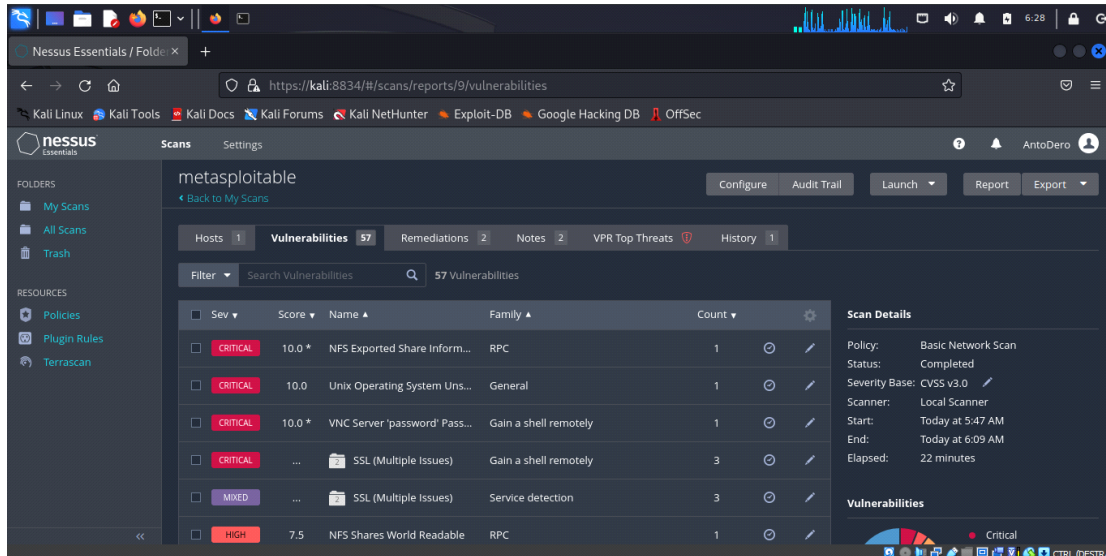


Attraverso Nessus ho effettuato una scansione completa sul target Metasploitable (192.168.50.101). Inizialmente ho trovato 4 vulnerabilità critiche.



Ho implementato delle azioni di rimedio.

1) NFS Exported Share Information Disclosure:

Descrizione

Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere file su host remoto.

Soluzione

Ho utilizzato il comando: `sudo nano /etc/exports` per poter aprire e modificare il file

```
GNU nano 2.0.7      File: /etc/exports

# /etc/exports: the access control list for filesystems which may be exported
#                to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4       gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,sync)
#
/192.168.50.100(rw,sync,no_root_squash,no_subtree_check)

[ Read 12 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^V Prev Page ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^U Next Page ^U UnCut Text ^T To Spell
```

2)VNC 'password' Password:

Descrizione

Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è stato in grado di accedere utilizzando l'autenticazione VNC e una password di "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttarlo per assumere il controllo del sistema.

Soluzione

```
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home/msfadmin#
```

Ho così protetto il servizio VNC con una password sicura.

3)Unix Operating System Unsupported version detection:

Descrizione

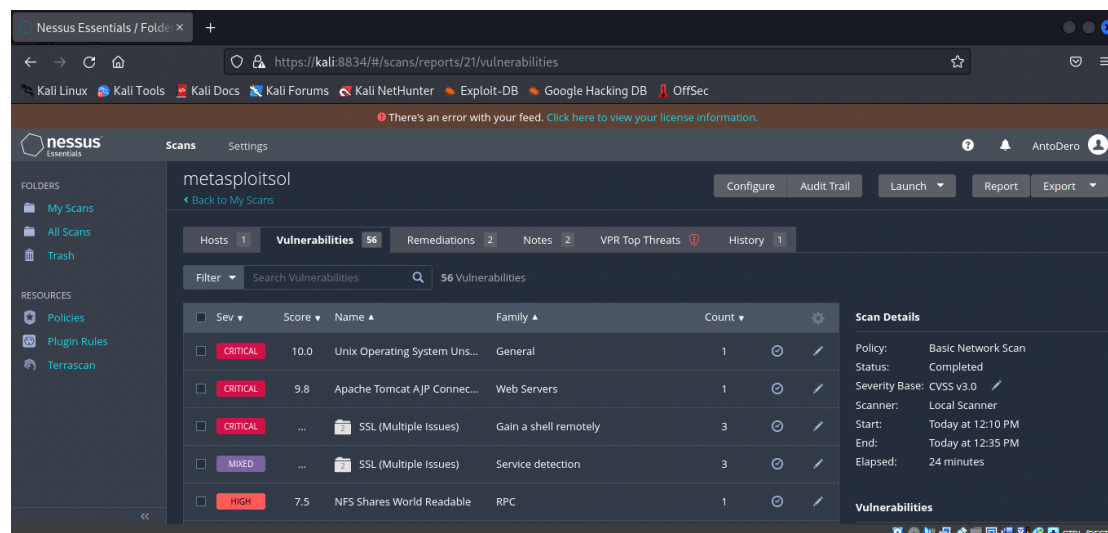
In base al numero di versione auto-riportato, il sistema operativo Unix in esecuzione sull'host remoto non è più supportato.

La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto. Di conseguenza, è probabile che contenga vulnerabilità di sicurezza.

Soluzione

Aggiorna a una versione del sistema operativo Unix attualmente supportata.

Infine per dimostrare l'efficacia delle azioni di rimedio, ho eseguito nuovamente la scansione sul target per poterla confrontare con quella precedentemente ottenuta.



Come si può vedere le due criticità precedentemente presenti non ci sono più, ora però ho trovato un'altra vulnerabilità critica per la quale per mancanza di tempo non sono riuscito ad effettuare delle azioni di rimedio:

<input type="checkbox"/>	CRITICAL	9.8	Apache Tomcat AJP Connector Request Inje...	Web Servers	1
--------------------------	----------	-----	---	-------------	---

Descrizione

È stata rilevata una vulnerabilità di lettura/inclusione di file nel connettore AJP. Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa vulnerabilità per leggere i file dell'applicazione Web da un server vulnerabile. Nei casi in cui il server vulnerabile consente il caricamento di file, un utente malintenzionato potrebbe caricare codice JSP (JavaServer Pages) dannoso all'interno di una varietà di tipi di file e ottenere l'esecuzione di codice remoto (RCE).

Soluzione

Aggiorna la configurazione AJP per richiedere l'autorizzazione e/o aggiornare il server Tomcat a 7.0.100, 8.5.51, 9.0.31 o versioni successive.