Informe Técnico — Laboratorio de Ingeniería Social

Resumen de la herramienta utilizada

LaZagne es una herramienta de post-explotación diseñada para extraer credenciales almacenadas localmente en sistemas Windows, Linux y macOS. Funciona analizando las configuraciones de aplicaciones comunes (navegadores, clientes de correo, bases de datos, etc.) y recuperando contraseñas en texto plano, hashes o tokens. En este laboratorio, se utilizó LaZagne en conjunto con **Meterpreter**, un payload de Metasploit que permite ejecución remota en la máquina víctima.

⚠️ Riesgos identificados

1. **Extracción silenciosa de credenciales** sin interacción del usuario.
2. **Persistencia del atacante** mediante payloads ocultos.
3. **Acceso remoto completo** a la máquina comprometida.
4. **Uso de herramientas legítimas** para fines maliciosos (Living off the Land).
5. **Dificultad de detección** si no se cuenta con monitoreo avanzado.

🧪 Pasos ejecutados en la demostración

1. Preparación de entorno virtual con Kali Linux y Windows 8.1.
2. Instalación de dependencias y clonación de LaZagne.
3. Generación de payload .exe con msfvenom.
4. Compartición del archivo vía Samba y ejecución en Windows.
5. Activación del handler en Kali con msfconsole.
6. Ejecución remota de LaZagne desde sesión Meterpreter.
7. Extracción de credenciales y recuperación de resultados.

🛡️ Recomendaciones de defensa y detección

1. **Implementar AppLocker o Software Restriction Policies** para bloquear ejecución de binarios desconocidos.
2. **Monitorear conexiones salientes** con IDS/IPS (ej. Suricata) para detectar tráfico de reverse shells.
3. **Auditar carpetas compartidas** y restringir acceso desde máquinas no autorizadas.
4. **Utilizar EDR con firmas de comportamiento** para detectar ejecución de herramientas como LaZagne.
5. **Aplicar segmentación de red y privilegios mínimos** para limitar el movimiento lateral y el acceso a credenciales.