Resultados de un análisis de seguridad de los protocolos TCP e IP

Fernando Gont
(proyecto de investigación realizado para UK CPNI)

4ta Jornada de Seguridad Informática
Colegio de Ingenieros Especialistas de Entre Ríos

25 de Noviembre de 2008, Paraná, Entre Ríos, Argentina

Acerca de….

- Miembro del Centro de Estudios de Informática (CEDI) de UTN/FRH, trabajando en el área de ingeniería de Internet.
- Participante activo de la IETF (Internet Engineering Task Force), participando en el proceso de estandarización de los protocolos de comunicaciones utilizados por la red Internet. Autor de cinco documentos adoptados oficialmente por la IETF para su futura publicación como RFCs.
- Realicé actividades de investigación en el área de seguridad de protocolos de comunicaciones para UK's NISCC (United Kingdom's National Infrastructure Security Co-ordination Centre).
- Actualmente trabajando para UK CPNI (United Kingdom's Centre for the Protection of National Infrastructure)
- Durante algún tiempo fue miembro del equipo de desarrollo de OpenBSD, focalizando mi actividad en la pila TCP/IP.
- Más información en: http://www.gont.com.ar

Agenda

- Descripción del problema
- Descripción del proyecto llevado a cabo por UK CPNI
- Breve repaso del protocolo IP
- Descripción de algunos de los resultados obtenidos como producto del proyecto anteriormente mencionado
- Conclusiones
- Preguntas (y posibles respuestas)

Enunciado del problema

- Durante los últimos veinte años, el descubrimiento de vulnerabilidades en implementaciones de los protocolos TCP/IP, y en los propios protocolos, han llevado a la publicación de un gran número de reportes de vulnerabilidad por parte de fabricantes y CSIRTs.
- Como resultado, la documentación de todas estas vulnerabilidades se encuentra esparcida en una gran cantidad de documentos que suelen ser difíciles de identificar.
- Asimismo, algunos de estos documentos proponen contramedidas a las mencionadas vulnerabilidades, sin realizar un análisis minucioso de las implicancia de las mismas sobre la interoperabilidad de los protocolos.
- Desafortunadamente, el trabajo de la comunidad en esta área no ha reflejado cambios en las especificaciones correspondientes de la IETF.

Enunciado del problema (II)

- Se hace notablemente dificultoso realizar una implementación segura de los protocolos TCP/IP a partir de las especificaciones de la IETF.
- No existe ningún documento que apunte unificar criterios sobre las vulnerabilidades de los protocolos, y las mejores prácticas para mitigarlas.
- No existe ningún documento que sirva como complemento a las especificaciones oficiales, para permitir que la implementación segura de los protocolos TCP/IP sea una tarea viable.
- Nuevas implementaciones de los protocolos re-implementan vulnerabilidades encontradas en el pasado.
- Nuevos protocolos re-implementan mecanismos o políticas cuyas implicancias de seguridad ya eran conocidas a partir de otros protocolos (por ejemplo, RH0 en IPv6).

Descripción del proyecto (I)

- En los últimos años, UK CPNI (Centre for the Protection of National Infrastructure) – antes UK NISCC (National Infrastructure Security Co-ordination Centre) – se propuso llenar este vacío para los protocolos TCP e IP.
- El objetivo fue producir documentos que sirvieran de complemento a las especificaciones de la IETF, con el fin de que, mínimamente, nuevas implementaciones no posean vulnerabilidades ya conocidas, y que las implementaciones existentes puedan mitigar estas vulnerabilidades.
- Dichos documentos se irían actualizando en respuesta a los comentarios recibidos por parte de la comunidad y al descubrimiento de nuevas vulnerabilidades.
- Finalmente, se espera llevar este material al ámbito de la Internet Engineering Task Force (IETF), para promover cambios en los estándares correspondientes.

Resultados preliminares

- Para el caso del protocolo IP, se generó un documento de 50 páginas, con mas de 70 referencias a reportes de vulnerabilidad y papers relevantes. El mismo se encuentra disponible en: http://www.cpni.gov.uk/Products/technicalnotes/3677.aspx
- Para el caso del protocolo TCP, se generó un documento de más de 100 páginas, con más de 100 referencias a reportes de vulnerabilidad y papers relevantes. Este documento todavía no ha sido publicado.
- Los documentos se beneficiaron de los comentarios de desarrolladores de implementaciones TCP/IP, tanto abiertas como cerradas.
- El documento “Security Assessment of the Internet Protocol” ha sido llevado al ámbito de la IETF, mediante el Internet-Draft `draft-gont-opsec-ip-security`

Revisión de IP

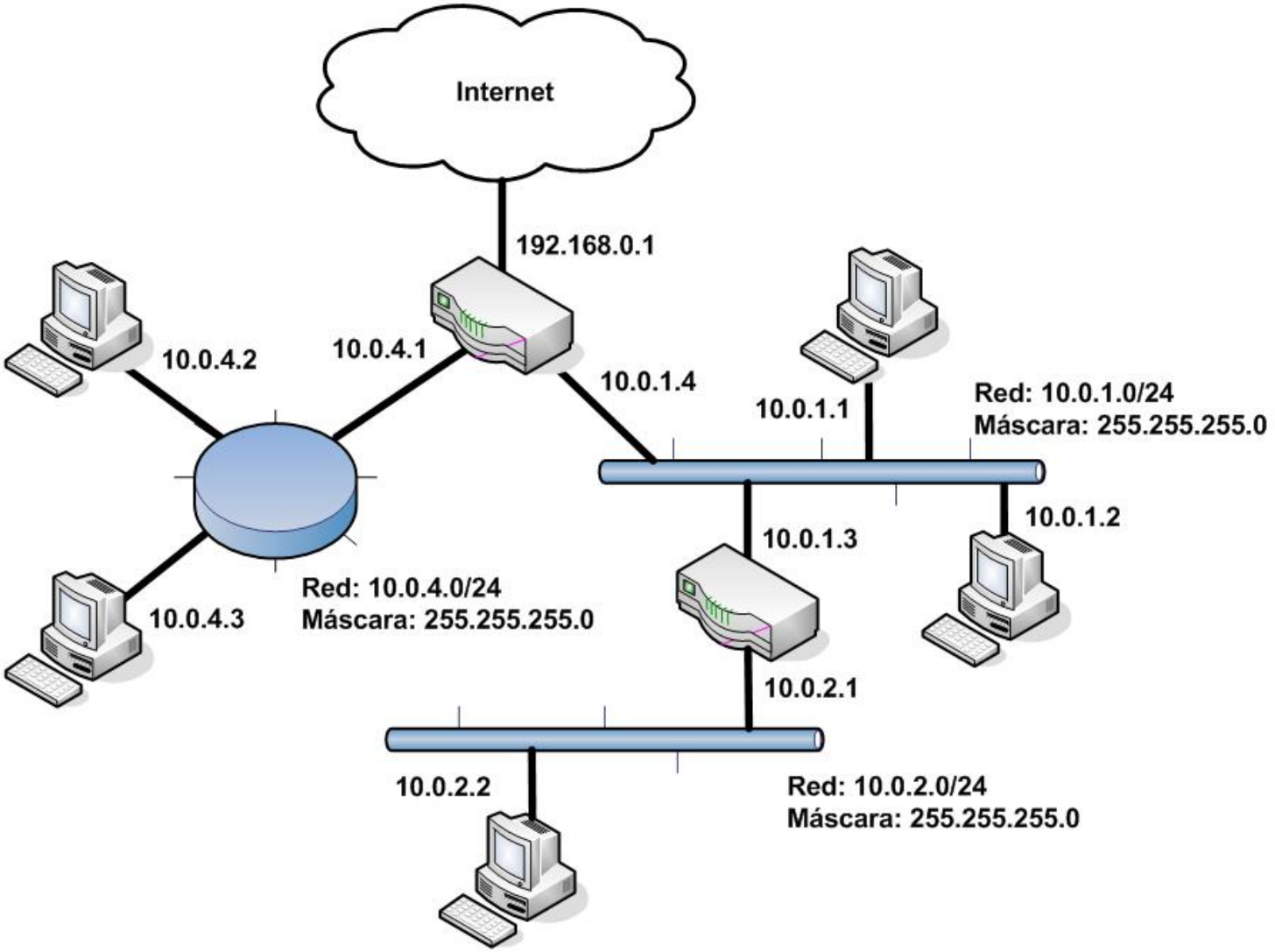
El protocolo IP

- Creado entre fines de la década del ’70 y comienzos de la década del ’80
- Se originó en el trabajo de Cerf y Kahn, titulado “A Protocol for Packet Network Interconnection”
- Ni lo que hoy es Internet, ni su antecesora (ARPANET), ni los protocolos en cuestión, fueron concebidos con la idea de ser “seguros”, ni de sobrevivir ataques nucleares. (Pese a lo documentado por virtualmente la totalidad de la bibliografía existente)
- Jamás se imaginó que los mismos pudieran llegar a ser de uso masivo
- El campo de las redes era nuevo: Habían muchísimas cosas por aprender.
- Todas estas consideraciones se reflejan en los actuales protocolos. Algunas, incluso en los “nuevos” protocolos (IPv6, etc.)

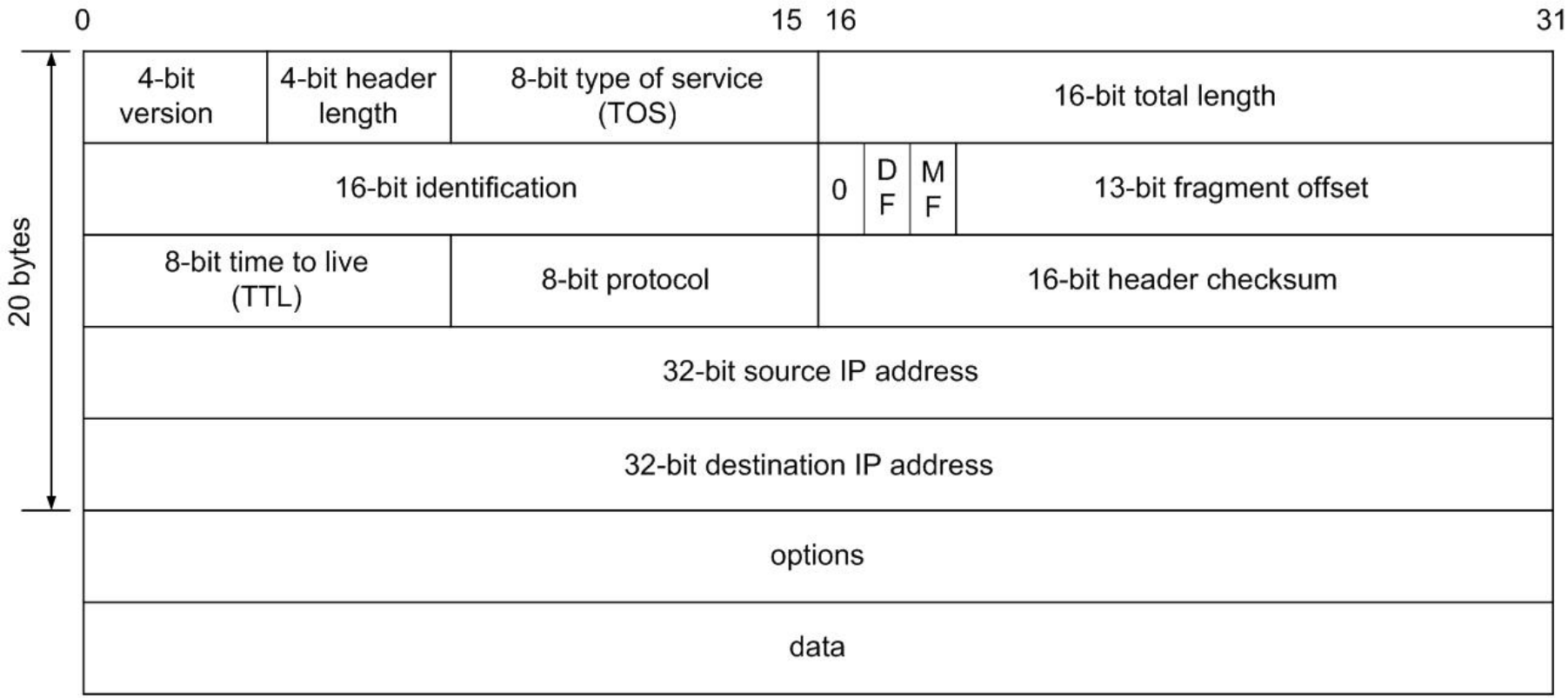
Servicio brindado por IP

- El servicio brindado por el protocolo IP es de tipo “best effort”
- No provee garantía alguna de que la información transmitida llegará a destino
- Los paquetes podrían ser descartados debido a corrupción de datos o congestión de la red
- Los paquetes podrían llegar duplicados
- Los paquetes podrían llegar fuera de orden
- La información contenida en los paquetes podría corromperse en el camino hacia su destino.

Ejemplo de red IP



Sintaxis del encabezado IP

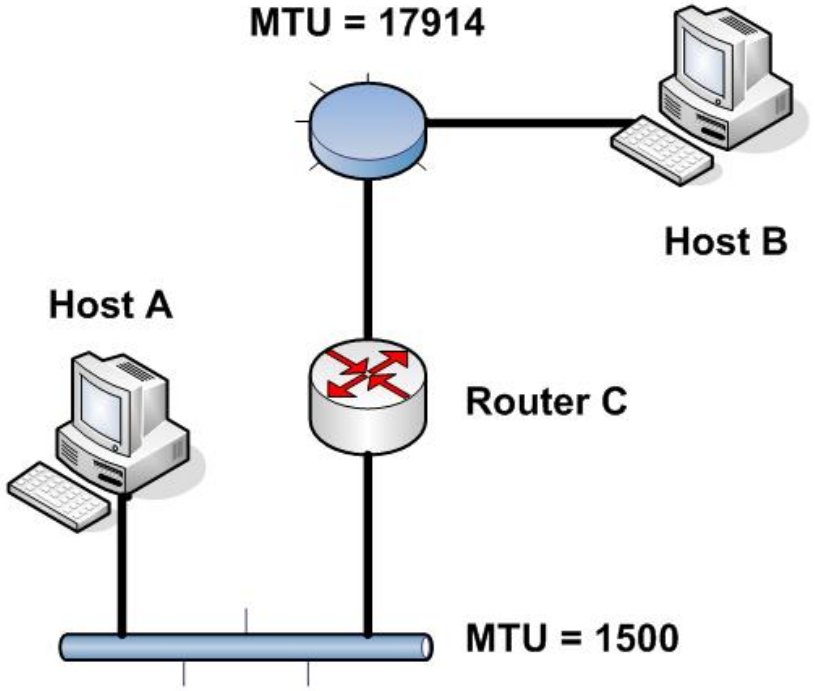


Minimizado el efecto de bucles de ruteo

- Si los routers de la red están bien configurados, cada paquete llegará a su destino.
- Si estuvieran mal configurados, o bien existieran problemas temporales con alguno de los enlaces, podría suceder que algún paquete quedara atrapado en un “bucle de ruteo”.
- Si IP no proveyera ningún mecanismo para controlar estas circunstancias, y varios paquetes quedaran atrapados en bucles de ruteo, la red podría quedar inutilizable, hasta que no se reiniciaran los equipos intervinientes.
- Para evitar esto, el encabezado IP contiene el campo TTL (`Time To Live`). El mismo se inicializa algún valor (usualmente mayor que 64). Cada vez que pasa por un router, se lo decrementa. Si al decrementarlo se hace cero, el router deberá descartar el paquete en cuestión.

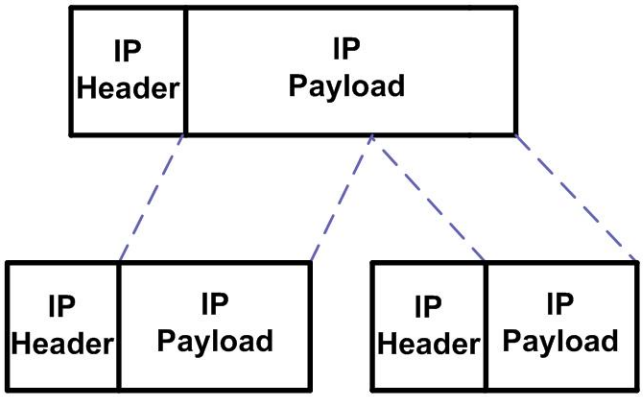
Salvando diferencias de MTUs

- Supongamos que hemos interconectado mediante un router dos redes de tecnología diferente, con distinto MTU. Si el Host B enviara un paquete de 17914 bytes, el mismo, en un principio, no podría ser enviado por la red a la cual pertenece el Host A.



Fragmentación IP

- El protocolo IP brinda un mecanismo para poder “fragmentar” los paquetes.
- Cuando un sistema deba enviar un paquete IP a traves de un enlace cuyo MTU es menor que el tamaño del paquete, dicho sistema fragmentará el paquete IP en cuestión.
- Cada fragmento tendrá su propio encabezado IP.
- Todos los fragmentos tendrán en común el mismo **Identification**.
- El **offset** de cada uno de los fragmentos será diferente.
- Todos los fragmentos, salvo el último, tendrán el bit **MF** (More Fragments) en 1.



Implicancias de seguridad del protocolo IP

Implicancias de seguridad del campo `Identification`

IP Identification

- En cada instante de tiempo determinado, la combinación {Source Address, Destination Address, Protocol, Identification} deberá ser única.
- Dicha combinación identificará a fragmentos correspondientes a un mismo paquete.
- Si se reutilizara para un nuevo paquete un juego de valores {Source Address, Destination Address, Protocol, Identification} que ya estuviera siendo utilizado para otro paquete, los fragmentos correspondiente a uno y otro paquete se “confundirían”, y en consecuencia el resultado de la operación de reensamble sería posiblemente incorrecto.
- Para evitar esto, muchos sistemas utilizaban para el campo Identification un contador global, que se incrementaba en 1 por cada paquete enviado.
- De este modo, no se reutilizaba un valor hasta que todos los otros valores del rango hubieran sido utilizados.

Implicancias de seguridad del campo Identification

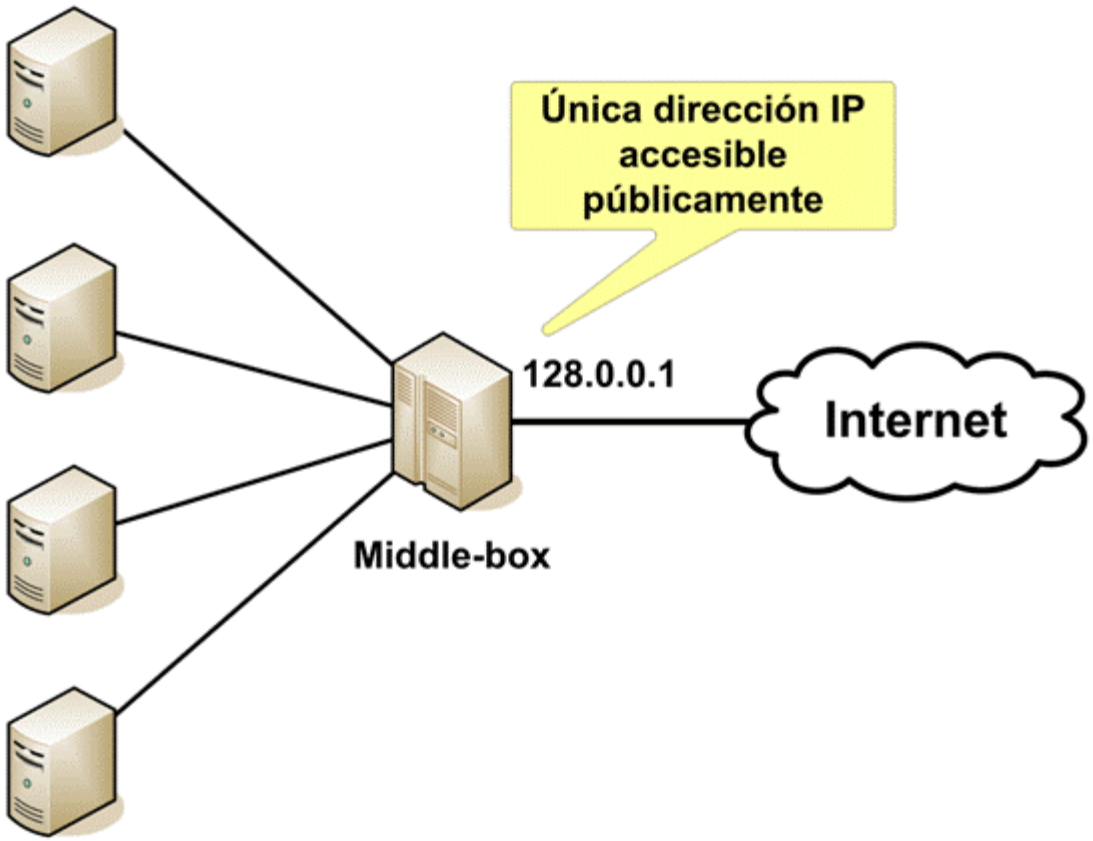
- Si se utiliza para la selección del campo Identification el esquema anteriormente descripto (contador global) el campo podrá ser explotado para:
  - Determinar el packet rate de un determinado sistema
  - Contar la cantidad de sistemas detrás de un NAT
  - Realizar un escaneo de puertos de tipo stealth

IP ID: Determinando el packet-rate de un sistema

- Enviaremos al sistema en cuestión cualquier paquete que genere una respuesta, y anotaremos el valor del campo IP ID de dicha respuesta (“IPID_1”).
- Luego, enviaremos una segunda petición, para obtener otra respuesta, y anotar el valor del campo IP ID incluido en la misma. (“IPID_2”).
- Así, el número de paquetes transmitido por el sistema en cuestión en el intervalo de tiempo transcurrido entre el envío de ambas pruebas será: cant_paquetes = IPID_2 - IP_1 -1

IP ID: Detectando sistemas detrás de un middle-box (I)

- Escenario:



IP ID: Detectando sistemas detrás de un middle-box (II)

- Utilizando herramientas tales como hping:

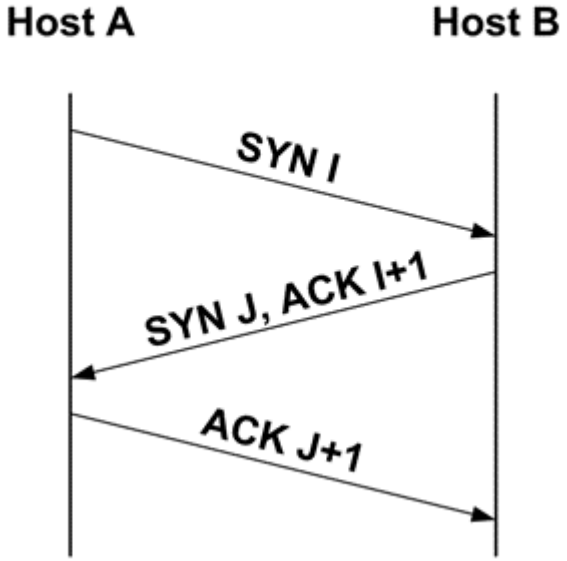
```
# hping2 -c 10 -i 1 -p 80 -S 128.0.0.1
HPING 128.0.0.1 (eth0 128.0.0.1): S set, 40 headers + 0 data bytes
46 bytes from 128.0.0.1: flags=SA seq=0 ttl=56 id=57645 win=16616 rtt=21.2 ms
46 bytes from 128.0.0.1: flags=SA seq=1 ttl=56 id=57650 win=16616 rtt=21.4 ms
46 bytes from 128.0.0.1: flags=RA seq=2 ttl=56 id=18574 win=0 rtt=21.3 ms
46 bytes from 128.0.0.1: flags=RA seq=3 ttl=56 id=18587 win=0 rtt=21.1 ms
46 bytes from 128.0.0.1: flags=RA seq=4 ttl=56 id=18588 win=0 rtt=21.2 ms
46 bytes from 128.0.0.1: flags=SA seq=5 ttl=56 id=57741 win=16616 rtt=21.2 ms
46 bytes from 128.0.0.1: flags=RA seq=6 ttl=56 id=18589 win=0 rtt=21.2 ms
46 bytes from 128.0.0.1: flags=SA seq=7 ttl=56 id=57742 win=16616 rtt=21.7 ms
46 bytes from 128.0.0.1: flags=SA seq=8 ttl=56 id=57743 win=16616 rtt=21.6 ms
46 bytes from 128.0.0.1: flags=SA seq=9 ttl=56 id=57744 win=16616 rtt=21.3 ms

--- 128.0.0.1 hping statistic ---
10 packets tramitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 21.1/21.3/21.7 ms
```

- Donde se pueden apreciar dos secuencias de IP ID

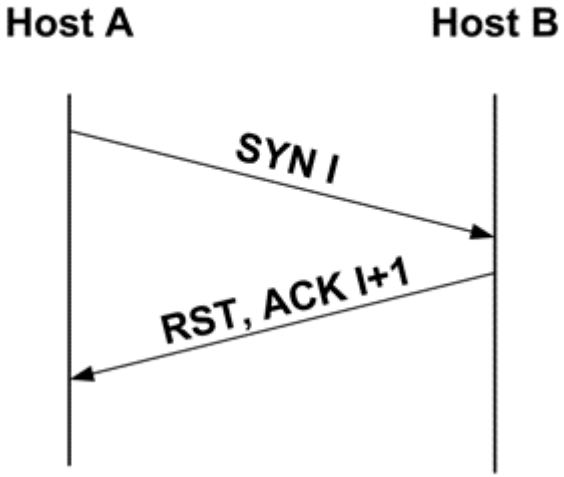
IP ID: Escaneo de puertos “stealth” (I)

- Dos escenarios posibles al intentar establecer una conexión TCP:

Conexión exitosa



Rechazo de conexión

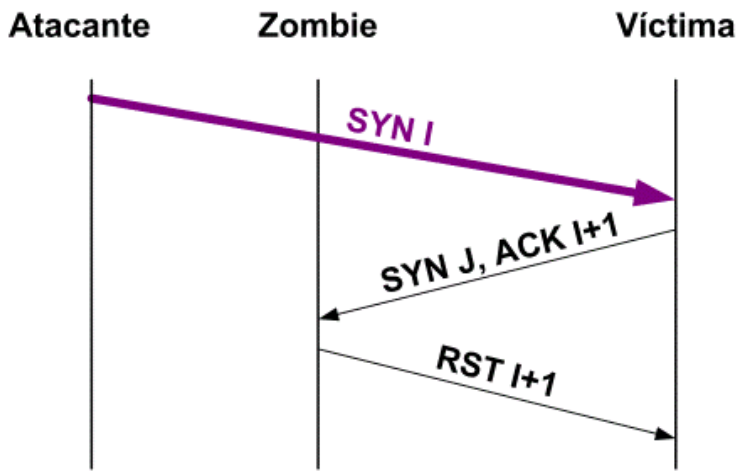


- En el primer caso, Host A envía dos paquetes. En el segundo caso, Host A envía un único paquete

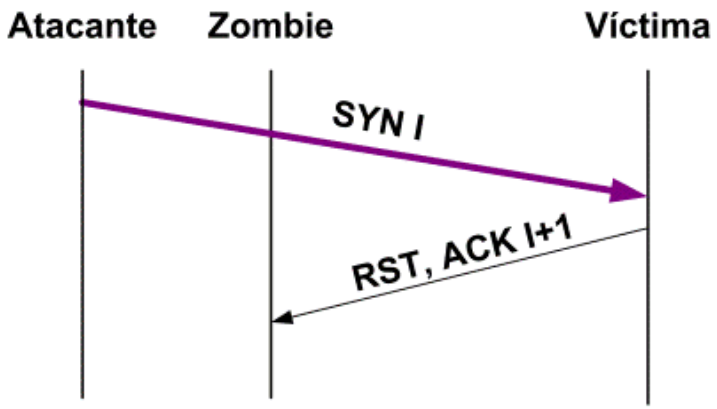
IP ID: Escaneo de puertos “stealth” (II)

- ¿Qué pasaría si el atacante enviara un SYN falsificado?

Puerto abierto

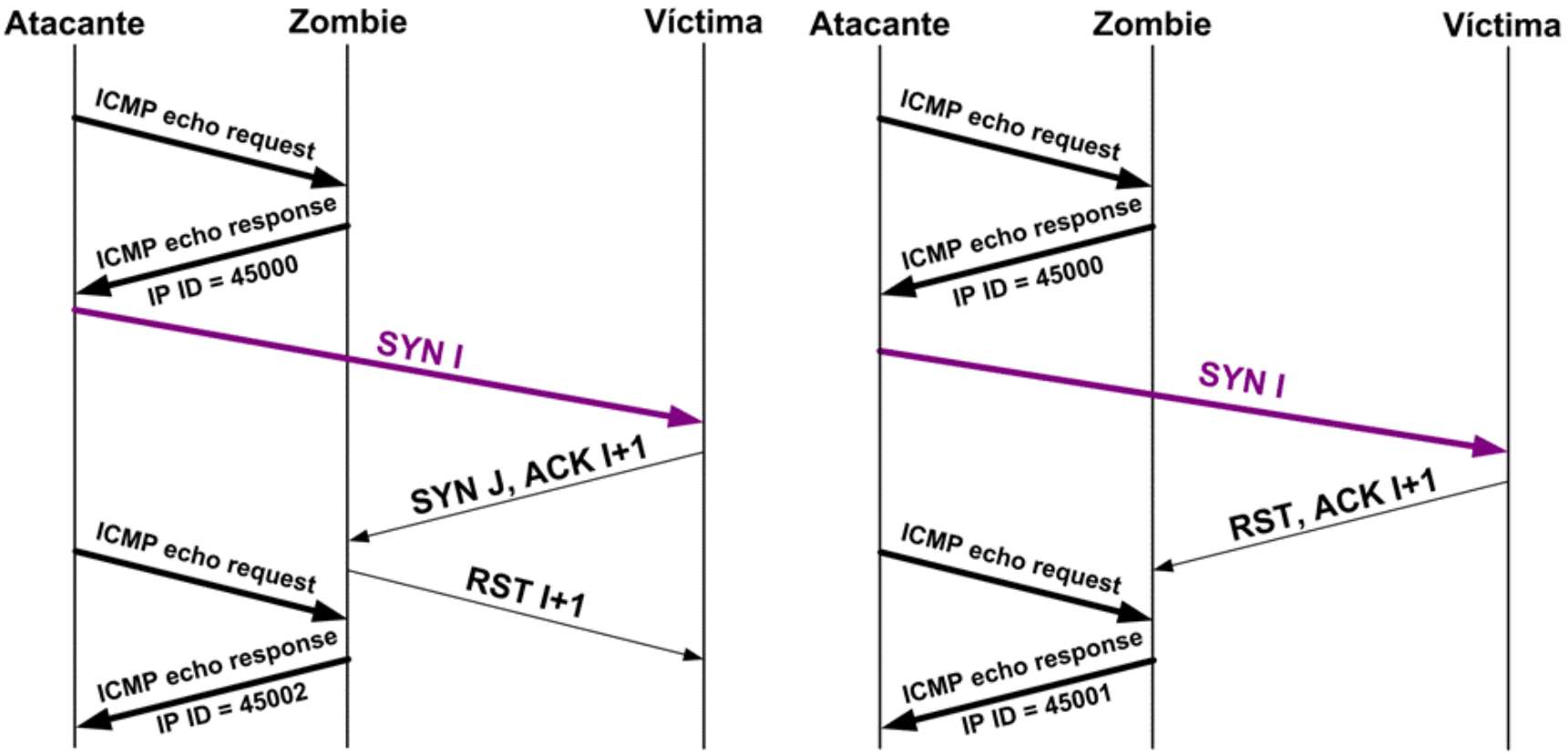


Puerto cerrado



- Si se pudiera detectar la cantidad de paquetes transmitidos por el sistema “zombie”, se podría realizar un escaneo de puertos de tipo “stealth”

IP ID: Escaneo de puertos “stealth” (III)



- Mediante un ICMP echo request (ping) se averigua la cantidad de paquetes transmitida por el zombie.

IP ID: Escaneo de puertos “stealth” (IV)

- Realización de escaneo de puertos stealth con nmap

```
# nmap -P0 -p- -sI kiosk.adobe.com www.riaa.com

Starting nmap V. 3.10ALPHA3 ( insecure.org/nmap/ )
Idlescan using zombie kiosk.adobe.com (192.150.13.111:80); Class:
   Incremental
Interesting ports on 208.225.90.120:
(The 65522 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
25/tcp     open        smtp
80/tcp     open        http
111/tcp    open        sunrpc
135/tcp    open        loc-srv
443/tcp    open        https
1027/tcp   open        IIS
1030/tcp   open        iad1
2306/tcp   open        unknown
5631/tcp   open        pcanywheredata

Nmap run completed -- 1 IP address (1 host up) scanned in 2594.472 seconds
```

Mitigación de estas vulnerabilidades

- Para evitar que el campo Identification revele información innecesariamente, se propone aleatorizar el valor del campo Identification de cada paquete transmitido.
- De este modo, no existirán “secuencias predecibles” de valores para el campo en cuestión

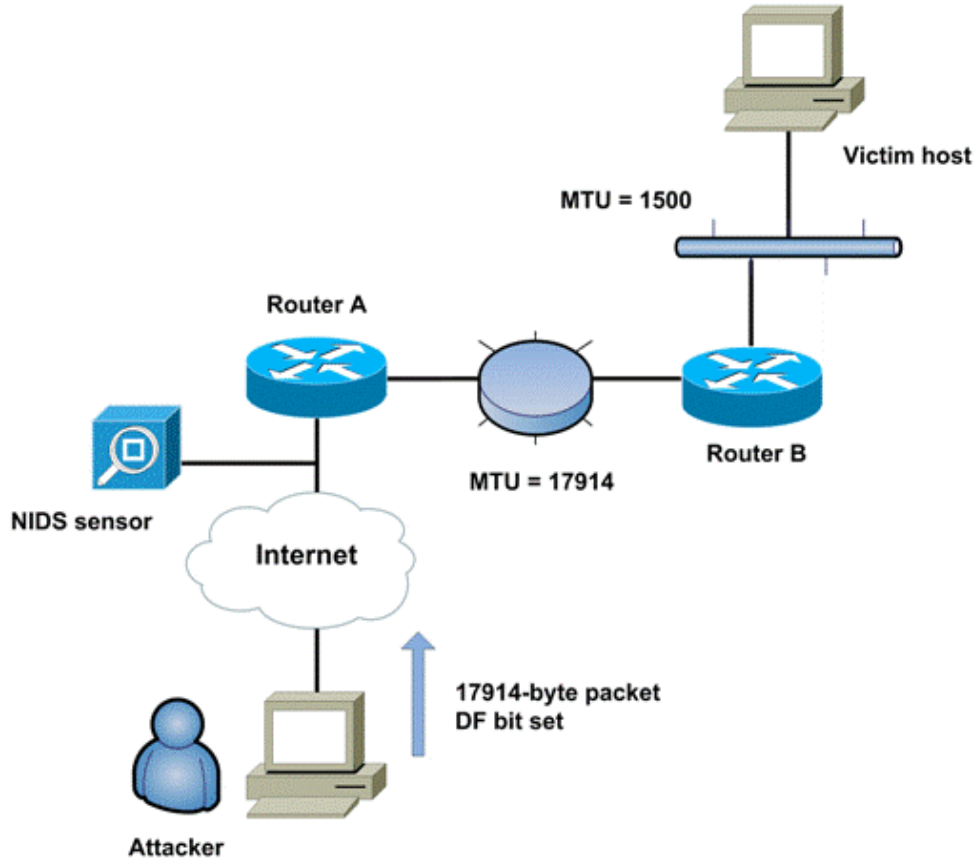
Implicancias de seguridad del bit "Don't Fragment" (DF)

Implicancias del bit “Don’t Fragment”

- Este bit se utiliza para indicar a los routers intermediarios que NO se debe fragmentar el paquete en cuestión.
- En caso que algún router deba fragmentar el paquete en cuestión apra poder reenviarlo a destino, pero el bit “Don’t Fragment” esté seteado, se descartará el paquete en cuestión, y se enviará un mensaje ICMP “Fragmentation Needed and DF bit set”.

Bit Don’t fragment: Evasión de NIDS (I)

- En determinadas topologías de red, un atacante se podría valer del bit DF para “engañar” al NDS.



Bit Don’t fragment: Evasión de NIDS (II)

- Para implicancias de seguridad anteriormente mencionadas, el NIDS debería tener conocimiento de la topología de red. (Por ejemplo, de acuerdo a lo descripto en “Active Mapping: Resisting NIDS Evasion Without Altering Traffic”, de Shakar y Paxson.

Implicancias de seguridad del mecanismo de reensamble de fragmentos

Implicancias de seguridad del mecanismo de reensamble de fragmentos

- El mecanismo de reensamble de paquetes consiste en reconstruir un paquete original, a partir de los fragmentos IP recibidos.
- Este mecanismo tiene una variedad de implicancias de seguridad.
- Entre ellas, analizaremos aquellas que se originan a partir de:
  - La longitud del campo Identification del encabezado IP
  - La complejidad del algoritmo de reensamble de fragmentos
  - La ambigüedad del proceso de reensamble

Problemas relacionados con la longitud del campo Identification (I)

- Tal como fuera mencionado anteriormente, en caso que en un determinado instante se utilizara un mismo valor de IP ID para mas de un paquete original, se corre el riesgo de que el sistema receptor de los fragmentos correspondientes reensamble mal dichos fragmentos, resultando en un paquete corrupto.
- Un atacante podría simplemente enviar fragmentos con todos los IP posibles (65K de paquetes), para un determinado {Source Address, Destination Address, Protocol}. De tal modo, futuros fragmentos entre determinados sistemas nunca serían reensamblados correctamente, posiblemente llevando a una situación de Denegación de Servicio (DoS).

Problemas relacionados con la longitud del campo Identification (II)

- Solución:
  - En la medida que sea posible, evitar el uso de fragmentación (por ejemplo, mediante la utilización del mecanismo Path-MTU Discovery).
  - Establecer limites en la cantidad de fragmentos aceptados, y liberar espacio (eliminar fragmentos almacenados) cuando se superen los límites preestablecidos.
  - Separar los buffers utilizados para el tráfico fragmentado del tráfico no fragmentado
  - Utilizar un buffer separado para el tráfico IPsec

Problemas relacionados con la complejidad de el algoritmo de reensamble

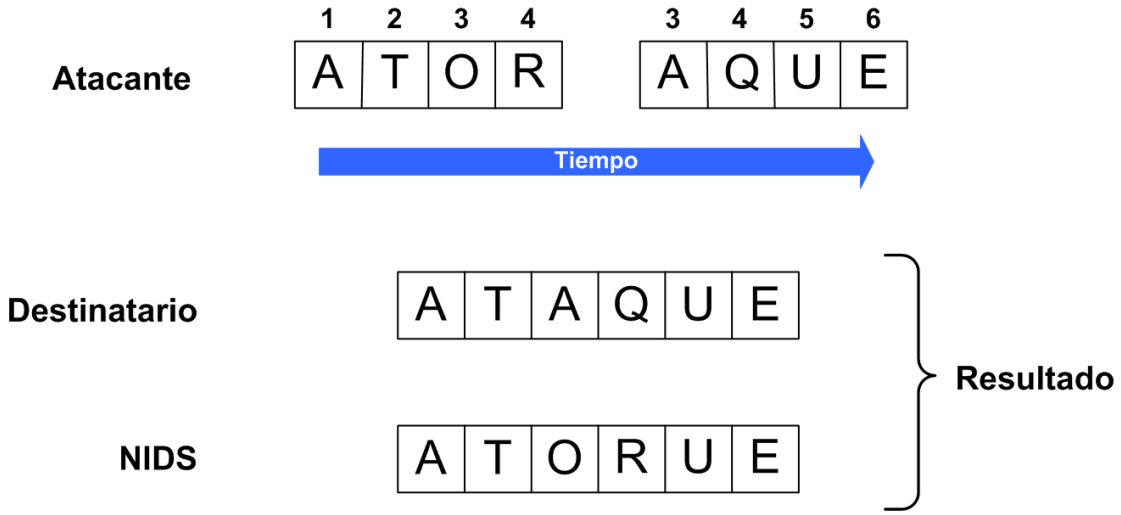
- Debido a que los fragmento IP pueden resultar duplicados en la red, y que asimismo cada fragmento puede tomar un camino distinto para llegar a destino, los fragmentos pueden llegar no solo fuera de orden, sino también solapados.
- Por tal motivo, la implementación de el algoritmo de reensamble de fragmentos dista de ser trivial.
- Durante los últimos 25 años se han encontrado una gran cantidad de vulnerabilidades (principalmente buffer overflows) en el código de reensamble de fragmentos de una variedad de implementaciones del protocolo IP.
- “Solución”: Realizar una implementación cuidadosa del algoritmo de reensamble de fragmentos.

Problemas relacionados con ambigüedad en el proceso de reensamble de fragmentos (I)

- Tal como se mencionara anteriormente, es legítimo recibir fragmentos “solapados”.
- En casos legítimos, aquellas fragmentos que se solapen encapsularán exactamente la misma información.
- Sin embargo, ¿Qué sucedería si la información contenida en los fragmentos solapados no fuera la misma?
- En esta situación, las especificaciones no hacen recomendación alguna, por lo cual existe ambigüedad en el resultado posible.

Problemas relacionados con ambigüedad en el proceso de reensamble de fragmentos (II)

- En el caso que una red estuviera siendo monitoreada mediante un NIDS, esta situación podría ser explotada por un atacante para evadir la detección por parte del NIDS.
- Básicamente, el atacante intentará que la visión del NIDS del tráfico de red sea distinta de aquella del sistema atacado.
- Ejemplo:



Problemas relacionados con ambigüedad en el proceso de reensamble de fragmentos (III)

- Algunas contramedidas posibles para evitar la evasión de NIDS mediante esta técnica:
  - Reensamblar los fragmentos en algún middle-box, antes de que los mismos sean examinados por el NIDS o lleguen al destinatario final.
  - Proveer al NIDS información tal como las políticas de reensamble de fragmentos utilizada por cada uno de los sistemas monitoreados.

Implicancias de seguridad del campo TTL

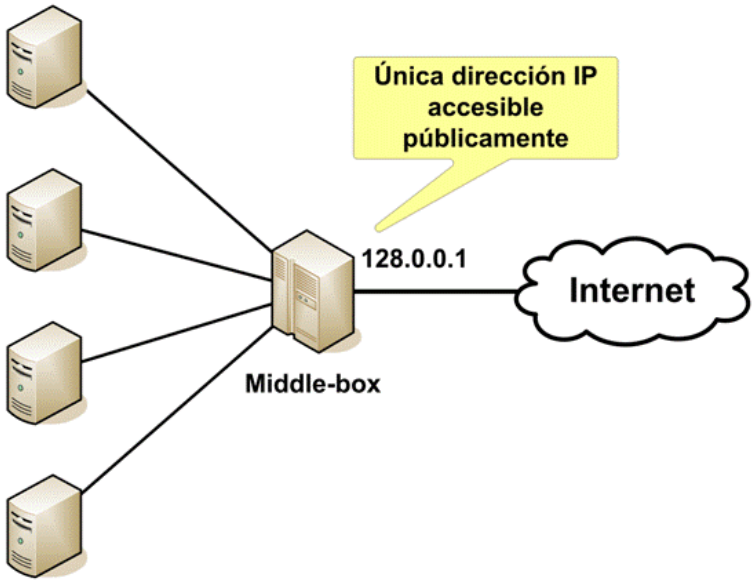
Implicancias de seguridad del campo TTL

- El campo TTL se puede utilizar para:
  - Identificar el sistema operativo utilizado por un sistema
  - Identificar sistemas físicos detrás de una dirección IP
  - Hallar un sistema en la topología de red
  - Evadir Sistemas de Detección de Intrusos en Red
  - Incrementar la seguridad de determinadas aplicaciones

Identificar el sistema operativo

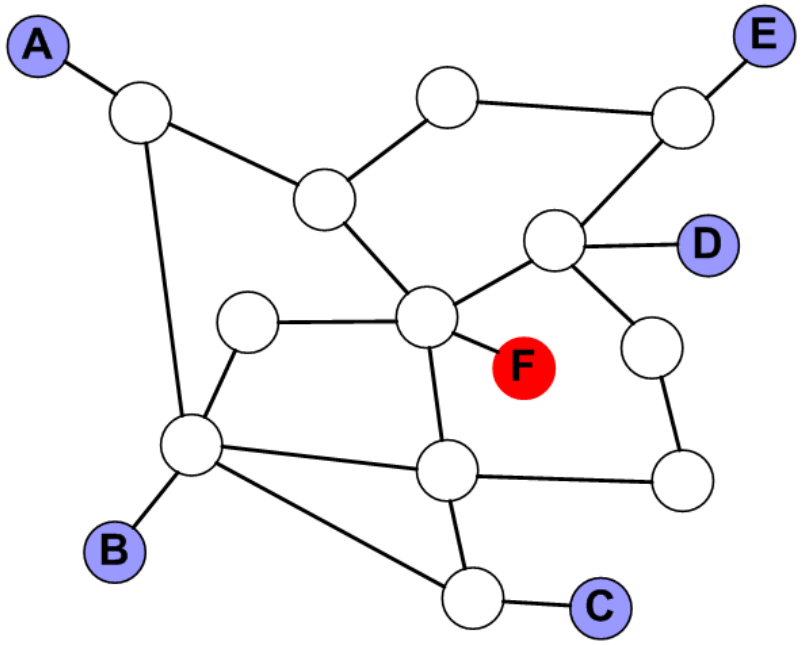
- Distintos sistemas operativos inicializan el campo TTL con distintos valores
- Valores usuales son: 64, 128, y 255
- Debido al “diámetro” limitado de la red Internet, es simple identificar/adivinar el valor con el cual se inicializó el campo TTL
- Identificado dicho valor, quedan determinados los posibles sistemas operativos que podría estar utilizando el sistema en cuestión.

Identificación de dispositivos físicos detrás de un middle-box



- Si distintos flujos de información con una misma dirección IP utilizaran valores para el TTL muy diferentes (por ej., 64 vs. 128), quedaría en evidencia que existen distintos dispositivos físicos detrás de un middle-box.

Hallar un sistema en la topología de red

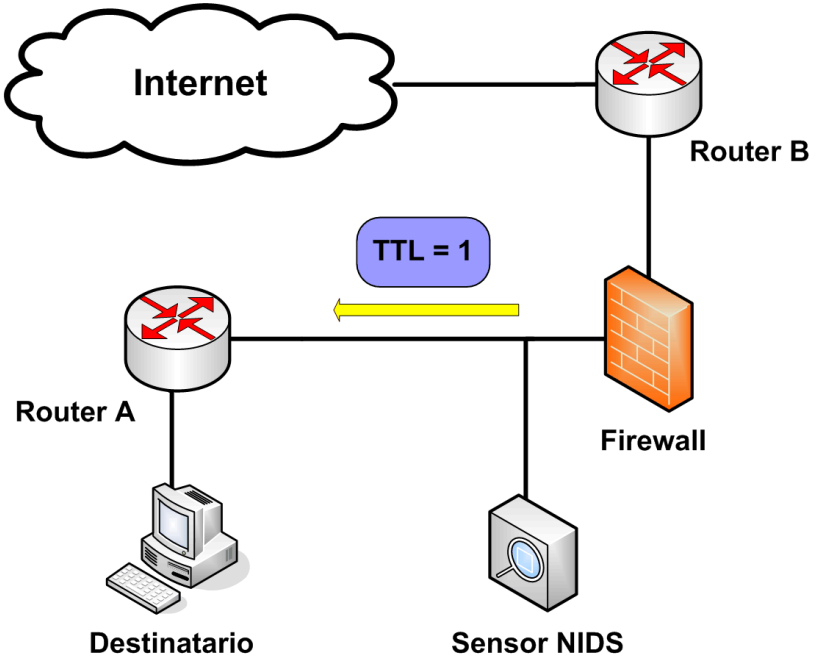


TTL visto por cada sistema:

A: 61
B: 61
C: 61
D: 62

- Un sistema está enviando paquetes a una variedad de sistemas de la red.
- Si el atacante está utilizando los valores “por defecto” del sistema operativo, el único atacante posible para este escenario es el sistema “**F**”

Evasión de NIDS



- El NIDS ve paquetes que el sistema atacado no ve.

Incrementar la seguridad de algunas aplicaciones

- Para escenarios en los cuales ambos sistemas (por ej., cliente y servidor) están en el mismo segmento de red, si se pudiera exigir al sistema que envía los paquetes que inicialice el TTL en 255, entonces se podría exigir que los paquetes recibidos tengan dicho TTL.
- De ese modo, todos los paquetes con cualquier otro valor de TTL serían descartados.
- Únicamente podrían realizar ataques exitosos sistemas que se encuentren en el mismo segmento de red.
- Ejemplo de aplicación: BGP

Conclusiones

Algunas conclusiones….

- Usualmente se asume que, debido a la antigüedad de los protocolos “core” de la suite TCP/IP, todas las implicancias negativas de seguridad del diseño de los mismos han sido resueltas, o solo pueden resolverse mediante uso de IPsec.
- Las vulnerabilidades publicadas incluso en los últimos cinco años parecen indicar lo contrario.
- Curiosamente, este es el primer proyecto que, en 25 años de utilización de los protocolos TCP e IP, intenta hacer un análisis completo de las implicancias de seguridad de los mismos.
- La respuesta de la comunidad a este proyecto ha sido muy positiva. Sin embargo, la colaboración por parte de fabricantes no fue la esperada.

Preguntas?

Información de contacto

Fernando Gont

fernando@gont.com.ar

Más información en:

http://www.gont.com.ar