Settimana 5 - Esercizio 5

Alessio Golfetto 12/01/2023

Traccia

Effettuare una scansione completa sul target Metasploitable.

Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche / high 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.

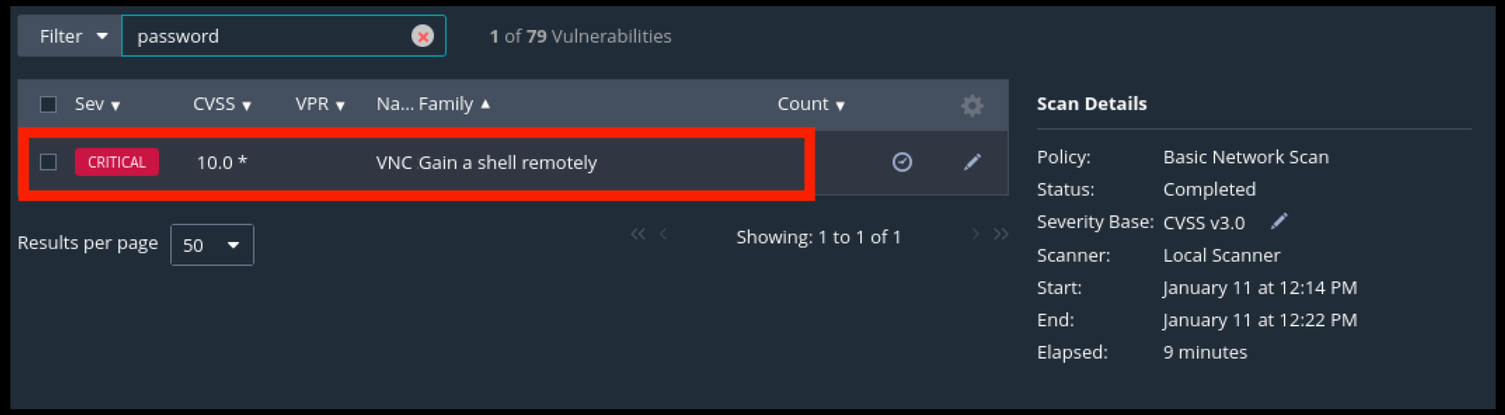
Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

Vulnerabilità 1

VCN Server “password” Password

Un server VNC (Virtual Network Computing) è un software che consente la condivisione del desktop di un computer o di un server tramite la rete. VNC è un protocollo che permette a un utente di controllare un sistema remotamente visualizzando il desktop e interagendo con esso attraverso un altro host.

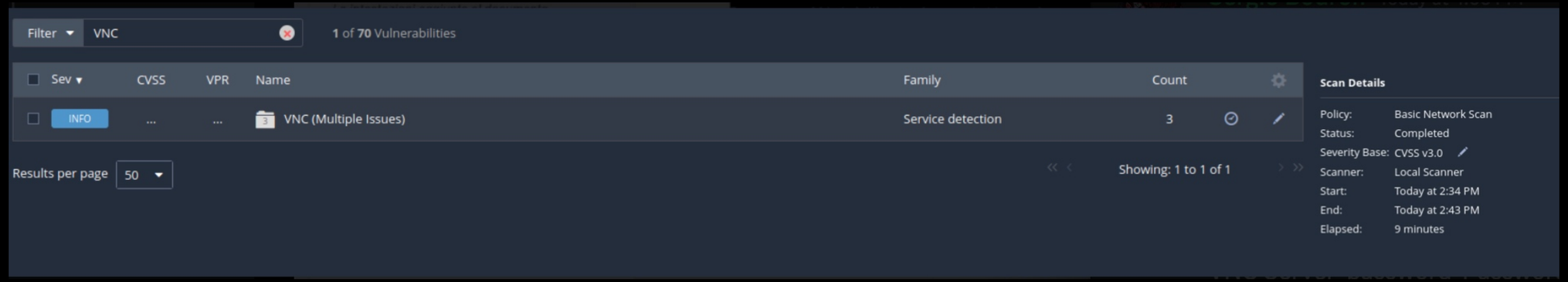
Questa vulnerabilità rilevata tramite Nessus ci informa che la password utilizzata a protezione del server VCN è “password”. Trattandosi di una password molto facile da individuare espone il server ad un altissimo rischio di un eventuale attacco da parte di terzi non autorizzati.



Risoluzione problematica 1

Utilizzando su Metasploitable il comando ***vncpasswd*** sono andato a sostituire la vecchia password vulnerabile con una nuova alfanumerica più sicura. Ora risulterà più complicato per un eventuale hacker individuare la password per entrare nel server VNC.

```
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#
```

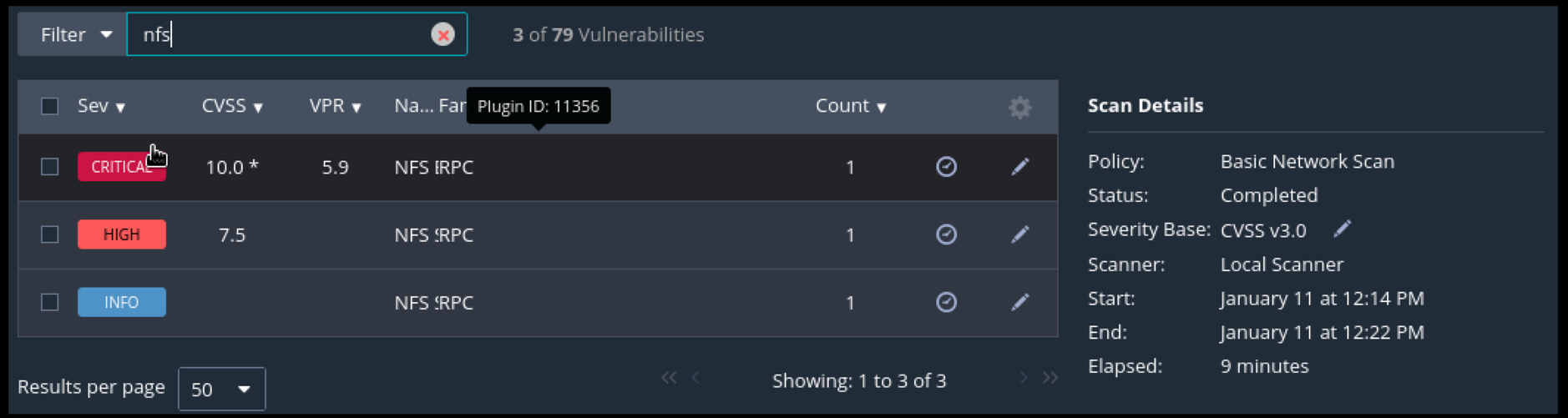


Vulnerabilità 2

NFS Exported share information disclosure

Network file system (NFS) è un protocollo utilizzato solitamente per condividere file o directory da un sistema Unix/Linux su una rete.

La vulnerabilità NFS Exported share information disclosure si ha quando le informazioni sulle condivisioni effettuate possono essere intercettate da host non autorizzati, i quali potrebbero potenzialmente leggere o anche scrivere file sul server remoto.



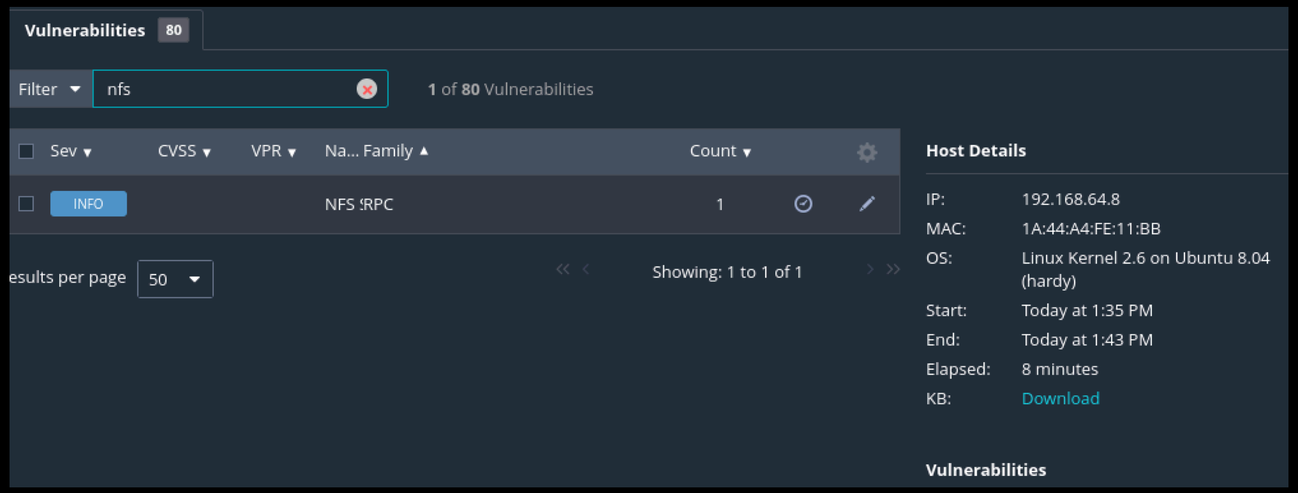
Risoluzione vulnerabilità 2

Da Metasploitable ho inserito il comando ***sudo nano etc/exports*** e sono andato ad eliminare l'ultima riga che autorizzava chiunque ad avere accesso al server. Con l'operazione svolta nessuno altro host , me escluso, avrà accesso al server.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
Sorry, try again.
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# sudo nano 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)
#

        *(rw,sync,no_root_squash,no_subtree_check)
```

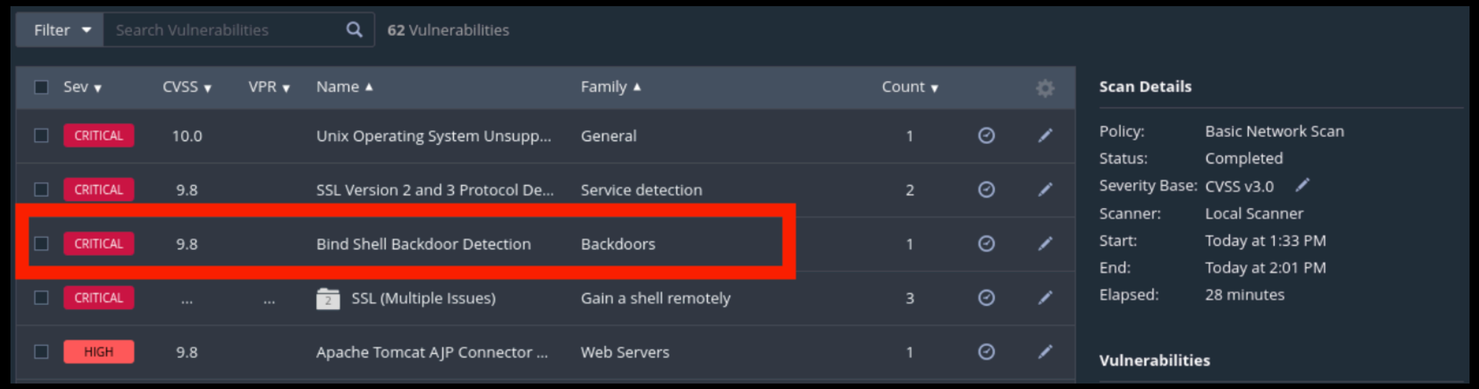


Vulnerabilità 3

Bind shell backdoor detection

Una backdoor è un tipo di accesso segreto o nascosto a un sistema informatico. Questo accesso consente a un hacker di controllare il sistema senza essere rilevato e senza autorizzazione del proprietario. La backdoor può essere utilizzata per eseguire comandi, raccogliere informazioni, modificare configurazioni o svolgere altre attività malevole.

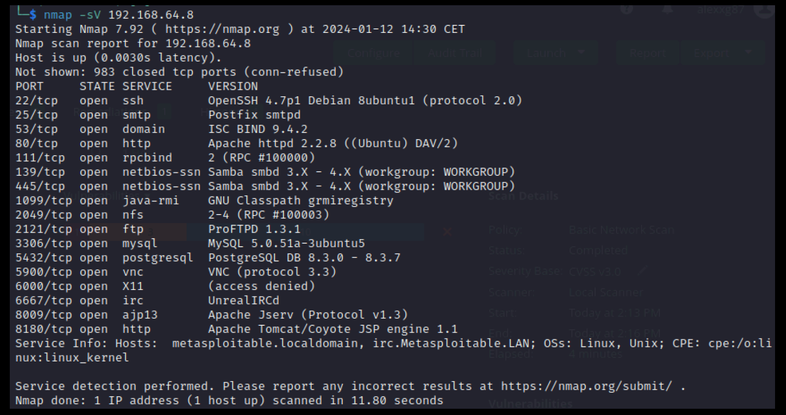
Con una backdoor spesso si intende la creazione di un punto di accesso segreto che bypassa le normali procedure di autenticazione. Può essere incorporata nel codice di un'applicazione, nascosta in un file eseguibile o implementata come un servizio di sistema.

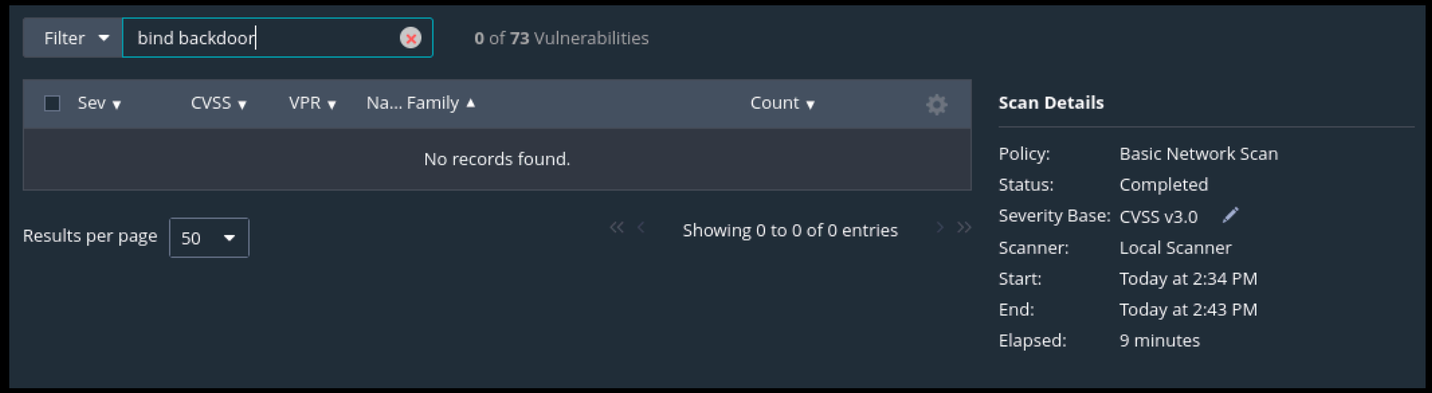


Risoluzione vulnerabilità 3

Grazie al software Nessus ero a conoscenza che la backdoor si trovasse sulla porta 1524 del nostro sistema.

Utilizzando su Metasploitable il comando ***lsof -i :1524*** sono riuscito a risalire al pid del processo in corso su quella porta (nel mio caso 4437). Successivamente con il comando ***kill 4437*** sono andato a chiudere la porta sulla quale era stata rilevata la backdoor. Come ulteriore conferma ho eseguito anche uno scan sull'ip di meta con Nmap per verificare che la porta fosse realmente chiusa.





Fine