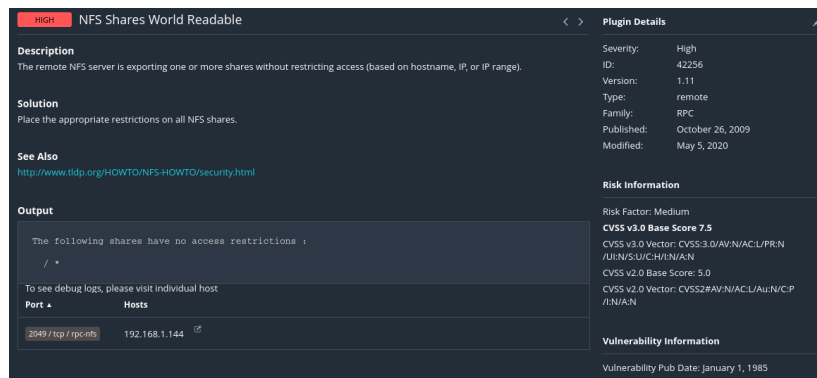


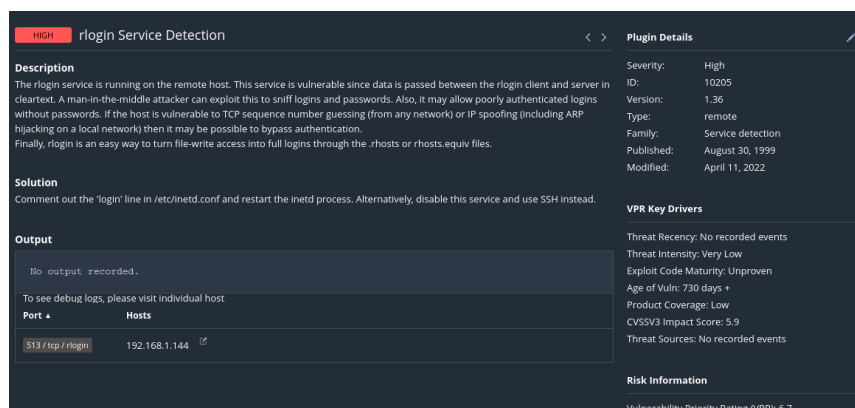
La condivisione NFS era configurata in modo che tutti gli utenti potessero leggere i dati.



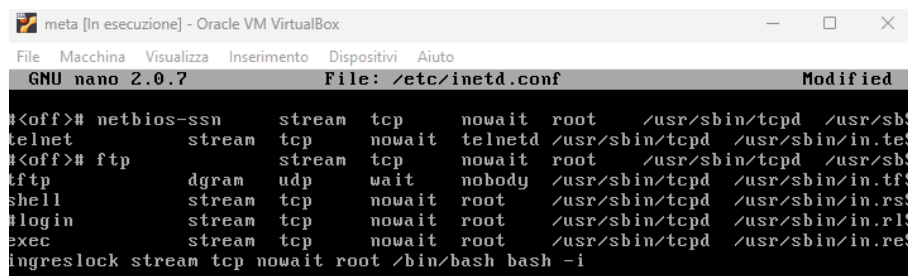
La configurazione di NFS Exported Share Information ha permesso di ridurre il rischio anche di questa vulnerabilità

rlogin Service Detection:

Il servizio rlogin era attivo, esponendo il sistema a potenziali rischi di sicurezza.



Il servizio rlogin è stato disabilitato commentando la linea nel file di login.



VNC Server 'password' Password:

Il server VNC utilizzava una password debole (password).

CRITICAL

VNC Server 'password' Password

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

Output

Nessus logged in using a password of "password".

To see debug logs, please visit individual host

Port	Hosts
5900 /tcp /vnc	192.168.1.144

Plugin Details

Severity: Critical

ID: 61708

Version: \$Revision: 1.2 \$

Type: remote

Family: Gain a shell remotely

Published: August 29, 2012

Modified: September 24, 2015

Risk Information

Risk Factor: Critical

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

Default Account: true

Exploited by Nessus: true

La password VNC è stata cambiata con una più sicura (M5F@dm1n).

```
meta [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

La macchina virtuale segnala che il sistema guest supporta integrazione del puntatore del mouse. Ciò significa che non è
Password:
Last login: Fri Jan 12 10:18:10 EST 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
VNC directory /home/msfadmin/.vnc does not exist, creating.
Password:
Verify:
```

Qui possiamo vedere come nella seconda scansione il livello di criticità delle 4 vulnerabilità sia sceso e non compaiono più tra le vulnerabilità **CRITICAL** e **HIGH**.

<input type="checkbox"/> Sev ▼	CVSS	VPR	Name	Family	Count	
<input type="checkbox"/> CRITICAL	10.0		Unix Operating S...	General	1	🔍 ✎
<input type="checkbox"/> CRITICAL	10.0 *	7.4	UnrealIRCd Back...	Backdoors	1	🔍 ✎
<input type="checkbox"/> CRITICAL	9.8		SSL Version 2 an...	Service detection	2	🔍 ✎
<input type="checkbox"/> CRITICAL	9.8		Bind Shell Back...	Backdoors	1	🔍 ✎
<input type="checkbox"/> MIXED	DNS (Multip...	DNS	5	🔍 ✎
<input type="checkbox"/> MIXED	Apache To...	Web Servers	4	🔍 ✎
<input type="checkbox"/> CRITICAL	SSL (Multipl...	Gain a shell remotely	3	🔍 ✎
<input type="checkbox"/> HIGH	7.5	6.7	Samba Badlock ...	General	1	🔍 ✎
<input type="checkbox"/> MIXED	SSL (Multipl...	General	28	🔍 ✎
<input type="checkbox"/> MIXED	ISC Bind (M...	DNS	5	🔍 ✎