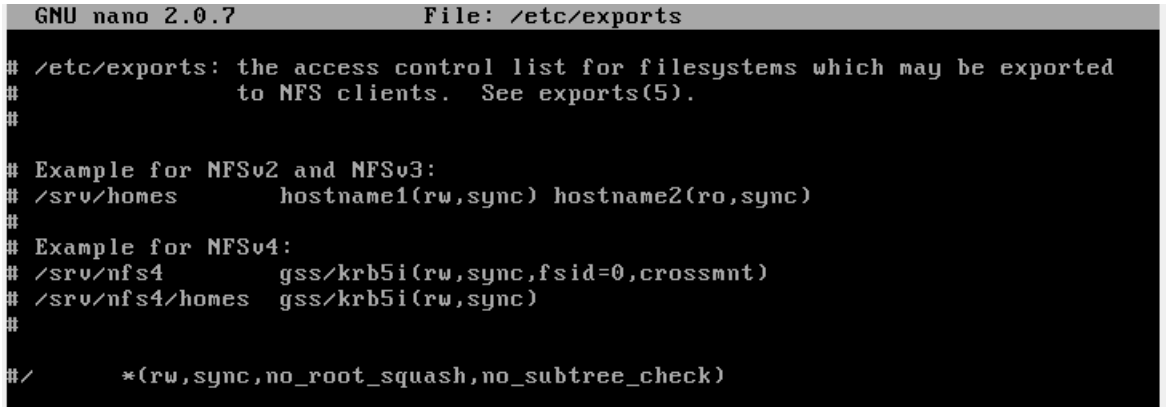
Test modulo M3

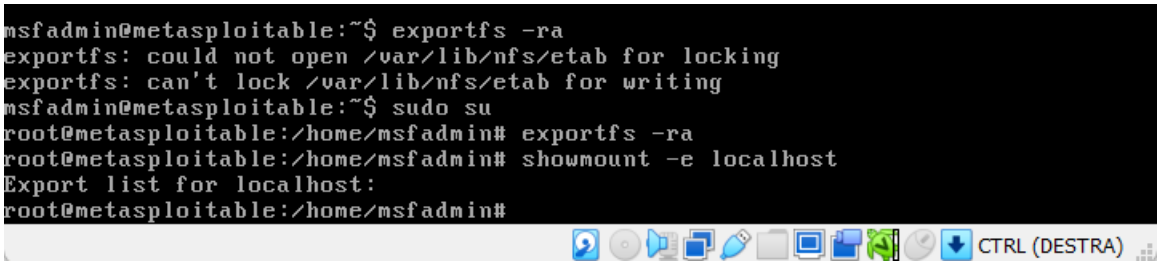
Qui vedremo la risoluzione di alcune problematiche che erano risultate nella prima scansione effettuata.

Problematica 1

NFS Exported Share Info Disclosure

Questa vulnerabilità permetteva ad un malintenzionato di poter leggere e scrivere file sulla nostra macchina.
Risoluzione: per risolvere questa vulnerabilità entriamo nella configurazione di NFS e andiamo a commentare con il '#' l'ultima stringa di codice che permetteva a qualsiasi host di poter creare sessioni remote.
Altra soluzione era quella di andare a specificare host per host quelli autorizzati alla condivisione.
Successivamente col comando **'exportfs -ra'** andiamo ad aggiornare le esportazioni NFS senza andare a riavviare il servizio e con il comando **'showmount -e localhost'** andiamo a verificare quali esportazioni sono presenti (nel nostro caso non visualizziamo risultati).



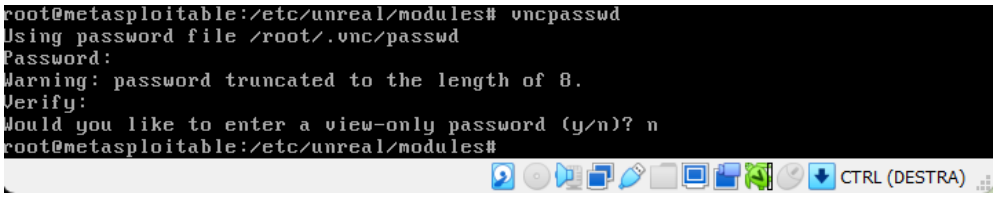


Problematica 2

VNC Server 'password' Password

Ci viene rilevata una password debole del sistema

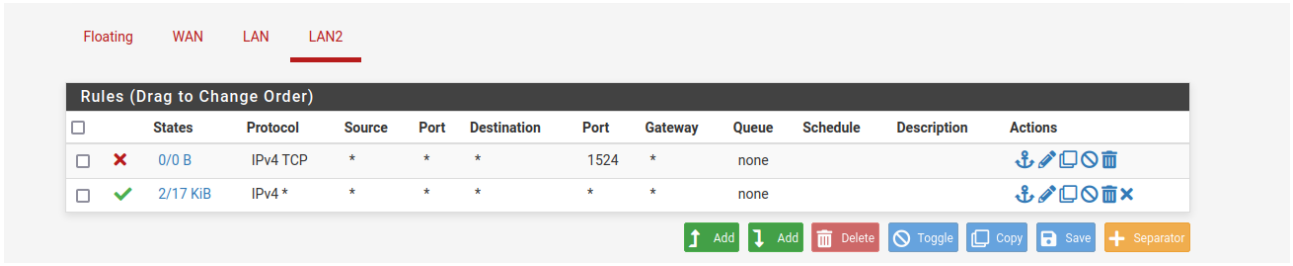
Risoluzione: qui molto semplicemente, utilizzando i privilegi d'amministratore, siamo andati a modificare una password considerata dal sistema debole andando a inserirne una più forte ed efficace con il comando '**vncpasswd'** (nello screen per questioni di privacy la password non viene mostrata).

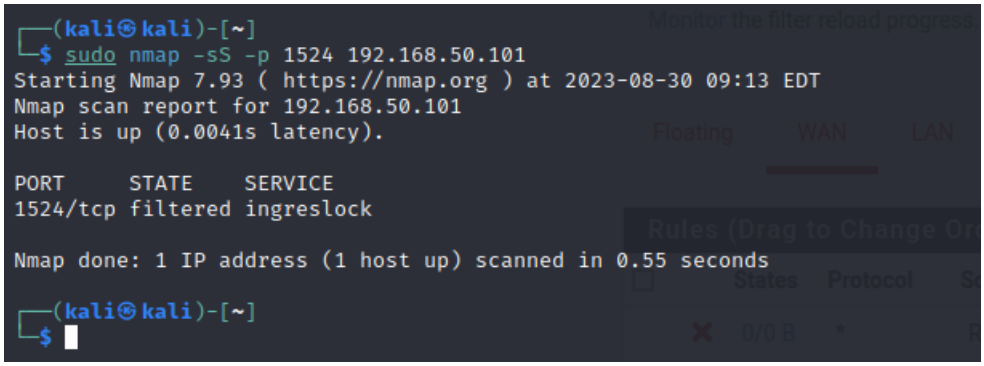


Problematica 3

Bind Shell Backdoor Detection

Qui la problematica rilevata faceva riferimento ad una shell in ascolto senza alcuna necessità di autenticazione.
Risoluzione: Tramite il nostro firewall Pfsense abbiamo creato una regola che andasse a bloccare il traffico verso la porta 1524. Questa prima risoluzione lascia la porta attiva, ma filtrata permettendo cosi una gestione del traffico sulla porta sicura.
Un'altra soluzione è quella di andare a chiudere completamente la porta eliminando così ogni possibilità di accesso. Purtroppo questo non è sempre possibile perché non sappiamo l'utilizzo che il cliente o l'azienda va a farne.
Qui verifichiamo come la regola Firewall abbiamo correttamente filtrato il traffico sulla porta.



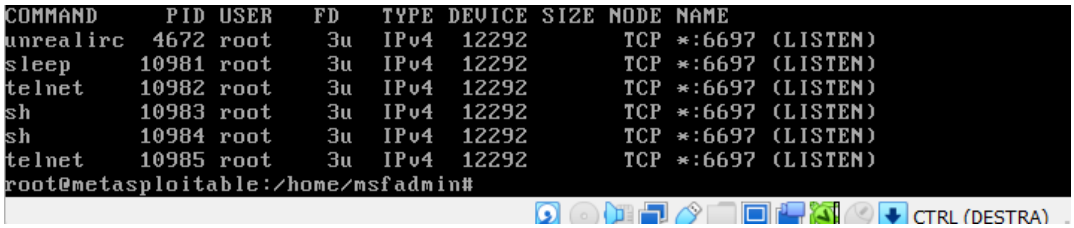


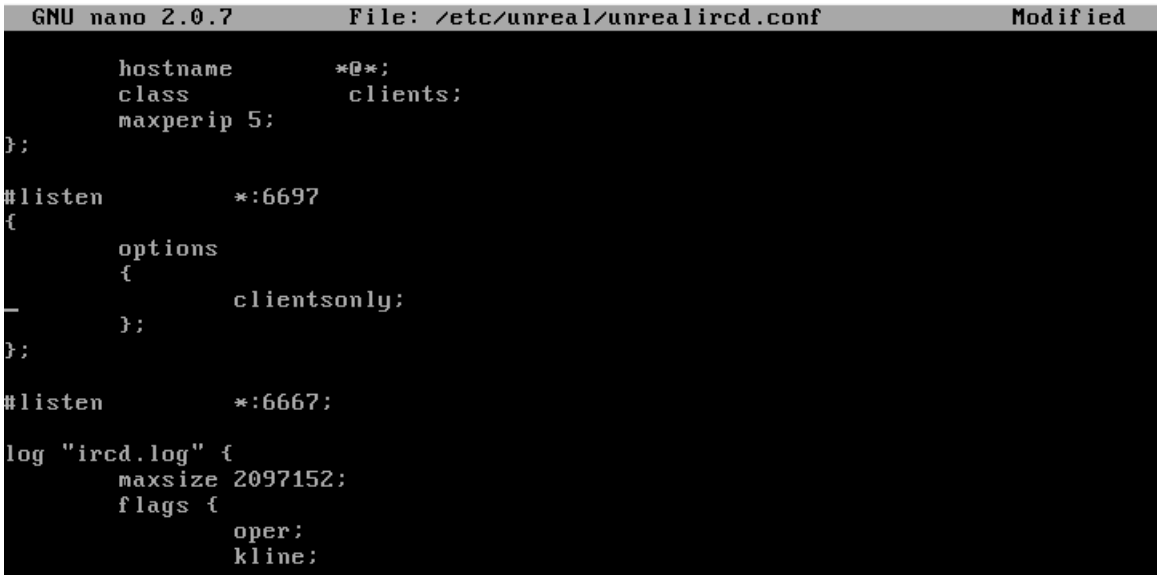
Problematica 4

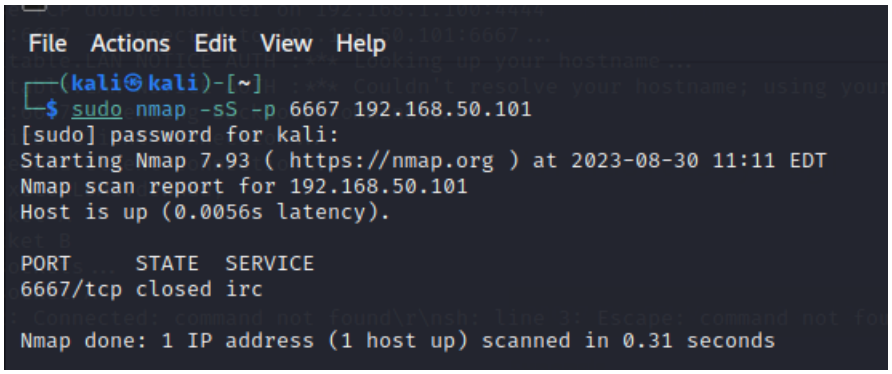
UnrealIRCd Backdoor Detection

Qui ci viene segnalata una backdoor sul server ICR
Soluzione: possiamo vedere nel primo screen che la porta 6697, designata all' ICR server è sempre in ascolto.
Per risolvere la problematica nel nostro caso è quello di dover chiudere la porta 6697 entrando nei file di configurazione e andando a ricercare la porta "incriminata" e andandola a chiudere (aggiungendo un '#' affianco al valore LISTEN della porta).

Successivamente si dovrà procedere con la sanificazione della porta per evitare la trapelazione di informazioni sensibili, effettuare test e analisi e verificare ulteriormente tutti gli accessi.





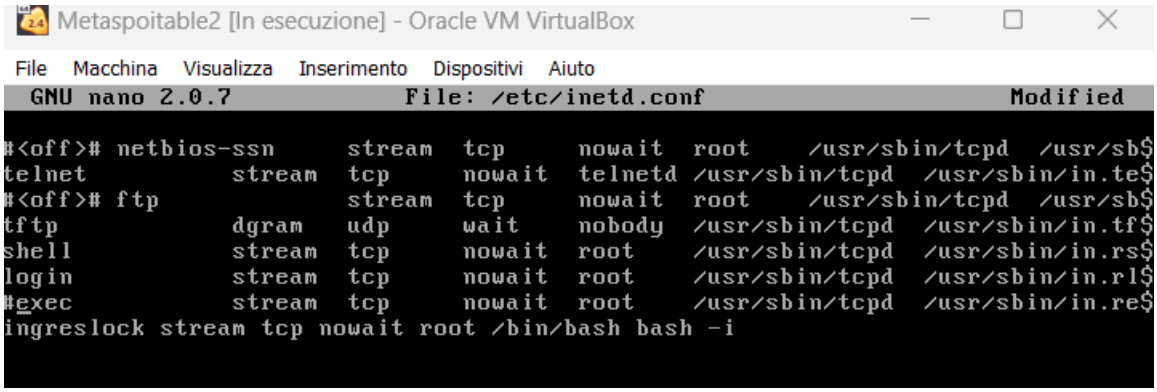


Problematica 5

Rexecd Service Detection

Rexecd è un servizio che consente agli utenti di una rete di eseguire i comandi da remoto, purtroppo questo metodo non ha dei buoi mezzi di autenticazioni quindi potrebbe essere utilizzato facilmente da malintenzionati.

Risoluzione: Per rimuovere la problematica dobbiamo entrare nella cartella del processo, essendoci prima autenticati come amministratore e disattivarlo o aggiornarlo alle nuove normative. Nel nostro caso lo disabilitiamo aggiungendo un semplice ‘#’ alla sua riga di comando andando a disabilitare il servizio.


Metaspoitable2 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /etc/inetd.conf Modified
#<off># netbios-ssn stream tcp nowait root /usr/sbin/tcpd /usr/sb$
telnet stream tcp nowait telnetd /usr/sbin/tcpd /usr/sbin/in.te$
#<off># ftp stream tcp nowait root /usr/sbin/tcpd /usr/sb$
tftp dgram udp wait nobody /usr/sbin/tcpd /usr/sbin/in.tf$
shell stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rs$
login stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rl$
#exec stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.re$
ingreslock stream tcp nowait root /bin/bash bash -i