Seguimos atrasando el laboratorio porque me es más fácil y rápido hacer esto. Sino, próximamente voy a terminar sin hacer el video y haciendo solo el tutorial escrito :/ no porque no quiera, pero hay que ver las facilidades que tendré.

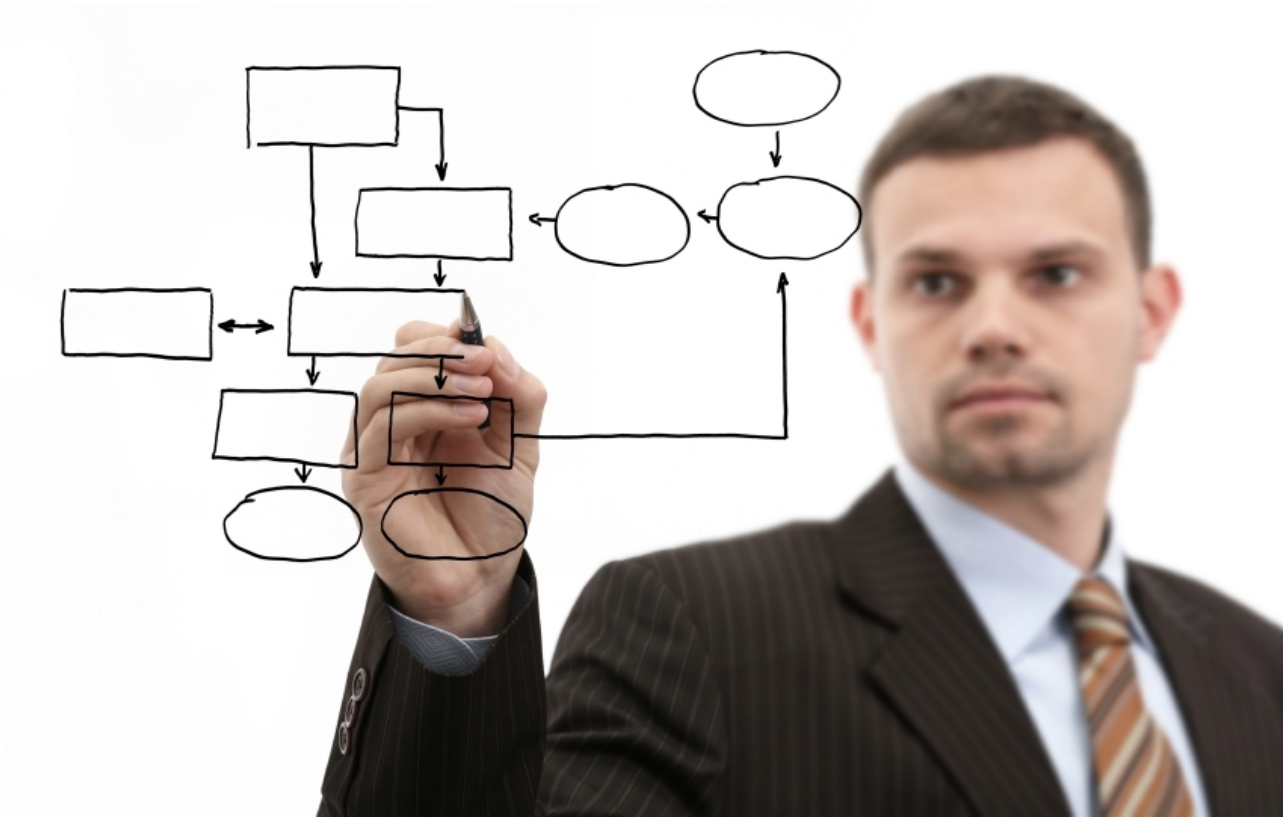
Sabemos que en los sistemas se contiene mucha información. Tanto en una industria gigante como en el usuario común como lo puede ser tu abuela. Y nosotros vamos a tener que proteger esta información -aunque seguramente muchos están con la idea contraria-. Entonces, cuando a esa información lo hacemos mediante procesos de software, se le llama **defensa lógica.**

La defensa lógica intenta protegernos de los famosos hackers porque, simplemente, **no podemos confiar en nadie.**

"¿Ni siquiera en mi abuelita?"

Ni siquiera en ella, Manolo. Nunca podemos estar seguros de quien podría poner nuestra información o nuestro trabajo en riesgo.

Nos vamos a concentrar en los ataques **más habituales**. En una terminal casera no podemos darle mucho énfasis si no es necesario. Si vamos a ser unos locos de la seguridad y psicóticos como tal, debemos darle una justificación apropiada pues si les decimos a nuestra abuelita que debe poner una contraseña de 40 carácteres con mayúsculas, minúsculas, números y carácteres especiales; variando entre cada cuenta y cambiándola cada 1 mes, vamos a tener serios problemas familiares. Entonces, primero habría que **armar un plan** sobre lo que realmente vamos a hacer y el por qué de ésto.



Veamos las herramientas de uso común que **no deben faltar** en ningún sistema.

Antivirus

Famoso y querido antivirus. Hoy en día ya no es simplemente un antivirus -aunque sigan manteniendo la denominación- sino que se extendió a frenar **todo tipo de malware**. Y quisiera aclarar que en realidad, si un desarrollador de malware quiere pasar desapercibido a sus queridos hijos lo va a lograr, pero si se masifica o si es un virus conocido y peligroso que anda dando vueltas **no debemos estar desprotegidos**. No es una herramienta fantástica porque además de su corto desarrollo en base al tiempo, también hay muchas de ellas que son bastante pobres con respecto a su heurística, pero no por esto debemos pasarlo de largo.

"Heu... ¿Què?"

Heurística. Ésta es una técnica que apareció para evolucionar a las herramientas, porque lo único que harían estos programillas sería comparar los hashes de los software que hay allí con los hashes que residen en una base de datos propia. Estos hashes se le llaman firmas digitales ¿Recuerdan?

Entonces, la técnica que antes estábamos mencionando se encarga de hacer varias cosas.

1. Compara **partes del programa** -y no al programa entero- con sus **firmas**. Detectando así partes de código maliciosos y pudiendo encontrarlos en una versión modificada de un virus o en un ejecutable modificado.
2. Puede encontrar código malicioso intentando de **leer el código fuente de un ejecutable**. Luego lo veremos mejor pero un ejecutable puede ser **desensamblado** -que significa ver el código del programa en lenguaje ensamblador y así poder interpretarlo-, aunque muchas veces la industria del software utiliza técnicas para que alguien no pueda desensablarlo y , por ejemplo, hacer el crack de dicho programa comercial.
3. Como muchos virus son camuflados (**empaquetados**), el antivirus realiza una prueba en una caja de arena, **virtualizando un ambiente para desempaquetar** el virus y ver su comportamiento real. Igualmente, esta pelea no es de un solo lado ya que muchos virus varían el comportamiento analizando el entorno en el que está.

"Hace un montón de cosas, ya entendí. Pero entonces ni pago para tener un antivirus corporativo."

En realidad, **es conveniente pagar** por la versión comercial del producto ya que trae muchas funcionalidades que de otra manera no traería.

No nos quedemos interiorizándonos en los antivirus. Vayamos al próximo defensor.

Firewall

Firewall o **cortafuegos**. Éste es **importantísimo**. Aunque muchos (muchos en serio -.-) lo desactiven o lo usen con la configuración por defecto, hay que tener en cuenta que es una de las herramientas más poderosas para nuestra defensa. Algunas propiedades que hay en esta preciosa herramienta son:

1. **Elige** el **tráfico** saliente, **filtrando** por **reglas** prehechas o personalizadas por el usuario. Puede manejar todo tipo de capas (siempre suponiendo que es un firewall completo), y genera reglas genéricas o puntuales. A los paquetes los puede **dropear** -descartar, desechar-, realizar una **alerta**, guardarlo en un **log**, o lo que sea necesario.
2. **Elige** y **filtra** el **tráfico** entrante. Lo mismo que sucede con el anterior punto, y puede realizar contestaciones muy acertadas ante ciertos ataques. También puede prohibir la conexión a ciertas IP's o MAC's y hacer de ésta, una regla dinámica que va a cambiando en el transcurso del tiempo.

Parece poco pero realmente es muchísimo, ya que controla el tráfico de datos **en el sistema alojado y en las conexiones del mismo.** Aclaro que a veces se usan distintos firewalls para distintas cosas.

Otra de las cosas interesantes es que los firewall no están únicamente en los terminales cliente, sino que también suceden ser una de las piezas más importantes en una red, existiendo así, **firewalls sobre hardware dedicado**, o firewalls en ciertos dispositivos como **switchs** o **routers**.

Si esta pieza **falla**, lamento decir esto pero, **estamos realmente jodidos**.

Otra de las medidas que se pueden usar ya van de la mano del usuario, pero algunas irán en esta sección y algunas otras en la seguridad física.

Contraseñas.

Seamos conscientes del ataque que podemos recibir. Luego veremos la eficacia con los laboratorios, pero ahora fíjense que sacar una clave es tan fácil como intentar muchas veces hasta dar en el clavo. Entonces las recomendaciones para ésto serían:

1. Usar contraseñas de una longitud **extensa**
2. Usar **distintas** contraseñas para cada cuenta (imaginen que sino, una contraseña perdida es igual a todas las cuentas arriesgadas. Mejor no pasar vergüenza).
3. **No** usar una contraseña que sea idéntica al usuario
4. **No** usar una contraseña muy usada ya que los diccionarios más pobres la sacarán sin problemas.
5. Usar **carácteres especiales, minúsculas, mayúsculas y números**. Esto hará que un ataque de fuerza bruta sea mucho más lento.
6. Usar **carácteres propios de la lengua**, como una ñ o ç porque hay muchos programas que ni siquiera tienen la posibilidad de usarla para el ataque, además de ser desconocida para la mitad del mundo.
7. **No** utilizar datos obvios como nombres de conocidos, o propios, fechas especiales, números de documentos, gustos propios. Esta información está muy digitalizada, más que nada por las redes sociales.
8. Usar contraseñas para todos los **accesos** posibles a la computadora personal

Luego veremos más consejos para ésto.

Algunos **consejos cortos** para el usuario:

Antivirus.

1. No desactivarlo
2. No colocar más excepciones de las que deberíamos
3. Hacerle caso xD
4. Si es posible, tener uno pago y uno bueno
5. Configurarlo o pedirle a alguien que lo haga por usted
6. No instalar más de uno al mismo tiempo ya que es muy complicada la convivencia entre ellos.

Firewall.

1. Configurarlo bien y a medida, ni que sea imposible conectarse a internet, ni que le fuera fácil al atacante saber lo que uno tiene dentro
2. Utilizar tanto uno de host como uno de router
3. No descactivarlo (los conozco -.-)
4. Leer el manual respectivo
5. No utilizar el de Windows por defecto
6. Claramente no usar más de uno al mismo tiempo

Descargas.

1. No descargar material que sabemos que puede ser malicioso, a menos que estemos desesperados y sea completamente necesario
2. Utilizar enlaces de sitios oficiales
3. Si usa android, leer qué es lo que necesita la aplicación y usar el sentido común para darle acceso
4. Tener mucho cuidado con las redes P2P, más que nada con las carpetas compartidas ya que a veces damos más información de la que deberíamos
5. Leer cuando uno instala, el acuerdo y cada ventanita antes de apretar "siguiente" (estoy seguro que nadie lo hace)

6. Intentar de usar programas que no sea muy general si es posible. Los programas con mas popularidad entre los clientes son también los mas targeteados entre los hackers

Acceso de usuario restringido.

1. No dar acceso de Administrador, o de elevados permisos a ningún usuario. Simplemente crear un usuario Administrador (Root, en linux) que tenga permisos para todo lo que sea configuración y permisos un poco elevados, con otro usuario que lo complemente y usarlo cuando sea necesario. No usar estos usuarios frecuentemente.
2. A los otros usuarios no darle más ni menos privilegios de los que deben tener.
3. Usar distintas contraseñas para los distintos usuarios
4. No crear un usuario sin protección por contraseña
5. Si usamos una cuenta de información muy sensible, no conectarla a internet o lo menos posible y no hacer otra cosa que los manejos de esa información
6. Que la cuenta se bloquee si no estamos
7. Que no comparta servicios de manera insegura

Bueno, esto sería lo fundamental para un dispositivo personal. Intenten de seguir estas reglas al pie de la letra y verán que no les va a ser fácil, ya que no hay una masificación de la seguridad informática en América Latina, aún.

Cualquier cosa pueden mandarme mail a: r0add@hotmail.com

Para donaciones, pueden hacerlo en bitcoin en la dirección siguiente:

1HqpPJbbWJ9H2hAZTmpXnVuoLKkP7RFSvw

Roadd.
