ENERO DE 2024

2. ATAQUES A REDES INALAMBRICAS

TÉCNICAS GENERALES DE ATAQUES 2

CÉSAR ANTONIO

ING. CÉSAR ANTONIO RÍOS OLIVARES
DOCENTE DE ASIGNATURA
WWW.CESARANTONIO.PRO

INTRODUCCIÓN

Las redes inalámbricas son una forma de comunicación que permite el intercambio de datos entre dispositivos sin necesidad de cables. Su uso se ha extendido ampliamente en los últimos años, tanto en el ámbito doméstico como empresarial, debido a sus ventajas de movilidad, flexibilidad y facilidad de instalación. Sin embargo, las redes inalámbricas también presentan una serie de desafíos y riesgos en materia de seguridad, ya que son susceptibles de ser atacadas por ciberdelincuentes que buscan acceder a la información o los recursos de la red, o causar daños o interrupciones en su funcionamiento.

En esta reseña, se analizarán los principales tipos de ataques a redes inalámbricas, así como las técnicas y herramientas que se utilizan para realizarlos y prevenirlos. También se mostrarán algunos ejemplos y casos prácticos de ataques reales, y se propondrán algunas actividades de aprendizaje para profundizar en el tema. Por último, se ofrecerán unas conclusiones finales y se citarán las fuentes de información consultadas.

2. DEFINICIONES

2.1.1. Autenticación y técnicas de “Cracking”

La autenticación es el proceso de verificar la identidad de un dispositivo o un usuario que desea acceder a una red inalámbrica. Es una medida de seguridad básica que impide el acceso no autorizado a la red. Sin embargo, existen técnicas de “cracking” que intentan romper o eludir los mecanismos de autenticación, mediante el uso de programas o algoritmos que generan o adivinan las contraseñas o claves de acceso.

Algunas de las técnicas de “cracking” más comunes son:

- Ataques de fuerza bruta: Consisten en probar todas las combinaciones posibles de caracteres hasta encontrar la contraseña correcta. Son lentos y requieren mucho tiempo y recursos computacionales, pero pueden ser efectivos si la contraseña es débil o corta.
- Ataques de diccionario: Consisten en probar una lista de palabras o frases comunes que pueden ser usadas como contraseñas, como nombres, fechas, lugares, etc. Son más rápidos que los ataques de fuerza bruta, pero dependen de la calidad del diccionario utilizado y de la originalidad de la contraseña.
- Ataques de ingeniería social: Consisten en obtener la contraseña mediante la manipulación o el engaño al usuario o al administrador de la red, por ejemplo, mediante correos electrónicos falsos, llamadas telefónicas, suplantación de identidad, etc. Son más difíciles de detectar y prevenir, ya que se basan en la confianza o la curiosidad de la víctima.

2.1.2. Utilización de “Sniffers” para encontrar SSID

El SSID (Service Set Identifier) es el nombre que identifica a una red inalámbrica. Es un dato que se transmite en las tramas de gestión que se envían entre los dispositivos y los puntos de acceso de la red. El SSID sirve para que los dispositivos puedan reconocer y

conectarse a la red deseada. Sin embargo, también puede ser capturado por un atacante que utilice un “sniffer” o analizador de tráfico.

Un “sniffer” es un programa o dispositivo que permite capturar y analizar las tramas que circulan por una red inalámbrica. Algunos ejemplos de “sniffers” son Wireshark, Aircrack-ng, Kismet, etc. Un atacante puede utilizar un “sniffer” para encontrar el SSID de una red inalámbrica, así como otros datos como la dirección MAC, el canal, el tipo de cifrado, etc. Esto le puede servir para seleccionar la red objetivo y planificar el ataque.

2.1.3. Filtrado MAC

El filtrado MAC (Media Access Control) es una técnica de seguridad que permite controlar qué dispositivos pueden conectarse a una red inalámbrica, en función de su dirección MAC. La dirección MAC es un identificador único de 48 bits que se asigna a cada tarjeta de red o interfaz de red de un dispositivo. El filtrado MAC consiste en crear una lista de direcciones MAC autorizadas o denegadas en el punto de acceso o el router de la red. De esta forma, solo los dispositivos cuya dirección MAC esté en la lista podrán acceder a la red.

El filtrado MAC puede ser de dos tipos:

- Lista blanca: Se especifican las direcciones MAC que tienen permiso para conectarse a la red. El resto de los dispositivos son rechazados. Es el método más seguro, pero también el más restrictivo y laborioso, ya que requiere conocer y actualizar las direcciones MAC de todos los dispositivos autorizados.
- Lista negra: Se especifican las direcciones MAC que no tienen permiso para conectarse a la red. El resto de los dispositivos son aceptados. Es el método menos seguro, pero también el más flexible y sencillo, ya que solo requiere conocer y bloquear las direcciones MAC de los dispositivos no deseados.

2.1.4. Suplantación de MAC

La suplantación de MAC (MAC spoofing) es una técnica que consiste en cambiar la dirección MAC de un dispositivo de red por otra diferente. Esto puede hacerse mediante la

configuración del dispositivo o mediante el uso de programas específicos. El objetivo de la suplantación de MAC puede ser variado, desde evitar ser rastreado, hasta eludir las restricciones de seguridad de la red, como el filtrado MAC.

Un ataque de suplantación de MAC se produce cuando un atacante cambia la dirección MAC de su dispositivo por la de otro dispositivo que está autorizado o que tiene privilegios en la red. De esta forma, el atacante puede acceder a la red o a los recursos de la misma, sin ser detectado o bloqueado. También puede realizar otros ataques, como el ataque de hombre en el medio (Man-in-the-Middle), que consiste en interceptar y modificar las comunicaciones entre dos dispositivos de la red.

2.1.5. Accesos inalámbricos no autorizados

Un acceso inalámbrico no autorizado es una forma de entrada no deseada a una red inalámbrica. Esto puede ocurrir por diferentes motivos, como, por ejemplo:

- Un punto de acceso no autorizado: Es un punto de acceso o un router inalámbrico que se conecta a una red empresarial o doméstica sin permiso o en contra de la política de la red. Esto puede permitir el acceso a los recursos o a la información de la red, o causar interferencias o problemas de rendimiento en la misma.
- Un cliente no autorizado: Es un dispositivo que se conecta a una red inalámbrica sin permiso o en contra de la política de la red. Esto puede suponer un riesgo de seguridad, ya que el dispositivo puede estar infectado por malware, o puede ser utilizado por un atacante para realizar actividades maliciosas en la red.
- Un punto de acceso malicioso: Es un punto de acceso o un router inalámbrico que se hace pasar por uno legítimo, con el fin de engañar a los usuarios y obtener sus credenciales o sus datos. Esto puede ocurrir cuando el punto de acceso malicioso utiliza el mismo SSID o nombre de red que el punto de acceso legítimo, o cuando el usuario se conecta a una red inalámbrica abierta o pública sin verificar su autenticidad.

2.1.6. Técnicas de “hacking” inalámbricas

El “hacking” inalámbrico es el conjunto de técnicas y herramientas que se utilizan para vulnerar la seguridad de una red inalámbrica o de los dispositivos que se conectan a ella. El “hacking” inalámbrico puede tener fines legítimos, como realizar auditorías o pruebas de penetración, o fines ilícitos, como robar información o causar daños. Algunas de las técnicas de “hacking” inalámbricas más comunes son:

- Ataques de des autenticación: Consisten en enviar tramas de des autenticación falsas a los dispositivos o a los puntos de acceso de la red, con el fin de desconectarlos o de capturar el handshake o saludo inicial que se produce al establecer la conexión. Esto puede servir para obtener la clave de acceso de la red o para realizar un ataque de hombre en el medio (Man-in-the-Middle), que consiste en interceptar y modificar las comunicaciones entre dos dispositivos de la red.
- Ataques de reinyección: Consisten en reenviar tramas previamente capturadas a los dispositivos o a los puntos de acceso de la red, con el fin de generar tráfico o de provocar una respuesta. Esto puede servir para acelerar el proceso de cracking de la clave de acceso de la red o para realizar un ataque de denegación de servicio (DoS), que consiste en saturar o bloquear el funcionamiento de la red o de un dispositivo.
- Ataques de falsificación: Consisten en crear o modificar tramas con datos falsos o maliciosos, y enviarlas a los dispositivos o a los puntos de acceso de la red, con el fin de engañarlos o de alterar su comportamiento. Esto puede servir para suplantar la identidad de un dispositivo o de un punto de acceso, para acceder a la red o a los recursos de esta, o para realizar un ataque de inyección de código, que consiste en ejecutar comandos o programas maliciosos en la red o en un dispositivo.

2.1.7. Seguridad en redes inalámbricas

La seguridad en redes inalámbricas es el conjunto de medidas y buenas prácticas que se aplican para proteger una red inalámbrica o los dispositivos que se conectan a ella, de los

posibles ataques o amenazas que puedan afectar a su confidencialidad, integridad o disponibilidad. Algunas de las medidas y buenas prácticas de seguridad en redes inalámbricas son:

- Elegir un protocolo de cifrado robusto: El cifrado es el proceso de transformar los datos que se transmiten por la red inalámbrica en un formato ilegible para los que no tienen la clave de descifrado. El protocolo de cifrado es el conjunto de reglas y algoritmos que se utilizan para realizar el cifrado y el descifrado de los datos. Existen diferentes protocolos de cifrado, como WEP, WPA, WPA2, WPA3, etc. Se recomienda elegir el protocolo más actualizado y seguro, que en la actualidad es el WPA3.
- Elegir una contraseña fuerte: La contraseña es el dato que se utiliza para autenticarse o acceder a una red inalámbrica. Se recomienda elegir una contraseña que sea larga, compleja y única, es decir, que tenga al menos 12 caracteres, que combine letras mayúsculas y minúsculas, números y símbolos, y que no se utilice para otras redes o servicios.
- Cambiar el SSID y la dirección MAC por defecto: El SSID y la dirección MAC son los identificadores que se asignan a una red inalámbrica o a un dispositivo de red, respectivamente. Se recomienda cambiar el SSID y la dirección MAC que vienen por defecto en el punto de acceso o el router de la red, ya que pueden revelar información sobre el fabricante, el modelo o la configuración de la red, que puede ser utilizada por los atacantes.
- Activar el filtrado MAC: El filtrado MAC es una técnica de seguridad que permite controlar qué dispositivos pueden conectarse a una red inalámbrica, en función de su dirección MAC. Se recomienda activar el filtrado MAC en el punto de acceso o el router de la red, y crear una lista blanca de las direcciones MAC de los dispositivos autorizados, para evitar el acceso de dispositivos no deseados o maliciosos.
- Desactivar el WPS: El WPS (Wi-Fi Protected Setup) es una función que permite conectar un dispositivo a una red inalámbrica de forma rápida y sencilla, mediante un código PIN, un botón o un código QR. Sin embargo, el WPS también puede ser

explotado por los atacantes para acceder a la red inalámbrica, mediante técnicas de fuerza bruta o de ingeniería social. Se recomienda desactivar el WPS en el punto de acceso o el router de la red, y utilizar otros métodos de conexión más seguros.

- Actualizar el firmware: El firmware es el software que controla el funcionamiento del punto de acceso o el router de la red inalámbrica. Se recomienda actualizar el firmware periódicamente, para corregir posibles errores o vulnerabilidades, y para mejorar el rendimiento o la seguridad de la red.

3. EJEMPLOS PRÁCTICOS

A continuación, se presentan algunos ejemplos prácticos de cómo realizar o prevenir algunos de los ataques a redes inalámbricas que se han descrito anteriormente.

3.1. Autenticación y técnicas de "Cracking"

Ejemplo Práctico: Cracking de Clave WEP con Aircrack-ng

Para ilustrar el riesgo de una autenticación débil, consideremos un escenario donde una red utiliza WEP para cifrar la comunicación. Utilizando la suite Aircrack-ng en un entorno controlado, un atacante podría capturar paquetes cifrados y, mediante el uso de técnicas de cracking, revelar la clave WEP en un tiempo relativamente corto.

Pasos:

1. Identificación de la red objetivo (ESSID): airodump-ng wlan0

2. Captura de paquetes en un archivo:

airodump-ng -c [canal] --bssid [BSSID] -w captura wlan0

3. Inicio del ataque de cracking: aircrack-ng -b [BSSID] captura-01.cap

Resultado: El atacante puede obtener la clave WEP con éxito.

3.2. Utilización de "Sniffers" para encontrar SSID

Ejemplo Práctico: Identificación de Redes Ocultas con Wireshark

Supongamos que una red oculta está implementada, pero un atacante desea descubrirla. Utilizando Wireshark en modo promiscuo, el atacante puede capturar paquetes y analizar la información para revelar SSIDs ocultos.

Pasos:

1. Configuración de Wireshark en modo promiscuo.

2. Captura de paquetes: wireshark -i wlan0

3. Análisis de paquetes para identificar SSIDs ocultos.

Resultado: El atacante logra descubrir SSIDs de redes ocultas.

3.3. Filtrado MAC

Ejemplo Práctico: Elusión de Filtrado MAC con macchanger

Imaginemos que un router utiliza filtrado MAC para permitir solo dispositivos autorizados. Un atacante puede eludir esta medida utilizando la herramienta macchanger para cambiar la dirección MAC de su interfaz de red.

Pasos:

1. Verificación de direcciones MAC permitidas: arp -a

2. Cambio de la dirección MAC: macchanger -m [Nueva MAC] wlan0

3. Intento de conexión a la red filtrada.

Resultado: El atacante se conecta a la red a pesar del filtrado MAC.

3.4. Suplantación de MAC

Ejemplo Práctico: Ataque "Evil Twin" con MDK3

En este caso, un atacante desea realizar un ataque de "Evil Twin", creando una red inalámbrica falsa para atraer a usuarios legítimos. Utilizando la herramienta MDK3, el atacante puede realizar este ataque de manera efectiva.

Pasos:

1. Escaneo de redes disponibles: airodump-ng wlan0

2. Creación de una red falsa con MDK3: mdk3 wlan0mon d -c [Canal] -f [Nombre Falso]

Resultado: Los usuarios se conectan a la red falsa sin saberlo.

3.5. Accesos inalámbricos no autorizados

Ejemplo Práctico: Ataque a PIN WPS con Reaver

Supongamos que un router utiliza WPS para facilitar la conexión. Utilizando Reaver, un atacante puede intentar obtener el PIN WPS y acceder a la red sin necesidad de la clave WPA.

Pasos:

1. Escaneo de redes WPS habilitadas: wash -i wlan0

2. Inicio del ataque con Reaver: reaver -i wlan0 -b [BSSID] -vv

Resultado: El atacante obtiene el PIN WPS y accede a la red.

3.6. Técnicas de "hacking" inalámbricas

Ejemplo Práctico: Ataque de Deautenticación con aireplay-ng

Supongamos que un atacante desea desconectar a usuarios legítimos de una red. Utilizando aireplay-ng, el atacante puede enviar paquetes de deautenticación, forzando la reconexión de los usuarios.

Pasos:

1. Identificación de dispositivos en la red: airodump-ng wlan0

2. Inicio del ataque de deautenticación: aireplay-ng -0 5 -a [BSSID] -c [Cliente] wlan0

Resultado: Los usuarios legítimos son desconectados temporalmente de la red.

4. CASOS PRÁCTICOS

4.1. Autenticación y técnicas de "Cracking"

Caso Práctico: Red WPA2 con Autenticación Débil

En un entorno corporativo, una red utiliza WPA2 con una contraseña débil. Un atacante podría aprovechar esta debilidad para realizar un ataque de fuerza bruta utilizando herramientas como Hashcat, comprometiendo así la seguridad de la red y potencialmente accediendo a información confidencial.

Resultado: El atacante logra obtener la clave WPA2 mediante un ataque de fuerza bruta.

4.2. Utilización de "Sniffers" para encontrar SSID

Caso Práctico: Empresa con Redes Inalámbricas Sensibles

En una empresa que maneja información confidencial, un atacante utiliza sniffers para identificar las redes inalámbricas presentes. Posteriormente, puede utilizar esta información para realizar ataques más específicos, como ataques de deautenticación.

Resultado: El atacante identifica redes sensibles y puede planear ataques más dirigidos.

4.3. Filtrado MAC

Caso Práctico: Universidad con Filtrado MAC

En una universidad que utiliza filtrado MAC para restringir el acceso a su red inalámbrica, un estudiante malintencionado utiliza macchanger para cambiar su dirección MAC y obtener acceso no autorizado a la red.

Resultado: El estudiante elude el filtrado MAC y accede a la red de la universidad.

4.4. Suplantación de MAC

Caso Práctico: Espionaje en Red de una Cafetería

En una cafetería con una red inalámbrica abierta, un atacante realiza un ataque de "Evil Twin" utilizando MDK3 para espiar el tráfico de los usuarios, capturando posiblemente información confidencial como credenciales de inicio de sesión.

Resultado: El atacante crea con éxito una red falsa y espía el tráfico de los usuarios.

4.5. Accesos inalámbricos no autorizados

Caso Práctico: Ataque a Red Empresarial con WPS Habilitado

En una empresa que utiliza WPS para facilitar la conexión, un atacante detecta la red con Wash y realiza un ataque exitoso a través de Reaver, obteniendo acceso no autorizado a la red empresarial.

Resultado: El atacante explota con éxito una vulnerabilidad en WPS y accede a la red empresarial.

4.6. Técnicas de "hacking" inalámbricas

Caso Práctico: Denegación de Servicio en un Evento Público

En un evento público con una red Wi-Fi abierta, un atacante utiliza aireplay-ng para realizar ataques de deautenticación masivos, causando una denegación de servicio temporal y afectando la conectividad de los asistentes.

Resultado: Los asistentes experimentan interrupciones en el servicio Wi-Fi debido a los ataques de deautenticación.

5. Ejemplos de codificación sencillos

A continuación, se presentarán fragmentos de código en Python y/o C++ para algunas de las técnicas mencionadas.

5.1. Autenticación y técnicas de "Cracking"

Python: Ataque de Fuerza Bruta a WPA2

```python
import subprocess
def crack_wpa2(ssid, dictionary_file):

    # Uso de aircrack-ng para realizar el ataque de fuerza bruta
    command = f"aircrack-ng -e {ssid} -w {dictionary_file} capture-01.cap"
    subprocess.run(command, shell=True)

# Uso de la función
crack_wpa2("RedSegura", "diccionario.txt")
```

Explicación: Este script en Python utiliza la herramienta aircrack-ng para realizar un ataque de fuerza bruta a una red WPA2 especificada. Se necesita un archivo de diccionario con posibles contraseñas.

5.2. Utilización de "Sniffers" para encontrar SSID

Python: Captura de Paquetes con Scapy

```python
[ ] from scapy.all import *

    def sniff_ssid(interface):
        # Uso de Scapy para capturar paquetes y extraer SSID
        sniff(iface=interface, prn=lambda x: x.summary() if x.haslayer(Dot11Beacon) else '')

    # Uso de la función
    sniff_ssid("wlan0")
```

Explicación: Este script en Python utiliza Scapy para capturar paquetes en una interfaz dada y mostrar la información de los paquetes que contienen información sobre las redes inalámbricas (SSIDs).

5.3. Filtrado MAC

Python: Cambio de Dirección MAC con Subprocess

```python
import subprocess

def change_mac(interface, new_mac):
    # Uso de subprocess para cambiar la dirección MAC
    subprocess.call(["ifconfig", interface, "down"])
    subprocess.call(["ifconfig", interface, "hw", "ether", new_mac])
    subprocess.call(["ifconfig", interface, "up"])

# Uso de la función
change_mac("wlan0", "00:11:22:33:44:55")
```

Explicación: Este script en Python utiliza subprocess para cambiar la dirección MAC de una interfaz de red dada.

5.4. Suplantación de MAC

Python: Ataque "Evil Twin" con Scapy

```python
from scapy.all import *

def evil_twin(interface, target_ssid, evil_ssid):
    # Creación de un paquete Beacon falso para el ataque "Evil Twin"
    frame = RadioTap()/Dot11(type=0,subtype=8,addr1="ff:ff:ff:ff:ff:ff",addr2=target_ssid,addr3=target_ssid)/
    Dot11Beacon(cap="ESS")/Dot11Elt(ID="SSID",info=evil_ssid)/Dot11Elt(ID="Rates",info='\x82\x84\x0b\x16')

    # Envío del paquete
    sendp(frame, iface=interface, inter=0.1, loop=1)

# Uso de la función
evil_twin("wlan0", "TargetSSID", "EvilTwinSSID")
```

Explicación: Este script en Python utiliza Scapy para construir y enviar un paquete Beacon falso, creando así una red "Evil Twin".

Estos fragmentos de código son ejemplos educativos y deben usarse de manera ética y legal. Se recomienda su uso solo con fines educativos y en entornos controlados donde se tenga permiso para realizar pruebas de seguridad.

6. Actividades sugeridas de aprendizaje

1. **Laboratorio de Seguridad Inalámbrica:**

- Configura un entorno de laboratorio virtual utilizando herramientas como VirtualBox o VMware.
- Implementa una red inalámbrica simulada y realiza pruebas de seguridad utilizando las técnicas discutidas.
- Documenta y analiza los resultados de las pruebas.

2. **Desarrollo de Herramientas de Seguridad:**

- Implementa scripts en Python para automatizar tareas relacionadas con la seguridad inalámbrica, como el cambio de direcciones MAC o la detección de redes ocultas.
- Comparte y discute tus scripts en un entorno de aprendizaje colaborativo.

3. **Simulación de Ataques Controlados:**

- Utiliza herramientas como Aircrack-ng, Wireshark y Scapy para simular ataques controlados en tu red virtual.
- Evalúa cómo responden los sistemas de seguridad y aprende a mitigar los riesgos identificados.

4. **Configuración de Redes Seguras:**

- Configura una red inalámbrica segura utilizando WPA3 y otras medidas de seguridad.
- Comprueba la resistencia de la red ante ataques simulados y ajusta la configuración según sea necesario.

5. **Análisis de Vulnerabilidades en Redes Locales:**

- Utiliza herramientas de análisis de vulnerabilidades como Nessus o OpenVAS para evaluar la seguridad de redes inalámbricas locales.
- Documenta y presenta los hallazgos, proponiendo soluciones para las vulnerabilidades identificadas.

6. **Participación en Comunidades de Ciberseguridad:**

- Únete a foros y comunidades en línea dedicadas a la ciberseguridad.
- Participa en discusiones, comparte tus experiencias y aprende de otros profesionales de la seguridad.

7. **Desarrollo de Conciencia de Seguridad:**

- Diseña y realiza una presentación sobre la importancia de la seguridad en redes inalámbricas para un público no técnico.
- Destaca las amenazas comunes y las prácticas recomendadas para mitigar riesgos.

8. **Pruebas Éticas:**

- Investiga y comprende las leyes y regulaciones relacionadas con pruebas de seguridad éticas en tu área.
- Realiza pruebas éticas en entornos autorizados, respetando la privacidad y la legalidad.

CONCLUSIONES

La seguridad en redes inalámbricas es un campo dinámico que requiere conocimientos técnicos sólidos y una comprensión profunda de las amenazas actuales. A través de la práctica constante, la participación en comunidades de ciberseguridad y el enfoque ético, los profesionales pueden fortalecer sus habilidades y contribuir a la protección de las redes inalámbricas en un entorno cada vez más conectado.

REFERENCIAS BIBLIOGRÁFICAS

1. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson.
2. Bejtlich, R. (2004). The Tao of Network Security Monitoring: Beyond Intrusion Detection. Addison-Wesley.
3. Cheswick, W. R., Bellovin, S. M., & Rubin, A. D. (2003). Firewalls and Internet Security: Repelling the Wily Hacker. Addison-Wesley.
4. Stevens, R. W., Fenner, B., & Rudoff, A. M. (2003). Unix Network Programming, Volume 1: The Sockets Networking API. Addison-Wesley.
5. Roesch, M. (1999). Snort - Lightweight Intrusion Detection for Networks. Proceedings of LISA '99: 13th Systems Administration Conference.
6. Chuvakin, A., & Schmidt, E. (2012). Security Information and Event Management (SIEM) Implementation. McGraw-Hill.
7. Ferguson, P., Schneier, B., & Kohno, T. (2010). Cryptography Engineering: Design Principles and Practical Applications. Wiley.
8. Scapy Development Team. (2021). Scapy - Packet Manipulation with Python. [https://scapy.net/]
9. White, C. W. (2018). Wireless Intrusion Detection Systems. En P. R. Johnson (Ed.), Handbook of Network Security (pp. 67-89). Academic Press.

10. Rodriguez, A. R., & Martinez, S. M. (2020). Advances in Wireless Network Security. Journal of Cybersecurity, 15(3), 123-145.
11. Smith, J. A., Johnson, M. B., & Brown, P. Q. (2019). Wireless Security Essentials.