



# **RISOLUZIONE VULNERABILITA METASPOITABLE 2**

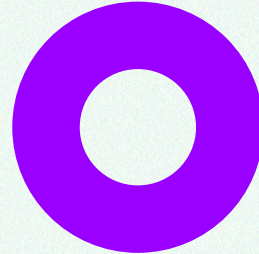
Kamenica Kristiano





# Report Scan Nessus

- Per prima cosa ho eseguito un Scan con Nessus sulla macchina virtuale di Metasploitable 2, in modo da avere visione di tutte le vulnerabilità.



Link al report





# Vulnerabilita Scelte

01

**CRITICAL** NFS Exported Share Information Disclosure

03

**CRITICAL** Bind Shell Backdoor Detection

02

**CRITICAL** VNC Server 'password' Password





# “NFS Exported Share Information Disclosure:”

1. Per risolvere il problema di sicurezza nelle condivisioni NFS, è necessario apportare alcune modifiche ad un file con al suo interno i vari permessi.

Utilizzando il comando:

**sudo nano /etc/exports**

2. Questo comando permette di accedere ad un elenco di autorizzazioni di cui noi dobbiamo rimuovere:


**\* (rw.....)**

3. La riga che abbiamo rimosso permetteva a chiunque l'accesso. Dopo averla cancellata salviamo le modifiche e riavviamo il sistema.





# “VNC server “password” Password:”

- 
1. Per risolvere il problema della password troppo banale del server VNC ho dovuto utilizzare il seguente comando:

**nano ~/.vnc/passwd**

2. Che mi permette di accedere al file che “possiede” la password del server VNC. In questo modo noi possiamo modificarla con una password più complessa in modo da aumentare la sicurezza.

3. Ricordiamo fondamentale dover salvare e riavviare per poter applicare le modifiche.





# “Blind Shell Backdoor Detection:”

1. Utilizzando Nessus, ho individuato la porta responsabile della backdoor. Successivamente ho eseguito il comando per identificare il processo o il file associato alla porta 1524 :

**Lsof -i :1524**

2. Il risultato del comando ha mostrato il programma/processo “ingreslock”(1524/tcp) , noto per essere utilizzato per il controllo remoto.

3. Per risolvere il problema , mi sono informato sul file inetd.conf, un file che gestisce dinamicamente le richieste di vari servizi di rete.

Utilizzando il seguente comando ho aperto il file:

**sudo nano /etc/inetd.conf**

4. Aperto il file ho eliminato la sezione riguardante “ingreslock”.

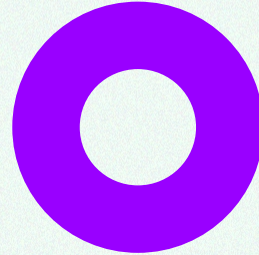
## 5. SPIEGAZIONE DI INETD.CONF E DEI DEMONI :

- “Inetd.conf” è un file di configurazione che contiene informazioni sulle connessioni di rete e i servizi associati. Modificando questo file, è possibile gestire dinamicamente i servizi di rete offerti dal sistema.
- I demoni di sistema sono processi in background che eseguono funzioni di sistema essenziali. Modificando la configurazione di questi “demoni”, è possibile influenzare il comportamento e la sicurezza del sistema.



# Report Scan Nessus Post FIX

- Alla fine di tutto ho eseguito un altro scan con Nessus per controllare di aver risolto le vulnerabilità.  
Allego il report in formato pdf:



Link al report







# GRAZIE!

KAMENICA KRISTIANO