Amenazas Lógicas - Tipos de Ataques - Ataques de Autenticación

volver a Tipos de Ataques

volver a Ataques

Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y password.

- **Spoofing-Looping**

  Spoofing puede traducirse como "hacerse pasar por otro" y el objetivo de esta técnica, justamente, es actuar en nombre de otros usuarios, usualmente para realizar tareas de Snooping o Tampering (ver a continuación Ataques de Modificación y Daño).
  Una forma común de Spoofing es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él.
  El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza este para entrar en otro, y así sucesivamente. Este proceso, llamado Looping, tiene la finalidad de "evaporar" la identificación y la ubicación del atacante.
  El camino tomado desde el origen hasta el destino puede tener muchas estaciones, que exceden obviamente los límites de un país. Otra consecuencia del Looping es que una compañía o gobierno pueden suponer que están siendo atacados por un competidor o una agencia de gobierno extranjera, cuando en realidad están seguramente siendo atacado por un Insider, o por un estudiante a miles de Kilómetros de distancia, pero que ha tomado la identidad de otros.
  La investigación de procedencia de un Looping es casi imposible, ya que el investigador debe contar con la colaboración de cada administrador de cada red utilizada en la ruta.
  El envío de falsos e-mails es otra forma de Spoofing que las redes permiten. Aquí el atacante envía e-mails a nombre de otra persona con cualquier motivo y objetivo. Tal fue el caso de una universidad en EE.UU. que en 1998, que debió reprogramar una fecha completa de exámenes ya que alguien en nombre de la secretaría había cancelado la fecha verdadera y enviado el mensaje a toda la nómina de estudiantes.
  Muchos ataques de este tipo comienzan con Ingeniería Social, y los usuarios, por falta de cultura, facilitan a extraños sus identificaciones dentro del sistema usualmente través de una simple llamada telefónica.

- **Spoofing**
  Este tipo de ataques (sobre protolocos) suele implicar un buen conocimiento del protocolo en el que se va a basar el ataque. Los ataques tipo Spoofing bastante conocidos son el IP Spoofing, el DNS Spoofing y el Web Spoofing
  - **IP Spoofing**

    Con el IP Spoofing, el atacante genera paquetes de Internet con una dirección de red falsa en el campo From, pero que es aceptada por el destinatario del paquete. Su utilización más común es enviar los paquetes con la dirección de un tercero, de forma que la víctima "ve" un ataque proveniente de esa tercera red, y no la dirección real del intruso.
    El esquema con dos puentes es el siguiente:

    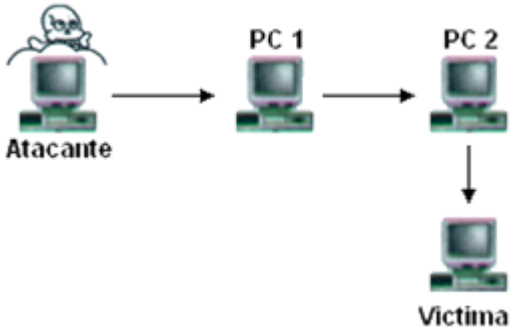

    Gráfico 7.3 – Ataque Spoofing

    Nótese que si la Victima descubre el ataque verá a la PC_2 como su atacante y no el verdadero origen.
    Este ataque se hizo famoso al usarlo Kevin Mitnick (ver Anexo II).

  - **DNS Spoofing**

    Este ataque se consigue mediante la manipulación de paquetes UDP pudiéndose comprometer el servidor de nombres de dominios (Domain Name Server–DNS) de Windows NT©. Si se permite el método de recursión en la resolución de "Nombre«Dirección IP" en el DNS, es posible controlar algunos aspectos del DNS remoto. La recursión consiste en la capacidad de un servidor de nombres para resolver una petición de dirección IP a partir de un nombre que no figura en su base de datos. Este es el método de funcionamiento por defecto.

  - **Web Spoofing**

    En el caso Web Spoofing el atacante crea un sitio web completo (falso) similar al que la víctima desea entrar. Los accesos a este sitio están dirigidos por el atacante, permitiéndole monitorear todas las acciones de la víctima, desde sus datos hasta las passwords, números de tarjeta de créditos, etc.
    El atacante también es libre de modificar cualquier dato que se esté transmitiendo entre el servidor original y la víctima o viceversa.

- **IP Splicing–Hijacking**

  Se produce cuando un atacante consigue interceptar una sesión ya establecida. El atacante espera a que la victima se identifique ante el sistema y tras ello le suplanta como usuario autorizado.
  Para entender el procedimiento supongamos la siguiente situación:

```
IP Cliente : IP 195.1.1.1
IP Servidor: IP 195.1.1.2
IP Atacante: IP 195.1.1.3
```

  1. El cliente establece una conexión con su servidor enviando un paquete que contendrá la dirección origen, destino, número de secuencia (para luego armar el paquete) y un número de autentificación utilizado por el servidor para "reconocer" el paquete siguiente en la secuencia. Supongamos que este paquete contiene:

```
IP Origen : 195.1.1.1 Puerto 1025
IP Destino: 195.1.1.2 Puerto 23
SEQ = 3DF45ADA (el primero es al azar)
ACK = F454FDF5
Datos: Solicitud
```

  2. El servidor, luego de recibir el primer paquete contesta al cliente con paquete Echo (recibido).

```
IP Origen : 195.1.1.2 Puerto 1025
IP Destino: 195.1.1.1 Puerto 23
SEQ = F454FDF5 (ACK enviado por el cliente)
ACK = 3DF454E4
Datos: Recepción OK (Echo)
```

  3. El cliente envía un paquete ACK al servidor, sin datos, en donde le comunica lo "perfecto" de la comunicación.

```
IP Origen : 195.1.1.1 Puerto 1025
IP Destino: 195.1.1.2 Puerto 23
SEQ = 3DF454E4 (ACK enviado por el servidor)
ACK = F454FDFF
Datos: Confirmación de Recepción (ACK)
```

  4. El atacante que ha visto, mediante un Sniffer, los paquete que circularon por la red calcula el número de secuencia siguiente: el actual + tamaño del campo de datos. Para calcular el tamaño de este campo:

```
1° Paquete ACK Cliente = F454FDF5
2° Paquete ACK Cliente = F454FDFF
Tamaño del campo datos = F454FDFF - F454FDF5 = 0A
```

  5. Hecho esto el atacante envía un paquete con la siguiente aspecto:

```
IP Origen : IP 195.1.1.1 (IP del Cliente por el atacante)
IP Destino: IP 195.1.1.2 (IP del Servidor)
SEQ = 3DF454E4 (Ultimo ACK enviado por el Cliente)
ACK = F454FE09 (F454FDFF + 0A)
```

El servidor al recibir estos datos no detectará el cambio de origen ya que los campos que ha recibido como secuencia y ACK son los que esperaba recibir. El cliente, a su vez, quedará esperando datos como si su conexión estuviera colgada y el atacante podrá seguir enviando datos mediante el procedimiento descripto.

- **Utilización de BackDoors**

  "Las puertas traseras son trozos de código en un programa que permiten a quien las conoce saltarse los métodos usuales de autentificación para realizar ciertas tareas. Habitualmente son insertados por los programadores del sistema para agilizar la tarea de probar código durante la fase de desarrollo"(1).
  Esta situación se convierte en una falla de seguridad si se mantiene, involuntaria o intencionalmente, una vez terminado el producto ya que cualquiera que conozca el agujero o lo encuentre en su código podrá saltarse los mecanismos de control normales.

- **Utilización de Exploits**

  Es muy frecuente ingresar a un sistema explotando agujeros en los algoritmos de encriptación utilizados, en la administración de las claves por parte la empresa, o simplemente encontrando un error en los programas utilizados.
  Los programas para explotar estos "agujeros" reciben el nombre de Exploits y lo que realizan es aprovechar la debilidad, fallo o error hallado en el sistema (hardware o software) para ingresar al mismo.
  Nuevos Exploits (explotando nuevos errores en los sistemas) se publican cada día por lo que mantenerse informado de los mismos y de las herramientas para combatirlos es de vital importancia.

- **Obtención de Passwords**

  Este método comprende la obtención por "Fuerza Bruta" de aquellas claves que permiten ingresar a los sistemas, aplicaciones, cuentas, etc. atacados. Muchas passwords de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario y, además, esta nunca (o rara vez) se cambia. En esta caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y "diccionarios" que prueban millones de posibles claves hasta encontrar la password correcta.
  La política de administración de password será discutida en capítulos posteriores.

- **Uso de Diccionarios**

Los Diccionarios son archivos con millones de palabras, las cuales pueden ser posibles passwords de los usuarios. Este archivo es utilizado para descubrir dicha password en pruebas de fuerza bruta.
El programa encargado de probar cada una de las palabras encripta cada una de ellas, mediante el algoritmo utilizado por el sistema atacado, y compara la palabra encriptada contra el archivo de passwords del sistema atacado (previamente obtenido). Si coinciden se ha encontrado la clave de acceso al sistema, mediante el usuario correspondiente a la clave hallada.
Actualmente es posible encontrar diccionarios de gran tamaño orientados, incluso, a un área específico de acuerdo al tipo de organización que se este atacando.
En la tabla 7.4 podemos observar el tiempo de búsqueda de una clave de acuerdo a su longitud y tipo de caracteres utilizados. La velocidad de búsqueda se supone en 100.000 passwords por segundo, aunque este número suele ser mucho mayor dependiendo del programa utilizado.

Cantidad de Caracteres	26–Letras minúsculas	36–Letras y dígitos	52–Mayúsculas y minúsculas	96–Todos los caracteres
6	51 minutos	6 horas	2,3 días	3 meses
7	22,3 horas	9 días	4 meses	24 años
8	24 días	10,5 meses	17 años	2.288 años
9	21 meses	32,6 años	890 años	219.601 años
10	45 años	1.160 años	45.840 años	21.081.705 años

Tabla 7.4 – Cantidad de claves generadas según el número de caracteres empleado

Aquí puede observarse la importancia de la utilización de passwords con al menos 8 caracteres de longitud y combinando todos los caracteres disponibles. En el siguiente Capítulo podrá estudiarse las normas de claves relativamente seguras y resistentes.