# Progetto M3

*Fabrizio Meini*

*"Analisi di Vulnerabilità e Implementazione di Azioni di Rimedio su Metasploitable"*

**Analisi ed implementazione azioni di rimedio (MITIGAZIONE):**

VULNERABILITA': NFS Exported Share Information Disclosure
AZIONI DI RIMEDIO: Per mitigare questa vulnerabilità, è necessario configurare correttamente le autorizzazioni delle condivisioni NFS e implementare misure di sicurezza come l'accesso controllato e l'autenticazione per limitare l'esposizione delle informazioni sensibili attraverso la condivisione NFS.

*Per risolvere questo problema ho deciso di dare l'autorizzazione per l'accesso al file NFS solo all'indirizzo ip 192.168.1.100 (che corrisponde a quello della machina metasploitable) in modo da far si che risulti inaccessibile dall'esterno.*

```
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes       hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes  gss/krb5i(rw,sync)
#

/       192.168.1.101(rw,sync,no_root_squash,no_subtree_check)
```

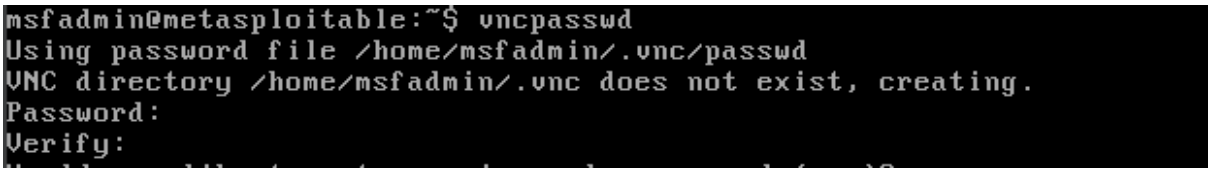
VULNERABILITA': Bind Shell Backdoor
AZIONI DI RIMEDIO: Per rilevare un bind shell backdoor, possono essere adottati vari approcci, tra cui: monitoraggio delle porte aperte, analisi dei processi in esecuzione, analisi del traffico di rete, controllo dei file di configurazione, scansione antivirus e antimalware, analisi delle attività di accesso. Utilizzando una combinazione di questi metodi, è possibile individuare e mitigare con successo la presenza di un bind shell backdoor sul sistema.

*In questo caso, non potendo stabilire direttamente da metasploitable se esiste effettivamente un programma che mantiene attivo una backdoor, possiamo limitarci a eseguire dei controlli nel file di sistema ed utilizzare degli antivirus.*

VULNERABILITA': Vnc server password password

AZIONI DI RIMEDIO: Per configurare correttamente una password per il server VNC, è consigliabile utilizzare una password robusta e complessa che includa una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali. Inoltre, è buona prassi evitare parole comuni o facilmente indovinabili.

*Questa vulnerabilità è la più facile da ridurre, in quanto basterà sostituire la password con una molto più sicura e mantenerla aggiornata. Per farlo utilizzo i seguenti comandi:*




VULNERABILITA': SSL Version 2 and 3 Protocol Detection

AZIONI DI RIMEDIO: Una volta identificati i protocolli SSL obsoleti, è consigliabile disabilitarli sul server e utilizzare solo versioni più recenti e sicure del protocollo, come TLS 1.2 o TLS 1.3, per garantire la sicurezza delle comunicazioni.

*Per risolvere la criticità basta disattivare i protocolli SSL2 e SSL3, sostituendoli con uno più aggiornato come TLS 1.2.*