Report vulnerabilità del client meta

La scansione fatta con Nessus sul target Meta ha prodotto i seguenti risultati:

- **Vulnerabilità critiche: 7**
- **Vulnerabilità alte: 4**
- **Vulnerabilità medie: 12**
- **Vulnerabilità basse: 4**
- **Informazioni non protette: 105**

Parto con l' anlizzare le vulnerabilità con maggiore minaccia fino ad arrivare a quelle la cui minaccia è trascurabile, di seguito le descriverò e riporterò una possibile soluzione per queste. **Ho inserito anche le vulnerabilità di livello critico che avevo già riportato, non avendo vulnerabilità di livello alto dopo quelle**

Vulnerabilità critiche:

51988 - Bind Shell Backdoor Detection:

- Descrizione: la shell di meta è in ascolto su una porta senza nessuna autenticazione richiesta. Un attaccante potrebbe connettersi alla porta e potrebbe mandare comandi direttamente alla shell.
- Soluzione: Verificare se meta fosse stato compromesso, reinstallare il sistema se necessario.
- Rischio: Critico
- Plugin Output: tcp/1524/wild_shell

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness:

- Descrizione: Le chiavi SSH di meta sono state generate su una versione Debian che ha un bug per qui il generatore di numeri crea numeri che sono prevedibili, questo fa si che per un attaccante sia più facile fare un attacco brute force sulla chiave crittografata.
- Soluzione: Considerare tutto il materiale crittografato del host meta compromesso. In particolare tutte le chiavi SSH, SSL e OpenVPN dovranno essere rigenerate con una crittografia migliore.
- Rischio: Critico
- Plugin Output: tcp/22/ssh

32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check):

- Descrizione: Il certificato x509 del server SSL di meta è staro generato su una versione di Debian che ha un bug nella generazione delle chiavi di crittografia.
- Soulzione: Anche per questa vulneraniltà la soluzione è quella di ri-crittografare tutto il materiale del SSH, SSL e OpenVPN.
- Rischio: Critico

- Plug-in output= tcp/5432/postgresql

11356 - NFS Exported Share Information Disclosure:

- Descrizione: Almeno un NFS può essere approcciato scannerizzando meta. Un attaccante potrebbe essere capace di leggere o scrivere i file di meta.
- Soluzione: Configurare l' NFS in modo che vi possano accedere solo host autorizzati.
- Rischio: Critico
- Plugin Output: udp/2049/rpc-nfs

Vulnerabilità Alto:

136769 - ISC BIND Service Downgrade / Reflected DoS:

- Descrizione: La versione di ISC BIND 9 presente su meta e affetto da downgrade delle prestazioni e vulnerabilità al reflected DoS. Questo è dovuto al fatto che BIND DNS non limita sufficientemente il numero di richieste che dovrebbero essere prese mentre si sta processando l'elaborazione di una risposta di rinvio. Un attaccante potrebbe usare questa vulnerabilità per causare il declino del servizio del server o per usare quest' ultimo come un riflettore in un attacco 'Reflected DoS'.
- Soluzione: Implementare la versione aggiornate di ISC BIND.
- Rischio: Alto
- Plug-in Output: udp/53/dns

42256 - NFS Shares World Readable:

- Descrizione: Il server NFS sta esponendo una o più condivisioni senza restringere l'accesso(con hostname,IP o IP range).
- Soluzione: Inserire restrizioni appropriate su tutte le condivisioni NFS
- Rischio: Alto
- Plug-in Output: tcp/2049/rpc-nfs

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32):

- Descrizione: Meta supporta l'uso di crittografie SSL che offrono una crittografia di livello medio. Nessus valuta livello medio come qualsiasi crittografia che utilizzi lunghezze di chiave di almeno 64 bit e inferiori a 112 bit, oppure che utilizza la suite di crittografia 3DES.Si noti che è notevolmente più semplice aggirare la crittografia di medio livello se l'attaccante si trova sulla stessa rete fisica.
- Soluzione: Riconfigurare l'applicazione interessata, se possibile, per evitare l'uso di cifrature di livello medio.
- Rischio: Alto
- Plugin Output: tcp/5432/postgresql