EPICODE

Andrea Rocca
CSPT0323

Cybersecurity Analyst

Week 12 - W12D4

M3: Progetto Remediations

VULNERABILITÀ PRESE IN ESAME

LIVELLO	CVSS	NOME
CRITICA	10.0	NFS Exported Share Information Disclosure
CRITICA	10.0	VNC Server 'password' Password
CRITICA	9.8	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICA	9.8	Bind Shell Backdoor Detection

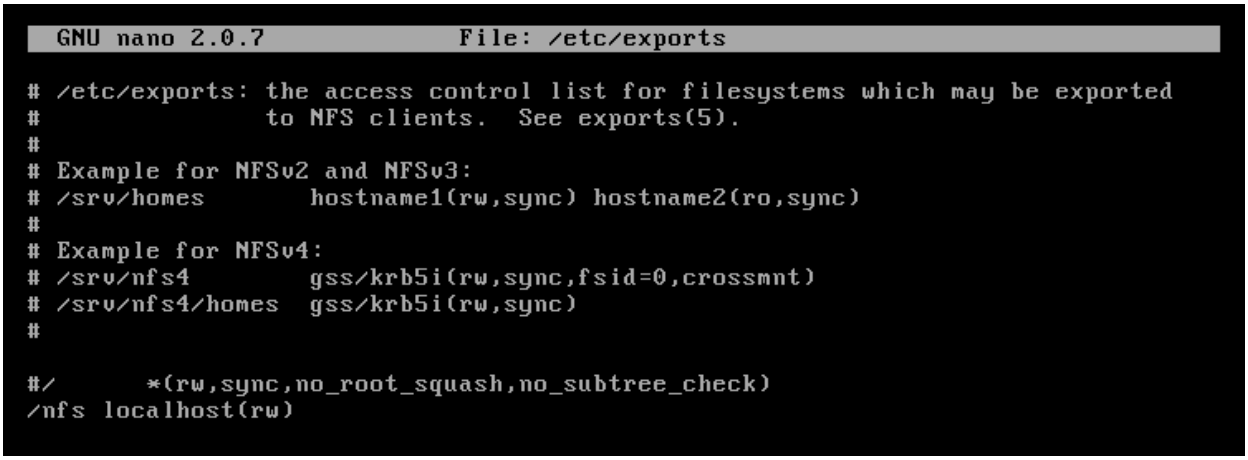
NFS Exported Share Information Disclosure

It is possible to access NFS shares on the remote host.
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.

CORREZIONE VULNERABILITÀ

La vulnerabilità in oggetto è stata corretta attraverso la limitazione dell'accesso alle condivisioni NFS solo al localhost sulla macchina Metasploitable.

- Modifica del file **/etc/exports**, aggiungendo una riga che specifica che solo il localhost (192.168.40.100) ha l'autorizzazione in lettura/scrittura (rw) sulla condivisione NFS.



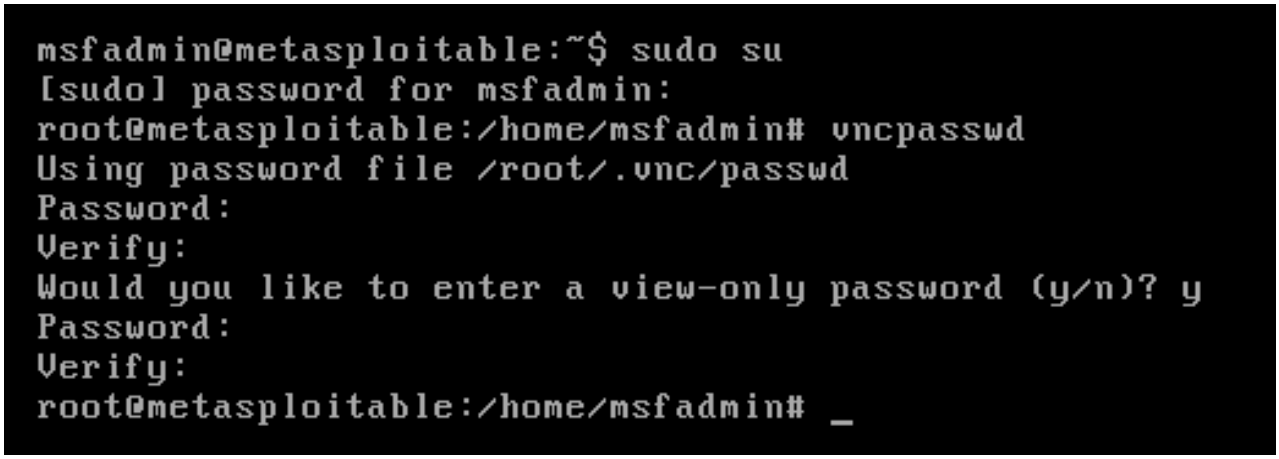
VNC Server 'password' Password

A VNC server running on the remote host is secured with a weak password (“password”).
A remote, unauthenticated attacker could exploit this to take control of the system.

CORREZIONE VULNERABILITÀ

Per risolvere la vulnerabilità della password debole del server VNC su Metasploitable, sono state eseguite le seguenti azioni:

- Eseguito l'accesso come superuser con il comando **sudo su**
- Cambiata la password del server VNC con il comando **vncpasswd**



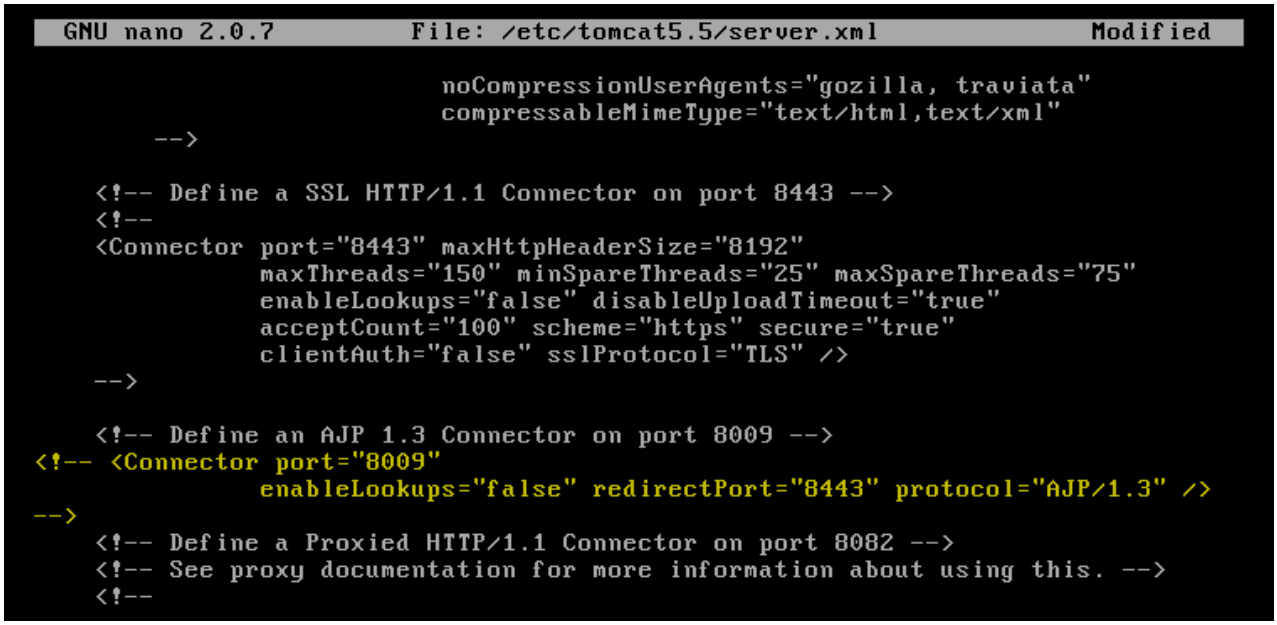
Apache Tomcat AJP Connector Request Injection (Ghostcat)

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

CORREZIONE VULNERABILITÀ

La vulnerabilità in oggetto è un problema di sicurezza noto che può consentire a un attaccante remoto di eseguire attacchi di lettura di file, incluso l'accesso a file di configurazione sensibili. Per risolvere questa vulnerabilità, è possibile aggiornare Apache Tomcat o (come in questo caso) disabilitare l'utilizzo di AJP connector, componente deprecato e rimosso negli ultimi aggiornamenti.

- Commentata la riga relativa al connector in oggetto nel file **server.xml**



Bind Shell Backdoor Detection

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

CORREZIONE VULNERABILITÀ

La vulnerabilità in oggetto indica la presenza di un servizio di shell remota (bind shell) sulla porta TCP 1524. Per mitigare questa vulnerabilità, è possibile aggiungere una regola firewall che blocca le connessioni in entrata per la porta in questione (qualora quest'ultima non sia necessaria per altri servizi).

- Aggiunta della regola firewall per chiudere la porta 1524 tramite comando:
  sudo iptables -A INPUT -p tcp --dport 1524 -j DROP