



Universidad
Francisco de
Vitoria

*Centro de
Documentación
Europea*

UFV Madrid

Caso práctico de Shodan

1. Posible PLC o sistema SCADA accesible: 3
2. Servidor RDP público:..... 5
3. Dispositivos con firmware desactualizado: 7


1. Posible PLC o sistema SCADA accesible:

Esta búsqueda encuentra dispositivos de la empresa en el puerto 502

El que vamos a analizar es el de la siguiente imagen.

166.148.196.183

Verizon Business

 United States, Crozet

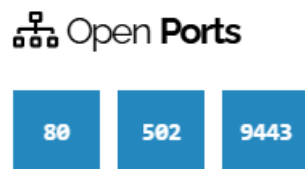
ics

Podemos observar el país, ciudad etc.

General Information

Country	United States
City	Crozet
Organization	Verizon Business
ISP	Verizon Business
ASN	AS6167

A continuación vemos todos los puertos que hay abiertos.



- Riegos observados en el banner (Puerto 502/TCP):
 - Exposición del Modbus a internet.
 - Cualquiera que encuentre este host en Shodan puede enviar comandos Modbus directamente al dispositivo o al PLC conectado detrás del bridge.
 - Si el dispositivo controla algún equipo industrial un atacante podría leer registros de procesos, escribir valores en registros y por lo tanto alterarlos y provocar fallos en sistemas SCADA.

```
// 502 / TCP

Unit ID: 0

Unit ID: 1

Unit ID: 255
-- Device Identification: Modbus/TCP to RTU Bridge Bridge V3.3.25.0RC6
```

- Recomendaciones:
 - Bloquear el acceso público al puerto modbus.
 - Aislar el dispositivo de la red.
 - Restringir acceso a host solo autorizados.

2. Servidor RDP público:

Esta búsqueda nos muestra los dispositivos de la empresa que tienen el puerto 3389 abierto que este puerto corresponde al RDP por defecto (Escritorio remoto).

Port:3389 org:"Verizon Business"

Q

Vamos a analizar el de la siguiente imagen.

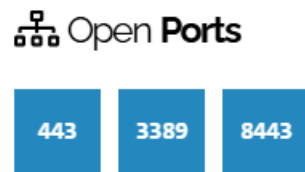
166.167.176.212
Verizon Business
 United States, Santa Ana
self-signed

observamos el hostname, país, ciudad, el sistema operativo etc.

General Information

Country	United States
City	Santa Ana
Organization	Verizon Business
ISP	Verizon Business
ASN	AS6167
Operating System	Windows (build 10.0.14393)

Como podemos ver solo hay tres puertos abiertos en esta ip.



- Riesgos observados en el banner (3389/TCP)
 - El RDP está expuesto por lo que puede ser un buen objetivo para los atacantes.
 - Se muestran usuarios reales lo que puede facilitar ataques de fuerza bruta.
 - Se muestra que el equipo está unido a un dominio I, esto puede llevar a que si se compromete esa maquina con privilegios del dominio un atacante podría escalar privilegios en la red corporativa.
 - El sistema operativo no está actualizado (Windows 10 Server versión 1607).

// 3389 / TCP 1929304744 | 2025-10-27T11:01:19.102

Remote Desktop Protocol

Remote Desktop Protocol

\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00

Remote Desktop Protocol NTLM Info:

OS: Windows 10 (version 1607)/Windows Server 2016 (version 1607)

OS Build: 10.0.14393

Target Name: VEH2326

NetBIOS Domain Name: VEH2326

NetBIOS Computer Name: VEH2326

DNS Domain Name: VEH2326

FQDN: VEH2326

CONDUENT

CONDUENT Pye

IVU 4000

I

omens: VU 4000

JO URC 0 Wile



- Recomendaciones
 - Bloquear el acceso RDP público.
 - Permitir conexiones desde una vpn o una red interna segura.
 - Revisar los accesos a logs para ver posibles intentos de accesos sospechosos.
 - Cambiar las contraseñas y revisar los usuarios expuestos.
 - Actualizar el sistema operativo.


3. Dispositivos con firmware desactualizado:

Esta búsqueda nos muestra los dispositivos NAS QNAP de la empresa que tienen el firmware en la versión 4.3.6.

os:"QTS 4.3.6" org:"Verizon Business"




Vamos a analizar el de la siguiente imagen.

96.235.19.98 

pool-96-235-19-98.pitbpa.fios.verizon.net

Verizon Business

 United States, Coraopolis

observamos el hostname, país, ciudad, el sistema operativo etc.

General Information

Hostnames	pool-96-235-19-98.pitbpa.fios. verizon.net
Domains	<div>verizon.net</div>
Country	United States
City	Coraopolis
Organization	Verizon Business
ISP	Verizon Business
ASN	AS701
Operating System	QTS 4.3.6

Como podemos ver solo hay un puerto abierto en esta ip.

Open Ports



- Riesgos observados en el banner (8080/TCP)
 - Interfaz de administración web expuesta por HTTP.
 - Se muestra el modelo (TS-231), la versión del firmware (4.3.6).
 - App filestation expuesta.

// 8080 / TCP 

QNAP TS-231 4.3.6

```
HTTP/1.1 200 OK
Date: Sun, 26 Oct 2025 11:03:43 GMT
Server: http server 1.0
X-Frame-Options: SAMEORIGIN
Content-type: text/html; charset=UTF-8
Last-modified: Wed, 19 Jun 2024 04:31:13 GMT
Accept-Ranges: bytes
Content-length: 580
Vary: Accept-Encoding
```

```
QNAP TS-231:
  Hostname: RYFTCLOUD-2
  Model:
    Model Name: TS-X31
    Display Model Name: TS-231
    Platform: TS-NASARM
    Platform Ex: ARM_MS
  Firmware:
    Version: 4.3.6
    Number: 2805
    Build: 20240619
  Apps:
    Filestation:
      Version: 5.1.0
      Build: 20240619
```

- Recomendaciones
 - Aislar el acceso, permitir acceso solo desde la red interna de la empresa.
 - Habilitar HTTPS.
 - Actualizar el firmware a una versión 5.x
 - Revisar las credenciales y cambiarlas.
 - Bloquear automáticamente ips después de varios intentos fallidos.
 - Activar notificaciones por correo o app movil de inicios de sesion.
 - Minimizar la información expuesta como ocultar versiones.



Universidad
Francisco de
Vitoria

*Centro de
Documentación
Europea*

UFV Madrid