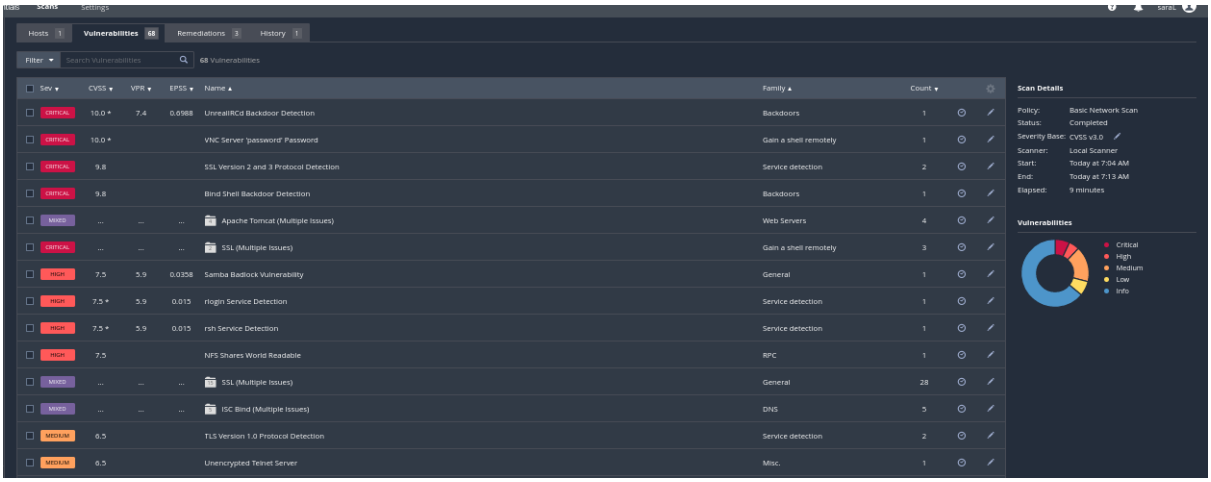
NESSUS PER SCANSIONARE LE VULNERABILITA':

Nel compito di oggi abbiamo installato Nessus su Kali e abbiamo fatto una scansione di un indirizzo IP target che era quello della nostra macchina di Metaploitable: 192.168.1.30.

In questa scansione quello che noi vogliamo sapere sono le vulnerabilità che ha Metaploitable, quindi impostando l'indirizzo IP e il range di porte (abbiamo scelto quelle comuni) abbiamo lanciato la scansione e questo è il risultato:



Come possiamo vedere dalla nostra scansione sono uscite fuori 68 vulnerabilità di diverso livello.

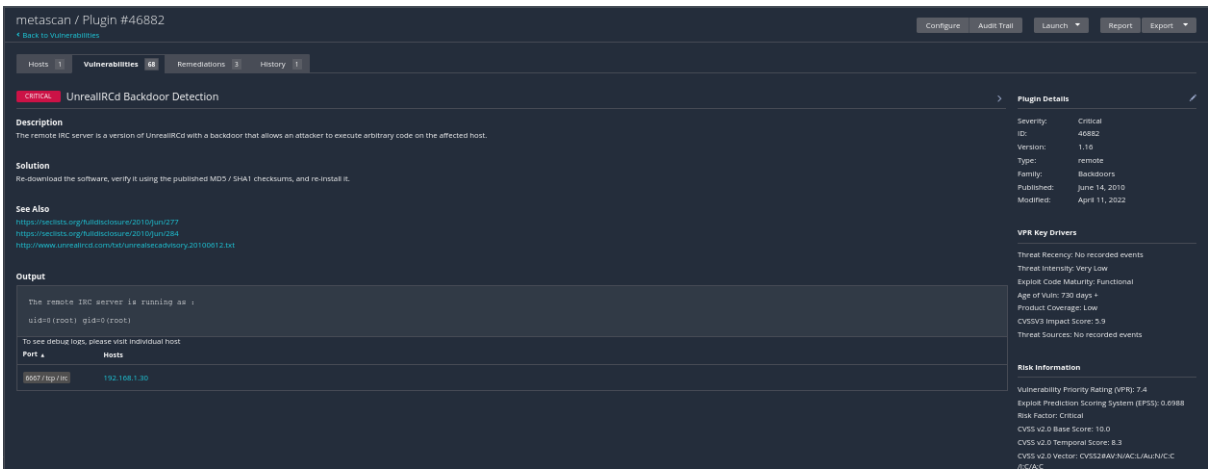
I livelli di vulnerabilità sono 5:

1. CRITICAL: come dice gia la parola è quella più pericolosa
2. HIGH: meno pericolosa della critical ma comunque ancora troppo alto il rischio
3. MEDIUM: rischio medio
4. LOW: basso rischio
5. INFO: questa vulnerabilità è abbastanza sicura anche se ovviamente non al 100%

Una volta finita la scansione possiamo scaricare in pdf un report, dove vengono elencate e spiegate tutte le vulnerabilità.

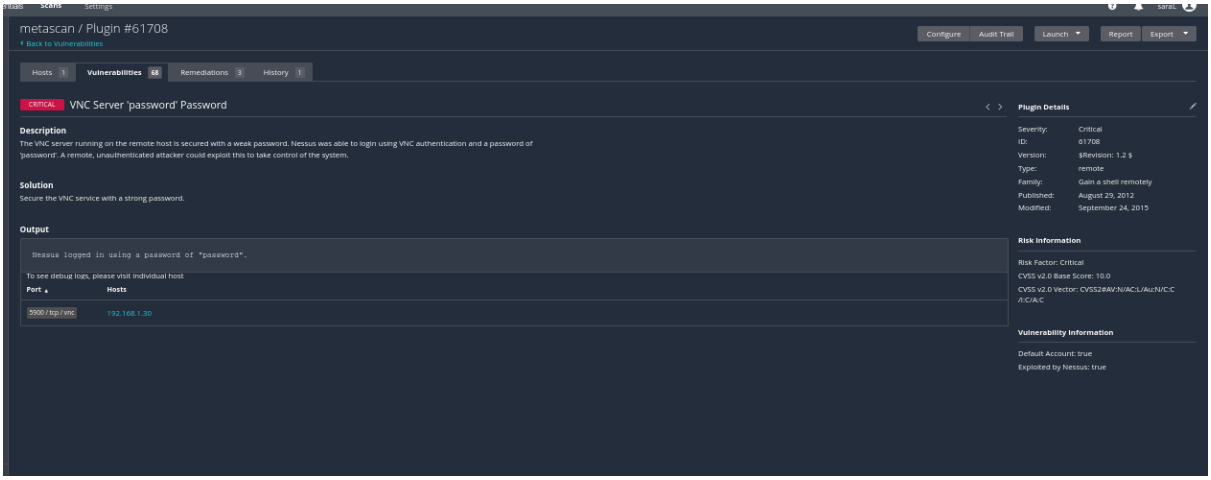
Fatto questo, oggi ne analizzeremo 5.

VULNERABILITA' 1: UnrealIRCd Backdoor Detection **CRITICAL**



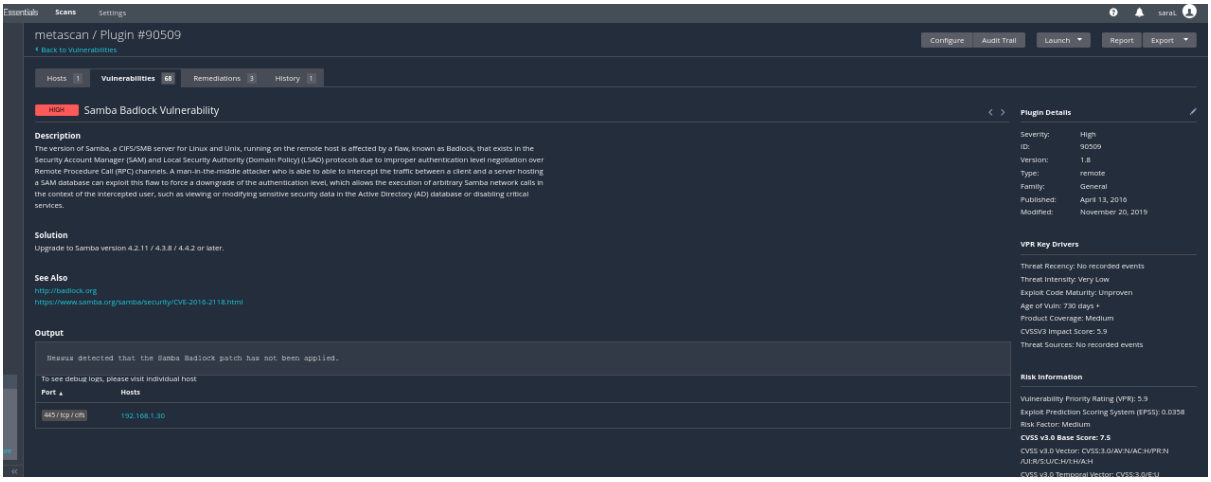
Il server IRC remoto è una versione di UnrealIRCd con una backdoor che consente a un utente malintenzionato di eseguire codice arbitrario sull'host interessato. Scaricare nuovamente il software, verificarlo utilizzando i checksum MD5/SHA1 pubblicati e reinstallarlo.

VULNERABILITA' 2: VNC Server 'password' Password **CRITICAL**



Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e una password "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa situazione per assumere il controllo del sistema. Proteggi il servizio VNC con una password complessa.

VULNERABILITA' 3: Samba Badlock Vulnerability **HIGH**

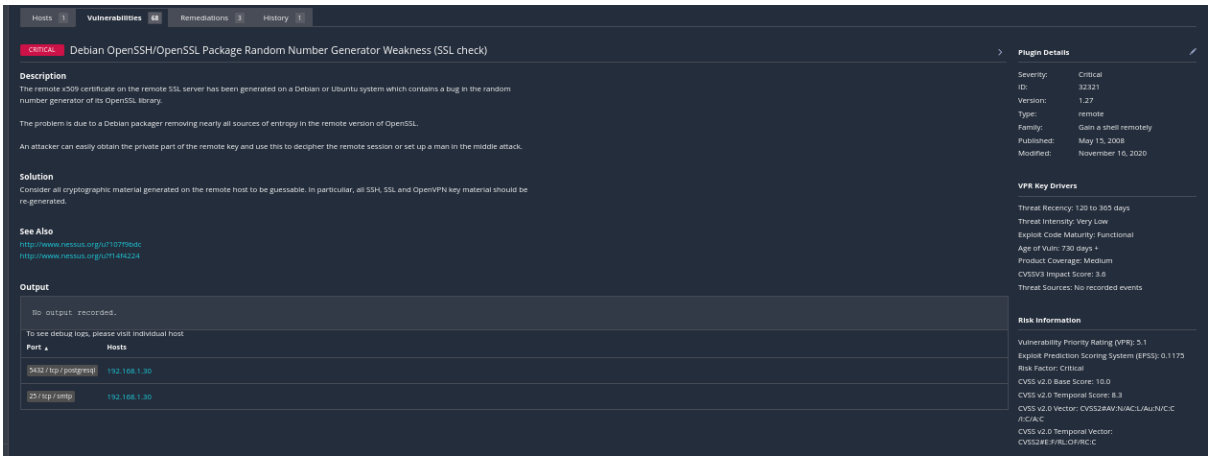


La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è affetta da un difetto, noto come Badlock, presente nel Security Account Manager (SAM) e nella Local Security Authority (Domain Policy) (LSAD) a causa di una negoziazione impropria del livello di autenticazione sui canali RPC (Remote Procedure Call). Un utente malintenzionato man-in-the-middle in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questa falla per forzare un downgrade del livello di autenticazione, che consente l'esecuzione di chiamate di rete Samba arbitrarie nel contesto dell'utente intercettato, come visualizzare o modificare dati sensibili di sicurezza nel database di Active Directory (AD) o disabilitare servizi critici. Aggiorna alla versione Samba 4.2.11 / 4.3.8 / 4.4.2 o successiva.

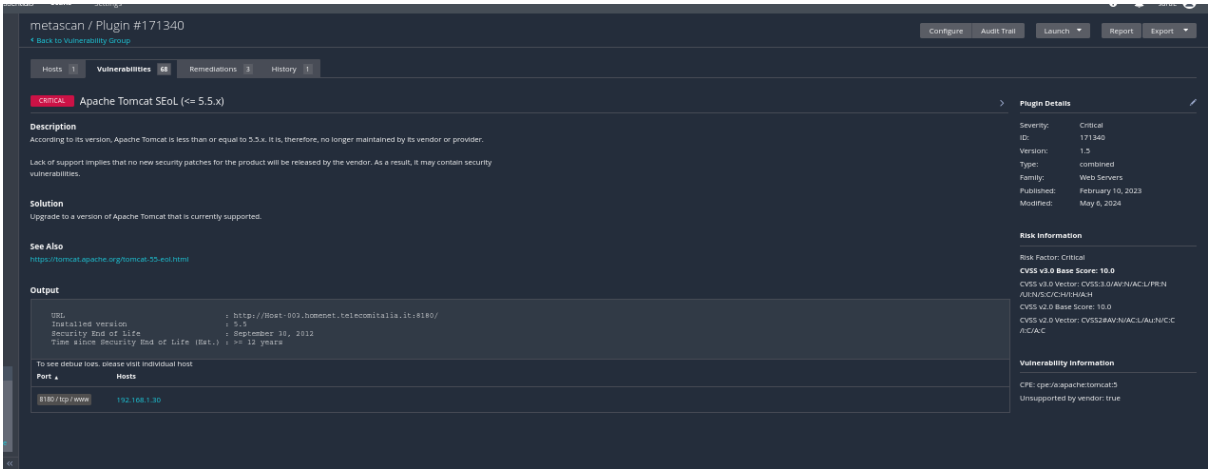
VULNERABILITA' 4: Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) **CRITICAL**

Il certificato x509 remoto sul server SSL remoto è stato generato su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL.Il problema è dovuto al fatto che un pacchettizzatore Debian ha rimosso quasi tutte le fonti di entropia nella versione remota di OpenSSL.Un aggressore può facilmente ottenere la parte privata della

chiave remota e usarla per decifrare la sessione remota o impostare un attacco man in the middle.Considerare tutto il materiale crittografico generato sull'host remoto come indovinabile. In particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN dovrebbe essere rigenerato.



VULNERABILITA' 5: Apache Tomcat SEoL (<= 5.5.x) **CRITICAL**



In base alla sua versione, Apache Tomcat è inferiore o uguale a 5.5.x. Pertanto, non è più mantenuto dal suo fornitore o provider. La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto. Di conseguenza, potrebbe contenere vulnerabilità di sicurezza. Esegui l'aggiornamento a una versione di Apache Tomcat attualmente supportata.