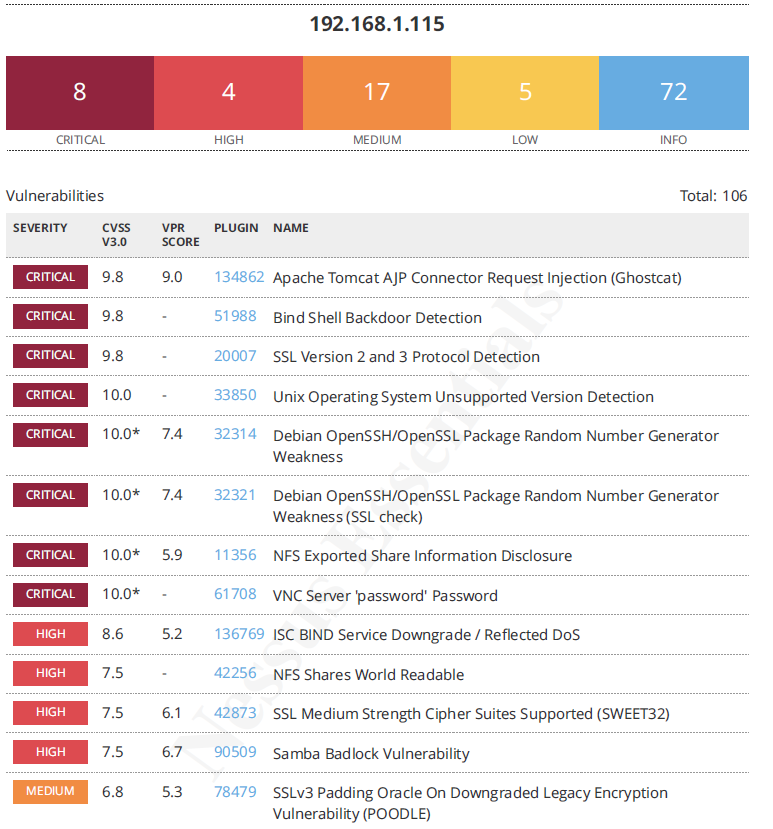
**Vulnerability scan and remediation**

**Andrea Volterra**

**Target: Metasploitable**

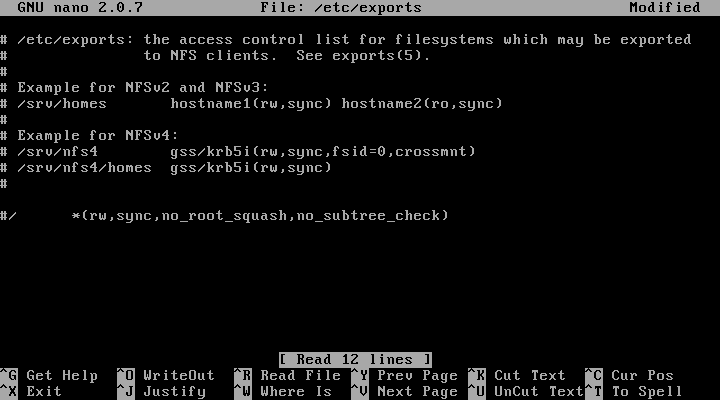
**SCANSIONE NESSUS PRELIMINARE**

****

**VULNERABILITY REMEDIATION METASPLOITABLE**

****

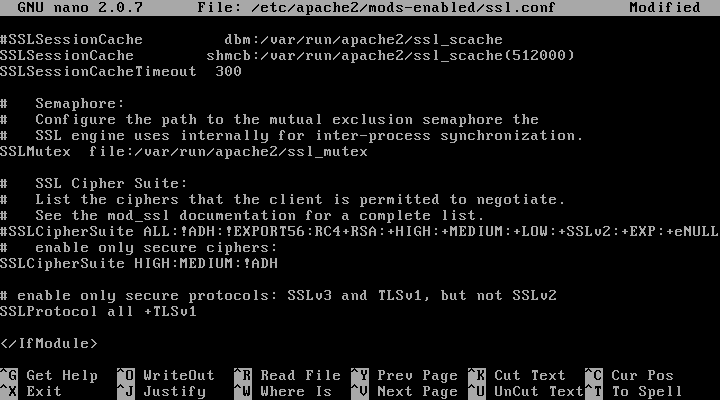
**La directory root viene rimossa tramite commento sulla riga relativa nel file exports**

****

****

**Avvio prima il servizio SSL**

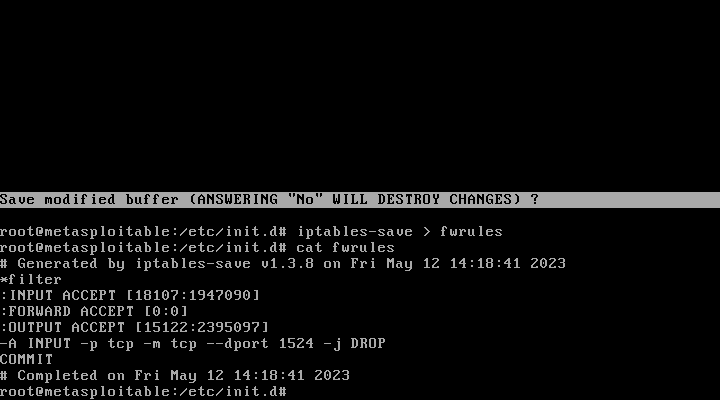
****

**Per poi modificare il file ssl.conf, disabilitando il protocollo SSL per attivare il TLS**

****

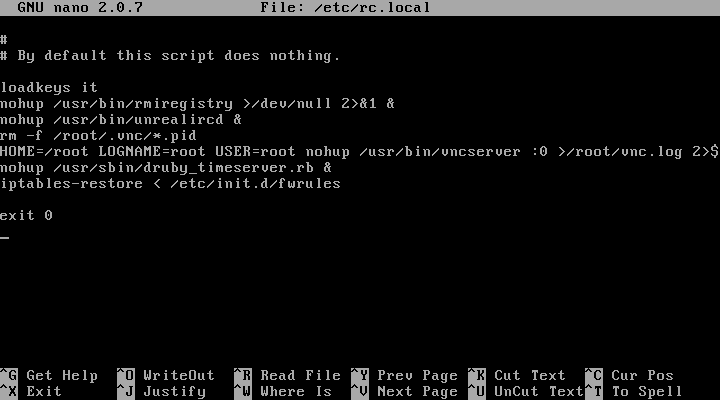
**Imposto la regola firewall che rifiuta il traffico sulla porta 1524 con il comando:**

*iptables -A INPUT -p tcp –dport 1524 -j DROP*



**E salvo la regola nel file fwrules all’interno della directory /etc/init.d**

**Per caricare la regola ad ogni boot modifico il file rc.local inserendo la stringa**

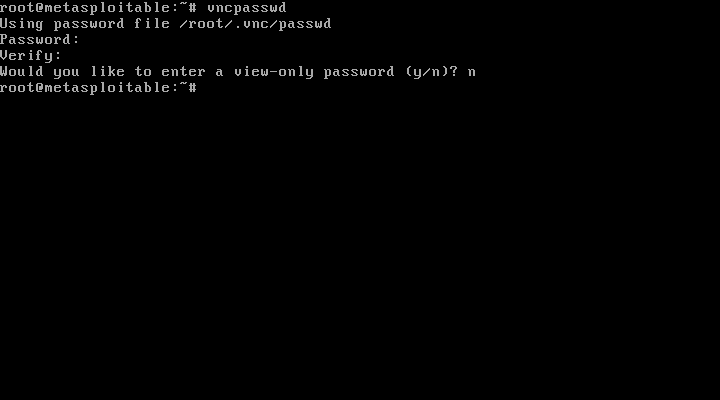
*Iptables-restore </etc/init.d/fwrules* ****

**Disattivo anche i servizi shell, telnet e exec commentandoli sul file inetd.conf nella directory /etc/**

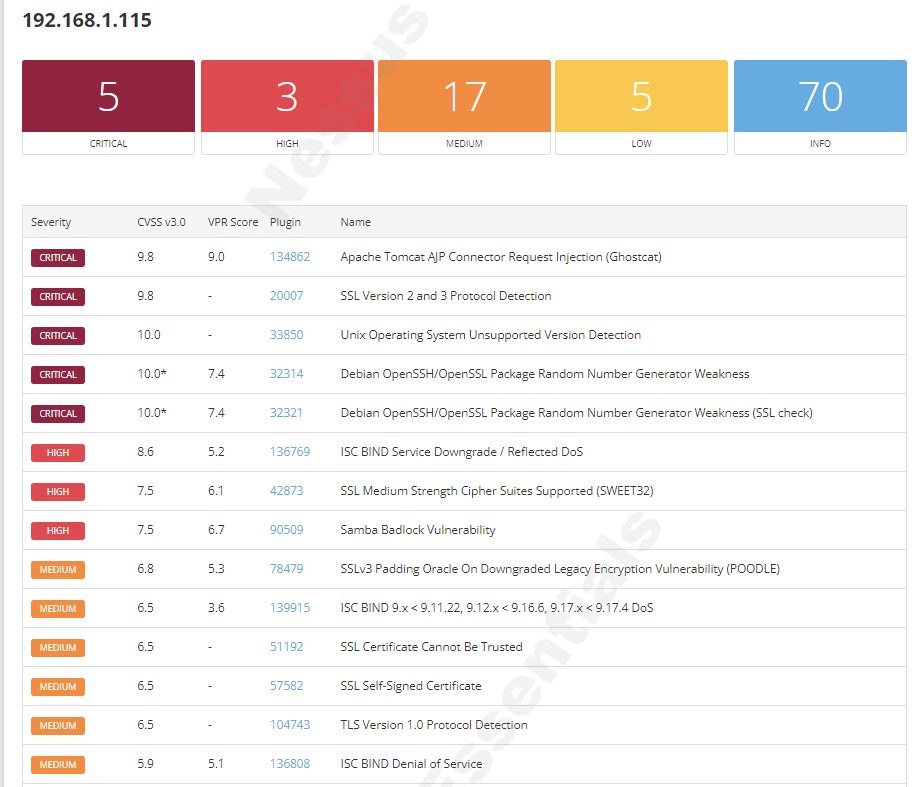
****

****

**Per risolvere la vulnerabilità della password di VNC modifico il file passwd nella directory /root/.VNC/**

****

**VULNERABILITY SCAN POST FIX**

****