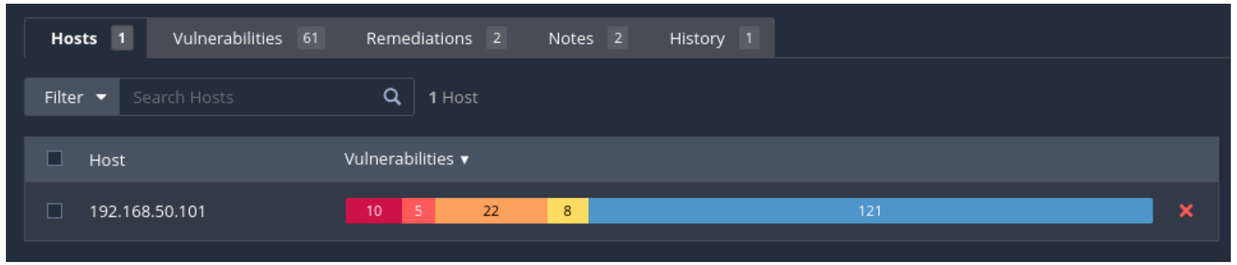
S5L5

Elaborato da: Antonio Perna.



Panoramica

Il progetto di oggi ci chiedeva di fare una scansione completa sulla macchina di metaspoitable da nessus, vedere le vulnerabilità e dare delle soluzioni per correggerle.

Apache Tomcat AJP Connector Request Injection (Ghostcat)

Bind Shell Backdoor Detection

SSL Version 2 and 3 Protocol Detection

VNC Server 'password' Password

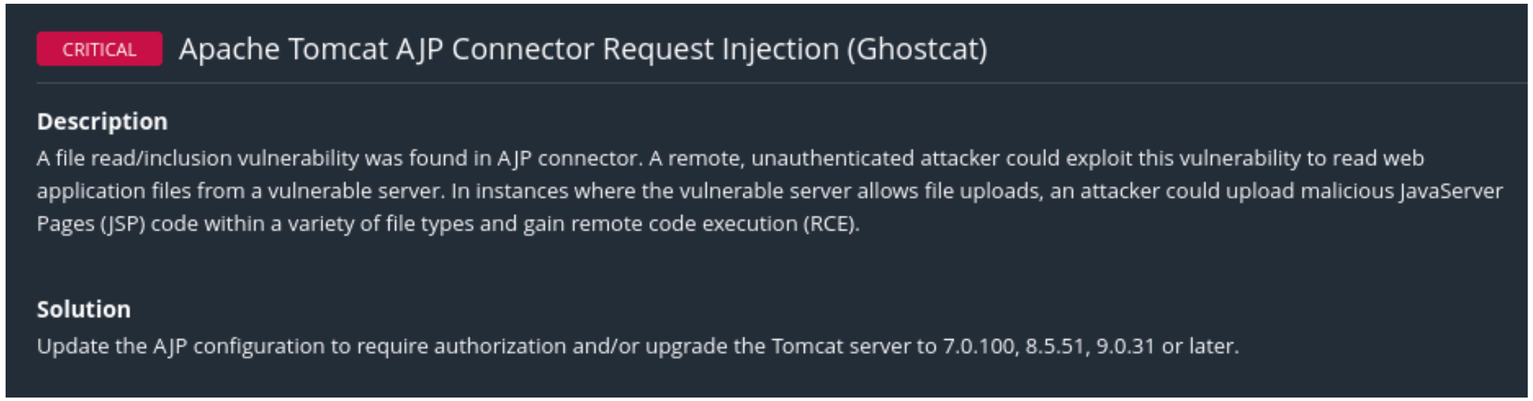
Unix Operating System Unsupported Version Detection

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

NFS Exported Share Information Disclosure

Indice

Apache Tomcat AJP Connector Request Injection (Ghostcat)



Descrizione

Questa è una vulnerabilità critica che consente agli attaccanti di eseguire codice arbitrario sul server utilizzando una richiesta appositamente progettata.

Soluzione

- Aggiorna Apache Tomcat alla versione più recente che risolve questa vulnerabilità.
- Configura correttamente le impostazioni di sicurezza di Apache Tomcat per mitigare questo tipo di attacco.

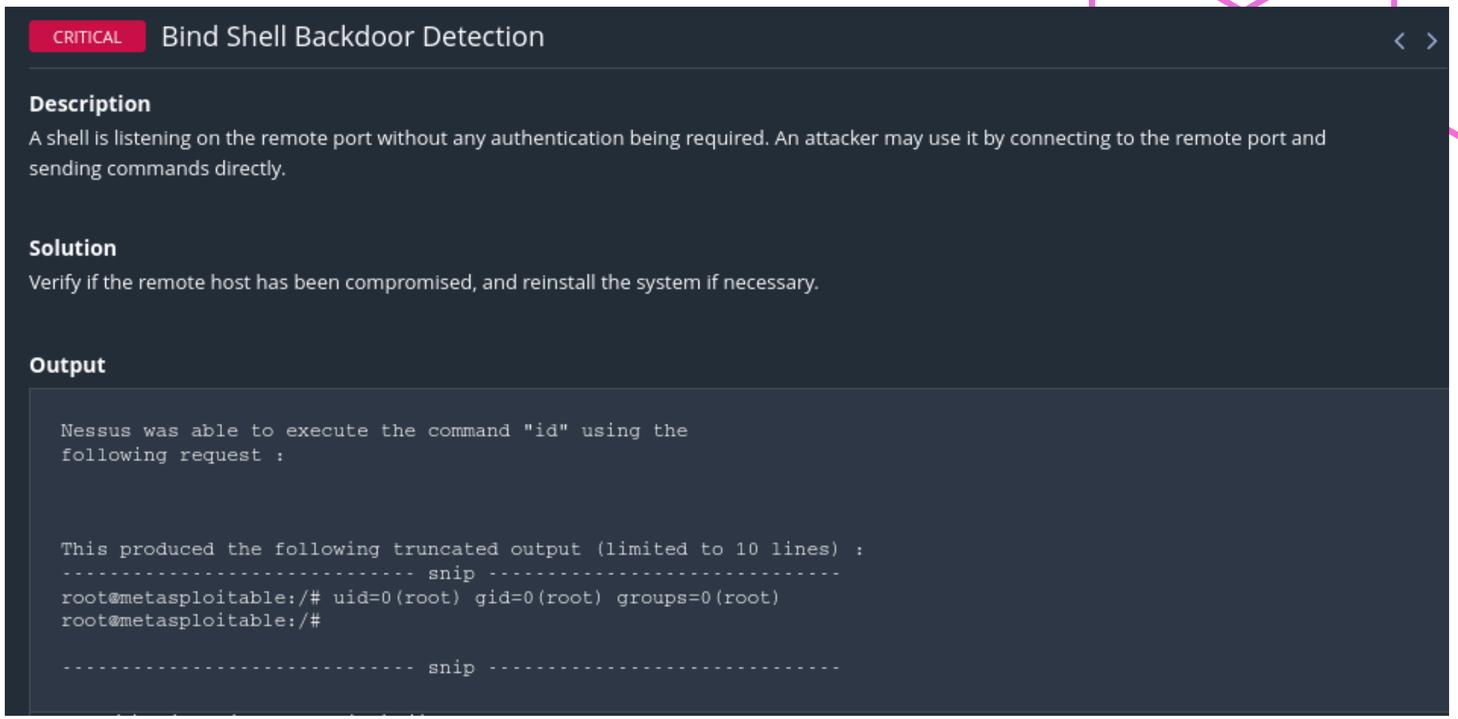
Bind Shell Backdoor Detection

Descrizione

Questa vulnerabilità indica la presenza di un backdoor nel sistema che potrebbe essere utilizzato per ottenere accesso non autorizzato.

Soluzione

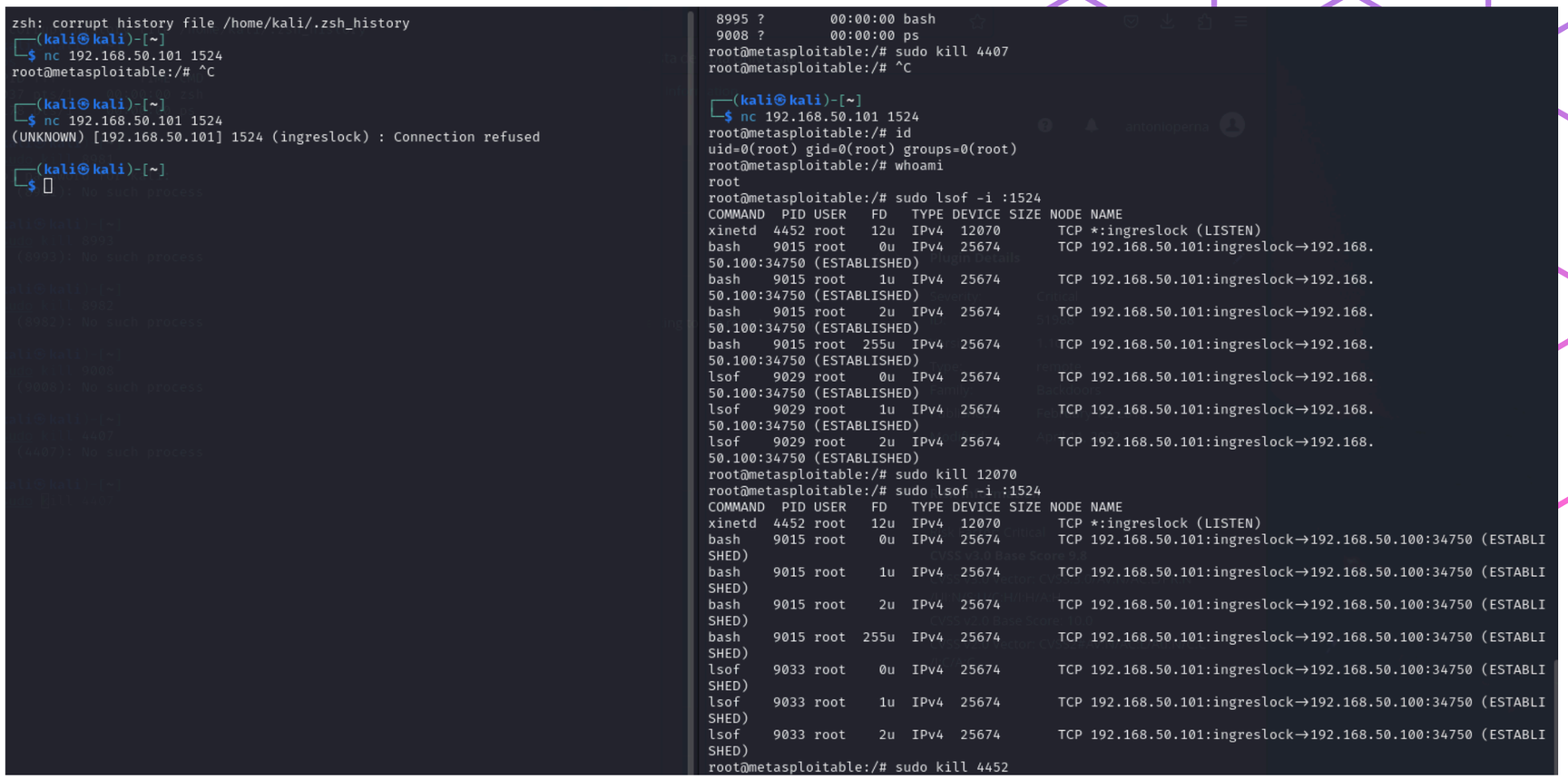
- Indaga sulla presenza del backdoor e rimuovilo dal sistema.
- Analizza i file di log e l'attività di rete per identificare come è stato introdotto il backdoor.



Bind Shell Backdoor Detection

Soluzione

- Indaga sulla presenza del backdoor e rimuovilo dal sistema.
- Analizza i file di log e l'attività di rete per identificare come è stato introdotto il backdoor.



Soluzione

Andiamo ad accedere alla root di meta con il comando “nc ip porta” poi con il comando sudo lsof -i :1524 vediamo il pid e con kill pid togliamo l’accesso

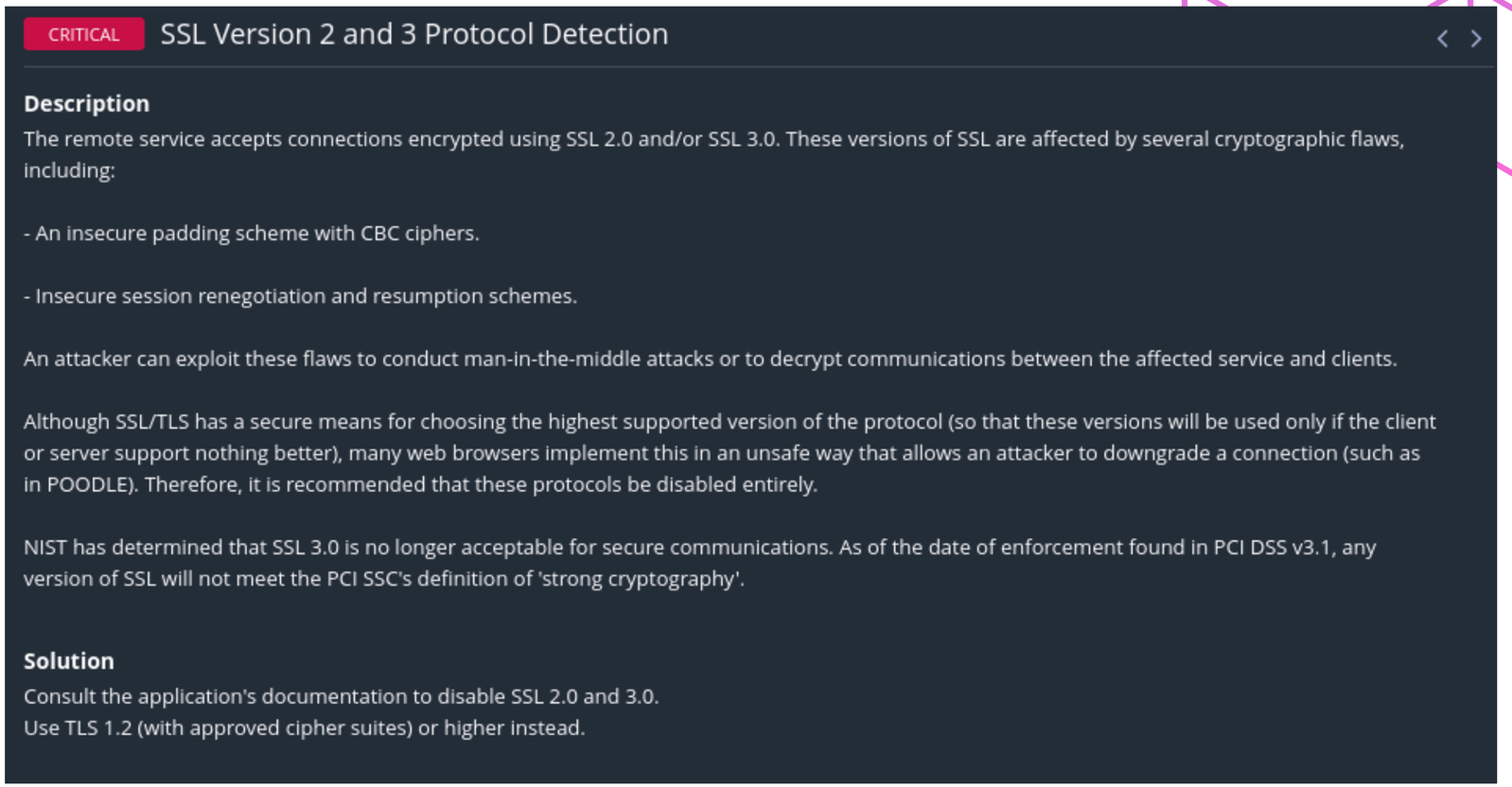
SSL Version 2 and 3 Protocol Detection

Descrizione

Indica la presenza di supporto per i protocolli SSL versione 2 e 3, che sono noti per avere vulnerabilità di sicurezza serie.

Soluzione

- Disabilita il supporto per SSL versione 2 e 3 e utilizza solo TLS.
- Aggiorna i servizi e le librerie SSL/TLS a versioni più recenti che non supportano SSL v2 e v3.



Unix Operating System Unsupported Version Detection

1

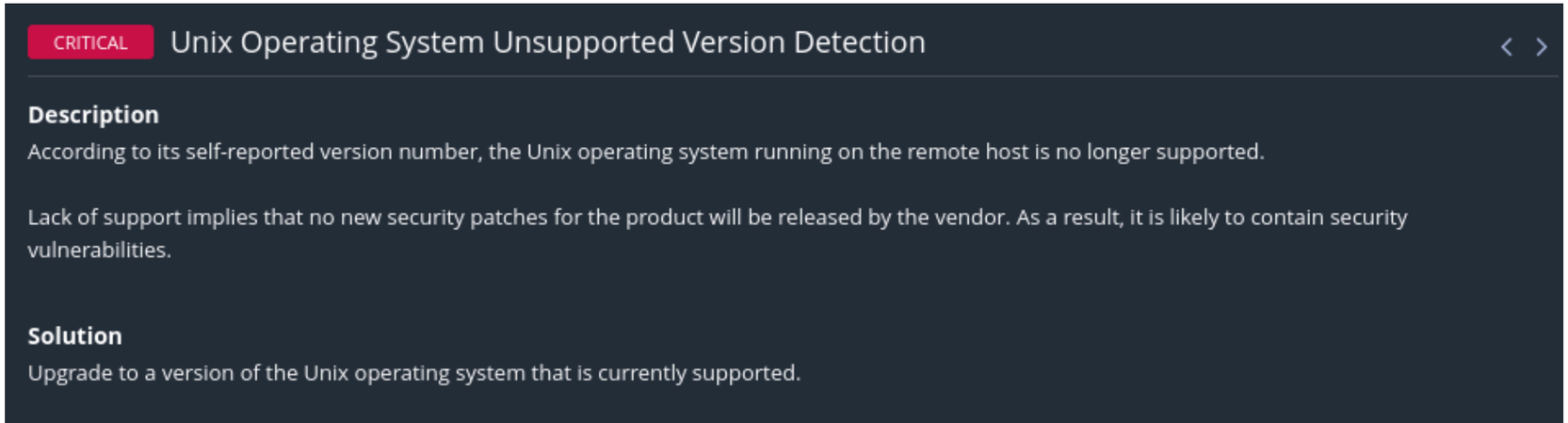
Descrizione

Questa vulnerabilità segnala l'uso di una versione non supportata di un sistema operativo Unix, che potrebbe non ricevere più aggiornamenti di sicurezza.

2

Soluzione

- Aggiorna il sistema operativo Unix a una versione supportata che riceva ancora aggiornamenti di sicurezza.



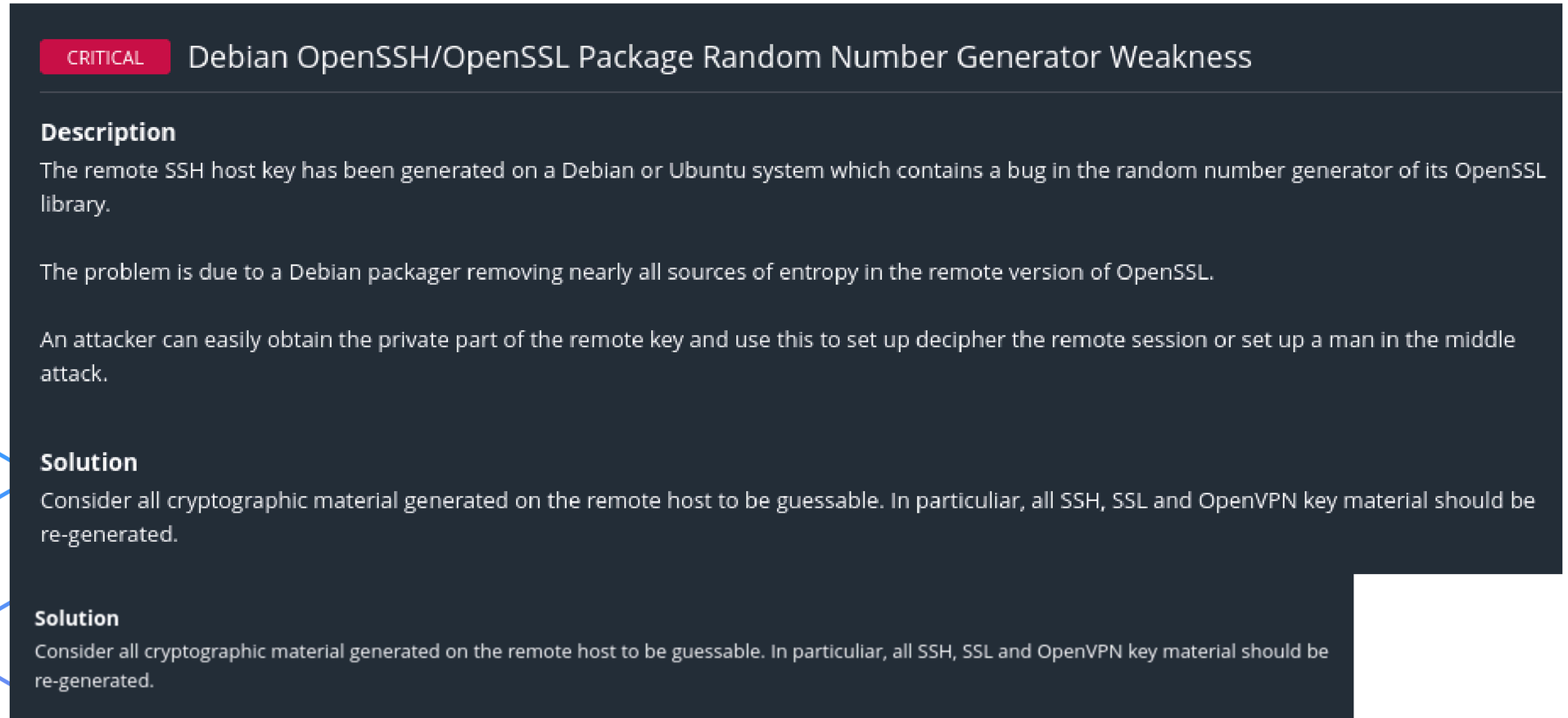
Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

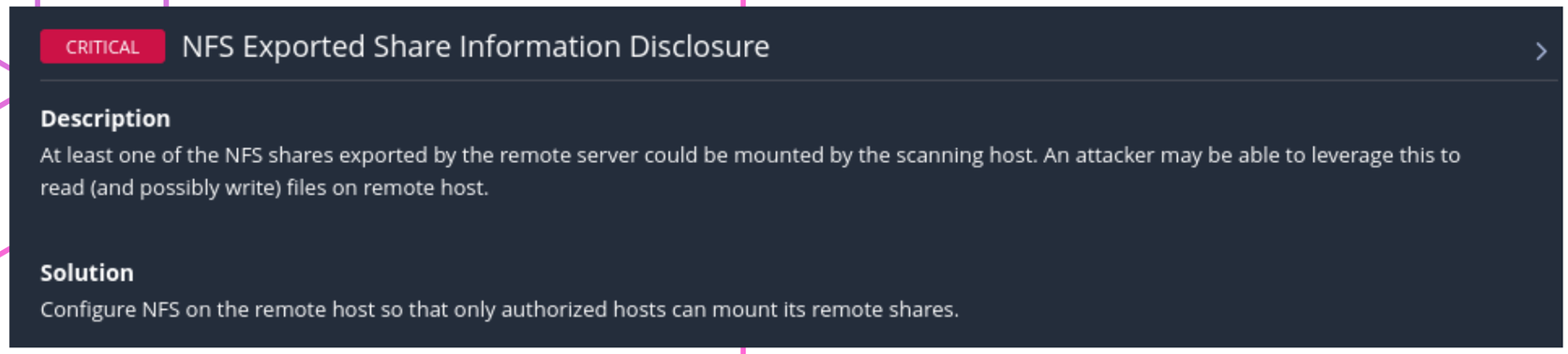
Descrizione

Queste sono vulnerabilità che coinvolgono la generazione casuale di numeri nei pacchetti di OpenSSH/OpenSSL su sistemi Debian. Potrebbero consentire ad un attaccante di prevedere i numeri casuali utilizzati per crittografare le comunicazioni.

Soluzione

- Aggiorna i pacchetti OpenSSH e OpenSSL a versioni che risolvono questa vulnerabilità.
- Monitora l'attività del sistema per eventuali segni di compromissione.





NFS Exported Share Information Disclosure

Descrizione

Indica una vulnerabilità che consente agli attaccanti di accedere a informazioni sensibili da condivisioni NFS esposte.

Soluzione

- Limita l'accesso alle condivisioni NFS solo ai client autorizzati.
- Imposta correttamente le autorizzazioni sui file e sulle cartelle esportate via NFS per proteggere i dati sensibili.

NFS Exported Share Information Disclosure

Soluzione

- Limita l'accesso alle condivisioni NFS solo ai client autorizzati.
- Imposta correttamente le autorizzazioni sui file e sulle cartelle esportate via NFS per proteggere i dati sensibili.

```
msfadmin@metasploitable:~$ /etc/exports
-bash: /etc/exports: Permission denied
msfadmin@metasploitable:~$ /etc/hosts.allow
-bash: /etc/hosts.allow: Permission denied
msfadmin@metasploitable:~$ /etc/hosts.deny
-bash: /etc/hosts.deny: Permission denied
```

Soluzione

Per limitare l’accesso ai file andiamo ad inserire i comandi “/etc/exports”, “/etc/hosts.allow” e “/etc/hosts.deny” e vediamo che toglie tutti i permessi

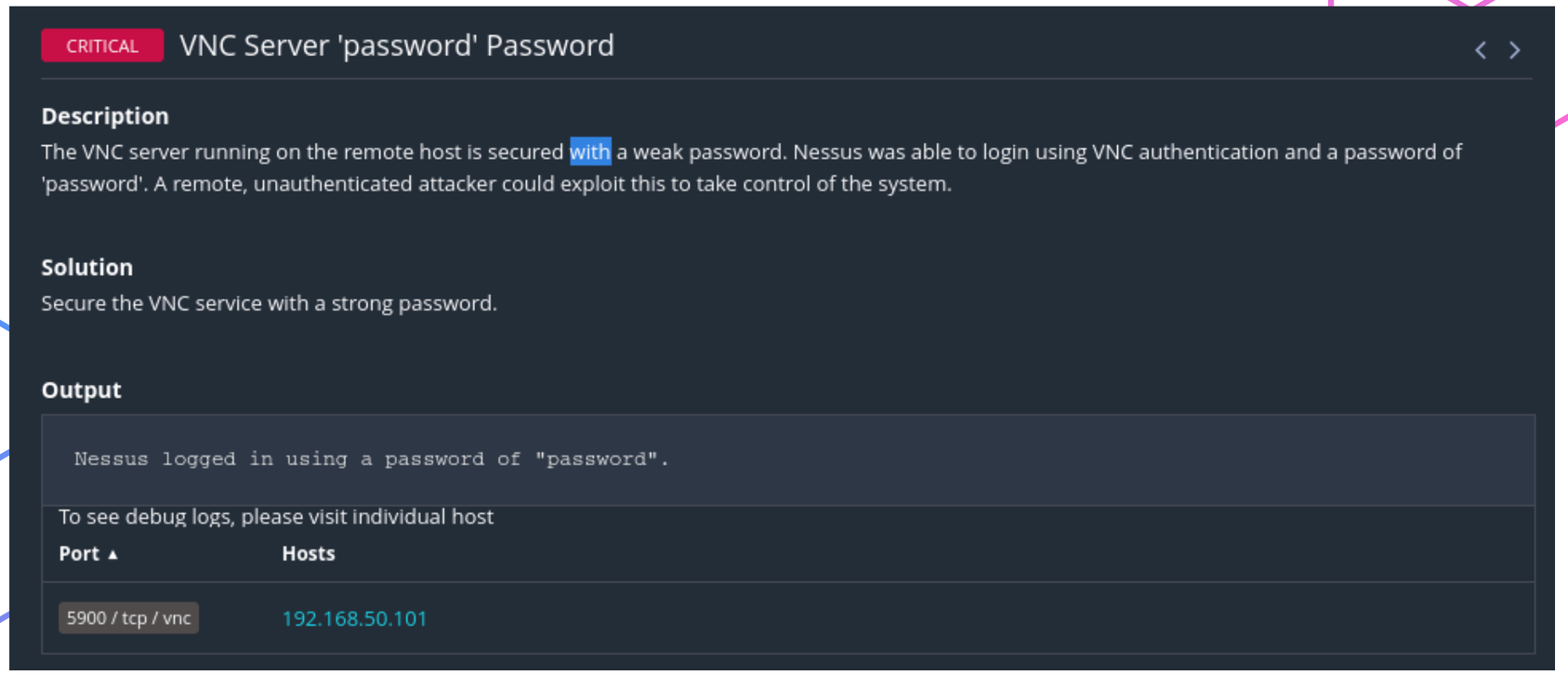
VNC Server 'password' Password

Descrizione

Indica la presenza di password predefinite o facilmente prevedibili per un server VNC, che potrebbero essere sfruttate per ottenere accesso non autorizzato.

Soluzione

- Cambia la password predefinita del server VNC.
- Se possibile, usa meccanismi di autenticazione più robusti, come l'uso di chiavi SSH anziché password.



VNC Server 'password' Password

Soluzione

- Cambia la password predefinita del server VNC.
- Se possibile, usa meccanismi di autenticazione più robusti, come l'uso di chiavi SSH anziché password.

```
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
VNC directory /home/msfadmin/.vnc does not exist, creating.
Password:
Warning: password truncated to the length of 8.
Verify:
Passwords do not match. Please try again.

Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
msfadmin@metasploitable:~$
```

Soluzione

Su metaspoitable, per risolvere questa vulnerabilità, andiamo a digitare il comando “vncpasswd” che ci fa reimpostare la password e risolviamo.