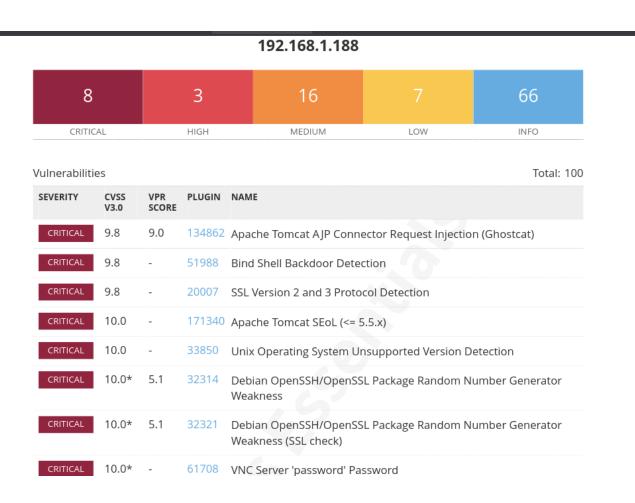
## Report S5L4

Per questo Report prenderemo in considerazione le criticità di livello critico riscontrate dallo scan di Nessus sulla macchina metasploitable.



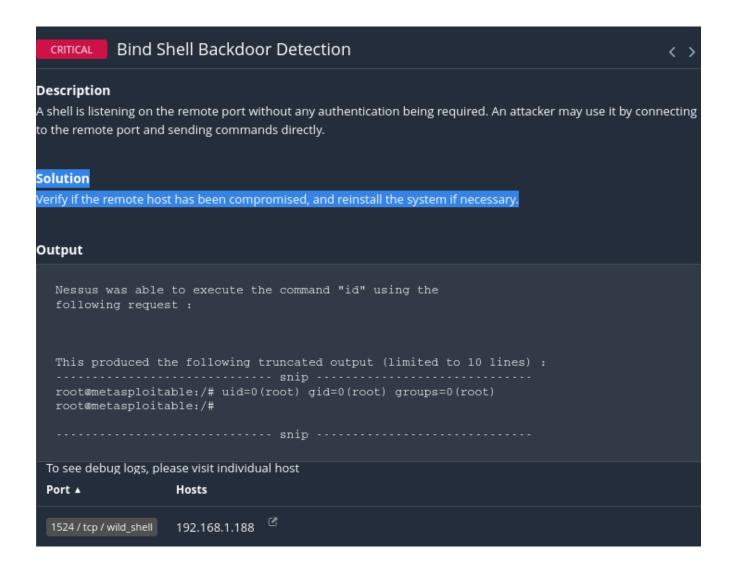
## **Apache Tomcat AJP Connector Request Injection (Ghostcat)**

Una vulnerabilità di lettura/inclusione di file è stata trovata nel connettore AJP. Un attaccante remoto, non autenticato, potrebbe sfruttare questa vulnerabilità per leggere i file delle applicazioni web da un server vulnerabile. Nei casi in cui il server vulnerabile permette il caricamento di file, un attaccante potrebbe caricare codice JSP (JavaServer Pages) malevolo all'interno di vari tipi di file e ottenere l'esecuzione di codice remoto (RCE).

Per mitigare la vulnerabilità nel connettore AJP di Apache Tomcat, è necessario aggiornare la configurazione di AJP per richiedere l'autorizzazione e/o aggiornare il server Tomcat alle versioni 7.0.100, 8.5.51, 9.0.31 o successive.

## **Bind Shell Backdoor Detection**

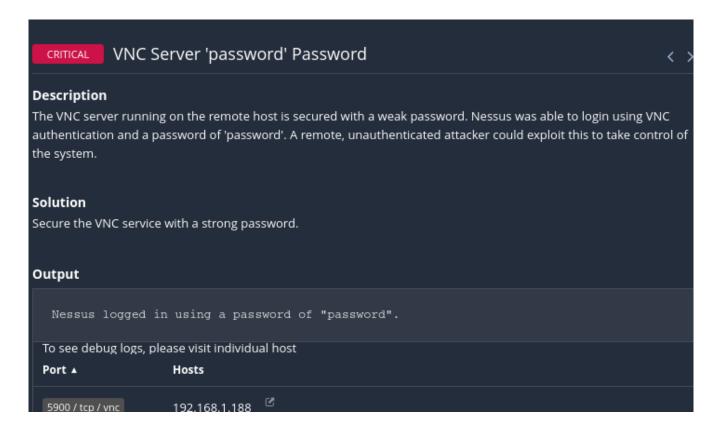
Una shell è in ascolto sulla porta remota senza richiedere alcuna autenticazione. Un attaccante può utilizzarla connettendosi alla porta remota e inviando comandi direttamente.



Come possiamo osservare Nessus ha rilevato una backdoor per la metaploit, interessante è vedere che a fondo pagina ci illustra I comandi usati e parte dei risultati ottenuti.

## VNC Server 'password' Password

Come evidenziato il server remoto VNC della meta, ha impostato come password: "password", il che può permettere a chiunque di entrare nel VNC e prendere controllo del sistema da remoto.



Il VNC è molto delicato e va protetto con una password forte.