Cómo ser el mejor HACKER

Contenido

1. Actitud del hacker
2. Lenguajes de programación
3. Sistema operativo
4. La red
5. La memoria
6. Las herramientas

1.

Actitud del hacker

La parte más importante

“

El mundo está lleno de problemas maravillosos para ser resueltos”

Cómo piensa un HACKER?

Robar, atacar?

El término *hacker*, se utiliza muy a menudo en nuestra sociedad para referirse un delincuente informático. Esto es totalmente erróneo!. En realidad el internet existe actualmente gracias a la contribución de los verdaderos hackers. La mentalidad de un hacker está orientada a resolver problemas y construir cosas. Los valores más importantes que tiene un hacker son: compartir, cooperar y generar valor para los demás.

La actitud debe complementarse con la habilidad. A continuación explicaremos los conocimientos más importantes que un hacker debe perfeccionar.

Un hacker es un experto en informática. Está dispuesto a pasar horas resolviendo desafíos, construyendo y compartiendo sus proyectos y experiencia con la comunidad.

Qué **habilidades** son necesarias?

2.

Lenguajes de programación

Las piezas fundamentales

Conviértete en un gran PROGRAMADOR

C, Python, Perl?

La habilidad fundamental del hacker, por supuesto, es saber programar. A pesar de que existe una gran cantidad de lenguajes de programación, todos tienen en común la lógica con la que se resuelven los problemas.

Cada lenguaje tiene su enfoque específico y se utilizan de acuerdo a la situación en la que nos encontramos. Con la práctica necesaria llegaremos a aprender un nuevo lenguaje en unos par de días. Si aún no sabes programar te recomiendo **C++** y **Python**. Este último tiene una curva de aprendizaje corta, tiene una gran comunidad y es muy poderoso para realizar herramientas para hacking.

C++ nos permite administrar la memoria directamente, es decir, corre bajo nuestra responsabilidad la asignación y liberación de memoria.

3.

Sistemas Operativos

Windows o Linux?

Domina los SISTEMAS OPERATIVOS

Explotando Windows

Cuando accedemos al ordenador de un víctima, nos interesa desplazarnos a través del directorio y conocer en qué lugar se encuentra la información más importante. Esto solo es posible si estamos familiarizados con su Sistema Operativo.

Existen diferentes sistemas operativos, cada cual con un enfoque diferente. Windows está instalado en la mayoría de ordenadores. Por lo tanto, si queremos aprovechar sus vulnerabilidades debemos conocerlo muy bien.

En Windows es imperativo que aprendamos a utilizar herramientas como DOS, Powershell y WMIC.

Domina los SISTEMAS OPERATIVOS

Windows o Linux?

Linux es el OS más utilizado por los expertos en seguridad informática, debido a que nos brinda mayor flexibilidad y estabilidad y además, las mayoría de herramientas para hacking están en Linux. Una característica muy importante de Linux es el hecho de ser software libre, y para un hacker lleva esta filosofía profundamente.

Sin embargo, también es importante movernos con Windows. Esto debido a que la mayoría de ordenadores en el mundo lo usan, y lo más seguro es que nuestras víctimas lo están utilizando ahora mismo.

Las distribuciones de Linux más utilizadas por los hackers son:

- Kali Linux
- ParotSecurity OS
- BackBox

4.

La red

Nuestro campo
de batalla

Domina la Red & los protocolos

Transmitiendo

La red es el paraíso para un hacker. Ya que en este lugar podemos conectarnos con otros ordenadores y desafiar nuestras habilidades.

Al tener acceso a una red podemos hacer cosas increíbles. Por ejemplo, mirar el tráfico que viaja desde y hacia nuestra red o acceder a otro ordenador remotamente.

En primer lugar es necesario conocer la estructura, característica y protocolos de red..

La red funciona a través de una estructura en forma de capas. Cada capa representa un servicio para transportar los datos.

La red es un conjunto de equipos conectados por cables, ondas o algún medio para intercambiar datos.

Domina la Red & los protocolos

Protocolos de red

Internet está basado en el modelo **TCP/IP**, que es una descripción de un conjunto de protocolos.

Los protocolos son las reglas que sugieren cómo deben comunicarse los ordenadores y dispositivos en la red para transmitir datos hacia cualquier parte del mundo.

Los protocolos de red seguros como SSH o IPSec utilizan funciones criptográficas para garantizar que las operaciones realizadas en la red tengan un mayor nivel de seguridad.

Internet es la red de ordenadores más grande que existe. Internet es el vivo ejemplo de cooperaciòn y nos ha permitido tener un mundo hiperconectado.

5.

La memoria

Nuestra puerta
de entrada

Domina la Memoria

El procesador de un ordenador usa registros, como un tipo de memoria, de menor capacidad pero más rápida!

Ejecutando malware

Cuando un programa es ejecutado, el computador le asigna un espacio en la memoria. Desde este lugar el procesador se encargará de leer cada instrucción. Incluso el malware se ejecuta de forma similar. Por lo tanto, conocer el funcionamiento de la memoria es una de las habilidades más importantes.

Existen diferentes tipos de memoria, que podemos distribuirlos de forma jerárquica.

En la parte superior tenemos las memorias más rápidas y caras, pero de menor capacidad que las memorias que siguen en la pirámide.

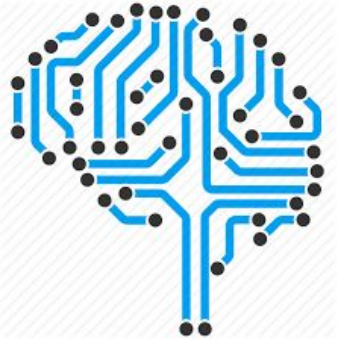
Domina la Memoria

Shellcode

Cuando encontramos una vulnerabilidad en un programa y queremos aprovecharnos esta situación, escribimos un shellcode. Este es un código que se inyecta en el programa vulnerable para ganar acceso a un ordenador remotamente. Uno de los pasos más importantes en la construcción de un shellcode es conocer las direcciones de memoria en las que estamos trabajando.

Otra área donde se trabaja continuamente con la memoria es en análisis forense. Los expertos en esta área buscan en la memoria pistas y evidencias sobre delitos informáticos. Además deben conocer el funcionamiento del sistema de archivos de un ordenador. Este sistema se encarga de gestionar la creación, modificación y borrado de archivos.

Cuando se elimina un archivo, es posible realizar un tratamiento directamente en la cinta de nuestro disco para recuperarlo!



6.

Herramientas

Cada escenario
es diferente

Prepara tu kit para la batalla

Manténte preparado

Existen actualmente cientos de programas en el mundo de la seguridad informática. Sin embargo solo unos pocos se adaptarán a cada ocasión. Debemos estar familiarizados con una gran cantidad de programas y saber como sacarles el máximo provecho. Por ejemplo para realizar un análisis de las vulnerabilidades podemos utilizar: nmap. Y para explotar fallos en un programa en cambio, utilizaremos metasploit. Los sistemas operativos orientados a la seguridad informática como Kali linux, poseen ya instaladas muchas de estas herramientas.

Ahora que ya sabemos programar, podemos incluso, escribir nuestros propios programas o mejorar los que ya existen!.

Academia de seguridad informática

OWLMIND.COM