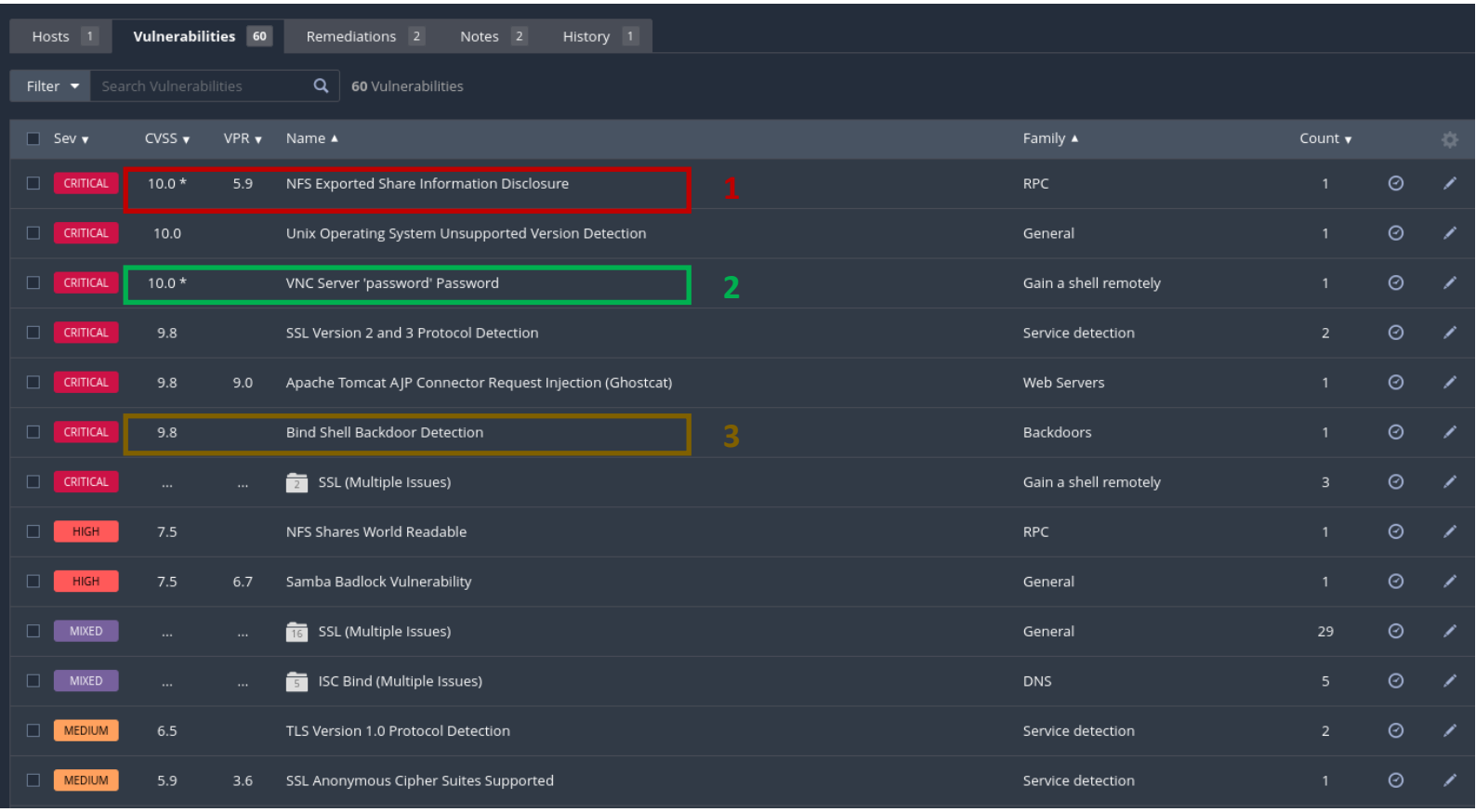
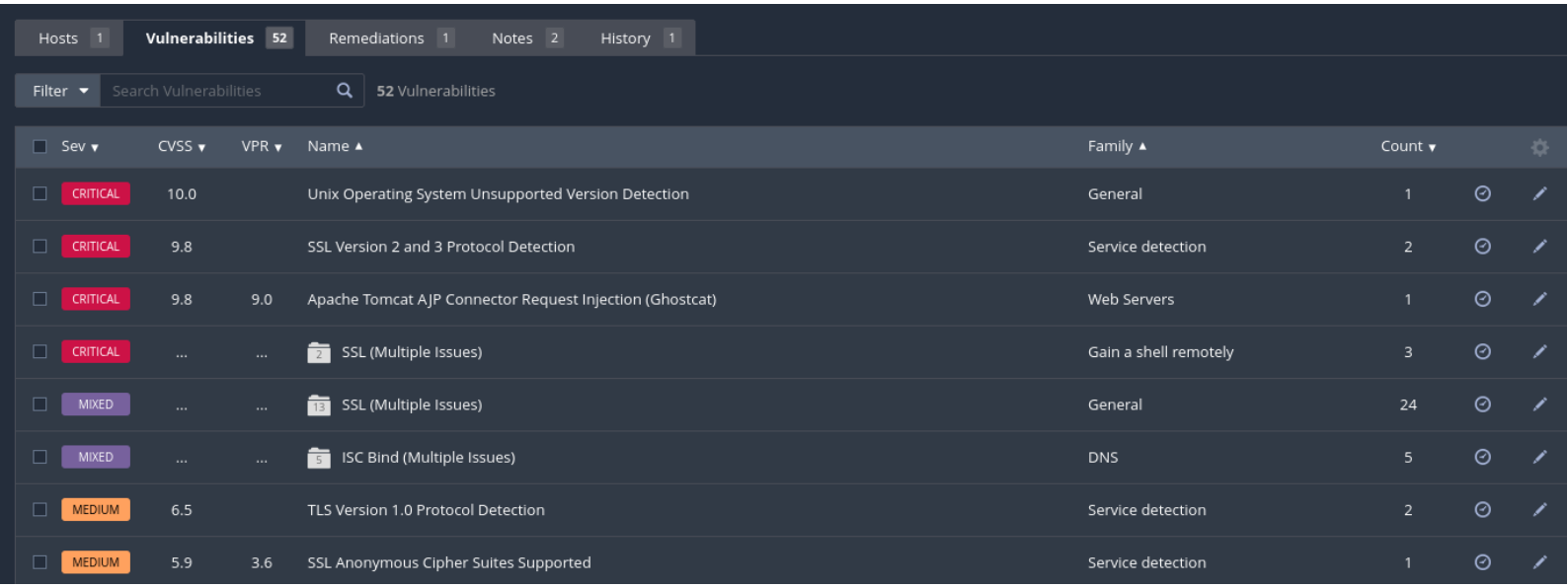
S5L5 Traccia: Effettuare una scansione completa sul target Metasploitable.

Andiamo ad effettuare una scansione con nessus per identificare e valutare le vulnerabilità di sicurezza all'interno di reti, sistemi e applicazioni. Nessus effettua una scansione approfondita delle reti alla ricerca di dispositivi, server, dispositivi di rete e altri sistemi connessi per identificare potenziali punti deboli o vulnerabilità. Scegliamo 3 vulnerabilità ed andiamo ad analizzarle e a trovare delle azioni di rimedio.
Alla fine andremo a fare una scansione finale per confrontare i risultati una volta sistemato le vulnerabilità.

Scansione iniziale



Scansione finale



1

11356 - NFS Exported Share Information Disclosure

Synopsis

It is possible to access NFS shares on the remote host.

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Risk Factor

Critical

VPR Score

5.9

CVSS v2.0 Base Score

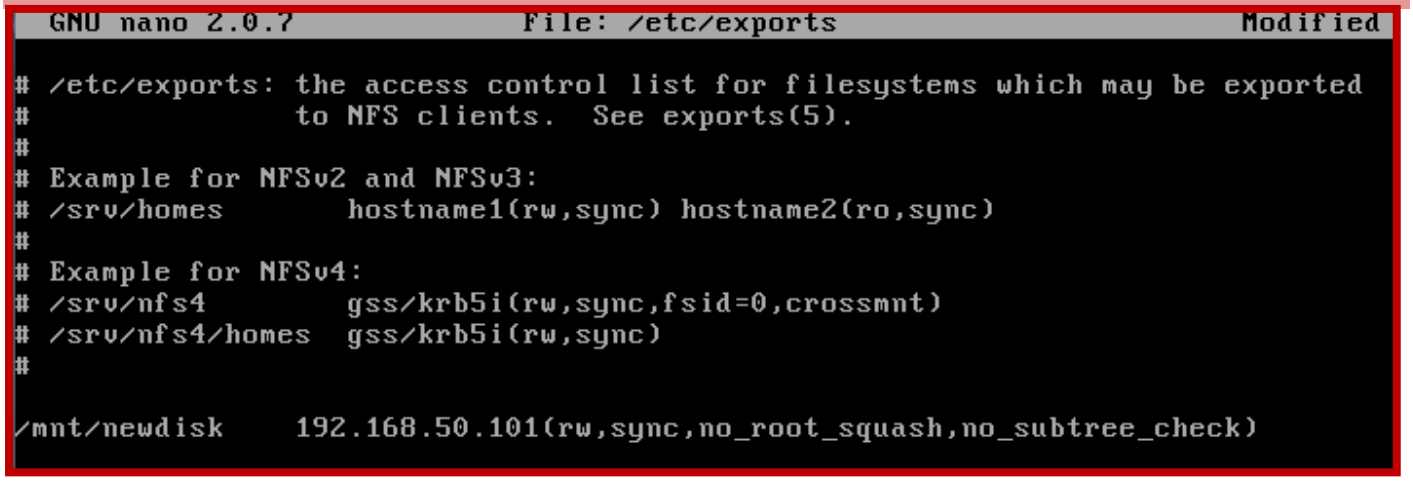
10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

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

Come soluzione ci viene consigliato di configurare il servizio NFS (Network File System) sul computer remoto in modo che solo i computer autorizzati siano in grado di montare (cioè accedere) alle condivisioni remote offerte da quel sistema tramite NFS.

Quindi specifichiamo l'indirizzo IP che sono autorizzati ad accedere alle condivisioni NFS, in questo caso l'IP di Metasploitable di 192.168.50.101.



CVE sta per "Common Vulnerabilities and Exposures" (Vulnerabilità e Esposizioni Comuni).

Il CVE è un elenco pubblico e gratuito di identificatori univoci assegnati a vulnerabilità informatiche note. Le informazioni fornite sul sito web CVE sono utili per gli esperti di sicurezza informatica, i ricercatori, i fornitori di software e gli utenti finali. Inoltre offre anche altri strumenti e risorse relative alla sicurezza informatica, come le linee guida per la gestione delle vulnerabilità e altre informazioni utili per affrontare e mitigare le minacce alla sicurezza informatica.

https://cve.mitre.org/ è il portale ufficiale del "Common Vulnerabilities and Exposures" (CVE) gestito dall'organizzazione MITRE Corporation in collaborazione con la comunità globale della sicurezza informatica.

Andiamo a cercare le nostre vulnerabilità

CVE-1999-0170

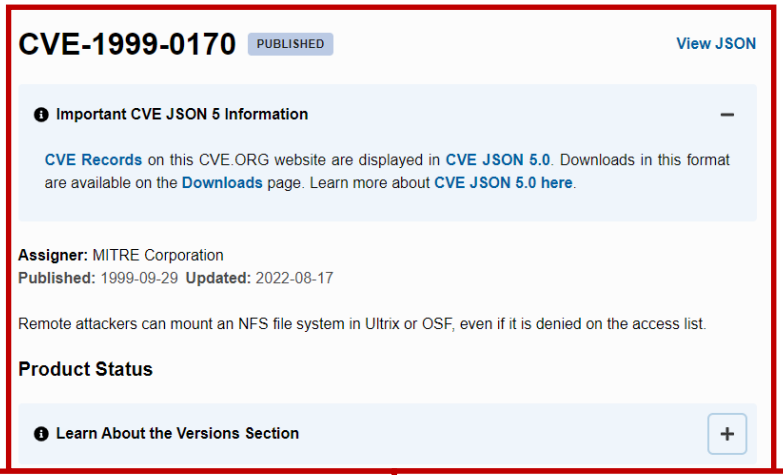
Gli attaccanti remoti possono montare un sistema file NFS su Ultrix o OSF, anche se è stato negato nell'elenco di accesso.

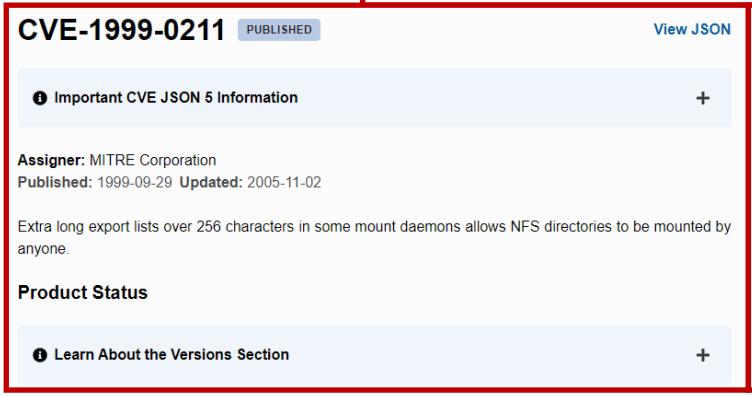
CVE-1999-0211

Le liste di esportazione molto lunghe, oltre i 256 caratteri, in alcuni daemon di mount consentono a chiunque di montare directory NFS.

CVE-1999-0554

Le esportazioni NFS mettono a disposizione dei dati critici del sistema al mondo esterno, ad esempio la directory radice (/) o un file di password.





2

61708 - VNC Server 'password' Password

Synopsis

A VNC server running on the remote host is secured with a weak 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.

Risk Factor

Critical

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information

Published: 2012/08/29, Modified: 2015/09/24

Plugin Output

tcp/5900/vnc

La soluzione della vulnerabilità è suggerita in alto.

Proseguiamo quindi a proteggere il servizio VNC modificando la password,

con una di sicurezza maggiore su Metaspoitable per proteggere il servizio VNC.

3

51988 - Bind Shell Backdoor Detection

Synopsis

The remote host may have been compromised.

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information

Published: 2011/02/15, Modified: 2022/04/11

Plugin Output

tcp/1524/wild_shell

La vulnerabilità di un "Bind Shell Backdoor" è un problema molto serio perché consente di ottenere un accesso non autorizzato al sistema. E' necessario identificare e rimuovere la backdoor dal sistema, per poter risolvere questa vulnerabilità.
Quindi andiamo a trovare la porta 1524 e con una regola chiudiamo tutti gli accessi, impedendo cosi agli attaccanti di entrare senza un permesso. E' importante sempre tenere il sistema sotto il controllo, per evitare che situazioni simili si ripresentano in futuro.

```
root@metasploitable:/home/msfadmin# ufw status
Firewall not loaded
root@metasploitable:/home/msfadmin# ufw enable
Firewall started and enabled on system startup
root@metasploitable:/home/msfadmin# ufw default allow
Default policy changed to 'allow'
(be sure to update your rules accordingly)
root@metasploitable:/home/msfadmin# ufw deny 1524
Rule added
root@metasploitable:/home/msfadmin# ufw status
Firewall loaded

To                         Action  From
--                         ------  ----
1524:tcp                   DENY    Anywhere
1524:udp                   DENY    Anywhere

root@metasploitable:/home/msfadmin#
```