



# INICIO GRABACIÓN



**SANJOSÉ**  
FUNDACIÓN DE EDUCACIÓN SUPERIOR



## Escaneo y enumeración con nmap

un auditor informático es visto como un profesional altamente capacitado independiente que evalúa la eficiencia de un sistema con el objetivo principal de detectar fallas que deben ser solucionadas

# DEFINICIÓN DE INGENIERÍA SOCIAL



Los autores de este hecho (criminales, terceros malintencionados, timadores, falsos técnicos, etc.) engañan a sus víctimas para que hagan algo por ellos (enviar correo, hacer clic, comprar algo...) o les den información confidencial o sensible como:

- Sus contraseñas de acceso a equipos informáticos,
- sus credenciales bancarias,
- información relacionada con productos y servicios,
- información y datos de proveedores y clientes, etc.



La obtención de las credenciales (usuario y contraseña) de acceso a nuestros equipos y aplicaciones puede ser utilizada para suplantarlos e instalar secretamente software malicioso. Este software podrá, por ejemplo, darles:

- acceso a otras credenciales (de aplicaciones, cuentas de correo o de acceso a entidades financieras,...)
- el control sobre nuestros equipos y aplicaciones que pondrán a trabajar a su servicio



Las tácticas de ingeniería social son más eficaces y menos costosas, en relación al tiempo y esfuerzo que requieren, que los ataques informáticos complejos necesarios para obtener el mismo resultado.

Es decir, es más fácil convencer a alguien para que te de sus contraseñas que intentar romper la contraseña por medios informáticos (a menos que la contraseña sea muy débil).

Aunque invirtamos en recursos tecnológicos debemos ser conscientes de que es necesario aumentar la formación y concienciación en materia de seguridad de todos los miembros que utilicen y gestionen los sistemas de información en la empresa, para evitar o reducir los incidentes y engaños.

- «Una cadena es tan fuerte como su eslabón más débil»



- «El usuario es el eslabón más importante de la cadena de la seguridad»

# ¿QUÉ VALOR TIENE NUESTRA INFORMACIÓN EN INTERNET?



Los ciberdelincuentes tienen formas de hacer negocio con la información que roban. Utilizan la ingeniería social para engañarnos y robarnos información para venderla o pedirnos un rescate, suplantarnos, realizar acciones ilícitas en nuestro nombre o infectarnos para aprovechar nuestros recursos para su propio interés.

Además del fraude y del robo de información, otras actividades ilegales también tienen su base en la red aunque no sean evidentes. Esto es porque utilizan los bajos fondos de internet, la Darknet, a la que sólo se accede con software específico que permite el anonimato y la confidencialidad.

Es dónde se encuentran los mercados negros de Internet. La Darknet es el sitio ideal para todo tipo de actividades maliciosas y delictivas. También la usan activistas y periodistas de regímenes con limitada libertad de expresión.

La Darknet es una parte de la **Internet profunda o Deep Web**, la que no indexan los buscadores. No debemos confundirlas pues en la *Deep Web* no todo es delictivo también existen blogs, revistas académicas o bases de datos no indexados, es decir que no se accede con los navegadores de uso común.

En la **Darknet** se encuentran todo tipo de **contenidos y actividades ilegales** que van desde la pornografía infantil, la venta de armas, el desarrollo de software malicioso y los mercados de información robada (credenciales bancarias, tarjetas de crédito,...).





# TIPOS DE ATAQUE DE INGENIERÍA SOCIAL




## 1.BASADOS EN COMPONENTE HUMANO

Engañar y conseguir la confianza del usuario para conseguir:

- que revelemos datos confidenciales que compremos productos/servicios fraudulentos (falsos antivirus, adware,...)
- que contribuyan a sus objetivos de distribuir malware, redireccionar tráfico,...
- ingresos directos a través del engaño: fraude pago por clic, suscripción a servicios Premium,...
- secuestrar datos y pedir un rescate

## 2.BASADOS EN SOFTWARE MALICIOSO

Engañar al usuario para que instale en su ordenador software malicioso que:

- extraerá datos confidenciales del usuario
  - le hará pertenecer a una botnet para enviar spam, distribuir malware,...
- 





### Suplantación de la empresa de servicios

- Un atacante se hace pasar por su compañía de internet o su compañía de transportes para pedirle sus datos de conexión, contraseñas, cuentas bancarias, etc.

### Suplantación de un operador autorizado

- Un atacante se hace pasar por un ayudante de un empleado autorizado de uno de sus proveedores, que se encuentra enfermo o de vacaciones, para pedirle sus datos de conexión, contraseñas, etc.

### Suplantación de una Autoridad del Estado

- Un atacante se hace pasar por un agente de la policía, bombero o técnico de hacienda para solicitarle datos como nombres, teléfonos, etc.

### Suplantación de una empresa de encuestas

- Un atacante se hace pasar por una empresa de encuestas, solicitando sus datos para verificar la encuesta.



#### VISHING

a la persona que contesta, se le pide **comunicarse con un número específico** de su entidad bancaria donde una locución le pedirá datos (tarjeta bancaria, credenciales generalmente); o simplemente se le solicita **verificar algunos datos personales llamando a un número telefónico específico.**

#### SMISHING

En este caso, la estafa se realiza mediante **mensajes SMS**, en los **que se solicitan datos, se pide que se llame a un número o se pide que se acceda a una web.**





## VENTANAS POP-UP


Ventanas emergentes que piden instalar software o complementos en el ordenador para que puedan verse videos o programas, pero que realmente esconden software malicioso.

**Lo mejor es bloquear las ventanas emergentes del navegador de internet. A través de las opciones de configuración podemos saber cómo bloquear las ventanas emergentes en los distintos navegadores de Internet.**

## PHISHING

Un correo electrónico o web falsa que se hace pasar por una persona o comunicación oficial electrónica. Al seguir las instrucciones comunicación proporciona acabamos siendo nuestras credenciales de acceso al servicio

### CÓMO DETECTAR UN ATAQUE DE PHISHING

- **Direcciones sospechosas.**
  - **Errores ortográficos.**
  - **Fallos en logos o imágenes copiadas.**
  - **Comprobar la identidad** del remitente o del departamento.
  - Y, sobre todo, **sospechar si nos piden datos confidenciales** sin nosotros hayamos **realizado** ninguna solicitud.
- 





### **WEBS ENGAÑOSAS**

Ofrecen una publicidad engañosa sobre un servicio gratis o un premio de un concurso en el que para solicitar el servicio es necesario registrarse. Muy a menudo utilizamos las mismas contraseñas para registrarnos en varios servicios, por lo que probablemente estemos aportando sin darnos cuenta las credenciales de acceso a nuestro banco o nuestra red social.

### **SPAM CON ADJUNTOS MALICIOSOS**

Son correos electrónicos con publicidad engañosa que también pueden contener archivos adjuntos que instalan software malicioso en nuestros equipos.





## VULNERABILIDADES

El objetivo es poder brindar un mayor conocimiento sobre el análisis de las vulnerabilidades, los tipos, las diferentes formas de escaneos y la detección de las diferentes vulnerabilidades y como poder resolverlas.



# análisis de vulnerabilidades



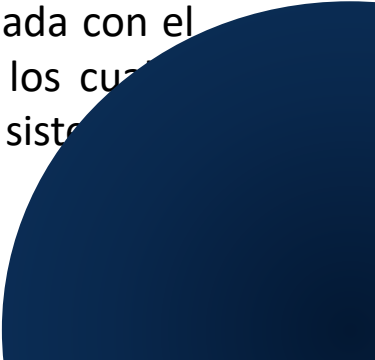
Definiendo a muy grandes rasgos que es una vulnerabilidad, una vulnerabilidad de una manera muy general es un fallo en un sistema que puede ser explotada por un atacante generando un riesgo para la organización o para el mismo sistema.

Existen dos tipos de vulnerabilidades que se mencionan a continuación:

- Las lógicas
- Las físicas

Existen una gran gama de escáner de vulnerabilidades, muchos son de pago otros son gratuitos y se los puede utilizar sin mayor problema para su ejecución, hay escáneres como Acunetix que son muy buenos en la parte web y no sólo permiten escanear, también permiten la explotación real de ciertas vulnerabilidades o incluso la comprobación de estas.

**Escáneres de vulnerabilidades** Muchos de los escáneres web trabajan con proxys y a partir de estos se realiza la captura de las tramas de la información y se puede realizar la modificación. Algunos escáneres utilizan métodos que van a permitir listar el contenido del servidor de acuerdo a los directorios más conocidos, uno de esos escáneres es “Acunetix”, el cual es una herramienta que está diseñada con el objetivo de encontrar agujeros de seguridad en las aplicaciones web, los cuales puedan ser aprovechados por determinados atacantes para acceder a los sistemas y la información.



# Tipos de vulnerabilidades

**Desbordamiento de buffer,** El desbordamiento de buffer ocurre cuando el programador no controla el espacio de memoria del programa, entonces alguna persona puede introducir su propio código en ese espacio de memoria y la máquina lo va a ejecutar antes que cualquier otra tarea, por ejemplo, eso normalmente se da mucho con los payloads, en los cuales se inyectan cierta cantidad de memoria o inclusive dentro de los backdoor o puerta trasera, los cuales inyectan en la memoria RAM un cierto o una cierta cantidad de código, el cual se arranca antes, inclusive de arrancar toda la parte del sistema operativo o de algunos de los archivos dentro del mismo sistema que se utilizan para arrancar de manera normal.



# Tipos de vulnerabilidades

**Errores de configuración**, Otra de las principales vulnerabilidades, son los errores de configuración, se puede mencionar, por ejemplo, los password por default, password débiles, usuarios con demasiados privilegios e inclusive la utilización de protocolos de encriptación obsoletos, normalmente una de las cosas más típicas en las organizaciones es que utilizan algún sistema de encriptación web, lo cual con una aplicación de teléfono celular se puede crackear en menos de 10 o 15 segundos o inclusive con una laptop.

**Errores Web**, Otros tipos de vulnerabilidades son las WEB, aquí simple y sencillamente se tiene errores de validación de input, Scripts inseguros, errores de configuración de aplicaciones web, entre algunas otras situaciones, que a final de cuenta todos y cada uno de esos errores son los medios para algún ataque de XSS (Cross Site Scripting) o inyección SQL.

**Errores de protocolo**, Por último, se tiene la parte de las vulnerabilidades de protocolos, existen diversas cantidades de protocolos que normalmente fueron definidos sin la necesidad o sin tener en cuenta precisamente la parte de la seguridad y en muchas veces no se preveo el crecimiento que estos iban a tener y como el internet no estaba preparado para ser tan grande, no se pensó en la parte de la seguridad.






# Detección de vulnerabilidades



Las vulnerabilidades pueden ser detectadas mediante herramientas de detección, realizar un escaneo de puertos con el objetivo de verificar cuales están abiertos para intentar obtener información sobre el servicio que se encuentre corriendo en ese momento y con esta información buscar vulnerabilidades asociadas precisamente a esos servicios. Se tienen tres formas de detectarse.

1. Escáner de vulnerabilidades.
2. Análisis manuales.
3. Consultando información.

A través del **escáner de vulnerabilidades** se tienen herramientas como Nikto la cual funciona buscando fallos en base a servidores, Nessus, Nmap, etc. Una de las ventajas de la parte del escáner de vulnerabilidades, es que funcionan de manera automática, trabajan ubicando un rango de direcciones IP e inicia el escaneo, la máquina realiza todo el proceso prácticamente sola.







# Métodos de escaneo de vulnerabilidades



## *Caja blanca*

El método de escaneo de caja blanca tiene una visión total de la red a analizar, así como, acceso a todos los equipos como súper usuario, aquí es donde se tiene la parte de toda la administración de los servicios, la parte de análisis de caja blanca actúa como un usuario legítimo dentro de la red, que puede utilizar los servicios de diversas formas a la que otra persona los pueda estar utilizando. De una manera más detallada, este método utilizará ciertos usuarios con ciertos privilegios dentro de la red y accediendo a los servicios, dentro de los productos, dentro de los softwares que se quieren auditar y así poder verificar si se puede realizar alguna acción adicional en base los privilegios que se han brindado.

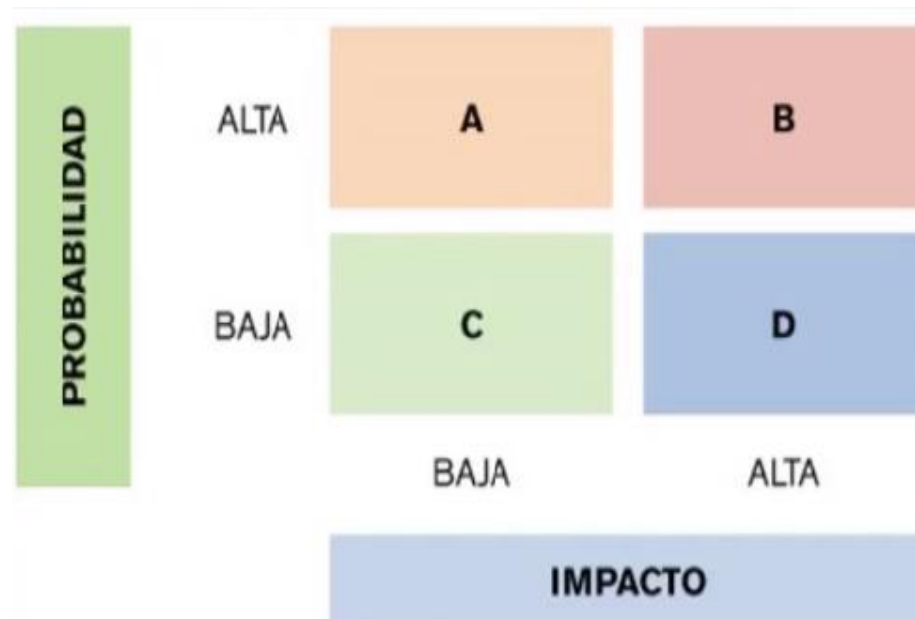
## *Caja negra*

También existe el método de escaneo de caja negra, aquí es donde normalmente se proporciona información de acceso de red, aquí a los analistas les van a proporcionar sólo información de acceso a red o al sistema, por ejemplo, una sola dirección IP, algún nombre de alguna empresa, etc., a partir de aquí empieza como tal a buscar información, todo lo posible relacionado para la exploración y así poder obtener la mayor cantidad de información posible de dicha dirección IP, del resto de los equipos probablemente que se encuentran dentro de algún rango de direcciones IP asociado, aquí no se realiza ninguna instrucción, solamente se detecta y se documenta la vulnerabilidad.

# Clasificar y priorizar riesgos



Es imposible arreglar todas las vulnerabilidades detectadas, es por eso, que es necesario clasificar y sobretodo priorizar el riesgo que está impondría en la organización. No se puede arreglar todas las fallas encontradas porque se tiene poco tiempo, poco personal y sobre todo poco dinero, por esto la organización se debe enfocar en arreglar primero las vulnerabilidades más graves en sistemas críticos, pero para esto se debe diseñar un esquema de prioridad que combine el nivel de severidad de una vulnerabilidad y qué tan importante es el sistema para la empresa.



# Probar parches y configuraciones



Una vez que se ha detectado las vulnerabilidades dentro del sistema, del inventario y se ha clasificado y priorizado los riesgos que pueden incurrir estas vulnerabilidades, el siguiente paso es probar parches y cambios de configuración. El proceso de parcheo puede poner en riesgo el sistema de la organización, ya que el software parcheado puede traer inclusive errores que aún no han sido detectados.

El parcheo se debe instalar principalmente en una sola máquina y hacer pruebas para verificar si se llega a detectar algún problema, con esto poder evitar al haber instalado en todos los sistemas o en todos los dispositivos que ese error se propague. Hay que tomar en cuenta que el software que está haciendo parchado puede venir con configuraciones por default, ya que probablemente se tendría que ajustarlo nuevamente.

Una vez que ya se ha probado los parches y los cambios de configuración, es necesario aplicarlos, cuando se ha comprobado que dichos partes funcionan correctamente, Una vez que ya se ha implementado todas las partes, se ha escaneado, clasificado riesgos, buscado los parches, aplicado dichos parches, la última parte es volver a escanear para verificar el parcheo, esto una vez que ya se haya parchado todos los sistemas o se hayan cambiado sus configuraciones inseguras, se debe escanear toda la red de nuevo para asegurarse que los parches estén adecuadamente instalados y no hayan faltado equipos, inclusive con toda esta situación de que se haya realizado un parcheo o una actualización es necesario volver a escanear para verificar si esos parches quedaron debidamente aplicados o bien generaron nuevas vulnerabilidades.



FUNDACIÓN DE EDUCACIÓN SUPERIOR

**SAN JOSÉ**

INSTITUCIÓN TECNOLÓGICA

FIN DE  
GRABACIÓN