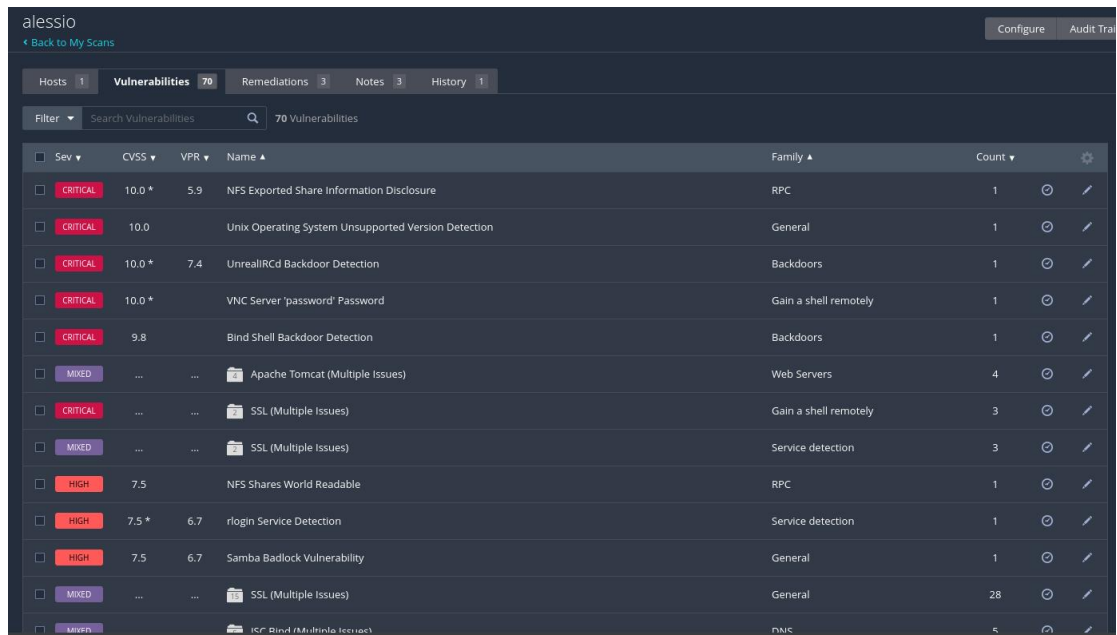


REPORT VULNERABILITIES



The screenshot shows the 'alessio' vulnerability scanner interface. At the top, there are tabs for 'Hosts' (1), 'Vulnerabilities' (70), 'Remediations' (3), 'Notes' (3), and 'History' (1). Below the tabs is a search bar with the text '70 Vulnerabilities'. The main table lists vulnerabilities with columns for 'Sev', 'CVSS', 'VPR', 'Name', 'Family', and 'Count'. The vulnerabilities are sorted by severity, with 'CRITICAL' items at the top. The 'VNC Server 'password' Password' vulnerability is highlighted.

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
MIXED	Apache Tomcat (Multiple Issues)	Web Servers	4
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3
MIXED	SSL (Multiple Issues)	Service detection	3
HIGH	7.5		NFS Shares World Readable	RPC	1
HIGH	7.5 *	6.7	rlogin Service Detection	Service detection	1
HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1
MIXED	SSL (Multiple Issues)	General	28
Low	ICP Bind (Multiple Issues)	DMC	5

Effettuiamo uno scan su nessus, rilevando questi rischi.

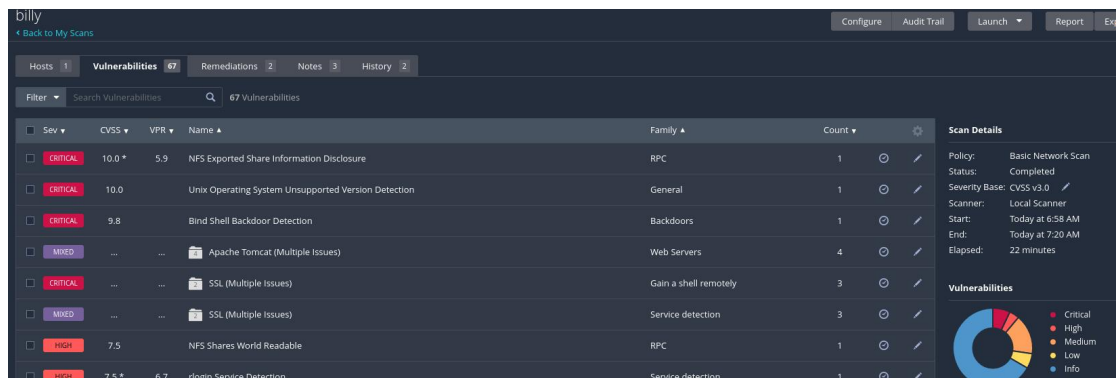
Procedendo alla risoluzione di 3 si loro.

● VNC SERVER PASSWORD

Il server VNC (Virtual Network Computing), accedendo al dispositivo dove situato il server (meta nel nostro caso), apriamo la sessione in Root e applichiamo il comando “vncpasswd” per poter cambiare password del server. In successione riavviamo il server e con questo processo dovrebbe essersi risolto quella vulnerabilità.

E per essere sicuri del cambio usiamo il comm “vncviewer” + ip, su Kali, cosi da poter aprire il software ed accedere con le nuove credenziali.

E in effetti rescannerizzando il problema sparisce.



The screenshot shows the 'billy' vulnerability scanner interface. At the top, there are tabs for 'Hosts' (1), 'Vulnerabilities' (67), 'Remediations' (2), 'Notes' (3), and 'History' (2). Below the tabs is a search bar with the text '67 Vulnerabilities'. The main table lists vulnerabilities with columns for 'Sev', 'CVSS', 'VPR', 'Name', 'Family', and 'Count'. The vulnerabilities are sorted by severity, with 'CRITICAL' items at the top. The 'VNC Server 'password' Password' vulnerability is no longer present. On the right side, there is a 'Scan Details' panel showing the scan policy, status, severity base, scanner, start/end times, and elapsed time. Below the scan details is a 'Vulnerabilities' section with a donut chart showing the distribution of vulnerabilities by severity.

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
MIXED	Apache Tomcat (Multiple Issues)	Web Servers	4
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3
MIXED	SSL (Multiple Issues)	Service detection	3
HIGH	7.5		NFS Shares World Readable	RPC	1
HIGH	7.5 *	6.7	rlogin Service Detection	Service detection	1

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v2.0
- Scanner: Local Scanner
- Start: Today at 6:58 AM
- End: Today at 7:20 AM
- Elapsed: 22 minutes

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

(assenza del VNC SERVER vulnerability)

- NFS EXPORTED SHARE INFORMATION DISCLOSURE

L’NFS esposeva i dati perche nel file di configureazione cera una riga esposta. Togliendo quella riga l’NFS non si espone piu.

```
GNU nano 2.0.7 File: /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)
```

L’ultima riga è stata commentata per contenere il problema.

Scannerizzando possiamo vedere che anche in questa occasione si risolve il problema.

billy

[Back to My Scans](#) Configure Audit Tra

Hosts 1 Vulnerabilities 66 Remediations 2 Notes 3 History 3

Filter Search Vulnerabilities 66 Vulnerabilities

<input type="checkbox"/>	Sev	CVSS	VPR	Name	Family	Count	
<input type="checkbox"/>	CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	
<input type="checkbox"/>	CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1	
<input type="checkbox"/>	MIXED	Apache Tomcat (Multiple Issues)	Web Servers	4	
<input type="checkbox"/>	CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	
<input type="checkbox"/>	MIXED	SSL (Multiple Issues)	Service detection	3	
<input type="checkbox"/>	HIGH	7.5 *	6.7	rlogin Service Detection	Service detection	1	
<input type="checkbox"/>	HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1	
<input type="checkbox"/>	MIXED	SSL (Multiple Issues)	General	28	
<input type="checkbox"/>	MIXED	ISC Bind (Multiple Issues)	DNS	5	

(assenza del NFS)

● BIND SHELL BACKDOOR DETECTION

Questa vulnerabilità è data al fatto che probabilmente un blackhat possa accedere a questa porta esposta così da poter attaccare.

Abbiamo attivato il firewall perché era spento, e abbiamo applicato una regola: “deny 1524” perché era la porta esposta, ora è una porta quasi obsoleta dato che controllava il DBMS di Ingres Corporation. Dato che ora si usano di più metodi come MySQL.

Chiudendola abbiamo chiuso la entrata per la backdoor.

Scannerizzando possiamo vedere che ora non appare più.

The screenshot shows the Billy security scanner interface. The main panel displays a list of vulnerabilities under the 'Vulnerabilities' tab. The filter is set to 'ba', showing 7 of 63 vulnerabilities. The table lists the following items:

Sev	CVSS	VPR	Name	Family	Count	Actions
CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1	Info / Edit
MISC	7.5	6.7	Samba Badlock Vulnerability	General	1	Info / Edit
INFO			Unknown Service Detection: Banner Retrieval	Service detection	4	Info / Edit
INFO			Backported Security Patch Detection (FTP)	General	1	Info / Edit
INFO			Backported Security Patch Detection (WWW)	General	1	Info / Edit
INFO			Samba Server Detection	Service detection	1	Info / Edit
INFO			Samba Version	Misc.	1	Info / Edit

On the right, the 'Scan Details' panel shows: Policy: Basic Network Scan, Status: Completed, Severity Base: CVSS v3.0, Scanner: Local Scanner, Start: Today at 9:21 AM, End: Today at 9:43 AM, Elapsed: 22 minutes. Below this is a 'Vulnerabilities' donut chart showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

(assenza del BIND BACKDOOR)