Remediation delle vulnerabilità

Vulnerabilita risolte:

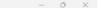
Bind Shell Backdoor Detection NFS Exported Share Information Disclosure VNC server 'password" Password

1.Bind Shell Backdoor Detection

Per quanto riguarda la risoluzione di questa vulnerabilità, ho abilitato il firewall di Mestasploitable con il comando "UFW ENABLE"

Dopodichè, ho detto al firewall di acconsentire a tutte le regole di default con "UFW DEFAULT ALLOW*

File Macchina Visualizza Inserimento Dispositivi Aiuto

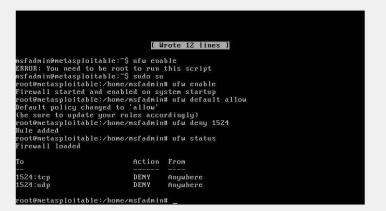


Integrazione del mouse...

Acquisizione automatica della tastiera... 🛜 🗯

即@

20 83





2. NFS Exported Share Information Disclosures

Per quanto riguarda la prima vulnerabilità, la remediation da applicare e quella di inserire all'interno della sottocartella del root /etc.

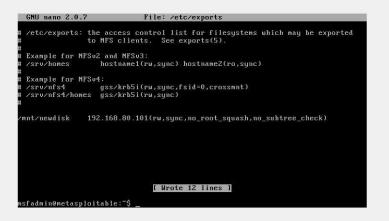
La prima cosa da fare è quella di visualizzare all'interno delle sottocartelle del root con "Is -a".

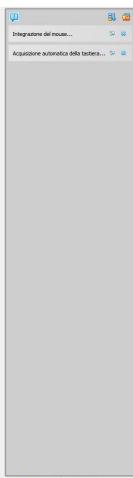
Cerchiamo la directory "/etc" e apriamo il file "exports".

All'interno di questo file, andremo a modificare 1'* in fondo alla pagina con l'ip della nostra macchina.

Una volta fatto, riavviamo la macchina.









3. VNC Server 'password' Password

Per modificare la password del VNC Server, troviamo all'interno della directory msfadmin, con il comando Is-a, il directory .vne. All'interno di questa directory, andremo a eseguire il comando "vnopasswd" per cambiare la password.

Alla fine riavviamo la macchina.

File Macchina Visualizza Inserimento Dispositivi Aiuto



