modbus

Modbus

Configuración

Esclavo

Máquina virtualbox ejecutando ubuntu 192.168.2.100. Descargamos el esclavo http://www.modbusdriver.com/downloads/diagslave.2.12.zip . descomprimimos y le damos permisos de ejecución Lanzamos con sudo para poder abrir puertos por debajo del 1024 en ubuntu sudo ./diagslave

Maestro

Máquina maestro con ubuntu 192.168.2.200 . Descargamos el maestro http://www.focus-sw.com/assets/files/products/fieldtalk/modpoll/modpoll.3.4.zip Descomprimimos y le damos permisos de ejecución Lanzamos con sudo para poder abrir puerto por debajo del 1024 sudo ./modpoll -m tcp 192.168.2.100 Arrancamos también el wireshark y ponemos el filtro modbus

Características del protocolo Modbus

- Cada dispositivo de la red Modbus debe tener una dirección única.
- Cualquier dispositivo puede enviar órdenes Modbus, aunque lo habitual es permitirlo sólo a un dispositivo maestro.
- Cada comando Modbus contiene la dirección del dispositivo destinatario de la orden.
- Todos los dispositivos reciben la trama pero sólo el destinatario la ejecuta (salvo un modo especial denominado “Broadcast”).
- Cada uno de los mensajes incluye información redundante que asegura su integridad en la recepción.
- Según el estándar Modbus y dada su implementación, en una red Modbus habrá un Master y hasta un máximo de 247 dispositivos Slaves. Esta limitación está determinada por el simple hecho que en una trama Modbus la dirección del esclavo se representa con un solo Byte
- No soporta File Transfer.

Funcionamiento

Las comunicaciones MODBUS se pueden realizar en modo ASCII o en modo RTU. En modo ASCII los bytes se envían codificados en ASCII, es decir, que por cada byte a transmitir se envian dos caracteres ASCII (2 bytes) con su representación hexadecimal. En modo RTU se envían en binario, tal cual. En el modo ASCII las tramas comienzan por 3AH (carácter ':'), y terminan en 0DH-0AH (CR LF Carrier Return Line Feed) y cada byte se envía como dos caracteres ASCII. En modo RTU no se utiliza indicador de inicio y final de trama.

Como se puede ver en las capturas, la secuencia básica en las comunicaciones MODBUS consiste

siempre en una trama de pregunta, seguida de su correspondiente trama de respuesta

Vulnerabilidades

- No posee indicadores de hora y día en su trama.
- No incluye mecanismos de autentificación entre el maestro y los clientes
- Lee los valores de los rangos de entradas o salidas por la emisión de una única solicitud.
- Todos los datos son tratados como valor actual, por tanto, sin un dato no es leído, se pierde.
- Las operaciones de control que soporta son a través de la lectura/escritura de los Data Types
- Posibilidad de hacer fingerprinting a través de su puerto estándar TCP 502. Mediante la función 43 del protocolo puede averiguarse el registro de identificación de PLCs y conseguir información como: tipo de dispositivo, fabricante, versión y otras informaciones útiles para posteriores ataques.

Además de lo anterior hay documentadas varias vulnerabilidades
http://tools.cisco.com/security/center/viewAlert.x?alertId=23280

- An unauthenticated, remote attacker could exploit this vulnerability by sending crafted function codes to carry out reconnaissance on the targeted network.
- An unauthenticated, remote attacker could exploit this vulnerability by sending queries that contain invalid addresses to the targeted network and gathering information about network hosts from returned messages.
- The protocol specification does not include an authentication mechanism for validating communication between MODBUS master and slave devices. This flaw could allow an unauthenticated, remote attacker to issue arbitrary commands to any slave device via a MODBUS master.

Referencias

- http://es.wikipedia.org/wiki/Modbus
- http://www.tolaemon.com/docs/modbus.htm
- http://iaci.unq.edu.ar/materias/laboratorio2/transparencias%5Cmodbus.pdf
- http://vtroger.blogspot.com.es/2010/08/seguridad-scada-fingerprinting-de.html
- http://modbusfw.sourceforge.net/