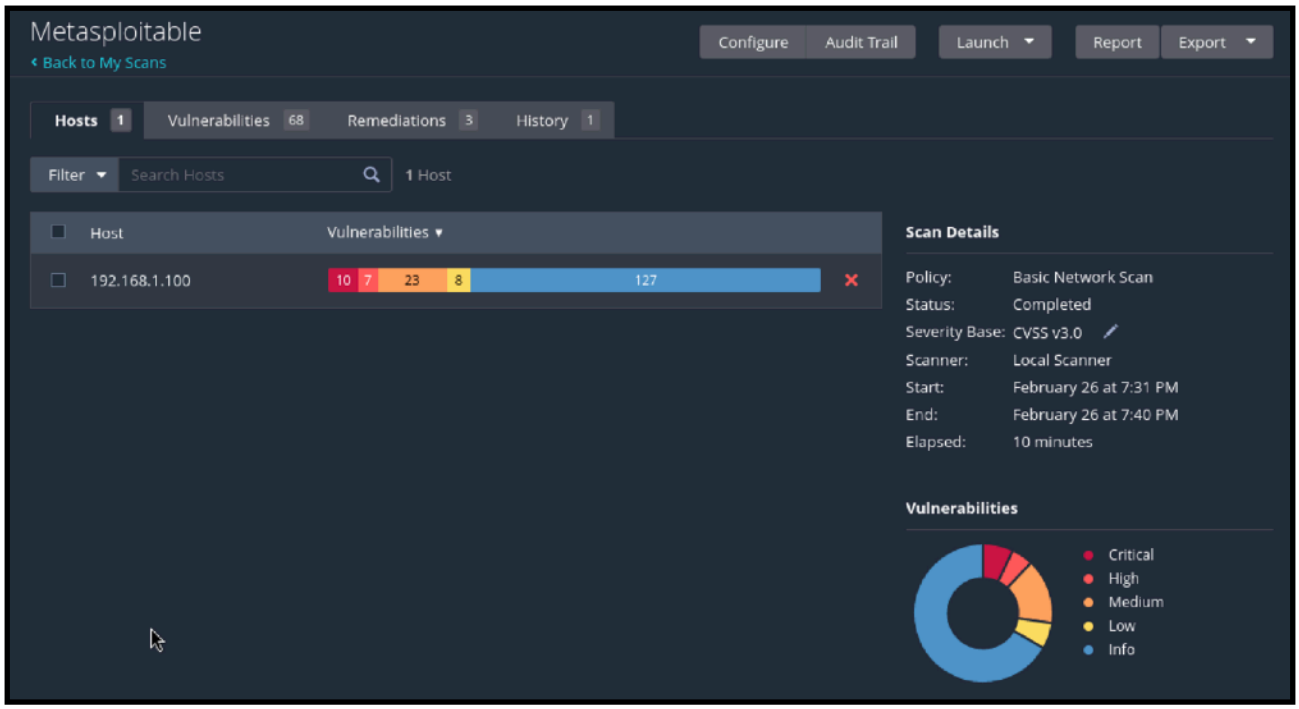
M3_W12D1

Effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable, indicando come target solo le porte comuni.
Abbiamo utilizzato come metodo di scansione il «Basic Network Scan».
A valle del completamento della scansione, analizzeremo attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all'interno dei report e/o con contenuto da Web.

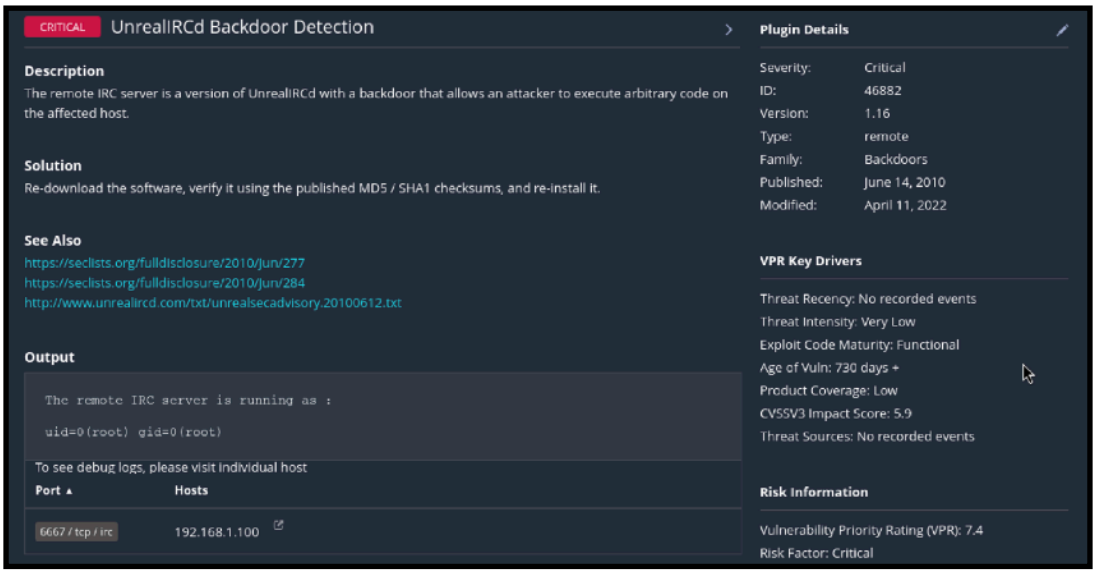
Ultimata la scansione il target presenta:

10 Critical Vulnerabilities
7 High Vulnerabilities
23 Medium Vulnerabilities
8 Low Vulnerabilities
127 Info System

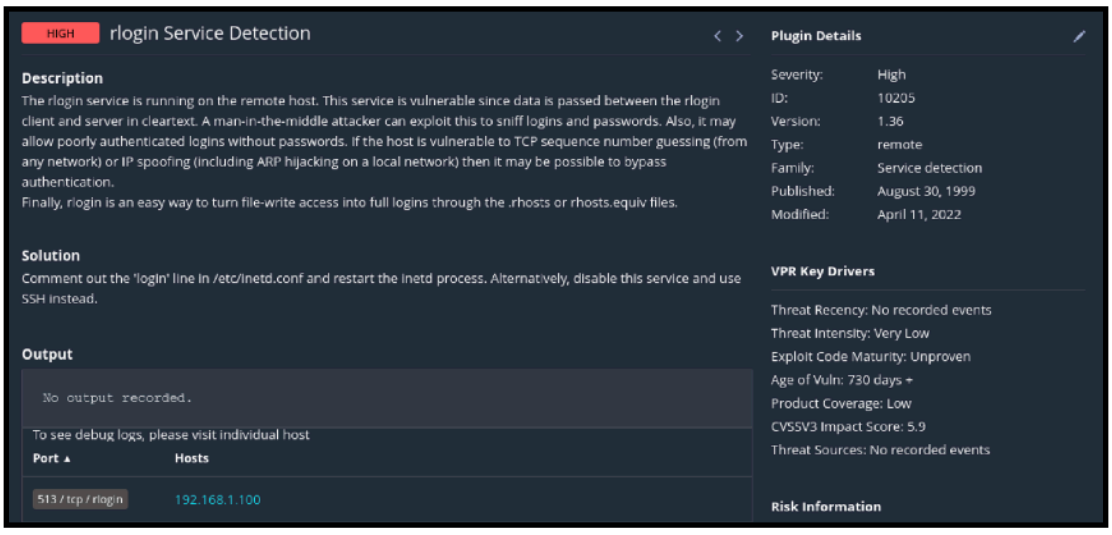


Nessus mette a disposizione un Vulnerability Priority Rating (VPR) ed un Common Vulnerability Scoring System (CVSS). Sulla base di questi filtri quantificheremo il rischio associato ad ogni vulnerabilità e stabiliremo delle priorità per ogni remediation action da applicare.

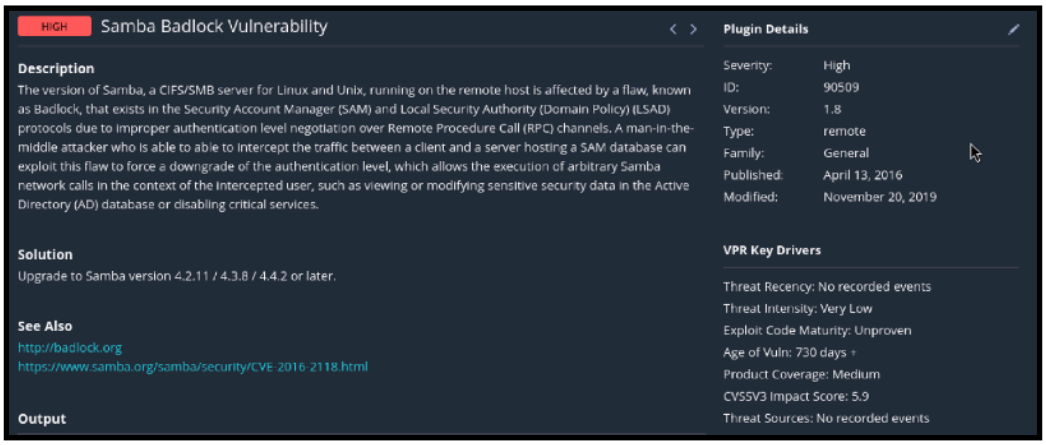
Al primo posto per fattore di rischio legato alla criticità della vulnerabilità sul sistema target troviamo UnrealRCd Backdoor Detection: server Internet Relay Chat open source e dunque una backdoor che consentirebbe ad un malintenzionato la possibilità di eseguire comandi arbitrari sul server.
Soluzione: Per scongiurare il rischio dobbiamo installare una versione pulita e quindi aggiornata del software.



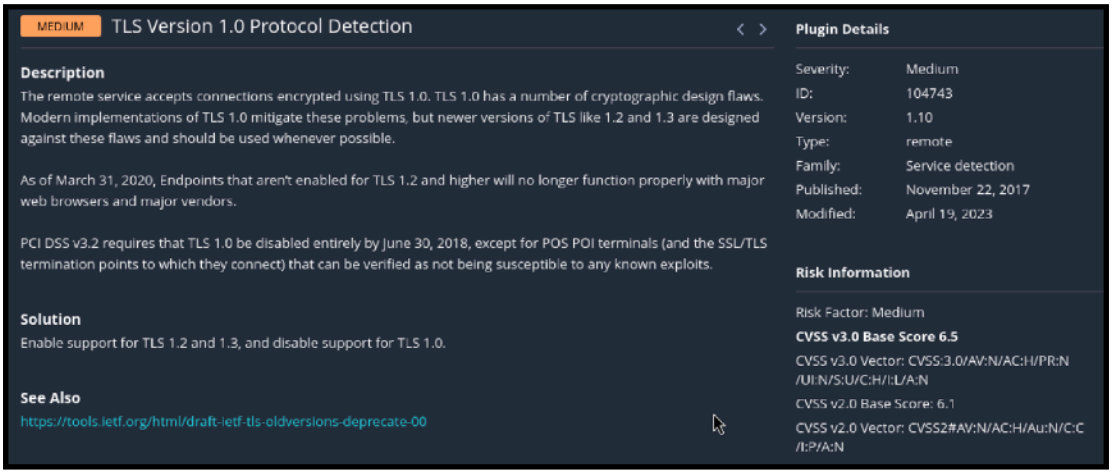
Una vulnerabilità high-level riscontrata sul sistema target è login Service Detection: questo servizio rappresenta un'importante risorsa per l'attacante poiché i dati transitano in chiaro in una comunicazione client-server. Un attacco con man-in-the-middle rende facilmente sfruttabile questa vulnerabilità che oltretutto può consentire accessi scarsamente autenticati senza password.
Soluzione: commentare la riga "login" in /etc/inetd.conf e riavviare il processo inetd. In alternativa, disabilitare questo servizio e utilizzare SSH instead.



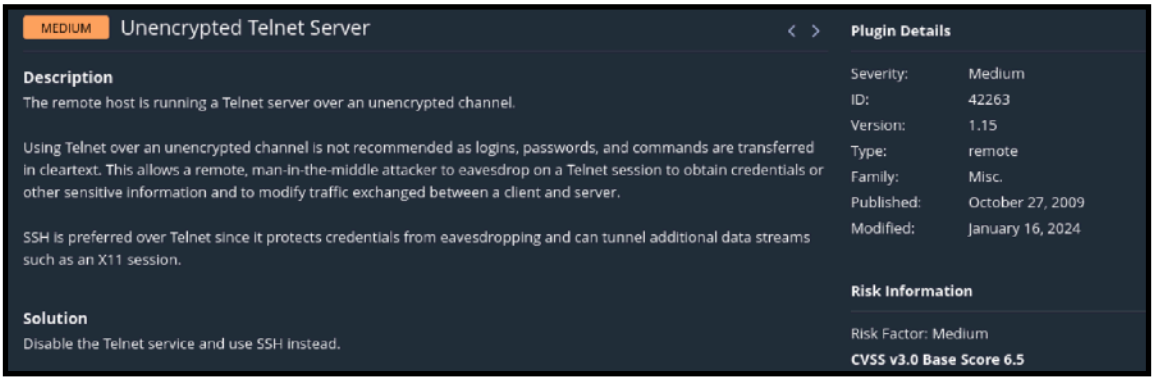
Un’altra vulnerabilità high-leve altamente impattante per il nostro sistema target è Samba Badlock Vulnerability: questa versione è affetta da una falla, nota come Badlock, presente nei protocolli Security Account Manager (SAM) e Local Security Authority (Domain Policy) (LSAD). Un utente malintenzionato intercettando il traffico tra un client e una server che ospita un database SAM può sfruttare questa falla per forzare il declassamento del livello di autenticazione con lo scopo di modificare dati di sicurezza nel database Active Directory o la disabilitazione dei servizi critici.
Soluzione: Aggiornare Samba alla versione 4.2.11/4.3.8/4.4.2 o successive.



Vulnerabilità medium level importante da fixare TLS Version 1.0 Protocol Detection: questa versione presenta una serie di difetti di progettazione crittografica che potrebbe rivelarsi fatale durante il trasferimento di dati sensibili.
Soluzione: Abilitare TLS 1.2 e 1.3 e disabilitare TLS 1.0



Un’altra vulnerabilità medium level riscontrata sul sistema target è Unencrypted Telnet Server: questo servizio su un canale non crittografato è altamente sconsigliato poiché login, password e comandi vengono trasferiti in chiaro. Soluzione: Disattivare il servizio Telnet e utilizzare SSH in quanto capace di proteggere le credenziali da intercettazioni aggiungendo flussi di dati aggiuntivi in grado di proteggere contenuti sensibili.



E’ altamente consigliato, indipendentemente dal livello di criticità, aggiornare ogni servizio che presenta vulnerabilità alla sua ultima versione oppure disattivarlo o sostituendolo con un servizio in grado di proteggere meglio qualsiasi tipo di dato sulla macchina qualora non fosse possibile eseguire un upgrade della versione.