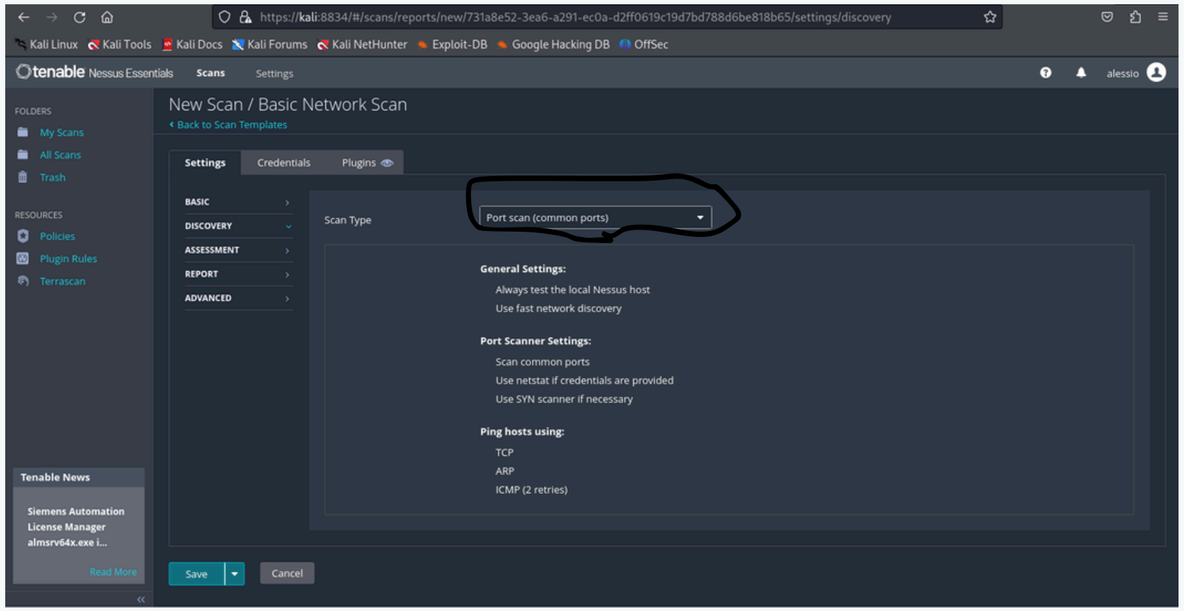
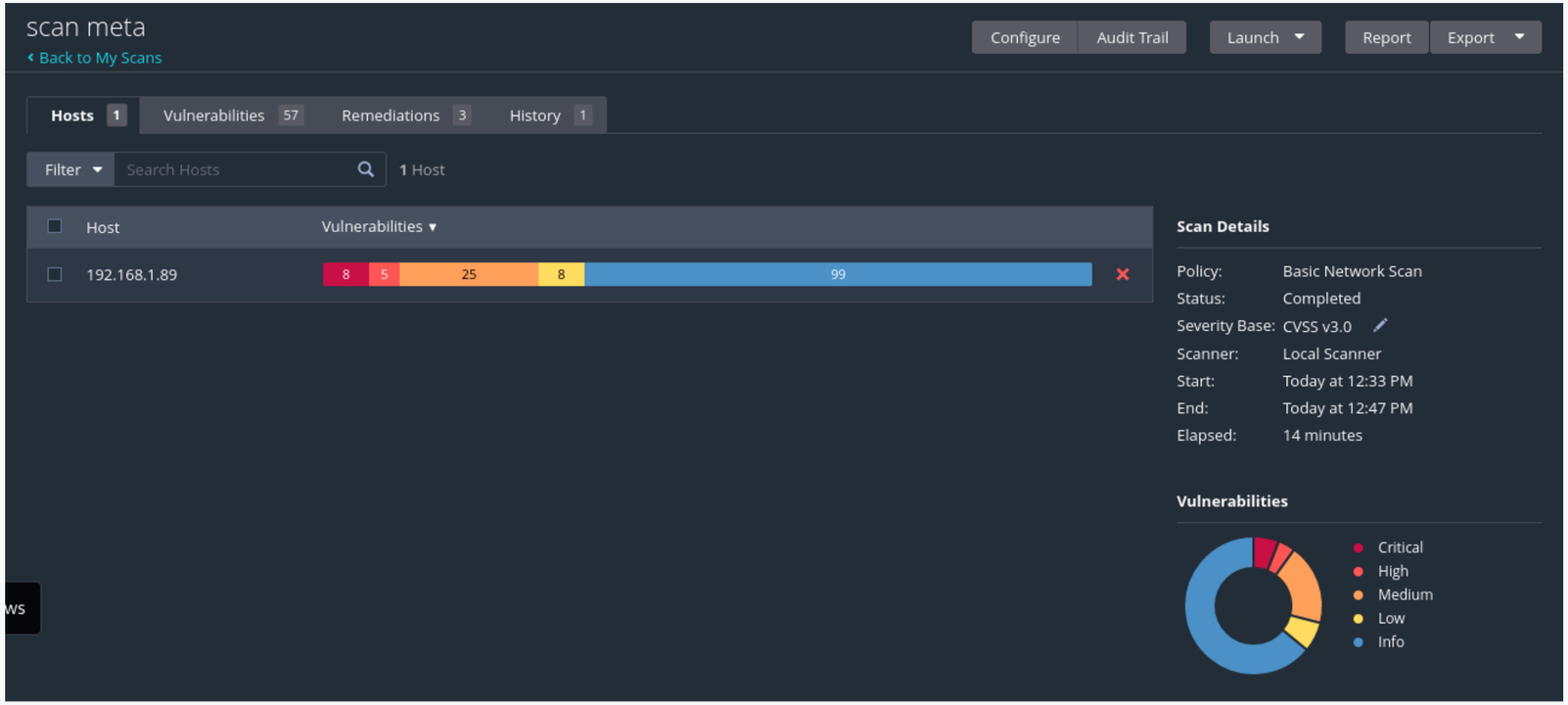
Pratica Nessus

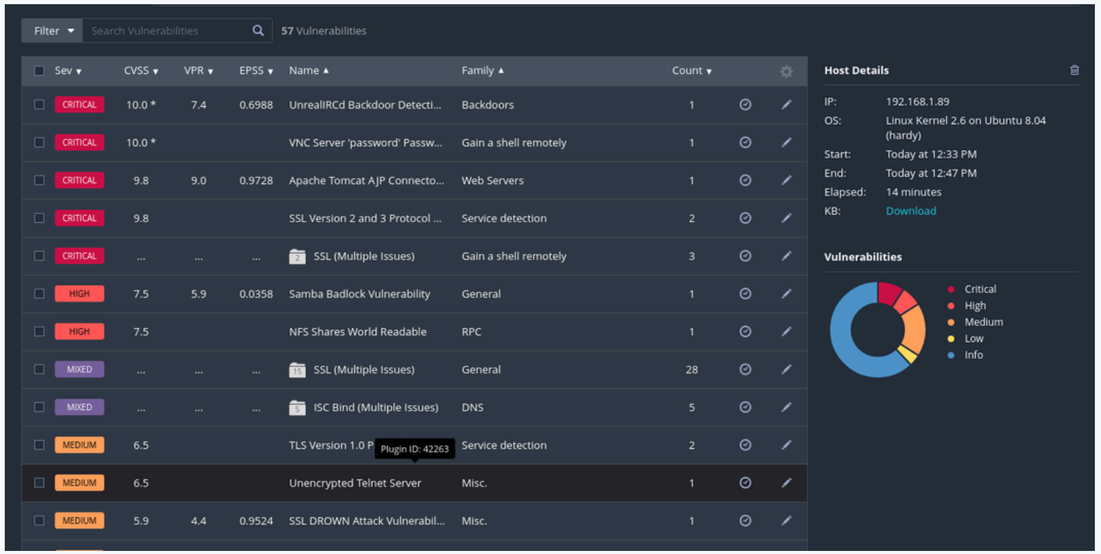
Nessus è un popolare strumento di vulnerability assessment utilizzato per identificare vulnerabilità di sicurezza in reti, sistemi e applicazioni. Sviluppato da Tenable, Nessus è particolarmente apprezzato per la sua capacità di eseguire scansioni approfondite e generare report dettagliati sui rischi di sicurezza presenti in un ambiente IT.



Inserimento dati Nessus per scansionare le porte comuni di Metasploitable

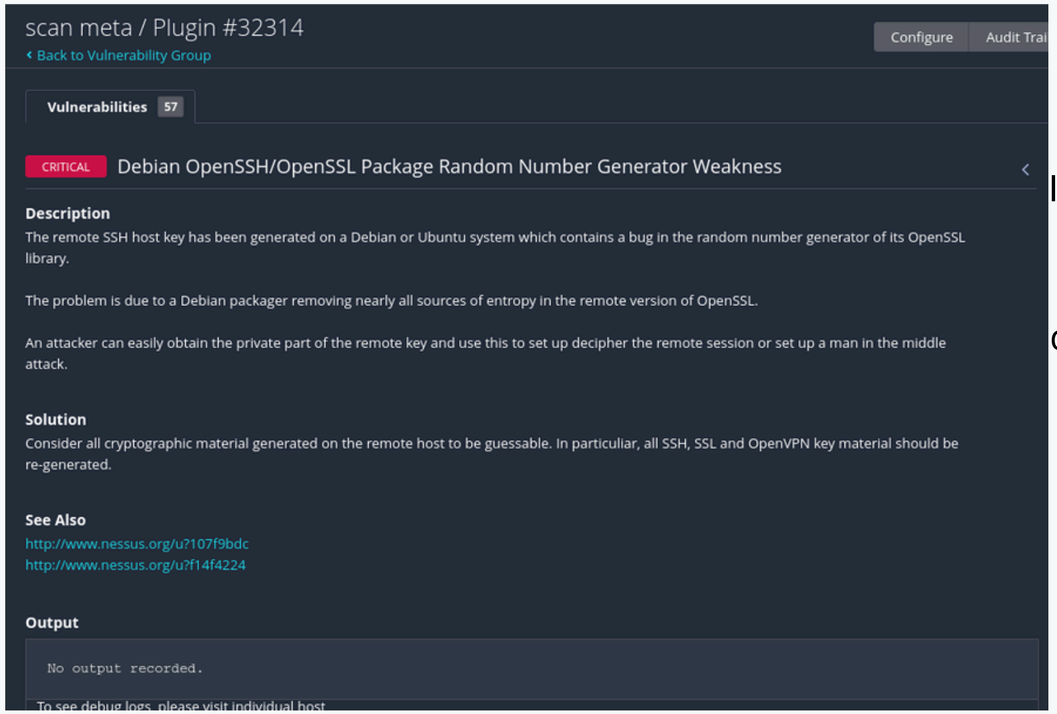


Avvio scansione del programma per la ricerca delle criticità



Alla fine della mia scansione avrò un report generale con tutti i livelli di criticità e consigli su come risolverli

Descrizione e soluzione delle criticità

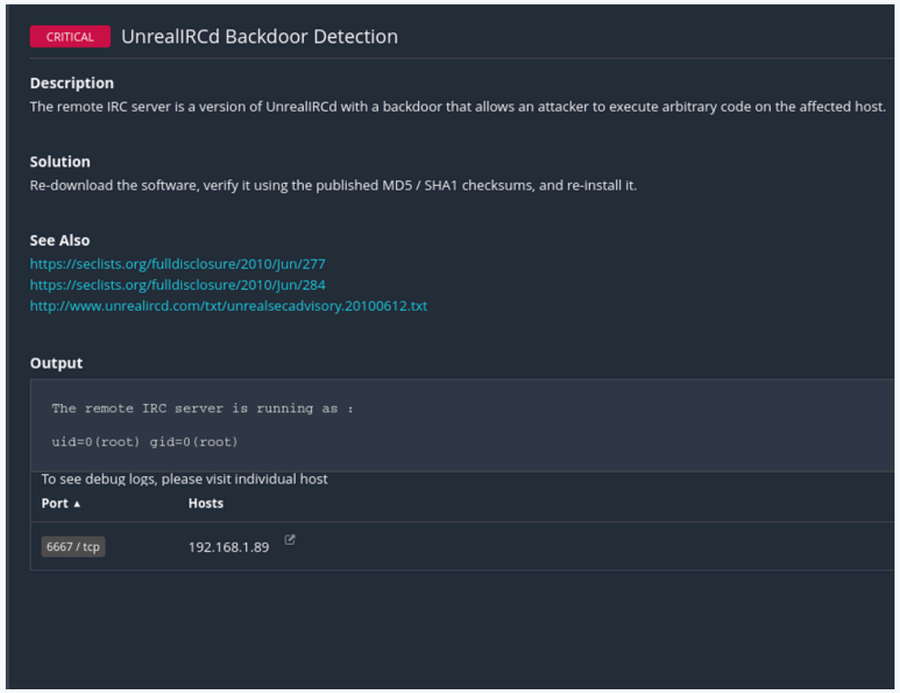


Descrizione

La chiave SSH remota è stata generata su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL.
Il problema è causato da un pacchettizzatore Debian che ha rimosso quasi tutte le fonti di entropia nella versione remota di OpenSSL.
Un attaccante può facilmente ottenere la parte privata della chiave remota e utilizzare questa informazione per decifrare la sessione remota o per impostare un attacco man-in-the-middle.

Soluzione

Considera tutto il materiale crittografico generato sull'host remoto come indovinabile. In particolare, tutte le chiavi SSH, SSL e OpenVPN dovrebbero essere rigenerate.



Descrizione problema

La UnrealIRCd Backdoor è una vulnerabilità di tipo backdoor che colpisce UnrealIRCd, un noto software di IRC (Internet Relay Chat) server. Questa vulnerabilità è il risultato di una compromissione del codice sorgente in una versione specifica di UnrealIRCd, che includeva una backdoor nascosta. La backdoor consente a un attaccante remoto di eseguire comandi arbitrari sul server senza alcuna autenticazione, permettendogli di prendere il controllo completo del sistema vulnerabile.

Soluzione

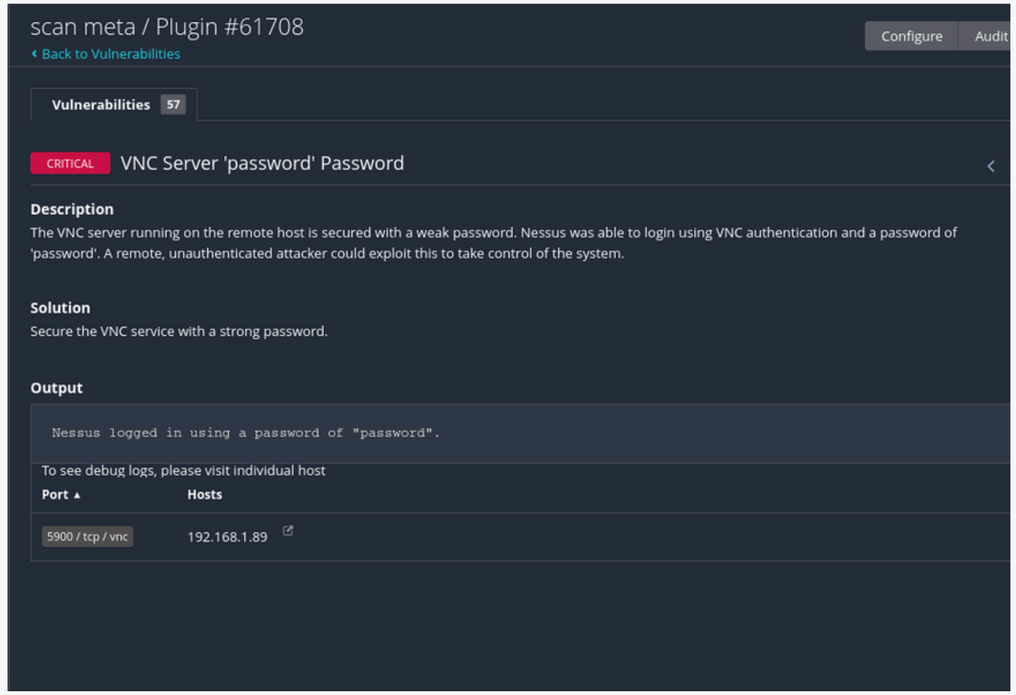
Riscarica il software, verificane l'integrità utilizzando i checksum MD5 / SHA1 pubblicati (Stringhe di caratteri generate da algoritmi criptografici) e reinstallalo.

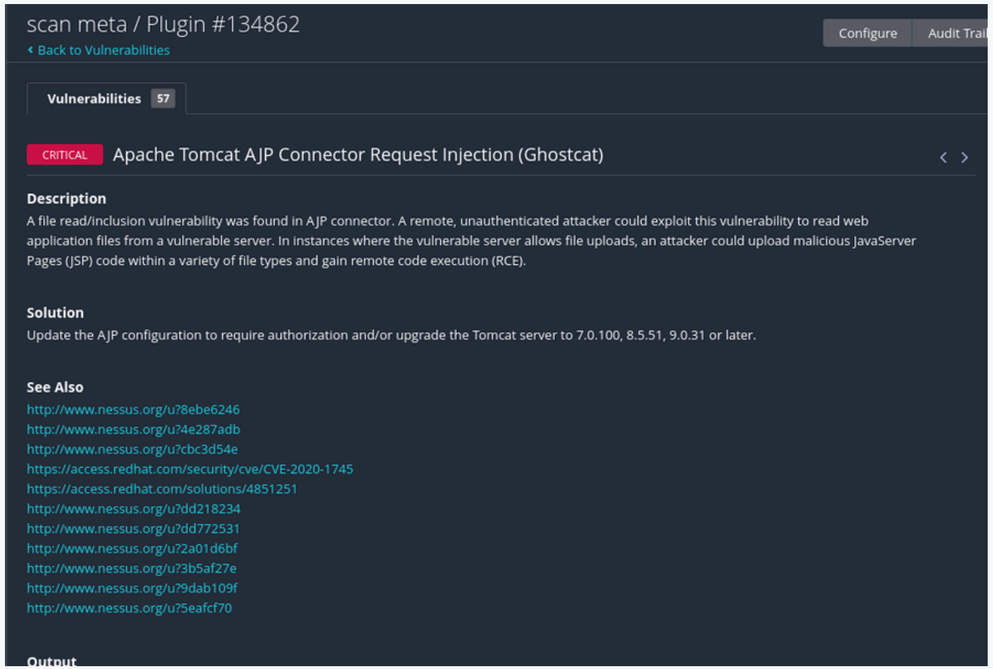
Descrizione problema

Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e la password "password". Un attaccante remoto non autenticato potrebbe sfruttare questa vulnerabilità per prendere il controllo del sistema.

soluzione

Proteggi il servizio VNC con una password forte.





Descrizione

È stata rilevata una vulnerabilità di lettura/inclusione di file nel connettore AJP. Un attaccante remoto non autenticato potrebbe sfruttare questa vulnerabilità per leggere file dell'applicazione web da un server vulnerabile. Nei casi in cui il server vulnerabile consente il caricamento di file, un attaccante potrebbe caricare codice JavaServer Pages (JSP) dannoso in diversi formati di file e ottenere l'esecuzione di codice remoto (RCE).

Soluzione

Aggiorna la configurazione AJP per richiedere l'autorizzazione e/o aggiorna il server Tomcat alla versione 7.0.100, 8.5.51, 9.0.31 o successive.

Descrizione

Il servizio remoto accetta connessioni criptate utilizzando SSL 2.0 e/o SSL 3.0. Queste versioni di SSL sono affette da diversi difetti crittografici, tra cui:

Uno schema di padding insicuro con cifrari CBC.

Schemi di rinegoziazione e ripristino della sessione insicuri.

Un attaccante può sfruttare queste vulnerabilità per condurre attacchi man-in-the-middle o per decriptare le comunicazioni tra il servizio interessato e i client.

Sebbene SSL/TLS disponga di un metodo sicuro per scegliere la versione più alta supportata del protocollo (in modo che queste versioni vengano utilizzate solo se il client o il server non supportano nulla di migliore), molti browser web implementano questo in modo non sicuro, consentendo a un attaccante di degradare una connessione (come nel caso del POODLE). Pertanto, si raccomanda di disabilitare completamente questi protocolli.

Il NIST ha stabilito che SSL 3.0 non è più accettabile per comunicazioni sicure. A partire dalla data di applicazione trovata nel PCI DSS v3.1, qualsiasi versione di SSL non soddisferà la definizione di "crittografia forte" del PCI SSC.

Soluzione

Consulta la documentazione dell'applicazione per disabilitare SSL 2.0 e 3.0. Utilizza invece TLS 1.2 (con suite crittografiche approvate) o versioni superiori.