Remediation meta

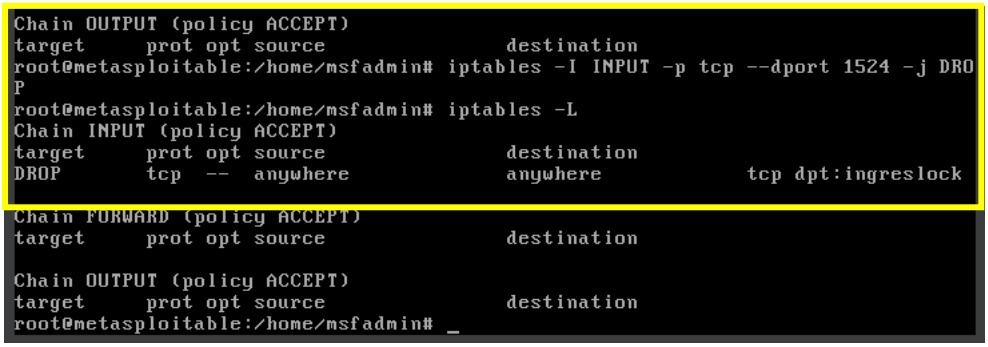
Scan meta

Report generated by Nessus™ Thu, 24 Nov 2022 09:12:45 EST

51988 - Bind Shell Backdoor Detection:

Per la risoluzione di questa minaccia si può procedere in questo modo: andiamo sulla shell di meta e avremmo bisogno dei privilegi di root (SUDO), andiamo a digitare il comando **iptables** questo comando corrisponde al firewall dei sistemi operativi LINUX, per andare bloccare il traffico verso la porta 1524 il comando e il seguente: **iptables -I INPUT -p tcp –dport 1524 -j DROP** .

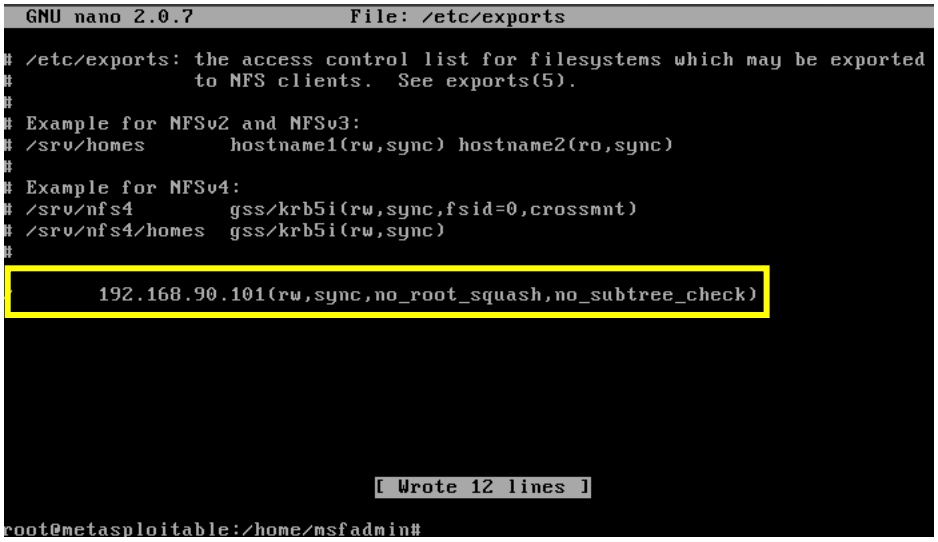
Ho eseguito poi il comando: **iptables -L** per controllare che la regola sia stata inserita correttamente.



11356 - NFS Exported Share Information Disclosure:

Per ovviare a questo problema dobbiamo andare sulla shell di meta avere i privilegi root(SUDO) la procedura è la seguente. Accedere al file di configurazione del NFS con il comando nano /etc/exports e come si può vedere nell' ultima riga c'è * che permette la comunicazione, per permettere la comunicazione dobbiamo sostituire * con l'hostname delle macchine autorizzate.

Ho inserito l'IP di meta così da non permettere la comunicazione con altri client.



61708 - VNC Server 'password' Password:

Per risolvere questa criticità la soluzione è la seguente: andare nella shell di meta eseguire il comando **vncpasswd** e inserire una password più complessa