## INFECTAR EL SISTEMA DE DESTINO CON UN VIRUS

Un virus informático es un programa autorreplicante que produce su código adjuntando copias de sí mismo a otros códigos ejecutables y opera sin el conocimiento ni el deseo del usuario.

## ESCENARIO DE LABORATORIO

Los virus son las plagas de la informática moderna. Los virus informáticos pueden causar estragos tanto en los ordenadores personales como en los de las empresas. La vida de un virus depende de su capacidad para reproducirse. Por ello, los atacantes diseñan el código de cada virus de tal manera que éste se replique n veces, siendo n un número especificado por el atacante. En todo el mundo, la mayoría de las empresas han sido infectadas por un virus en algún momento. Al igual que un virus biológico, un virus informático es contagioso y puede contaminar otros archivos; sin embargo, los virus sólo pueden infectar máquinas externas con la ayuda de usuarios de ordenadores.

Al igual que los virus, los gusanos informáticos son programas maliciosos autónomos que se replican, ejecutan y propagan de forma independiente a través de las conexiones de red, sin intervención humana. Los gusanos son un subtipo de virus. Los intrusos diseñan la mayoría de los gusanos para que se repliquen y propaguen por una red, consumiendo así los recursos informáticos disponibles y, a su vez, provocando que los servidores de red, los servidores web y los sistemas informáticos individuales se sobrecarguen y dejen de responder. Sin embargo, algunos gusanos también llevan una carga útil para dañar el sistema anfitrión.

Un hacker ético y un pen tester durante una auditoría de una organización objetivo deben determinar si los virus y gusanos pueden dañar o robar la información de la organización. Puede que necesiten construir virus y gusanos e intentar inyectarlos en la red objetivo para comprobar su comportamiento, saber si un antivirus los detectará y averiguar si pueden saltarse el cortafuegos.

## OBJETIVOS DEL LABORATORIO

- Crear un virus utilizando la herramienta JPS Virus Maker Tool e infectar el sistema de destino.

## ENTORNO DE LABORATORIO

Para llevar a cabo este laboratorio, necesitas:

- Máquina virtual Windows 11
- Máquina virtual de Windows 10
- Navegadores web con conexión a Internet
- Privilegios de administrador para ejecutar las herramientas

### VISIÓN GENERAL DE LOS VIRUS Y WORMS

Los virus pueden atacar el sistema de un anfitrión utilizando diversos métodos. Pueden adherirse a programas y transmitirse a otros programas haciendo uso de eventos específicos. Los virus necesitan que se produzcan estos eventos, ya que no pueden autoiniciarse, infectar hardware ni transmitirse utilizando archivos no ejecutables. Los eventos de ''activación'' y ''ataque directo'' pueden hacer que un virus se active e infecte el sistema objetivo cuando el usuario activa archivos adjuntos recibidos a través de correo electrónico, sitios web, anuncios maliciosos, tarjetas de memoria, ventanas emergentes u otros métodos. A continuación, el virus puede atacar los programas integrados en el sistema, el software antivirus, los archivos de datos y la configuración de inicio del sistema, o realizar otras actividades maliciosas.

Al igual que un virus, un gusano no necesita un anfitrión para replicarse, pero en algunos casos, la máquina anfitriona del gusano también infecta. Al principio, los profesionales de Blackhat trataban los gusanos como un problema de mainframe. Más tarde, con la introducción de Internet, se concentraron y se dirigieron a los sistemas operativos Windows utilizando los mismos gusanos compartiéndolos por correo electrónico, IRC y otras funciones de red.

## TAREAS DE LABORATORIO TAREA L: CREAR UN VIRUS CON LA HERRAMIENTA JPS VIRUS MAKER E INFECTAR EL SISTEMA DE DESTINO

La herramienta JPS Virus Maker se utiliza para crear su propio virus personalizado. Esta herramienta tiene muchas opciones de construcción que se pueden utilizar para crear un virus. Algunas de las características de la herramienta son auto-inicio, apagado, desactivar el centro de seguridad, bloquear el ratón y el teclado, destruir el almacenamiento protegido, y terminar las ventanas.

Un hacker ético y pen-tester puede utilizar la herramienta JPS Virus Maker Tool como prueba de concepto para auditar los controles de seguridad perimetral de una organización.

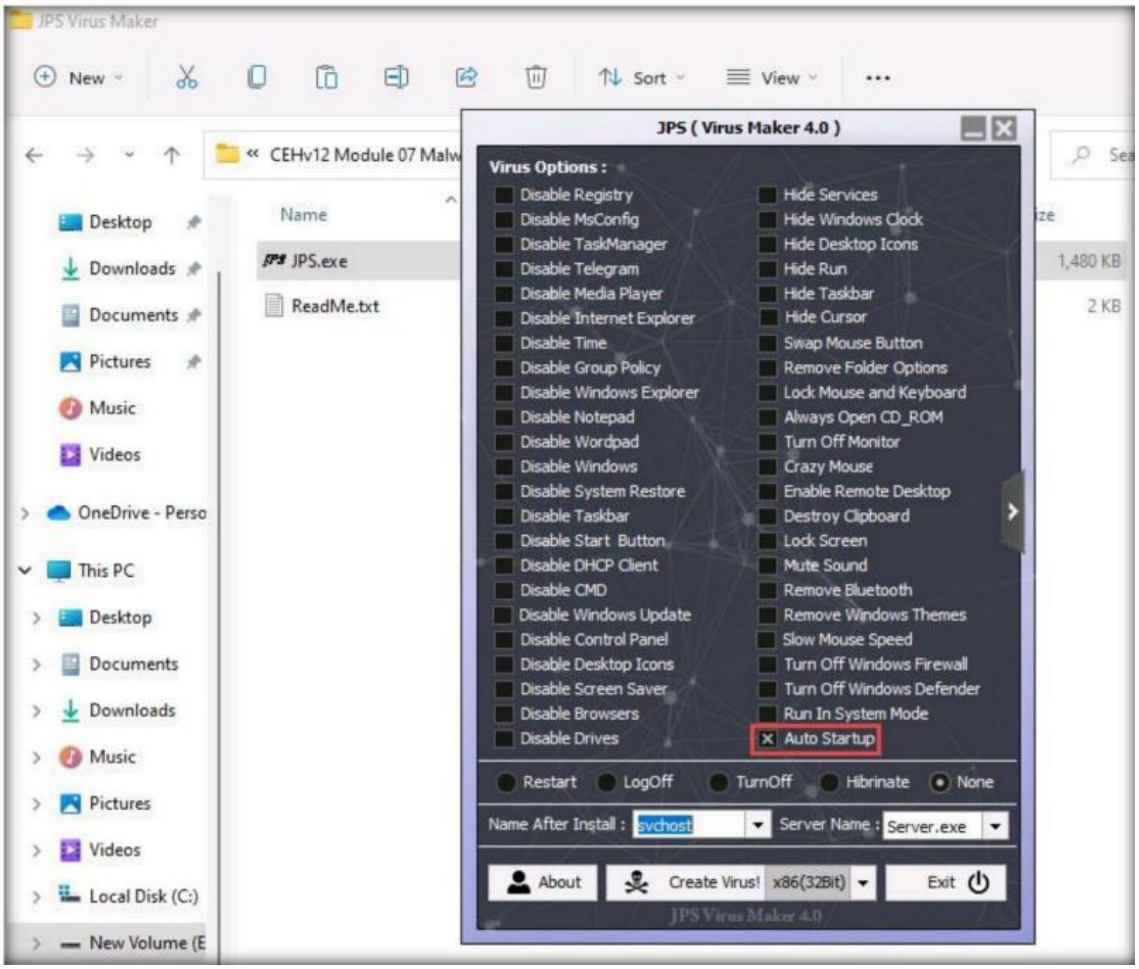
NOTA: TRAS REALIZAR ESTA TAREA, FINALIZAREMOS Y VOLVEREMOS A LANZAR LA INSTANCIA DE LABORATORIO, YA QUE LA MÁQUINA WINDOWS 10 ESTARÁ INFECTADA POR EL VIRUS.

1. Encienda las máquinas virtuales de Windows 11 y Windows 10.

2. En el equipo con Windows 11, vaya a C:\Tools\Virus Maker\JPS Virus Maker y haga doble clic en jps.exe.

NOTA: SI APARECE UNA VENTANA EMERGENTE ABRIR ARCHIVO - ADVERTENCIA DE SEGURIDAD, HAGA CLIC EN EJECUTAR.

3. Aparecerá la ventana JPS (Virus Maker 4.0); marque la casilla Auto Startup



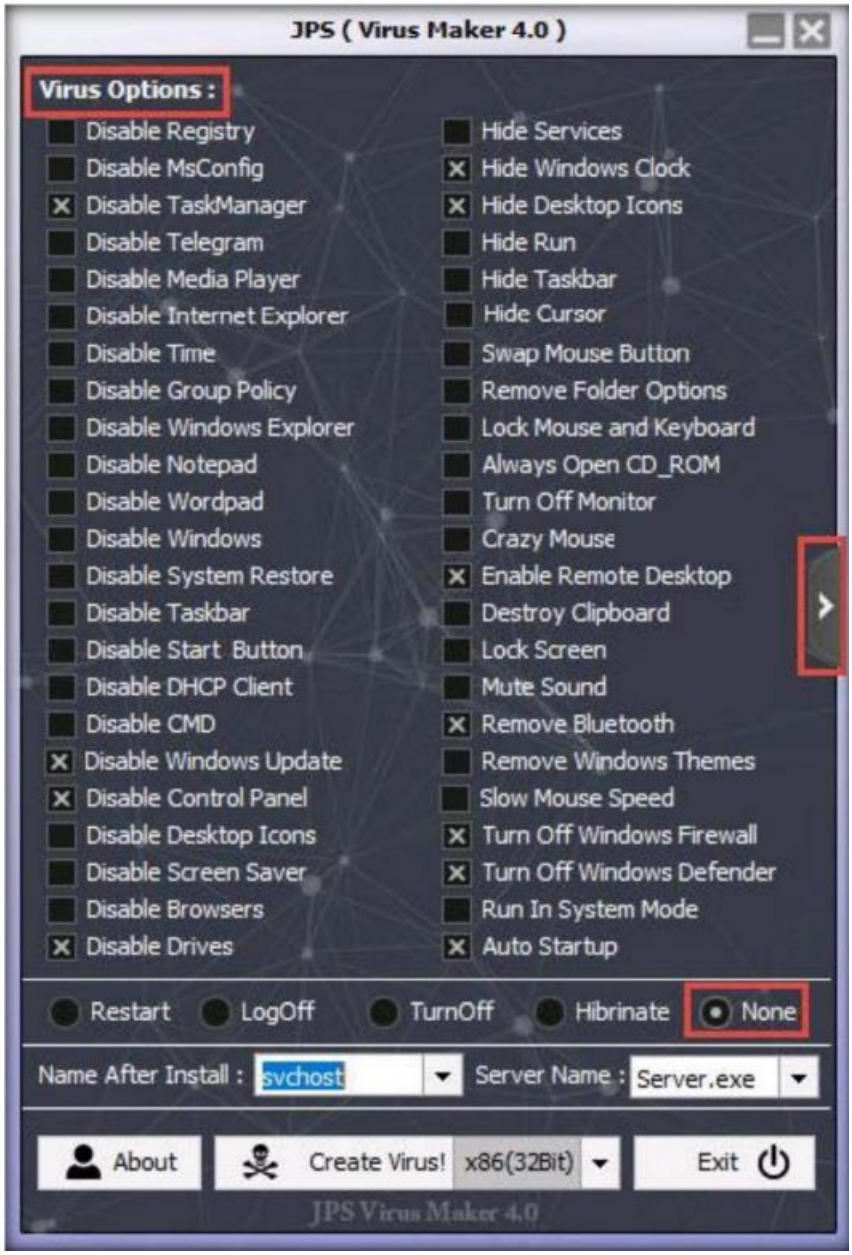

4. La ventana muestra varias características y opciones que se pueden elegir mientras se crea un archivo de virus.

5. En las Opciones de virus, marque las opciones que desee incrustar en un nuevo archivo de virus.

6. En esta tarea, las opciones incluidas en el archivo del virus son Desactivar TaskManager, Desactivar Windows Update, Desactivar Panel de Control, Desactivar Unidades, Ocultar Reloj de Windows, Ocultar Iconos del Escritorio, Activar Escritorio Remoto, Quitar Bluetooth, Desactivar Firewall de Windows, Desactivar Windows Defender e Inicio Automático.


7. Asegúrese de que el botón de opción Ninguno está seleccionado para especificar el evento desencadenante cuando el virus debe empezar a atacar el sistema después de su creación.

8. Ahora, antes de hacer clic en ¡Crear virus!, haga clic en el icono de la flecha derecha del panel derecho de la ventana para configurar las opciones del virus



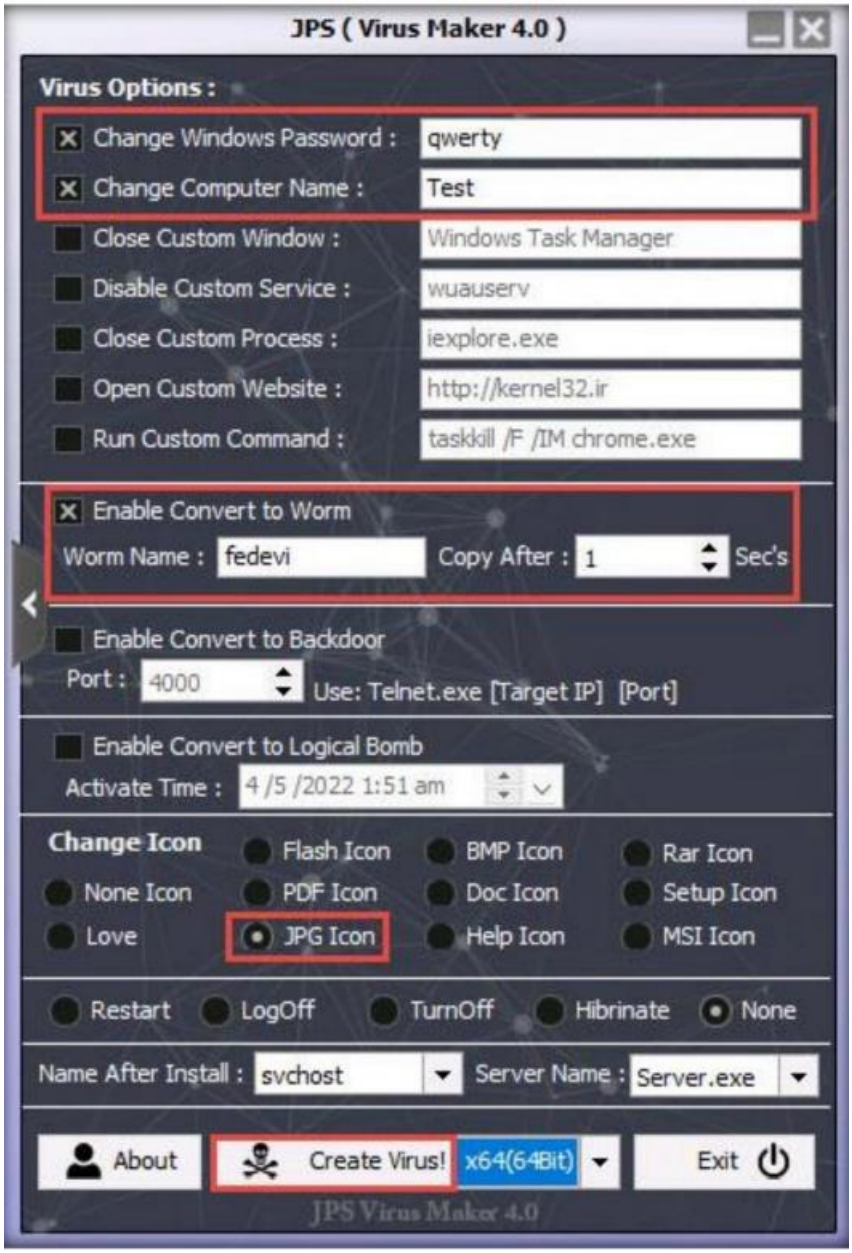

9. Aparecerá una ventana de Opciones de virus, como se muestra en la captura de pantalla.

10. Marque la opción Cambiar contraseña de Windows, e introduzca una contraseña (aquí, qwerty) en el campo de texto. Marque la opción Cambiar nombre de equipo y escriba Prueba en el campo de texto.

11. Incluso puede configurar el virus para que se convierta en gusano. Para ello, marque la casilla Habilitar conversión a gusano y proporcione un Nombre de gusano (aquí, fedevi). Para que el gusano se auto-replique después de un tiempo determinado, especifique el tiempo en segundos (aquí, 1 segundo) en el campo Copiar después de.

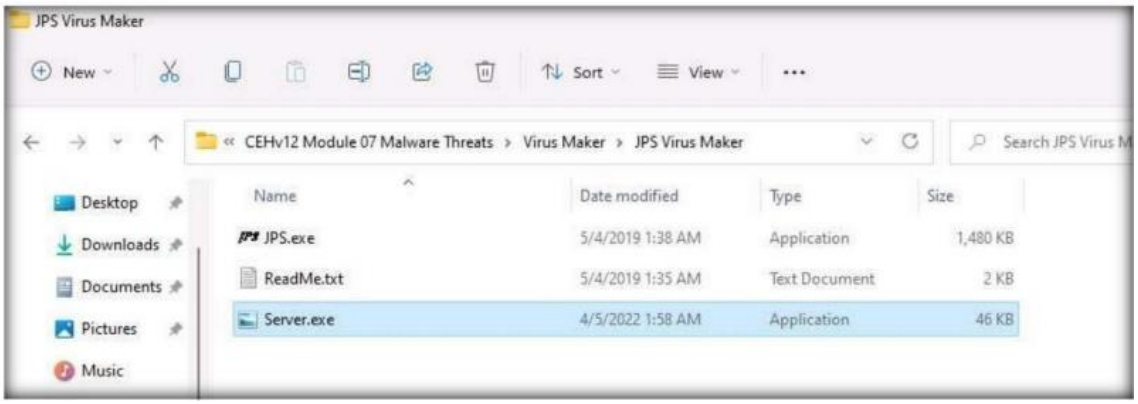
12. Asegúrese de que el botón de opción Icono JPG está seleccionado en la sección Cambiar icono. Asegúrese de que el botón de opción Ninguno está seleccionado en la parte inferior de la ventana.

13. Tras completar la selección de opciones, haga clic en el icono desplegable situado junto al botón ¡Crear virus! y seleccione x86(64Bit); haga clic en ¡Crear virus!




14. Aparecerá una ventana emergente ¡Virus creado con éxito!; haga clic en Aceptar.


15. El virus recién creado (servidor) se coloca automáticamente en la carpeta donde se encuentra jps.exe, pero con el nombre Server.exe. Navegue a C:\Tools\Virus Maker\JPS Virus Maker y observe que el virus recién creado con el nombre Server.exe está disponible en la ubicación especificada.



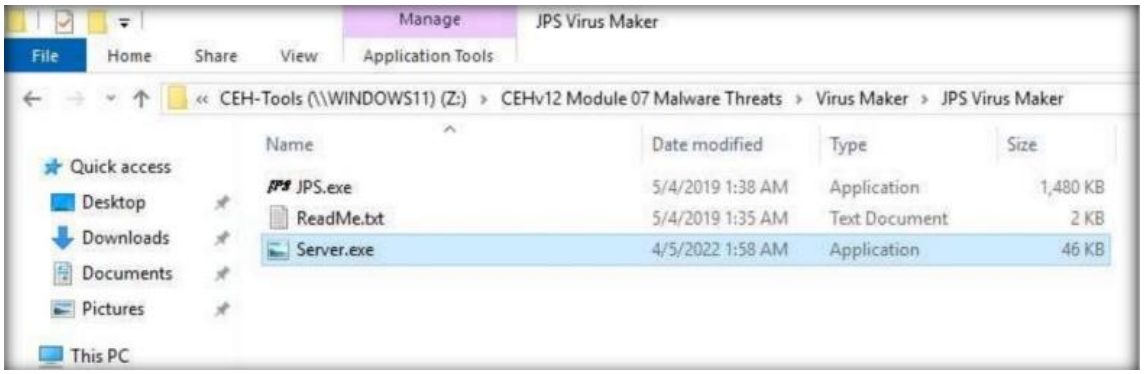

16. Ahora, empaqueta este virus con una carpeta o empaquetador de virus y envíalo a la máquina víctima a través de correo electrónico, chat, una unidad de red mapeada u otro método.

17. En esta tarea, estamos utilizando una unidad de red mapeada para compartir el archivo del virus con la máquina víctima. Suponga que usted es una víctima y que ha recibido este archivo.

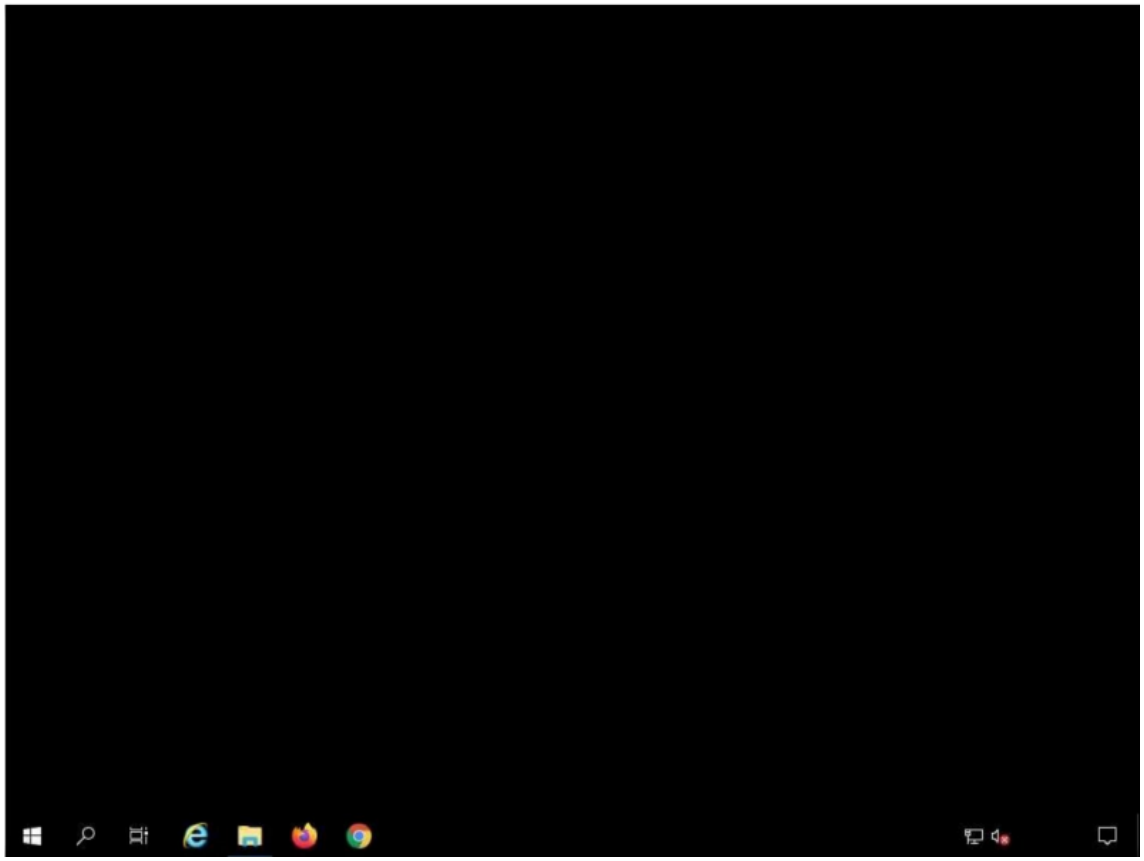
18. Cambie a la máquina Windows 10.

NOTA: AQUÍ, ESTAMOS ENTRANDO EN LA MÁQUINA COMO VÍCTIMA.


19. Vaya a C:\Virus Maker\JPS Virus Maker y haga doble clic en el archivo Server.exe para ejecutar el virus.

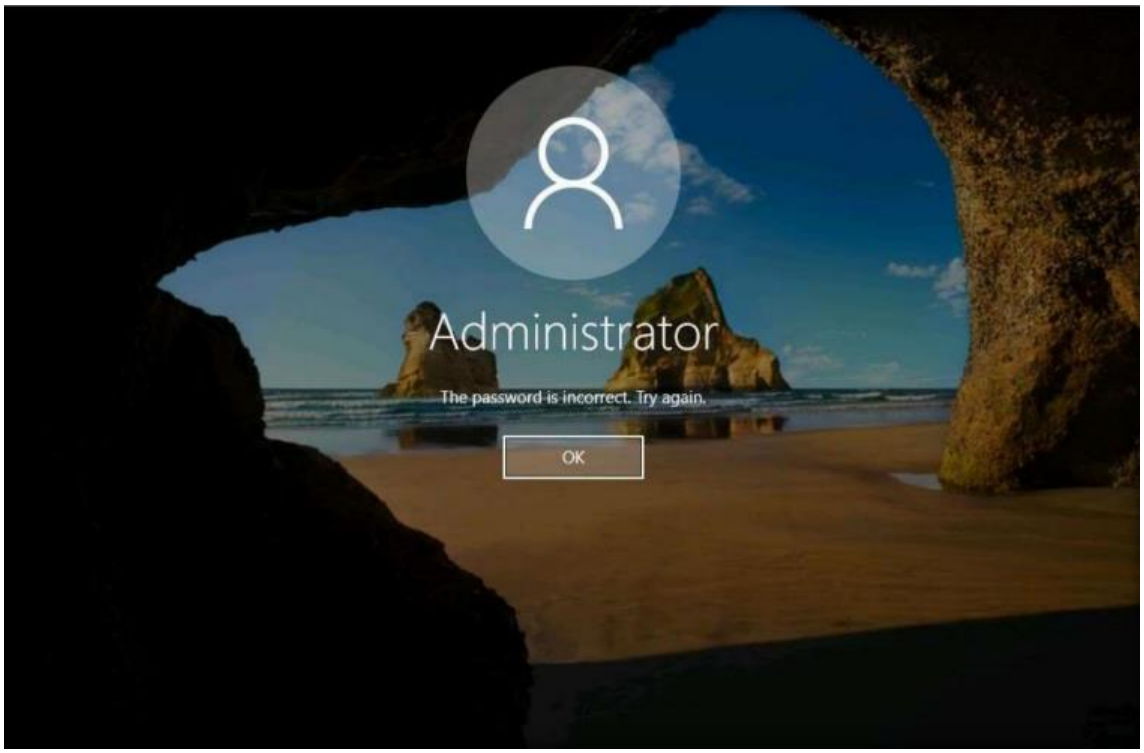



20. Una vez ejecutado el virus, cierre la ventana y podrá observar que la pantalla del Escritorio se queda en blanco, indicando que el virus ha infectado el sistema, tal y como se muestra en la captura.

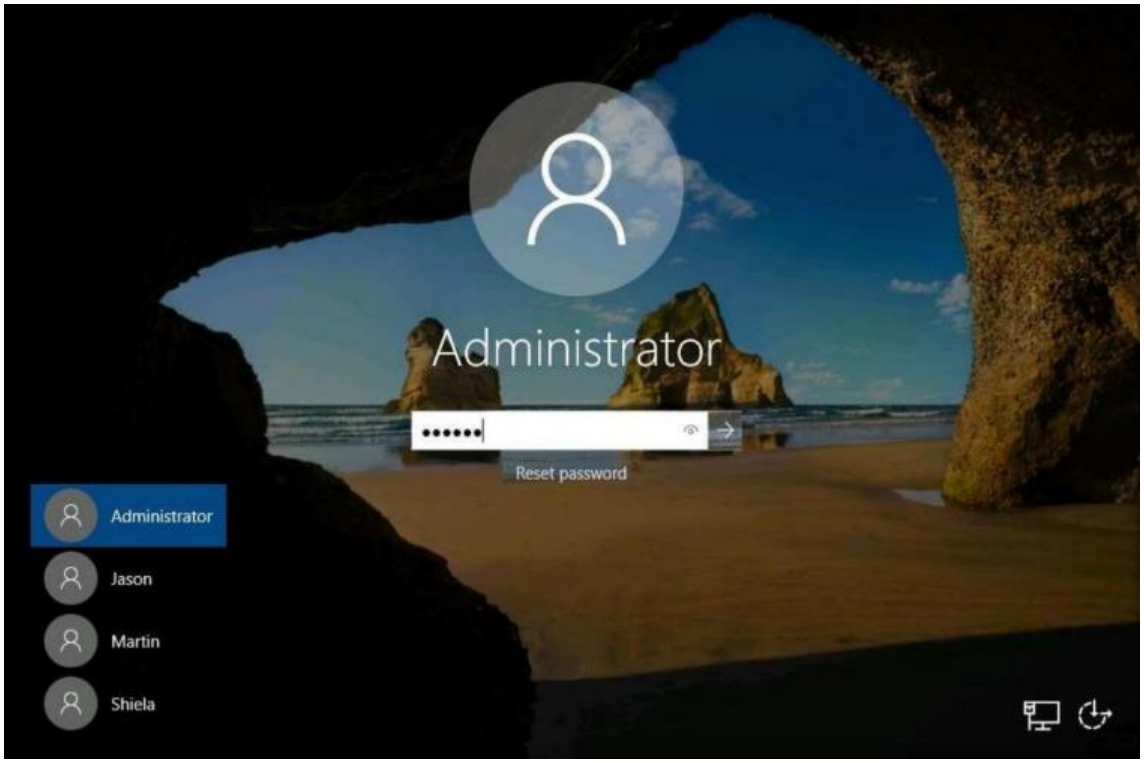


21. Sorprendida por el comportamiento del sistema, la víctima (tú) intenta arreglar la máquina reiniciándola. Una vez que la máquina se ha reiniciado, intenta iniciar sesión en la máquina con el nombre de usuario y la contraseña proporcionados. Deberías recibir el mensaje de error ''la contraseña es incorrecta. Inténtelo de nuevo".

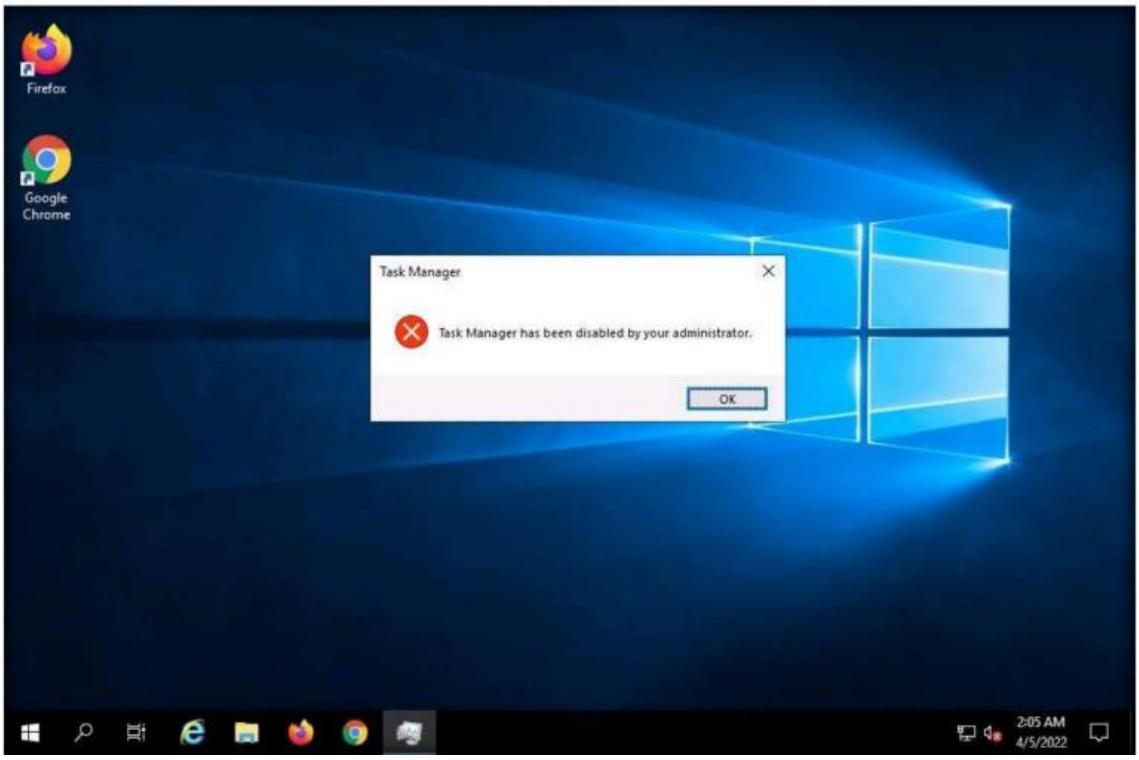
22. Active la máquina, escriba Pala contraseña y pulse Intro.




23. Haga clic en Aceptar e inicie sesión con la contraseña que proporcionó en el momento de la creación del virus (es decir, qwerty). Deberá iniciar sesión en la máquina con la nueva contraseña.




24. Ahora, intente abrir el Administrador de tareas; observe que aparece una ventana emergente de error de apertura y, a continuación, haga clic en Aceptar.




25. Obtendrá un error similar para todas las aplicaciones que estén deshabilitadas por el virus.

26. Así es como los atacantes infectan un sistema con virus. Ahora, antes de pasar a la siguiente tarea, finalice el laboratorio y vuelva a iniciarlo para reiniciar las máquinas. Para ello, en el panel derecho de la consola, haga clic en el botón Finalizar presente en la sección Banderas.

27. Apague las máquinas virtuales de Windows 11 y Windows 10.