Ejercicio 1

Un atacante ha logrado acceder a un entorno corporativo. Con base en información de un incidente anterior, se sabe que el atacante utilizó las siguientes tácticas y técnicas:

Tactic	Technique	MITRE ID
Initial Access	Spearphishing Attachment	T1566.001
Execution	User Execution: Malicious File	T1204.002
Persistence	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001
Privilege Escalation	Process Injection: Dynamic-link Library Injection	T1055.001
Defense Evasion	Obfuscated Files or Information: Command Obfuscation	T1027.010
	Impair Defenses: Disable or Modify Tools	T1562.001
	Indicator Removal on Host	T0872
Credential Access	OS Credential Dumping: LSASS Memory	T1003.001
Lateral Movement	Use Alternate Authentication Material: Pass the Hash	T1550.002
	Remote Services: SMB/Windows Admin Shares	T1021.002
Impact	Data Encrypted for Impact	T1486

Instrucciones del Ejercicio

1. **Objetivo:**
   Usando **MITRE ATT&CK Navigator**, identifica y resalta las tácticas y técnicas relacionadas con este ataque. Luego, analiza qué técnicas tienen cobertura en tus herramientas actuales y cuáles no.
2. **Pasos a seguir:**
   - **Paso 1:** Accede a **MITRE ATT&CK Navigator** (enlace).
   - **Paso 2:** Selecciona la matriz correspondiente a **Enterprise**.
   - **Paso 3:** Crea una capa personalizada.
     - Resalta las técnicas indicadas anteriormente.
     - Usa colores para representar diferentes categorías:

        - **Verde:** Técnicas detectadas actualmente por tus herramientas.
        - **Amarillo:** Técnicas parcialmente cubiertas o detectadas de manera limitada.
        - **Rojo:** Técnicas sin cobertura.
    - **Paso 4:** Analiza los resultados:
        - Identifica las áreas donde el equipo azul necesita mejorar su detección.
        - Propón al equipo rojo un plan para simular estas técnicas en ejercicios futuros.
3. **Resultados esperados:**
    - Un mapa visual que muestre las técnicas utilizadas en el ataque.
    - Identificación de brechas de seguridad en las defensas actuales.
    - Planes de acción para mejorar la colaboración entre los equipos.