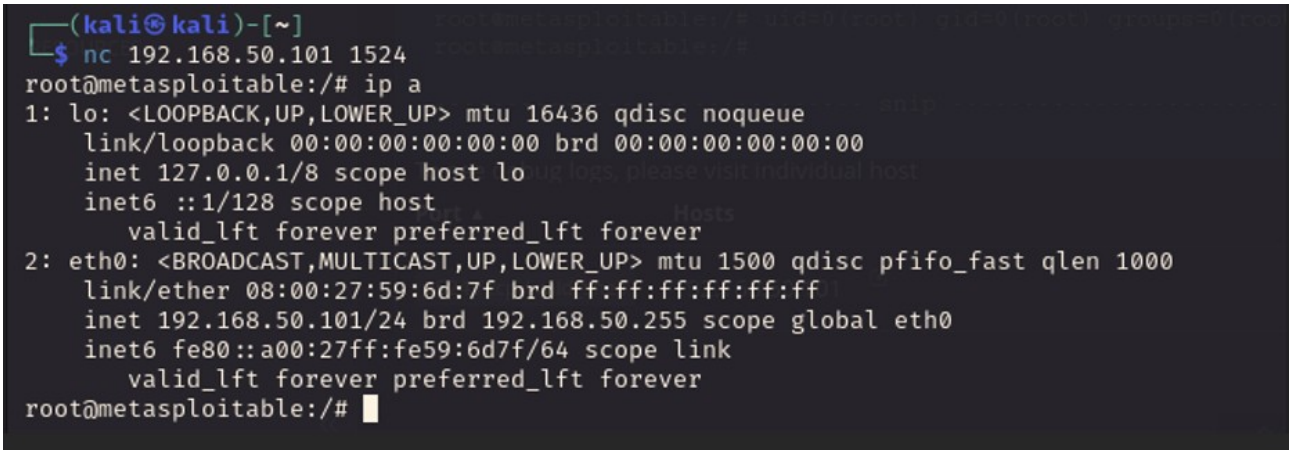
Benchmark M3 – Daniele Rufo

Dopo aver analizzato il report di nessus, risolviamo le vulnerabilità come richiesto:

1-Bind shell backdoor detection

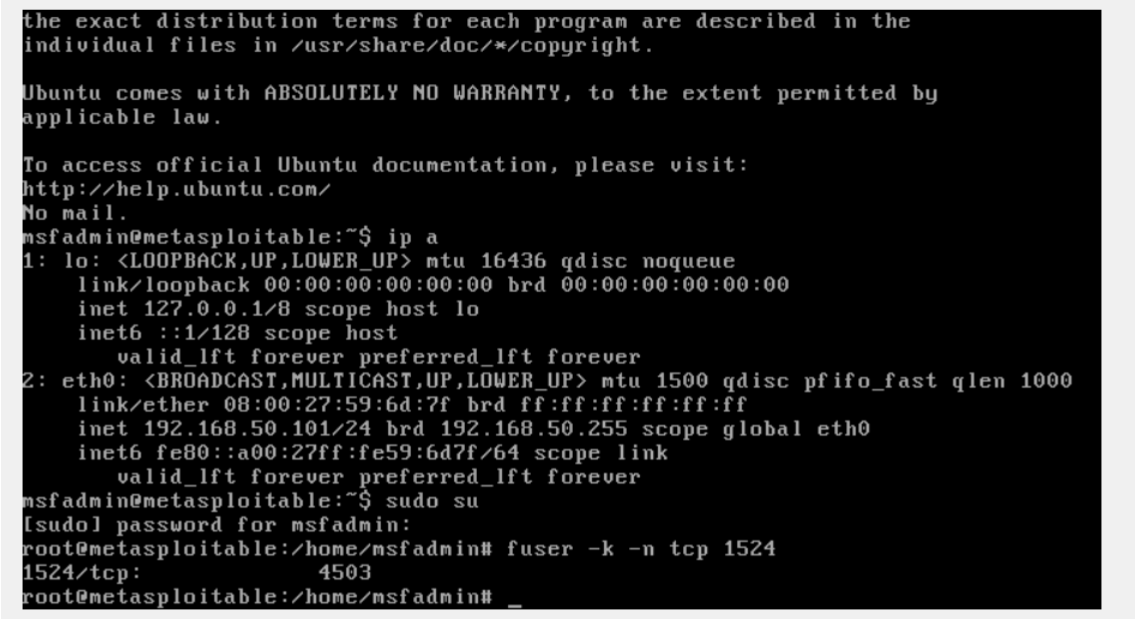
Critical 9.8 scoperta tramite il plugin 51988

La vulnerabilità fa riferimento ad una shell in ascolto su una porta senza che sia necessaria alcuna autenticazione. Un attaccante potrebbe quindi connettersi alla porta ed usare la shell. Per verificarlo ho usato netcat ed ha funzionato. Una volta connesso alla porta in questione (1524) ero in grado di usare una shell su kali ed eseguire comandi in metasploitable. Il tutto in figura sotto.

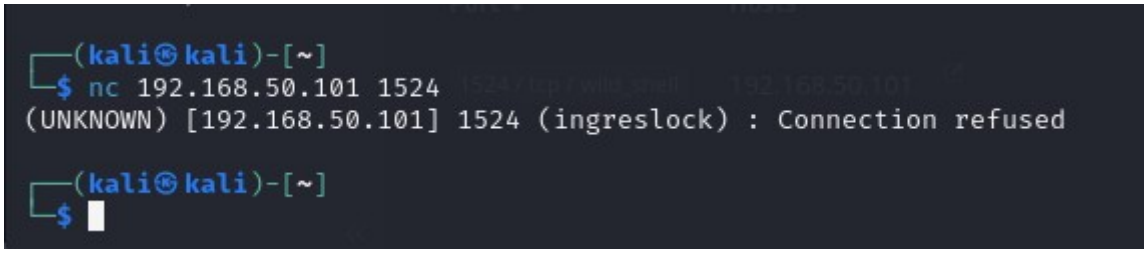


Lanciando un semplice “ip a” ricevo le informazione della configurazione di rete di Metasploitable.

La remediation trovata è stata la seguente: “fuser -k -n tcp 1524. Il comando fuser permette di individuare processi in base alle directory o ai socket a cui accede il processo stesso. Lo switch -n tcp specifica che ricerchiamo un processo che utilizza un socket tcp, mentre il -k è un kill (“sigkill”) che ci permette di eleminare il processo. In ogni caso viene riportato il PID del processo (4503).



Per conferma di quanto fatto ho tentato nuovamente di connettermi alla porta tramite netcat, ma senza successo, sintomo quindi che la vulnerabilità è risolta.



Nessus infatti non riportava più la vulnerabilità. Mi sono però accorto che dopo aver riavviato la macchina Metasploitable la backdoor tornava in funzione, ho quindi cercato il file usando il numero del PID (stavolta 4482) del processo (senza killarlo) e poi ho usato i comandi negli screen per prendere più info possibili. Così sono risalito alla directory xinetd da cui ho investigato per poi capire che le configurazioni erano in un altro file nella stessa directory /etc/inetd.conf.
Alla fine il problema era una riga di codice che usava ingreslock per lanciare una shell. Una volta eliminata il problema non si è più ripresentato.
Nello screenshot la configurazione con la riga, poi eliminata, che causava il problema.

2-NFS Exported Information Disclosure

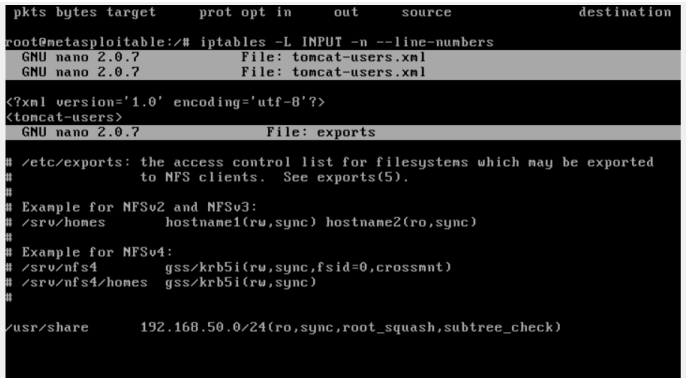
Critical 10.0 scoperta tramite il plugin 11356

Indica la possibilità di accesso a nfs share da remoto. Vanno riconfigurate le Esportazioni NFS che in pratica è la conf. del server che specifica quali directory sono condivise e quali permessi sono concessi ai client. Il file si trova in “etc/exports”. [**/usr/share 192.168.50.0/24 (ro,sync,root_squash,subtree_check**]
La configurazione è riportata nello screenshot più in basso. La spiegazione è la seguente:

- **/usr/share** specifica la directory da condividere (share appunto), l’impostazione precedente dava accesso a tutte le directory della macchina
- **192.168.50.0/24** specifica gli ip con cui viene condivisa la directory e quindi i file al suo interno. Ho indicato tutta la rete su cui è connessa metasploitable quindi una condivisione esclusivamente interna

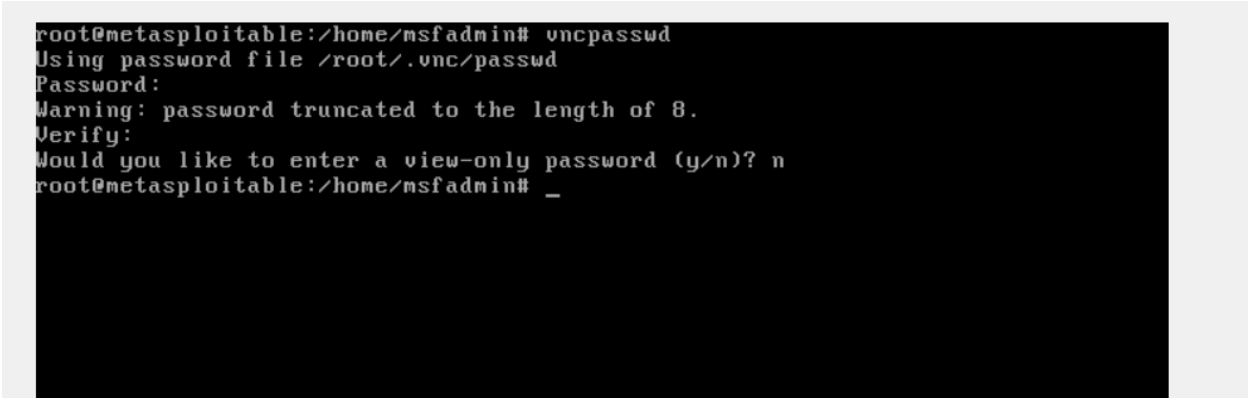
Le parentesi indicano invece i permessi che hanno i client a cui è consentito l’accesso:

- **ro** permette la sola lettura
- **sync** garantisce che i dati non vadano persi in caso di crush del server
- **root_squash** non garantisce privilegi di amministratore
- **subtree_check** verifica che tutte le opzioni sopra citate siano state rispettate



3-VNC server “password” password

Critical 10.0 scoperta tramite il plugin 61708
Virtual Network Computer è un sistema di controllo remoto che permette di interagire con un computer da remoto quindi potenzialmente molto pericoloso se sfruttato da un attaccante. Nessus evidenziava una password di accesso troppo debole che era riuscita a trovare nella lista “password”. Per risolverla è bastato impostare una password più sicura. I passaggi sono quelli visibili nello screenshot sottostante.



4-Apache Tomcat AJP connector request injection (Ghostcat)

Critical 10.0 scoperta tramite il plugin 134862

Vulnerabilità conosciuta come “Ghostcat” (CVE 2020-1938) che permette di leggere file arbitrari sul server oppure, in caso il server consenta upload, l’attaccante potrebbe caricare malware (con JSP...Javaserver page) e guadagnare accesso remoto.
La remediation consiste nel modificare le configurazioni del file “server.xml” di Tomcat. In particolare del connettore AJP (Apache Jserve Protocol) che consente la comunicazione tra un server web ed uno applicativo come Tomcat.
La modifica riguarda l’aggiunta dell’indirizzo di loopback nella configurazione della comunicazione gestita dal protocollo AJP così che sia quello che rimane in ascolto sulla porta.
Ecco la configurazione: