Herramienta o comando de respuesta a incidentes

|  |  |  |
| --- | --- | --- |
| **Herramienta o comando de respuesta a incidentes** | **Objetivo** | **Disponibilidad** |
| command.com | El comando command.com es el intérprete de comandos de MS-DOS y es necesario para la mayoría de los sistemas operativos de Microsoft.  Sin el intérprete de comandos command.com, la computadora que ejecuta un sistema operativo de Microsoft no podría  arrancar. | Dentro del sistema operativo Windows 2000: c:\winnt\system32 |
| edit.com | El comando edit.com permite al usuario ver, crear y modificar archivos de computadora. | Dentro del sistema operativo Windows 2000:  c:\winnt\system32 |
| fdisk.exe | El comando fdisk permite al usuario eliminar y crear particiones en la unidad de disco duro. | <http://www.23cc.com/free-fdisk/> |
| format.com | El comando format.com se usa para borrar toda la  información del disquete o de la unidad fija de una computadora. | Dentro del sistema operativo Windows 2000:  c:\winnt\system32 |
| fport.exe | El programa Fport informa de todos los puertos TCP/IP y UDP abiertos, y los asigna a la aplicación correspondiente.  Esta es la misma información que usted vería usando el comando 'netstat –an', pero también asigna esos puertos a los procesos de ejecución con el PID (número de identificación de proceso), el nombre del proceso y la ruta de acceso.  El programa Fport puede usarse para identificar rápidamente puertos abiertos desconocidos y sus aplicaciones asociadas. | [http://www.foundstone.com/knowledge/proddesc/fport.](http://www.foundstone.com/knowledge/proddesc/fport) html |



|  |  |  |
| --- | --- | --- |
| **Herramienta o comando de respuesta a incidentes** | **Objetivo** | **Disponibilidad** |
| listdlls.exe | El programa ListDLLs le muestra los nombres completos de las rutas de acceso de los módulos cargados, no sólo sus nombres base.  Además, ListDLLs marca los DLLs cargados que tienen números de versión distintos de sus archivos correspondientes en el disco (lo cual ocurre cuando se actualiza el archivo después de que un programa carga el DLL), y puede indicarle a usted cuáles DLLs se reubicaron  porque no están cargados en su dirección base. | <http://www.sysinternals.com/ntw2k/freeware/listdlls.sht> ml |
| md5sum.exe | El programa Md5sum genera una "huella dactilar" o "síntesis del mensaje" de 128 bits por cada archivo de entrada, y puede verificar con la salida de una ejecución anterior si las síntesis del mensaje siguen siendo las mismas (es decir, si  los archivos cambiaron). | <http://www.etree.org/md5com.html> |
| md5summer.exe | MD5Summer es una aplicación de Microsoft Windows 9x, NT, ME, 2000 y XP que genera y verifica las sumas de comprobación md5.  Su archivo de salida es compatible con la salida del Linux GNU MD5Sum, y también lee archivos generados en Linux. | <http://www.md5summer.org/download.html> |
| nc.exe | Netcat ha sido apodado la navaja multiusos de la red. Es una utilidad Unix sencilla que lee y graba datos en todas las conexiones de la red usando el protocolo TCP o UDP.  Está diseñado como una herramienta segura 'back-end' que puede ser usada directamente o controlada con facilidad por otros programas y secuencias de comandos.  Al mismo tiempo, es una herramienta de exploración y depuración de red, rica en funciones dado que puede crear  casi cualquier tipo de conexión que usted pudiera necesitar y tiene varias capacidades integradas. | <http://www.atstake.com/research/tools/network_utilitie> s/ |



|  |  |  |
| --- | --- | --- |
| **Herramienta o comando de respuesta a incidentes** | **Objetivo** | **Disponibilidad** |
| netstat.exe | El comando netstat se utiliza para mostrar información y estadísticas del protocolo de red TCP/IP. | Dentro del sistema operativo Windows 2000:  c:\winnt\system32 |
| ntlast.exe | El programa NTLast se destina específicamente a la seguridad y administración a fondo de IIS. El análisis programado de sus registros de eventos NT es indispensable para su red.  Mediante una auditoría periódica del sistema, puede descubrirse una infracción al servidor. En la actualidad, con NTLast, es más fácil realizar la identificación y el seguimiento de quién haya tenido acceso a su sistema, así como la documentación subsiguiente de los detalles.  Esta herramienta puede informar rápidamente sobre el estado de los usuarios de IIS, y filtrar además los inicios de sesión  del servidor web de los inicios de sesión de la consola. | <http://www.foundstone.com/knowledge/proddesc/ntlas> t.html |
| psinfo.exe | La herramienta Psinfo enumera información del sistema acerca de la computadora. | <http://www.sysinternals.com/ntw2k/freeware/pstools.s> html |
| pslist.exe | La herramienta Pslist enumera información detallada sobre los procesos que se ejecutan en la computadora. | <http://www.sysinternals.com/ntw2k/freeware/pstools.s> html |
| psloggedon.exe | La herramienta Psloggedon enumera los usuarios conectados localmente y por medio de recursos compartidos (se incluye el origen completo). | <http://www.sysinternals.com/ntw2k/freeware/pstools.s> html |
| psuptime.exe | La herramienta PsInfo enumera información acerca del sistema. | <http://www.sysinternals.com/ntw2k/freeware/pstools.s> html |
| pwdump.exe | La herramienta Pwdump extrae los hash de contraseñas del registro. | <http://www.atstake.com/research/lc/download.html> |
| ritedisk.exe | El comando ritedisk hace el borrado físico o absoluto (lógico) de una unidad específica. | <http://www.sydex.com/forensic.html> |



|  |  |  |
| --- | --- | --- |
| **Herramienta o comando de respuesta a incidentes** | **Objetivo** | **Disponibilidad** |
| uptime.exe | El comando uptime imprime la hora actual, el tiempo que el sistema ha estado activado, el número de usuarios en línea y el promedio de carga. | <http://www.microsoft.com/ntserver/nts/downloads>  /management/uptime/default.asp |
| viewdisk.exe | El programa ViewDisk busca datos ocultos o eliminados en los disquetes de computadora, cualquiera que sea el formato. También analiza el contenido y la coherencia de los disquetes, verificando los casos en los que la extensión de un archivo puede no coincidir con el tipo de archivo real.  Busca valores definidos por el usuario en cualquier disquete, imprime datos por sector físico o por archivo, y copia casi cualquier tipo de disquete sin considerar el formato o el tipo. Como protección contra la alteración accidental de los datos, el programa ViewDisk requiere que los disquetes examinados estén protegidos contra escritura. Una traza de auditoría con la fecha y hora estampadas mantiene un registro de todas las  operaciones de ViewDisk durante una sesión. | <http://www.sydex.com/forensic.html> |
| more.com | El comando more.com es un filtro que permite examinar un texto continuo, una pantalla a la vez, en una terminal de copia virtual. Por lo general, hace una pausa después de cada pantalla, imprimiendo el nombre del archivo actual al pie de la pantalla o 'More' si la entrada es de una canalización.  Si el usuario presiona luego la tecla Enter (Entrar), aparece otra línea.  Si el usuario presiona la tecla de espacio, aparece otra pantalla. | Dentro del sistema operativo Windows 2000: c:\winnt\system32 |