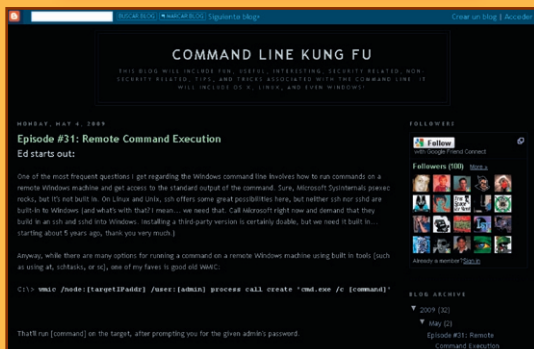




VISITA RECOMENDADA

commandlinekungfu.com



La línea de comando: nuestra mejor aliada o nuestra peor enemiga, en clara competencia con la interfaz gráfica de usuario. La primera, poco atractiva, rudimentaria y con una curva de aprendizaje empinada al principio, pero fiable, potente y precisa. La segunda, mucho más seductora, sofisticada y con una pendiente de aprendizaje mucho más suave pero menos rápida y eficaz. En el campo de la seguridad, estas diferencias son evidentes. Las herramientas de seguridad más básicas, que en muchas ocasiones son las más necesarias, ofrecen la posibilidad de ser utilizadas mediante la línea de comando. Es más, cuando se trata de realizar secuencias de acciones (en inglés "scripts"), especialmente si éstas se ejecutan en todo un parque de ordenadores, la línea de comando es la única alternativa.

El sitio que recomiendo visitar en este número estival de SIC tiene su origen en una conversación de Ed Skoudis en "Twitter". Su nombre es commandlinekungfu.com. Consiste en un *blog* en inglés de muy reciente creación, nada sofisticado en su formato, con una estructura de navegación básica, pero con propuestas de uso de la línea de comando muy interesantes para aquellos profesionales de la seguridad que trabajen en una consola, realizando pruebas forenses o auditorías de seguridad.

Commandlinekungfu.com está dedicado en exclusiva a las casi infinitas posibilidades que ofrece la línea de comando en Linux, Windows y, en ocasiones, también Mac OS X para realizar tareas muy concretas. Estas actividades están presentes en las auditorías de seguridad en sistemas. El número de autores en este blog se reduce a tres gurús en administración y seguridad en sistemas: **Ed Skoudis**, en Windows; **Hal Pomeranz**, en Linux; y **Paul Asadoorian**, principal "culpable" de la difusión de este *blog* —como se puede escuchar en el episodio 146 del "podcast" de "pauldotcom"— en Linux y Mac OS X. Todos

ellos son profesores en los cursos de seguridad del Instituto Sans. Hay un cuarto autor, el señor **Bucket** (ver nota), que proporciona ideas alternativas.

Al menos una vez por semana, los autores de este *blog* lanzan un desafío técnico que puede llevarse a cabo a través de la línea de comando, como comprobar si un parche ya ha sido instalado. Es entonces cuando comienza la diversión. Por ejemplo, Hal propone cómo realizar esa acción utilizando la línea de

comando en Linux. A continuación responde Ed exponiendo cómo se realizaría la misma operación con la línea de comando de Windows. Unas líneas más abajo, Paul sugiere algún que otro cambio en los comandos propuestos para hacerlos más efectivos, más orientados hacia el objetivo final o, simplemente, más cortos y elegantes. Se produce así una conversación, en las páginas de este *blog*, llena de buenas ideas sobre cómo utilizar de forma avanzada la línea de comando de Linux y Windows en tareas de seguridad.

La densidad de información por línea publicada es muy alta. Para aquellos que tengan que realizar en sus pruebas de seguridad actividades como consultar registros en un servidor de dominios ("DNS snooping"), averiguar la fecha de creación de un usuario, encontrar todos los ficheros cuyo nombre contenga determinados caracteres o borrar los contenidos de un fichero, este sitio es de recomendada visita. Es una oportunidad para ver en acción utilidades tan potentes, y a la vez complejas de usar, como "awk" en Linux o los bucles anidados, ("F loops") en Windows. Por cierto, los lectores podemos enviar sugerencias o preguntas a la dirección "suggestions@commandlinekungfu.com".

Una anécdota que sirve también de ejemplo del nivel avanzado que alcanzan con la línea de comando: el pasado 8 de abril de este 2009 los autores se enfrascaron en una "interesante" competición para realizar un "ping" y provocar que la máquina que envía el paquete ICMP "ping" emita un pitido cada vez que no reciba el esperado paquete de respuesta. Sólo queda confiar en que este sitio no sea una estrella fugaz en el firmamento de Internet.

Nota. Es posible que el nombre esté inspirado en un curioso juguete lanzado en Estados Unidos en 1992. Aquellos interesados en saber cómo era el juguete y el eslogan que lo promocionaba pueden visitar http://en.wikipedia.org/wiki/Mr._Bucket



Alberto Partida Rodríguez
Especialista en Seguridad TI
Securityandrisk.blogspot.com
Sugerencias y comentarios:
apartidar@gmail.com