# W12D4 - Pratica - parte due - remediation

Giacomo di Giacinto

EPICODE | W12D4 - Pratica PDF | Esercizio — Traccia e requisiti

**Traccia:**

Effettuare una scansione completa sul target Metasploitable.

Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità **critiche** e provate ad **implementare delle azioni di rimedio**.

N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili.
Vi consigliamo tuttavia di utilizzare magari questo approccio **per non più di una vulnerabilità**.

Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

Ai fini della soluzione, abbiamo scelto le vulnerabilità in giallo nella figura in slide 3.

**Consegna:**

1. Scansione iniziale dove si vede il grafico con tutte le vulnerabilità e le vulnerabilità da risolvere (tecnico, già riassunto) - **ScansioneInizio.pdf**
2. **Screenshot e spiegazione dei passaggi della remediation - RemediationMeta.pdf**
3. Scansione dopo le modifiche che evidenzia la risoluzione dei problemi/vulnerabilità (il grafico che mostra tutte le vulnerabilità) - **ScansioneFine.pdf**

   **Oppure un report unico, a vostra scelta. Penso sia più comodo farne tre comunque.**

**Nota: i report possono essere lasciati in inglese, senza problemi.**

Se risolvete le 4 vulnerabilità, potete risolverne una quinta (a scelta), ad esempio con una regola di firewall


Di seguito saranno riportate le criticità oggetto di studio e la sua remediation.

| | | | | |
|---|---|---|---|---|
| CRITICAL | 10.0* | 5.9 | 11356 | NFS Exported Share Information Disclosure |


Sinossi

È possibile accedere alle condivisioni NFS sull'host remoto.

Descrizione

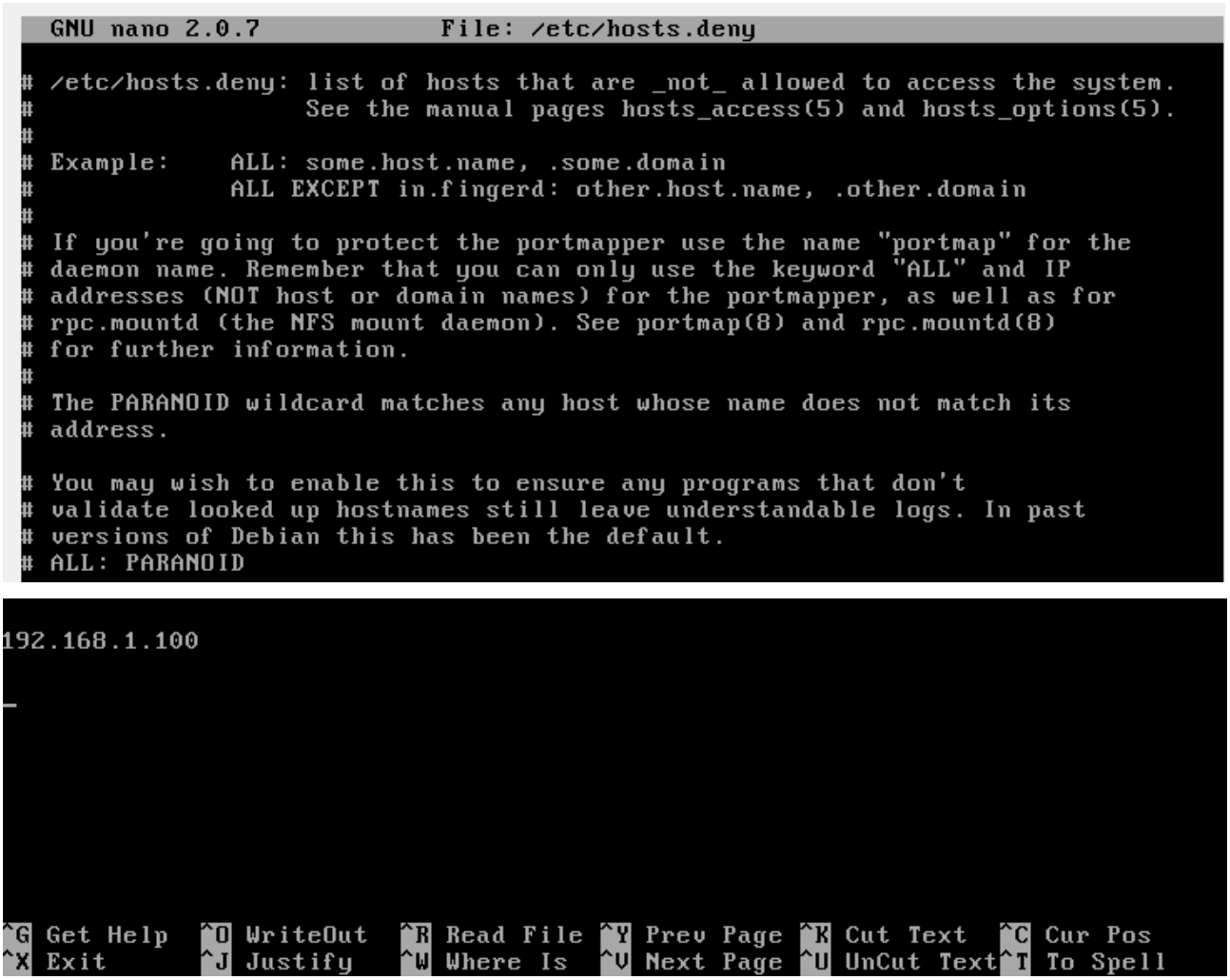
Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un attaccante potrebbe essere in grado di sfruttare ciò per leggere (e eventualmente scrivere) file sull'host remoto.

Soluzione

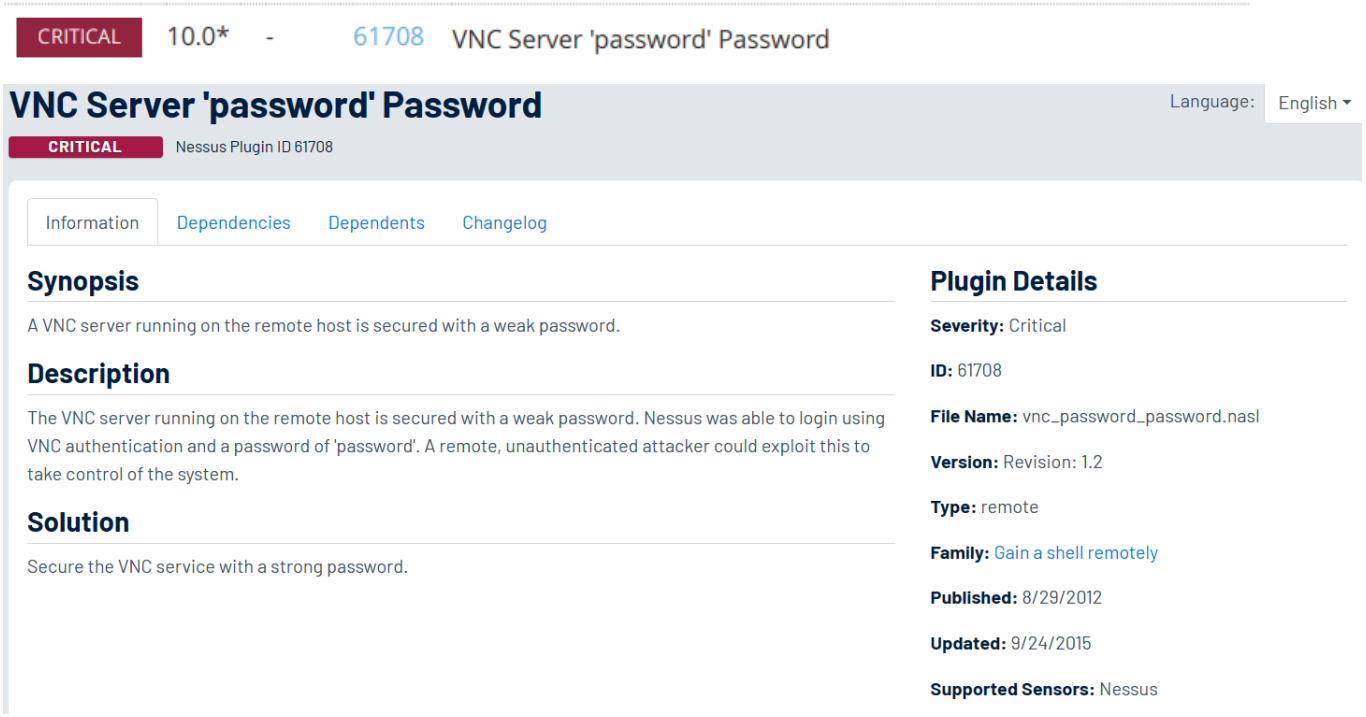
Configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.

Remediation

Attraverso il comando da shell sudo nano /etc/hosts.deny posso negare l’accesso alle cartelle condivise. Modifico il file inserendo l’IP di kali in modo da negare l’accesso e porre rimedio alla criticità


GNU nano 2.0.7 File: /etc/hosts.deny
# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
# See the manual pages hosts_access(5) and hosts_options(5).
#
# Example: ALL: some.host.name, .some.domain
# ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you're going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper, as well as for
# rpc.mountd (the NFS mount daemon). See portmap(8) and rpc.mountd(8)
# for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID


192.168.1.100
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell




Sinossi

Un server VNC in esecuzione sull'host remoto è protetto con una password debole.

Descrizione

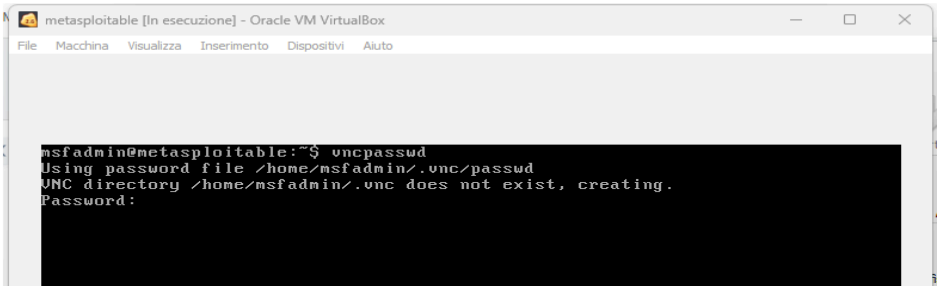
Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è stato in grado di effettuare il login utilizzando l'autenticazione VNC e una password 'password'. Un attaccante remoto e non autenticato potrebbe sfruttare ciò per prendere il controllo del sistema.

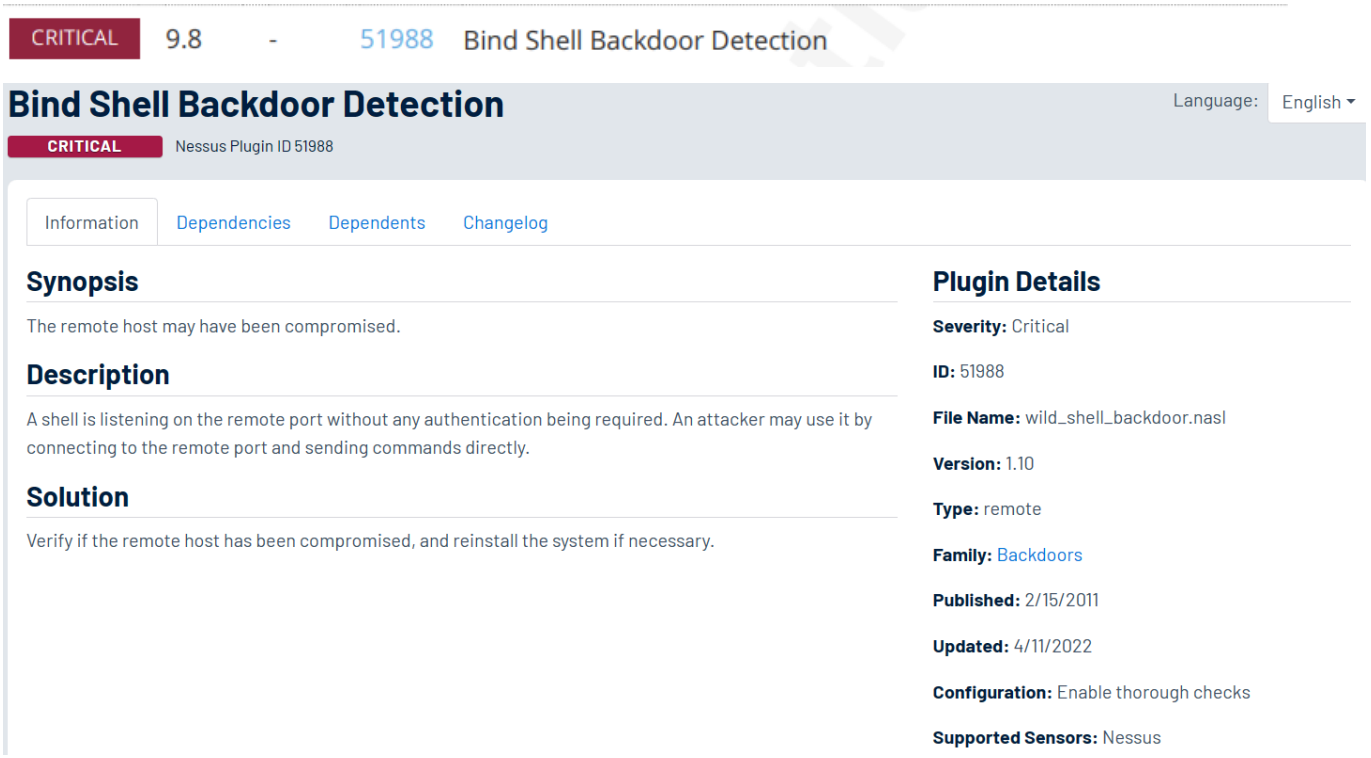
Soluzione

Proteggi il servizio VNC con una password forte.

Remediation:

Dovrà essere inserita una password al servizio VNC con il comando vncpasswd






Sinossi

L'host remoto potrebbe essere stato compromesso.

Descrizione

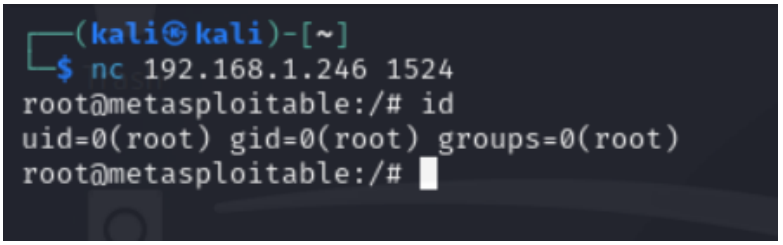
Una shell è in ascolto sulla porta remota senza richiedere alcuna autenticazione. Un attaccante potrebbe utilizzarla connettendosi alla porta remota e inviando comandi direttamente.

Soluzione

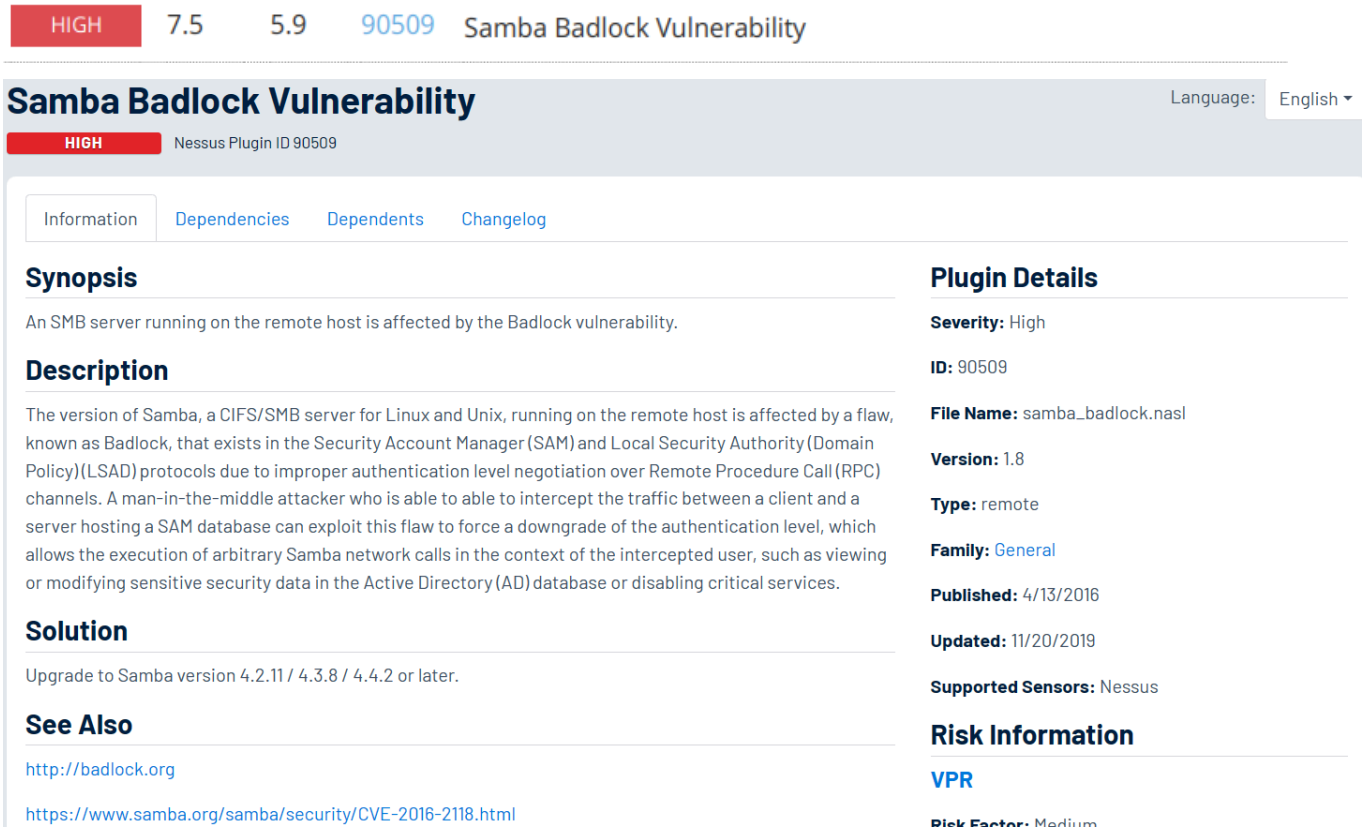
Verificare se l'host remoto è stato compromesso e reinstallare il sistema se necessario.

Remediation:

Nessus ci segnala che sulla porta 1524 c'è una backdoor attiva.




Creando una regola ad hoc sul firewall possiamo disporre che nessun utente posso accedere alla porta, oppure possiamo selezionare gli utenti autorizzati all'accesso.




Sinossi:
Un server SMB in esecuzione sull'host remoto è affetto dalla vulnerabilità Badlock.

Descrizione

La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è affetta da una falla, nota come Badlock, che esiste nei protocolli Security Account Manager (SAM) e Local Security Authority (Domain Policy) (LSAD) a causa di una negoziazione del livello di autenticazione non corretta su canali di chiamata di procedura remota (RPC). Un attaccante man-in-the-middle che è in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questa falla per forzare un declassamento del livello di autenticazione, il che consente l'esecuzione di chiamate di rete Samba arbitrarie nel contesto dell'utente intercettato, come la visualizzazione o la modifica di dati di sicurezza sensibili nel database Active Directory (AD) o la disabilitazione di servizi critici.

Soluzione

Aggiornare alla versione di Samba 4.2.11 / 4.3.8 / 4.4.2 o successiva.

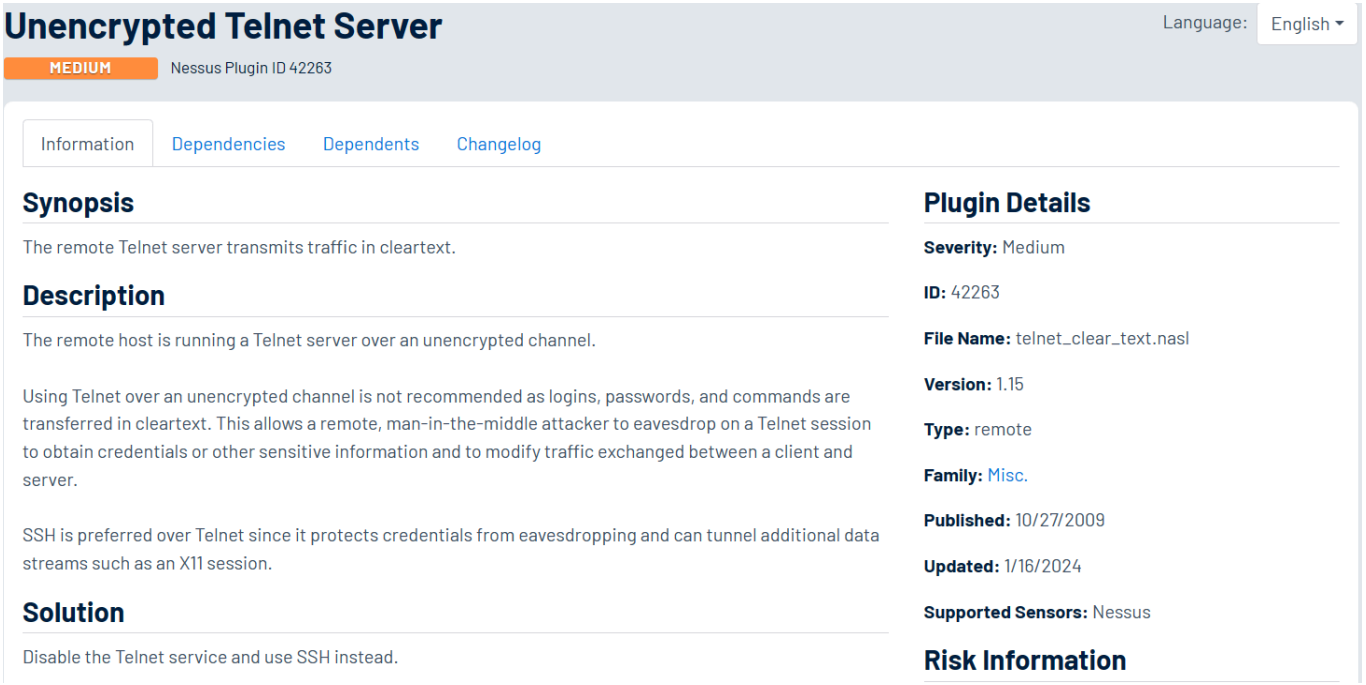
Vedi anche

http://badlock.org

https://www.samba.org/samba/security/CVE-2016-2118.html

Remediation:

Installare come da soluzione una versione aggiornata della versione di Samba.


Sommario

Il server Telnet remoto trasmette il traffico in testo non criptato.

Descrizione

L'host remoto sta eseguendo un server Telnet su un canale non crittografato.

L'utilizzo di Telnet su un canale non crittografato non è consigliato poiché i login, le password e i comandi vengono trasferiti in chiaro. Ciò consente a un attaccante remoto man-in-the-middle di intercettare una sessione Telnet per ottenere credenziali o altre informazioni sensibili e per modificare il traffico scambiato tra un client e un server.

SSH è preferibile rispetto a Telnet poiché protegge le credenziali dall'intercettazione e può tunnelare flussi di dati aggiuntivi come una sessione X11.

Soluzione

Disabilitare il servizio Telnet e utilizzare invece SSH.

Remediation:

L’azienda dovrà abbandonare l’utilizzo di telnet ed, al suo posto, utilizzare SSH