

## Report interventi effettuati (Modulo 3, Master Cybersecurity)

### VNC Server 'password' Password

Il Server VNC ha bisogno di una password per autenticare il client, per evitare vulnerabilità ho aggiornato la password pre-esistente (password), con una nuova, per farlo ho eseguito i seguenti passaggi:

Modificato il file contenete la password:

nano ~/.vnc/config

```
GNU nano 2.0.7      File: /home/msfadmin/.vnc/passwd      Modified
GNU nano 2.0.7      File: /home/msfadmin/.vnc/passwd

Authentication=UncAuth
Encryption=AlwaysOn
PasswordFile=~/.vnc/passwd
```

Una volta modificata la password ho salvato il file e fatta la kill vncServer per effettuare il riavvio:

```
[ Wrote 3 lines ]

msfadmin@metasploitable:~$ vncserver /kill :1
TightVNC server version 1.2.9
```

Riavviato il server con la nuova password:

```
-pixelformat bgr<NNN>

See tightvncserver and Xtightvnc manual pages for more information.
msfadmin@metasploitable:~$ vncserver :1
xauth:  creating new authority file /home/msfadmin/.Xauthority

New 'X' desktop is metasploitable:1

Creating default startup script /home/msfadmin/.vnc/xstartup
Starting applications specified in /home/msfadmin/.vnc/xstartup
Log file is /home/msfadmin/.vnc/metasploitable:1.log
msfadmin@metasploitable:~$ _
```

## Apache Tomcat AJP connector Request Injection (Web Servers)

Apache Tomcat AJP accetta connessioni da tutti i client se non viene specificato il contrario all'interno server.xml

Una volta dentro la cartella di tomcat, ho modificato il file server.xml, per la connessione alla porta 8009 evitando connessioni dall'esterno, bloccando così eventuali minacce.

```
        acceptCount="100" scheme="https" secure="true"
        clientAuth="false" sslProtocol="TLS" />
    -->

    <!-- Define an AJP 1.3 Connector on port 8009 -->
    <Connector port="8009"
        enableLookups="false" redirectPort="8443" protocol="AJP/1.3">
        <Deny from="all" />
    </Connector>
    <!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
    <!-- See proxy documentation for more information about using this. -->
    [ Wrote 385 lines ]

msfadmin@metasploitable:/etc/tomcat5.5$
```