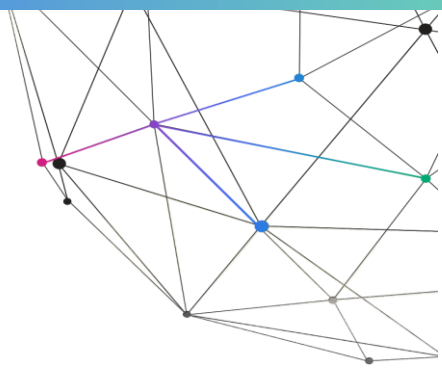


CRONUS
CYBER TECHNOLOGY

CyBot Pro
Guía POC

V2.7
Octubre 2018

Tabla de Contenido

1 Introducción

El documento está diseñado para proporcionar a los clientes de Cronus información sobre la instalación de CyBot Pro y Enterprise, así como los parámetros de una prueba de concepto (PoC) exitosa. Este capítulo proporciona información sobre los requisitos de software y hardware y las consideraciones de toplogía de red.

Nota: Para cualquier problema que ocurra durante el PoC, no dude en ponerse en contacto con su representante de Cronus.

1.1 Requerimientos Mínimos

1.1.1 CyBot Pro

- **RAM**: 8 GB
- **Disco Duro Disponible**: 120 GB
- **Procesador**: de 4 cores
- **Red**: Tarjeta Ethernet de 100 Mb
- **Plataforma**: VMware ESX v5.5 /Hyper-V 3.0 o superior.

1.1.2 CyBot Enterprise

- **RAM**: 8 GB
- **Disco Duro Disponible**: 1000 GB
- **Procesador**: de 4 cores
- **Red**: Tarjeta Ethernet de 100 Mb
- **Plataforma**: VMware ESX v5.5 /Hyper-V 3.0 o superior.

1.1.3 CyBot MSSP

- **RAM**: 16 GB
- **Procesador**: de 8 cores
- **Red**: Tarjeta Ethernet de 100 Mb
- **Plataforma**: VMware ESX v5.5 /Hyper-V 3.0 o superior.

1.1.4 Para implementar CyBot (todas las ediciones), la siguiente información es requerida para la instalación:

- Dirección IP: se recomienda un IP estático
- La máscara de subred en la que se instalará CyBot Pro y Enterprise
- La puerta de enlace (gateway)
- Servidores DNS
- Cuenta para las credenciales de WMI (miembro de los grupos de operadores de servidor y administradores locales en AD / DA)
- Credenciales para la Cuenta SSH (root)
- Si usa CyBot Enterprise, verifique que los puertos 443 y 6432 estén abiertos desde CyBot Pro a CyBot Enterprise

Nota: Cronus suministra una plantilla de VM, preconfigurada con los requisitos mínimos.

1.1.5 Requisitos del entorno de PoC

Diseñe el entorno PoC para que incluya al menos 50 máquinas (físicas o virtuales) con los siguientes criterios:

- Al menos el 50% de la red debe estar compuesto por estaciones de trabajo.
- Al menos un controlador de dominio (Domain Controller - DC).
- Al menos el 10% de la red debe incluir servidores.
- Las estaciones de trabajo y los servidores deben incluir sistemas operativos Linux y Windows. Se recomienda emplear varios sistemas operativos basados en Windows y Linux, para maximizar la eficiencia del PoC.

Notas:

- Es necesario proporcionar a CyBot las credenciales de WMI y SSH para un escaneo rápido y eficiente.
- Todos los hosts escaneados deben cumplir con los requisitos mínimos descritos por el proveedor específico.

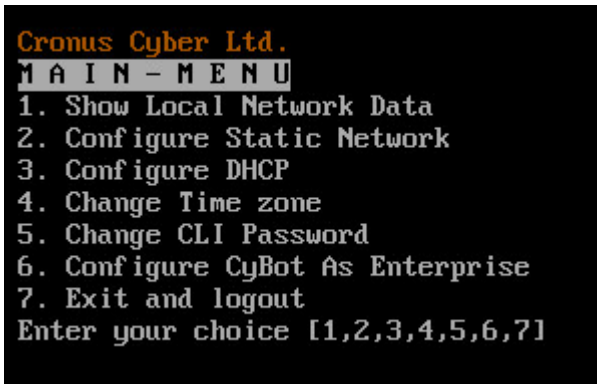
  i.e. – Las máquinas Windows deben cumplir con los requisitos descritos en TechNet, etc.

2 Instalar CyBot Pro

Para instalar CyBot Pro, ejecute la máquina virtual que recibió.

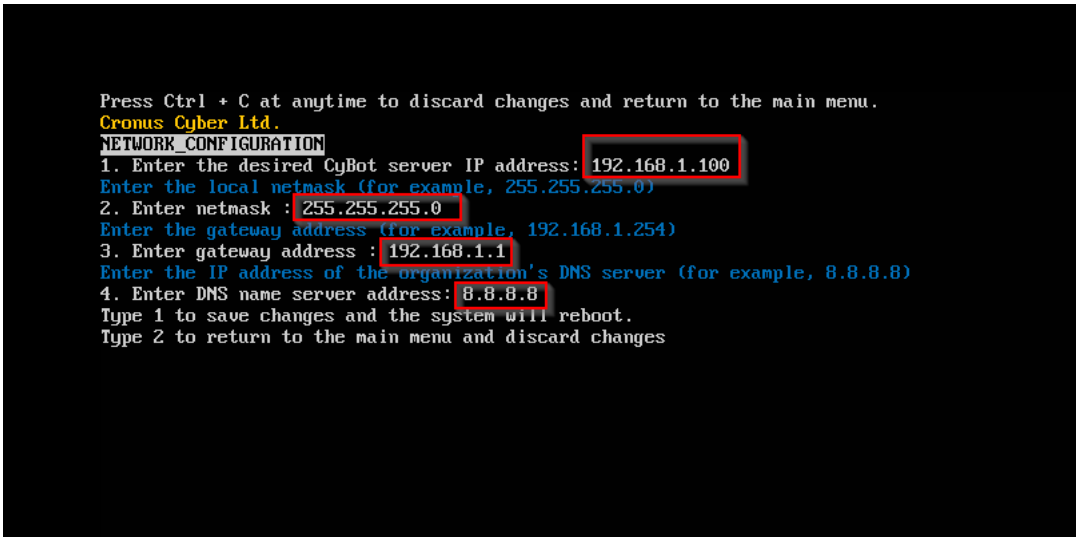
2.1 Iniciar sesión en la consola usando las siguientes credenciales:

- Username: client
- Password: Cr0nu5$$$



2.2 Cuando se le solicite, seleccione la configuración de red que prefiera:

- Para configurar una dirección IP estática específica para el servidor CyBot MSSP, ingrese 3, seguido de la dirección IP. Esta es la configuración recomendada.



- Para configurar una dirección IP usando el servidor DHCP, ingrese 3.

1. Guardar los cambios de configuración. La máquina virtual se reinicia automáticamente.
2. Haga login de nuevo e ingrese 1 para verificar su dirección IP.

Aparecerá una ventana similar a la siguiente. Utilice la dirección IP indicada para conectarse a la interfaz web de CyBot MSSP.

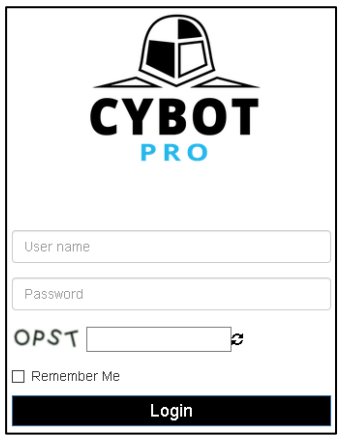
3 Accediendo a la GUI de CyBot

Use **Google Chrome**.

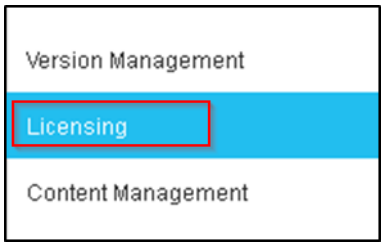
1. Ingrese el CyBot Pro IP en la URL de Chrome.
   - **https://**X.X.X.X
2. Una vez cargada, aparecerá una pantalla diciendo que su conexión no es privada.
   a. Clic en **ADVANCED**.
   b. Clic en **Proceed to XXX.XXX.XXX.XXX (unsafe)**.
   c. La página de login de CyBot Pro se cargará.
3. Ingrese las credenciales predeterminadas de CyBot Pro cuando aparezca la pantalla de login:

Username: cronus
Password: cyberdog

NOTA: Las credenciales se pueden cambiar y / o eliminar una vez que se complete la configuración inicial.



4 Licencia

1. Para subir una licencia a CyBot Pro:
2. Seleccione botón de Common Functions ≡ y seleccione Licensing
3. 

4. Haga clic en Agregar licencia y continúe con el asistente de instalación de licencias.
5. Lea y acepte los "Términos y Condiciones"
6. Suba el archivo de licencia, haciendo clic en Select file o arrastrando y soltando el archivo de licencia.
7. Después de cargar con éxito su archivo de licencia, seleccione el método de activación de la licencia; se prefiere usar la "Activación en línea", pero si no hay una conexión a Internet activa disponible, use el método de "Activación sin conexión".
8. Activación fuera de línea:
9. Clic en “Offline Activation”.
10. Clic en “Copy to Clipboard”.
11. Log in al portal Cronus: https://portal.cronus-cyber.com
12. Clic en “Activate Product” desde el menú superior derecho.
13. Pegue la clave copiada al “Unique Machine Key”.
14. Clic en “Activate” y copie la "Clave de activación"
15. Vuelva a la ventana de CyBot Pro y haga clic en 

16. Pegue la clave de activación copiada desde el Portal y haga clic en "Activar ahora".

5 Credenciales

1. Seleccione el botón de Common Functions ≡ y seleccione Credentials
2. Cuenta para las credenciales de WMI (miembro de los grupos de operadores de servidor y administradores locales en AD o administrador de dominio)

3. Cuenta para credenciales SSH (root)
4. Certificado SSH

6 Escaneos

1. Vaya al menú principal de escaneos y haga clic en “Infrastructure Scan”.
2. Clic en 

3. El menú Configurar escaneo tiene la opción de programar un escaneo o escanearlo de inmediato al marcar "Escanear ahora" (Scan Now).
4. Los horarios se pueden hacer por hora, día, semana y mes a una hora determinada.
5. Se puede cargar un archivo CSV de IPs para acelerar la administración con múltiples CyBot Pro o al agregar IP a un nuevo escaneo haciendo clic en el botón Upload from file.
6. Inserte el alcance (scope) del escaneo haciendo clic en el botón +
7. Guarde cada “Range“ y/o “CIDR” y haga clic en “Scan”
8. La información sobre el estado del escaneo se puede encontrar en el menú Infrastructure Scan

7 Criterios de éxito

Este capítulo describe los criterios de éxito para evaluar CyBot Pro y Enterprise. Cada sección de este capítulo incluye una prueba diferente para el PoC. El avance a la siguiente sección se realiza solo cuando la prueba tiene éxito y el criterio se cumple.

7.1.1 Identificación de hosts de red

El primer criterio de éxito CyBot Pro es un sistema diseñado para identificar y detectar la topología de la red escaneada. Se logra un éxito cuando **al menos el 85%** de los hosts y dispositivos en el rango escaneado se identifican correctamente:

- Sistema Operativo
- Rol
- Servicios
- Puertos abiertos

7.1.2 Detección de vulnerabilidades

CyBot Pro y Enterprise deben realizar un escaneo en el sistema y producir un informe sobre los hallazgos críticos. Cada host, que contiene hallazgos críticos, se debe probar y verificar manualmente que la vulnerabilidad existe en el sistema. La verificación de la existencia de la vulnerabilidad se puede realizar buscando el número CVE en el sitio del fabricante del sistema operativo y verifique si el parche que corrige la vulnerabilidad no está instalado en el host. Un criterio de éxito para este paso es la verificación de **al menos el 85%** de los hallazgos críticos.

7.1.3 Detección de Escenarios de ruta de ataque (Attack Path Scenarios - APS)

CyBot Pro y Enterprise deben realizar una exploración en el sistema y producir un informe sobre los escenarios de la ruta de ataque. Cada APS con un factor de 80 o más debe ser probado para su verificación. El proceso de verificación se realiza verificando cada paso (host) de la ruta APS y reconociendo los siguientes factores:

- Cada hallazgo de CVE relacionado con APS existe en el host.
- Cada hallazgo de CVE relacionado con APS permite que un atacante tome el control del host.
- Todos los pasos de la ruta APS están conectados viablemente en la red.
- El paso final (host de destino) de cada APS se considera un activo valioso (por ejemplo, DC, servidor SQL, etc.).

Un criterio de éxito del paso es la verificación de **al menos el 85%** de los APS.

8 Preguntas de preinstalación recomendadas para los clientes (si es necesario):

- Descripción general de Hypervisor - VMware / Hyper-V: Verifique cuántos recursos están disponibles
- ¿Cuál es la versión actual de ESXi / Hyper-V en ejecución (y hay planes para actualizar)?
- ¿Existen restricciones de vNet o limitaciones de ancho de banda en la red?
- Compruebe la configuración y las velocidades de la NIC para encontrar la configuración de red óptima para CyBot VM: pregunte al cliente si tiene una NIC de 1GB / 10GB.
- Restricciones de la intranet, conectividad y reglas de la puerta de enlace: discuta si hay alguna configuración de puerta de enlace o FW que pueda limitar y / o afectar las exploraciones, también verifique si las VM pasan el Switch distribuido dentro de VMware.
- Configuración de la red activa general - Qué y cuántos - Enrutadores, conmutadores, cortafuegos.
- Enumere los dispositivos activos que están conectados a la red: impresoras, relojes, teléfonos IP, televisores inteligentes, consolas, etc.
- Compruebe si hay servicios de monitoreo de red en ejecución.
- Solicite lista blanca / lista de puertos: confirme que los puertos de CyBot no están bloqueados / filtrados / reenviados.
- Confirme y verifique las credenciales recuperadas que se utilizarán.
- Pregunte si hay algún NLB habilitado. También pregunte por el momento ideal para ejecutar escaneos (cuando la red está cargada)
- Breve bosquejo de la topología de red.
- Es el puerto al que está conectado el ESX en el conmutador en modo troncal y permite todas las VLAN
- Los puertos que deben estar abiertos: 445 / 139,22 (WMI, SSH)
- PRO + ENT + MSSP necesita Puertos: 443, 6432 abiertos entre ellos, si están en segmentos diferentes, deben verificar si hay FW interno.
- ¿Está el ESX conectado a la red troncal?
- ¿Qué tipo de interruptores hay en los pisos?
- ¿Está la red segmentada?
- ¿ Cuáles son las VLAN?
- ¿Cuáles son las redes a escanear y en qué clases están, A, B, C?

9 Apéndice A:

9.1 Agregar usuarios como administradores locales en todas las PC conectadas al dominio

Este procedimiento debe crearse en el DC (controlador de dominio) y se replicará en todos los equipos que sean miembros del dominio.

En el DC (Domain Controller):

Defina un grupo de seguridad en usuarios de AD y computadoras. En este ejemplo estoy creando un grupo de seguridad llamado IT_Admins

1. Inicie sesión en un controlador de dominio 2. Haga clic con el botón derecho del mouse en Usuarios, Nuevo-> Grupo-> Seguridad Llámelo IT_Admins 3. Agregue los miembros adecuados para que tengan los permisos de seguridad adecuados en las computadoras locales.Create the User

1. Cree un usuario que tendrá los privilegios de administrador local 2. Vaya a las propiedades del usuario 3. Vaya a miembro de 4. Agregue grupos llamados "Operadores de servidor", "IT_Admins" 5. Establezca "IT_Admins" como grupo principal

A continuación, debe crear una política de grupo o usar la Política de dominio predeterminada (no se recomienda).

1. Cree una política separada llamada "Administradores locales" 2. Abra la Consola de administración de políticas de grupo 3. Haga clic derecho en su dominio o en la OU 4. Haga clic en Crear un GPO en este dominio y vincúlelo aquí 5. Llámelo "Administradores locales" ahora. Debería ver la política en el árbol.

Aquí agregará el grupo IT_Admins a la política del administrador local y los colocará en los grupos que desea que utilicen. 1. Haga clic con el botón derecho en la Política de "administradores locales" 2. Expanda Configuración del equipo \ Políticas \ Configuración de Windows \ Configuración de seguridad \ Grupos restringidos 3. En el panel derecho de Grupos restringidos, haga clic con el botón derecho y presione "Agregar grupo ..." Escriba IT_Admins y presione "Aceptar" 4. Haga clic en Agregar debajo de "Este grupo es miembro de:" 5. Agregue el grupo de "Administradores" 6. Aceptar Espere 15 minutos, o inicie sesión en una PC y escriba gpupdate / force y verifique el grupo de administradores locales. Debería ver IT_Admins en el grupo ahora. El usuario que creó ahora tiene acceso a todas las PC de forma remota como administrador local. Enlace a explicación de YouTube: https://youtu.be/n2dDOKUIFI0

10 Apéndice B:

10.1 Stand Alone Servers 2008 y superiores - configuración UAC

Tras el endurecimiento de Microsoft UAC en el Sistema Operativo del Servidor 2012 en adelante, el acceso predeterminado a las ventanas compartidas se permite solo después del acuerdo de seguridad emergente incluso para el grupo de Administradores.

Trabajar con herramientas de penetración automatizadas requiere acceso completo a los recursos compartidos predeterminados para el nivel de administrador. No existe ningún riesgo para el sistema al permitir y administrar adecuadamente el grupo de administradores y permitir el acceso completo al grupo de administradores para compartir de forma predeterminada.

Este nivel de seguridad se consigue mediante las siguientes políticas:

Computer Configuration --> Windows Settings --> Security Settings --> Local Policies --> Security Options

- Control de cuentas de usuario: Modo de aprobación de administrador para la cuenta de administrador incorporado
- Control de cuentas de usuario: comportamiento del indicador de elevación para administradores en Modo de aprobación de administrador
- Control de cuentas de usuario: ejecute todos los administradores en modo de aprobación de administrador

Para permitir el acceso de solo administradores del grupo sin preguntar, siga estos pasos:

Establezca la configuración de políticas de la siguiente manera en el siguiente orden según la captura de pantalla a continuación:

- Disabled
- Elevate without prompting
- Disabled