Esame D3 Di Angelo Gravanti

Data scansione: 13/05/2024

10	6	19	8	75
CRITICAL	**HIGH**	**MEDIUM**	**LOW**	**INFO**

Come possiamo vedere abbiamo rilevato 10 Critical, 5 High, 22 Medium, 8 Low e 120 info.
Il progetto d'esame attuale richiede di risolvere almeno 2 Critical.

Le due richieste che oggi andremmo a risolvere sono le seguenti:

CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	7.4	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	61708	VNC Server 'password' Password

Host Information

- **Netbios Name:** Metasploitable
- **IP:** 192.168.1.58
- **MAC Address:** 08:00:27:4A:6A:02
- **OS:** Linux Kernel 2.6 Ubuntu 8.04

NFS Exported Share Information Disclosure (11356)

CRITICAL

Che cos'è?
Questa vulnerabilità permette a un attaccante di accedere a file e directory sensibili esportati tramite NFS senza le necessarie autorizzazioni. Tra i dati esposti vi sono file di configurazione, dati utente, informazioni di sistema e altri dati sensibili memorizzati nei file system condivisi.

Come si risolve?
Per garantire la sicurezza del sistema NFS, è fondamentale configurare correttamente le autorizzazioni dei file, utilizzare un firewall per limitare l'accesso alle porte NFS solo agli utenti autorizzati, mantenere il sistema aggiornato con le ultime patch di sicurezza, implementare autenticazione e crittografia per proteggere i dati sensibili e monitorare attentamente il traffico di rete per rilevare attività sospette.

VNC Server 'password' Password(61708)

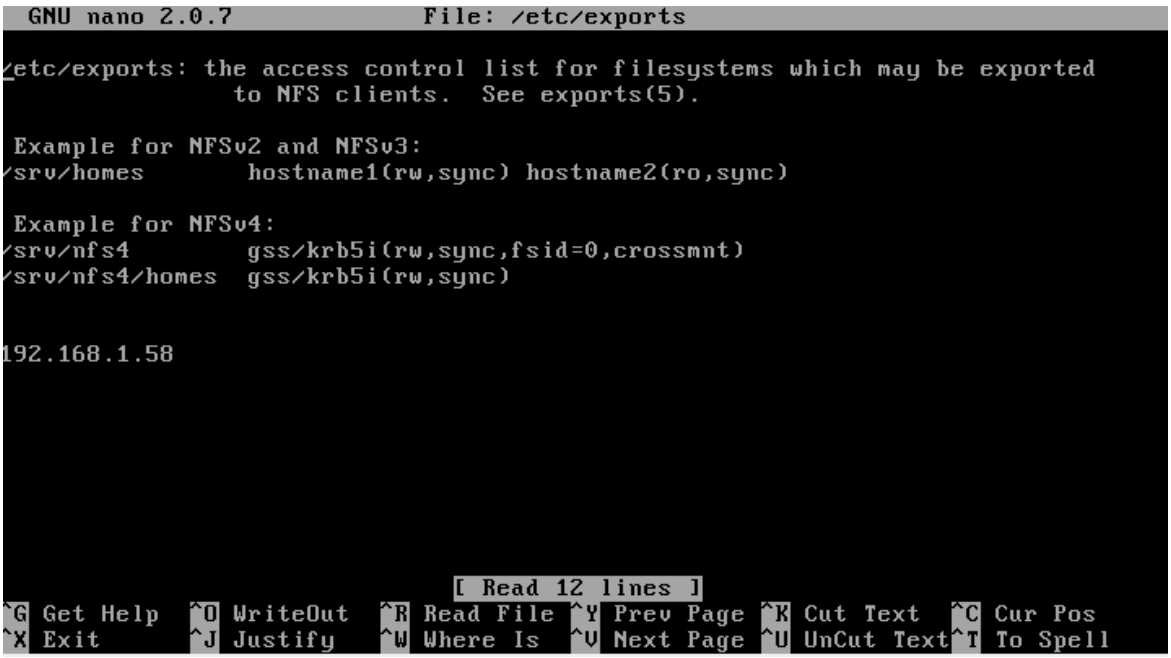
CRITICAL

Che cos'è?
Un sistema remoto configurato con una password predefinita o debole per l'autenticazione VNC consente a un attaccante di accedere in modo non autorizzato. Ciò potrebbe portare all'accesso non autorizzato al desktop remoto o alle risorse del sistema, compromettendo la sicurezza e la riservatezza dei dati.

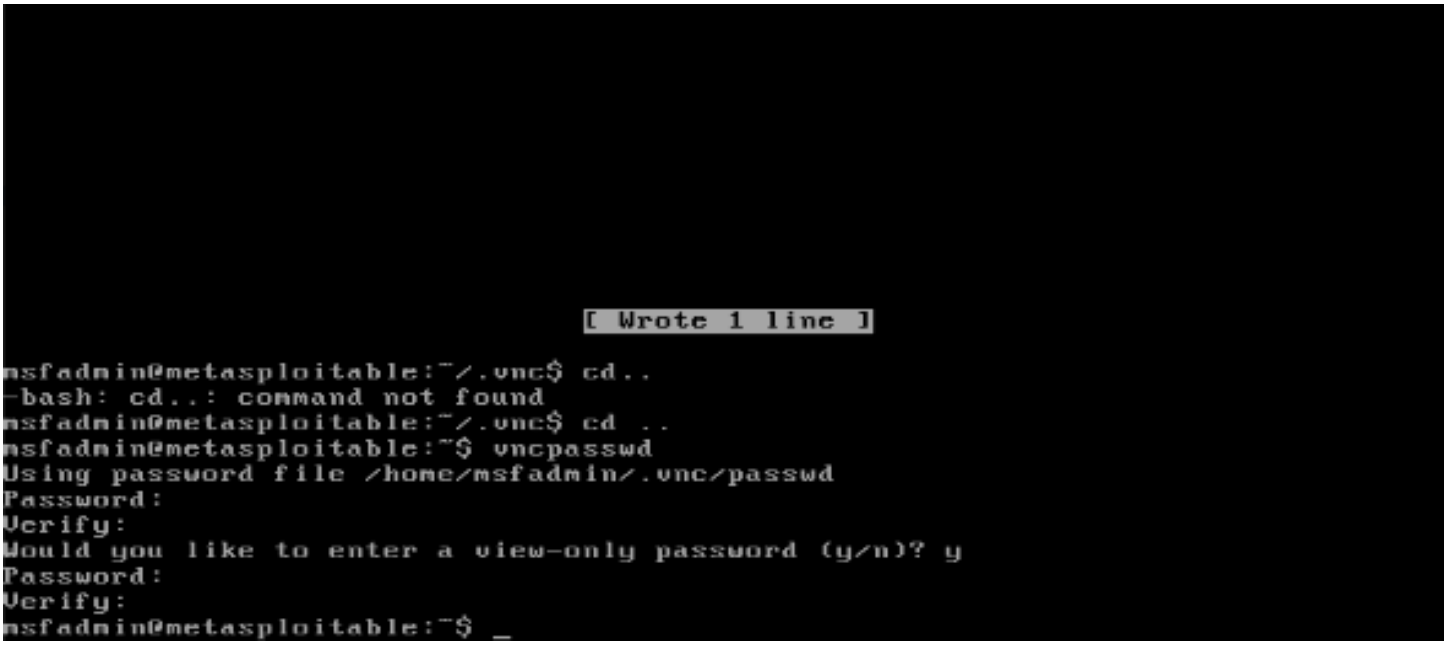
Come si risolve?
Per migliorare la sicurezza del server VNC, è essenziale cambiare immediatamente la password predefinita con una password forte e unica per ogni sistema. Se possibile, utilizzare l'autenticazione basata su chiavi anziché le password, poiché le chiavi SSH offrono un livello superiore di sicurezza. Limitare l'accesso al server VNC solo agli utenti autorizzati e alle reti attendibili utilizzando firewall o altre misure di controllo dell'accesso. Monitorare attentamente gli accessi al server VNC per individuare eventuali tentativi di accesso non autorizzato o attività sospette. Infine, mantenere il server VNC aggiornato con gli ultimi aggiornamenti di sicurezza e patch per ridurre il rischio di sfruttamento di vulnerabilità note.

Risoluzione

- **NFS Exported Share Information Disclosure.**
  Per risolvere il problema, abbiamo impostato un nuovo device che faccia da server connettore con i client esterni e limitato l'accesso a questo solo server cob indirizzo ip 192.168.1.58 nel file di configurazione degli esporti NFS (/etc/exports).



- **VNC Server 'password' Password**
  Per mitigare questa vulnerabilità, ho individuato se fosse presente una password VNC predefinita o debole sul server Metasploitable. Una volta rilevata, l'ho sostituita con una password forte.



Conclusione

Dopo aver fatto questi passaggi ho fatto di nuovo la scansione ed è uscito questo risultato.

In chiusura, il report evidenzia le vulnerabilità individuate su Metasploitable, fornendo una base solida per migliorare la sicurezza complessiva del sistema. Sono disponibili raccomandazioni specifiche per mitigare le vulnerabilità rilevate e proteggere l'ambiente da potenziali minacce. Grazie per l'attenzione dedicata a questo importante processo di valutazione della sicurezza.

Angelo Gravanti