

# Monitoreo y grabación de la actividad web con Power Spy 2014

*El software Power Spy 2014 le permite monitorear y registrar en secreto todas las actividades en su computadora, lo cual es completamente legal.*

## Objetivos del laboratorio

Este objetivo de este laboratorio es ayudar a los estudiantes a usar la herramienta Monitor de actividad. Después de completar este laboratorio, los estudiantes podrán:

- Instalar y configurar Power Spy 2014
- Monitoree las pulsaciones de teclado, los sitios web visitados y los datos de tráfico internos.

## Visión general del laboratorio

Esta práctica de laboratorio demuestra a los alumnos cómo establecer una conexión de escritorio remoto con una máquina víctima y ejecutar Power Spy para realizar un seguimiento secreto de las actividades de los usuarios.

- Esta práctica de laboratorio solo funciona si la máquina de destino está encendida.
- Como ha visto cómo escalar privilegios en el laboratorio anterior (Escalating Privileges by Exploiting Client Side Vulnerabilities), usará la misma técnica para escalar privilegios y luego volcar los hashes de contraseña.
- Al obtener los hashes, utilizará la aplicación de descifrado de contraseñas como RainbowCrack para obtener contraseñas de texto sin formato.
- Una vez que tenga las contraseñas a mano, establecerá una Conexión de escritorio remoto como atacante, instalará Power Spy y lo dejará en modo oculto.

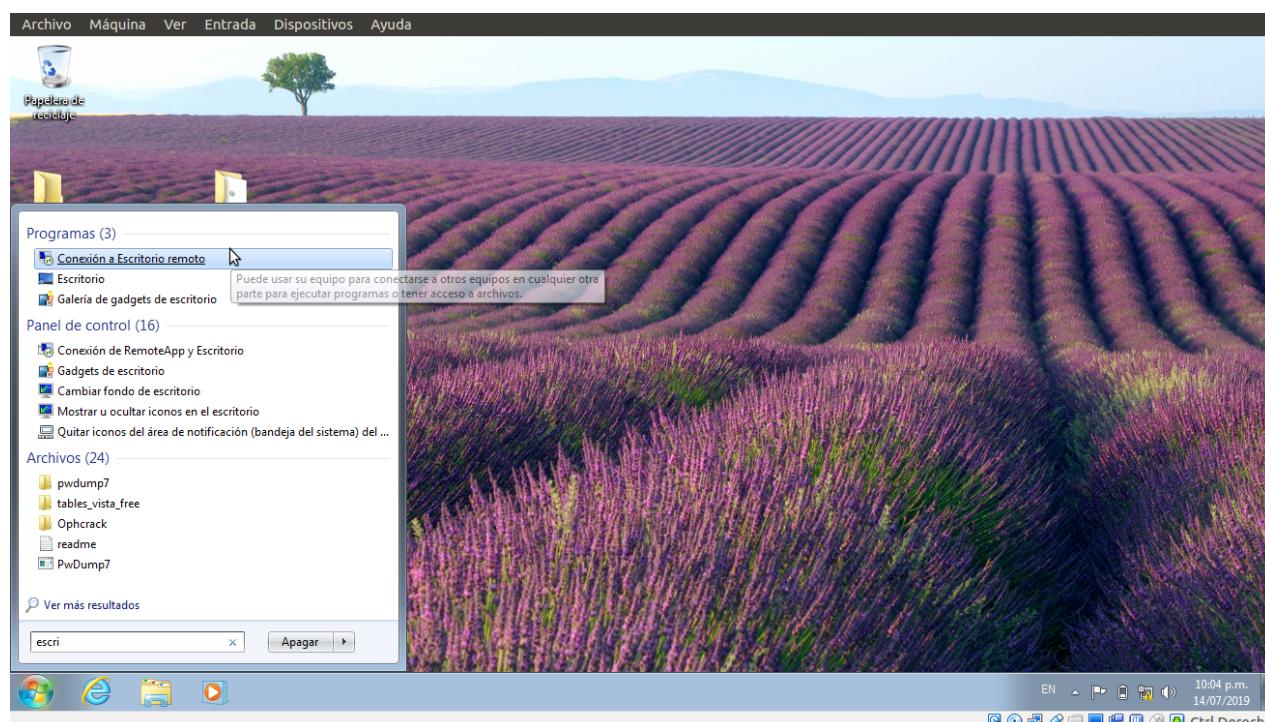
**Nota:** En esta práctica de laboratorio, se está conectando de forma remota a una máquina virtual de Windows Server 2016. Puede establecer una conexión remota

solo para una cuenta de usuario con privilegios administrativos (aquí, Administrador tiene privilegios administrativos)

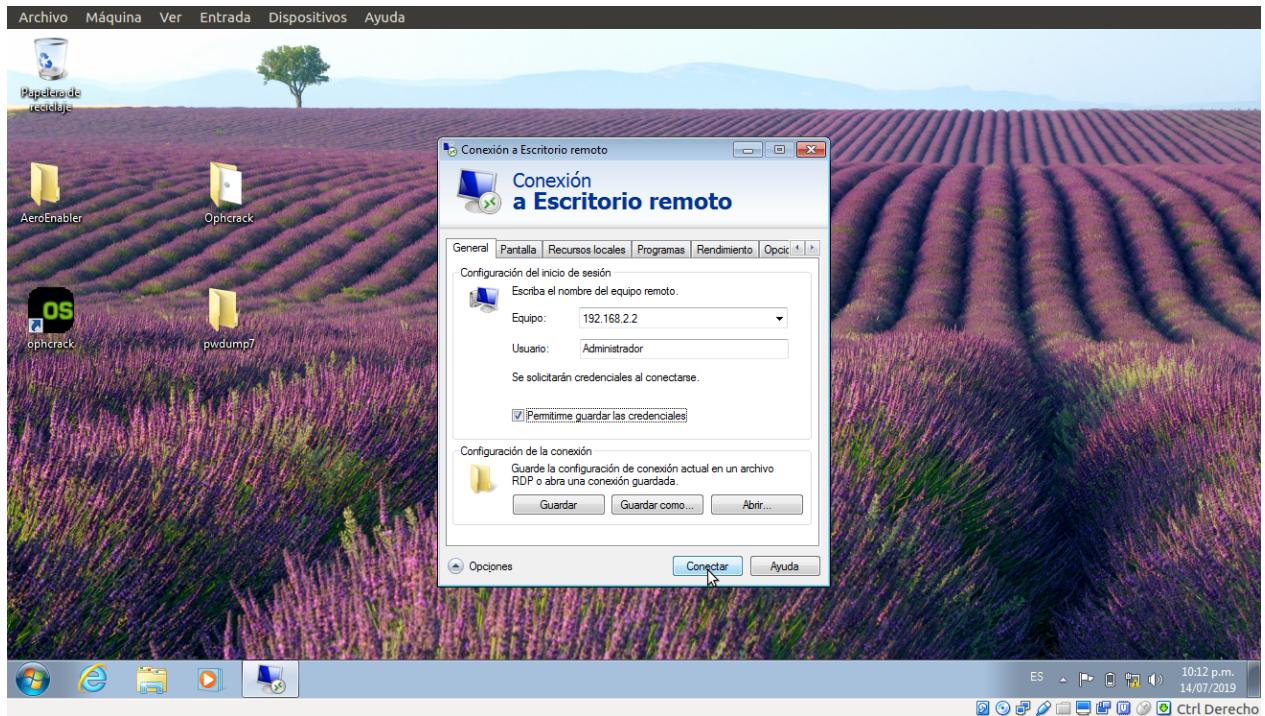
- La próxima tarea será iniciar sesión en la máquina virtual como un usuario legítimo (en este caso, usted) y realizar las actividades del usuario sin tener conocimiento de la aplicación que realiza el seguimiento de sus actividades.
- Una vez hecho esto, volverá a establecer una Conexión de escritorio remoto como un atacante, sacará la aplicación del modo invisible y supervisará las actividades realizadas en las máquinas virtuales por la víctima (usted)

## Tareas del laboratorio

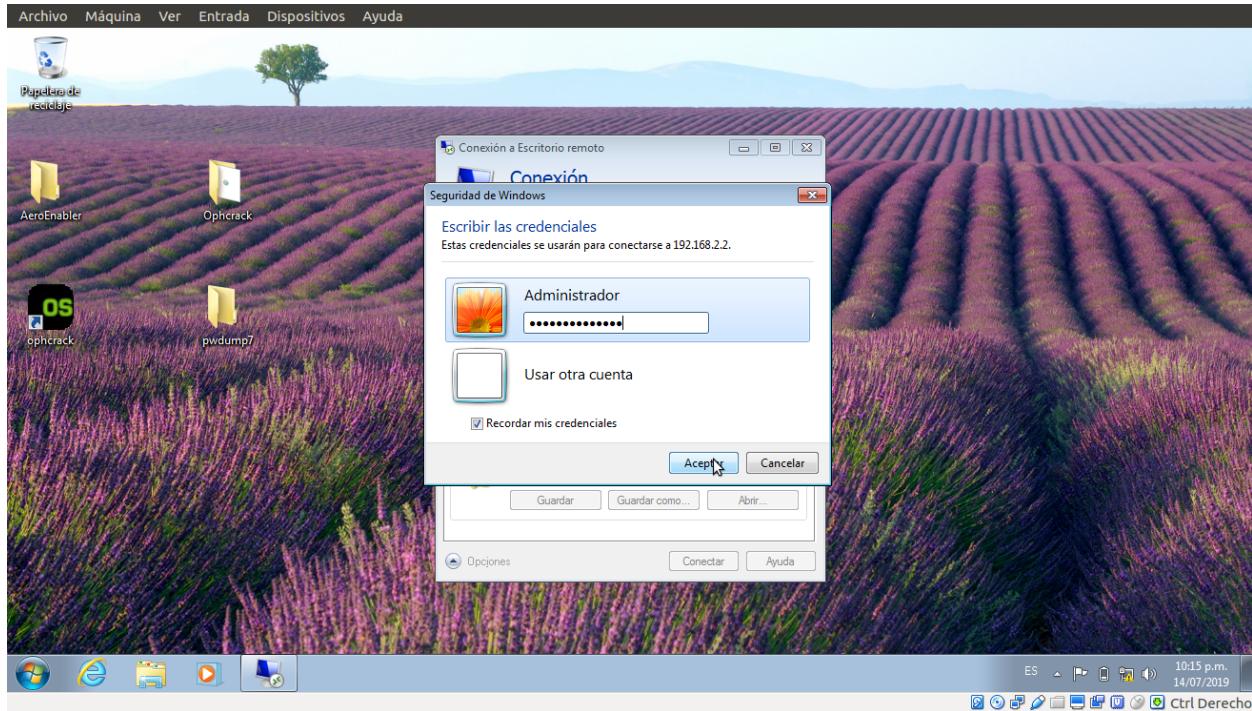
1. Haga clic derecho en el ícono de Windows, y haga clic en Buscar
2. En el panel derecho, busque **Conexión a Escritorio remoto**.
3. Haga clic en **Conexión a escritorio remoto** en el campo Buscar.



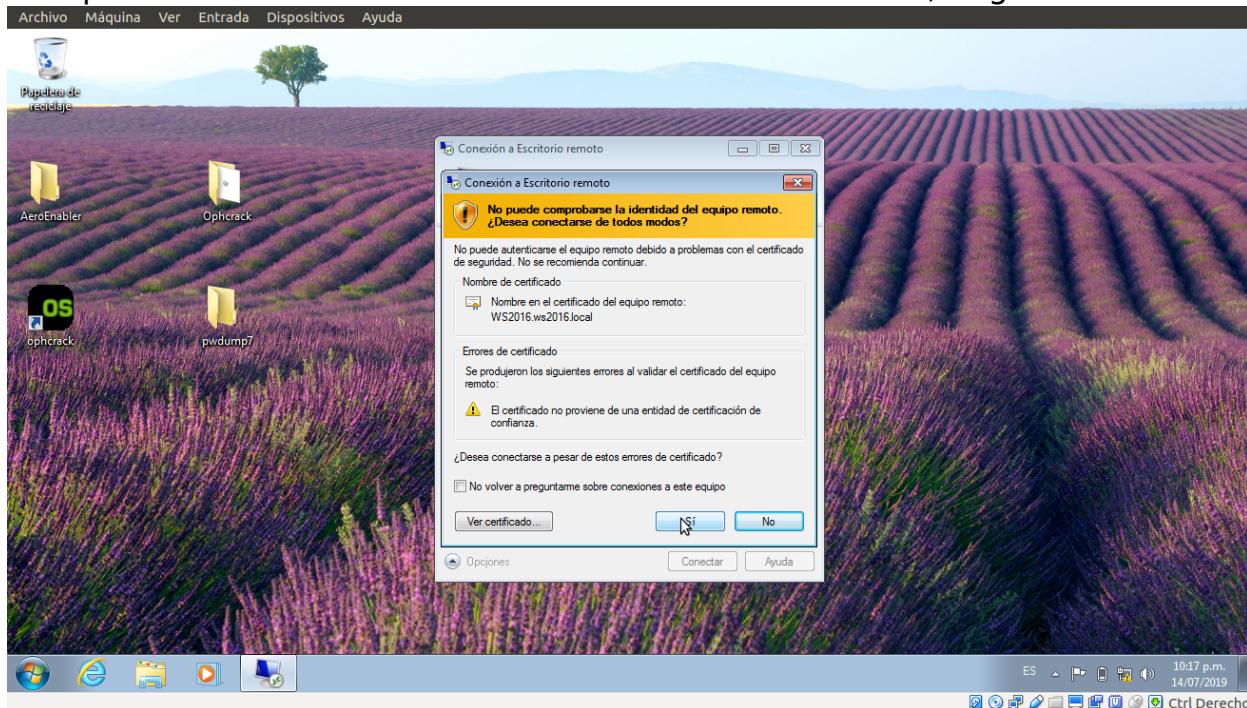
4. Aparece la ventana de conexión de escritorio remota; ingrese la dirección IP de **Windows Server 2016** (en este laboratorio, **192.168.2.2**, que podría diferir en su entorno de laboratorio) en el campo **Computadora** y haga clic en **Mostrar opciones**.
5. Ingrese un **nombre de usuario** cuya cuenta tenga privilegios administrativos (aquí, **Administrador**) y haga clic en Conectar.



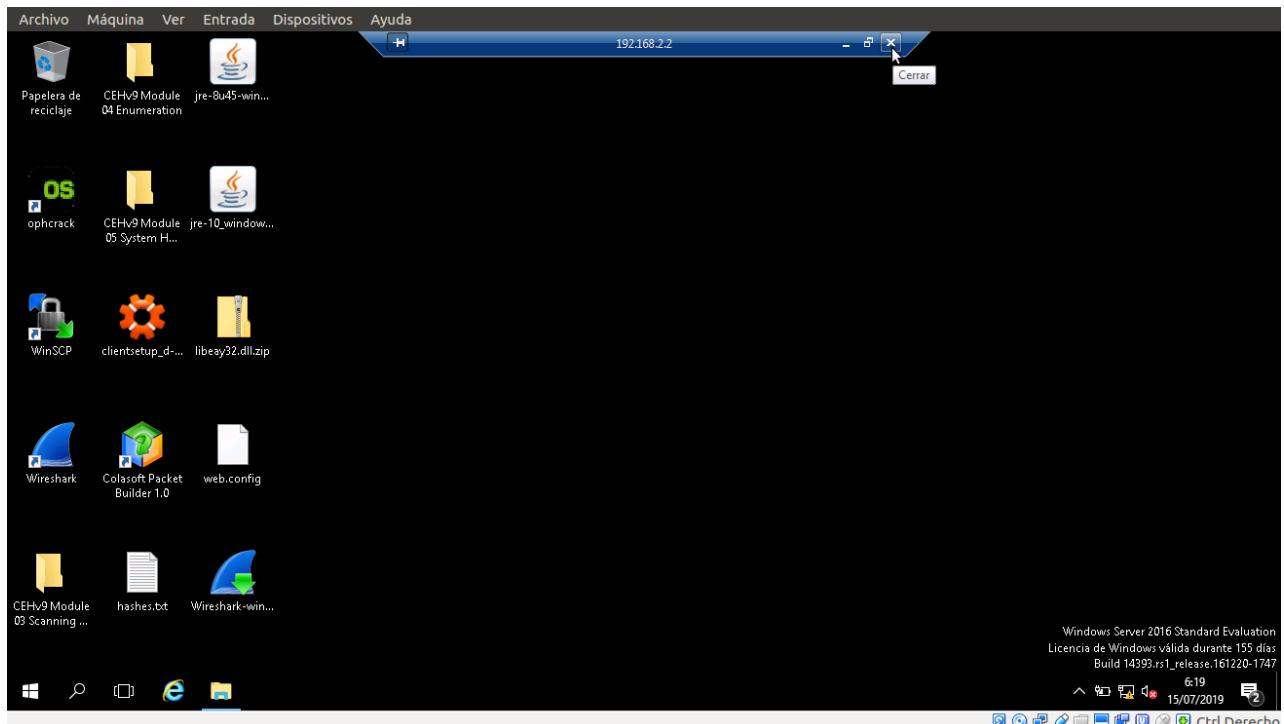
6. La máquina host intenta establecer una conexión remota con la máquina de destino.
7. Aparece una ventana emergente de **seguridad de Windows**, ingrese la contraseña y haga clic en **Aceptar**.



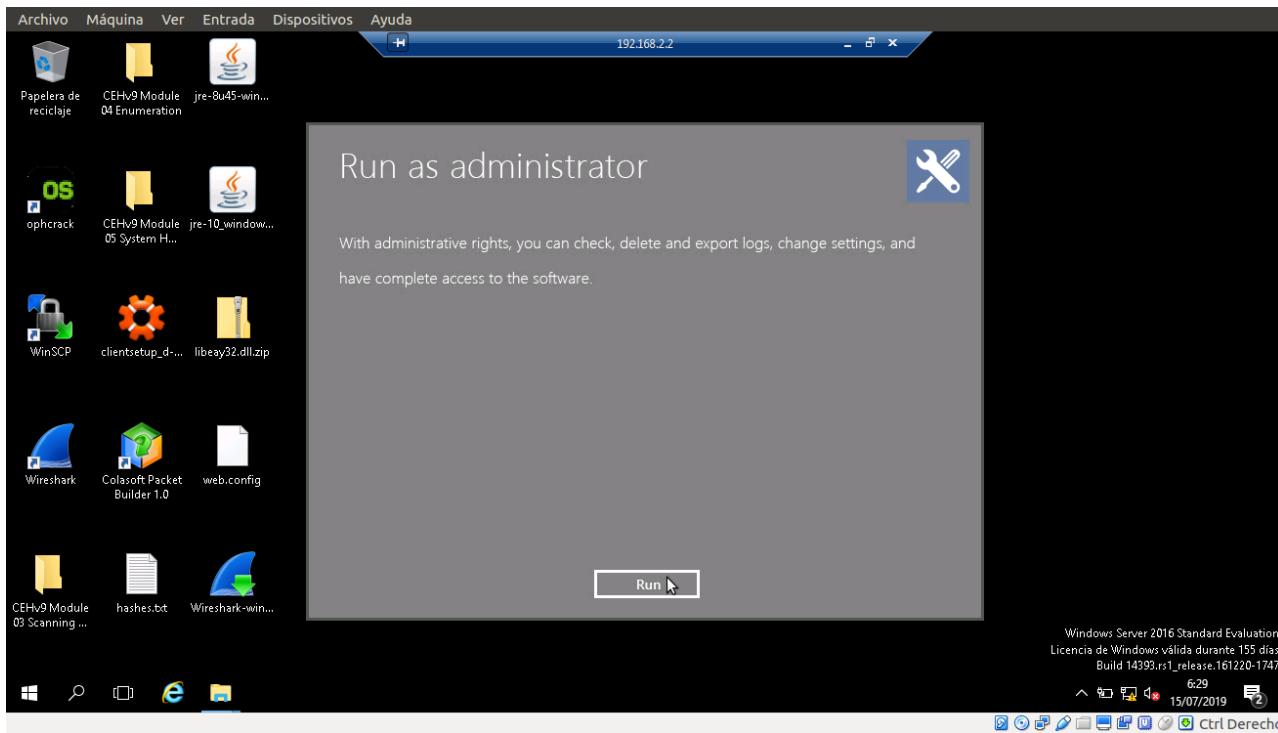
8. Aparece una ventana de Conexión a Escritorio remoto; haga clic en **Sí**.



9. Se estableció con éxito una **conexión de Escritorio remoto**, como se muestra en la siguiente captura de pantalla.

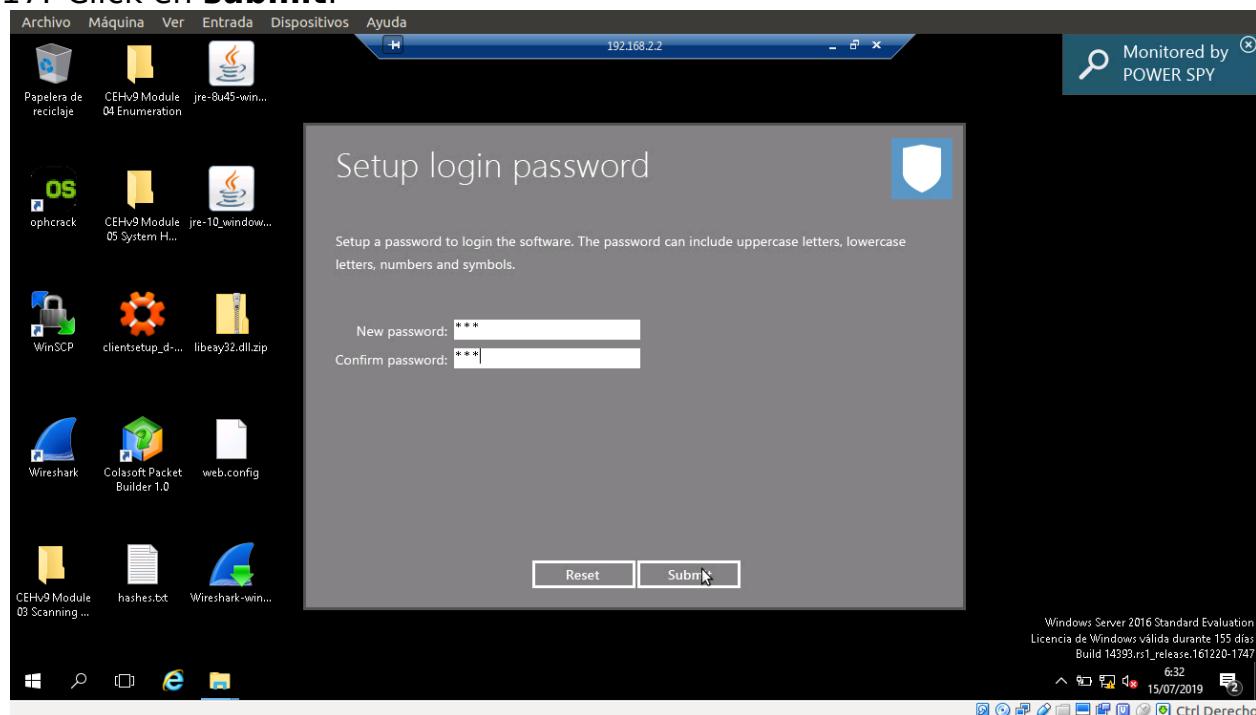


10. Cierre la ventana del administrador del servidor.
11. Navegar a la carpeta donde tengas el ejecutable de **Power Spy 2014**.
12. Doble click en pcspy14.exe
13. Si aparece la ventana emergente Abrir archivo - Advertencia de seguridad, haga clic en **Ejecutar**.
14. Siga los pasos de instalación para instalar **Power Spy**.
15. Al completar la instalación, aparece la ventana **Run as administrator**, haga clic en **Run**.



16. Aparece la ventana de configuración de la contraseña de inicio de sesión; ingrese la contraseña en los campos **New Password** y **Confirm Password**.

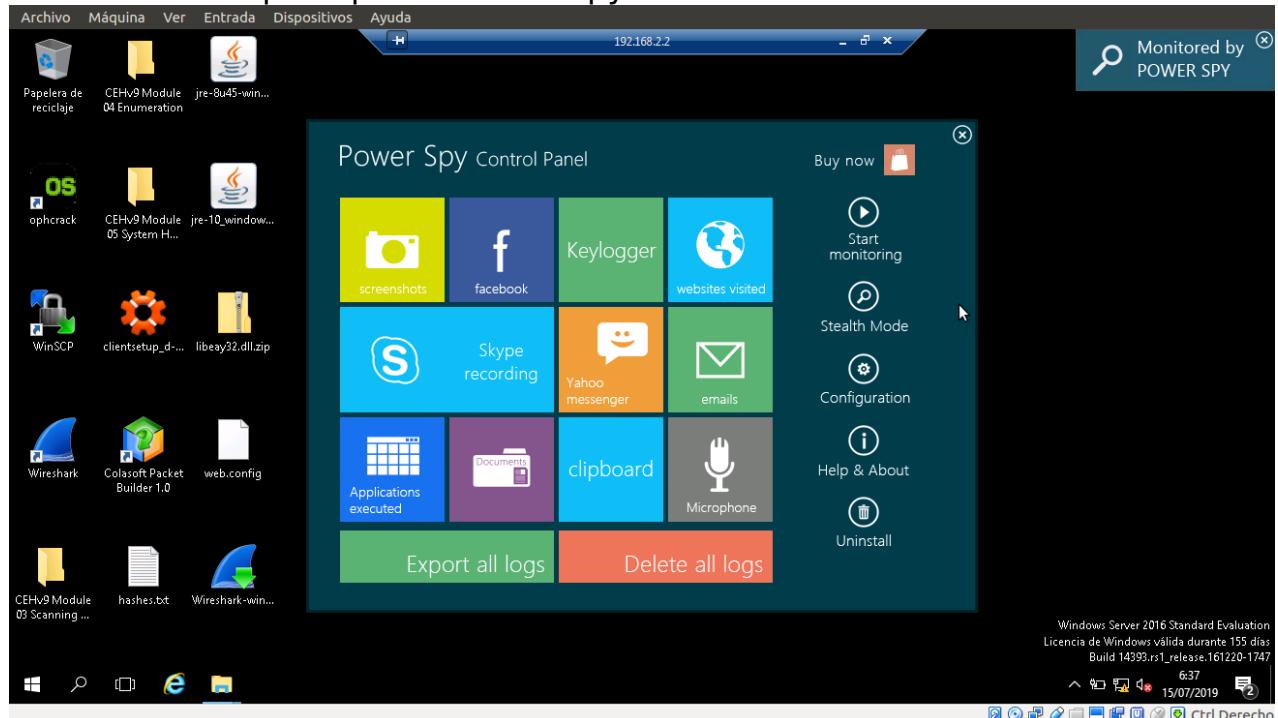
17. Click en **submit**.



18. ¡Bienvenido al panel de control de Powero Spy! La página web aparece en el navegador predeterminado. Cierra el navegador.

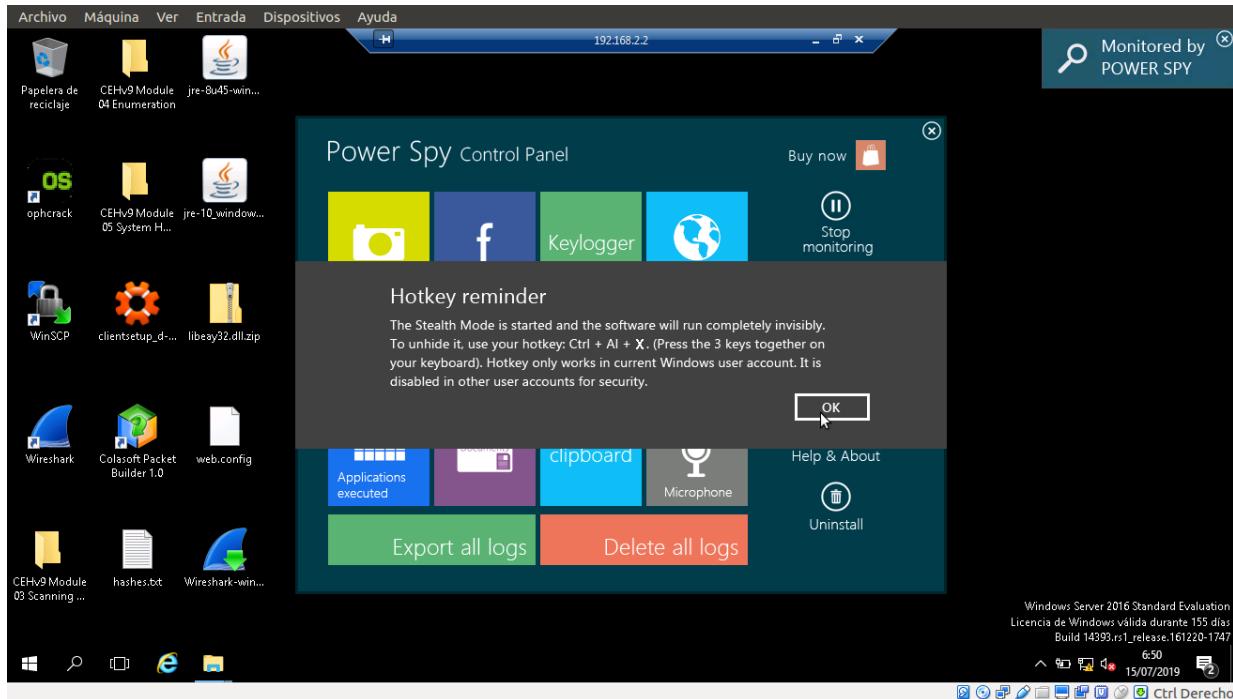
19. Si aparece la ventana emergente del filtro de phishing de Microsoft, seleccione Preguntarme más tarde.
20. El cuadro de diálogo de información aparece en la ventana de configuración de la contraseña de **inicio de sesión**, haga clic en **Aceptar**.
21. Aparece la ventana **Ingresar contraseña de inicio de sesión**; ingrese la contraseña (que usted estableció en el **paso 16**).
22. click submit.
23. Aparece la ventana **Registrar producto**; haga clic **más tarde** para continuar.

24. La ventana principal de Power Spy se abre como se muestra a continuación.

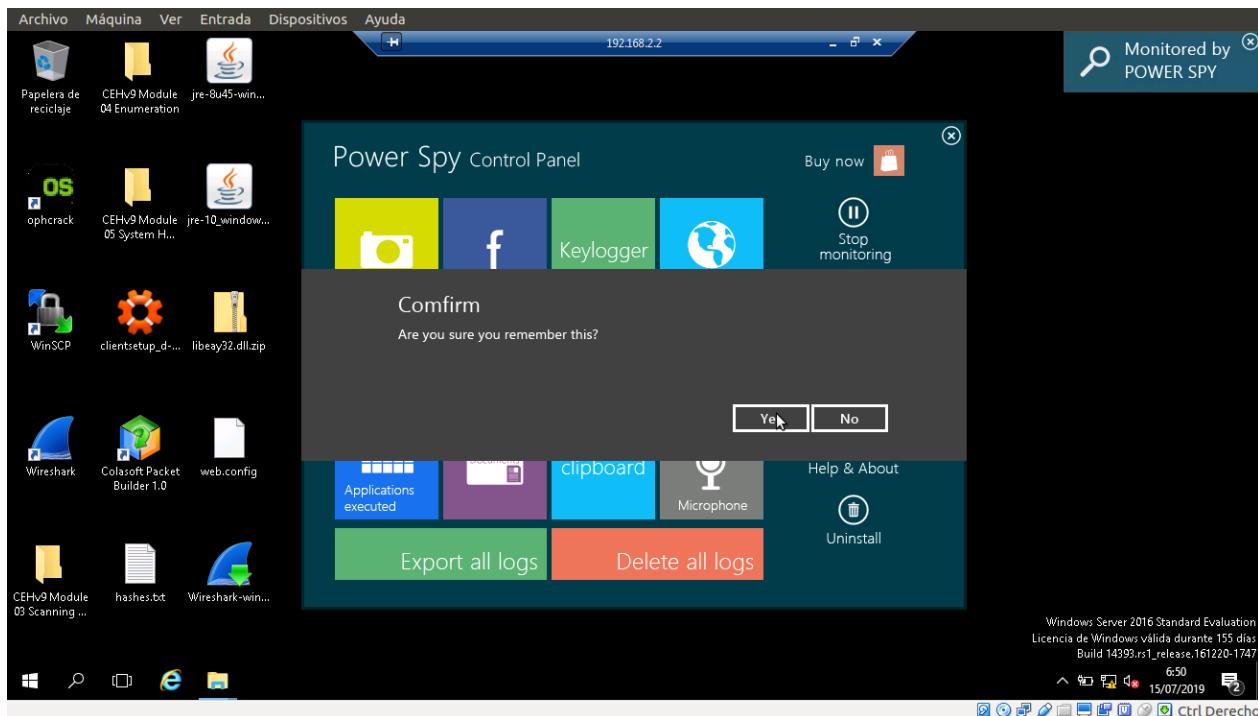


25. Haga clic en Iniciar monitoreo.
26. Si aparece la ventana **Recomendado para reiniciar el sistema**, haga clic en **Aceptar**.
27. Haga clic en **Modo invisible** (Power Spy se ejecuta completamente invisible en la computadora).

28. Aparece el cuadro de diálogo de recordatorio de teclas rápidas; haga clic en **Aceptar** (para mostrar las teclas Power Spy, Usar **Ctrl + Alt + X**) en el teclado de su PC.

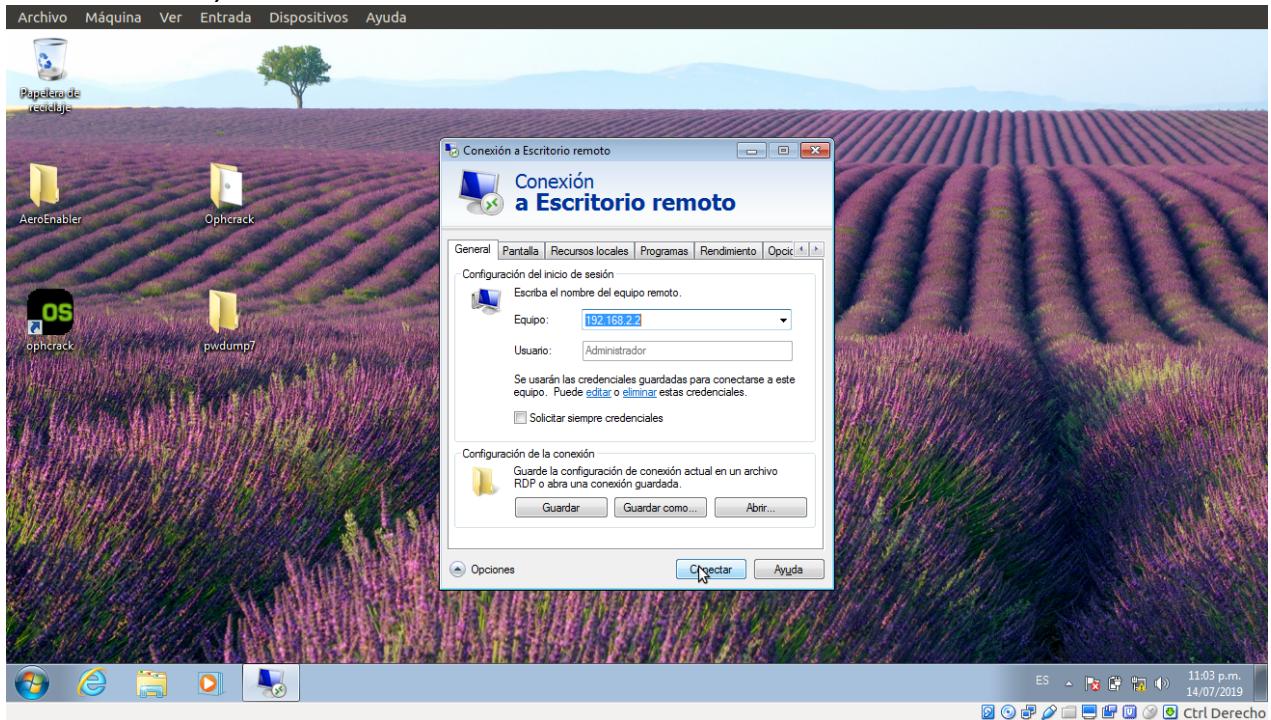


29. Aparece el cuadro de diálogo **Confirmar**; haga clic en **Sí**.

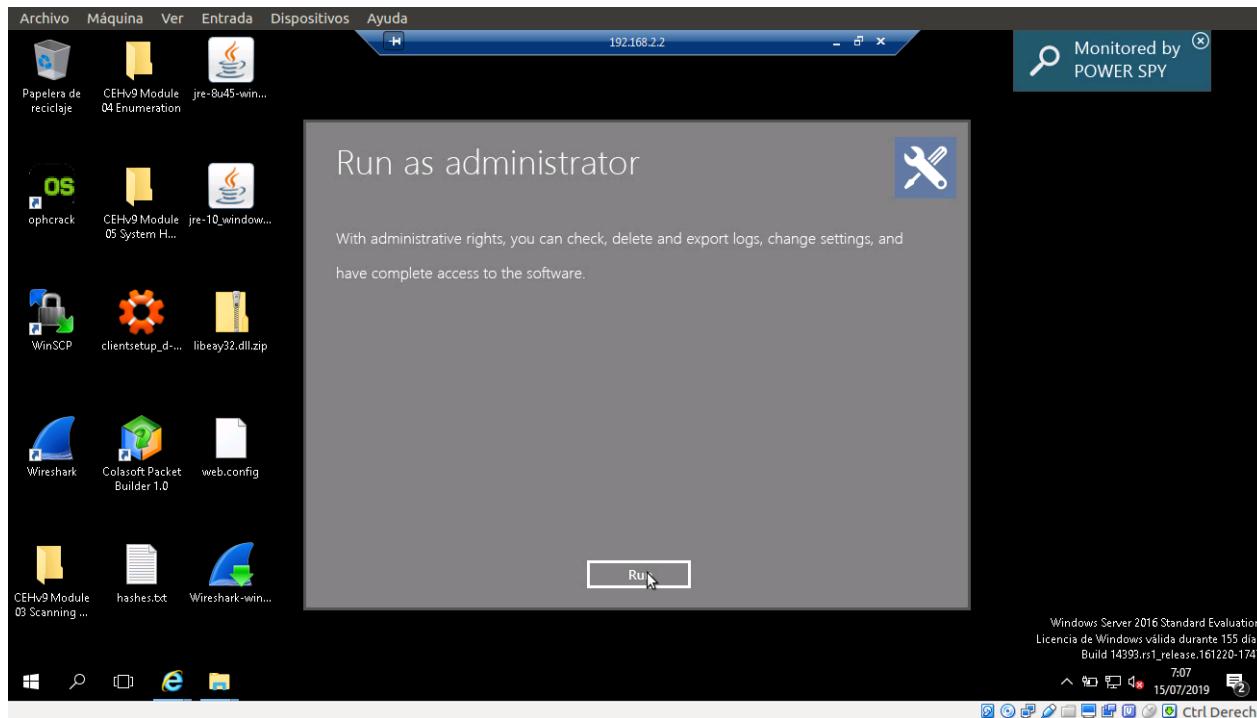


30. Cierre la conexión de escritorio remoto.

31. Inicie sesión en la cuenta de Administrador de la máquina virtual de Windows Server 2016 como usuario legítimo (en este caso, suponga que está actuando como víctima).
32. Navega por internet o realiza alguna actividad de usuario. En este laboratorio se han navegado los sitios web de Facebook y Mega.
33. Una vez que haya realizado algunas actividades de usuario, siga los pasos 1-8 para iniciar la Conexión a Escritorio remoto, (está iniciando sesión como atacante).

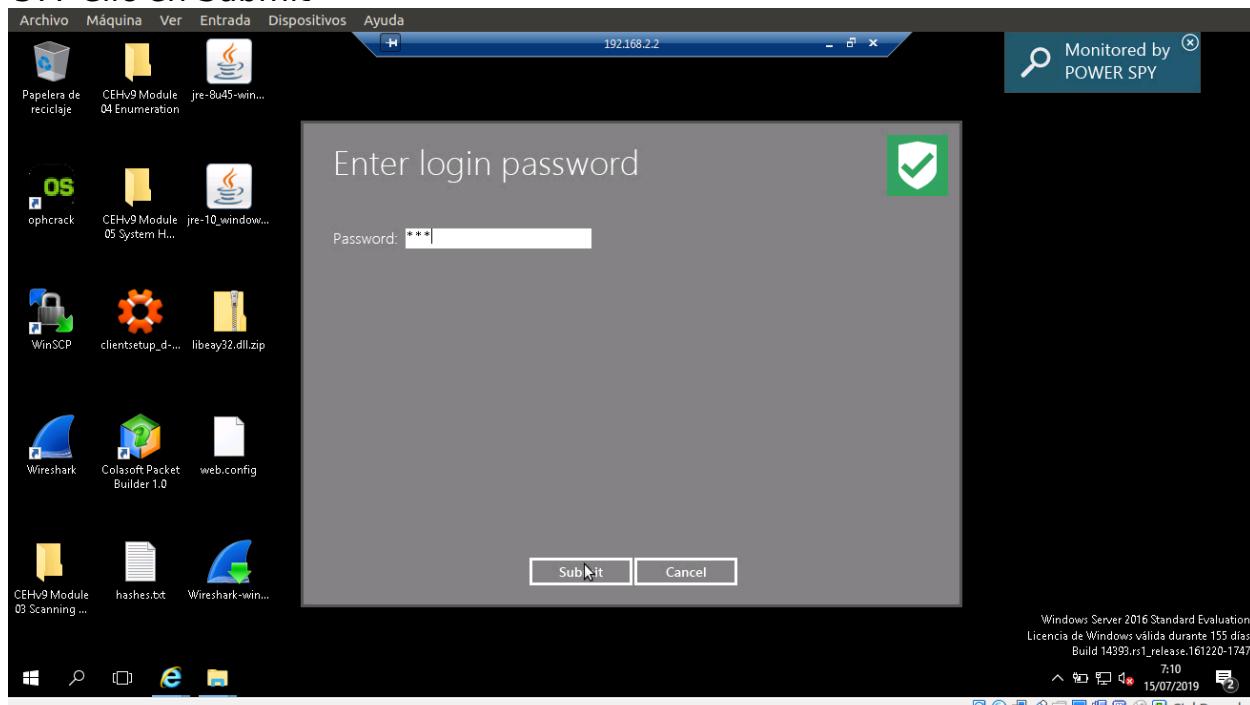


34. Para sacar a Powero Spy del modo invisible, presione Ctrl + Alt + X
35. Aparece la ventana **Ejecutar como administrador**; haga clic en **Ejecutar**.



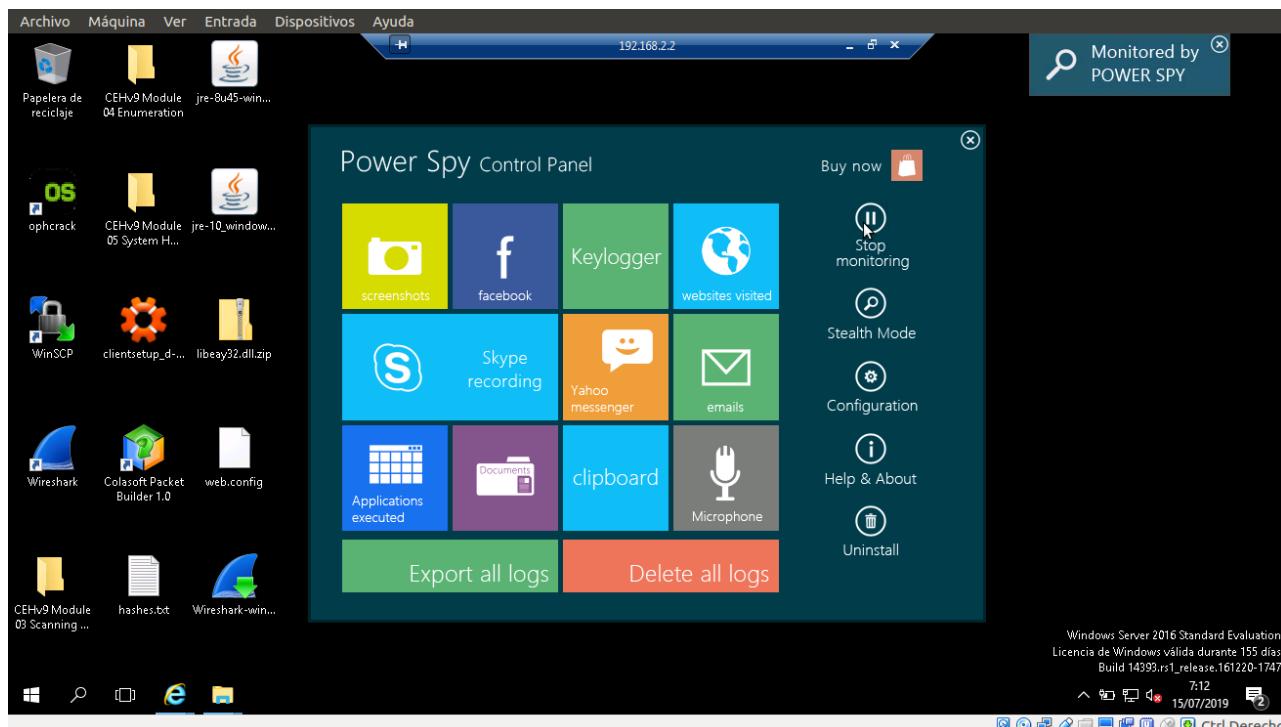
36. Aparece la ventana Ingresar contraseña de inicio de sesión; introduzca la contraseña (que estableció en el paso 16).

### 37. Clic en Submit



38. Haga clic en más tarde en la ventana **Registrar producto** para continuar.

39. Haga clic en **Detener supervisión** para detener la supervisión.



40. Para verificar las pulsaciones de teclado del usuario, haga clic en **Keylogger** desde el Panel de control de **Power Spy**.

41. Mostrará todas las pulsaciones resultantes, como se muestra en la captura de pantalla.

Log View - Keystrokes (5 records)				
Timestamp	User Name	Keystroke Content	Window Caption	Application Path
15/07/2019 7:02:30	Administrador	{Shift}{Medu}{Back Space}ium{Enter}	Medium - ????? Google - Internet Explorer	c:\program files\internet explorer\explorer.exe
15/07/2019 7:02:09	Administrador	{Back Space}{Back Space}oogle{Back Space}ogel{En...	mega - ????? Google - Internet Explorer	c:\program files\internet explorer\explorer.exe
15/07/2019 7:01:12	Administrador	serwinantonio{Ctrl}{Alt}{Tab}{->}erwin-97{E...	Facebook - Internet Explorer	c:\program files\internet explorer\explorer.exe
15/07/2019 6:59:39	Administrador	Face{Down}{Enter}	Facebook - Entrar o registrarse - Internet Explorer	c:\program files\internet explorer\explorer.exe
15/07/2019 6:57:40	Administrador	{Ctrl}{Alt}{x}{Ctrl}{Alt}{x}{Ctrl}{Caps Lock}{Ctrl}{Alt}{x}{C...	Ejecutar	c:\windows\explorer.exe

42. Para consultar el sitio web visitado por el usuario, haga clic en el sitio web visitado desde el panel de control de **Power Spy**.

43. Mostrará los resultados completos de los sitios web visitados por los usuarios, como se muestra en la siguiente captura de pantalla.

Screenshot of a computer interface showing log history and a browser window.

The top menu bar includes: Archivo, Máquina, Ver, Entrada, Dispositivos, Ayuda. The title bar says "Log View - Websites Visited (66 records)" and the IP address is 192.168.2.2.

The left sidebar shows "Logged Users:" with one entry: "Administrador". It also lists "Log Types:" including Screenshot, Keystrokes, Applications, and Websites Visited (which is selected).

The main content area displays a table of log entries:

Timestamp	User Name	Website URL
15/07/2019 7:04:31	Administrador	https://medium.com/
15/07/2019 7:02:44	Administrador	https://medium.com/
15/07/2019 7:02:41	Administrador	https://app.link/
15/07/2019 7:02:41	Administrador	https://medium.com/
15/07/2019 7:02:40	Administrador	https://app.link/
15/07/2019 7:02:38	Administrador	https://medium.com/
15/07/2019 7:02:37	Administrador	https://cdn.branch.io/
15/07/2019 7:02:35	Administrador	https://medium.com/
15/07/2019 7:02:35	Administrador	https://cdn.branch.io/
15/07/2019 7:02:35	Administrador	https://medium.com/
15/07/2019 7:02:30	Administrador	https://medium.com/
15/07/2019 7:02:30	Administrador	https://medium.com/
15/07/2019 7:02:27	Administrador	https://www.google.com/search?hl=be&ei=zAgS%a7zCc7RtAaGo6TABA&q=Medium&oq=Medium&gs_l=psy-ab..0.019l0.2143.5196..5525...1.0..0.0146.896.0j....0...
15/07/2019 7:02:20	Administrador	https://www.google.com/search?hl=be&source=hp&ei=yAgS%aCVa7Lf5glXqlSQBg&q=mega&oq=mega&gs_l=psy-ab..0.019l0.1019j019l5.1223.3200..2.0....
15/07/2019 7:02:13	Administrador	https://mega.nz/update.html

The bottom part of the interface shows a browser window with the Medium website open. The page title is "Medium". The navigation bar includes: HOME, ONEZERO, ELEMENTAL, GEN, ZORA, FORGE, HUMAN PARTS, STARTUPS, SELF, TECHNOLOGY, HEATED, MO. Below the navigation is a large image of a shopping cart with an Amazon logo. To the right, there's an article thumbnail for "The One When 'Star Trek' Used Technology to Excuse a Shopping Spree" by Rob Bricken, published on Jul 12, with a 7 min read duration. Another article thumbnail below it is titled "You've Probably Never Had".

The taskbar at the bottom shows various icons and the date/time: 7:18, 15/07/2019.