UT01: Adopción de pautas de seguridad informática - Vulnerabilidades

Nombre: Francisco Jesús García – Uceda Díaz - Albo
Curso: 2º ASIR.

Índice

c) Realiza un breve informe referente a:

- ¿Qué es un exploit? Formas de protegerse.

Un exploit es un programa o código que se aprovecha de agujero de seguridad (vulnerabilidad) en una aplicación o sistema, un atacante podría aprovechar está vulnerabilidad para conseguir control total del sistema.

Un ejemplo muy bueno es el que nos tiene la página welivesecurity (ESET Security): "Trasladado a la vida real, sería como si un modelo de cerradura (sistema o aplicación) tuviera un fallo de diseño que nos permitiera crear llaves que la abrieran (exploit) y poder así acceder al sitio que trata de proteger y realizar actos delictivos (malware)."

Tras dicho esto, nos podemos proteger de las siguientes maneras:

- Mantener todas nuestras aplicaciones y sistemas actualizados: sabiendo que los exploits se aprovechan de los agujeros de seguridad, resulta vital cerrarlos cuanto antes.
- Mitigar los efectos de posibles exploits usados en nuestra contra. Puede suceder que el fabricante del sistema o aplicación vulnerable no haya lanzado todavía una actualización que solucione el problema. En este caso, se pueden utilizar herramientas como el Kit de herramientas de Experiencia de Mitigación mejorada (EMET) para Windows.
- Navegar de forma segura y estar al corriente de las últimas noticias.
- Tener sentido común y adquirir hábitos de seguridad informática.
- Tener un antivirus instalado que nos proporcione una capa de seguridad extra y actualice el software de forma automática.

- Tipos de exploits.

- **Exploit remoto:** Si utiliza una red de comunicaciones para entrar en contacto con el sistema víctima. Por ejemplo, puede usar otro equipo dentro de la misma red interna o tener acceso desde la propia Internet.

- **Exploit local:** Si para ejecutar el exploit se necesita tener antes acceso al sistema vulnerable. Por ejemplo, el exploit puede aumentar los privilegios del que lo ejecuta. Este tipo de exploits también puede ser utilizado por un atacante remoto que ya tiene acceso a la máquina local mediante un exploit remoto.

- **Exploit en cliente:** Aprovechan vulnerabilidades de aplicaciones que típicamente están instaladas en gran parte de las estaciones de trabajo de las organizaciones. Ejemplos típicos de este tipo de software son aplicaciones ofimáticas (p. ej. Microsoft Office, Open Office), lectores de PDF (p. ej. Adobe Acrobat Reader), navegadores (p. ej. Internet

Explorer, Firefox, Chrome, Safari), reproductores multimedia (p. ej. Windows Media Player, Winamp, iTunes). El exploit está dentro de ficheros interpretados por este tipo de aplicaciones y que llega a la máquina objetivo por distintos medios (p. ej. mediante un correo o en una memoria USB). El archivo será usado por el programa y si no es detenido por ningún otro programa (p. ej. cortafuegos o antivirus) aprovechará la vulnerabilidad de seguridad.

- ¿Qué es Metasploit?

Metasploit es un proyecto de código abierto para la seguridad informática, que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración "Pentesting" y el desarrollo de firmas para sistemas de detección de intrusos.

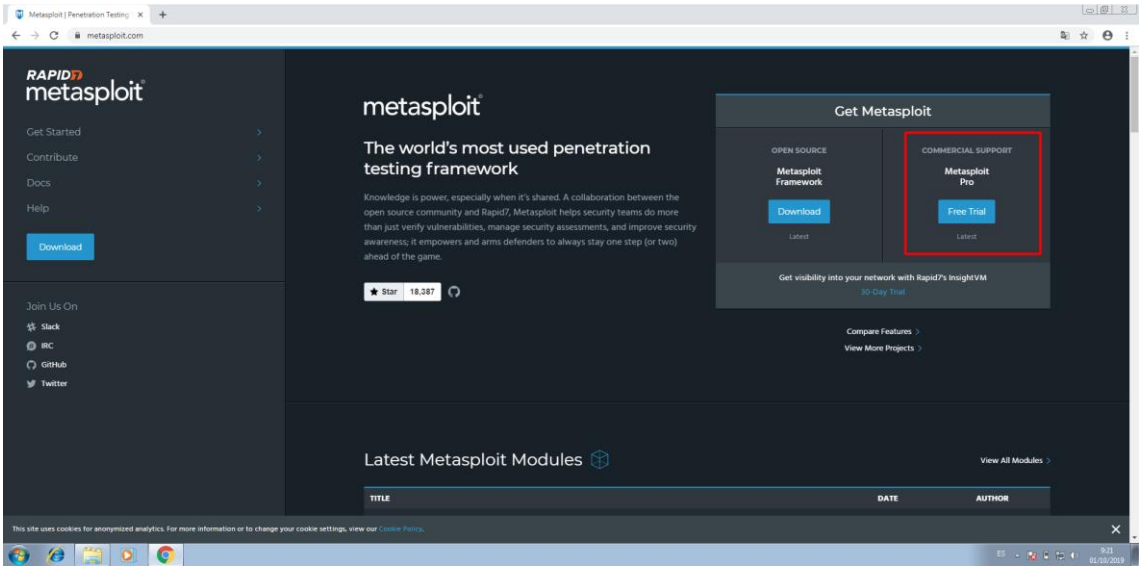
Metasploit Framework, es una de las herramientas más utilizadas por los auditores de seguridad. Incluye una gran colección de exploits, a parte de proporcionale un entorno de desarollo para los propios exploits. esta herramienta también es muy utilizada por los auditores de seguridad debido a su fácil implementación con otras herramientas como nmap, escaners de vulneravilidades, etc.

Podemos destacar como sus características principales:

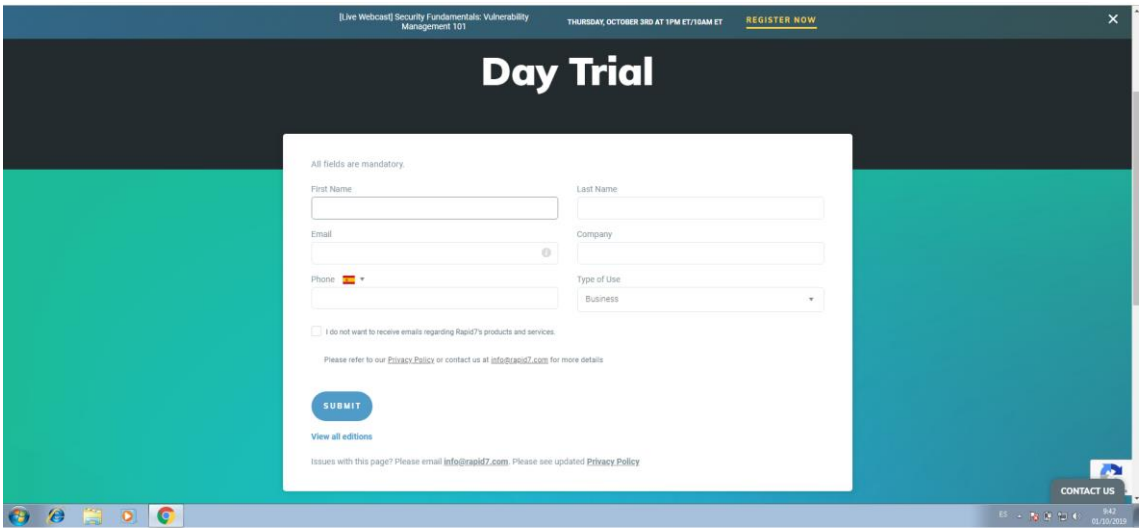
- Es una herramienta muy completa que tiene muchísimos exploits, que son vulnerabilidades conocidas, en las cuales tienen también unos módulos, llamados payloads, que son los códigos que explotan estas vulnerabilidades.
- También dispone de otros tipos de módulos, por ejemplo, los encoders, que son una especie de códigos de cifrado para evasión de antivirus o sistemas de seguridad perimetral.
- Otra de las ventajas de este framework es que nos permite interactuar también con herramientas externas, como Nmap o Nessus.
- Además, ofrece la posibilidad de exportar nuestro malware a cualquier formato, ya sea en sistemas Unix o Windows.
- Es multiplataforma y gratuito, aunque tiene una versión de pago, en la que se nos ofrecen exploits ya desarrollados, pero cuyo coste es bastante elevado. La versión gratuita es muy interesante porque contiene todas las vulnerabilidades públicas.

- Utiliza Metasploit para intentar descubrir vulnerabilidades en tu PC local o en tu red.

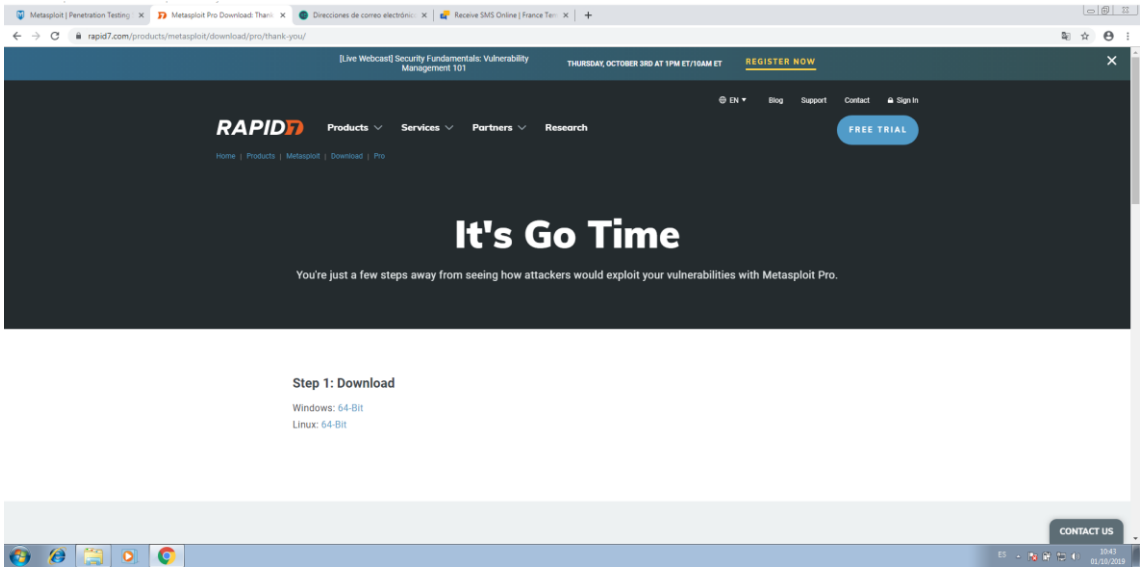
Lo primero que haremos será descargar Metasploit desde la página oficial, en este caso **probaremos Metasploit Pro** para compararlo con Nessus o NMAP: Link.



Completamos con nuestros datos personales para que nos envíen una clave.

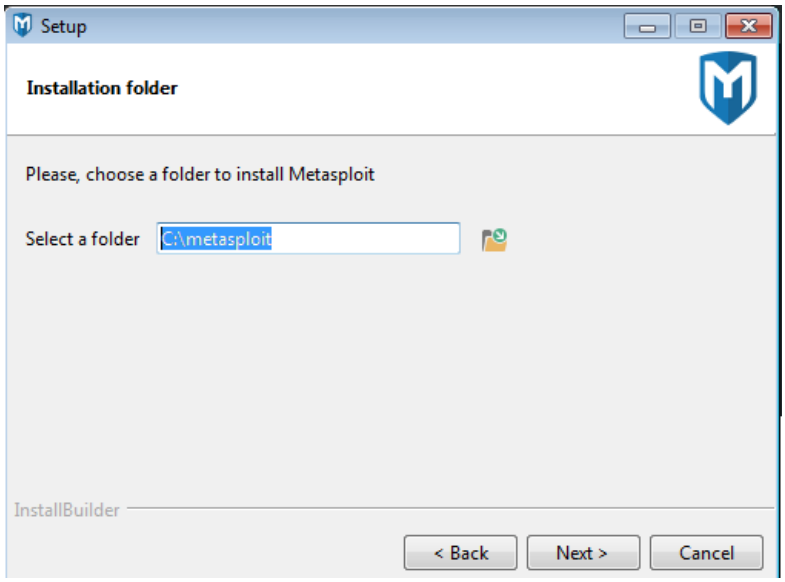


Descargamos el archivo necesario para nuestro sistema operativo.

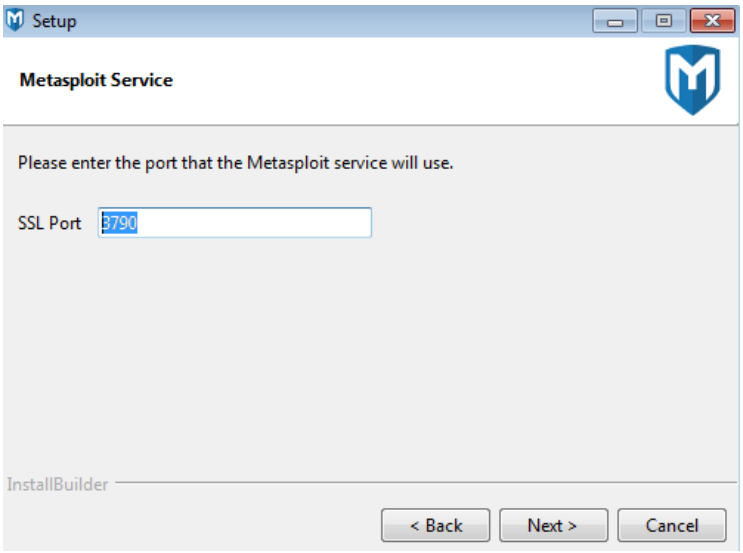


Aceptamos los términos y condiciones:

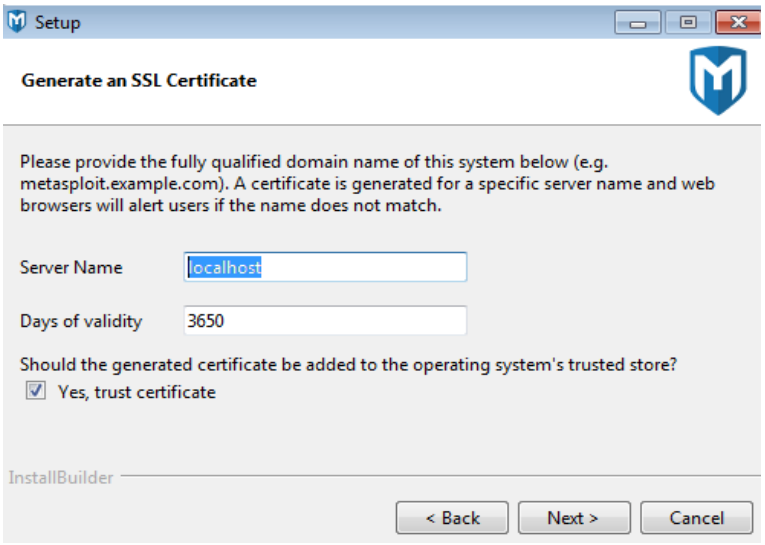
Escogemos la ruta de instalación.



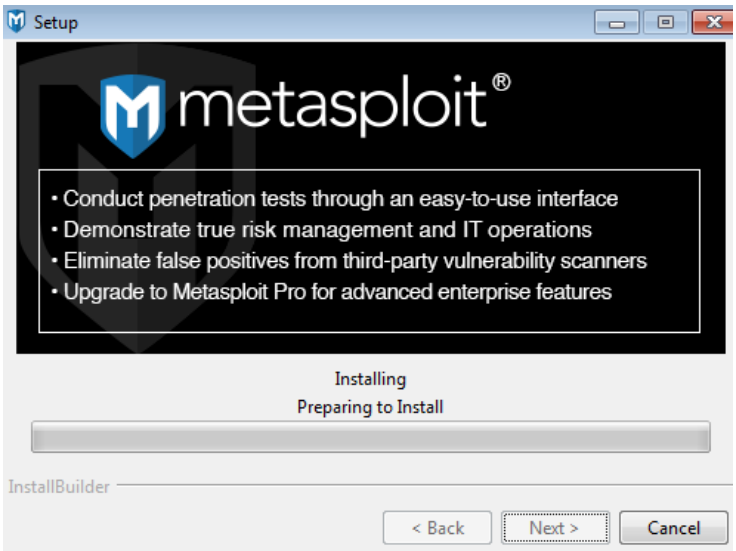
Dejaremos por defecto el puerto SSL.



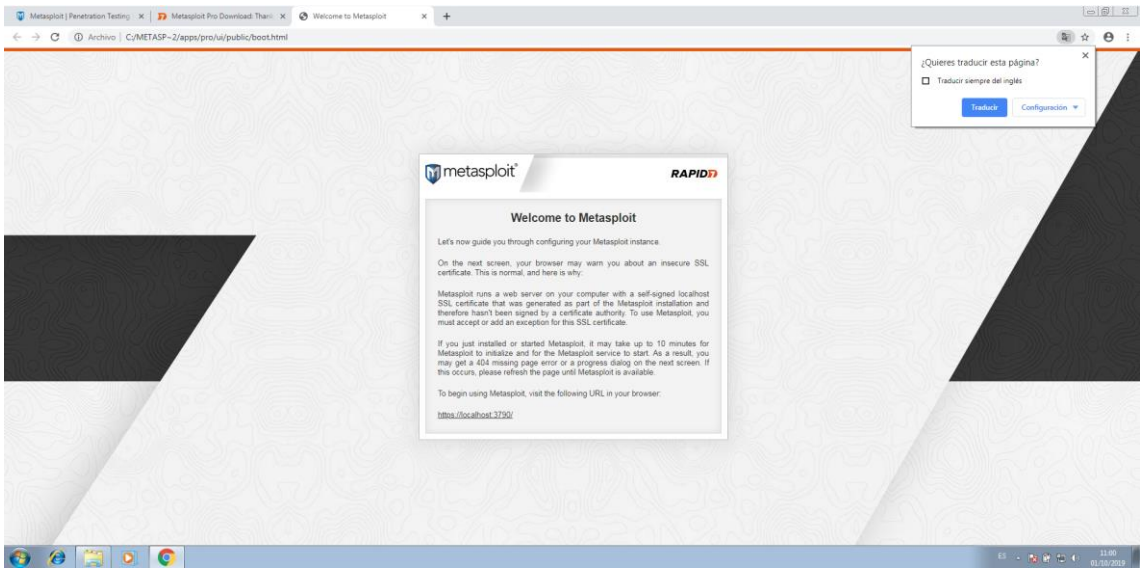
Dejamos los datos del certificado SSL por defecto.



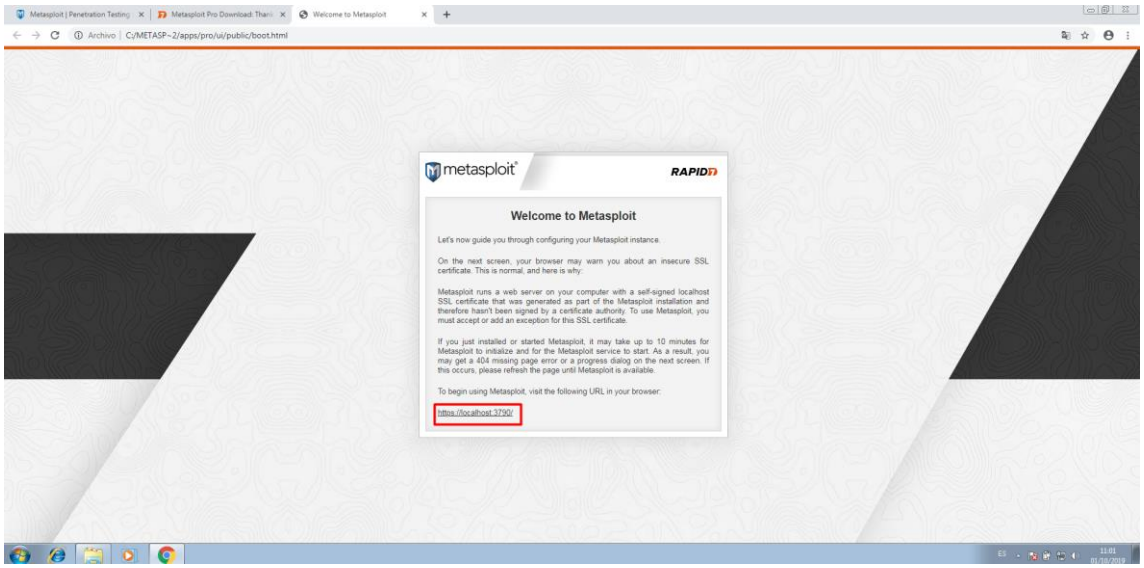
Esperamos a que se instale.



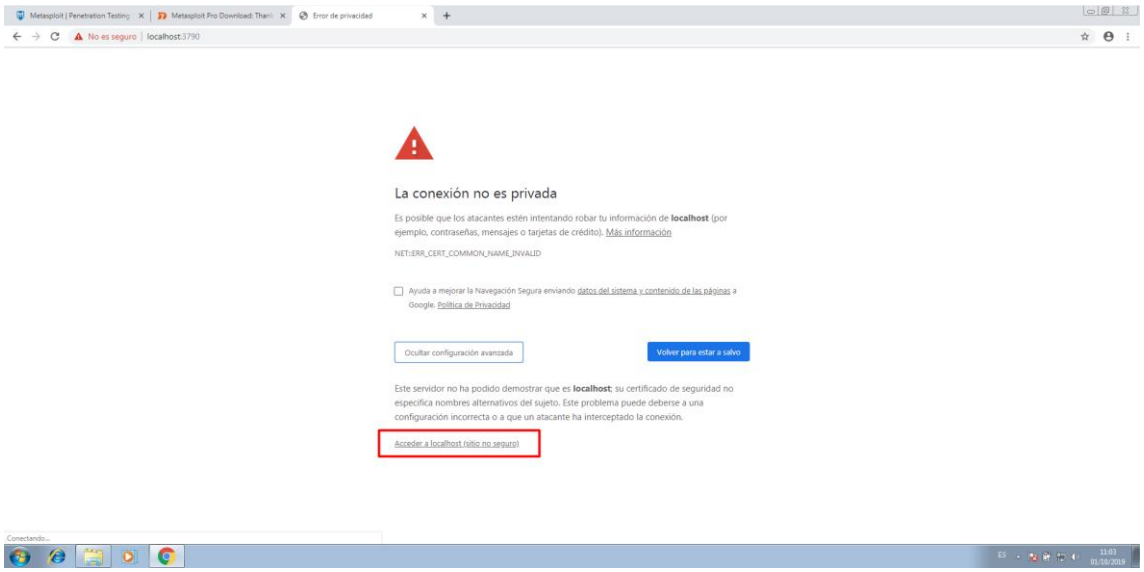
Una vez finalizado se nos abrirá el navegador web predeterminado en localhost entrando a Metasploit.



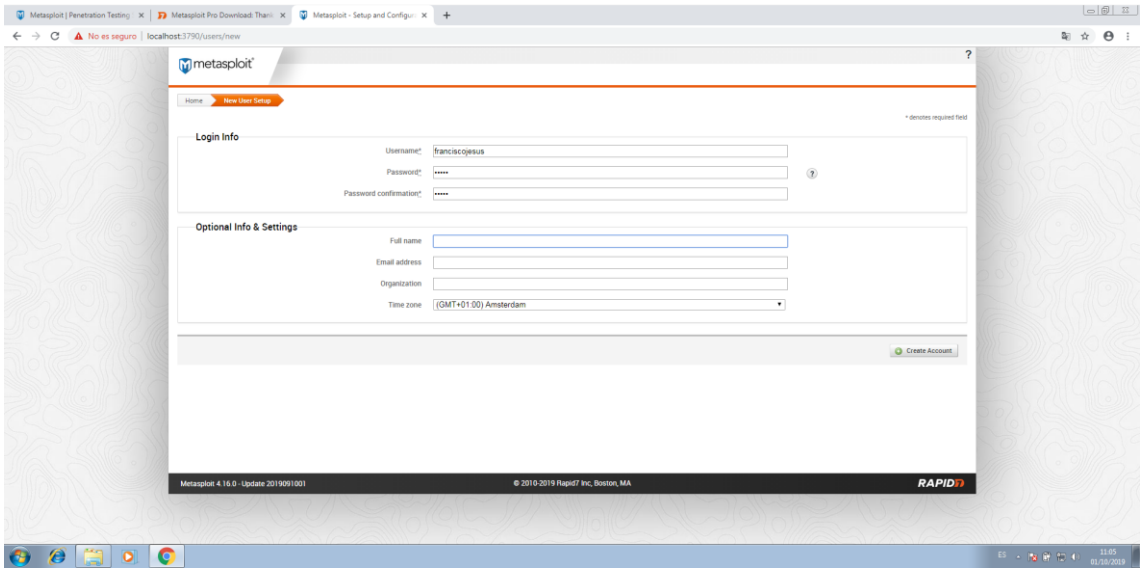
Cuando queramos entrar a Metasploit deberemos entrar por el link que nos indica (puerto SSL).



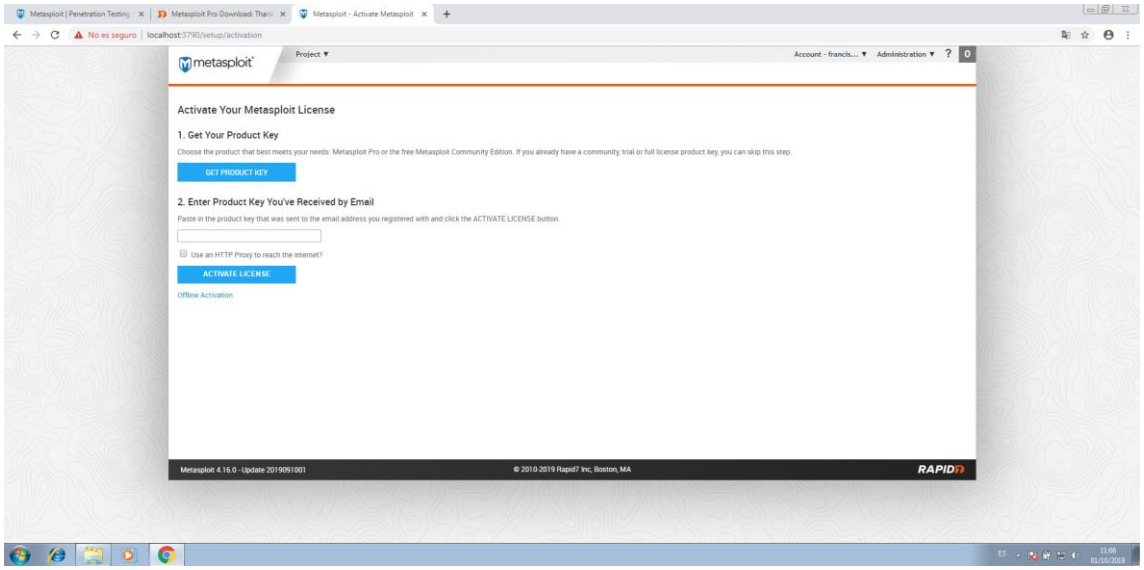
Pulsaremos en *<<Configuración Avanzada>>* y en *<<Acceder a localhost (sitio no seguro)>>.*



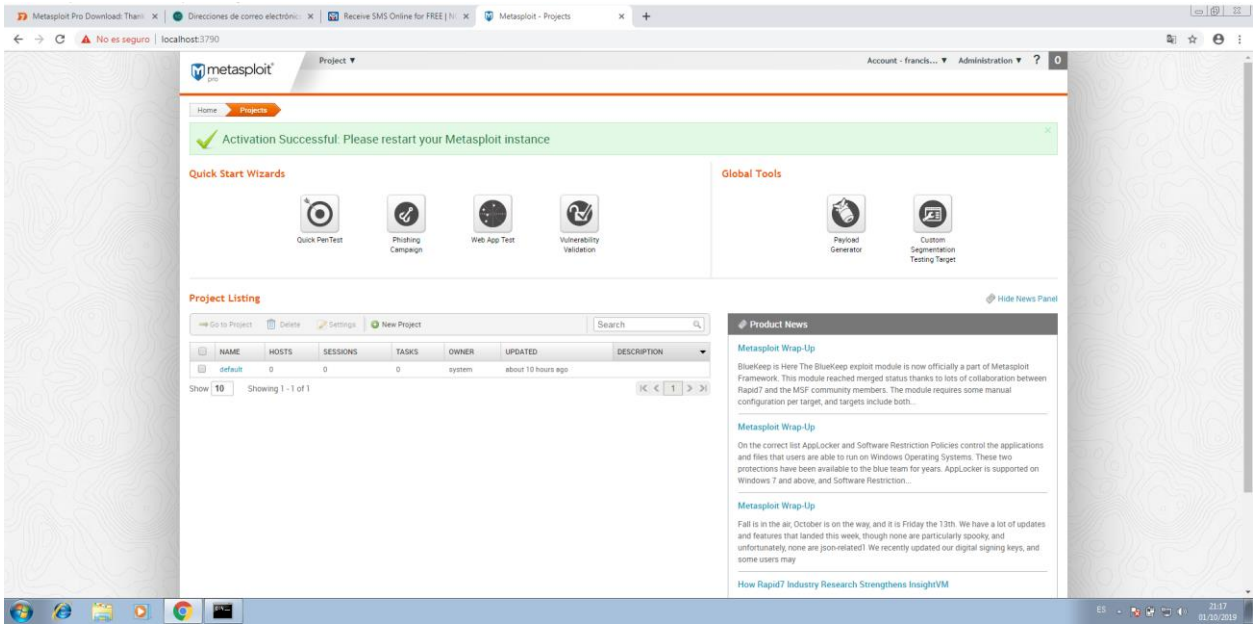
Nos llevará a la página principal de configuración. Configuraremos nuestros datos.



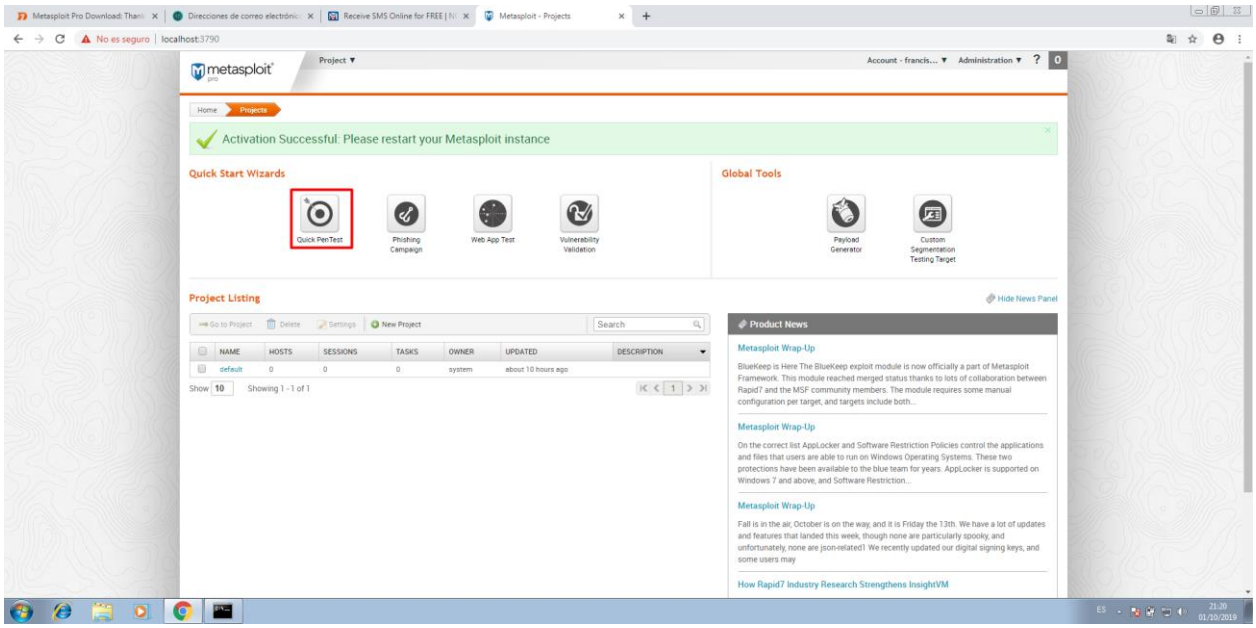
Activaremos el producto con una licencia de prueba.



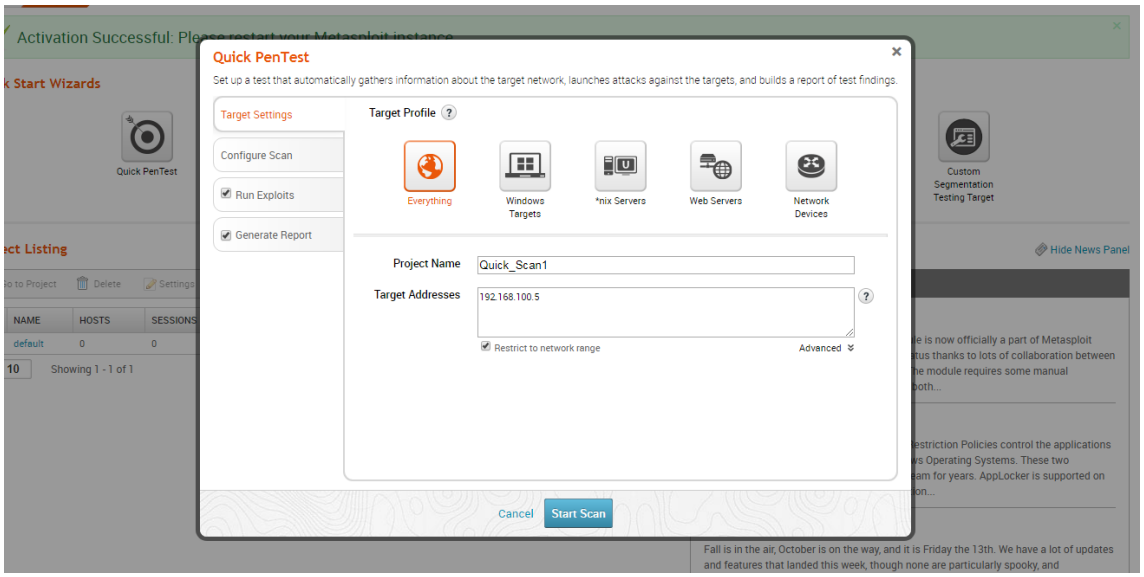
Una vez activado ya estará listo para el uso.



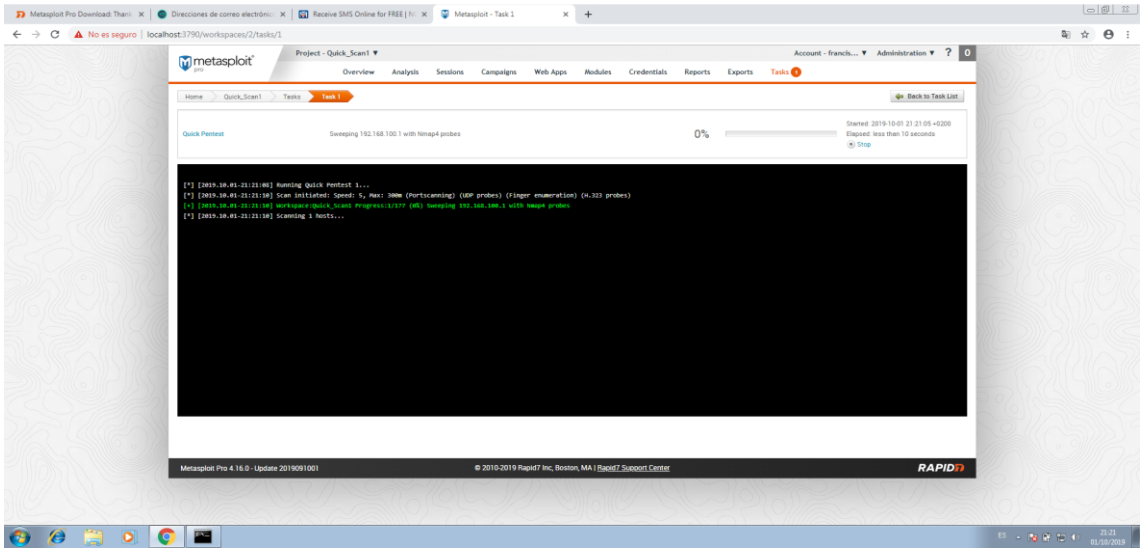
Lo primero que haremos será un escaneo rápido.



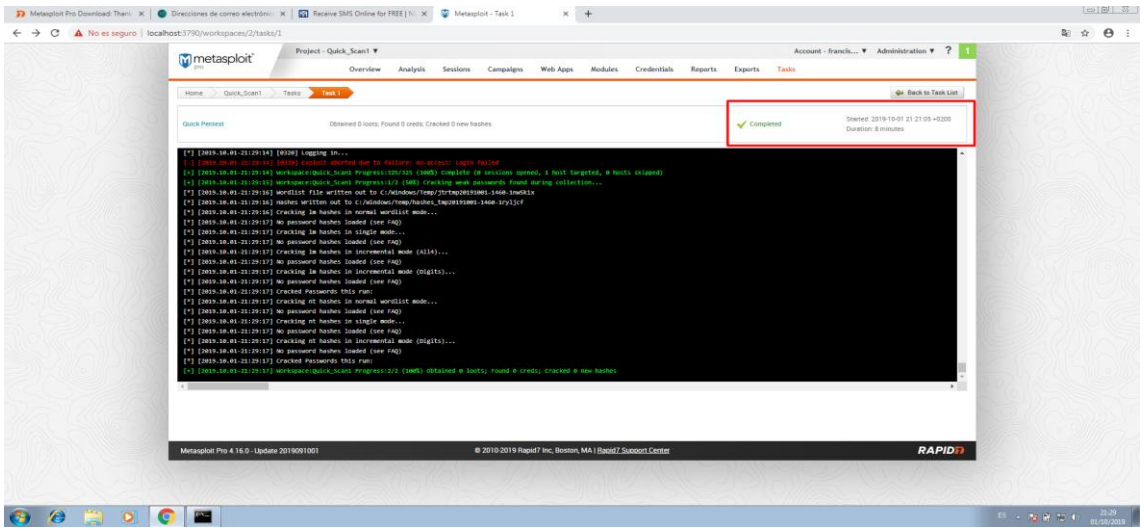
Le damos un nombre de proyecto y ponemos una IP o un rango de IPs.



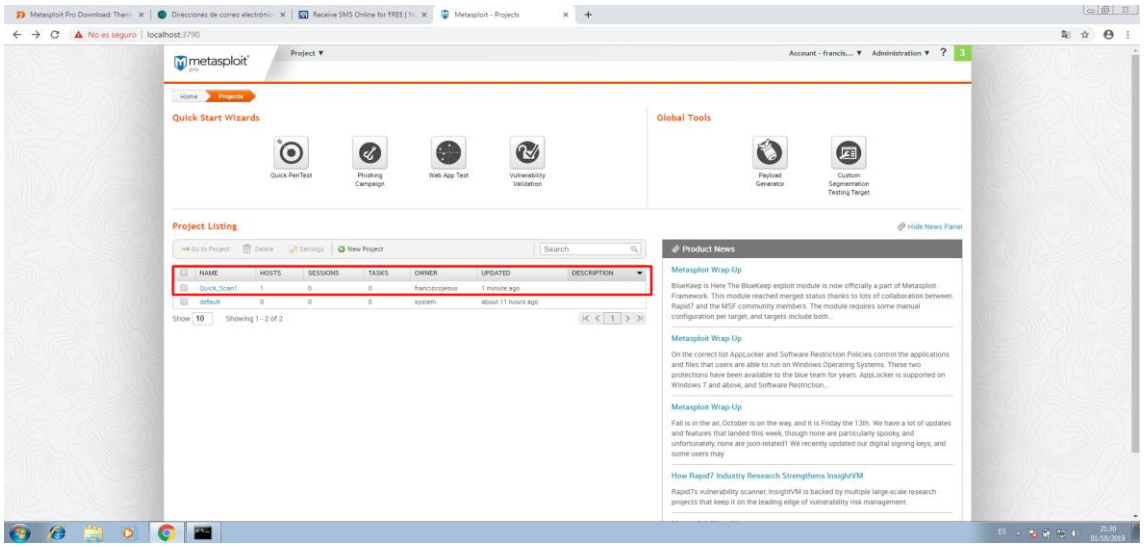
Empezará a realizar el escaneo. Nos irá indicando con una barra de progreso.



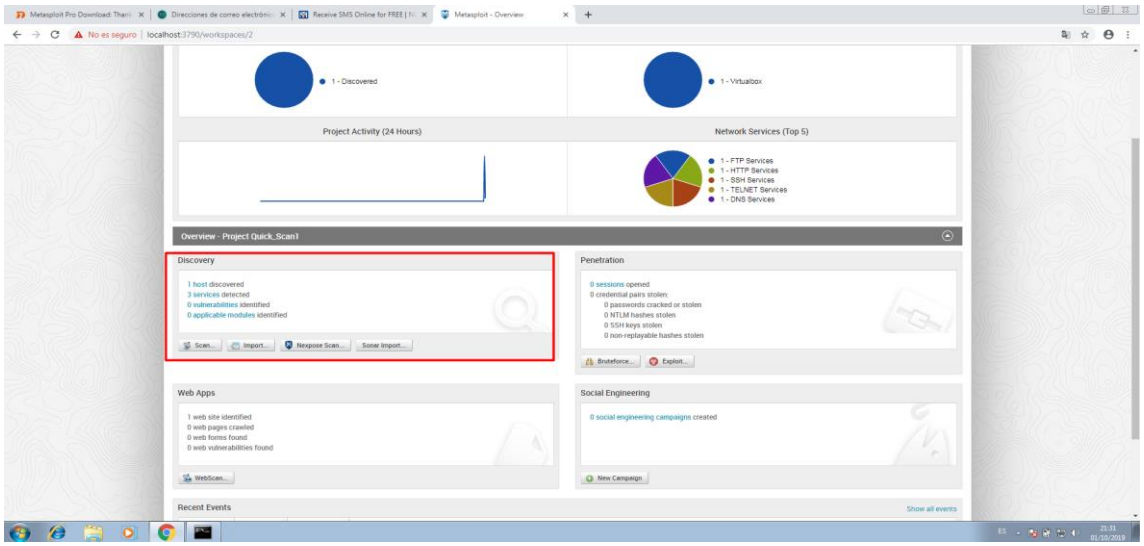
Una vez finalizado veremos el tiempo de duración, la fecha… y se nos quedará la tarea guardada.



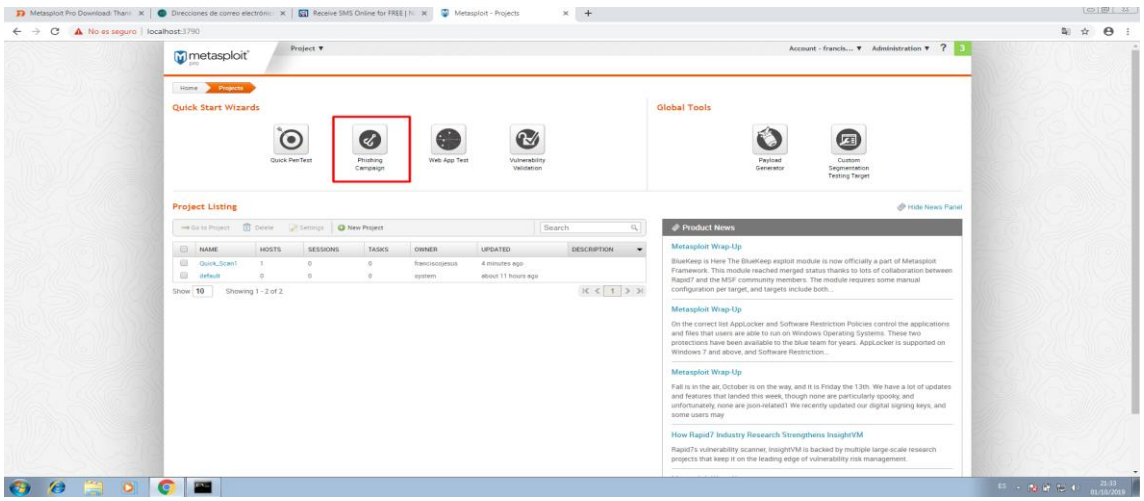
Si vamos al principio veremos la tarea creada.



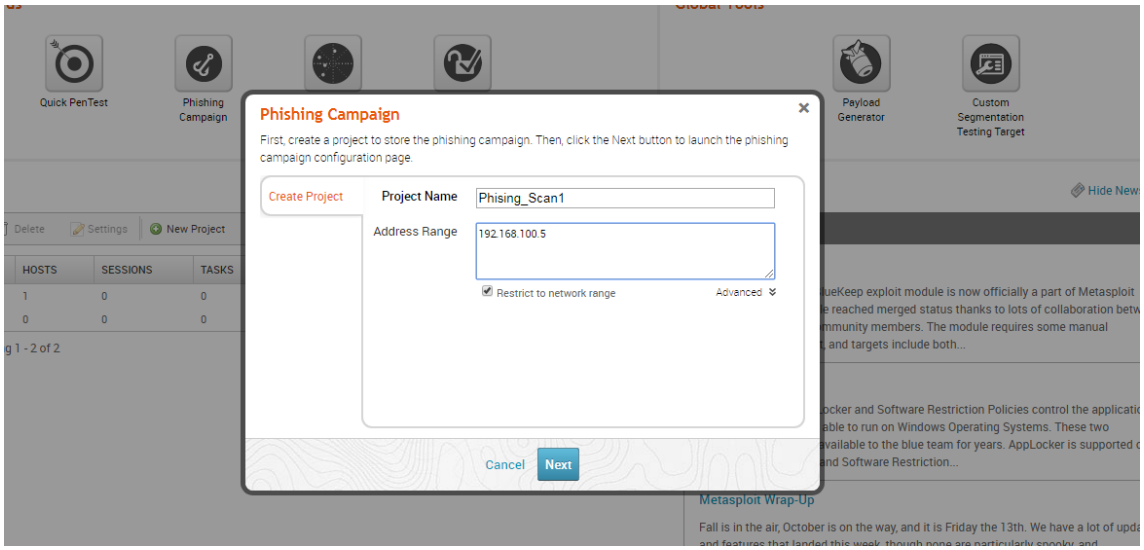
Si pulsamos sobre ella veremos más información. Veremos toda la información sobre el análisis (sistema operativo, si esta en una máquina virtual, el software utilizado los servicios o las vulnerabilidades…) Como vemos, en este caso no se detectaron vulnerabilidades.



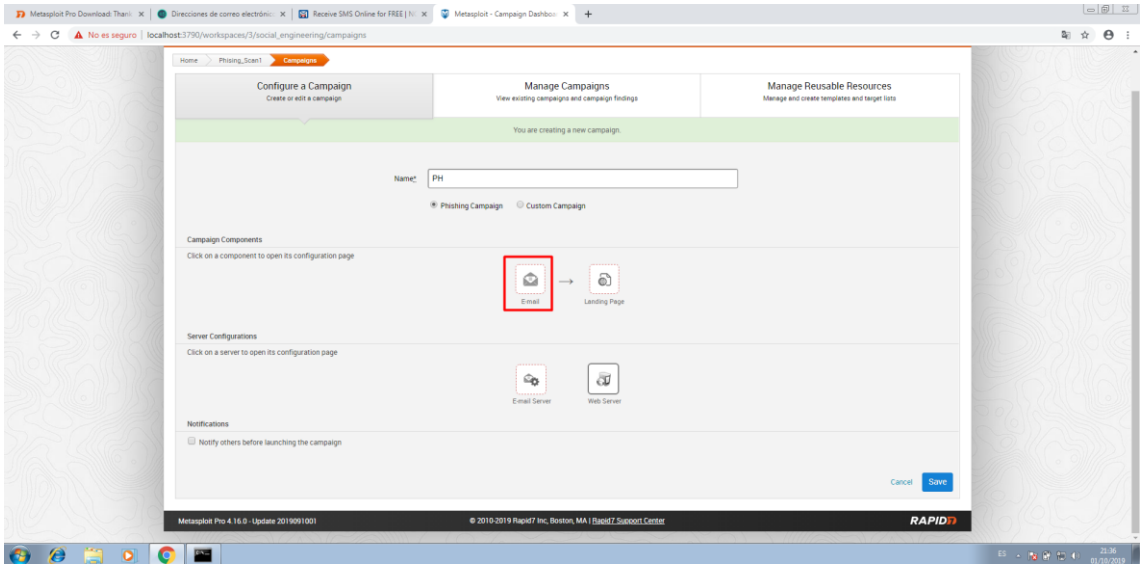
Volveremos a Home y realizaremos un nuevo proyecto, en este caso *Phising Campaing.*



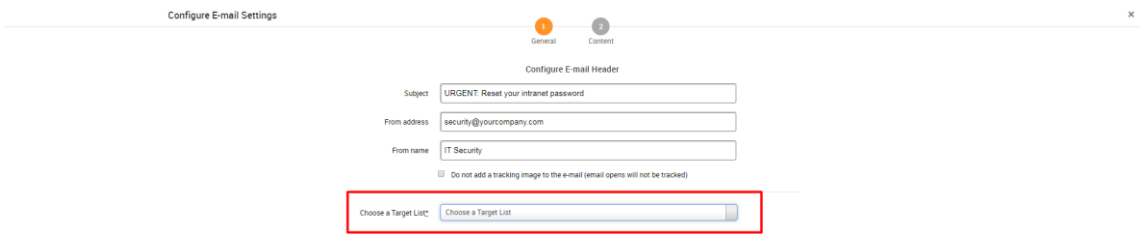
Le volveremos a dar un nombre y una IP o rango de IPs.

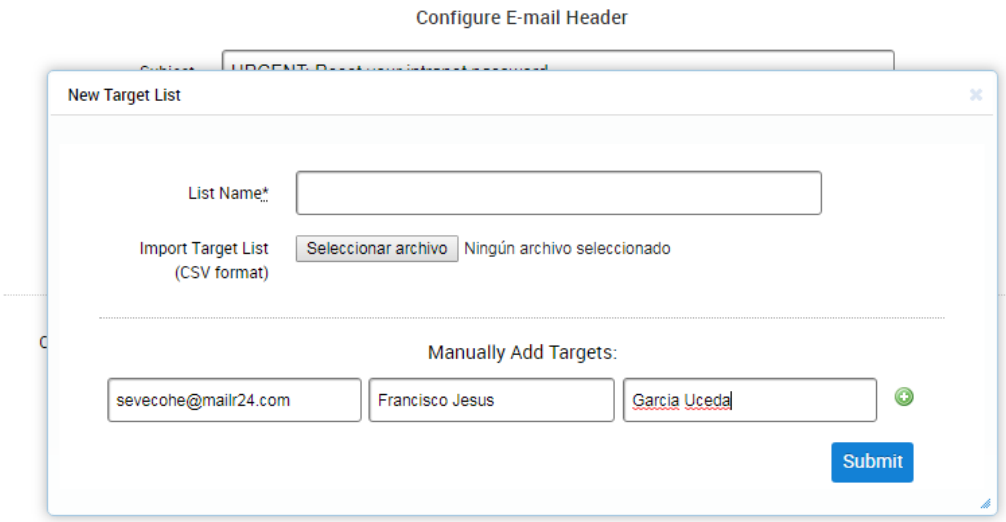


Le daremos un nombre y pulsaremos en *e-mail.*

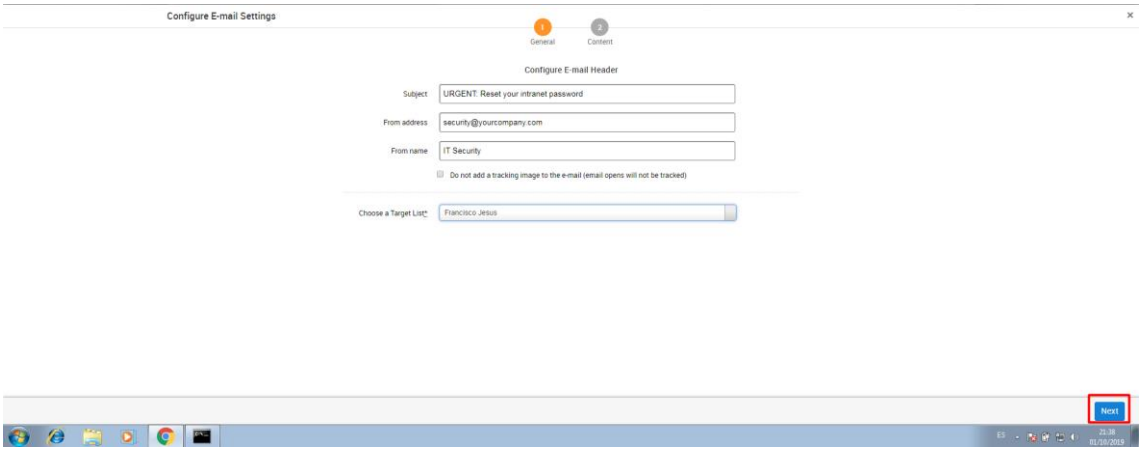


Lo editaremos a nuestro gusto e importaremos un correo (en mi caso será uno mío, usar bajo responsabilidad propia).

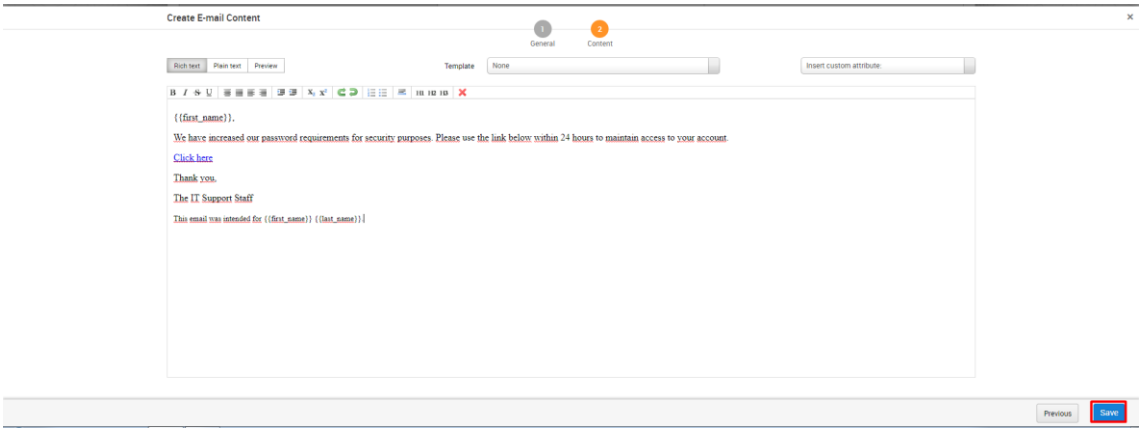




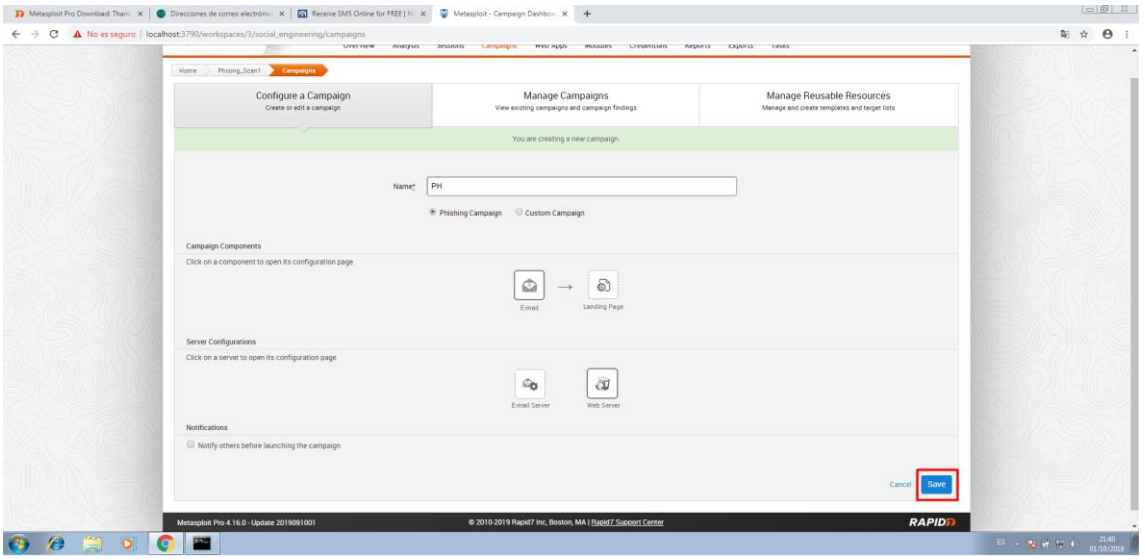
Pulsamos en *Next.*



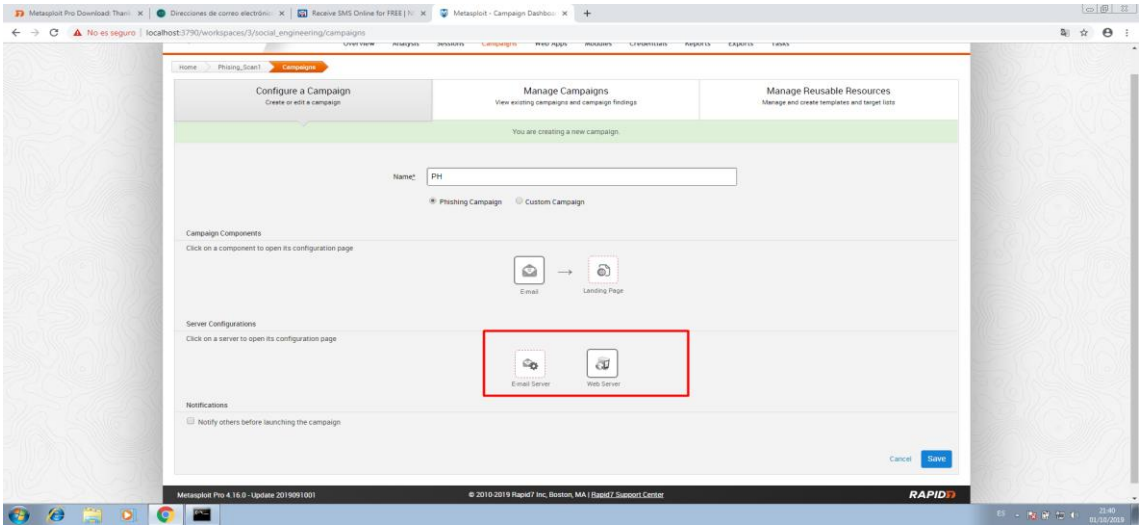
Escribiremos un breve texto y daremos a *Save.*



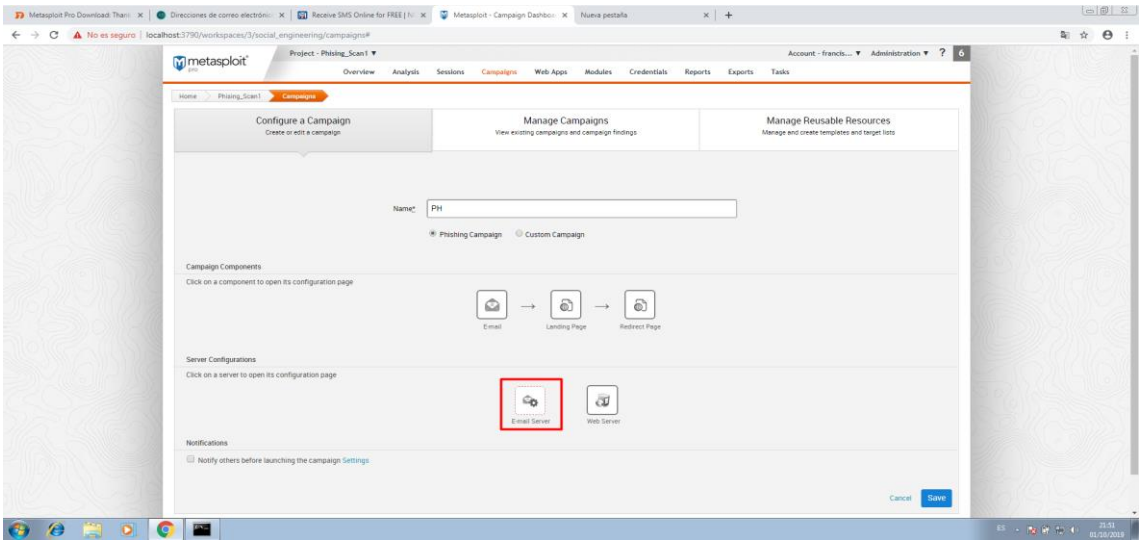
Lo siguiente que daremos es dar a *Save.*



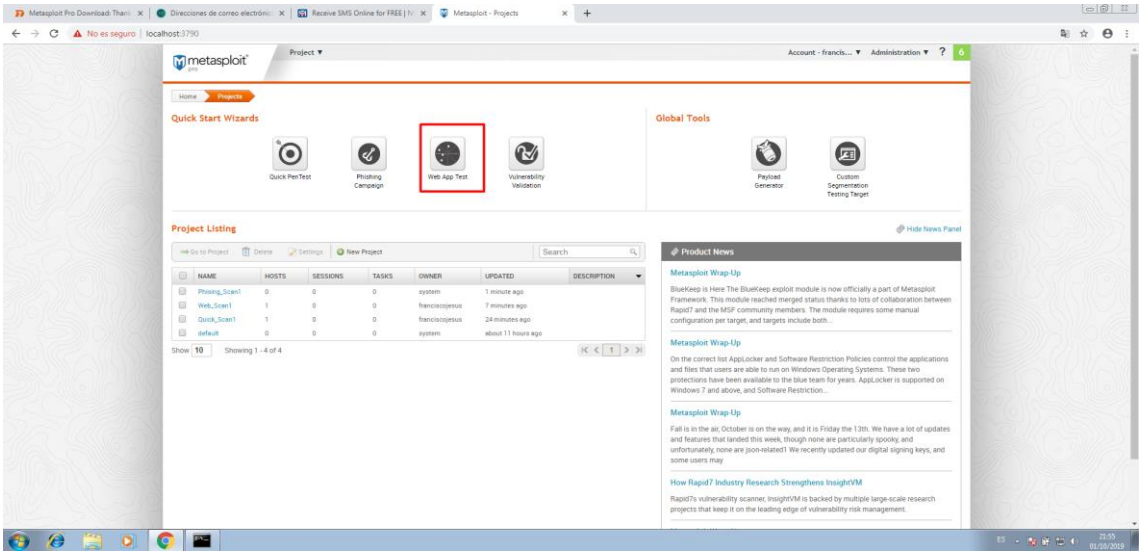
Como vemos también podemos cargar varios correos, o mandarlo por un correo en nuestro servidor web o externo.



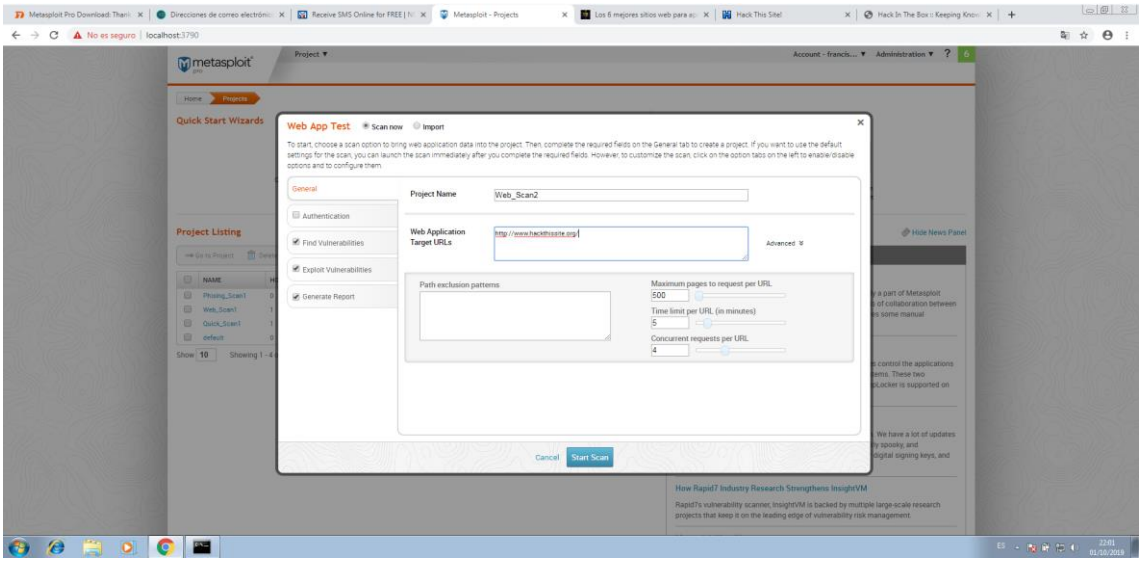
En nuestro caso como no tenemos un servidor de correo configurado no podemos enviarlo, ya que en la versión pro no nos deja usar un externo.



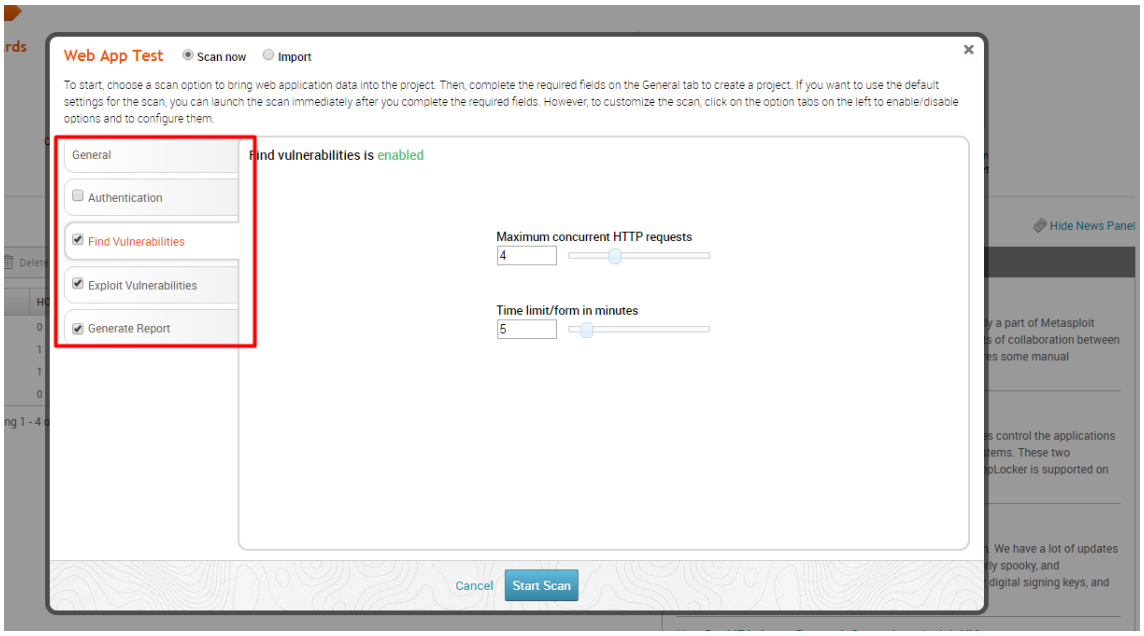
Lo siguiente que haremos será un escaneo Web, volveremos a *Home* y pulsamos en W*eb App Test.*



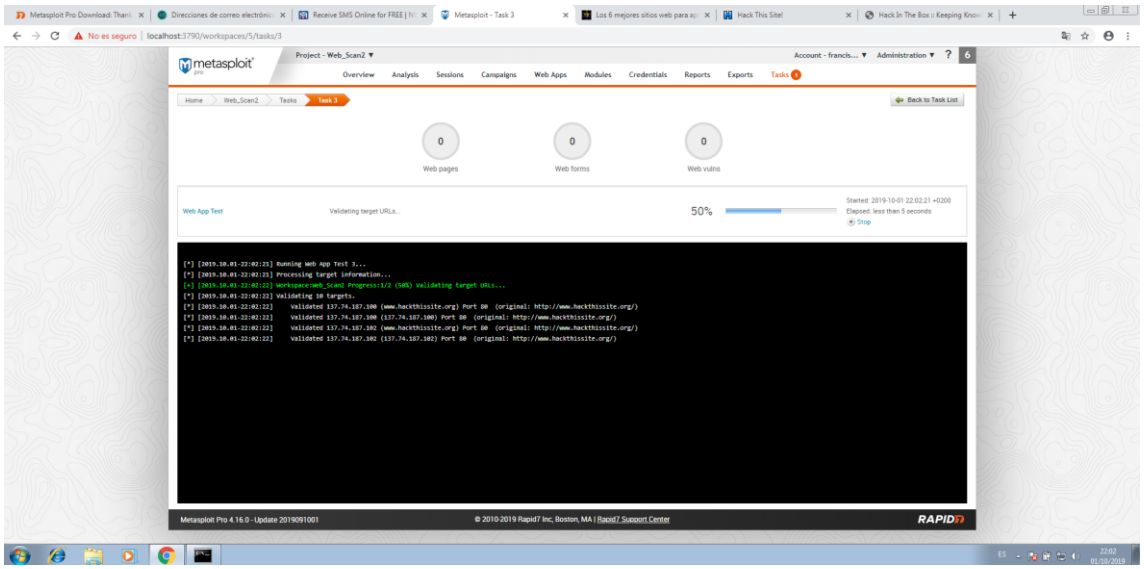
Pondremos como web una página que permite que se analizarla para probar y buscar vulnerabilidades. (Link),



Tendremos opciones avanzadas, pulsaremos *Start Scan* para comenzar el escaneo.

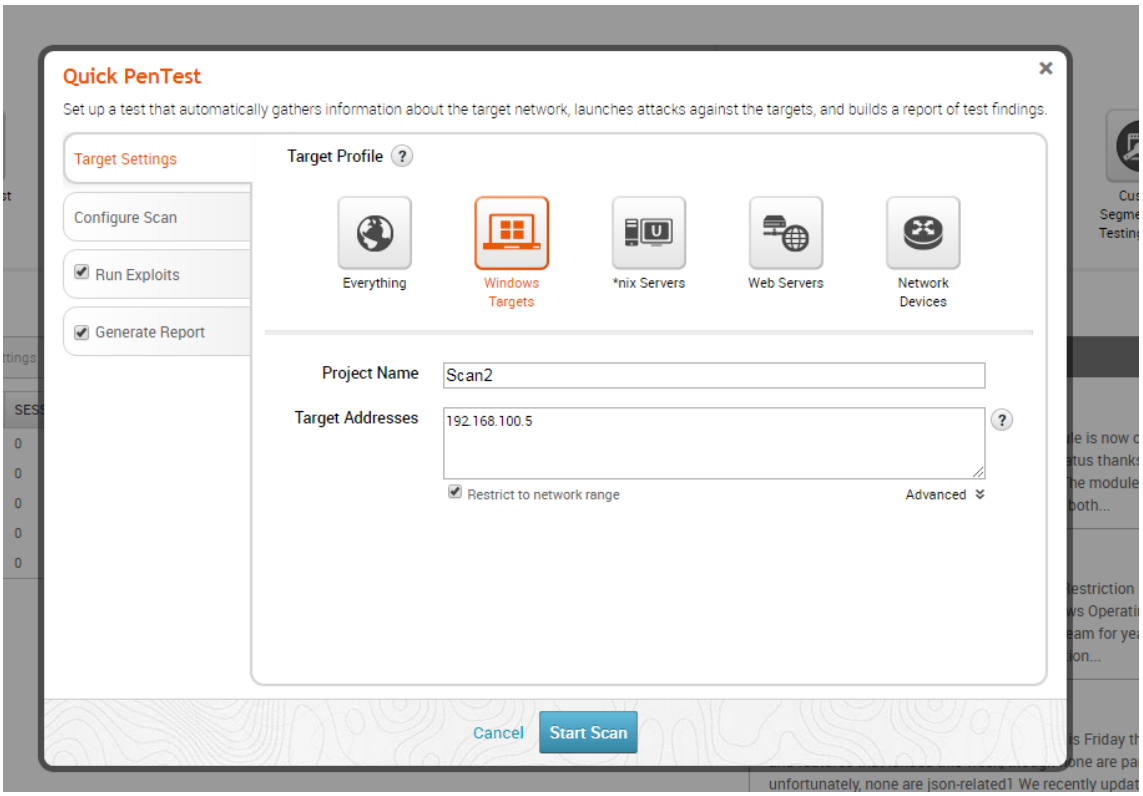


Esperaremos a que busque vulnerabilidades, como vemos, tenemos una barra de progreso también.

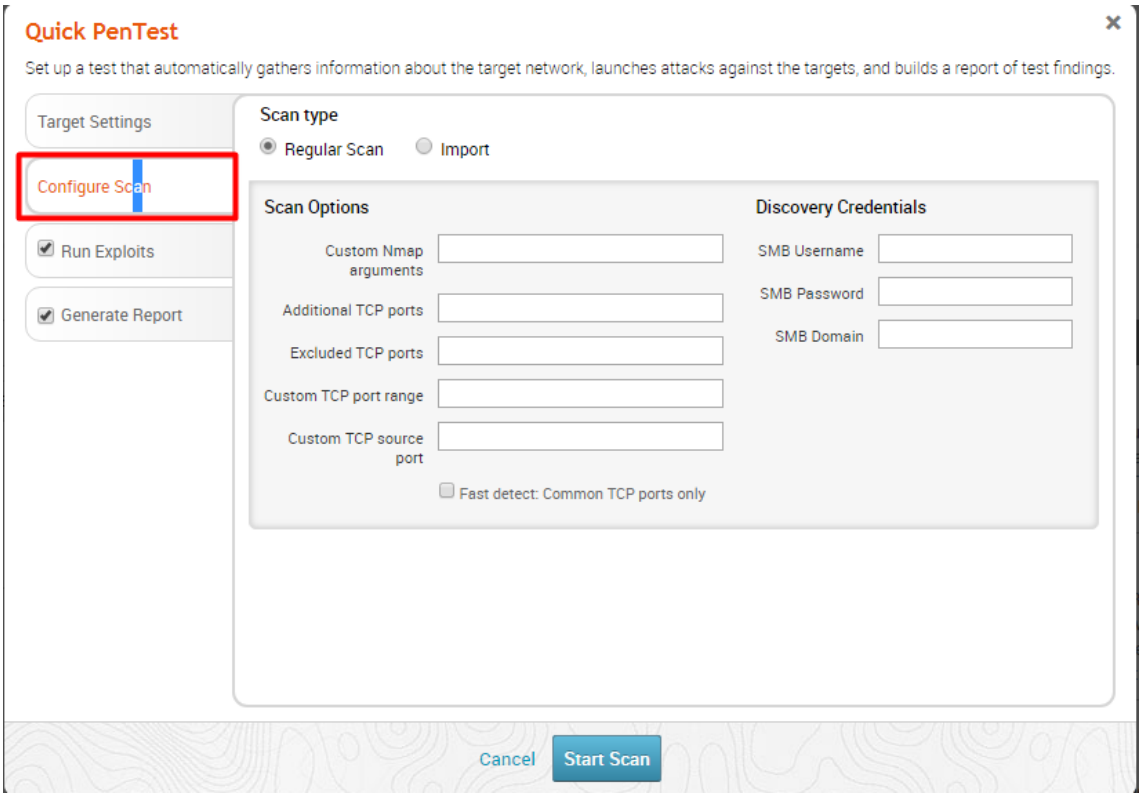


Mientras se realiza este test iremos a *Home* para realizar otro test rápido, pero viendo las opciones avanzadas.

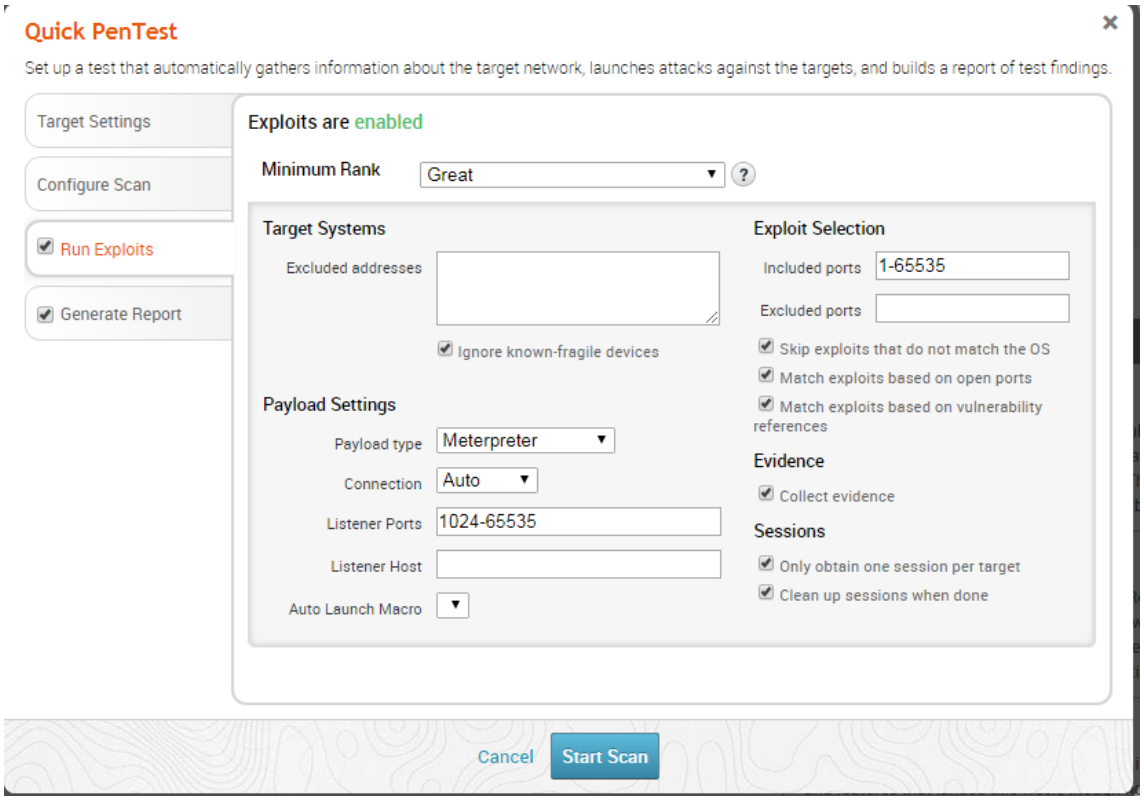
Podremos crear planes específicos de ataque (para máquinas Windows, servidores web, servidor nix o dispositivos de red). Seleccionare una máquina Windows.



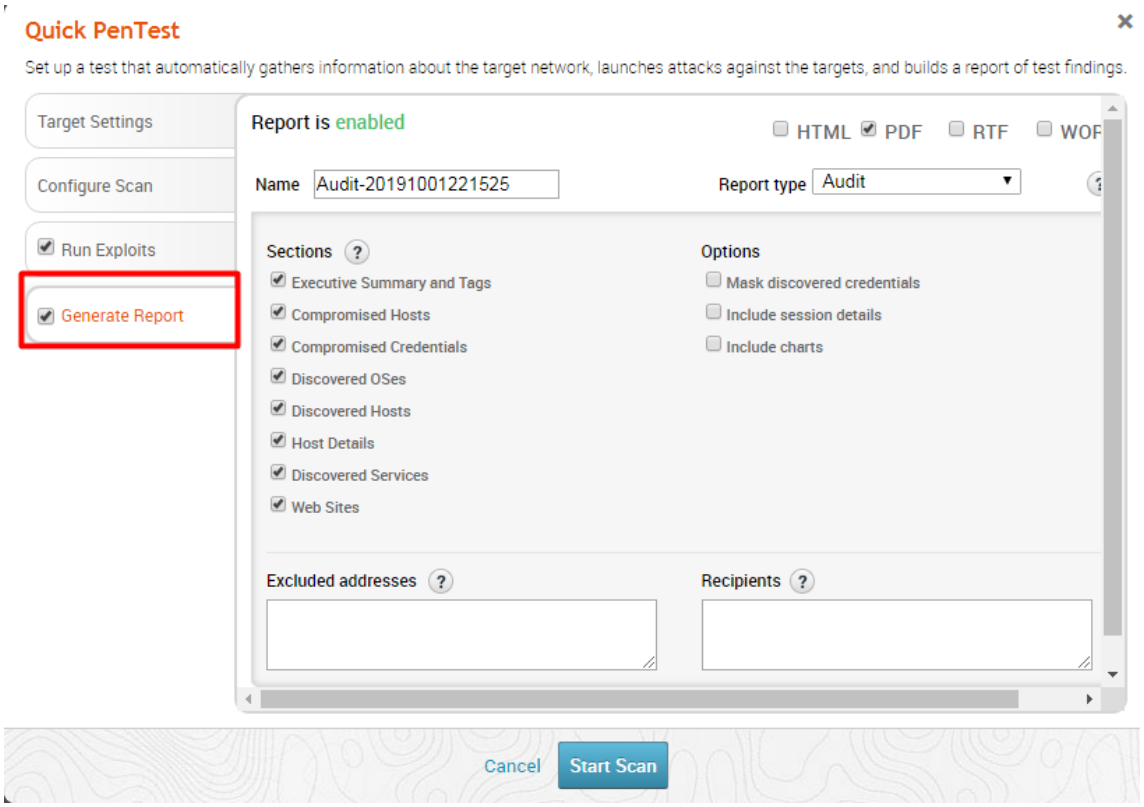
Si vamos a *Configure Scan* podremos ponerles argumentos personalizados para nmap.



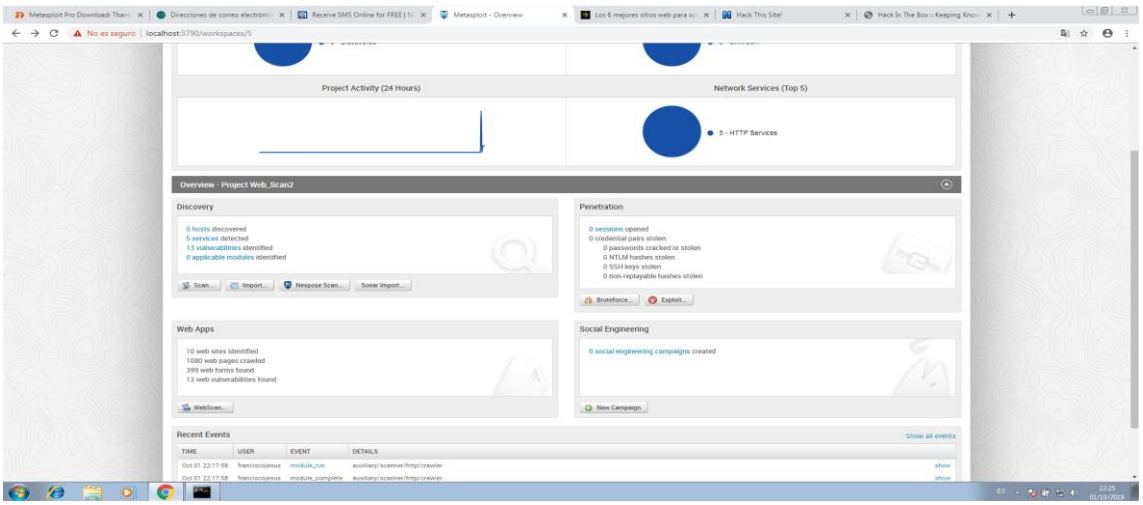
Podremos filtrar por exploit o correr nuestros propios exploits.



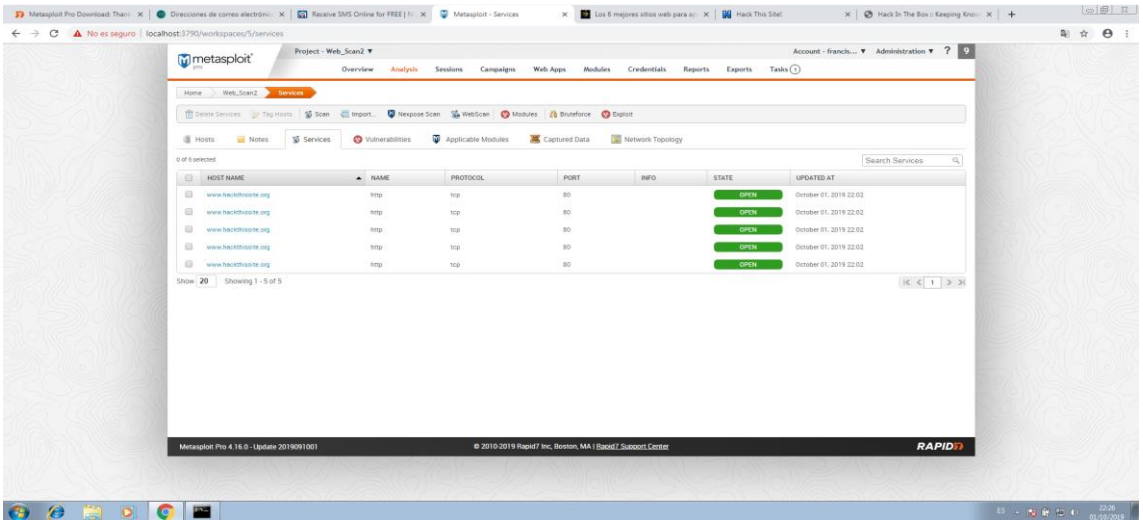
Podemos filtrar el reporte generado.



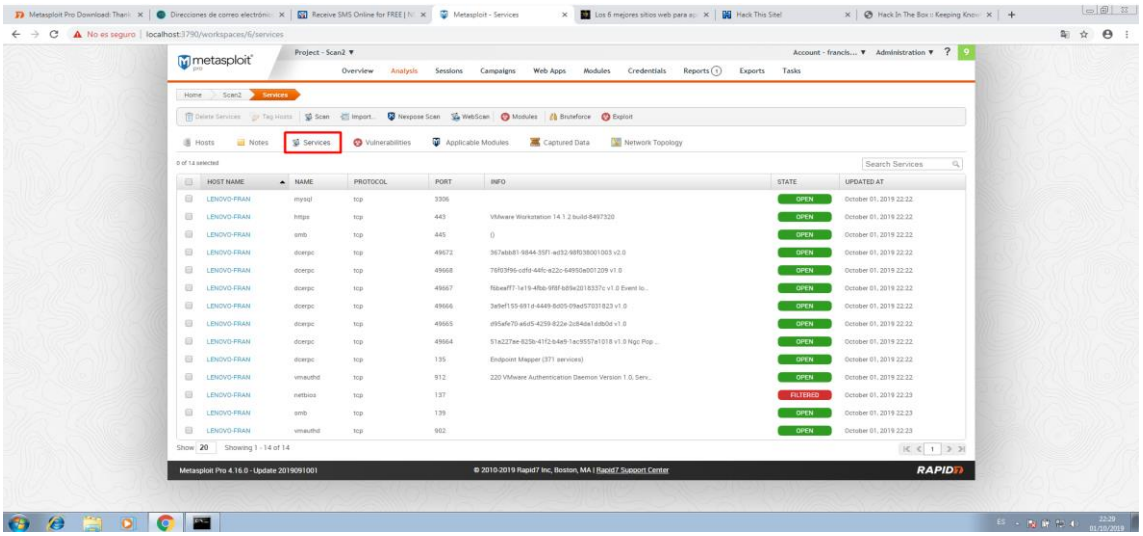
Le daremos a *Start Scan* y mientras este escaneo finaliza iremos al que hemos realizado a la web. Podemos observar cómo esta vez sí encontró vulnerabilidades.



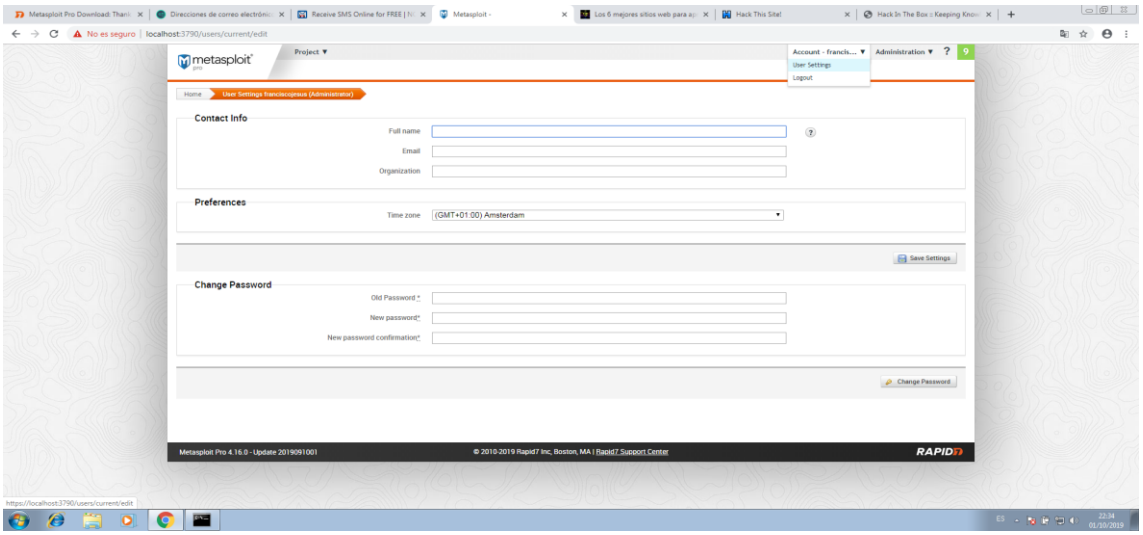
Si pulsamos sobre ellas encontraremos más información.



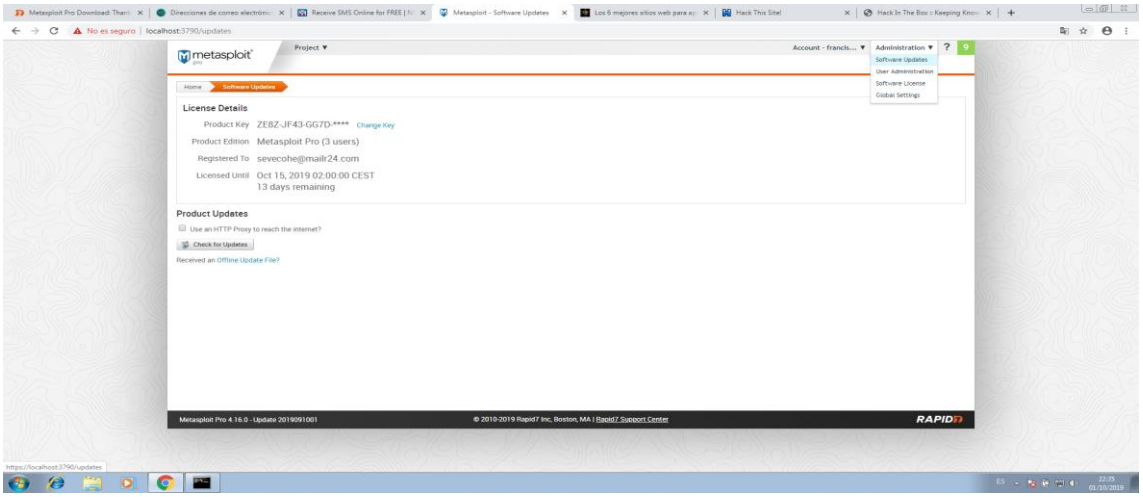
Volveremos al escaneo rápido que hemos puesto con distintas opciones. Si pulsamos en *Services* podemos ver todos los servicios que tiene el dispositivo activo.



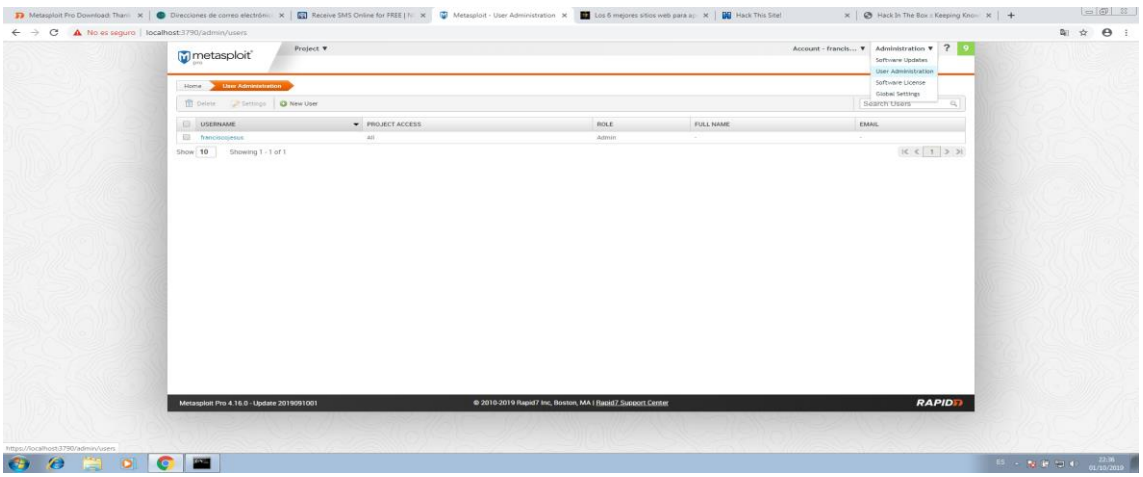
Por último, veremos opciones más relevantes de metasploit pro. Si vamos a *Account -> User Setting* podremos editar nuestro nombre, email, zona horaria o incluso cambiar nuestra contraseña.



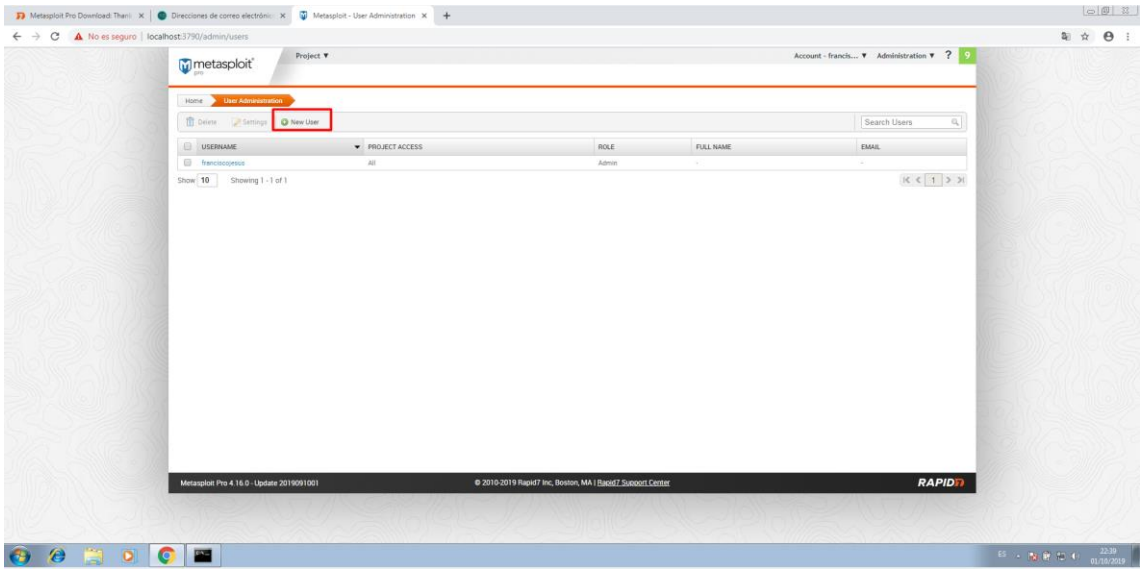
Si vamos a *Administrator -> Software Update* podemos ver nuestra licencia, el tiempo que le queda y comprobar actualizaciones.



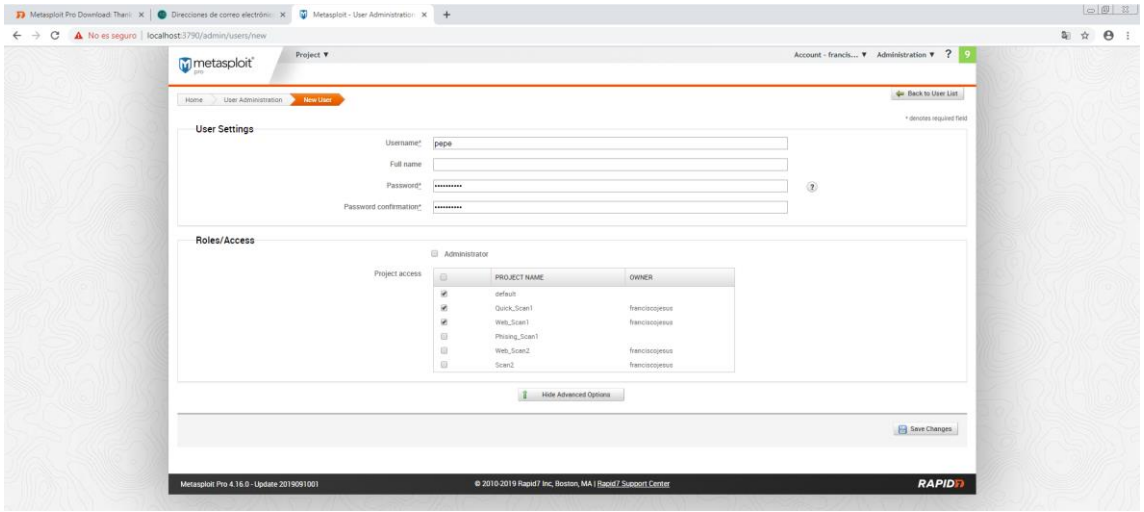
Si vamos a *Administrator -> User Administration* podremos crear nuevos usuarios (hasta 3 en la versión de prueba).



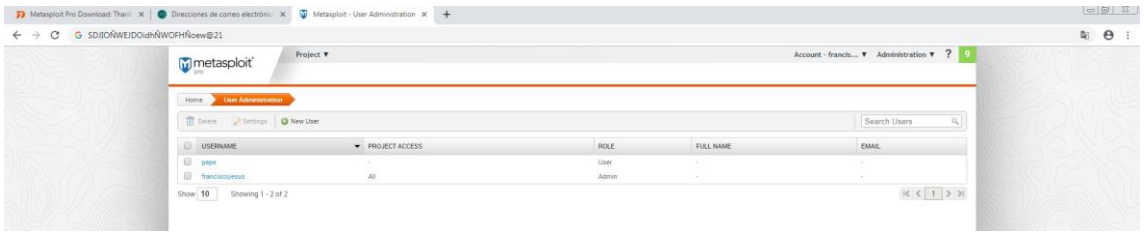
Damos a *New User.*



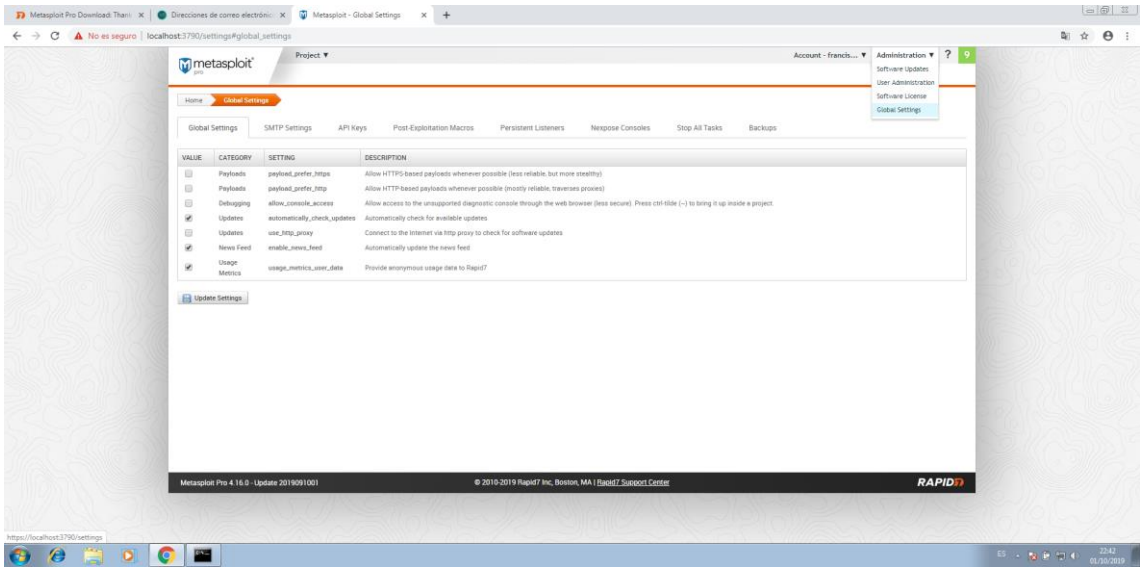
Rellenamos los datos y podemos darle permisos de Administrador o que tenga únicamente acceso a unos cuantos proyectos.



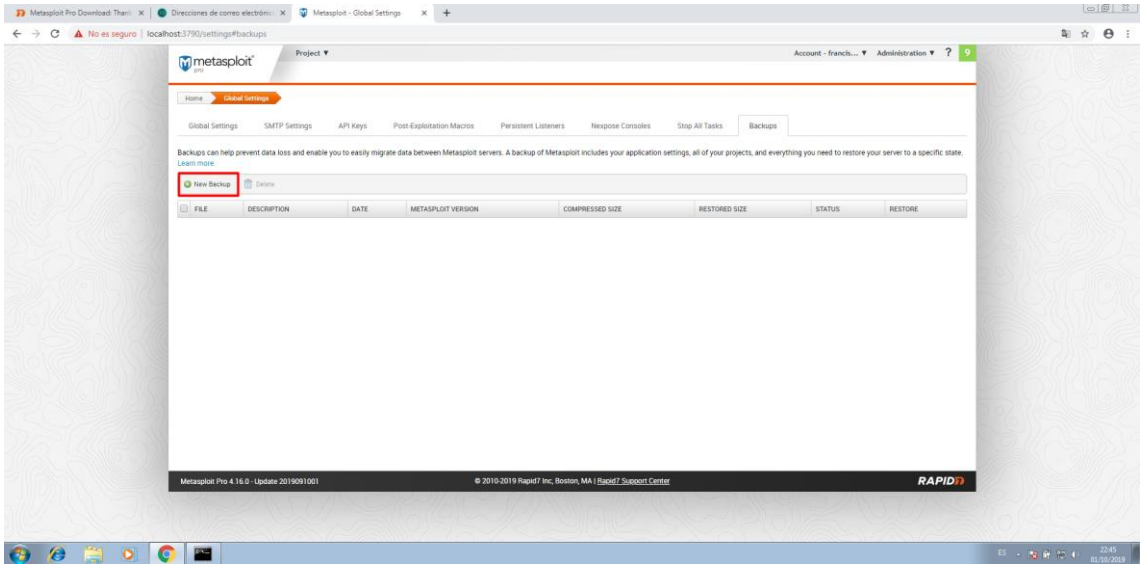
Ya tendremos el usuario creado.



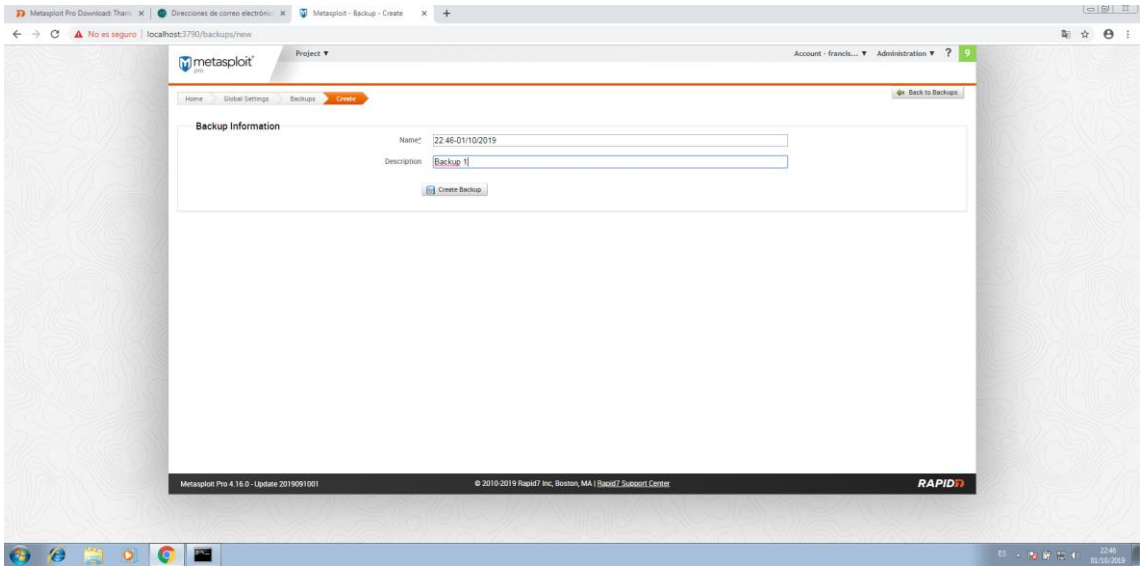
Para finalizar, tendremos las opciones globales donde podremos configurar API, opciones generales, exploit, parar todas las tareas o incluso hacer backups.



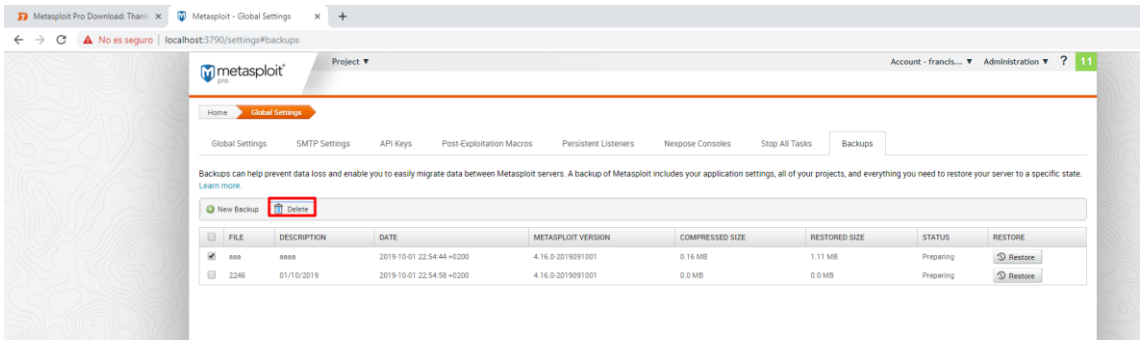
Pulsaremos en *New Backup.*

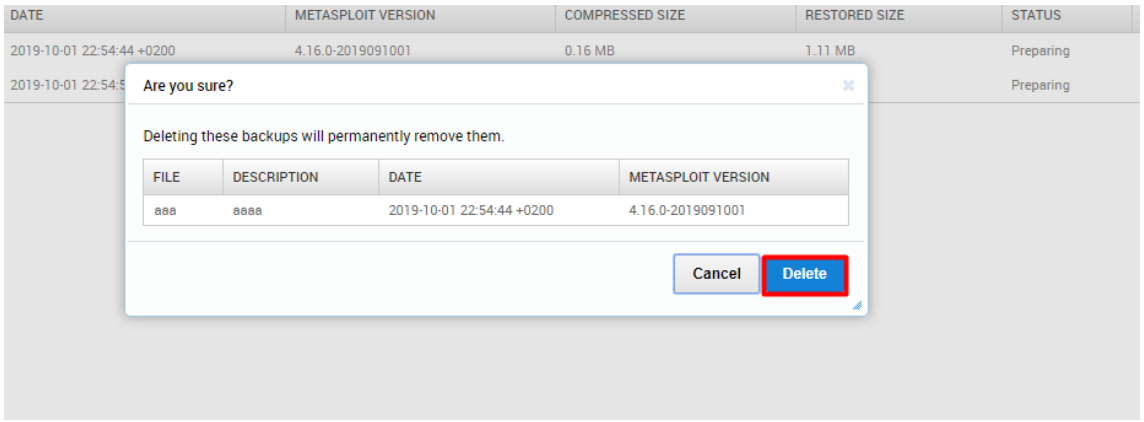


Le daremos un nombre y una descripción.

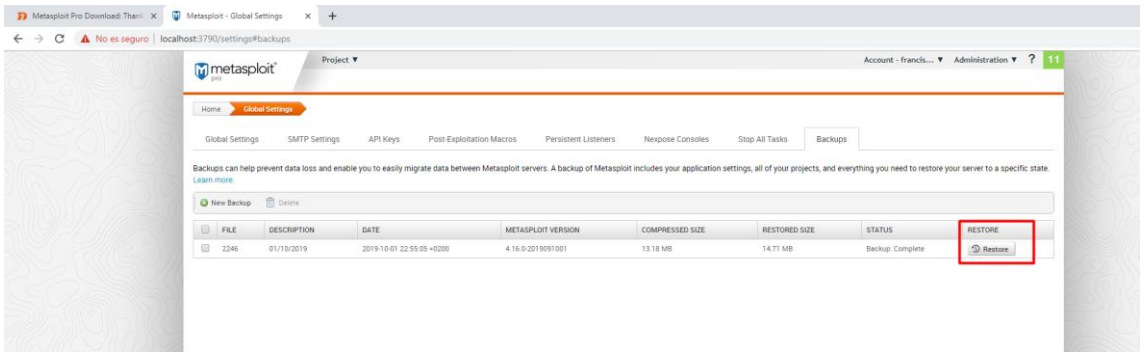


Ya tendremos creado nuestra copia de seguridad. Si pulsamos sobre ella y damos a *Delete* la borraremos.

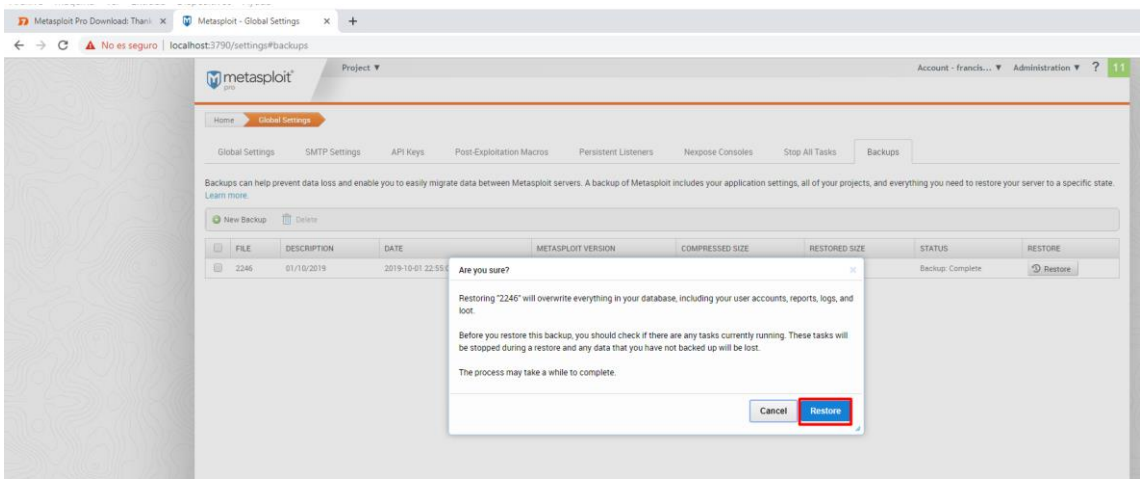




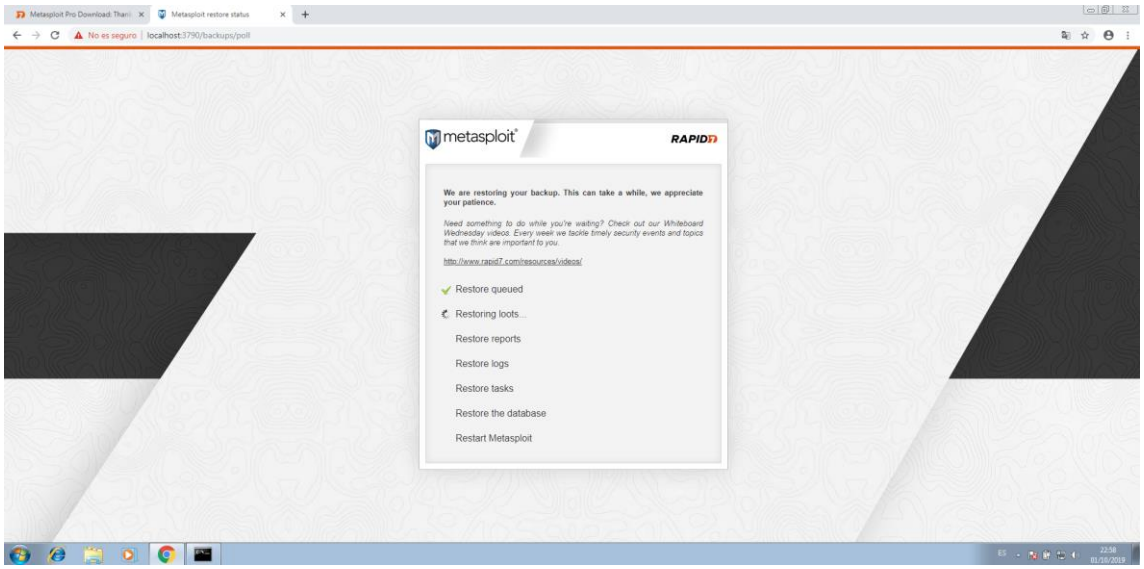
Si pulsamos en *Restore* restauraremos la copia de seguridad.



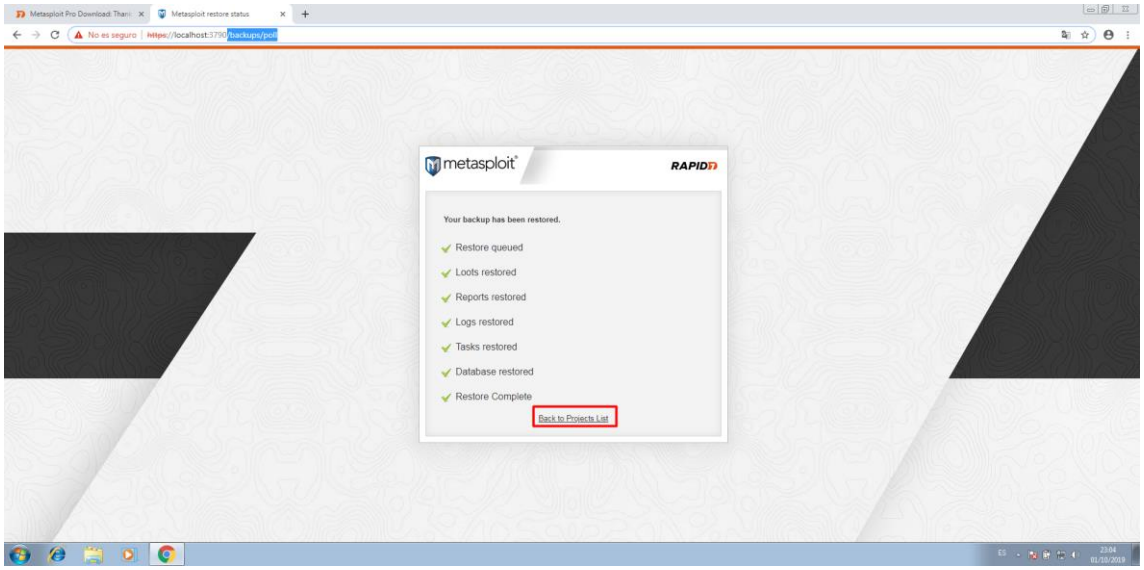
Pulsamos en *Restore.*

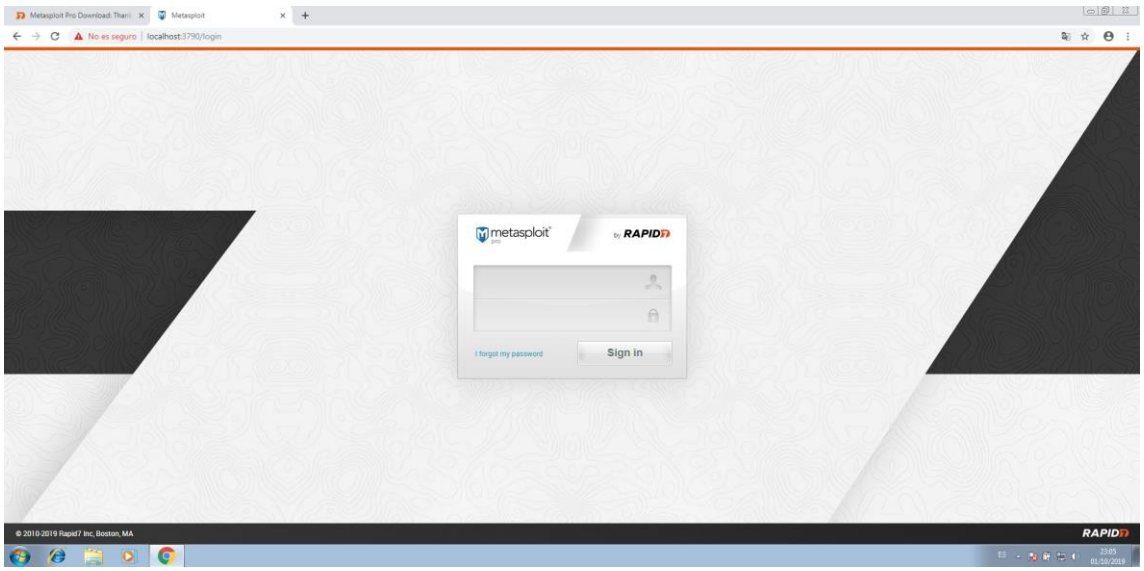


Esperamos a que se restaure.



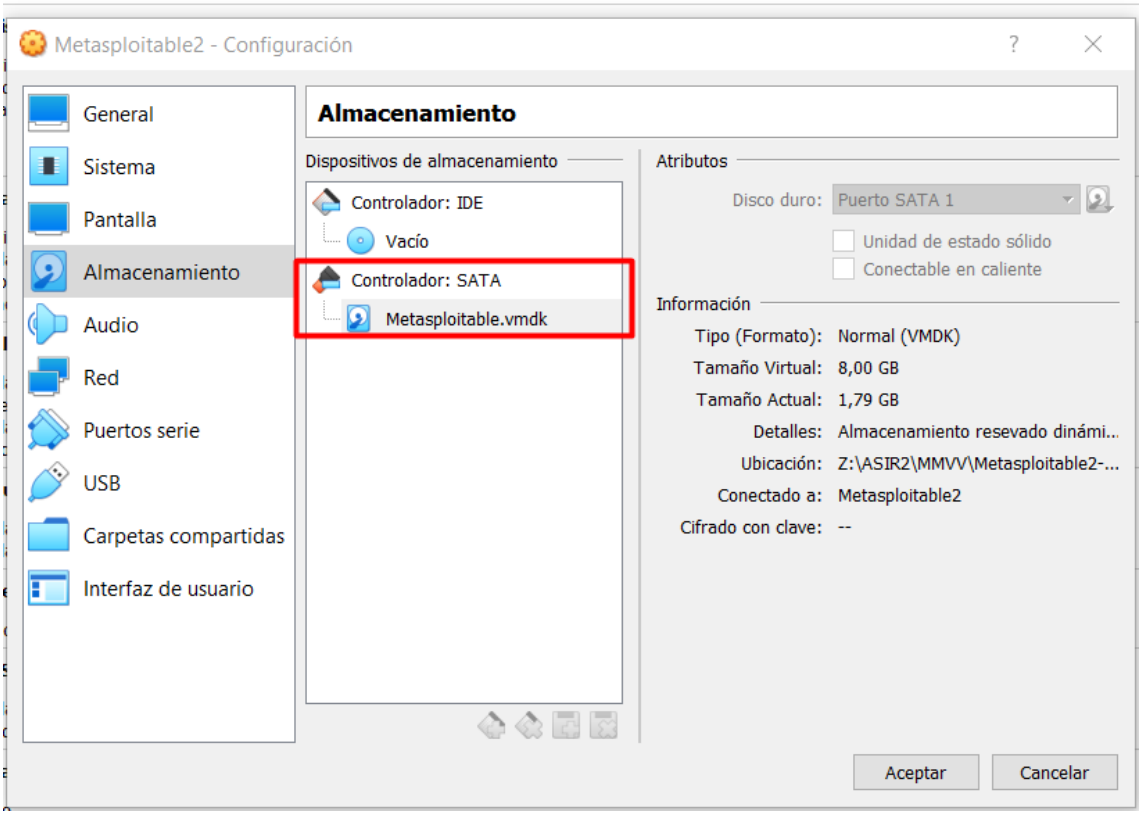
Una vez restaurado nos llevará a la pagina de inicio y estará la copia restaurada totalmente.

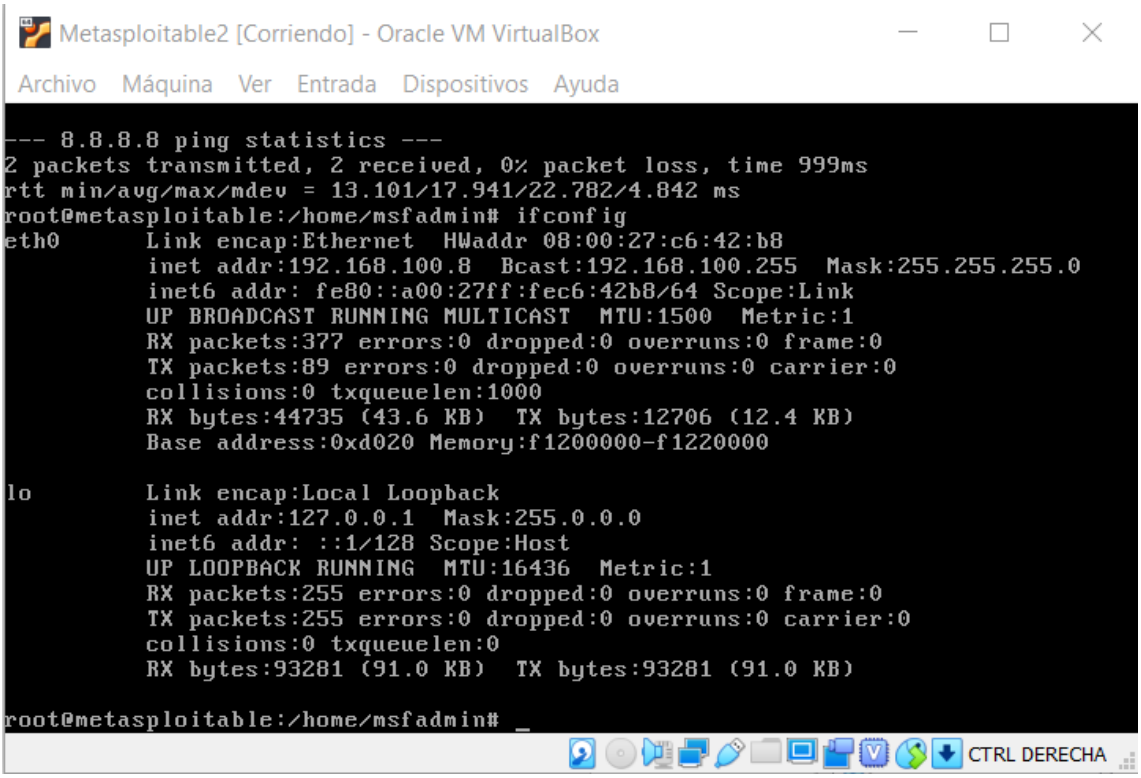




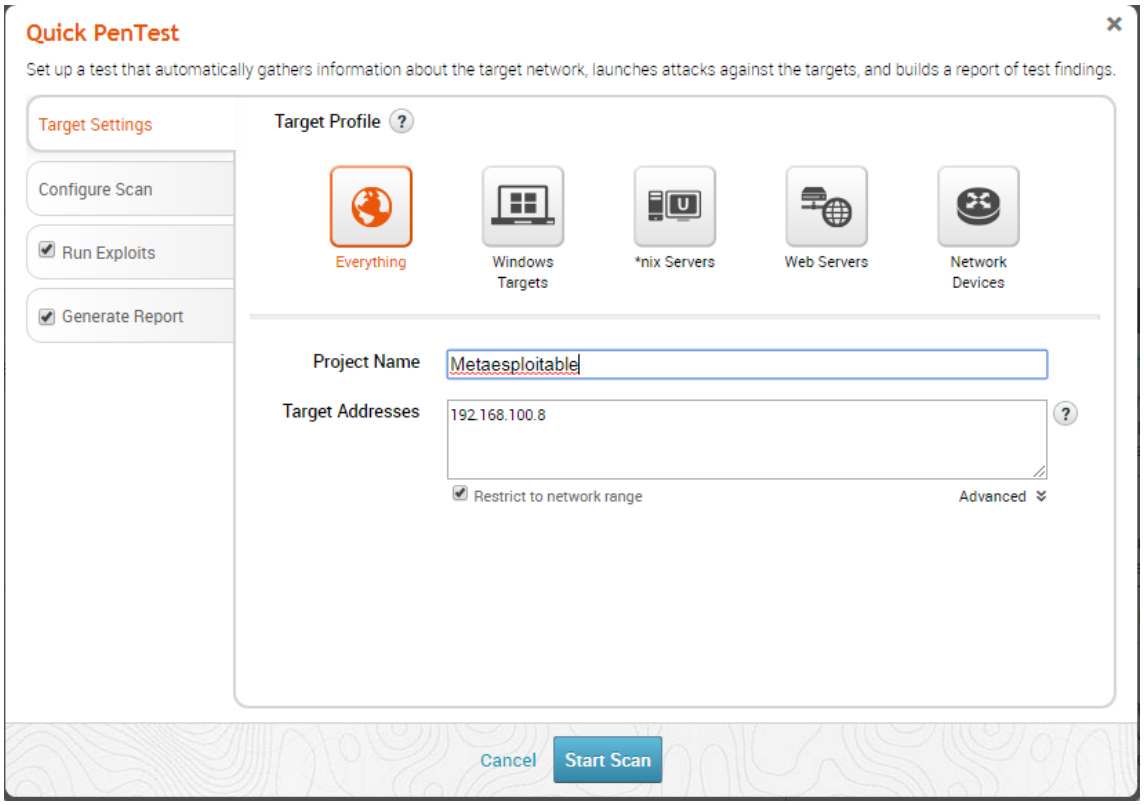
Extra – Máquina Metasploitable 2

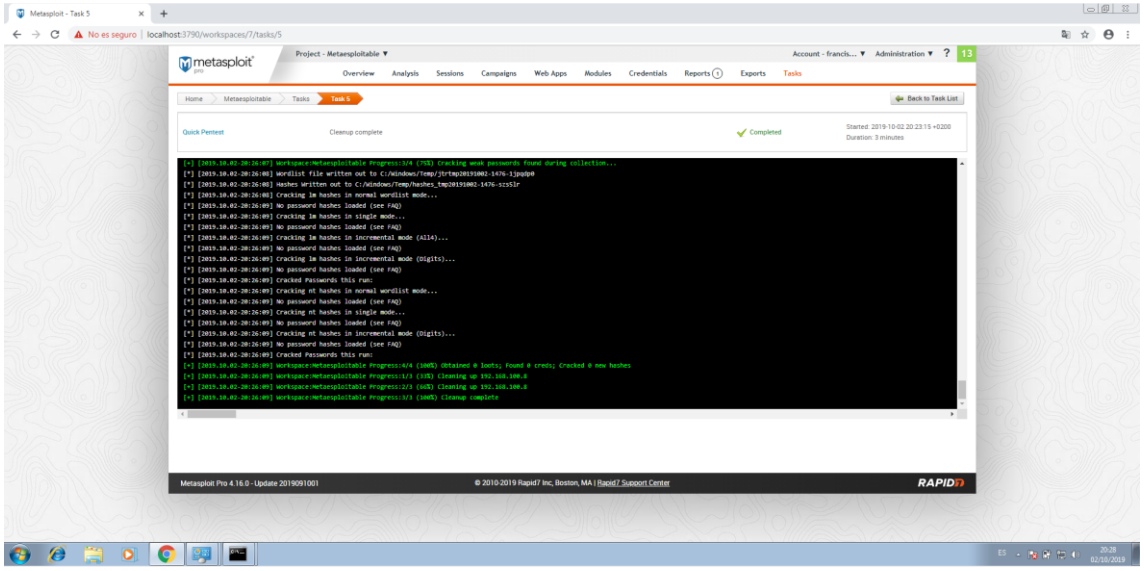
En VirtualBox hemos instalado la máquina Metasploitable 2. La máquina virtual Metasploitable es una versión de Ubuntu Linux intencionalmente vulnerable diseñada para probar herramientas de seguridad y demostrar vulnerabilidades comunes.



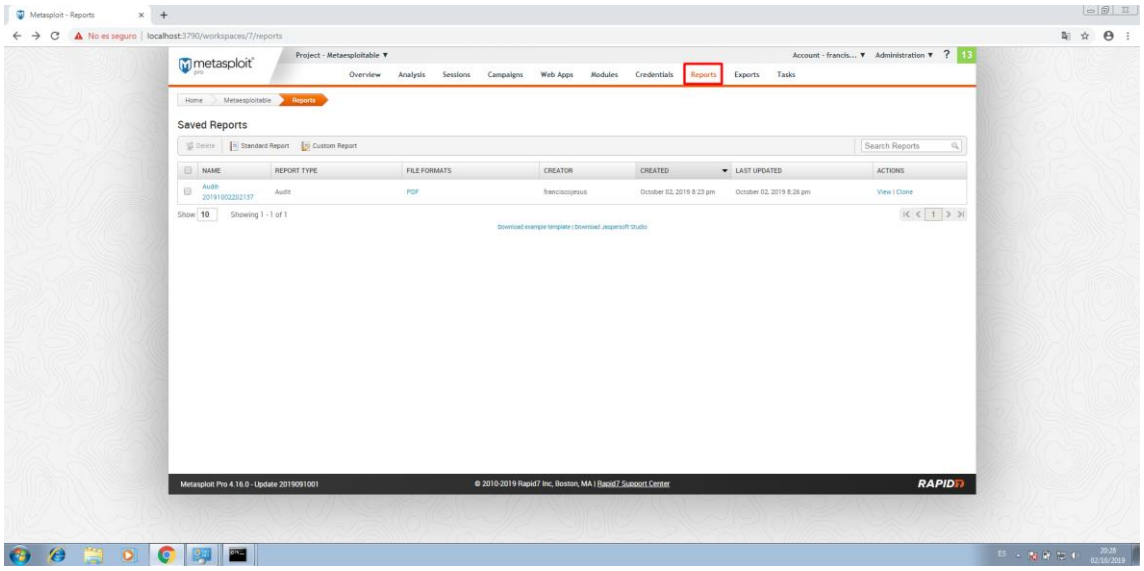


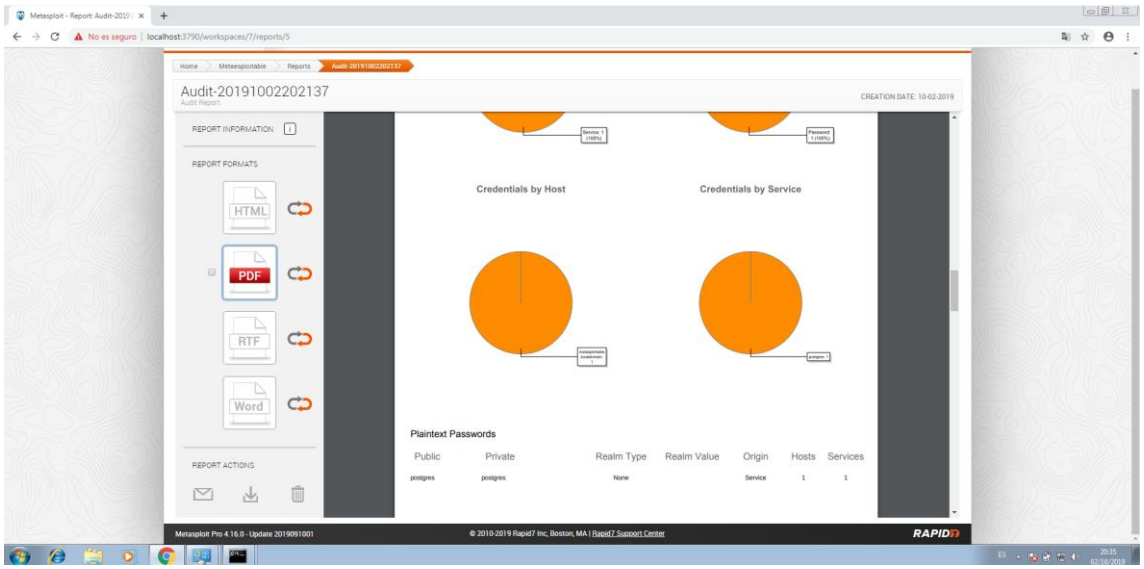
Le hemos realizado un escaneo rápido para mostrar todas las vulnerabilidades que tiene y ejecutar alguna de ellas.



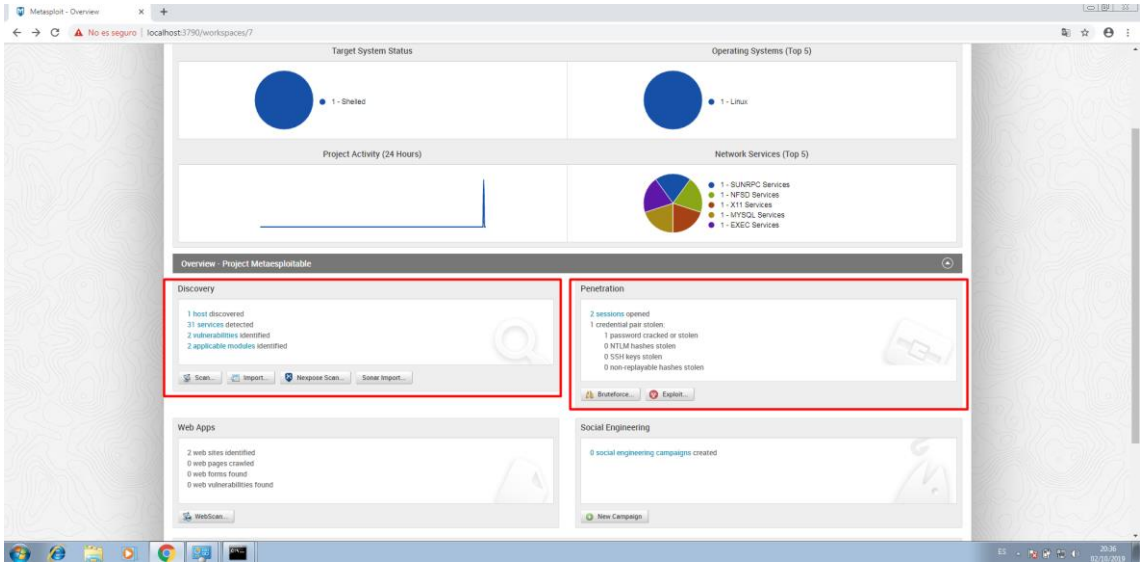


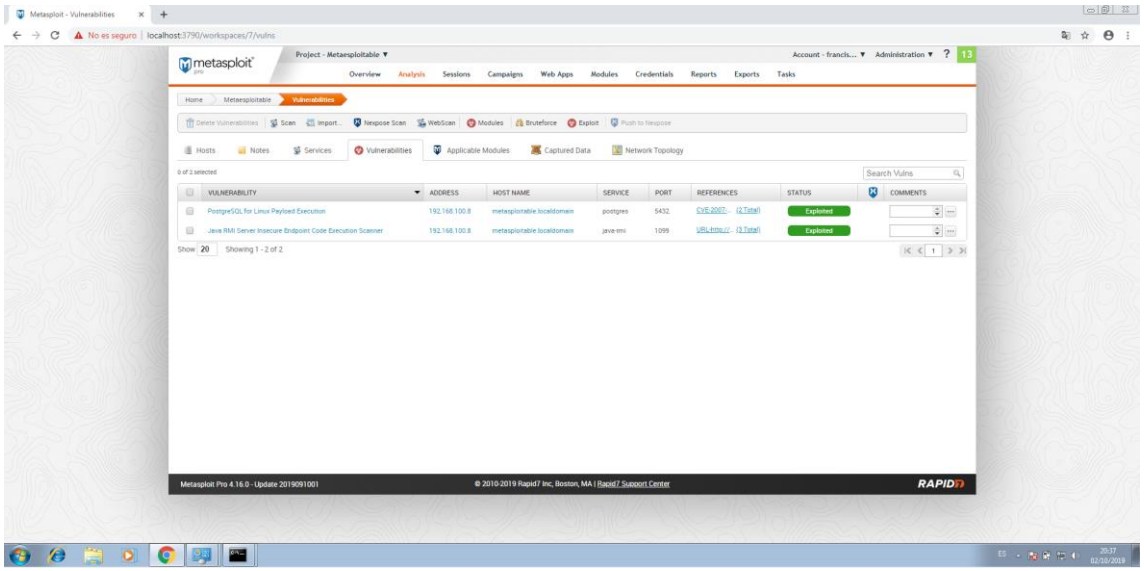
Metaesploit Pro nos generó automáticamente un reporte.



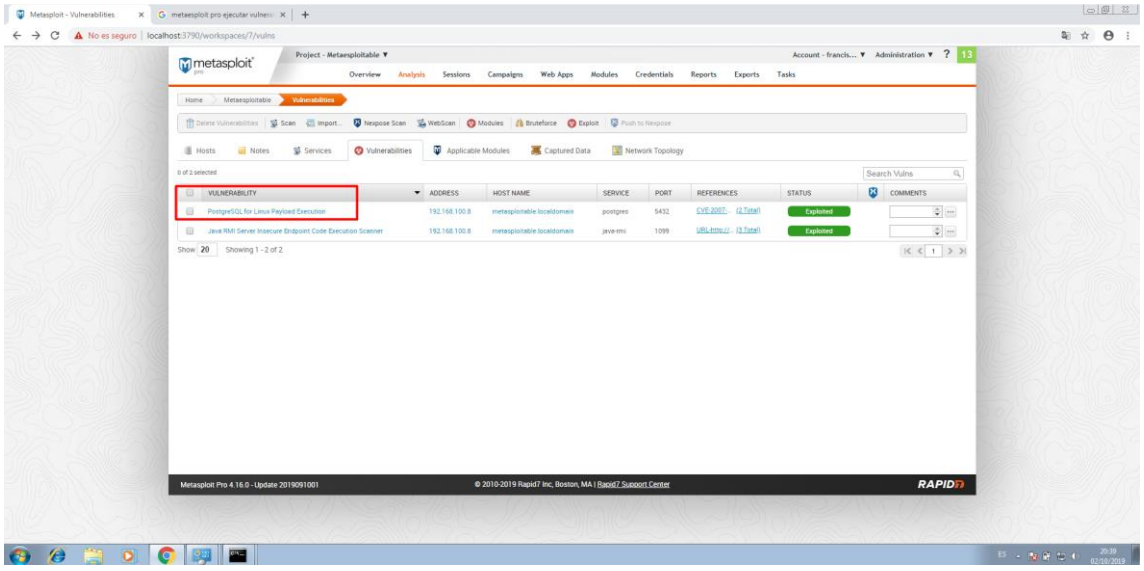


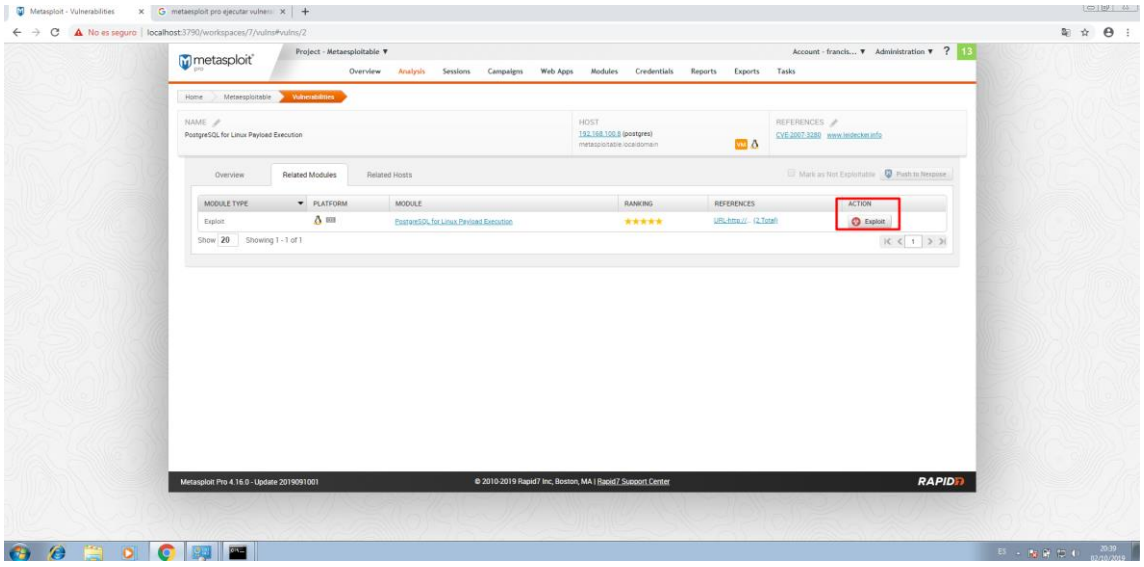
Si vamos a más detalles veremos como reconoce que es una Máquina Linux e incluso reconoce que es una máquina Metasploitable. Podemos ver sus vulnerabilidades encontradas, en este caso 2.



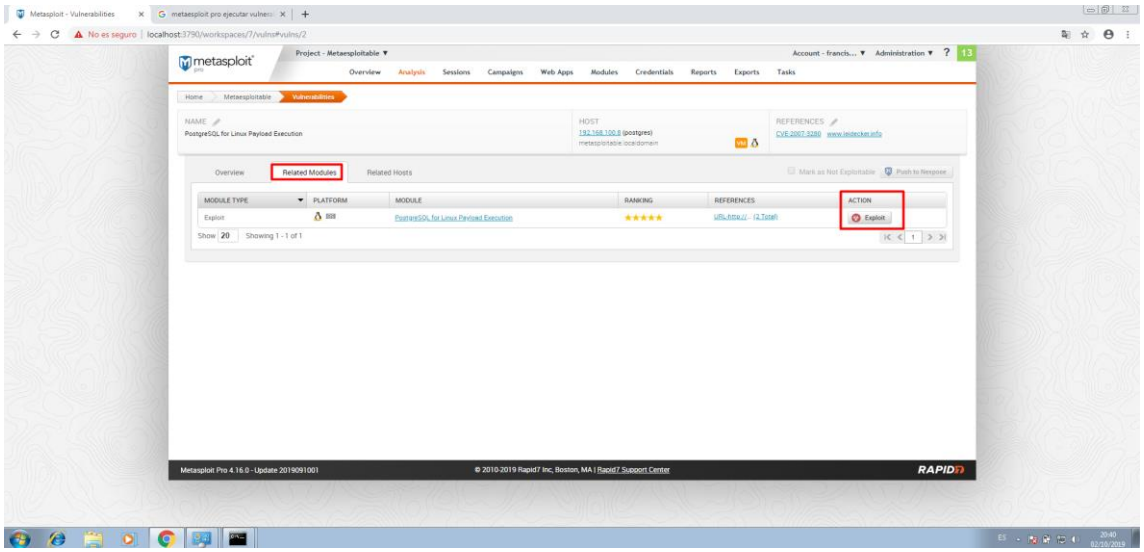


Si pulsamos sobre alguna vulnerabilidad podremos explotarla.

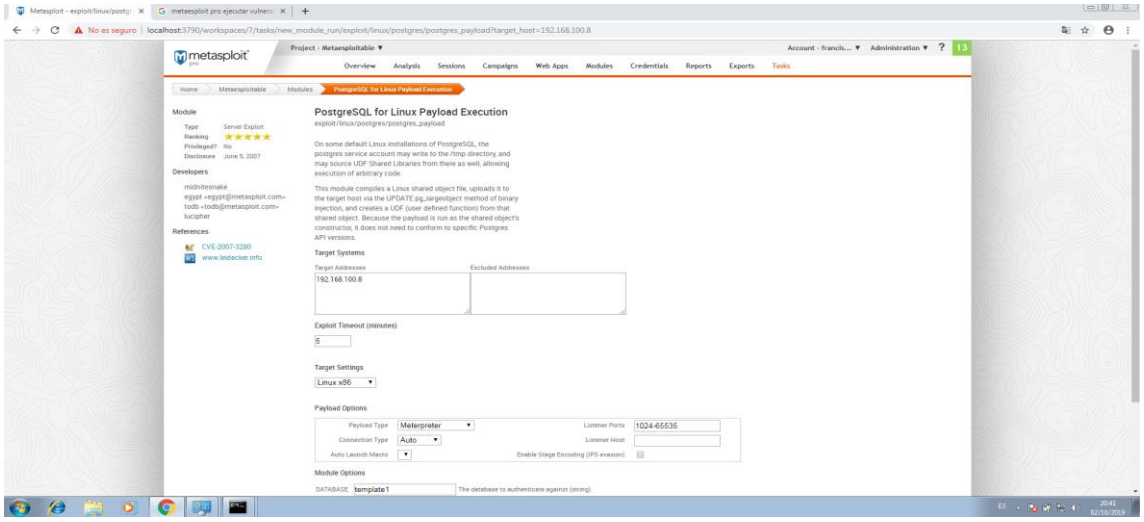




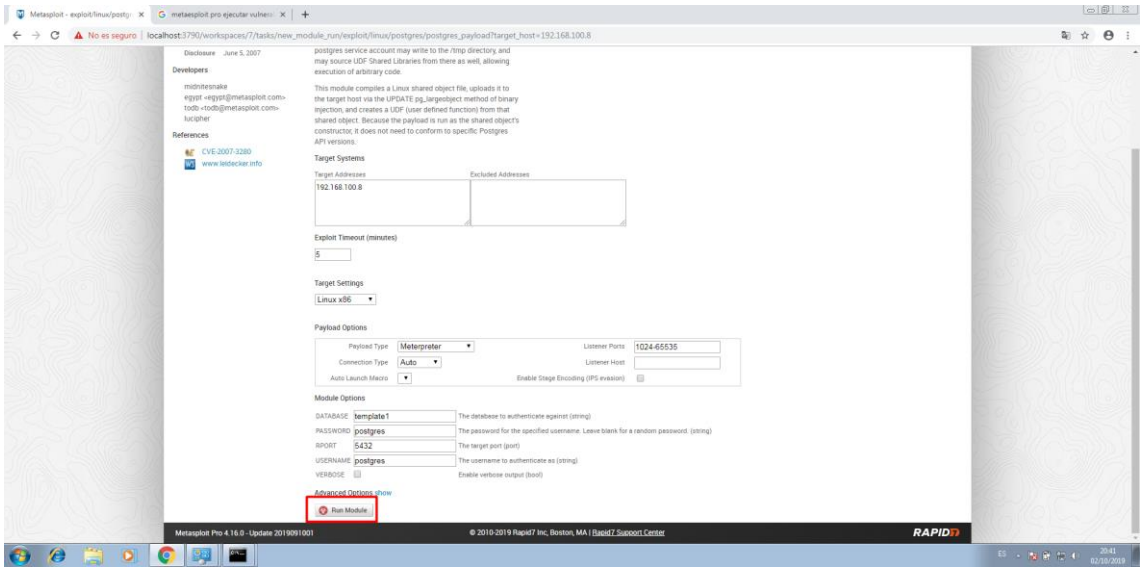
Como vemos, es una vulnerabilidad con 5 estrellas (catalogada muy grave).



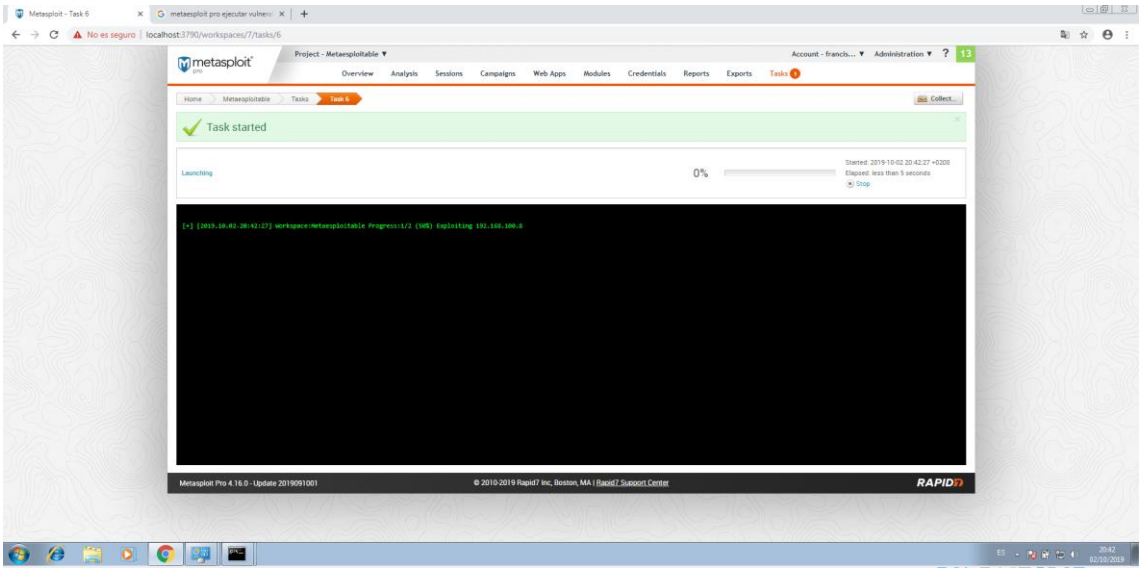
Antes de explotarla nos dará información sobre las vulnerabilidad y enlaces de referencia.



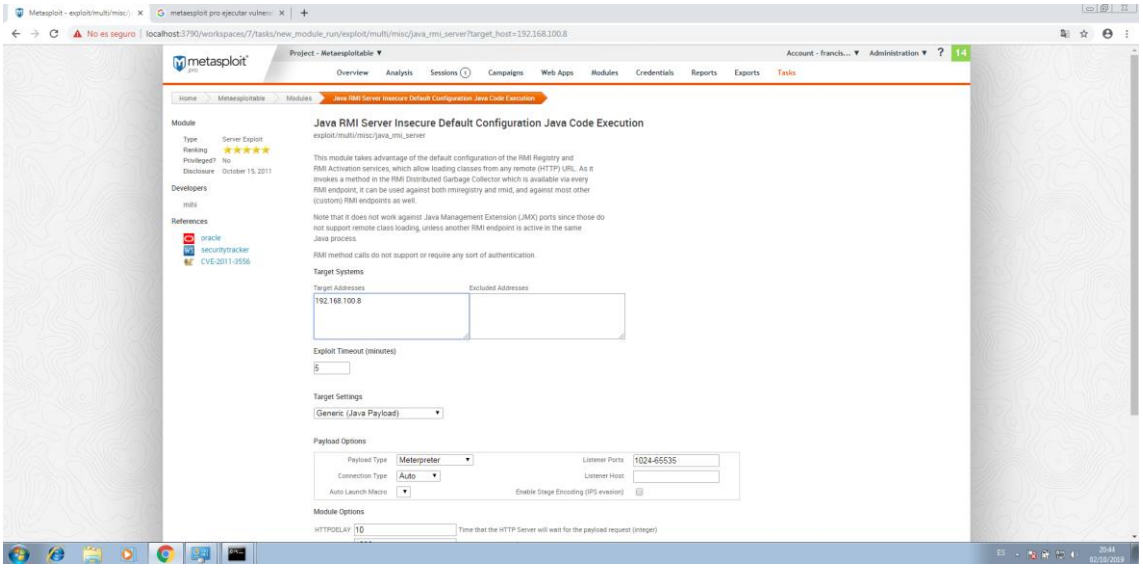
Bajaremos abajo del todo y pulsaremos en *run module.*

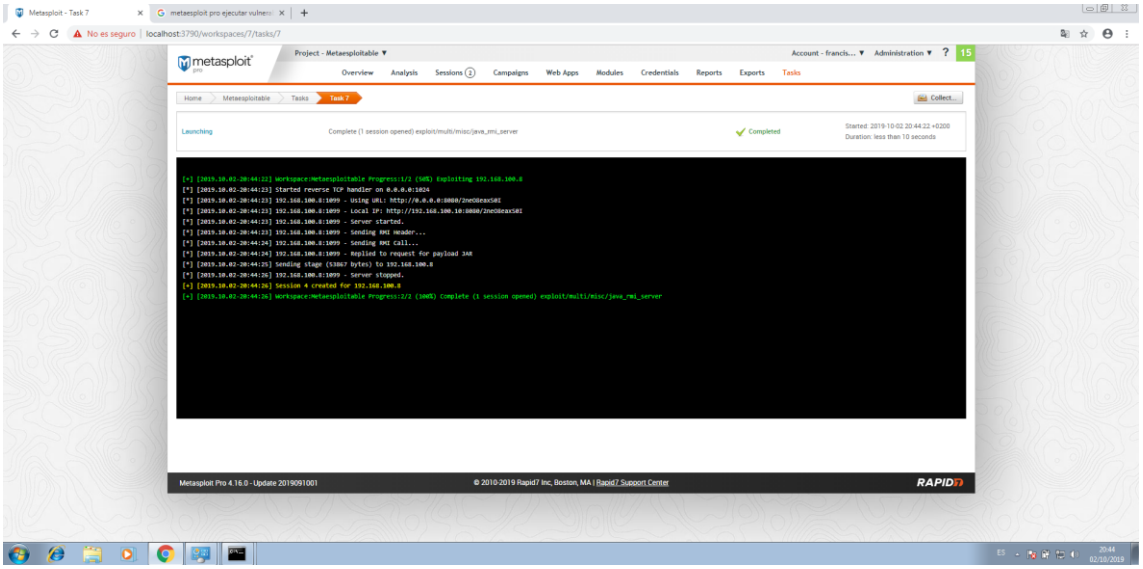


Automáticamente empezará a explotar la vulnerabilidad.

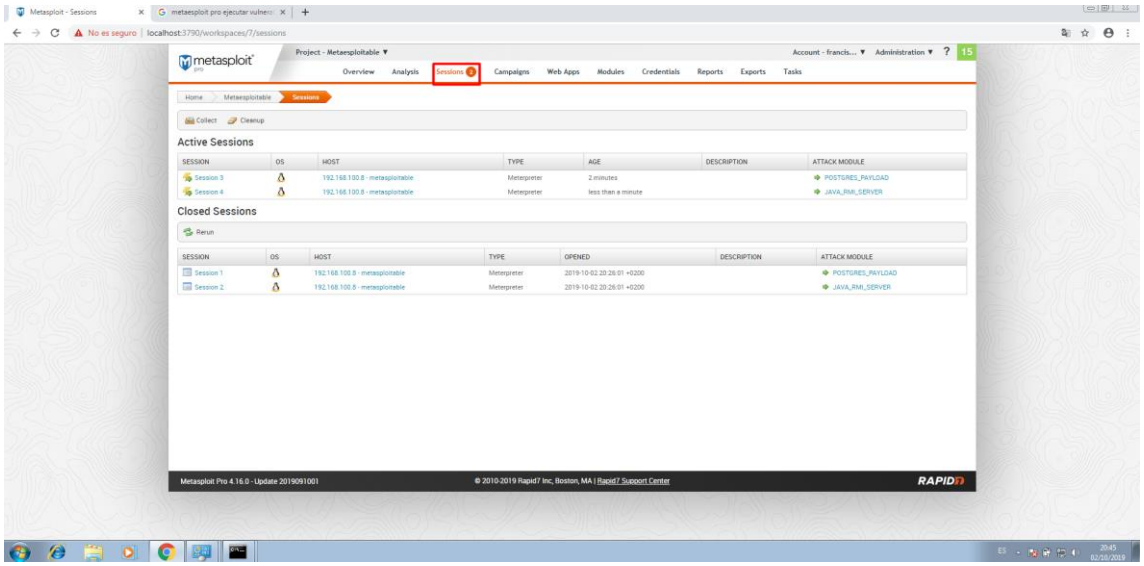


Podremos poner al mismo tiempo la otra vulnerabilidad.

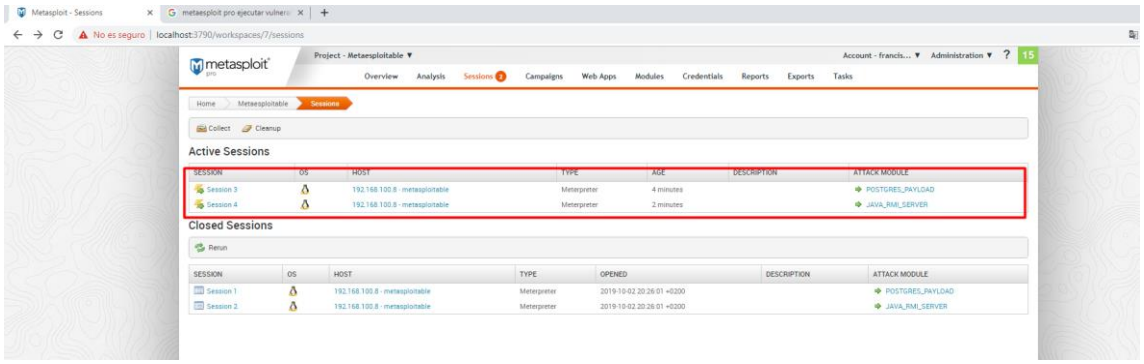


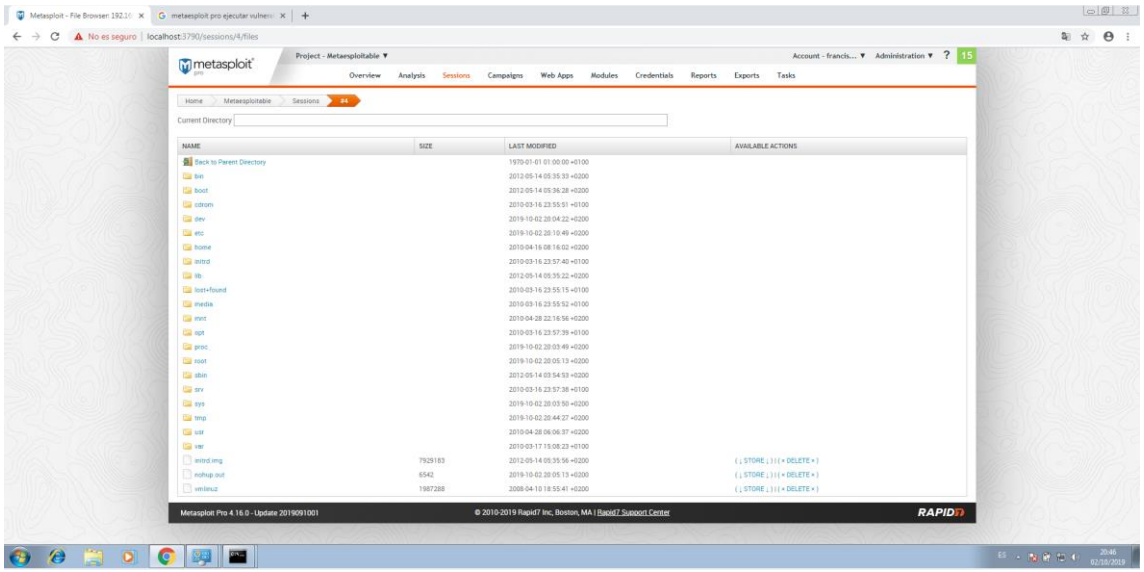


Si vamos a *Session* podremos ver los dos ataques.

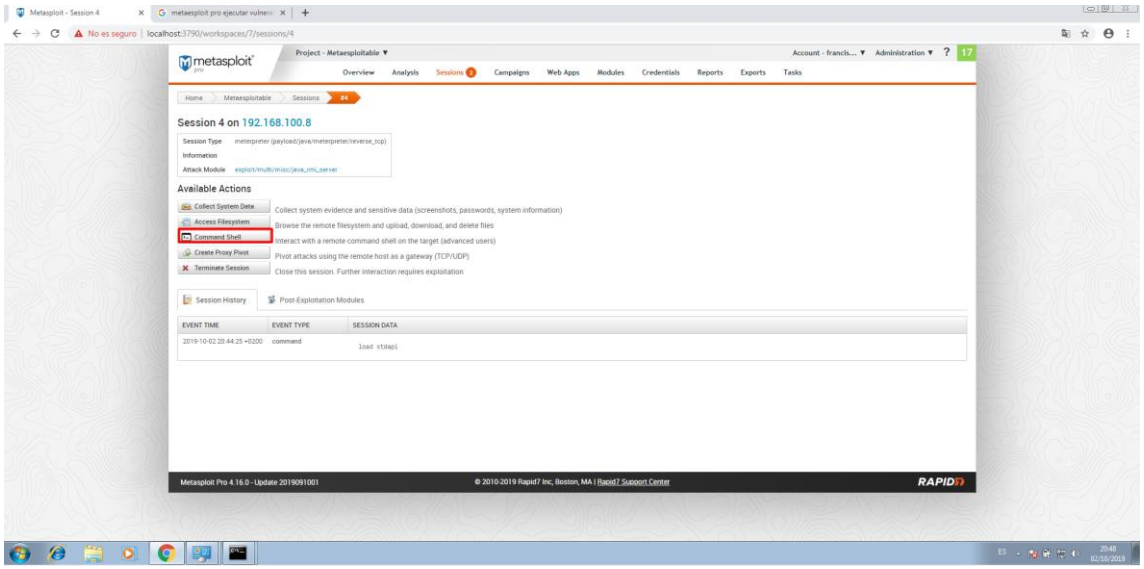


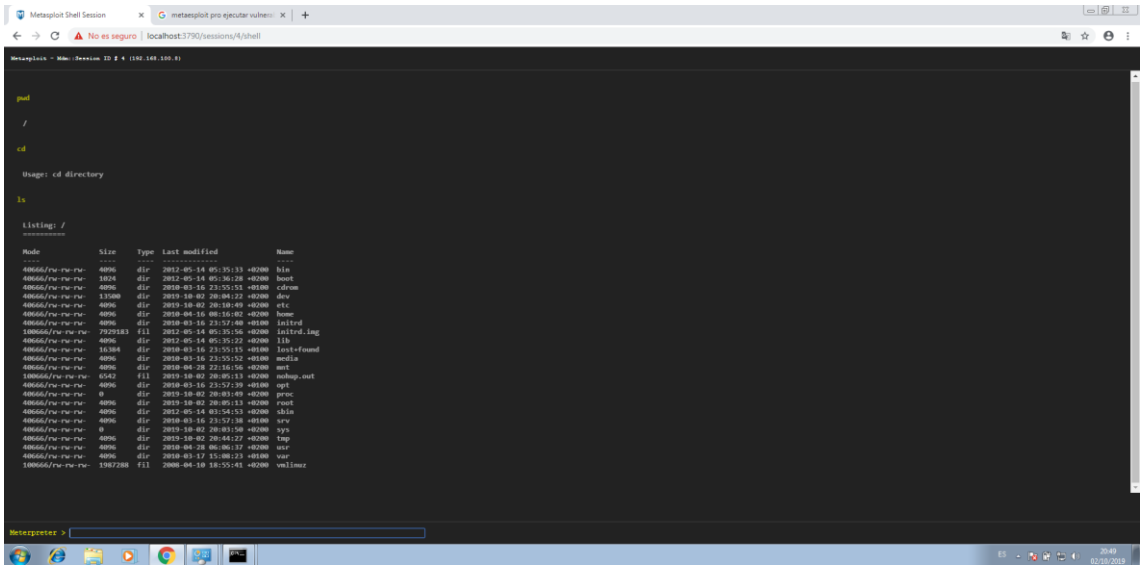
Si pulsamos sobre una de las dos sesiones **tendremos control total de la máquina.**

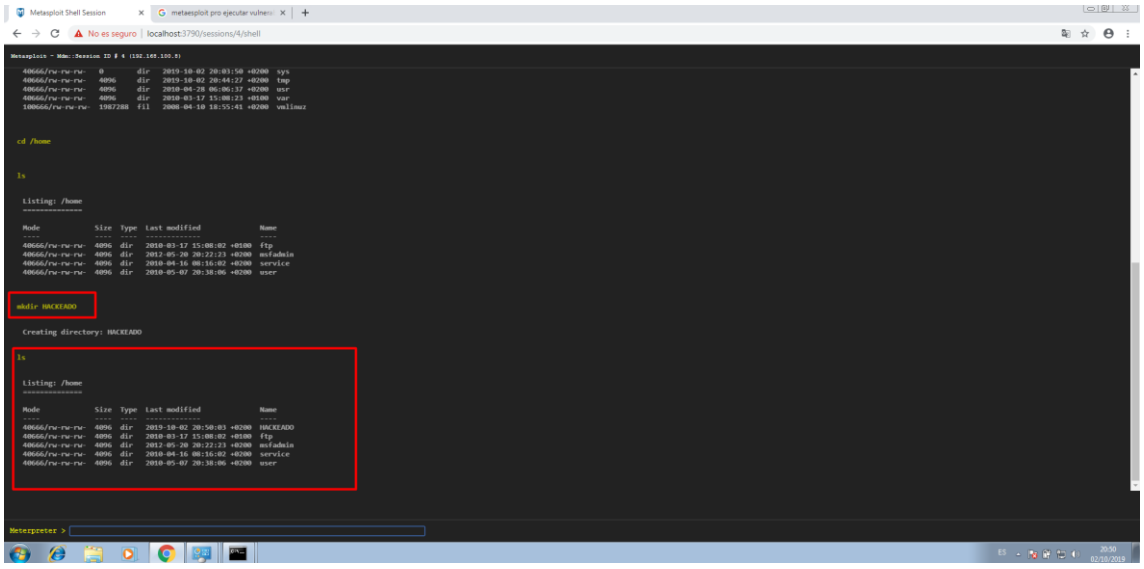




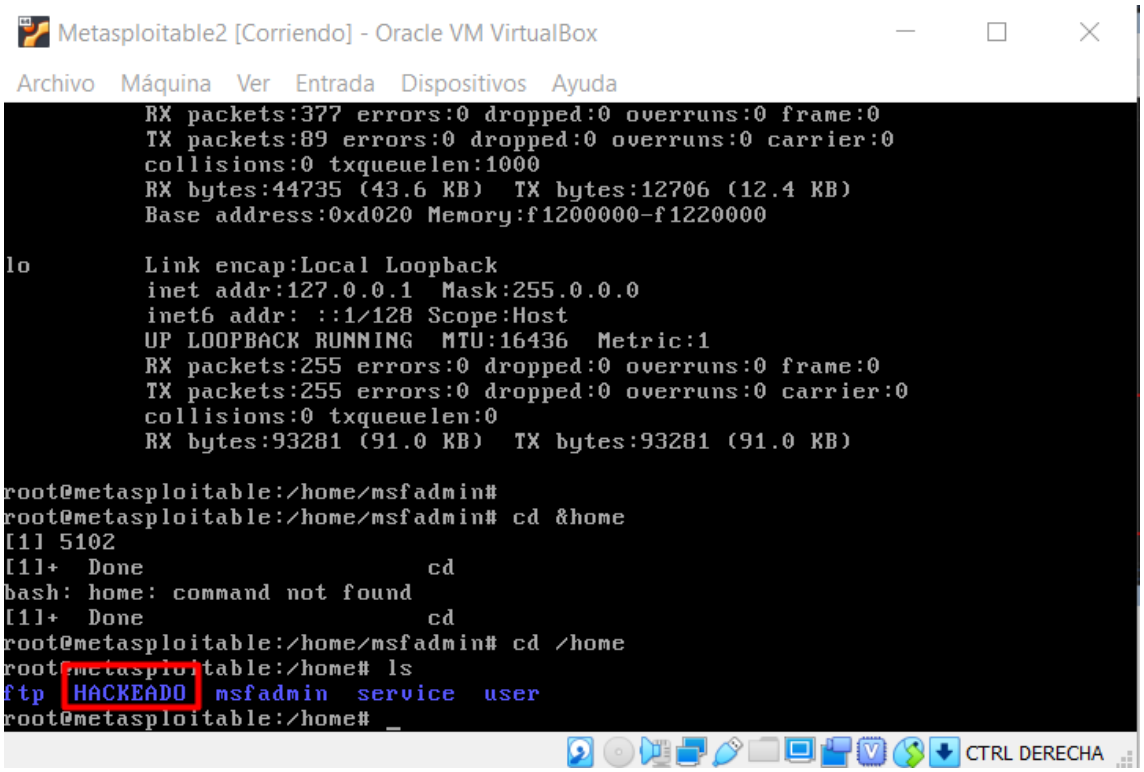
Si pulsamos en *command Shell* nos conectaremos al terminal de la máquina con **control total.**



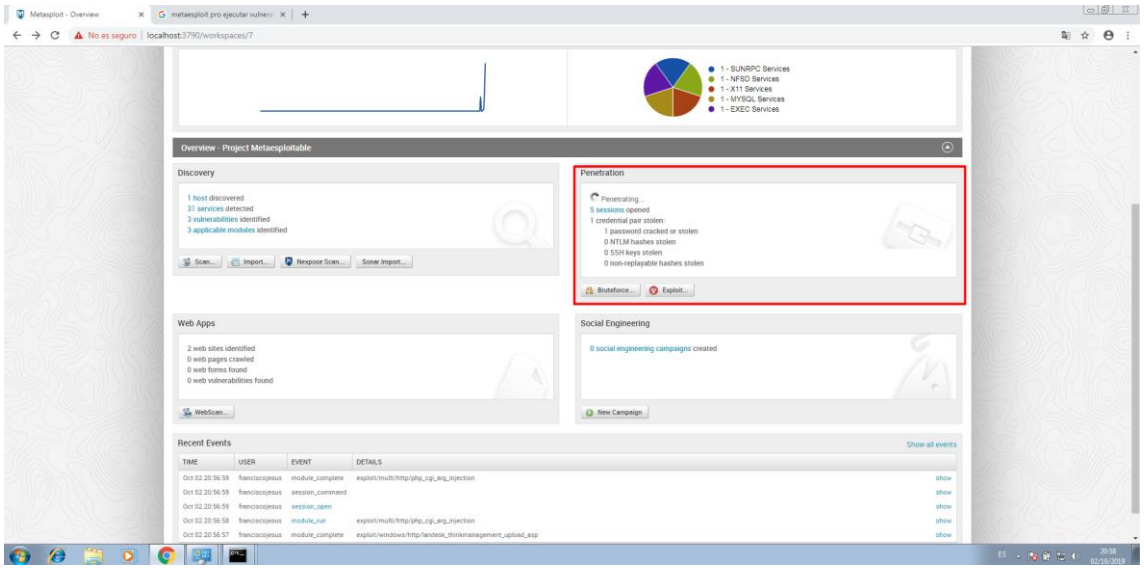




Le hemos creado una carpeta, pero si queremos le podemos borrar raíz entera y con eso fastidiar al completo el sistema.

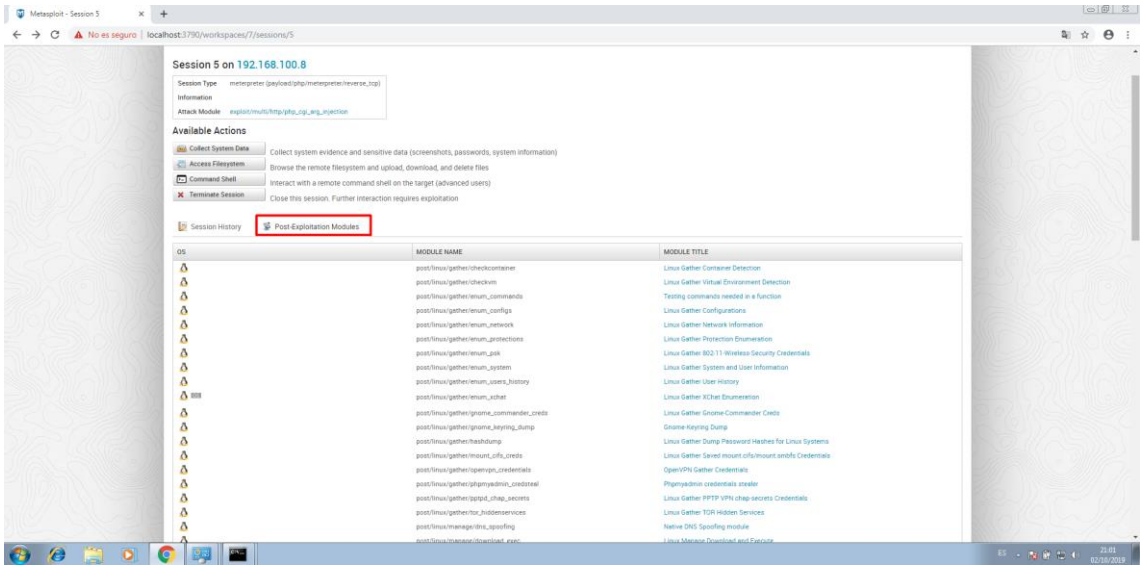


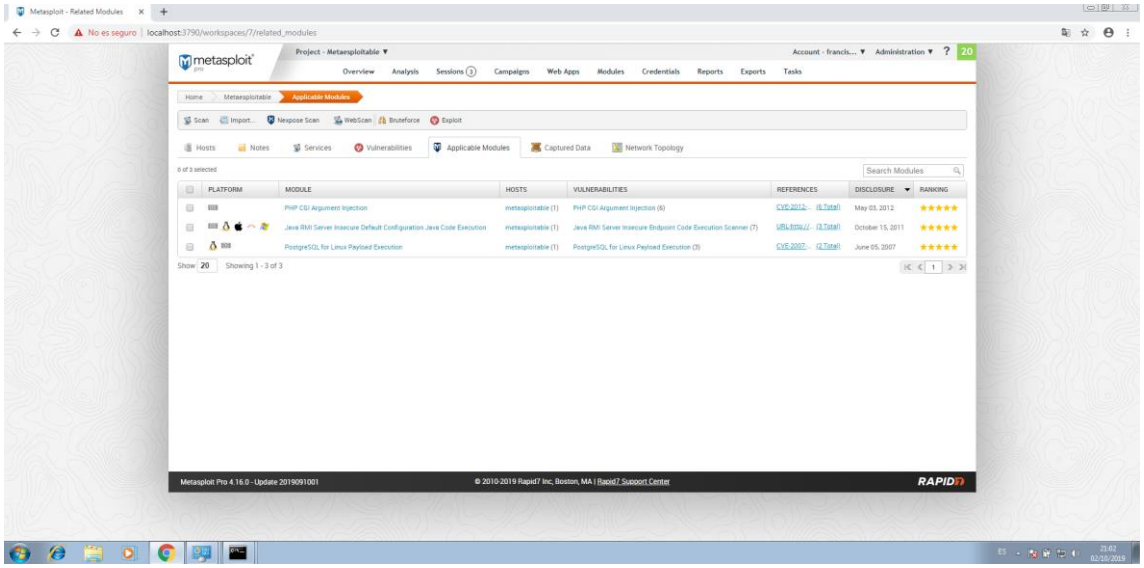
Podremos lanzar ataques de fuerza bruta para robar todas las contraseñas posibles o lanzar ataques de exploits.



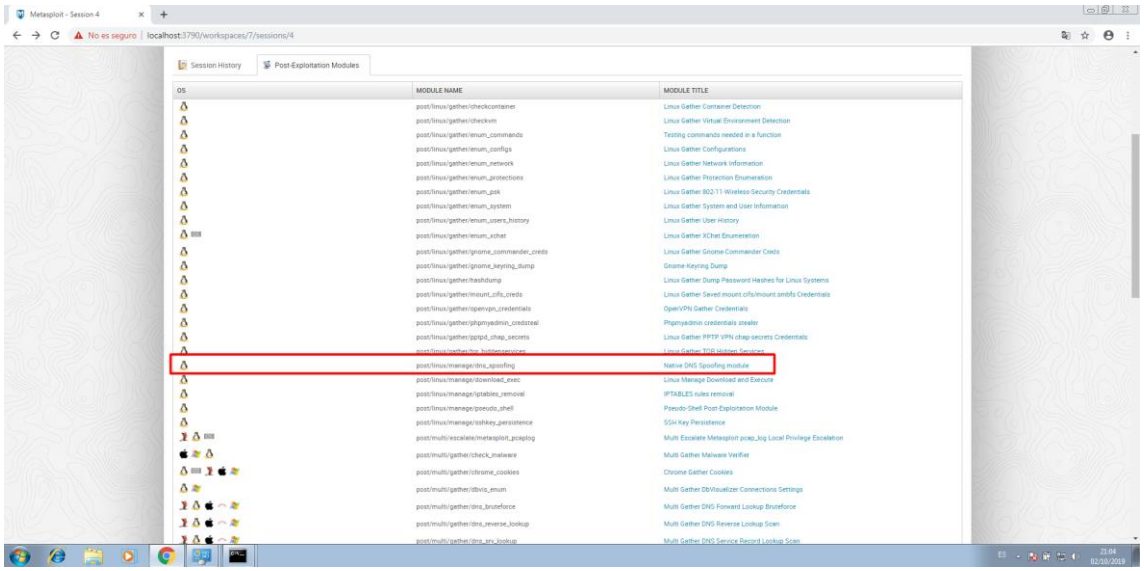
Hemos lanzado un ataque automático de exploits y se han encontrado más vulnerabilidades.

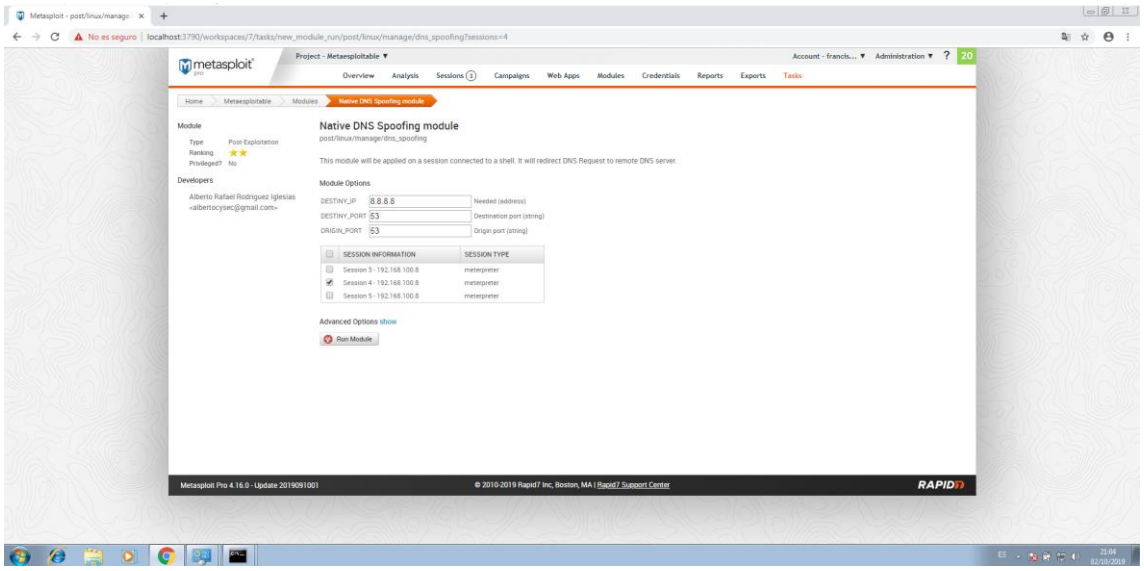
Si vamos a una vulnerabilidad y entramos en *Post-Explotation Modules* podremos explotar más vulnerabilidades.





Si queremos, le podremos cambiar los DNS por unos propios.





Creo que con esto hemos podido ver lo útil y eficaz que es Metasploit.

Conclusión

En la práctica hemos podido usar una herramienta muy potente y sencilla de usar, en ningún momento vi que era complicada de usar entrando en cosas avanzadas incluso. Comparado con Nessus me llama la atención que son aplicaciones web que entramos mediante el navegador, esto hace que sea muy práctico y útil, por ejemplo, podríamos entrar al servicio web desde oro equipo sin estar presente en él y tener Mestasploit o Nessus (o los dos) instalado en un servidor en local o que podamos acceder a él a través de la red. Entrando más en detalle me ha fascinado más Metasploit, no solo por su precio (aproximadamente 1.700€), si no por lo cómodo que es usarlo y la de cosas que se pueden realizar en él (hemos desde realizado una auditoría. Hasta recopilar información como contraseñar y vulnerar el sistema completamente), además, su instalación ha sido muy rápida y sencilla. Sin duda las dos herramientas son grandes utilidades profesionales para empresas.