Ataques informáticos

Debilidades de seguridad comúnmente explotadas

Centro de Ethical Hacking & Security

LNXnetwork
SOLUCIONES ALTERNATIVAS

Ataques informáticos

A lo largo del tiempo, el avance de los medios tecnológicos y de comunicación ha provocado el surgimiento de nuevos vectores de ataques y de nuevas modalidades delictivas que han transformado a Internet y las tecnologías informáticas en aspectos sumamente hostiles para cualquier tipo de organización, y persona, que tenga equipos conectados a la World Wide Web (WWW).

LNXnetwork
SOLUCIONES ALTERNATIVAS

Centro de Ethical Hacking & Security

Ataques informáticos

A diferencia de lo que sucedía años atrás, donde personas con amplias habilidades en el campo informático disfrutaban investigando estos aspectos con el ánimo de incorporar mayor conocimiento; en la actualidad se ha desvirtuado completamente dando origen a nuevos personajes que utilizan los medios informáticos y el conocimiento sobre su funcionamiento como herramientas para delinquir y obtener algún beneficio económico.

Ataques informáticos

Ataques informáticos

Cada día se descubren nuevos puntos débiles y, por lo general, son pocos los responsables de IT que comprenden en su justa medida la importancia que tiene la seguridad y cómo pueden abordar el grave problema que existe detrás de vulnerabilidades que permiten a un atacante, violar la seguridad de un entorno y cometer delitos en función de los datos robados.

Ataques informáticos

Bajo esta escenografía donde los principales actores son las organizaciones de cualquier magnitud y rubro, los sistemas de información, el dinero y delincuentes informáticos; se torna realmente necesario y fundamental idear estrategias de seguridad que permitan establecer
barreras defensivas orientadas a mitigar efectivamente ataques tanto externos como internos.

Ataques informáticos

Pero para lograr mitigar de manera eficaz el impacto provocado por los ataques informáticos, es de capital importancia conocer de qué manera atacan y cuáles son los puntos débiles de un sistema comúnmente explotados en los que se deben enfocar los esfuerzos de seguridad tendientes a la prevención de los mismos.

Ataques informáticos

¿De qué estamos hablando?

Un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización.

Ataques informáticos

Para minimizar el impacto negativo provocado por ataques, existen procedimientos y mejores prácticas que facilitan la lucha contra las actividades delictivas y reducen notablemente el campo de acción de los ataques.

Ataques informáticos

Uno de los pasos más importantes en seguridad, es la educación. Comprender cuáles son las debilidades más comunes que pueden ser aprovechadas y cuáles son sus riesgos asociados, permitirá conocer de qué manera se ataca un sistema informático ayudando a identificar las debilidades y riesgos para luego desplegar de manera inteligente estrategias de seguridad efectivas.

Ataques informáticos

Anatomía de un ataque informático

Conocer las diferentes etapas que conforman un ataque informático brinda la ventaja de aprender a pensar como los atacantes y a jamás subestimar su mentalidad.

Desde la perspectiva del profesional de seguridad, se debe aprovechar esas habilidades para comprender y analizar la forma en que los atacantes llevan a cabo un ataque.

Ataques informáticos

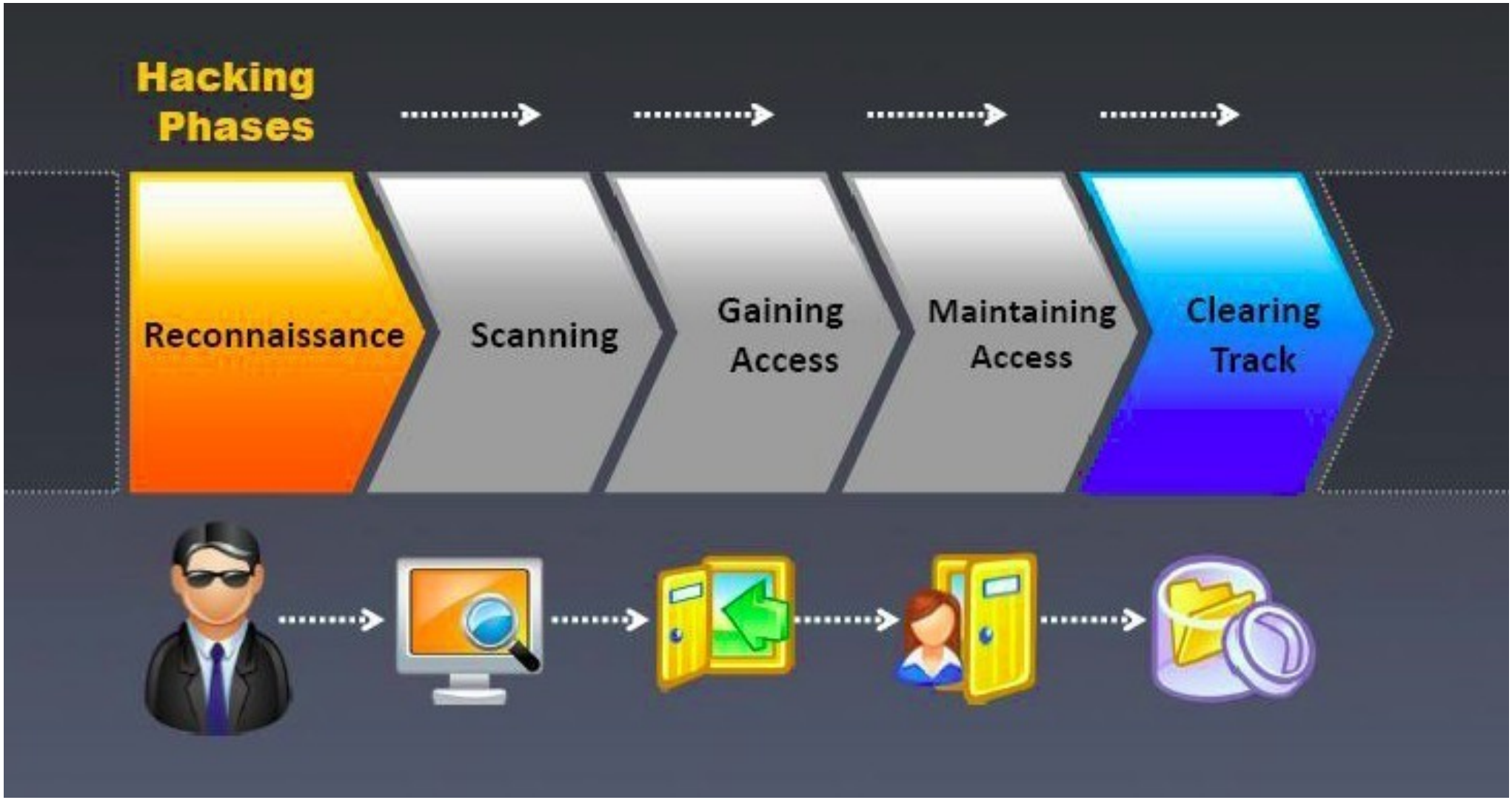


Figura 1. Fases comunes de un ataque informático

Ataques informáticos

Fase 1: Reconnaissance (Reconocimiento).

Esta etapa involucra la obtención de información (Information Gathering) con respecto a una potencial víctima que puede ser una persona u organización.

Por lo general, durante esta fase se recurre a diferentes recursos de Internet como Google, entre tantos otros, para recolectar datos del objetivo. Algunas de las técnicas utilizadas en este primer paso son la Ingeniería Social, el Dumpster Diving, el sniffing.

LNXnetwork
SOLUCIONES ALTERNATIVAS

Centro de Ethical Hacking & Security

Ataques informáticos

Fase 2: Scanning (Exploración).

En esta segunda etapa se utiliza la información obtenida en la fase 1 para sondear el blanco y tratar de obtener información sobre el sistema víctima como direcciones IP, nombres de host, datos de autenticación, entre otros.

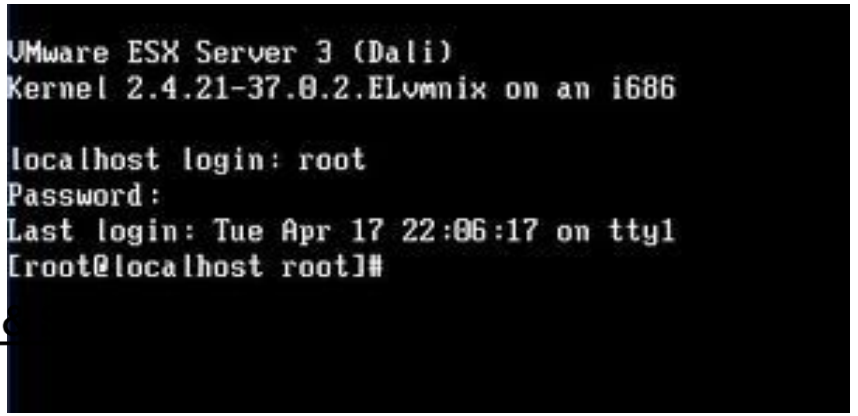
Ataques informáticos

Entre las herramientas que un atacante puede emplear durante la exploración se encuentra el network mappers, port mappers, network scanners, port scanners, y vulnerability scanners.

Ataques informáticos

Fase 3: Gaining Access (Obtener acceso).

En esta instancia comienza a materializarse el ataque a través de la explotación de las vulnerabilidades y defectos del sistema (Flaw exploitation) descubiertos durante las fases de reconocimiento y exploración.



Ataques informáticos

Algunas de las técnicas que el atacante puede utilizar son ataques de Buffer Overflow, de Denial of Service (DoS), Distributed Denial of Service (DDos), Password filtering y Session hijacking.

Ataques informáticos

Fase 4: Maintaining Access (Mantener el acceso).

Una vez que el atacante ha conseguido acceder al sistema, buscará implantar herramientas que le permitan volver a acceder en el futuro desde cualquier lugar donde tenga acceso a Internet. Para ello, suelen recurrir a utilidades backdoors, rootkits y troyanos.

Ataques informáticos

Fase 5: Clearing Tracks (Borrar huellas).

Una vez que el atacante logró obtener y mantener el acceso al sistema, intentará borrar todas las huellas que fue dejando durante la intrusión para evitar ser detectado por el profesional de seguridad o los administradores de la red. En consecuencia, buscará eliminar los archivos de registro (log) o alarmas del Sistema de Detección de Intrusos (IDS).

Ataques informáticos

La seguridad consta de tres elementos fundamentales que forman parte de los objetivos que intentan comprometer los atacantes. Estos elementos son la **confidencialidad**, la **integridad** y la **disponibilidad** de los recursos.

Ataques informáticos

Bajo esta perspectiva, el atacante intentará explotar las vulnerabilidades de un sistema o de una red para encontrar una o más debilidades en alguno de los tres elementos de seguridad.

Ataques informáticos

Para que, conceptualmente hablando, quede más claro de qué manera se compromete cada uno de estos elementos en alguna fase del ataque, tomemos como ejemplo los siguientes casos hipotéticos según el elemento que afecte.

Ataques informáticos

Confidencialidad.

Un atacante podría robar información sensible como contraseñas u otro tipo de datos que viajan en texto claro a través de redes confiables, atentando contra la confidencialidad al permitir que otra persona, que no es el destinatario, tenga acceso a los datos. Un ejemplo que compromete este elemento es el envenenamiento de la tabla ARP (ARP Poisoning).

Ataques informáticos

Integridad.

Mientras la información se transmite a través del protocolo de comunicación, un atacante podría interceptar el mensaje y realizar cambios en determinados bits del texto cifrado con la intención de alterar los datos del criptograma. Este tipo de ataques se denomina Bit-Flipping y son considerados ataques contra la integridad de la información.

Ataques informáticos

Disponibilidad.

En este caso, un atacante podría utilizar los recursos de la organización,
como el ancho de banda de la conexión DSL para inundar de mensaje el sistema víctima y forzar la caída del mismo, negando así los recursos y servicios a los usuarios legítimos del sistema. Esto se conoce como Denial of Service (DoS) y atenta directamente contra la integridad de la información.

Ataques informáticos

Debilidades de seguridad comúnmente explotadas

Afortunadamente, en la actualidad existe una gama muy amplia de herramientas de seguridad lo suficientemente eficaces que permiten obtener un adecuado nivel de seguridad ante intrusiones no autorizadas haciendo que la labor de los atacantes se transforme en un camino difícil de recorrer.

Ataques informáticos

Ingeniería Social

Más allá de cualquiera de los esquemas de seguridad que una organización pudiera plantear, existen estrategias de ataque que se basan en el engaño y que están netamente orientadas a explotar las debilidades del factor humano.

Ataques informáticos

Los atacantes saben cómo utilizar estas metodologías y lo han incorporado como elemento fundamental para llevar a cabo cualquier tipo de ataque. Si bien esta técnica es utilizada en cualquier ámbito, en lo que a informática se refiere, consiste en la obtención de información sensible y/o confidencial de un usuario cercano a una sistema u organización explotando ciertas características que son propias del ser humano.

Ataques informáticos

Ya sea por ignorancia, negligencia o coacción, pueden permitir a un atacante obtener acceso no autorizado, quien, de esta manera, podrá eludir los complejos esquemas y tecnologías de seguridad que se hayan implementado en la organización.

Ataques informáticos

Como contramedida, la única manera de hacer frente a los métodos de Ingeniería Social es la educación. Absolutamente todas las personas que forman parte de la organización, desde la secretaria, los administradores de la red y la cúpula mayor, deben estar capacitados en cuanto a las debilidades y los métodos de engaño más empleados por los atacantes para que logren identificarlos y dar aviso de cualquier anomalía que se produzca en el equipo o en determinado ambiente.

Ataques informáticos

Esto no significa que cada uno de los empleados deba realizar cursos de seguridad informática, sino que el proceso de capacitación debe formar parte de las Políticas de Seguridad de la Información y debe ser ejecutada a través de planes dinámicos de concientización.

Ataques informáticos

Por otro lado, es muy común que el personal crea erróneamente que su posición dentro de la Institución u organización es de poca importancia y que por lo tanto no podrían ser objeto de ataque, pero contrariamente, son en realidad los objetivo preferidos por los atacantes; en consecuencia, la educación es una contramedida muy efectiva, pero es de suma importancia que las personas tomen real conciencia de que ellos son el blanco perfecto de la Ingeniería Social.

Ataques informáticos

“Usted puede tener implementada la mejor tecnología, Firewalls,
sistemas de detección de intrusos o complejos sistemas de autenticación biométricos... Pero lo único que se necesita es una llamada telefónica a un empleado desprevenido y acceden al sistema sin más. Tienen todo en sus manos”

Ataques informáticos

Factor Insiders

Cuando se habla sobre las personas que se dedican a atacar sistemas informáticos, se asume que se trata de alguien desconocido que realiza el ataque y maneja todo desde un lugar remoto llevándolo a cabo a altas horas de la noche.

Ataques informáticos

Aunque en algunos casos puede
ser cierto, varios estudios han demostrado que
la mayoría de las violaciones de seguridad
son cometidos por el Factor Insiders, es decir,
por los mismos empleados desde dentro de
la Institución u Organización.

Ataques informáticos

Una de las formas más eficaces que posee un atacante para romper los esquemas de seguridad, es desde el interior de la organización. Por ejemplo, el atacante podría conseguir un empleo en la organización que desea atacar y obtener el suficiente nivel de confianza en la organización para luego explotar los puntos de acceso. Del mismo modo, cualquier integrante puede convertirse en un empleado disgustado y decidir robar información y/o causar daños como una forma de venganza.

Ataques informáticos

Cuando este tipo de actos es cometido con intenciones de obtener beneficios económicos a través de información corporativa, es denominado Insiders Trading (comercio de personal interno).

Ataques informáticos

En cualquiera de los casos, muchas de las herramientas y medidas de seguridad que se implementen en el entorno informático no serán eficaces. Bajo esta perspectiva, es necesario acudir a estrategias de defensa internas y específicas para el control de posibles ataques ocasionados por el personal de la organización. Estas estrategias defensivas funcionarán como **contramedidas**.

Ataques informáticos

Una de las mejores soluciones es realizar auditorias continuas que incluyan monitoreos a través de programas keyloggers que pueden ser por hardware o por software, mecanismos que impidan la instalación de programas por parte del personal, estricta configuración del principio de privilegios mínimos, deshabilitación de puertos USB y prohibición del uso de dispositivos de almacenamiento extraíbles para evitar la fuga de información y entrada de otras amenazas como malware, si las computadoras forman parte de un dominio es necesario establecer políticas rigurosas en el Active Directory, entre otras.

Ataques informáticos

Códigos maliciosos

Los códigos maliciosos, o malware, constituyen también una de las principales amenazas de seguridad para cualquier Institución u Organizaciones y aunque parezca un tema rivial, suele ser motivo de importantes pérdidas económicas.

LNXnetwork
SOLUCIONES ALTERNATIVAS

Centro de Ethical Hacking & Security

Ataques informáticos

Esta amenaza se refiere a programas que causan algún tipo de daño o anomalía en el **sistema informático. Dentro de esta categoría se incluyen los programas troyanos, gusanos, virus informáticos, spyware, backdoors, rootkits, keyloggers, entre otros.**

Ataques informáticos

Actualmente, casi el 80% de los ataques informáticos llevados a cabo por **códigos maliciosos, se realizan a través de programas troyanos.**

Ataques informáticos

La carga dañina que incorporan los troyanos puede ser cualquier cosa, desde instrucciones diseñadas para destruir algún sector del disco rígido, por lo general la MBR, eliminar archivos, registrar las pulsaciones que se escriben a través del teclado, monitorear el tráfico de la red, entre tantas otras actividades.

Ataques informáticos

Los atacantes suelen utilizar troyanos de manera combinada junto a otros tipos de códigos maliciosos. Por ejemplo, cuando han ganado acceso a través del troyano, implantan en el sistema otros códigos maliciosos como rootkits que permite esconder las huellas que el atacante va dejando en el equipo (Covering Tracks), y backdoors para volver a ingresar al sistema cuantas veces considere necesario; todo, de manera remota y sin que, en la mayoría de los casos, los administradores de la red adviertan su actividad.

Ataques informáticos

Las contramedidas tendientes a prevenir ataques a través de este tipo de amenazas, radican principalmente en la implementación de programas antivirus que operen bajo mecanismos de detección avanzados como la heurística, que también permitan monitorear, controlar y administrar de manera centralizada cada uno de los nodos involucrados en la red, junto a planes de educación orientados a crear conciencia en el personal sobre los riesgos de seguridad que representa el malware.

Ataques informáticos

Contraseñas

Otro de los factores comúnmente explotados por los atacantes son las contraseñas. Si bien en la actualidad existen sistemas de autenticación complejos, las contraseñas siguen, y seguirán, siendo una de las medidas de protección más utilizadas en cualquier tipo de sistema informático.

Ataques informáticos

En consecuencia, constituyen uno de los blancos más buscados por atacantes informáticos porque conforman el componente principal utilizado en procesos de autenticación simple (usuario/contraseña) donde cada usuario posee un identificador (nombre de usuario) y una contraseña asociada a ese identificador que, en conjunto, permiten identificarse frente al sistema.

Ataques informáticos

En este tipo de proceso, llamado de factor simple, la seguridad del esquema de autenticación radica inevitablemente en la fortaleza de la contraseña y en mantenerla en completo secreto, siendo potencialmente vulnerable a técnicas de Ingeniería Social cuando los propietarios de la contraseña no poseen un adecuado nivel de capacitación que permita prevenir este tipo de ataques.

Ataques informáticos

Si el entorno informático se basa únicamente en la protección mediante sistemas de autenticación simple, la posibilidad de ser víctimas de ataques de cracking o intrusiones no autorizadas se potencia.

Ataques informáticos

Si bien es cierto que una contraseña que supere los diez caracteres y que las personas puedan recordar, es mucho más efectiva que una contraseña de cuatro caracteres, aún así, existen otros problemas que suelen ser aprovechados por los atacantes. A continuación se expone algunos de ellos:

Ataques informáticos

La utilización de la misma contraseña en varias cuentas y otros servicios.

Acceder a recursos que necesitan autenticación desde lugares públicos donde los atacantes pueden haber implantado programas o dispositivos físicos como keyloggers que capturen la información.

Ataques informáticos

Utilización de protocolos de comunicación inseguros que transmiten la información en texto claro como el correo electrónico, navegación web, chat, etcétera.

Técnicas como surveillance (videoconferencia) o shoulder surfing (mirar por detrás del hombro), entre otras tantas, que permiten evadir los controles de seguridad.

Ataques informáticos

Como contramedida destinada a fortalecer este aspecto de la seguridad, es posible implementar mecanismos de autenticación más robustos como “autenticación fuerte de doble factor”

De nada sirve utilizar contraseñas fuertes si luego son olvidadas o compartidas, ya que con ello se compromete la seguridad de todo el mecanismo de autenticación.”

Ataques informáticos

Configuraciones predeterminadas

Las configuraciones por defecto, tanto en los sistemas operativos, las aplicaciones y los dispositivos implementados en el ambiente informático, conforman otra de las debilidades que comúnmente son poco atendidas por pensar erróneamente que se tratan de factores triviales que no se encuentran presentes en la lista de los atacantes.

Ataques informáticos

Sin embargo, las configuraciones predeterminadas hacen del ataque una tarea sencilla para
quien lo ejecuta ya que es muy común que las vulnerabilidades de un equipo sean explotadas a través de códigos exploit donde el escenario que asume dicho código se basa en que el objetivo se encuentra configurado con los parámetros por defecto.

Ataques informáticos

Muchas aplicaciones automatizadas están diseñadas para aprovechar estas vulnerabilidades teniendo en cuenta las configuraciones predeterminadas, incluso, existen sitios web que almacenan bases de datos con información relacionada a los nombres de usuario y sus contraseñas asociadas, códigos de acceso, configuraciones, entre otras, de los valores por defecto de sistemas operativos, aplicaciones y dispositivos físicos.

Ataques informáticos

Sólo basta con escribir en
un buscador las palabras claves “default passwords” (contraseña por defecto) para ver la infinidad de recursos disponibles que ofrecen este tipo de información.

Ataques informáticos

Por lo tanto, una de las contramedidas más eficaces para mitigar y prevenir problemas de seguridad en este aspecto, y que muchas veces se omite, es simplemente cambiar los valores por defecto. En este sentido, es importante no sacrificar la disponibilidad de los recursos por ganar seguridad. Se debe encontrar un equilibrio justo entre usabilidad y seguridad.

Ataques informáticos

La práctica de fortalecer el ambiente informático configurando de manera segura la tecnología para contrarrestar los vectores de ataque se denomina **hardening**. En este aspecto, la responsabilidad de realizar todo lo que se encuentre a su alcance para modificar los valores predeterminados recae en quienes
se encargan de la administración de los equipos.

Ataques informáticos

La práctica de fortalecer el ambiente informático configurando de manera segura la tecnología para contrarrestar los vectores de ataque se denomina **hardening**. En este aspecto, la responsabilidad de realizar todo lo que se encuentre a su alcance para modificar los valores predeterminados recae en quienes
se encargan de la administración de los equipos.

Ataques informáticos

LNXnetwork
SOLUCIONES ALTERNATIVAS

Centro de Ethical Hacking & Security