**ANTRO FABIO MARCELLO** **BENCHMARK M3**

## CSPT 0524

## Vulnerabilità risolte:

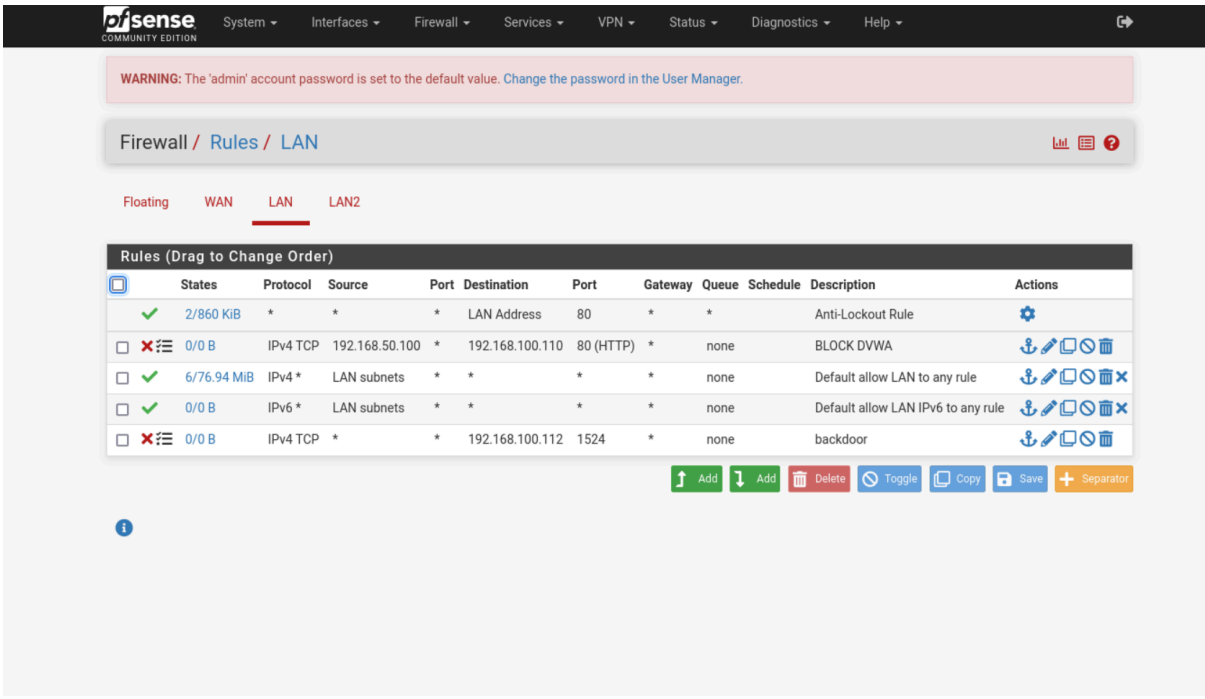
1. **Apache Tomcat AJP Connector Request Injection (Ghostcat) (CVE-2020-1938)**

Sono entrato nel file server.xml di tomcat5.5 e ho commentato la stringa riguardante la porta 8009 come segue, disabilitando il connettore:


Poi, ho restartato Tomcat utilizzando il comando “init.d”.

2. **Bind Shell Backdoor Detection (porta 1524)**
   - Rilevata nel primo report (09/02/2025) come una backdoor che permetteva l'accesso remoto non autenticato.
   - Nel secondo report (10/02/2025), questa vulnerabilità non compare più, il che indica che la backdoor è stata rimossa.

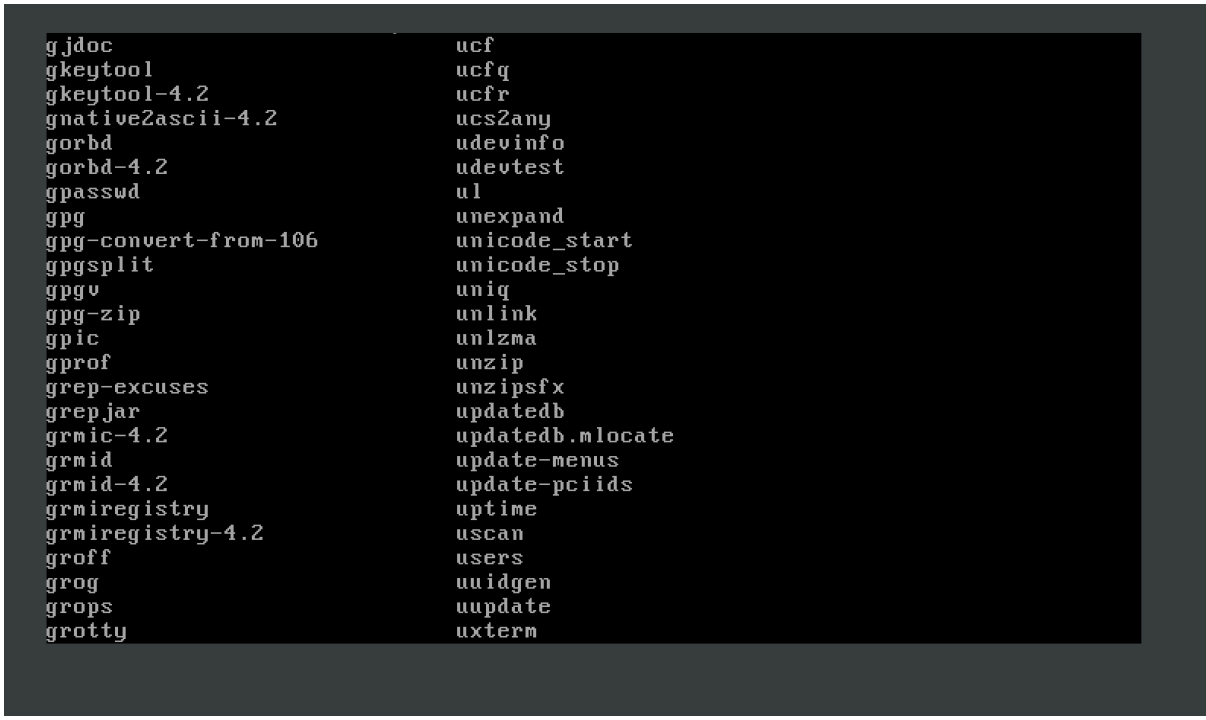
Ho inserito una regola firewall su pfsense come da screen per bloccare la porta 1524:

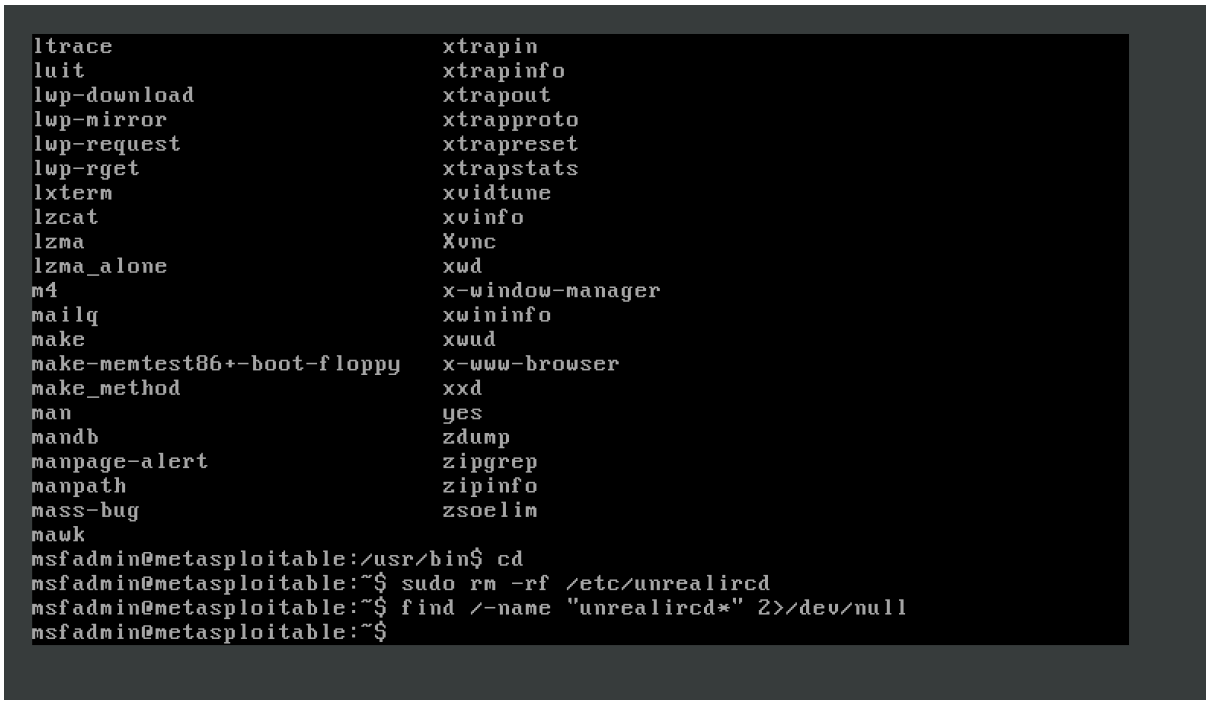


3.**UnrealIRCd Backdoor Detection (porta 6667)**

- Presente nella prima scansione, indicava la presenza di una versione compromessa di UnrealIRCd.
- Non più presente nel secondo report.

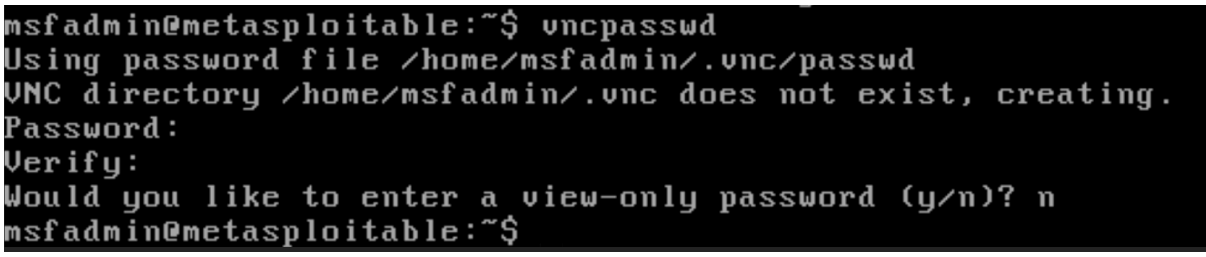
Ho rimosso unrealircd, killando il processo ed eliminando tutti i file del sw.



4.**VNC Server con password debole ("password") (porta 5900)**

- La prima scansione segnalava l'accesso remoto tramite VNC con la password di default.
- Nella seconda scansione, questa vulnerabilità non compare più, perché ho cambiato la password VNC, killato il processo, restartato il servizio con il comando “init.d” facendolo partire sul display 0 con il comando:”vncserver :0”




VULNERABILITA’ RISOLTE: 4