LABORATORIO N°3

PASO 1 Identificar el Vector de Ataque Inicial

El phishing es una técnica de ciberdelito que utiliza ingeniería social para engañar a usuarios y obtener información confidencial, como contraseñas, datos bancarios o información personal. Funciona mediante el envío de correos electrónicos falsos o mensajes que simulan ser de una entidad legítima, como un banco o una red social, para inducir al usuario a revelar datos personales o descargar malware

#	Escenario	Tipo de Ataque	Resumen del Ataque	Solución Propuesta
1	**La trampa del correo legítimo**	Spear Phishing + Credential Harvesting	El atacante suplanta a un proveedor y envía un correo con un enlace a una web falsa para robar credenciales.	- Activar 2FA. - Filtros anti-phishing y sandboxing en correo. - Capacitación al personal. - Monitorear y bloquear accesos sospechosos.
2	**El PDF silencioso**	Ataque de Día Cero (Zero-Day Exploit)	Se envía un archivo PDF malicioso que explota una vulnerabilidad no parchada para ejecutar un backdoor.	- Mantener software actualizado. - Abrir adjuntos en entornos aislados. - Usar EDR con detección por comportamiento. - Control de ejecución de aplicaciones.
3	**El pendrive olvidado**	Ataque USB (BadUSB)	Un USB infectado se deja en la oficina. Al conectarlo, ejecuta un payload que da acceso remoto al atacante.	- Desactivar puertos USB. - Soluciones de control de dispositivos. - Políticas de concientización. - Sistemas DLP para control de datos.
4	**El empleado resentido**	Amenaza interna (Insider Threat)	Un exempleado usa credenciales activas para	- Desactivar cuentas al finalizar relación laboral.

			robar datos sensibles y venderlos en la dark web.	- Auditorías de accesos y permisos. - SIEM con alertas de comportamiento anómalo. - Aplicar principio de mínimo privilegio.
5	**El falso sitio seguro**	DNS Spoofing + Man-in-the-Middle	El atacante altera el router para redirigir tráfico hacia sitios falsos que roban credenciales.	- Usar DNSSEC y segmentar red de administración. - Validar HTTPS con HSTS. - IDS/IPS para detectar tráfico anómalo. - Proteger configuración del router.
6	**La cadena de cifrado**	Ransomware dirigido	Acceso a red por VPN expuesta. El atacante despliega ransomware que cifra sistemas clave y exige rescate.	- MFA en VPN y desactivar accesos innecesarios. - Backups inmutables. - Segmentación de red. - EDR con protección contra ransomware. - Plan de respuesta a incidentes.

Paso 2: Analizar los Logs del Sistema para Encontrar Evidencias de Actividad Maliciosa

Sistema	Tipo de Log	¿Qué se debe buscar / identificar?
Servidor de Correo Electrónico	**Logs de envío/recepción (SMTP, etc.)**	**Correos con enlaces sospechosos, dominios falsos, actividad fuera de horario.**
	Logs de autenticación	**Inicios de sesión fallidos, logins desde IPs inusuales, cambios en configuración del buzón.**
	Análisis de encabezados (headers)	**Errores en SPF/DKIM/DMARC, campos "Reply-To" alterados, codificación rara.**
Sistema de Base de Datos	**Logs de consultas (query logs)**	**Consultas masivas o inusuales, extracción de datos fuera de horario, patrones de scraping.**
	Logs de actividad de usuarios	**Cambios de roles, creación de usuarios, accesos con privilegios elevados.**
	Logs de conexión	**Conexiones desde IPs desconocidas o externas, sesiones persistentes anómalas.**
	Logs de cambios estructurales	**Modificaciones de tablas, triggers sospechosos, comandos como xp_cmdshell.**
Sistemas de Seguridad / Terminales	**Logs de EDR / Antivirus**	**Ejecución de procesos sospechosos (cmd, powershell), alertas de malware, intentos de cifrado masivo.**
	Logs del firewall / IDS	**Conexiones salientes a IPs maliciosas, escaneos internos, tráfico no habitual.**
	Logs del sistema operativo	**Eventos de login (ID 4624, 4625), creación/eliminación de usuarios (ID 4720, 4726), cambios de servicios.**