**Vulnerability Scanning.**

**Nessus** è uno strumento di scansione delle vulnerabilità, utilizzato principalmente per identificare falle di sicurezza nei sistemi e nelle reti. Serve a:

1. **Individuare vulnerabilità**: Scansiona dispositivi, server, applicazioni e servizi per trovare vulnerabilità, come configurazioni errate, software obsoleti o bug noti che potrebbero essere sfruttati.

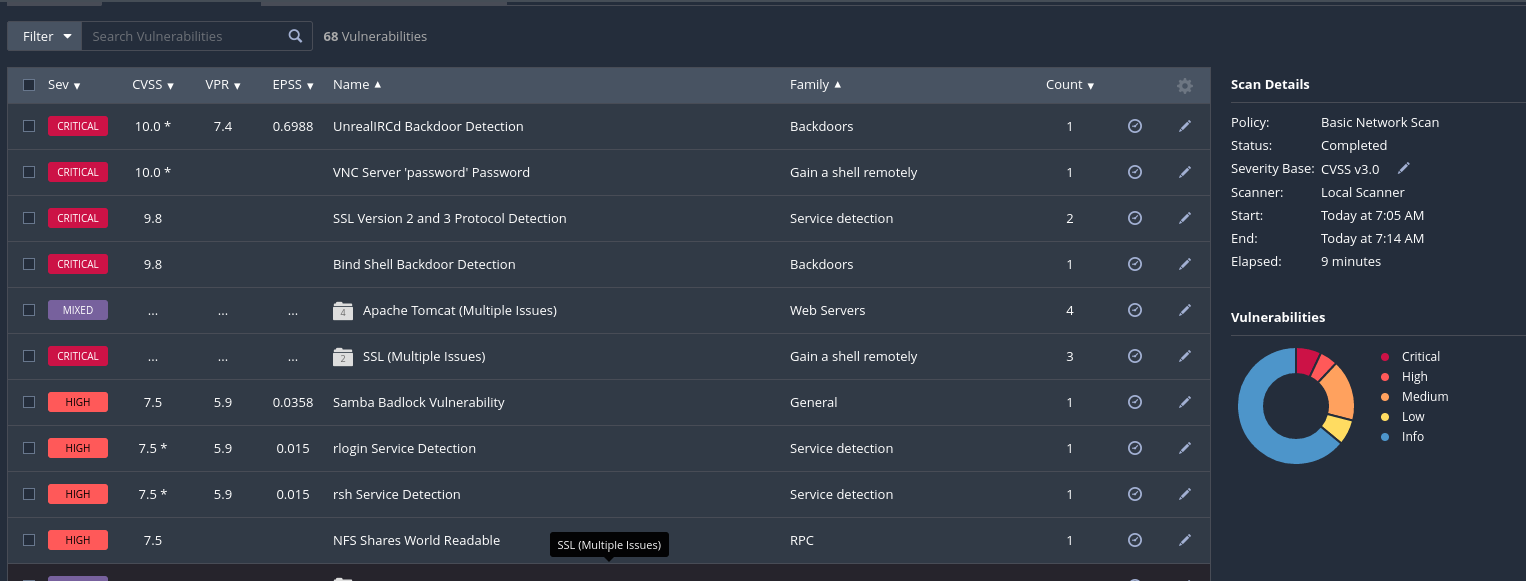
2. **Gestire la sicurezza di rete**: Identifica problemi di sicurezza nelle reti, suggerendo misure correttive per prevenire attacchi e compromissioni.

3. **Rispettare la conformità**: Aiuta le aziende a rispettare standard di sicurezza e normative (come PCI-DSS, HIPAA, ISO), generando report sulle vulnerabilità e sulle azioni necessarie per mitigare i rischi.

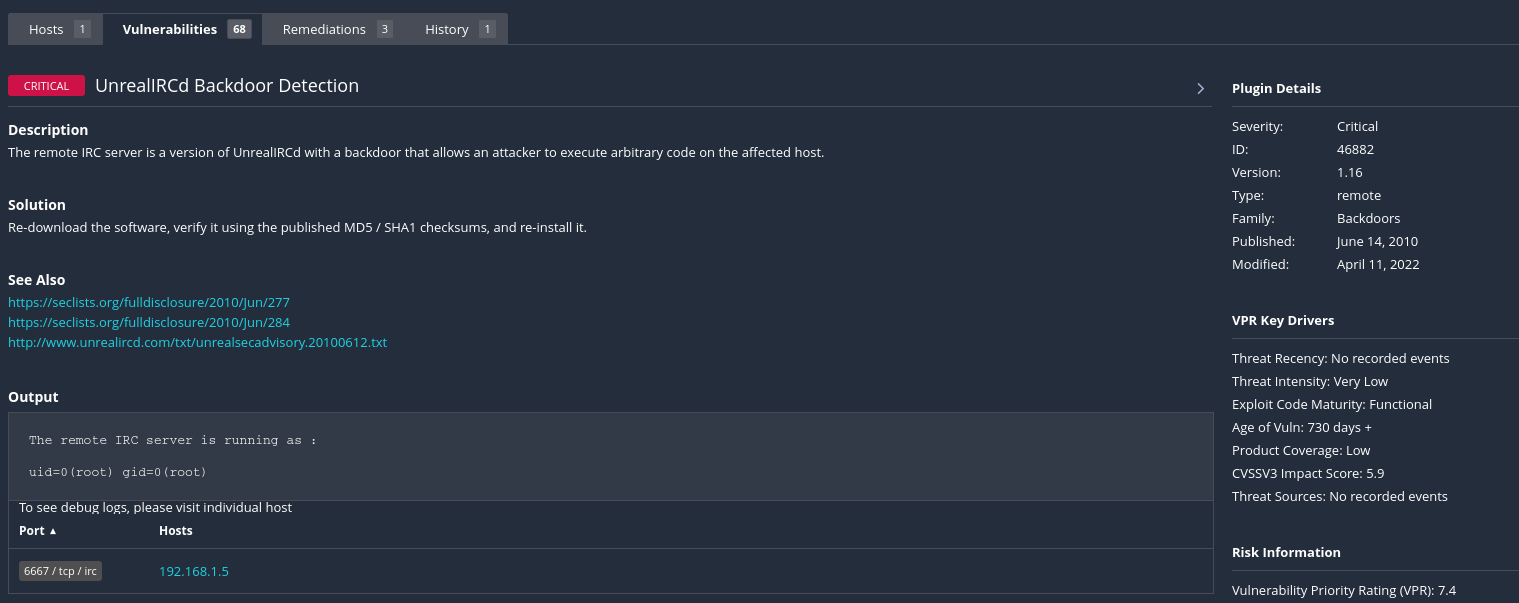
4. **Analizzare e monitorare i rischi**: Fornisce un’analisi del livello di rischio associato a ciascuna vulnerabilità e monitora costantemente l’ambiente per nuovi problemi di sicurezza.

In sintesi, Nessus è fondamentale per chi si occupa di cybersecurity perché consente di prevenire violazioni, migliorare la sicurezza della rete e mantenere il controllo su potenziali rischi.

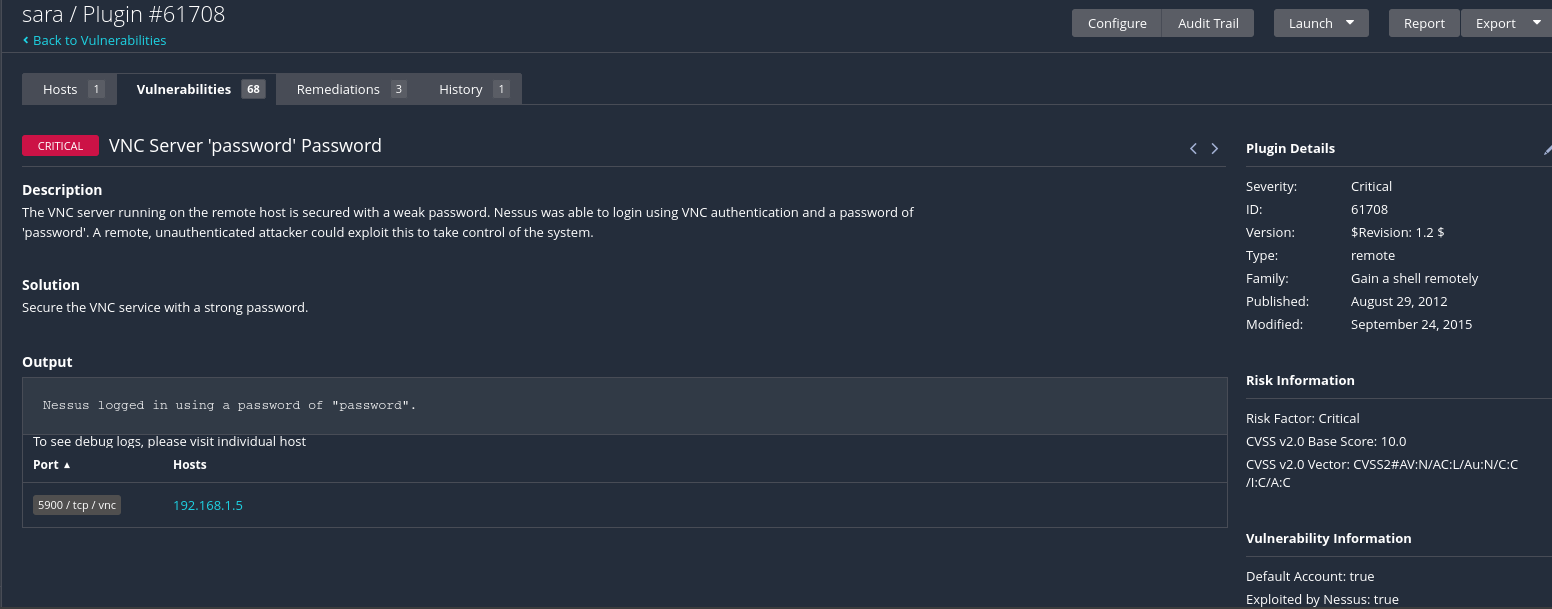
Dopo aver effettuato una scansione dell’host metaspoitable, sono emerse alcune vulnerabilità, tra cui analizzeremo cinque:



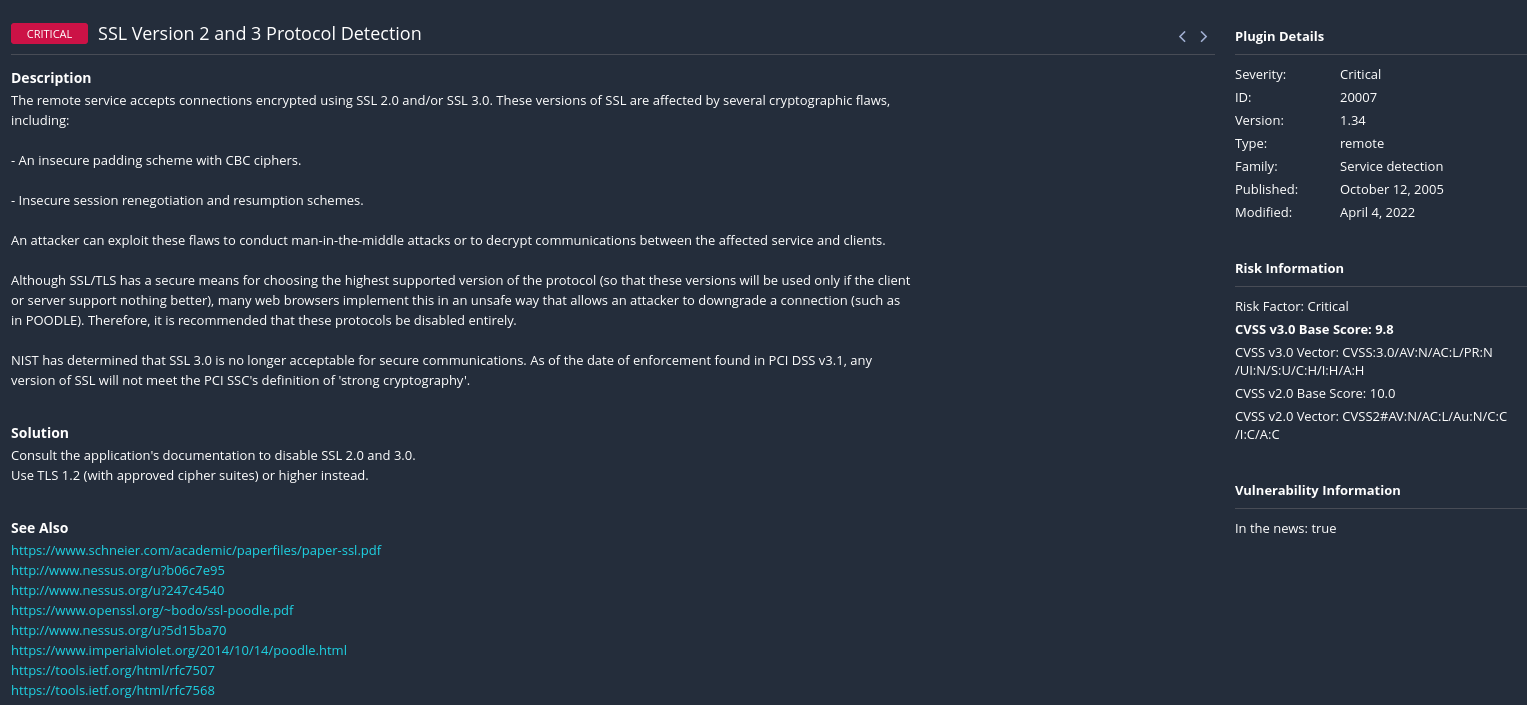
• **Rilevamento backdoor UnrealIRCd**: questa vulnerabilità potrebbe consentire a un attaccante di ottenere accesso non autorizzato e controllo sul sistema.



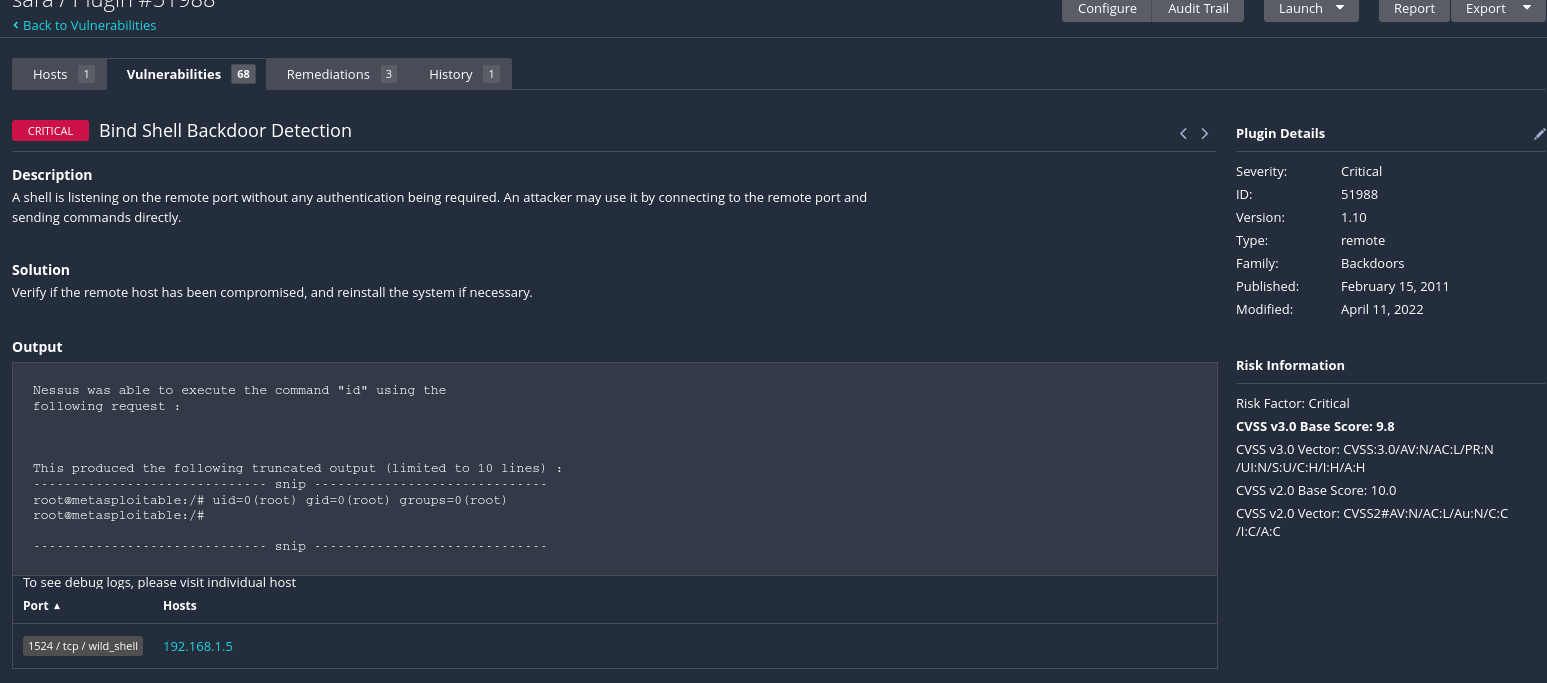
• **VNC Server con password debole (‘password’)**: Questo avviso segnala l’uso di una password predefinita molto debole, come “password”, che facilita l’accesso non autorizzato al server, permettendo agli attaccanti di controllare la macchina da remoto.



• **Rilevamento dei protocolli SSL Versione 2 e 3**: L’uso di SSL v2 e v3 è considerato non sicuro, in quanto vulnerabile a diversi tipi di attacchi. Questo può esporre i dati trasmessi a rischi di intercettazione e manipolazione.



• **Rilevamento backdoor Bind Shell**: Una bind shell è una backdoor che rimane in ascolto su una porta aperta, permettendo a un attaccante di connettersi e eseguire comandi da remoto, compromettendo la sicurezza dell’intero sistema.



• **Debolezza nel generatore di numeri casuali di Debian OpenSSH/OpenSSL**: Questa vulnerabilità può rendere le chiavi crittografiche prevedibili, facilitando potenzialmente l’accesso non autorizzato al sistema.

