Data: 27 ottobre 2023

Ore: 17:00

Presentatore: antonio spirin

Audienza: Azienda x

Introduzione

Oggi vi presenterò le vulnerabilità di sicurezza rilevate durante una scansione del sistema Unix. Queste vulnerabilità potrebbero essere sfruttate da un utente malintenzionato per accedere al sistema e comprometterne la sicurezza.

Principali vulnerabilità

* Le seguenti sono le principali vulnerabilità rilevate:
* Sistema Unix non aggiornato: il sistema Unix presente non è più supportato dalla casa madre, quindi non possono essere immessi aggiornamenti. Questo è molto pericoloso perché il sistema, essendo antiquato, potrebbe essere facilmente aggirato.
* NFS non configurato correttamente: il servizio NFS è in esecuzione, ma non ci sono limitazioni alle condivisioni NFS. Ciò significa che un utente malintenzionato potrebbe accedere a qualsiasi file sul sistema, leggerlo o scriverci un file malevolo.
* Server VNC con password debole: la password del server VNC è stata rilevata con un semplice attacco brute-force.
* Backdoor abilitata: è stata rilevata una shell che è in ascolto su una porta remota senza che sia richiesta alcuna autenticazione.
* Bug nel generatore di numeri casuali di OpenSSL: è stato rilevato un bug nel generatore di numeri casuali di OpenSSL che potrebbe consentire a un utente malintenzionato di ottenere la chiave privata del server.
* Servizio rlogin abilitato: il servizio rlogin è un protocollo obsoleto che trasmette tutti i dati in chiaro, inclusi nomi utente e password.

Azioni eseguite

* Cambio password del server VNC con una password forte.
* Configurazione del servizio NFS per limitare l'accesso alle condivisioni solo agli IP autorizzati.
* Blocco della backdoor con il firewall.

L'azione di cambio password del server VNC è stata eseguita per mitigare la vulnerabilità di una password debole. La password precedente era stata rilevata con un semplice attacco brute-force, il che significa che un utente malintenzionato avrebbe potuto accedervi facilmente.Per cambiare la password, è stato necessario accedere al sistema da root. Una volta effettuato l'accesso, abbiamo scritto i comandi che potete visualizzare sullo screen :Questo comando ha aperto un prompt per la nuova password. La nuova password è stata impostata secondo le seguenti linee guida:

* Almeno 8 caratteri di lunghezza
* Include caratteri speciali, alfanumerici, maiuscoli e minuscoli
* Non utilizza riferimenti all'azienda o nomi o numeri di telefono comunemente usati da noi

La nuova password è stata quindi salvata.

Motivazione per l'utilizzo di una password forte

L'utilizzo di una password forte è importante per proteggere il server VNC da attacchi. Una password forte è difficile da indovinare o da decifrare, anche con un attacco brute-force.

Conseguenze di una password debole

Una password debole potrebbe consentire a un utente malintenzionato di accedere al server VNC. Una volta che un utente malintenzionato ha accesso al server VNC, potrebbe utilizzare il server per controllare il sistema o per accedere a dati sensibili.

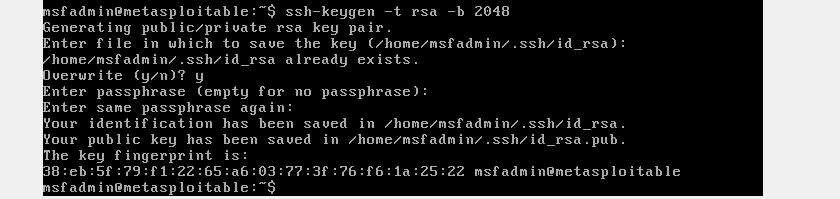
Conclusione

Il cambio password del server VNC è una misura importante per mitigare la vulnerabilità di una password debole. L'utilizzo di una password forte aiuterà a proteggere il server VNC da attacchi.

Altre considerazioni

Oltre al cambio password, è importante implementare altre misure per proteggere il server VNC. per esempio:

* Abilitare l'autenticazione a due fattori



La configurazione predefinita del servizio NFS consente a chiunque di accedere a tutte le condivisioni NFS, indipendentemente dall'indirizzo IP. Ciò significa che un utente malintenzionato potrebbe accedere a file e directory sensibili da qualsiasi luogo sulla rete.

Per mitigare questa vulnerabilità, è stato configurato il servizio NFS per consentire l'accesso solo agli IP aziendali. In questo caso, l'unico IP aziendale considerato è stato l'IP del server Meta.

La configurazione è stata eseguita seguendo i seguenti passaggi:

1. Accedere al server NFS come amministratore.
2. Aprire il file di configurazione di NFS.
3. Agiungere ta le partenetsi() il parametro ip\_aziendale.
4. Salvare il file di configurazione.

Il parametro ()=ip\_aziendale limita l'accesso alle condivisioni NFS agli IP che includono l'indirizzo IP aziendale.

In questo caso, l'indirizzo IP aziendale è 192.168.1.227. Pertanto, la letturra è la modifica dei del nfs è consentità solo a questo indirizzo ip.

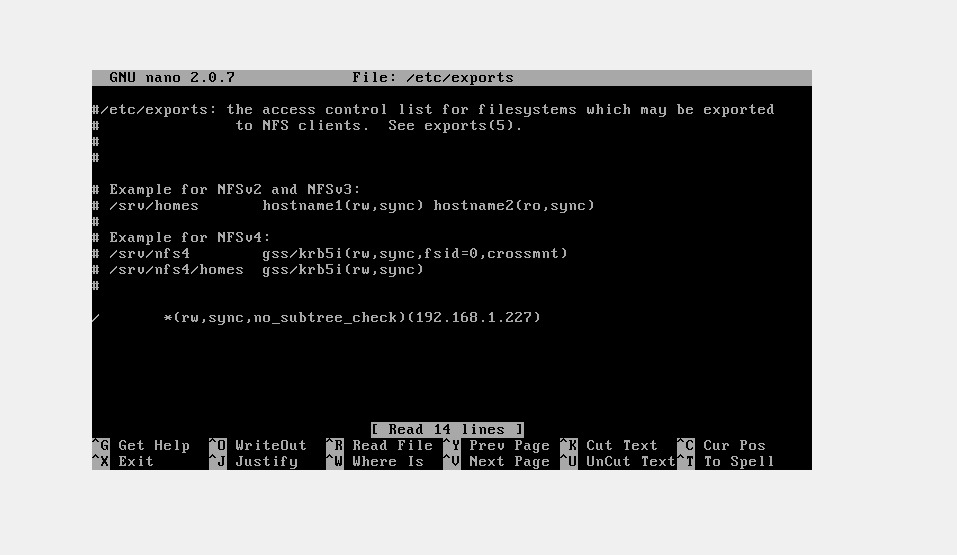
Questa configurazione limita l'accesso alle condivisioni NFS solo al server Meta.

Una considerazione aggiuntiva per la configurazione sicura del servizio NFS è l'utilizzo della cifratura NFS

Conclusione

La configurazione del servizio NFS per limitare l'accesso alle condivisioni NFS solo agli IP autorizzati è una misura importante per mitigare le vulnerabilità di NFS.

Questa configurazione aiuta a proteggere i dati sensibili da accessi non autorizzati. Si consglia di integrare una cifratura per l NFS



Una backdoor è una vulnerabilità che consente a un utente malintenzionato di accedere a un sistema senza autenticazione. In questo caso, la backdoor era in ascolto sulla porta 1524.

Per mitigare questa vulnerabilità, è stato configurato il firewall di Meta per bloccare tutte le connessioni in entrata sulla porta 1524.

La configurazione è stata eseguita seguendo i seguenti passaggi:

1Accedere al firewall di Meta come amministratore.

2Aprire la configurazione del firewall.

3Creare una nuova regola di firewall per bloccare le connessioni in entrata sulla porta 1524.

4Salvare la configurazione del firewall.

La nuova regola di firewall ha la seguente configurazione:

* Tipo di regola: Blocca
* Protocollo: TCP
* Porta: 1524
* Direzione: Ingresso
* Azione: Nega

Questa regola blocca tutte le connessioni in entrata sulla porta 1524, indipendentemente dall'indirizzo IP.

Conclusione

Il blocco della backdoor con il firewall di Meta è una misura importante per mitigare la vulnerabilità della backdoor.

Questa configurazione aiuta a proteggere il sistema da accessi non autorizzati.

Altre considerazioni

Oltre alla configurazione del firewall, è importante implementare altre misure per proteggere il sistema da backdoor. Queste misure includono:

* Installare gli aggiornamenti di sicurezza il prima possibile.
* Utilizzare un sistema di rilevamento e risposta alle intrusioni (IDS/IPS).
* Formare gli utenti sulle best practice di sicurezza.

