Write-Up: Reto Exfiltración

Descripción del Reto

Pues lo que dice el título. Durante una auditoría, se ha encontrado una captura de red en uno de nuestros servidores, y parece contener el tráfico de uno de nuestros empleados al servidor de la empresa... Al parecer, este empleado tenía una contraseña que aparecía en una filtración y nunca la ha cambiado.

Archivo Proporcionado

Se entrega un fichero de captura de red que debe ser analizado utilizando **Wireshark**.

Resolución

1. **Abrir el archivo en Wireshark**:
    - Se carga el fichero en Wireshark para comenzar el análisis de los paquetes capturados.
2. **Identificación de protocolos relevantes**:
    - Dado que el título del reto menciona "Exfiltración", se comienza analizando protocolos relacionados con transferencia de datos como **HTTP**, **DNS**, y **SMB2**.
    - En el tráfico HTTP se observa una contraseña en texto plano “estoesunacontraseña, soy un genio\n” dentro de un `HTTP GET`. Sin embargo, se descarta como parte de la solución, ya que el objetivo es encontrar una *flag*, no una contraseña para ingresar en algún sistema.
3. **Análisis del protocolo SMB2**:
    - Tras revisar otros protocolos, se identifica tráfico relacionado con SMB2 (Server Message Block).

- Dentro de una petición `SMB2 WRITE`, en el apartado **Data**, se encuentra un bloque hexadecimal sospechoso:

```
68666374667b5230634b7930555f6e5f683473686334745f7730303030306f306f306f303
06f303021212121213131317d0a
```

4. **Conversión del contenido hexadecimal**:
   - El bloque hexadecimal se convierte a texto ASCII utilizando herramientas como CyberChef o scripts simples en Python. La conversión revela la siguiente cadena:

```
hfctf{R0cKy0U_n_h4shc4t_w00000o0o0o00o00!!!!!1111}
```

5. **Método alternativo: strings + grep**:
   - Otra forma rápida y directa de obtener la *flag* es utilizando el comando `strings` para extraer cadenas legibles del archivo y luego filtrar las que contienen "hfctf" con `grep`. El comando sería:

```
strings archivo.pcap | grep "hfctf"
```

   - Esto imprime directamente la *flag* sin necesidad de analizar los protocolos manualmente.

Flag Encontrada

La *flag* es:

```
hfctf{R0cKy0U_n_h4shc4t_w00000o0o0o00o00!!!!!1111}
```