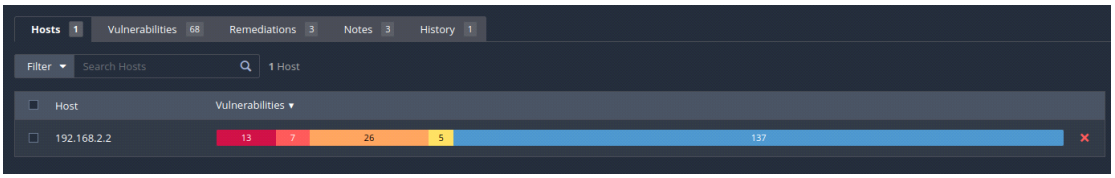
REPORT VA SCAN METASPLOITABLE

Nellesercirtazione di questo fine settimana vedremo le vulnerabilità sulla macchina virtuale Metasploitable 2 tramite il programma Nessus.

Nell'ambito della computer security Nessus è un software proprietario di tipo client-server di scansione di tutti i tipi di vulnerabilità. Costituito da nessusd, il demone, che effettua la scansione, e da nessus, il client, il quale fornisce all'utente i risultati della scansione, tramite lo scan e l'abilitazione di plugin appositamente configurabili a seconda della tipologia di host e vulnerabilità che si andrà ad analizzare, rileva le vulnerabilità presenti suggerendo le possibili soluzioni attraverso report di facile analisi in vari formati (html, pd e cls).

Per prima cosa scansionamo l'indirizzo ip di Metasploitable 2 (192.168.2.2):



Unavolta finito la scansione otteniamo queste criticità. Ora andremmo a vedere come risolvere alcune criticità:

51988 - Rilevamento Backdoor Bind Shell

Sinossi

L'host remoto potrebbe essere stato compromesso.

Descrizione

Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione.

Soluzione

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

Fattore di rischio

Critico

Punteggio base CVSS v3.0

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Punteggio base CVSS v2.0

10.0 (CVSS2#AV:N/CA:S/Au:N/DO:DO/MI:DO/LA:DO)

Informazioni sul plug-in

Pubblicato: 15/02/2011, Modificato: 11/04/2022

Uscita del plug-in

tcp/1524/wild_shell

per gestire questa vulnerabilità basta creare una regola di firewall che blocca l'accesso alla porta 1524 sul firewall pfsense.

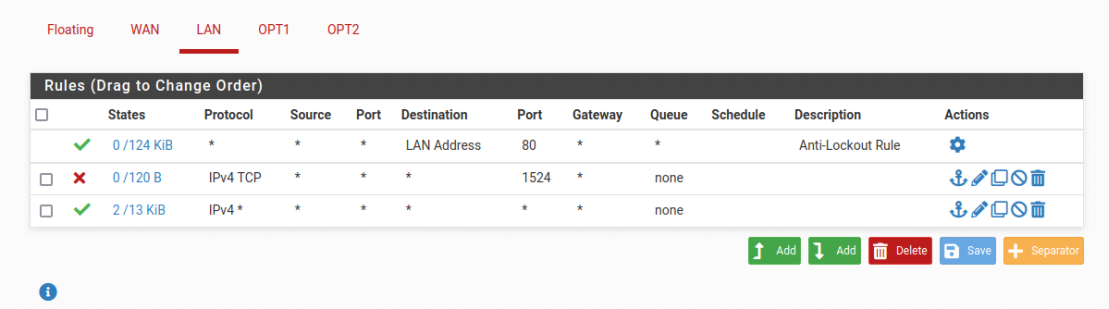
pfSense è una distribuzione completamente gratuita, basata su FreeBSD, customizzata per essere un firewall e router. Oltre ad essere una potente piattaforma firewall e router, essa include una lunga lista di pacchetti che permettono di espandere facilmente le funzionalità senza compromettere la sicurezza del sistema.

```
└─$ nmap -sV -p 1524 192.168.2.2
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-02 12:26 CEST
Nmap scan report for 192.168.2.2
Host is up (0.0011s latency).

PORT     STATE SERVICE   VERSION
1524/tcp open  bindshell Metasploitable root shell

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.94 seconds
```

Controlliamo se la port è realmente aperta con il comando Nmap come nello screenshot.



Andiamo quindi a creare la seguente regola di firewall all'interno di pfsense.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 1524 192.168.2.2
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-02 12:27 CEST
Nmap scan report for 192.168.2.2
Host is up (0.00096s latency).

PORT     STATE    SERVICE    VERSION
1524/tcp filtered ingreslock

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.00 seconds
```

Ricontrolliamo se la porta è realmente chiusa.

11356 - Divulgazione di informazioni sulla condivisione esportata NFS

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 e un utente malintenzionato potrebbe essere in grado di sfruttarla per leggere (ed eventualmente scrivere) file sull'host remoto.

Soluzione

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

Fattore di rischio

Critico

Punteggio VPR

5.9

Punteggio base CVSS v2.0

10.0 (CVSS2#AV:N/CA:S/Au:N/DO:DO/MI:DO/LA:DO)

Riferimenti

CVE	CVE-1999-0170
CVE	CVE-1999-0211
CVE	CVE-1999-0554

Sfruttabile con

Metasploit (vero)

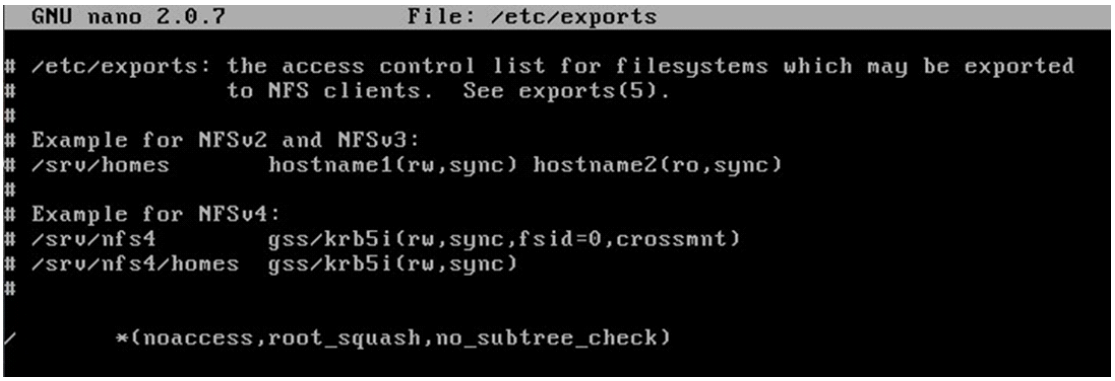
Informazioni sul plug-in

Pubblicato: 12/03/2003, Modificato: 17/09/2018

Uscita del plug-in

udp/2049/rpc-nfs

Per risolvere questa crticità basta andare all'interno dei file di configurazione di NFS e andare a configurare un file andando a specificare i permessi in solo lettura ed esecuzione per gli utenti normali.



Si cambia l'ultima riga con il seguente codice: /var/share/public *(rw,sync,no_root_squash).

10203 - Rilevamento servizio rexecd

Sinossi

Il servizio rexecd è in esecuzione sull'host remoto.

Descrizione

Il servizio rexecd è in esecuzione sull'host remoto.

Tuttavia, rexecd non fornisce alcun buon mezzo di autenticazione, quindi potrebbe essere abusato da un utente malintenzionato per scansionare un host di terze parti.

Soluzione

Commenta la riga 'exec' in /etc/inetd.conf e riavvia il processo inetd.

Fattore di rischio

Critico

Punteggio VPR

6.7

Punteggio base CVSS v2.0

10.0 (CVSS2#AV:N/CA:S/Au:N/DO:DO/MI:DO/LA:DO)

Riferimenti

CVE CVE-1999-0618

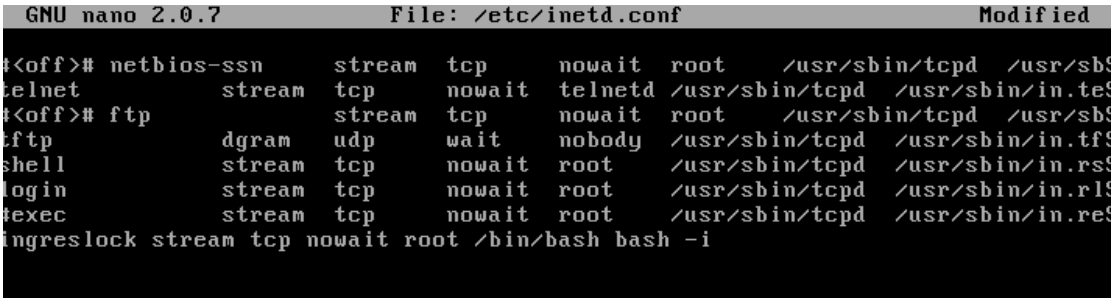
Informazioni sul plug-in

Pubblicato: 31/08/1999, Modificato: 13/08/2018

Uscita del plug-in

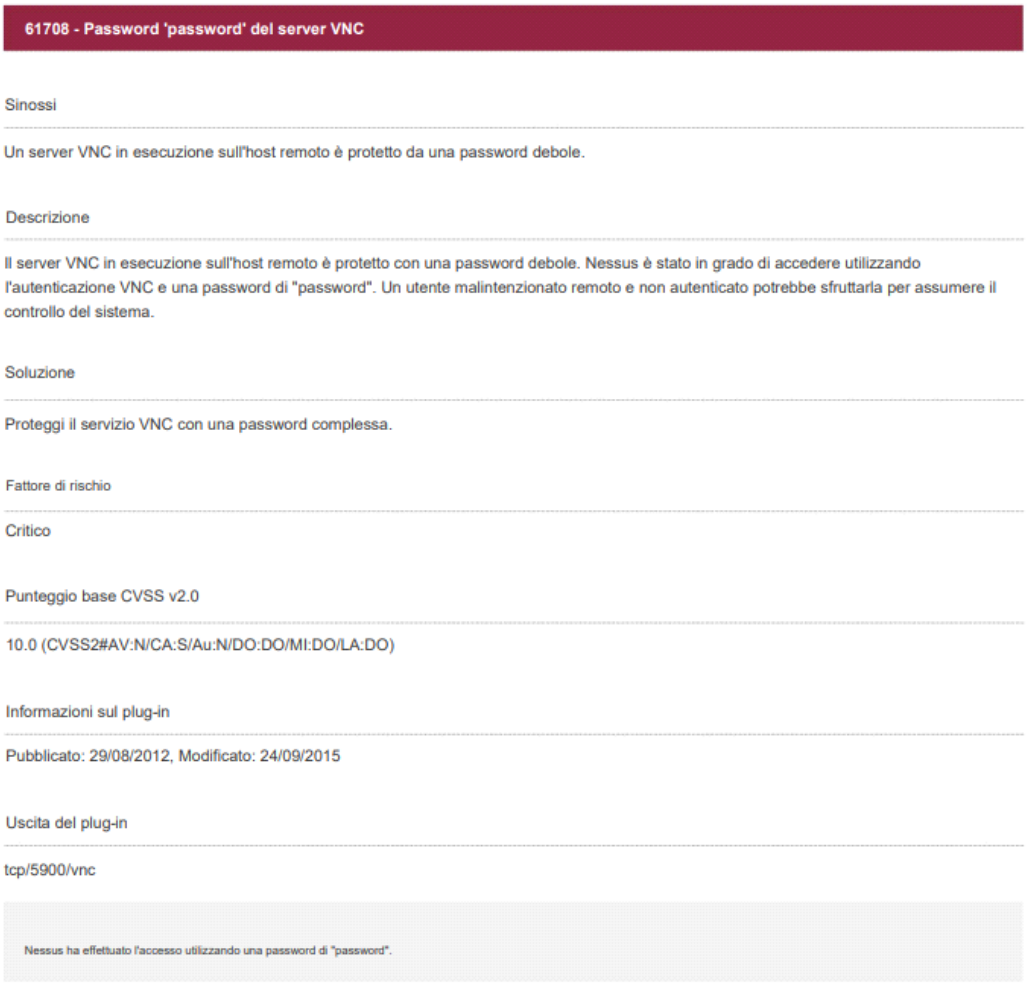
tcp/512/rexecd

Per risolvere questa criticità basta commentare la riga exec nel file di configurazione inet.conf:



Ci tengo a precisare che non basta solo commentare con # ma bisogna scrivere #<off># prima dall'exec.

Per risolvere questa



61708 - Password 'password' del server VNC

Sinossi

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

Descrizione

Il server VNC in esecuzione sull'host remoto è protetto con 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 sfruttarla per assumere il controllo del sistema.

Soluzione

Proteggi il servizio VNC con una password complessa.

Fattore di rischio

Critico

Punteggio base CVSS v2.0

10.0 (CVSS2#AV:N/CA:S/Au:N/DO:DO/MI:DO/LA:DO)

Informazioni sul plug-in

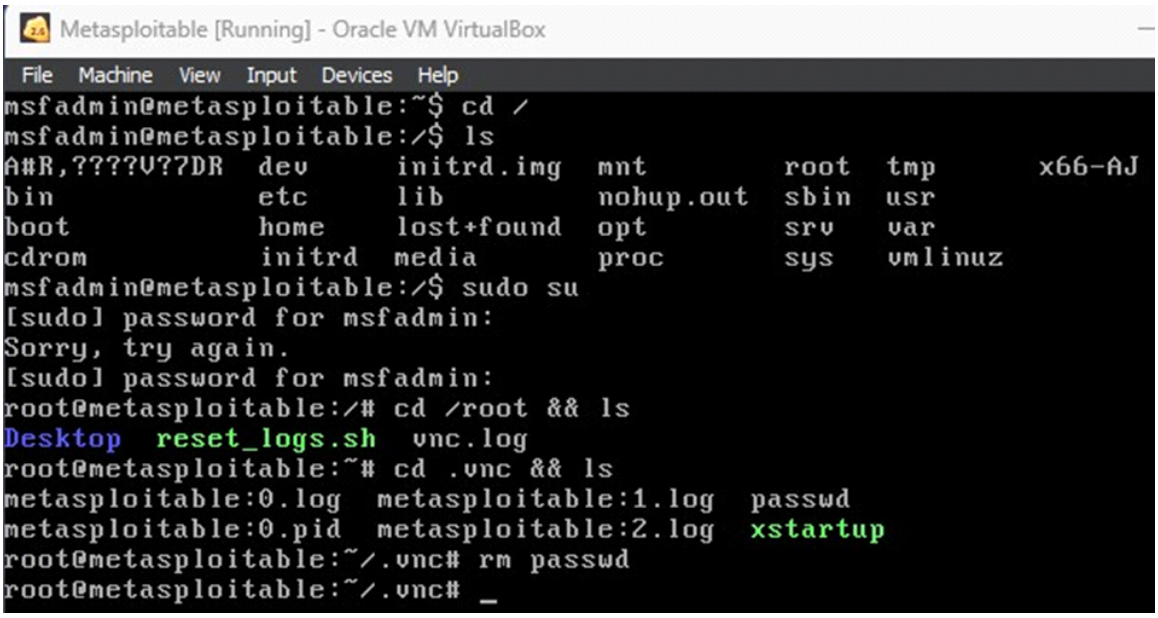
Pubblicato: 29/08/2012, Modificato: 24/09/2015

Uscita del plug-in

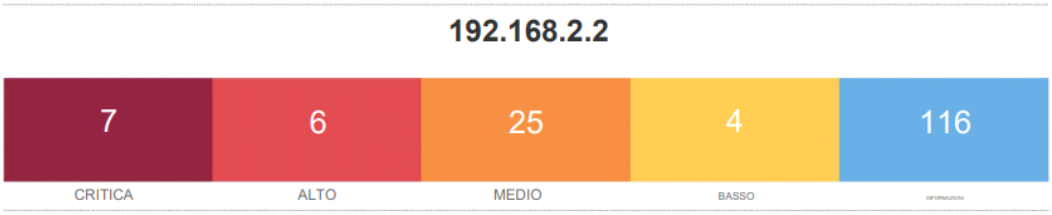
tcp/5900/vnc

Nessus ha effettuato l'accesso utilizzando una password di "password".

Per risolvere questa critricità basta rimuovere la password "password" dal file VNC:



IN CONCLUSIONE:



Dopo aver risolto le criticità principali le crititcità sono diminuite non di 4 ma di un numero superiore, poichè risolvnedo alcune criticità automaticamente alcune crititcità collegate a quelle risolte si sono automaticamente eliminate.