IPv6 Network Reconnaissance

Fernando Gont

LACSEC 2012
Quito, Ecuador. Mayo 10, 2012

Acerca de...

- Actualmente trabajando para SI6 Networks
- He trabajado en análisis de seguridad de protocolos de comunicaciones para:
  - UK NISCC (National Infrastructure Security Co-ordination Centre)
  - UK CPNI (Centre for the Protection of National Infrastructure)
- Participo activamente en la IETF (Internet Engineering Task Force)
- Actual moderador del Foro de Seguridad de LACNIC
- Más información en: http://www.gont.com.ar

IPv4 Network Reconnaissance (recap)

Revisión

- Direcciones de 32 bits
- Densidad de hosts en red elevada
- Técnica tradicional == fuerza bruta
  - Seleccionar el rango de direcciones deseado
  - Enviar pruebas (ICMP echo, TCP {SYN, ACK}, UDP
  - Esperar respuestas

La escala del problema es pequeña

Fuerza bruta == “suficientemente bueno”

Leyendas Urbanas sobre IPv6 Network Reconnaissance

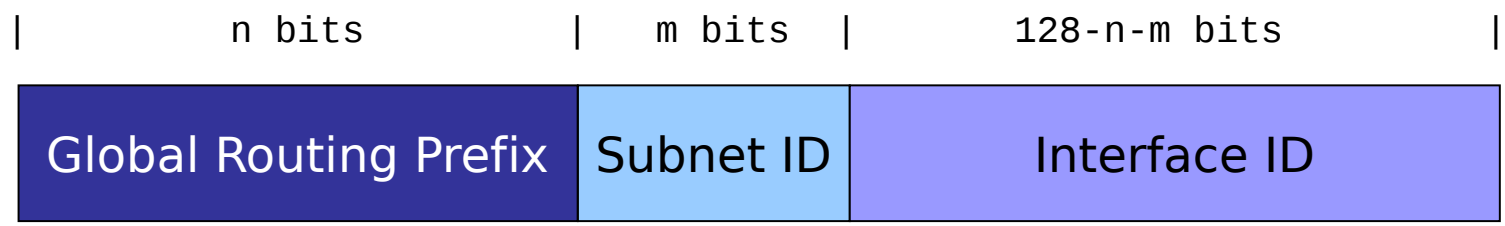
Leyenda urbana

"Debido al gran espacio de direcciones IPv6, los ataques de escaneo son imposibles. Escanear un /64 tomaría 500.000.000 años"

Es realmente el espacio de búsqueda de un /64 2^{64} direcciones?

IPv6 Network Reconnaissance (global)

Formato de Direcciones Globales IPv6



- Diferentes políticas de selección de IID:
  - Embeber la MAC address (SLAAC tradicional)
  - Embeber la dirección IPv4 (por ej., 2001:db8::192.168.1.1)
  - Low-byte (por ej., 2001:db8::1, 2001:db8::2, etc.)
  - Wordy (por ej., 2001:db8::dead:beef)
  - Indicado por una tecnología de transición

Direcciones IPv6 en el mundo real

- Malone midió (*) las politicas de asignación de direcciones en escenarios reales

Tipo dirección	Porcentaje
SLAAC	50%
IPv4-based	20%
Teredo	10%
Low-byte	8%
Privacy	6%
Wordy	<1%
Otras	<1%

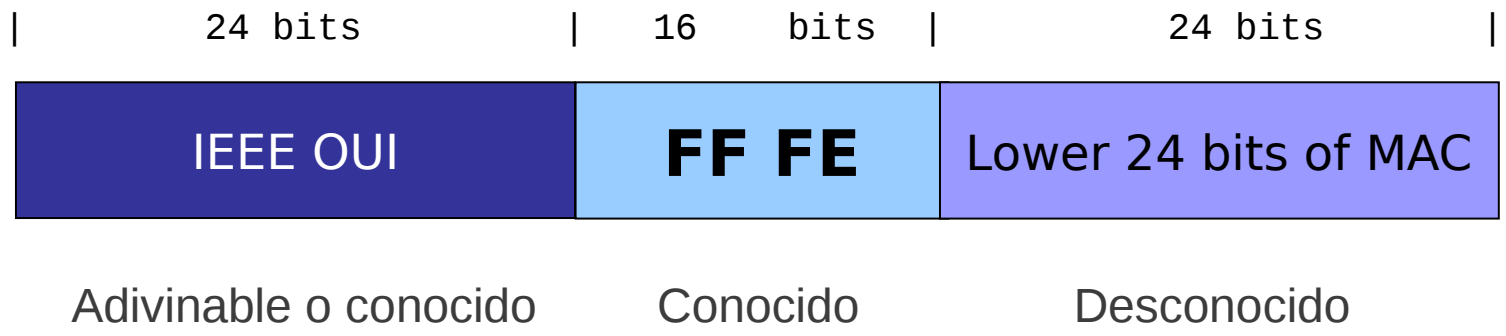
Hosts

Tipo dirección	Porcentaje
Low-byte	70%
IPv4-based	5%
SLAAC	1%
Wordy	<1%
Privacy	<1%
Teredo	<1%
Otras	<1%

Routers

Malone, D., "Observations of IPv6 Addresses", Passive and Active Measurement Conference (PAM 2008, LNCS 4979), April 2008, <http://www.maths.tcd.ie/~dwmalone/p/addr-pam08.pdf>.

Direcciones con IEEE IDs embebidos



- En la práctica, el espacio de búsqueda es a lo sumo ~2^{24} bits – **posible!**
- Los 24 bits de bajo orden no son necesariamente aleatorios:
  - Una organización compra una gran cantidad de equipos
  - Usualmente, los equipos tienen direcciones MAC consecutivas
  - Las MACs se suelen distribuir por regiones geográficas

Direcciones con IEEE IDs embebidos (II)

- Las tecnologías de virtualización presentan un caso interesante
- Virtual Box utiliza el OUI 08:00:27 (espacio de busqueda: ~2^{24})
- VMWare ESX utiliza:
  - MACs automaticas: OUI 00:05:59, y siguientes 16 bits tomados de la dirección IPv4 del host real (espacio de búsqueda: ~2^{8})
  - MACs manualmente configuradas:OUI 00:50:56 y restantes bits en el rango 0x000000-0x3fffff (espacio de búsqueda: ~2^{22})

Direcciones IPv6 basadas en IPv4

- Simplemente incluyen una dirección IPv4 en el IID
- Ejemplo: 2000:db8::192.168..1
- El espacio de búsqueda es el mismo que el correspondiente a IPv4

IPv6 Network Reconnaissance (local)

Escaneo local

- Se trata de un problema completamente diferente
- Se reduce notablemente el espacio de búsqueda utilizando direcciones multicast (por ej. ff02::1)
- Se pueden utilizar tecnicas adicionales como:
  - mDNS
  - LLNR
- En el peor de los casos, puede utilizarse sniffing
- En sintesis, es un problema muy dificil de mitigar

Mitigando
IPv6 Network Reconnaissance

Stable privacy-enhanced addresses

- draft-gont-6man-stable-privacy-addresses propone generar los Interface IDs como:

  F(Prefix, Iface_index, Network_ID, secret_key)

- Donde:
  - F() es una PRF (por ej., una función de hash)
  - Iface_index es un número pequeño que identifica a la NIC
  - Network_ID podría ser, por ejemplo el SSID de una red inalámbrica
  - El resto de los parametros deberían ser obvios ;-)

Stable privacy-enhanced addresses (II)

- Esta función proporciona direcciones que:
  - No son predecibles
  - Son estables en una misma subred (importante para O&M)
  - cambian al moverse de una red a otra
- Propuesta aceptada por el 6man wg de la IETF
  - Aunque parece haber resistencia a hacer un “update” formal de los estandares correspondientes.

Algunas conclusiones

Mitos, leyendas urbanas, y hechos...

"Cuando estudias cualquier materia o consideras cualquier filosofía pregúntate solamente: Cuales son los hechos, y cual es la verdad que los hechos corroboran. Nunca te desvíes, ya sea por lo que deseas creer, o lo por lo que tu piensas que podría tener un efecto benéfico en la sociedad; solo debes mirar única y exclusivamente cuales son los hechos"

– Bertrand Russell

Preguntas?

Gracias!

Fernando Gont

fgont@si6networks.com

IPv6 Hackers mailing-list

http://www.si6networks.com/community/

www.si6networks.com