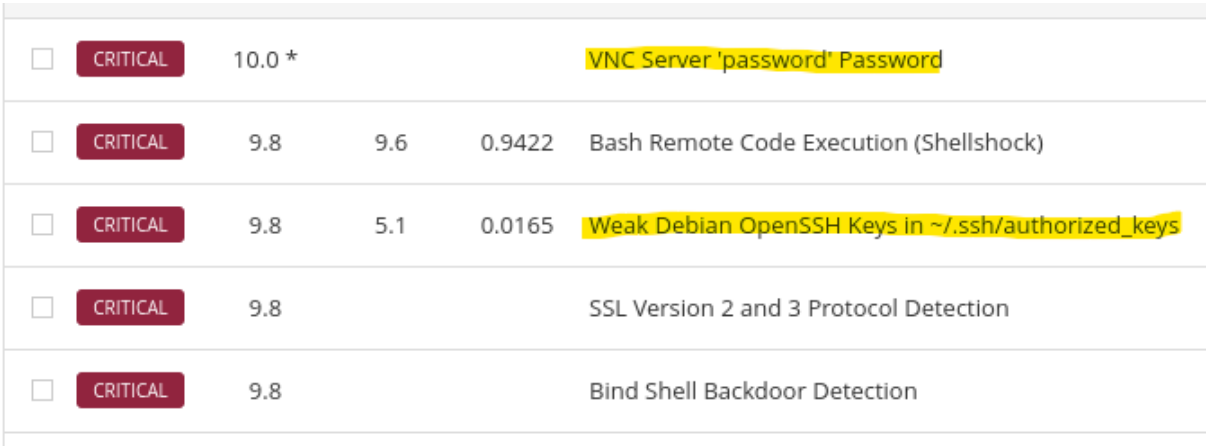
W12D4 - Progetto



☐	CRITICAL	10.0 *			VNC Server 'password' Password
☐	CRITICAL	9.8	9.6	0.9422	Bash Remote Code Execution (Shellshock)
☐	CRITICAL	9.8	5.1	0.0165	Weak Debian OpenSSH Keys in ~/.ssh/authorized_keys
☐	CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection
☐	CRITICAL	9.8			Bind Shell Backdoor Detection

per risolvere le vulnerabilità evidenziate ho eseguito la remediation da parte di Nessus:

per la vulnerabilità del servizio VNC, ho cambiato la password dal comando “vncpasswd“ e poi riavviato il servizio con vncserver.

per invece la vulnerabilità della chiave authorized_keys, ho modificato copiandolo da id_rsa.pub, *cp .ssh/id_rsa.pub .ssh/authorized_keys*

extra: non mi appariva la vulnerabilità dell’NFS dove chiedeva di disattivare il servizio, l’ho disattivato per prova, con il comando /etc/init.d/nfs(sia common che kernel) stop