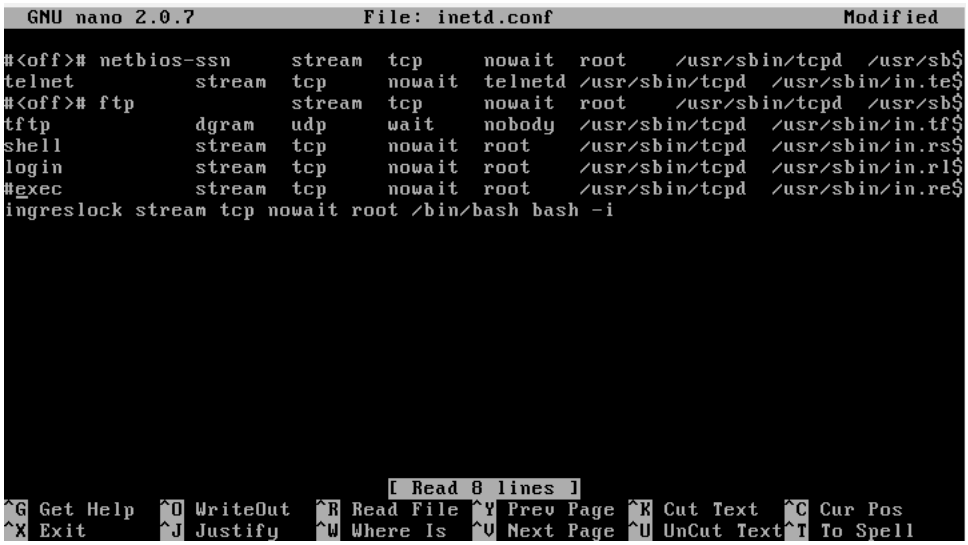
Report sulla Risoluzione delle Vulnerabilità nella VM Metasploitable

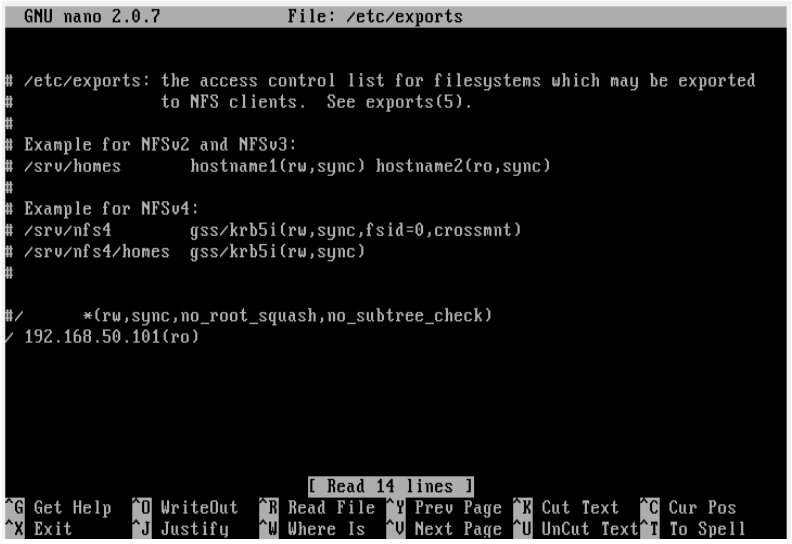
In questo report, descriverò come ho risolto le vulnerabilità trovate da Nessus nella macchina virtuale Metasploitable. Le vulnerabilità riguardano la rilevazione del servizio rexecd, la divulgazione delle informazioni sulle condivisioni esportate tramite nsf e la vulnerabilità della password del server VNC. Spiegherò brevemente ciascuna vulnerabilità e le azioni che ho intrapreso per risolverle.

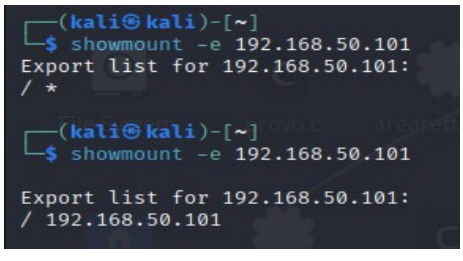
Vulnerabilità 1: Rilevazione del servizio rexecd



Il servizio rexecd è un servizio che permette di eseguire comandi su un computer remoto. È possibile sfruttare questo servizio per ottenere accesso non autorizzato al sistema. Per risolvere questa vulnerabilità, ho seguito il consiglio di Nessus e ho commentato la riga corrispondente nel file inetd.conf. In pratica, ho disabilitato il servizio rexecd nel sistema, impedendo a eventuali attaccanti di sfruttarlo.

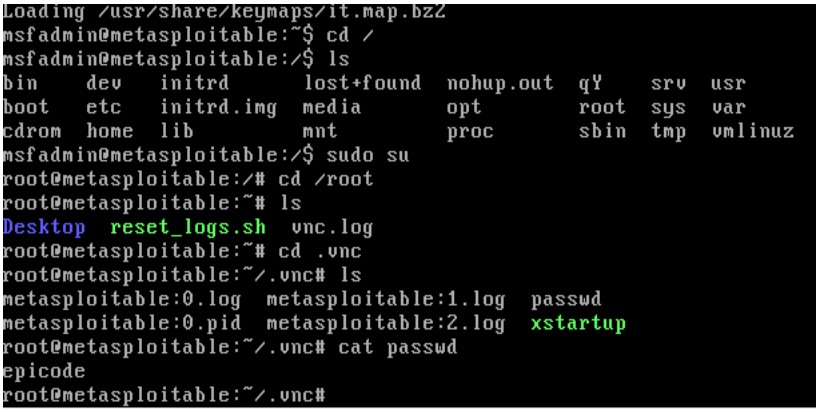
Vulnerabilità 2: Divulgazione delle informazioni sulle condivisioni esportate tramite nsf





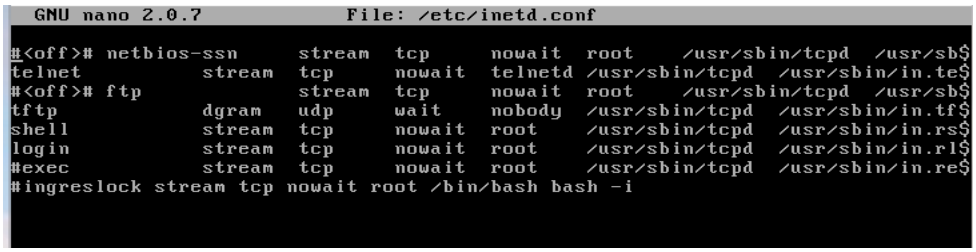
Questa vulnerabilità riguarda la divulgazione non autorizzata delle informazioni sulle condivisioni esportate tramite il servizio nfs. Un attaccante potrebbe ottenere accesso ai file e alle directory esposte, mettendo a rischio la sicurezza del sistema. Per risolvere questa vulnerabilità, ho modificato il file "exports" aggiungendo l'indirizzo IP della macchina Metasploitable come directory radice e ho commentato la riga precedente. In questo modo, ho limitato l'accesso alle condivisioni esportate solo alla macchina locale, impedendo agli attaccanti di sfruttare la vulnerabilità.

Vulnerabilità 3: Vulnerabilità della password del server VNC



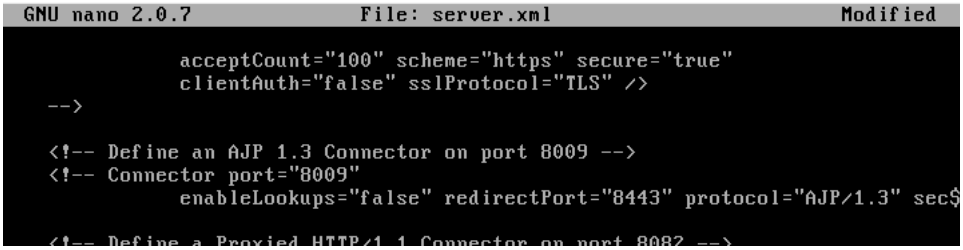
Questa vulnerabilità riguarda l'utilizzo di una password predefinita o debole per il server VNC, che potrebbe consentire a un attaccante di ottenere accesso non autorizzato al sistema. Per risolvere questa vulnerabilità, ho modificato la password nel file "passwd" utilizzato dal server VNC.

Vulnerabilità 4: Rilevamento della backdoor Bind shell



La quarta vulnerabilità riguarda la presenza di una backdoor Bind shell sulla macchina Metasploitable. Una Bind shell è una porta segreta che consente agli attaccanti di ottenere un accesso non autorizzato al sistema. Questa backdoor consente loro di eseguire comandi sul sistema compromesso a loro discrezione. Per risolvere questa vulnerabilità, ho modificato il file di configurazione appropriato, commentando la riga relativa al servizio "ingreslock stream". Questo ha impedito alla backdoor Bind shell di funzionare, rendendo impossibile l'accesso non autorizzato attraverso questa vulnerabilità.

Vulnerabilità 5: Connessione Apache Tomcat AJP



La quinta vulnerabilità che ho individuato riguarda il connettore AJP di Apache Tomcat. Il connettore AJP è un modo per far comunicare il server web Apache con il server Tomcat, ma può creare dei problemi di sicurezza se non viene configurato correttamente. Per risolvere questa vulnerabilità, ho disabilitato completamente il connettore AJP, in modo che non fosse più possibile comunicare tramite il protocollo AJP. Questo significa che non sarà più possibile sfruttare la vulnerabilità conosciuta come "Ghostcat" attraverso il connettore AJP. Disabilitando questa funzionalità, ho eliminato un possibile punto di ingresso per gli attaccanti, aumentando la sicurezza complessiva del sistema.