

Demostraciones prácticas de nuevos ataques de nivel dos

David Barroso Berrueta

Alfredo Andrés Omella

tomac@wasahero.org

slay@wasahero.org

<http://yersinia.sourceforge.net>

Resumen

El nivel dos del modelo OSI es uno de los puntos más críticos al implantar la seguridad de red en una organización. También es uno de los puntos comúnmente ignorados deb ido principalmente a la falta de implementaciones públicas de ataques en dicho nivel. Sin embargo, un ataque con éxito en nivel dos puede llegar a ser al menos tan peligroso como otro en cualquiera de las capas superiores.

1. Introducción

El nivel de Enlace es, a la vez, uno de los menos fortificados y uno de los más olvidados elementos de red. Es muy común que los administradores conecten los switches, los configuren y no vuelvan a preocuparse de ellos. En el transcurso de un Pen-testing habitualmente se descubren switches con una versión de IOS vulnerable o que no han sido fortificados de ninguna manera. Por otro lado, existe un pensamiento común respecto a que implementando VLAN en una red puedes mantener a raya a los atacantes. Sin embargo una arquitectura de red que descansa sobre VLANs puede ser igualmente superada y, por lo tanto, todos los ataques utilizados en niveles OSI superiores, como por ejemplo acceder a contraseñas en el tráfico de red o realizar Man-in-the-Middle, son posibles entre VLANs.

Lo bueno del nivel dos es el hecho de que los paquetes del nivel de Enlace no pueden viajar entre redes IP, como por ejemplo Internet. Por lo tanto, todos los ataques se encuentran limitados a redes internas. De nuevo las estadísticas muestran que los ataques realizados desde dentro de la organización pueden ser tan peligrosos como los ataques provenientes desde fuera.

También debe recordarse que si un intruso externo atraviesa nuestro cortafuegos y llega a la DMZ, sus ataques pueden permitirle escapar de dicha DMZ y centrarse en toda nuestra red. Veamos cómo son las vulnerabilidades más comunes en el nivel de Enlace, cómo pueden ser utilizadas por un atacante y qué podemos hacer para proteger

nuestros sistemas. Todos los ejemplos se han realizado con equipos Cisco, pero algunos pueden ser extrapolables a otros fabricantes.

La mayoría de las conclusiones y datos han sido obtenidos por los autores a través de la investigación y desarrollo de la herramienta Yersinia. En ocasiones ha sido imposible encontrar referencias o código disponible públicamente por lo que ciertas conclusiones están basadas en análisis de comportamientos y no en estándares publicados.

1.1. Estado del arte

Existen numerosas presentaciones en Internet comentando diversos ataques sobre los protocolos de nivel dos, siendo todos ellos ataques teóricos, como puede ser la excelente presentación de Sean Convery [1]; pero no existe ninguna implementación de algún ataque de nivel dos (exceptuando el ataque de CDP flood del grupo Phenoelit [2]). Es por ello que decidimos realizar la herramienta Yersinia [3].

2. La herramienta Yersinia

Con el fin de efectuar los mencionados ataques del nivel de Enlace, utilizaremos una herramienta llamada Yersinia [3]. Yersinia es portable escrita en C (usando libpcap y libnet) y multihilo (soporta múltiples usuarios y múltiples ataques concurrentes). Puede utilizarse para analizar, editar y observar paquetes de red e incluso guardar el tráfico en formato pcap. La última versión de Yersinia (0.5.5.1) soporta los siguientes protocolos:

- Spanning Tree Protocol (STP)
- Cisco Discovery Protocol (CDP)
- Dynamic Trunking Protocol (DTP)
- Dynamic Host Configuration Protocol (DHCP)
- Hot Standby Router Protocol (HSRP)
- IEEE 802.1Q

- Inter-Switch Link Protocol (ISL)
- VLAN Trunking Protocol (VTP)

Yersinia funciona en cualquiera de los siguientes tres modos:

- *línea de comandos*: puede usarse para efectuar ataques a medida este modo se implementó para ayudar a los pen-testers a utilizar Yersinia en sus scripts
- *demonio de red*: permite utilizar Yersinia en remoto el CLI is muy similar al usado por Cisco
- *GUI*: escrito en ncurses.

2.1. Ataques implementados

Los ataques que están implementados en la herramienta son los siguientes, de los cuales los más importantes serían presentados durante la conferencia.

- Spanning Tree Protocol
 1. Sending RAW Configuration BPDU
 2. Sending RAW TCN BPDU
 3. DoS sending RAW Configuration BPDU
 4. DoS sending RAW TCN BPDU
 5. Claiming Root Role
 6. Claiming Other Role
 7. Claiming Root Role dual home (MITM)
- Cisco Discovery Protocol
 1. Sending RAW CDP packet
 2. DoS flooding CDP neighbors table
 3. Setting up a virtual device
- Dynamic Host Configuration Protocol
 1. Sending RAW DHCP packet
 2. DoS sending DISCOVER packet (exhausting ip pool)
 3. Setting up rogue DHCP server
 4. DoS sending RELEASE packet (releasing assigned ip)
- Hot Standby Router Protocol
 1. Sending RAW HSRP packet
 2. Becoming active router
 3. Becoming active router (MITM)
- Dynamic Trunking Protocol

1. Sending RAW DTP packet
2. Enabling trunking

- 802.1Q
 1. Sending RAW 802.1Q packet
 2. Sending double encapsulated 802.1Q packet
 3. Sending 802.1Q ARP Poisoning
- VLAN Trunking Protocol
 1. Sending RAW VTP packet
 2. Deleting ALL VLANs
 3. Deleting selected VLAN
 4. Adding one VLAN

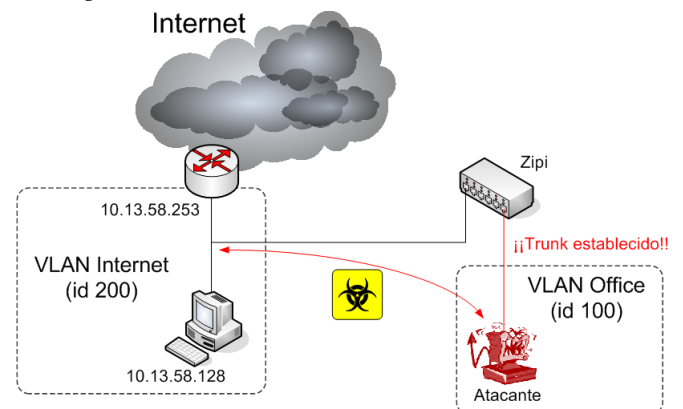
3. Realización de la presentación

Durante el transcurso de la presentación se hará especial hincapié en el ataque más espectacular, que es una mezcla de VLAN Hopping con ARP Spoofing, con el objetivo de realizar ataques Man in the Middle contra máquinas de otras VLAN que no sean la nuestra, permitiendo, de esta forma, tanto poder capturar tráfico generado en otra VLAN como realizar ataques más complejos.

Más aún, se presentará un zero-day presente en los Cisco Catalyst que causa que los switches se reinicien (Denegación de Servicio). Este zero-day será demostrado en directo, aunque no se podrá dar detalles del mismo hasta que Cisco PSIRT anuncie la vulnerabilidad (que se espera que sea en estas semanas).

La presentación es una mezcla teórico-práctica de las vulnerabilidades presentes en estos protocolos, por lo que para este efecto llevaríamos un switch Cisco y tres portátiles.

Con el objetivo de que la presentación sea lo más completa posible, es necesario la utilización de dos proyectores; en el primero de ellos se mostraría la consola del atacante, mientras que en el segundo de ellos se mostraría la consola de los dispositivos atacados.



References

- [1] Sean Convery, *Presentación sobre ataques de nivel dos*, <http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switch%es.pdf>.
- [2] Phenoelit, *Advisory de phenoelit sobre la vulnerabilidad en ios cdp*, <http://www.phenoelit.de/stuff/CiscoCDP.txt>.
- [3] Alfredo Andrés y David Barroso, *Yersinia*, <http://yersinia.sf.net>.