*Como tu RAS Gateway Secure revela el espacio de direccionamiento interno de la organización*

*Amador Aparicio (@amadapa)*

[Parallels RAS](https://www.parallels.com/es/products/ras/remote-application-server/?utm_source=google&utm_medium=cpc&creative=372603343563&keyword=ras%20parallels&matchtype=e&network=g&device=c&gclid=CjwKCAiA8ov_BRAoEiwAOZogwc9HrPj-7Xu7JC_venObXOHHHarjd2UU7KcdMEsPmjzkgn5g42TxnRoCz3QQAvD_BwE), *Remote Application Server*, es una solución de entrega de aplicaciones e infraestructura de escritorio virtual (VDI) que permite a empleados y clientes de una organización acceder y utilizar aplicaciones, escritorios y datos desde cualquier dispositivo, gracias a las capacidades de virtualización que ofrece.

## Arquitectura RAS

En la siguiente figura muestra un escenario en el que el *RAS* *Secure Gateways* *HTML5 Portal* se implementan en la DMZ. El *RAS Secure Gateway* reenviará las peticiones vía HTTP a un host de sesión de escritorio remoto, RAS RD, que tendrá instalada la función de *Servicios de Escritorio Remoto* (RDS). Como se aprecia, el host RDP se encuentra dentro de la LAN de la organización, aunque también cabría la posibilidad de que estuviese dentro de una DMZ y así reducir la superficie de exposición de los activos de la red interna de la organización.

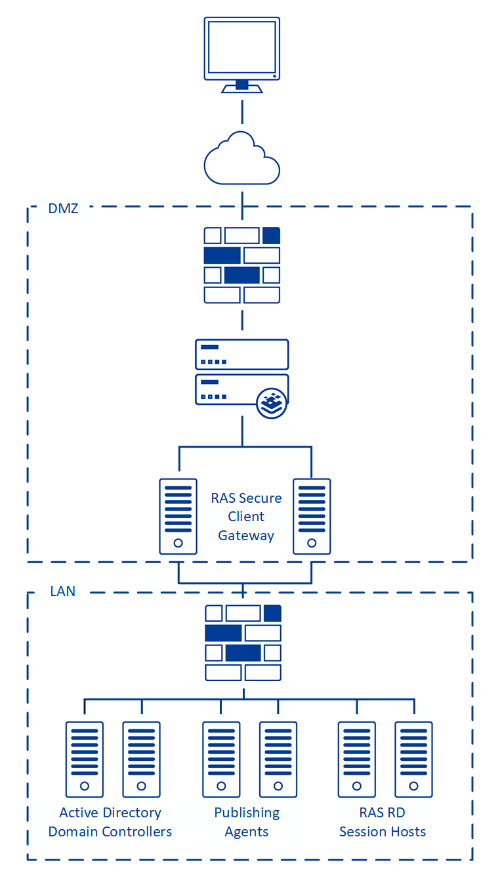


Figura 1. Arquitectura de red para una infraestructura Parallels RAS Secure Gateway y RAS RD.

## Búsqueda de Parallels Remote Application Server

Buscar dispositivos RAS HTML5 Gateway accesibles desde Internet es relativamente sencillo. Basta consultar [guía de administración del dispositivo](http://download.parallels.com/ras/docs/v15.5/en_US/Parallels-RAS-v15-5-Administrators-Guide/42080.htm) para poder extraer patrones de las URLs.



Figura 2. Guía de administración del dispositivo con información de las URL de acceso.

Como se ve en la imagen, las URLs de acceso a estos dispositivos tienen presentes las singularidades “/RASHTML5Gateway/” y “/RASHTML5Gateway/#/login”, lo que facilita en gran medida la localización del formulario de acceso de estos dispositivos conectados en Internet haciendo un poco de Hacking con Buscadores.

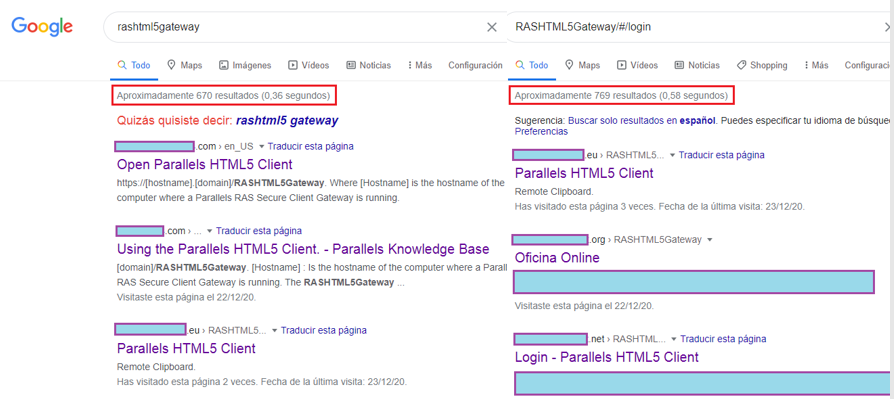


Figura 3. Resultados de las búsquedas con las singularidades en la URL.

Se observa que sin mucho esfuerzo en la realización de un dorking, Google ofrece un buen número de resultados relacionador con el formulario HTML5 de acceso al portal web de los dispositivos.

## Análisis del tráfico HTTP generado por el RAS de Parallels

Uno de aspectos más importantes en cualquier *pentest* o auditoría relacionada con sistemas web, sean del tipo que sean, es analizar las peticiones y respuestas HTTP para ver si el dispositivo revela información interesante que, a simple vista, y sin la ayuda de un proxy HTTP, podría pasar desapercibida. Para ello se selecciona uno de los resultados devueltos por Google y se observa que el formulario del RAS solicita en el campo del *login* un usuario centralizado un *Active Directory* (*user@domain*) y un password.

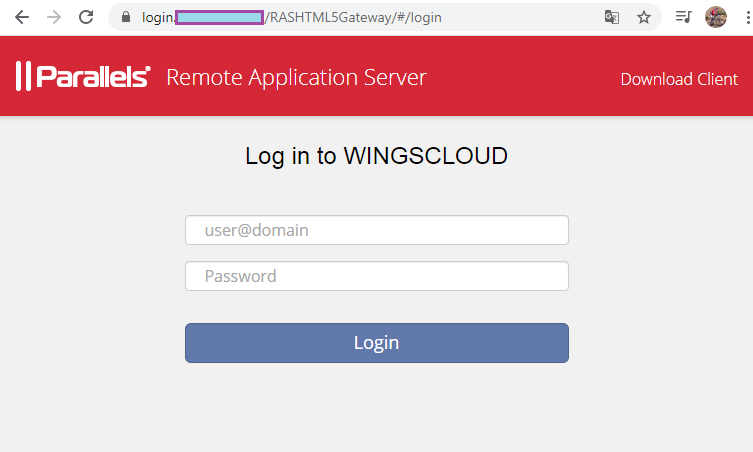


Figura 4. Formulario de acceso al RAS de Parallels.

Utilizando ZAProxy, se observa como al pulsar directamente sobre le botón *login*, sin la necesidad de introducir un user@domain con contraseña, el RAS Secure Gateway genera una petición HTTP por POST al RAS RD donde releva cuál es su dirección IPv4.

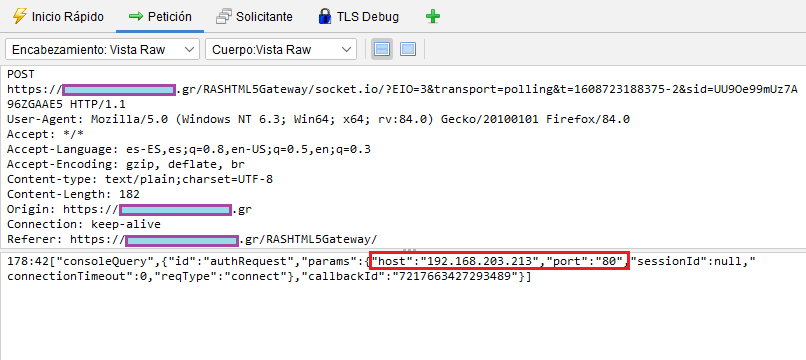


Figura 5. Dirección IPv4 del RAS RD que recibe las peticiones de los recursos de virtualización.

Si el RAS RD se encuentra en la red interna de la organización, el espacio de direccionamiento IPv4 de la organización estaría quedando expuesto. En el mejor de los casos, si el RAS RD se encuentra en una zona desmilitarizada (DMZ), su espacio de direccionamiento IPv4 estaría quedando expuesto.

## Cómo minimizar la fuga de información

Consultado la [información ofrecida por el fabricante](https://support.kemptechnologies.com/hc/en-us/articles/360043257011-Parallels-Remote-Application-Server-RAS-), cabe la posibilidad de que el *RAS Secure Gateway* pueda realizar las funciones de RAS RD dentro de la misma máquina. Como la máquina es la misma, todas las peticiones HTTP hacia los recursos virtualizados podrían realizarse sobre “localhost”. El resultado para este escenario sería el siguiente:

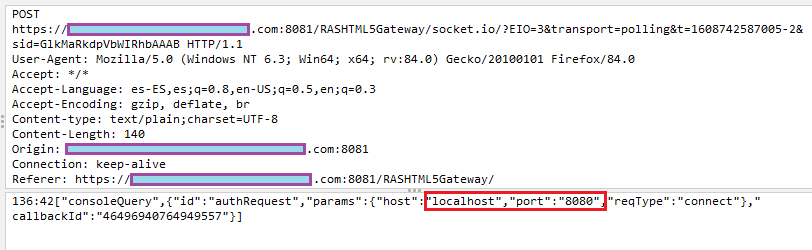


Figura 6. Petición HTTP desde el servicio del RAS Secure Gateway hacia el servicio RAS RD en la propia máquina.

La dirección IPv4 del RAS RD no estaría siendo revelada, pero sí que se estarían revelando los puertos TCP relacionados con el servicio *RAS Secure Gateway* (8080/TCP) y el RAS RD (8081/TCP).

En el caso de que el *RAS Secure Gateway* y el RAS RD se encuentren en redes diferentes, parece muy complicado eliminar la fuga de información presentada en este artículo, debido a que el *RAS Secure Gateway* tiene que realizar una petición HTTP por POST para comunicarse con el RAS RD.

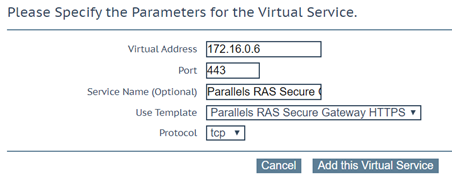


Figura 7. Opciones de configuración del RAS Secure Gateway para referenciar al RAS RD.

Autor: [Amador Aparicio](https://mypublicinbox.com/AmadorAparicio) ([@amadapa](https://twitter.com/amadapa)), escritor de los libros “[Raspberry Pi para Hackers & Makers: PoCs & Hacks Just for Fun!](https://0xword.com/es/libros/172-raspberry-pi-para-hackers-makers-pocs-hacks-just-for-fun.html)” y "[Hacking Web Technologies 2ª Edición](https://0xword.com/es/libros/81-hacking-web-technologies.html)" , CSE (*Chief Security Envoy*) de [ElevenPaths](https://www.elevenpaths.com/).