Remediation

Tabella versione software e ip delle macchine

Macchina/software	Versione
Kali (192.168.32.100)	2023.2
Meta (192.168.50.101)	Linux Kernel 2.6
Pfsense	2.6.0
Nessus	10.5.2

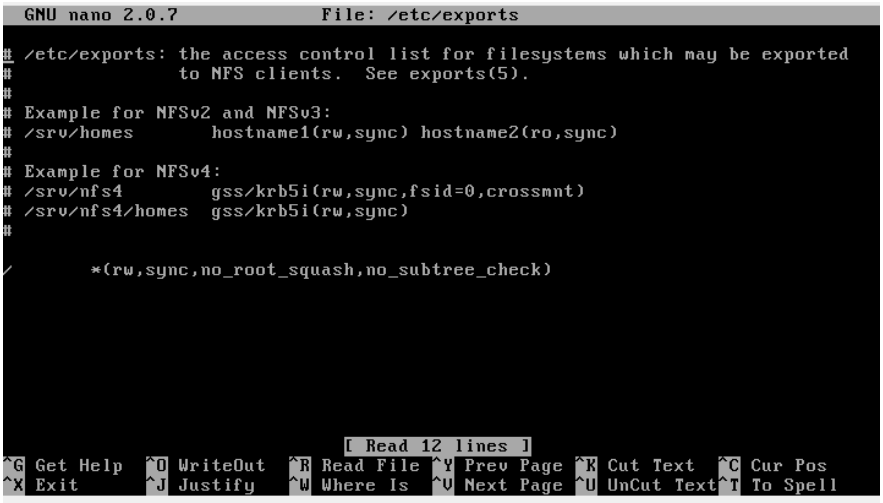
In questa rete, Pfsense fa da router tra kali e meta, poste su due reti differenti e verrà utilizzato anche per la Remediation con qualche regola firewall.

Vulnerabilità n1

1356 - NFS Exported Share Information Disclosure

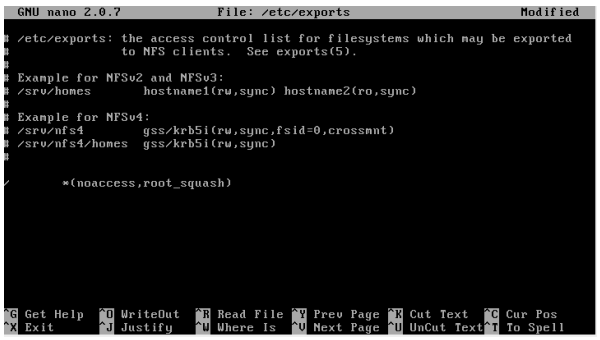
Una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un attaccante potrebbe sfruttare ciò per leggere (e eventualmente scrivere) file sull'host remoto.

Per risolvere questa vulnerabilità con il comando " sudo nano /etc/exports" accedo al file di configurazione dell'esportazioni NFS.



Vado a modificare l'unica riga attiva dove i client hanno permessi di scrittura e lettura. Col no_root_squash, consente all'utente root di mantenere i propri privilegi root sulla condivisione NFS.

Modifico la riga con no access, root_squash così da risolvere la vulnerabilità vietando l'accesso e evitando di far mantenere al client, i privilegi root sulla condivisione NFS.



Vulnerabilità n2

42256 - NFS Shares World Readable

Il server NFS remoto sta esportando una o più condivisioni senza restrizioni di accesso (basate su hostname, IP o intervallo IP).

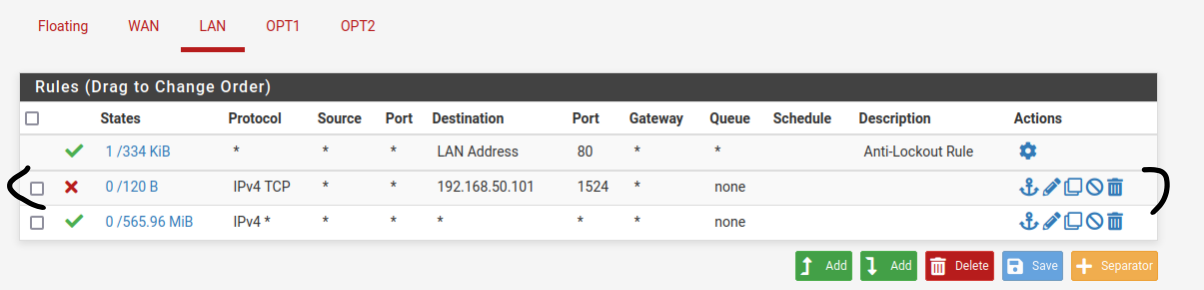
Con la modifica del file /etc/exports/ fatto nella vulnerabilità 1, si risolve anche quest'altra, in quanto collegate tra di loro.

Vulnerabilità n3

51988 - Bind Shell Backdoor Detection

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

Per rimuovere questa vulnerabilità utilizzo il firewall Pfsense, per andare a bloccare la porta specifica della backdoor "1524". Effettuando un nmap -p 1524 su meta, lo stato della porta infatti è passata da aperta a filtrata.

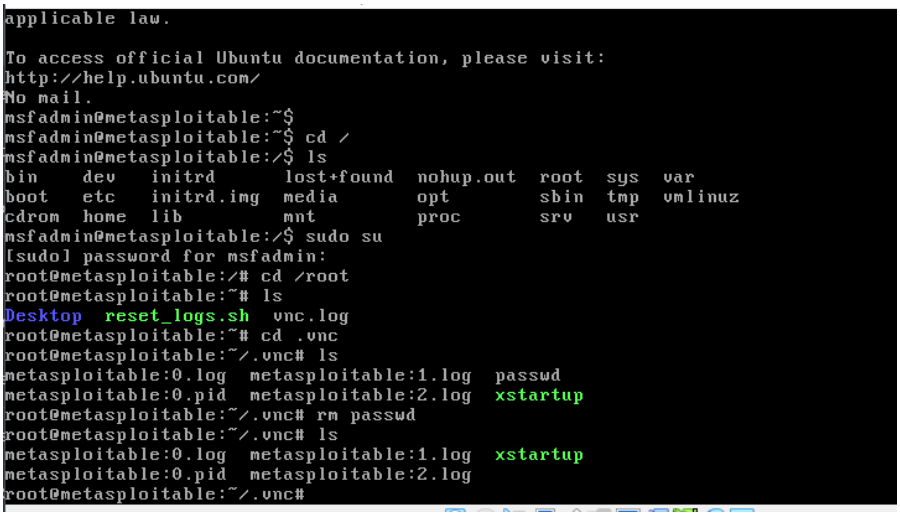


Vulnerabilità n4

61708 - VNC Server 'password' Password

Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è stato in grado di effettuare il login utilizzando l'autenticazione VNC e una password "password". Un attaccante remoto non autenticato potrebbe sfruttare questa vulnerabilità per prendere il controllo del sistema.

Per risolvere questa vulnerabilità vado nella directory root ed entro in vnc. Dentro la cartella di vnc trovo il file password, e lo rimuovo così da mantenere l'accesso solo con l'utente msfadmin ed un attaccante da remoto non è in grado di prendere i privilegi root.



Vulnerabilità n5

Rexecd Service Detection

Da traccia, dovevo risolvere anche questa vulnerabilità, che Nessus non mi ha rilevato. Facendo ricerche sul web, ho capito che ciò non è stata rilevata per la versione dei dispositivi. Quindi ho visto ugualmente come poter risolvere questa vulnerabilità e col comando " sudo nano/etc/inetd.conf" si accede alla configurazione del servizio e basta andare a commentare la riga del servizio exec, che è appunto il servizio con la vulnerabilità.