Lezly Dialid Cerón Rodríguez

Prueba de Concepto – Explotación de Stack BufferOverflow

La aplicación iSmartViewPro 1.5 es un software de videovigilancia.

Se replicó el exploit iSmartViewPro 1.5 - 'Password' Buffer Overflow con los siguientes pasos:

Se ejecutó el siguiente código en Python para obtener la cadena a pasar como argumento:

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-
buffer = "\x41" * 447
eip = "\x42" * 4
f = open ("generate.txt", "w")
f.write(buffer + eip)
f.close()
```

Este Código genera una cadena compuesta por 447 A que corresponden al tamaño del buffer, y 4 B que corresponden a la dirección a sustituir del eip.

El programa utiliza una función de comparación de cadenas vulnerable a bufferoverflow lo que hace posible este ataque.

Una vez que hemos generado la cadena, abrimos la aplicación iSmartViewPro.

Damos clic en el botón “+”

Seleccionamos “add device manually”

En device alias escribimos “admin”

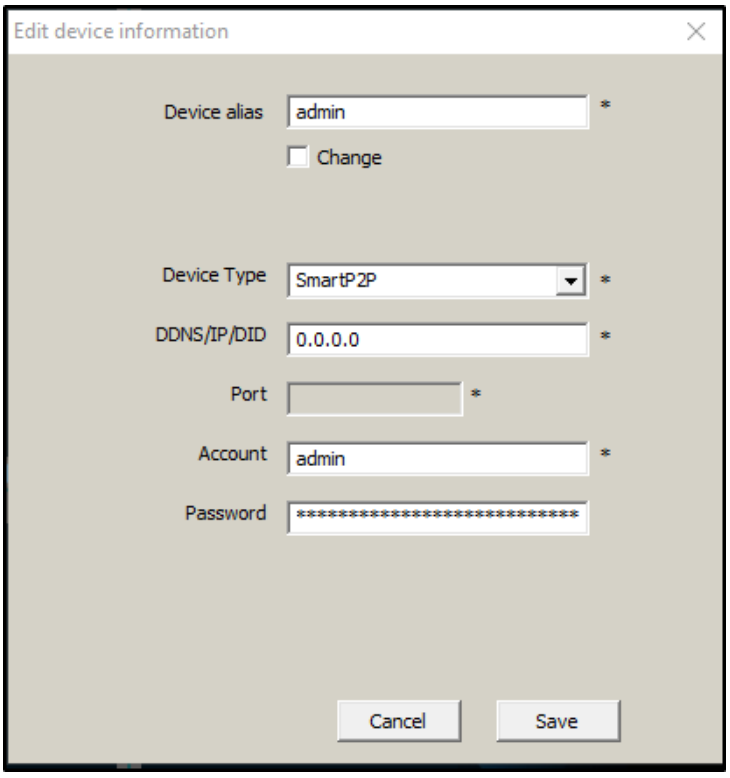
En DNS/IP/DID “0.0.0.0”

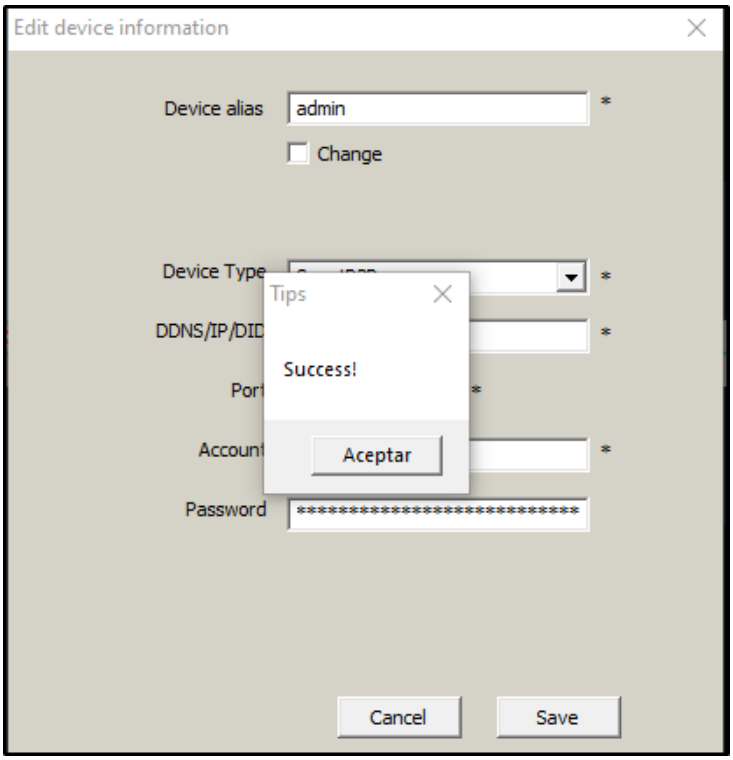
En account “admin”

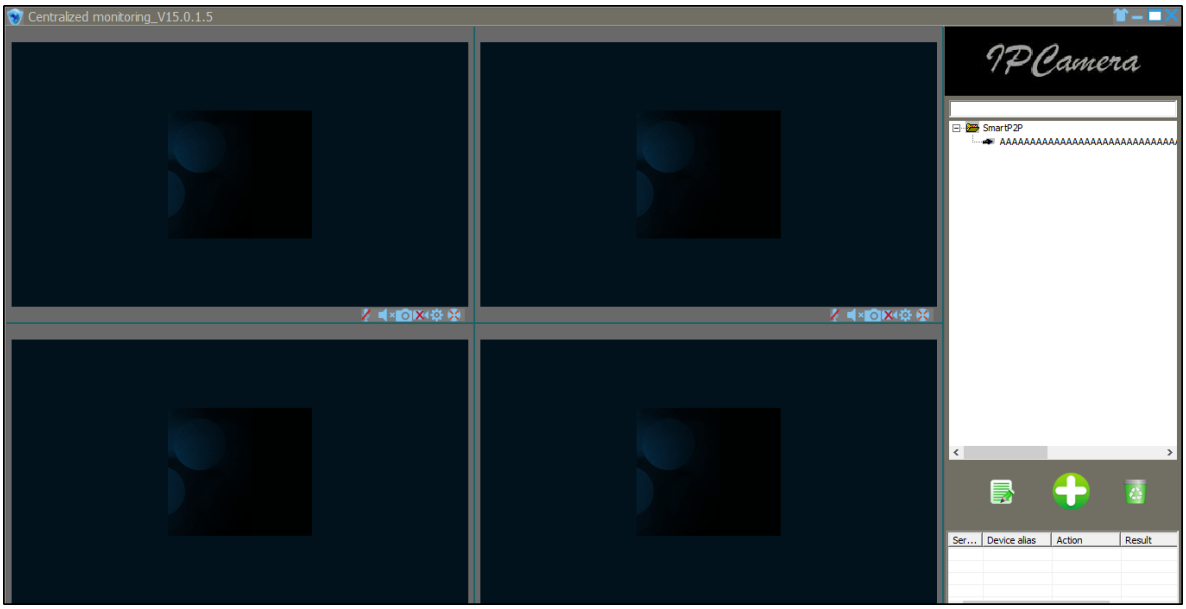
Y en “password” pegamos la cadena que hemos generado.

Damos clic en save.

Lezly Dialid Cerón Rodríguez







Y se crea el dispositivo con los datos proporcionados, en este caso observamos que se conservan las AAAA proporcionadas para el buffer, sin embargo eip fue sustituido por “\x42\x42\x42\x42”.

Internamente ocurrió un buffer overflow que, aunque en este caso sólo redirige a “\x42\x42\x42\x42”, potencialmente puede redirigir a la dirección de memoria de otra instrucción.