M/C

Progetto S5L5

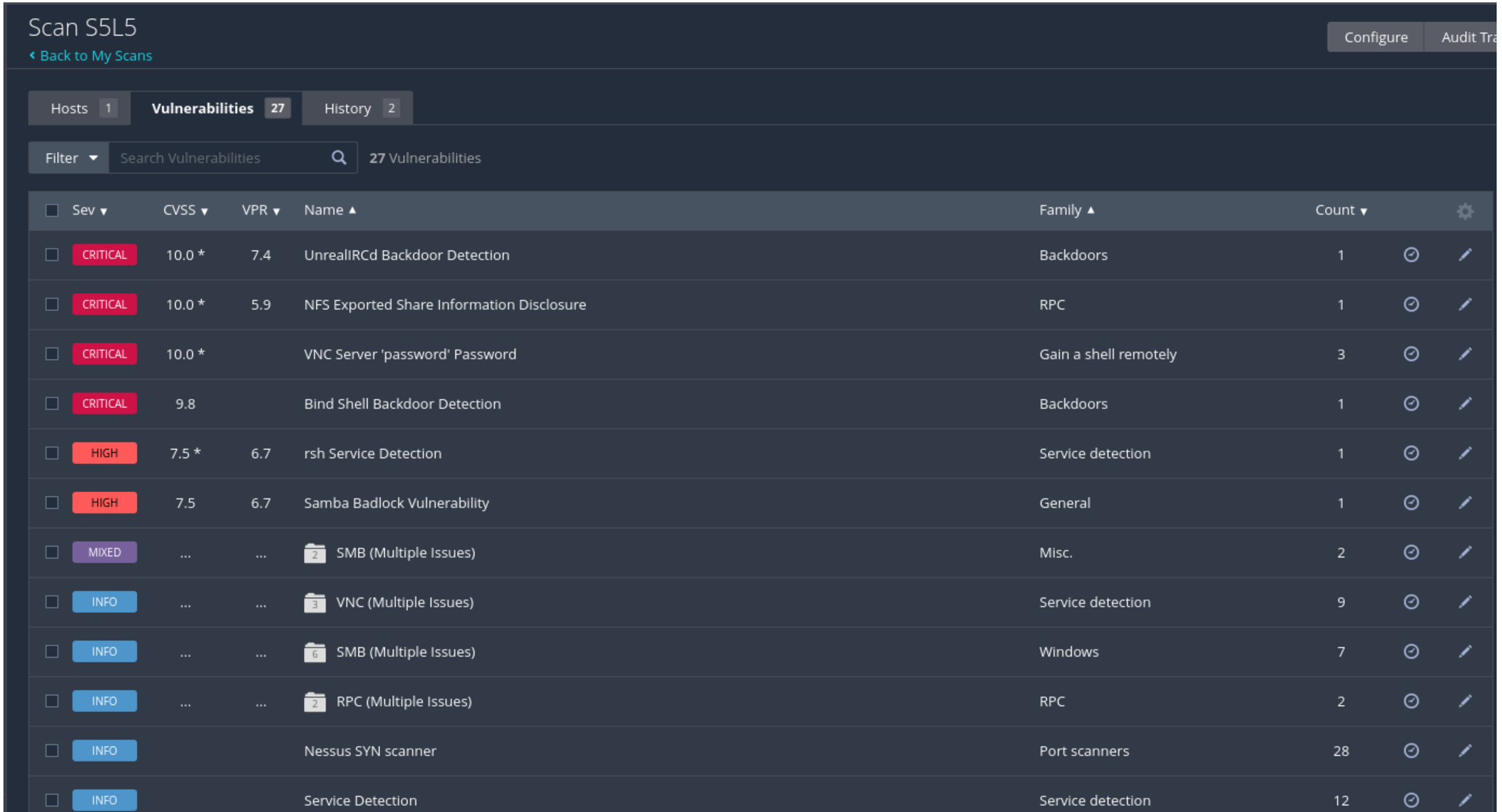
01

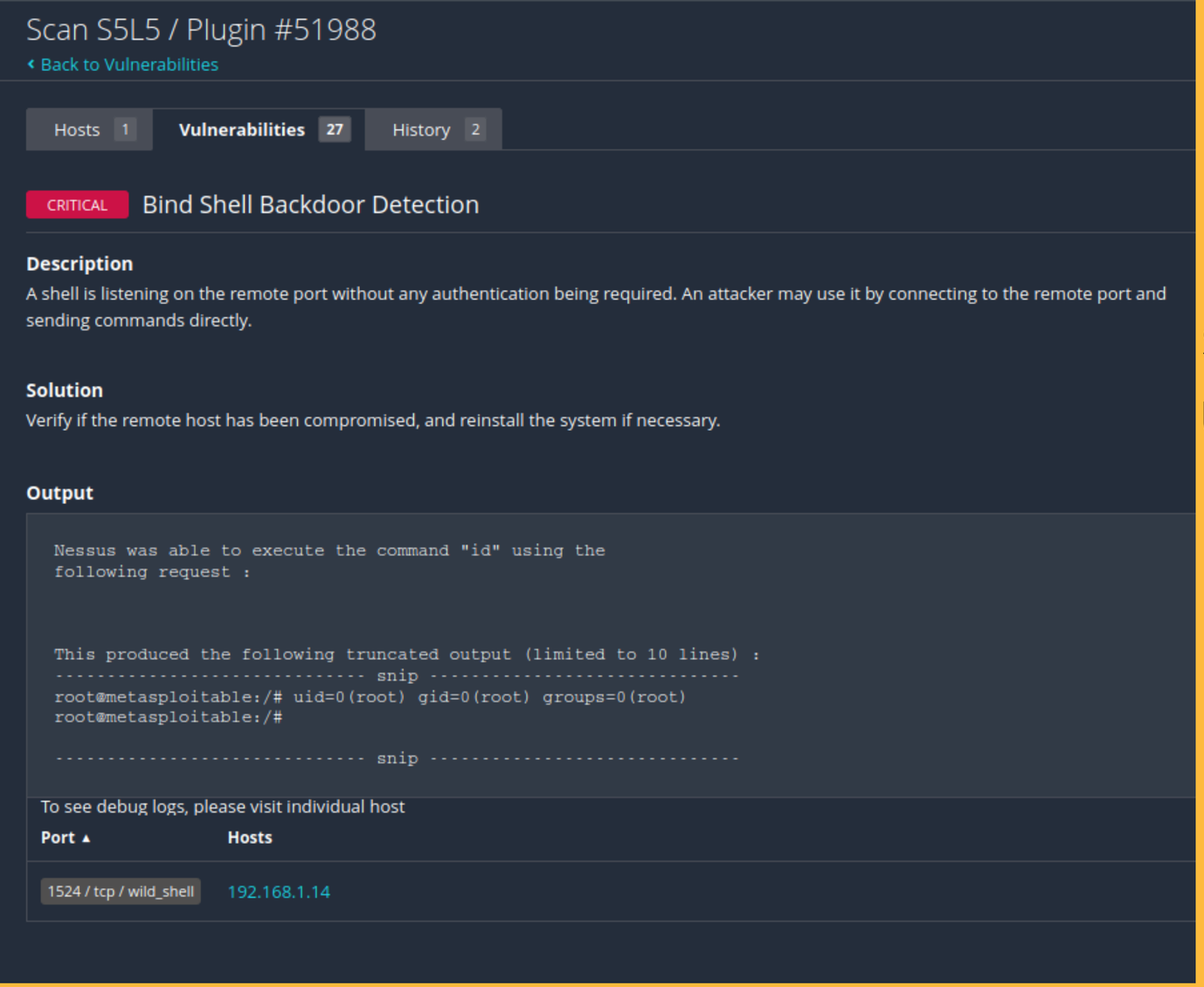
S5L5 Nessus

02

Nel progetto odierno andiamo ad utilizzare nessus un potente
vulnerability scanner. Questo tool professionale e preciso è tra i migliori in circolazione e ci permette di rilevare le vulnerabilità dei vari componenti di una rete.
Nelle prossime slide andremo a visualizzare un report
sulla nostra macchina meta e a risolvere alcune
vulnerabilità critiche

Andando ad effettuare il primo basic network scan questi sono i risultati ottenuti, nelle prossime slide andremo a vedere nello specifico alcune delle criticità trovate e le andremo a risolvere





Bind Shell Backdoor

Una "bind backdoor" è un tipo specifico di backdoor che consente a un attaccante remoto di stabilire una connessione di rete a una macchina compromessa. Questo tipo di backdoor può essere utilizzato per aprire una "shell" di comando remota, consentendo all'attaccante di eseguire comandi sul sistema remoto senza autenticazione.

Risoluzione bind shell backdoor

```
msfadmin@metasploitable:~$ sudo ufw enable
[sudo] password for msfadmin:
Firewall started and enabled on system startup
msfadmin@metasploitable:~$ sudo ufw default ALLOW
Default policy changed to 'allow'
(be sure to update your rules accordingly)
msfadmin@metasploitable:~$ sudo ufw deny 1524
Rule added
msfadmin@metasploitable:~$ _
```

Come si evince dalla slide precedente, Nessus ci segnala che sulla porta 1524 c'è una bind shell backdoor andiamo quindi a lavorare sulla porta in questione. Ho risolto questa vulnerabilità abilitando il Firewall di meta e andando a negare l'accesso alla porta in questione, che adesso è protetta dal firewall. Potenzialmente questo discorso va esteso a tutte le porte aperte e inutilizzate, le quali vanno chiuse o gestite con determinate politiche di sicurezza

Scan S5L5 / Plugin #11356

‹ Back to Vulnerabilities

Hosts 1 | **Vulnerabilities 27** | History 2

CRITICAL NFS Exported Share Information Disclosure

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.

Output

```
The following NFS shares could be mounted :

+ /
  + Contents of / :
    - .
    - ..
    - bin
    - boot
    - cdrom
more...
```

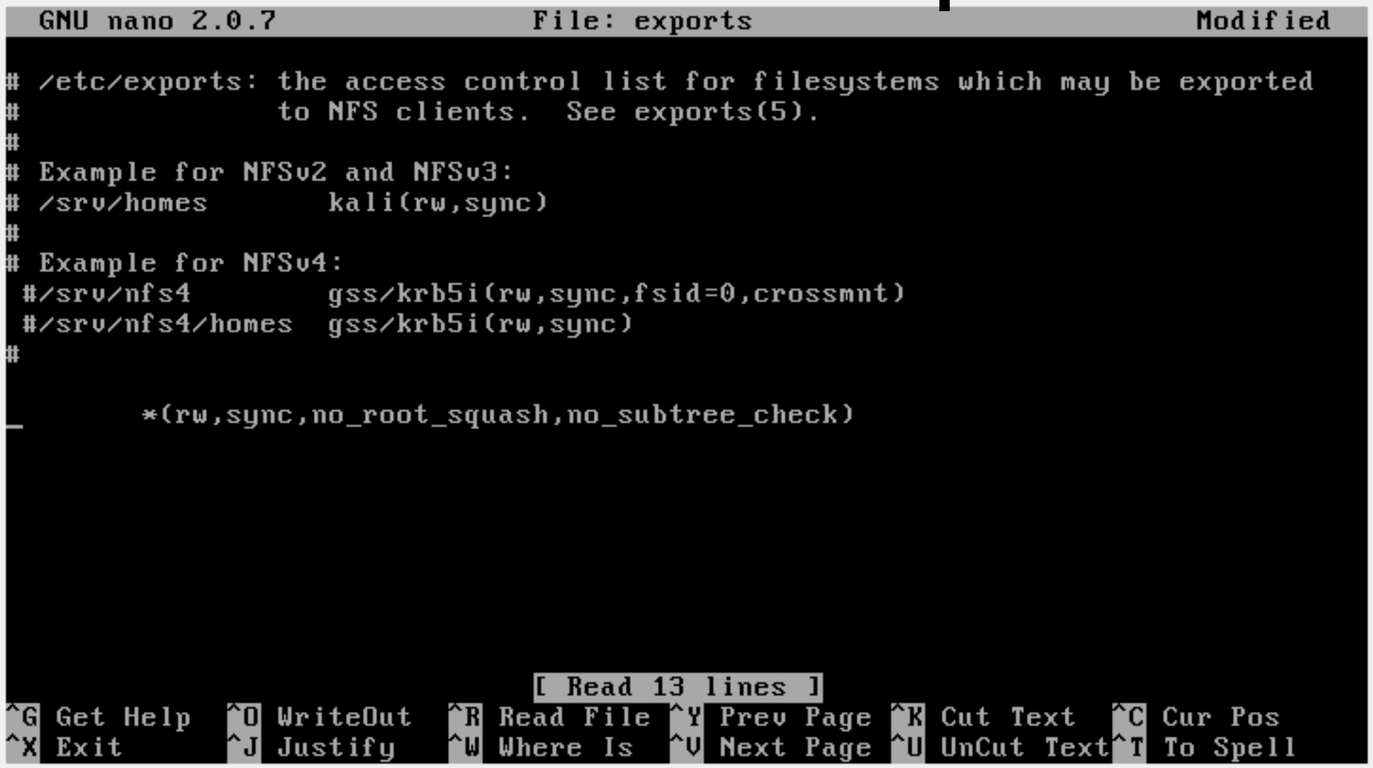
To see debug logs, please visit individual host

Port ▲	Hosts
2049 / udp / rpc-nfs	192.168.1.14

NFS Exported Share Information Disclosure

Si riferisce a una vulnerabilità nella configurazione di un server NFS (Network File System) che potrebbe consentire a utenti non autorizzati di ottenere informazioni sensibili sulle condivisioni NFS esistenti. Questa vulnerabilità può rivelare dettagli sulla configurazione del server NFS, inclusi i percorsi di condivisione, le autorizzazioni e le risorse disponibili.

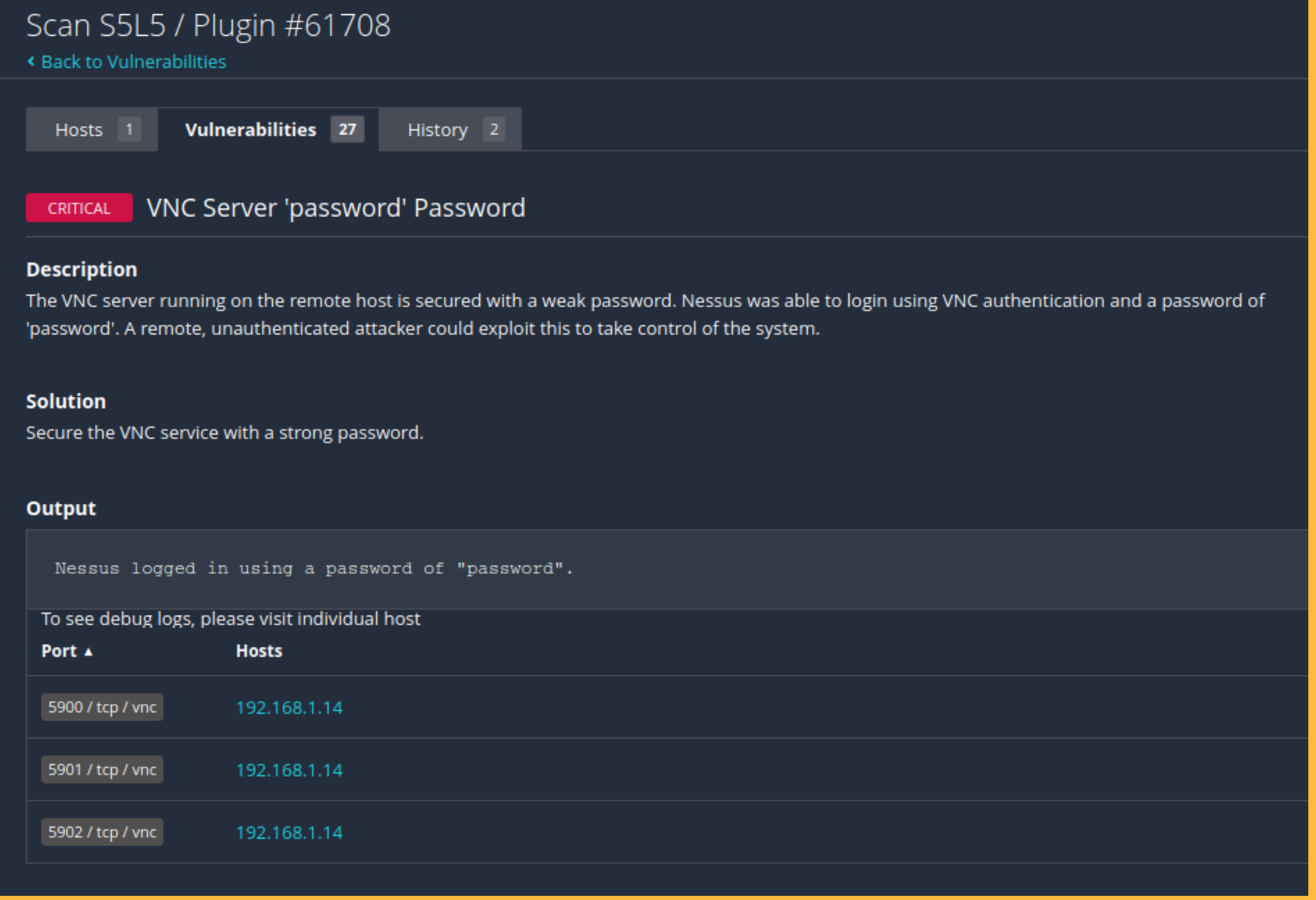
Risoluzione NFS Exported Share Information Disclosure



Questo è come si presentava il file di configurazione in /etc/exports che come possiamo vedere nella foto affianco, nel ultimo rigo consente azioni a chiunque in quanto presente quel asterisco. Come risoluzione ho pensato di commentare questa riga eliminando così il libero accesso. Sarebbe stato comunque possibile rimuovere l'asterisco e andare a indicare l'hostname degli host autorizzati, in modo da implementare una nuova regola di sicurezza

Qui sotto possiamo vedere la modifica apportata:

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



VNC Server ‘password’ Password

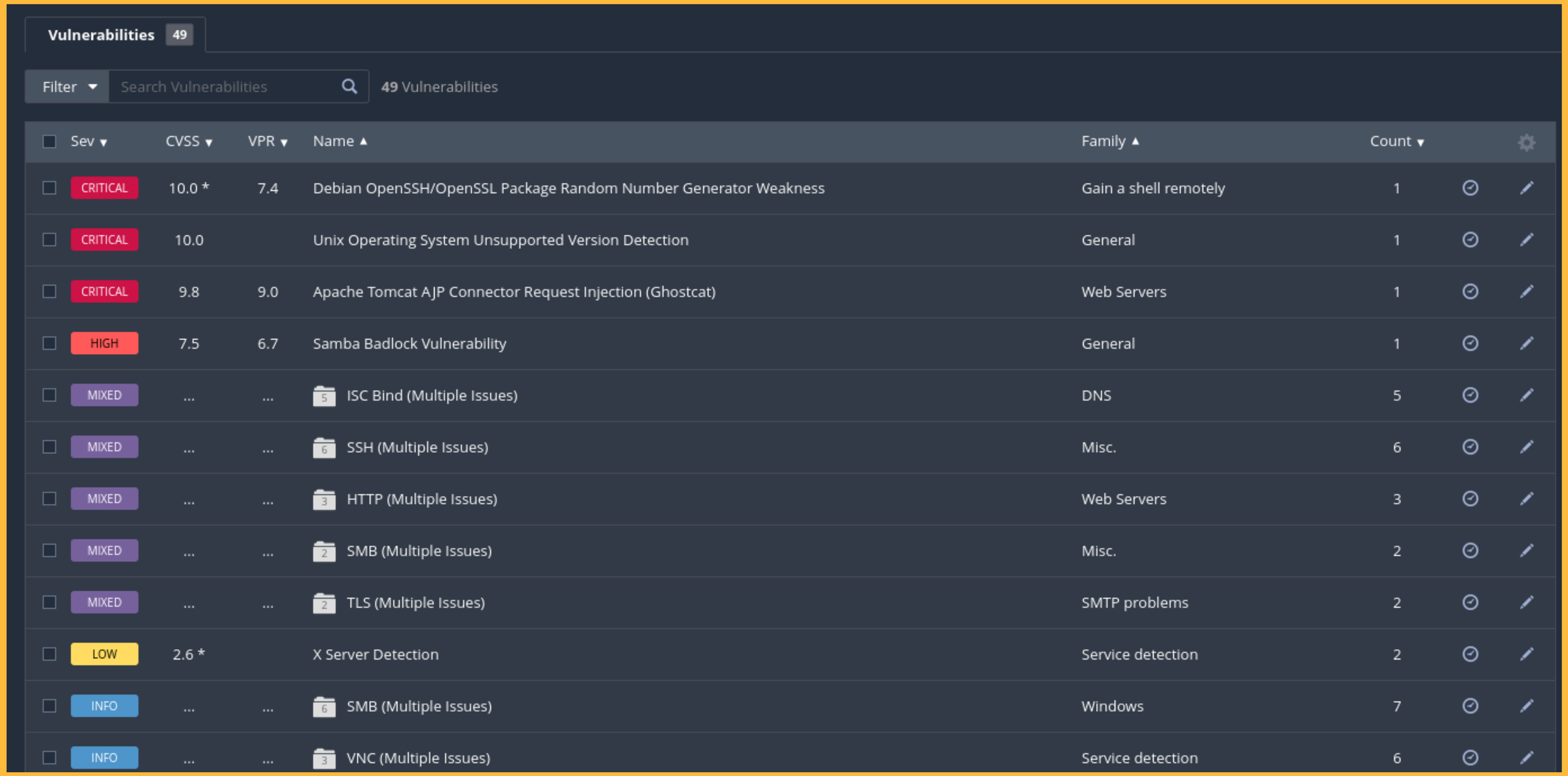
Questa vulnerabilità fa riferimento alla password per accedere al server in questione, ci segnala che abbiamo impostato una password debole, per l’appunto “password”. Nessus è riuscito a rilevare la password simulando un attacco brute force, questa una delle tantissime funzionalità del nostro tool.

Risoluzione VNC server password ‘password’

```
msfadmin@metasploitable:/etc$ sudo vncpassword
sudo: vncpassword: command not found
msfadmin@metasploitable:/etc$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
msfadmin@metasploitable:/etc$
```

Con i comandi sopraindicati siamo andati a impostare una nuova password più sicura per il nostro server VNC, risolvendo così la bassa sicurezza relativa alla password precedentemente usata. Siamo andati a impostare una password così composta : 3 lettere maiuscole, 3 lettere minuscole, 1 numero e 2 caratteri speciali.

Scansione post risoluzione delle vulnerabilità



Vulnerabilities 49

Filter | Search Vulnerabilities | 49 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	7.4	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	Gain a shell remotely	1
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1
MIXED	...	...	ISC Bind (Multiple Issues)	DNS	5
MIXED	...	...	SSH (Multiple Issues)	Misc.	6
MIXED	...	...	HTTP (Multiple Issues)	Web Servers	3
MIXED	...	...	SMB (Multiple Issues)	Misc.	2
MIXED	...	...	TLS (Multiple Issues)	SMTP problems	2
LOW	2.6 *		X Server Detection	Service detection	2
INFO	...	...	SMB (Multiple Issues)	Windows	7
INFO	...	...	VNC (Multiple Issues)	Service detection	6

Come possiamo vedere dopo il nostro intervento le 3 vulnerabilità non sono più presenti tra quelle critiche

M/C

S5 L5 NESSUS

Grazie !

Massimo Cinquegrana