Ataque y defensa en entorno de pruebas, de las comunicaciones inalámbricas (Hacking ético)

Comunicación inalámbrica

Las comunicaciones inalámbricas se implantan tanto en la empresa como en la industria por varios motivos, aunque principalmente las razones son la sencillez del despliegue y la reducción de costes. Estos factores hacen que su uso sea cada vez más extendido y que aparezcan modernos protocolos inalámbricos que ofrecen las mismas funcionalidades que las comunicaciones cableadas o incluso superiores. (Información obtenida en Incibe).

Los sistemas de control industrial demandan ciertas características de seguridad y robustez tanto físicas como lógicas que las comunicaciones inalámbricas deben satisfacer para contemplar su uso. Las principales son:

- Comunicación fiable y robusta.
- Funciones avanzadas de seguridad.
- Configuración y funcionamiento similares a las herramientas de automatización de uso común.
- Comportamiento en tiempo real y determinista.
- Gran rango de temperatura.
- Convivencia con las tecnologías inalámbricas existentes (sin interferencias).
- Bajo consumo de energía, para ciertas áreas de aplicación.

Modo infraestructura, ad-hoc y monitor

Modo infraestructura

El modo Infraestructura es una estructura de red inalámbrica que tiene un enrutador/punto de acceso WLAN en el corazón de la red. En el modo Infraestructura, los dispositivos inalámbricos se comunican el uno con el otro a través de un enrutador/punto de acceso WLAN. Cuando la máquina inalámbrica Brother hace parte de una red en modo infraestructura, recibe todos los trabajos de impresión a través del enrutador/punto de acceso WLAN.

El enrutador/punto de acceso WLAN tambien puede actuar como un puente o portal a una red cableada y los dispositivos inalámbricos podrán comunicarse entre ellos y con la red cableada.

Ad-hoc

El modo Ad-hoc también se conoce como modo «igual a igual». Las redes Ad-hoc no requieren un punto de acceso centralizado. Si se configuran dos ordenadores en modo inalámbrico ad-hoc, se conectarían directamente entre sí sin necesidad de un punto de acceso centralizado.

Más información

- https://www.jesusninoc.com/06/11/creating-a-wireless-backdoor/

Monitor

El modo monitor o modo RFMON permite a un ordenador con una interfaz de red inalámbrica ver el tráfico recibido en un canal o varios canales inalámbricos. A diferencia con el modo promiscuo (que a veces se mezclan) el modo monitor captura paquetes sin estar asociados a un punto de acceso o a una red Ad-hoc.

Análisis y recolección de datos en redes inalámbricas

Una de las herramientas más conocidas para hacer análisis y recolección de datos en redes inalámbricas es Airodump-ng se usa para capturar paquetes wireless 802.11 y es útil para ir acumulando vectores de inicialización IVs con el fin de intentar usarlos con aircrack-ng y obtener la clave WEP. Si tienes un receptor GPS conectado al ordenador, airodump-ng es capaz de mostrar las coordenadas de los puntos de acceso que vaya encontrando.

Ejemplos

- https://www.jesusninoc.com/05/04/redes-inalambricas-visibles/
- https://www.jesusninoc.com/01/18/intensidad-de-las-senales-de-las-conexiones-inalambricas-que-estan-accesibles/
- https://www.jesusninoc.com/04/28/ver-el-porcentaje-de-la-intensidad-de-las-conexiones-inalambricas-en-windows-con-powershell-utilizando-netsh/
- https://www.jesusninoc.com/01/19/mostrar-el-estandar-de-radio-de-las-conexiones-inalambricas/
- https://www.jesusninoc.com/03/13/ver-la-tabla-de-direcciones-arp-asociadas-a-un-router-de-fibra-optica-mitrastar-de-movistar-con-powershell/

Más información

- https://www.jesusninoc.com/10/14/ejecutar-airodump-ng-en-linux-realizando-una-conexion-ssh-desde-powershell-en-windows/

Técnicas de ataques y exploración de redes inalámbricas

Algunos ataques contra el cifrado WEB y WPA.

- Ataques al cifrado WEP (Aircrack-ng).
- Ataque 1+3 (Falsa asociación e inyección de tráfico).
- Ataque Chop Chop.
- Ataque fragmentación.
- Hirte Attack.
- Caffe Late Attack

Cifrado WPA y WPA2

- Obteniendo el handshake.
- Obteniendo la contraseña: Aircrack-ng.
- Obteniendo la contraseña: coWPAtty.
- Obteniendo la contraseña: Pyrit.
- Obteniendo la contraseña: Rainbow Table.
- Obteniendo la contraseña: Por Diccionario.

Más información

- https://www.jesusninoc.com/10/16/enviar-paquetes-de-desasociacion-con-aireplay-ng-a-un-cliente-que-actualmente-esta-asociado-con-un-punto-de-acceso-en-linux-

realizando-una-conexion-ssh-desde-powershell-en-windows/

Ataques a otros sistemas inalámbricos

Ataques típicos a sistemas inalámbricos:

- Escuchas en la red.
- Reenvío de paquetes.
- Suplantación.

Listado de los principales sistemas inalámbricos (Información obtenida en Incibe):

- Trusted Wireless: Trusted Wireless es una tecnología desarrollada específicamente para ser usada en sistemas de control industrial.
- Bluetooth: Bluetooth es una tecnología que comenzó a desarrollarse en el año 1994 por Ericsson como sustituto del cable. Para su comunicación utiliza la FHSS.
- Zigbee: ZigBee es una tecnología desarrollada por la ZigBee Alliance7 que adopta el estándar IEEE 802.15.4 para las capas bajas del modelo OSI, es decir, la capa física (PHY) y la subcapa de acceso al medio (MAC); y agrega la capa de red y de aplicación.
- WirelessHART: WirelessHART se basa, al igual que ZigBee, en el estándar IEEE 802.15.4 y se utiliza para la conexión inalámbrica de dispositivos de campo HART en la industria.
- WiMax: la tecnología inalámbrica WiMAX (Worldwide Interoperability for Microwave Access) se encuentra dentro de las llamadas tecnologías de última milla que permite la recepción de datos por microondas y retransmitirlos por ondas de radio.
- Redes móviles: los teléfonos móviles, teléfonos

inteligentes y tabletas se están haciendo cada día más imprescindibles. Su uso dentro de los sistemas de control también se ha incrementado para facilitar algunas tareas. Pero las comunicaciones móviles son solo se utilizan con estos dispositivos, comunicaciones punto a punto también son posibles con esta tecnología.

- Radiocomunicaciones: las tecnologías de radioenlace se utilizan para comunicaciones a largas distancias. Entre los radioenlaces más comunes están las comunicaciones vía satélite, las microondas y los radioenlaces terrestres.
- RFID: Radio-Frequency IDentification (RFID) es una tecnología de identificación y captura de datos automáticos (Automatic Identification and Data Capture, AIDC), que se basa en campos eléctricos o magnéticos de frecuencia de radio para transmitir información.
- ISA 100.11a o ISA100 Wireless: ISA100 Wireless es un estándar internacional (IEC 62734) que define un método de comunicación inalámbrica bajo IPv6 para el internet de las cosas industrial (Industrial Internet of Things, IIoT). Adopta el estándar IEEE 802.15.4 para las capas bajas del modelo OSI, es decir, la capa física (PHY) y la subcapa de acceso al medio (MAC) y agrega la capa superior de enlace y la de aplicación.

Realización de informes de auditoría y presentación de resultados

Una vez realizados los ataques hay que documentar y presentar un informe de los resultados obtenidos.