ATAQUES A IPv6: THC-IPv6

1. Introducción

En la actualidad existen pocas herramientas para realizar ataques específicos al protocolo IPv6. THC (acrónimo de *'The Hacker's Choice)* es un grupo de expertos internacionales en seguridad de redes y sistemas que destaca dentro de este campo al crear el primer paquete de herramientas específicamente diseñadas para ataques a este protocolo: Thc-IPv6.

Dentro de este paquete, además de una librería (en C) para la creación de paquetes que permite programar fácilmente nuestros propios exploits en apenas 5-10 líneas, se incluye un conjunto de potentes exploits para sistemas Linux pensados para atacar las debilidades inherentes a IPv6 e ICMP6. En las siguientes líneas se analizará una pequeña selección de estas herramientas, exponiendo sus características y mostrando además algunos de los ataques básicos que se podrían realizar con ellas.

Comenzaremos con una breve introducción a IPv6, mostrando las principales semejanzas/diferencias con el (por el momento) mayoritariamente extendido IPv4. De esta manera podremos comprender mejor que nos aporta Thc-IPv6 y que novedades debemos tener en cuenta para su utilización efectiva y así saber cómo atacar (y defendernos) mejor.

2. Resumen de IPv6

El protocolo IPv6 es una nueva versión de IP (*Internet Protocol*) diseñada para reemplazar a IPv4. Se encuentra definida en el RFC 2460. A continuación se exponen las características de IPv6 más interesantes y esenciales para la comprensión de los siguientes apartados:

- El primer dato salientable es que ipv6 permite un número de posibles direcciones IP muy superior a IPv4 (2^{128} del primero frente a 2^{32} del segundo). La restricción que IPv4 impone sobre el crecimiento de internet es la principal razón que Ipv6 esté destinado a sustituirlo.

- El tamaño de una subred en IPv6 es de 2^{64} (máscara de subred de 64 bits). Aunque probablemente el aprovechamiento del espacio de direcciones de la subred sea menor que en IPv4, el uso de direcciones más largas permite una asignación de las mismas de manera jerárquica y sistemática (mejorando así la administración de las redes debido a la reducción de costes operacionales), además de una agregación de rutas más eficiente.

- Permite la autoconfiguración de direcciones IP e interconexiones de equipos usando los mensajes de descubrimiento de routers de ICMPv6. También es posible utilizar DHCPv6 (*Dynamic Host Configuration Protocol* para IPv6) o configurar los nodos de forma estática. ICMPv6 es una nueva versión de ICMP (*Internet Control Message Protocol*) y es una parte importante de la arquitectura IPv6 que debe estar completamente soportada por todas las implementaciones y nodos IPv6. ICMPv6 combina funciones que anteriormente realizaban diferentes protocolos (ICMP, IGMP, ARP ...) y además introduce algunas simplificaciones eliminando tipos de mensajes obsoletos que estaban en desuso actualmente.

- IPv6 no implementa broadcast, aunque pueden enviarse paquetes a la dirección de multicast a todos los nodos (enlace local) con un efecto análogo.

- Se integran algunas características de seguridad, entre las que destaca la obligatoriedad del soporte a IPSec (*Internet Protocol Security*), protocolo utilizado para cifrado y autenticación IP (nivel de red).

- MIPv6 (*Movile* Ipv6), que permite a un nodo moverse por diferentes subredes manteniendo las conexiones de forma transparente, es tan eficiente como el IPv6 normal (a diferencia de Ipv4 móvil).

Las direcciones IPv6 tienen 128 bits de longitud y se escriben como ocho grupos de cuatro dígitos hexadecimales (por ejemplo: 3ffe:ffff:0:0:8:800:20c4:0). Cada grupo se separa por dos puntos y si uno o más grupos son nulos ("0000") se pueden comprimir (para el ejemplo anterior se tiene: 3ffe:ffff::8:800:20c4:0). La dirección ::1 es la de loopback y el prefijo ff00:: se usa para las direcciones multicast.

El formato de las direcciones IPv6 es el siguiente: una cabecera obligatoria de 40 Bytes, una serie de cabeceras opcionales situadas a continuación de la obligatoria y los datos (con cabeceras de protocolos de nivel superior incluidas). El nuevo formato de paquete que especifica IPv6 está diseñado para minimizar el procesamiento del encabezado de paquetes. Además, los cambios en la codificación de las opciones de la cabecera permiten una mayor flexibilidad a la hora de introducir nuevas opciones o variar su longitud. Como apunte, decir que IPv6 ya no limita la carga útil de los paquetes a 64 KB, sino que tiene soporte opcional de hasta 4 GB (los llamados jumbogramas).

Por último, cabe mencionar el sistema IPv6 6to4 que permite enviar paquetes IPv6 sobre una infraestructura IPv4 sin necesidad de configurar manualmente los túneles que encapsulan los paquetes IPv6 en paquetes IPv4.

3. Ejemplo de ataque

Una vez conocidas las características básicas de Ipv6, veamos como sacarle partido al uso de Thc-Ipv6. Como ejemplo básico, pensemos en un alumno que desea aprender el funcionamiento básico de IPv6 realizando un ataque "inofensivo" a otros compañeros que se encuentra dentro de su subred. El manejo de estas herramientas es sencillo y muy intuitivo, aunque la dificultad del ataque aumentaría si el objetivo fuesen máquinas fuera de nuestro segmento de red, como se comentará en la sección siguiente.

1: Fijar objetivo

Como suele pasar a la hora de pensar los ataques, lo primero es conocer cual es nuestro objetivo. Para un ataque a una subred con Ipv4, una forma típica de actuar sería utilizar una herramienta como Nmap para buscar las direcciones de las máquinas en la subred a atacar, escanear sus puertos, buscar vulnerabilidades en los puertos abiertos... Con Ipv6, la secuencia de acciones sería similar, pero debido al enorme rango de direcciones válidas dentro de una subred (2^{64}), el tiempo de

cómputo necesario para el escaneo inicial sería excesivo. Así, con IPv6, las fuentes de información principales (y por tanto uno de los objetivos clave) serán los servidores DNS (*Domain Name System*). Esto se debe a que los servidores públicos necesitan estar en servidores DNS para que los clientes puedan resolver sus direcciones IP y todas las máquinas necesitan estar en servidores DNS privados con la finalidad de ser administradas.

En esta tarea, nos puede ser de utilidad una de las herramientas incluidas en Thc-IPv6: **alive6**.

Si ejecutamos en un terminal:

> ./alive6 interfaz

La respuesta obtenida serán las N direcciones de las interfaces de red locales con direcciones Ipv6, entre las que podremos seleccionar algunas a atacar:

Alive: direccionIpv6-1
Alive: direccionIpv6-2
...
Alive: direccionIpv6-N
Found N systems alive

2: Buscar vulnerabilidades

Si quisiéramos realizar un ataque serio, una vez conocido nuestro objetivo deberíamos encontrar sus vulnerabilidades. En el apartado siguiente se comentan errores de seguridad típicos que se pueden encontrar (y aprovechar) para ataques a IPv6, en su mayoría debidos a descuidos o malas implementaciones. En todo caso, la búsqueda de vulnerabilidades se escapa al contenido de este documento, ya que no estaría ligada directamente con el uso de las herramientas proporcionadas por Thc-IPv6. Por tanto, se procede directamente a explicar algunos ejemplos de ataques.

3: Interceptar y falsificar mensajes

Podemos empezar por interceptar (y modificar) mensajes enviados entre dos máquinas de la subred, es decir, realizar el clásico MitM (*Man in the Middle*). La realización de este tipo de ataque en IPv4 se basa en el funcionamiento de las peticiones de ARP (para obtener la MAC correspondiente a una dirección IP) y mensajes DHCP (para asignar direcciones IP dinámicamente), enviados ambos a la dirección de broadcast de la subred. Por tanto, cualquiera puede responder a estos mensajes, falseando así la información. En IPv6 no se añade una seguridad especial a lo anterior, la diferencia radica en que se utiliza ICMP6 para realizar estas peticiones y se utilizan direcciones multicast (pues en IPv6 no hay direcciones de broadcast).

Un posible ataque MitM con IPv6 es el siguiente. Cuando un compañero1 víctima quiera comunicarse con un compañero2, enviará una petición ICMP6 (para solicitar la MAC de compañero2) a todos los nodos de la subred (dirección multicast). El atacante puede utilizar la herramienta **parasite6** para enviar una respuesta afirmando que la MAC solicitada se corresponde con su dirección IP.

Si ejecutamos en un terminal:

```
> ./parasite6 interfaz
Remember to enable routing (ip_forwarding), you will denial service otherwise!
Started ICMP6 Neighbor Solitication Interceptor (Press Control-C to end) ...
```

Estaremos redirigiendo el tráfico local a nuestro sistema. Como se indica al ejecutar el comando, se debe habilitar el enrutamiento para redirigir los paquetes interceptados a su destino correcto. De no hacerlo así, realmente estaríamos haciendo un ataque DoS (*Denial of Service*): el receptor legítimo de los paquetes no los recibirá.

Otra posibilidad relacionada con la asignación de IP's es utilizar el chequeo DAD (*Duplicate Address Detection*) necesario cuando se quiere asignar una IP a una interfaz de red. La máquina que desea utilizar una dirección IP envía un mensaje ICMP6 para comprobar si la dirección ya está siendo usada. El atacante puede utilizar la herramienta **dos-new-ip6** para impedir que se asignen nuevas IP's en la subred afirmando que utiliza todas las direcciones.

La sintaxis es análoga a los casos anteriores:

```
> ./dos-new-ip6 interfaz
Started ICMP6 DAD Denial-of-Service (Press Control-C to end) ...
```

Hay otras posibilidades relacionadas con estos ataques, como la proporcionada por el exploit **fake_router6** que se puede utilizar para hacerse pasar por router en la red (y así conseguir, por ejemplo, modificar las tablas de enrutamiento de las víctimas).

4: Enviar mensajes multicast

Con IPv4 se puede utilizar el envío de paquetes a la dirección de broadcast para realizar un ataque de DoS a una máquina. Se utiliza la dirección de la víctima como origen y todas las máquinas de la red (que no tengan deshabilitada la opción de respuesta a peticiones con destino broadcast) responden a la víctima, amplificando su tráfico y provocando la DoS. En IPv6, como se ha comentado anteriormente, no hay direcciones de broadcast. Pero se pude realizar un ataque análogo utilizando la dirección de multicast de todos los nodos locales. Para ello podemos utilizar **smurf6**.

La herramienta smurf6 se utiliza para ataques locales indicando como fuente de los paquetes ICMP6 la dirección de la víctima y destino la dirección de multicast local.

La sintaxis es la siguiente:

```
> ./smurf6 interfaz direccionIPv6-Víctima
Starting smurf6 attack against direccionIPv6-Víctima (Press Control-C to end) ...
```

Esto generaría una gran cantidad de tráfico local que sería enviado a la fuente. Debe notarse que este ataque sólo funcionará si las máquinas locales tienen habilitada la opción de respuesta a peticiones con destino una dirección multicast.

Otra herramienta que provee Thc-IPv6 es **rsmurf6**. Esta herramienta se utilizaría para ataques DoS con destino una máquina de remota y fuente la dirección de multicast local (todos los nodos). Para que este ataque funcione es necesaria una mala implementación, ya que el destino no debería responder a peticiones cuyo origen es una dirección multicast.

4. Dificultades en los ataques

Los ataques presentados en el apartado anterior están simplificados. Para empezar, si las máquinas víctima estuviesen fuera de nuestra subred, la dificultad aumentaría debido a la alta probabilidad de que un firewall tirase la paquetería enviada o de que las acciones "ilícitas" fuesen detectadas por un IDS (*Intrusion Detection System*). Además, y como se ha comentado en varias ocasiones, para que los ataque sean efectivos dependemos en muchas ocasiones de malas implementaciones o de descuidos por parte de los administradores de red.

Entre las características más salientables de IPv6 desde el punto de vista de la seguridad destacan el que es más sencillo realizar filtrado de las redes, la obligación de posibilitar el empleo de IPSec (que facilita el traceado de los ataques y dificulta el sniffing y los ataques MitM), etc. Aún así, la seguridad y los riesgos de IPv6 no difieren excesivamente de los de IPv4.

Por "suerte", muchos administradores descuidan la seguridad en lo que respecta a ipv6 debido a su menor uso. Además, a todo esto se suma que debido debido a su relativamente reciente aparición, hay un menor chequeo de IPv6 y, consecuentemente, una mayor probabilidad de encontrar posibles errores de implementación de la pila ipv6 y de aplicaciones que tengan habilitado su uso.

5. Otras posibilidades de Thc-IPv6

Cabe destacar que las posibilidades de Thc-IPv6 para ataques a IPv6 son muy amplias y crecerán con el mayor uso de este protocolo y según se investiguen sus vulnerabilidades. Algunas de las herramientas proporcionadas por Thc-IPv6 no comentadas con anterioridad son: **redir6** (redirige el tráfico al sistema del atacante en una LAN), **toobig** (reduce el MTU del destino), **fake_mipv6** (en caso de estar IPSec deshabilitado, redirige el tráfico de un nodo con IP móvil al destino elegido), etc.

Otra herramienta muy cómoda incluida en Thc-IPv6 es **detect-new-ip6**, que se puede utilizar para automatizar tareas. Simplemente detecta nuevos sistemas con IPv6 habilitado en la red local y si se le pasa un script como argumento, lo ejecuta con las nuevas direcciones detectadas.

La sintaxis es como sigue:

```
> ./detect-new-ip6 interfaz [script]
```

Además, como se ha comentado, es posible aprovechar posibles descuidos debidos a la convivencia de protocolos. Muchos sistemas operativos habilitan IPv6 por defecto y al haber dos pilas IP, es posible que por un despiste del administrador se filtre Ipv4 y no Ipv6. Si se conocen los dos routers "tunelizadores" en túneles 6to4, es muy sencillo inyectar tráfico y realizar IP spoofing.

Por otra parte, la tarea de los firewalls se hace más complicada: para el correcto funcionamiento de Ipv6, se debe permitir que pasen muchos de los mensajes ICMP6; IPSec oculta datos (y por tanto protocolos) de las capas superiores; la gran cantidad de cabeceras opcionales puede provocar "confusiones" (es decir, se hace más difícil distinguir la paquetería legítima de la que no lo es); etc.

Como conclusión, decir que, como se ha ido viendo a lo largo del presente texto, resulta un tanto "sorprendente" el comprobar que IPv6 (un protocolo destinado a sustituir a IPv4) tiene unas vulnerabilidades bastante similares a su (todavía en uso) predecesor (obviando las diferencias "técnicas" y de formatos entre uno y otro). Como se puede observar, las herramientas probadas tienen una sintaxis muy intuitiva, con lo que se puede intentar explotar estas vulnerabilidades de manera sencilla. Y como se comentaba al inicio del documento, también se pueden escribir exploits propios en unas cuantas líneas utilizando la librería proporcionada. Por tanto, animo al lector de este documento a realizar sus propias pruebas y a ampliar sus conocimientos sobre este tema. Además, con toda seguridad un buen conocimiento del funcionamiento de IPv6 será útil (y necesario) en los próximos años.

Pueden resultar de interés los siguientes enlaces:

- Para descargar el paquete Thc-IPv6 y encontrar más información sobre los exploits:
  http://freeworld.thc.org/thc-ipv6/

- Para obtener una información ampliada sobre IPv6 recomiendo la lectura del siguiente documento:
  http://www.cu.ipv6tf.org/pdf/Tutorial%20de%20IPV6.pdf