CORE SECURITY

Recolección furtiva de información

Ernesto Alvarez

2013-07-25

CORE SECURITY

Introducción

Quién soy yo

- Graduado del DC
- Ex-Ayudante de Teoría de las Comunicaciones
- Administrador de red por 8 años
- Actualmente consultor de seguridad senior en CORE

Temario

- Información de contexto
- IG Pasivo
- Identificación de entidades de red
- Ejemplos

Contexto

Distintos modos de trabajo

- Hacking
- Penetration Testing
  - Ataque simulado
  - Objetivo predeterminado
- Scan de vulnerabilidades
  - Busqueda amplia sin profundidad
- Análisis completo de seguridad

Penetration Testing

- Information Gathering
  - Descubrir información básica
  - Descubrir potenciales objetivos
- Ataque
  - Exploits Binarios
  - Errores de configuración o lógicos
  - Otras técnicas
- Pivot

Tipos de redes locales

- Cableadas
  - Medio compartido
  - Hubs
  - Switches
- Inalámbricas
  - Medio compartido
  - Control de acceso
  - Airodump-ng, Kismet, etc

Hubs vs. Switches

Hubs

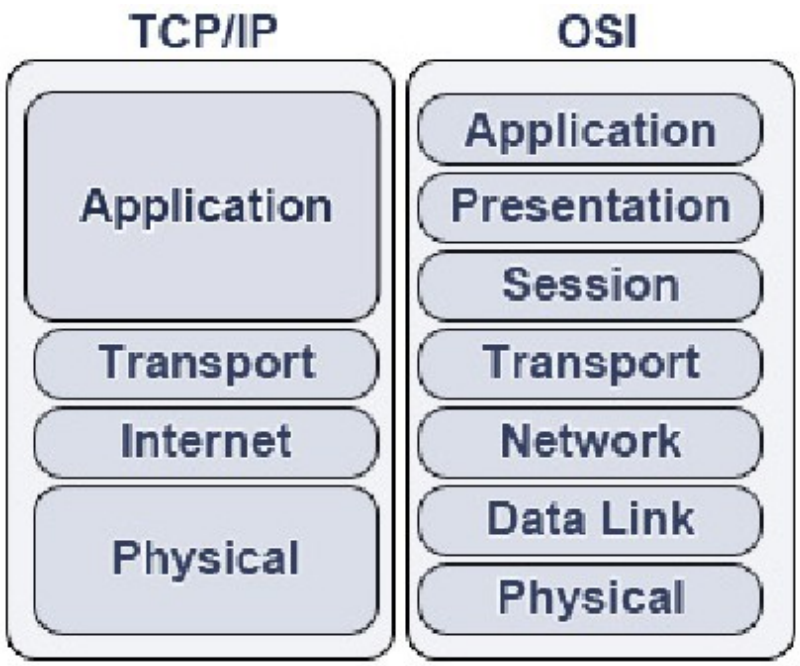
- Poco comunes
- Todo el tráfico se transmite a todos los puertos
- Obsoletos

Switches

- Muy comunes
- Aprenden direcciones de las estaciones
- Casi no se ve tráfico unicast

El stack de protocolos

- Diferentes problemas en diferentes capas
- Capa 2: ethernet
  - No ruteable
- Capa 3: IP
  - Ruteable



IG Pasivo vs. Activo

Pasivo

- No se transmiten paquetes
- Lento
- Dificil de detectar

Activo

- Se transmiten paquetes y se analizan las respuestas
- Preciso
- Detectable

Detección de sniffers

- Modos de conexión a la red
  - Normal
  - Promiscuo
- Detección de sniffers
  - Hacer que el S.O. Responda algo que en teoría nunca debería haber visto
  - ARP request a una MAC inexistente

IG Pasivo

Introducción

- IG pasivo es escuchar y esperar
  - A veces puede ser util tratar de evitar ser detectado en modo promiscuo
  - La mayoría de las veces nadie está buscando hosts en modo promiscuo
- Una vez que se escucha algo, identificar y clasificar
  - Obtener dirección IP y una identificación

Procesamiento en capa 3

- Método más usual
- Requiere conocer parámetros de la red
- Puede necesitar tener una dirección IP
- Complejo
  - Detectar e identificar al mismo tiempo
- Ignora todo lo que no corresponda al protocolo usado

Procesamiento en capa 2

- Dos fases
  - Detección
  - Identificación
- Unicidad de MAC Address
- No es necesario conocer los parámetros de red
  - No depende de ningún protocolo de capa 3 para detección
  - Pero si depende para identificación
- Se basa en que los protocolos de capa 2 no son ruteables normalmente
  - Proxy ARP puede traer problemas
- La identificación debe hacerse con mucho cuidado
  - Una mala identificación puede arruinar todo el proceso

Tráfico detectable en capa 2

- ARP
- STP
- CARP
- Tráfico mal formado
- Internet Protocol

Cualquier frame recibido en la interfaz puede ser usado para detectar la estación de origen

Identificación

Introducción

- La detección en capa 2 solamente deja una lista de MAC address
  - Generalmente no es muy interesante
  - Para obtener esa lista alcanza con Wireshark
- Se pueden obtener datos de capa 3 analizando los datos de los paquetes capturados

Qué conviene capturar

- Tráfico local
  - Hacerlo mal nos puede dar como resultado que toda la Internet esta en nuestra LAN
- No ruteable
  - La mejor forma de asegurarnos que sea local
- Tráfico no IP
  - ARP es un excelente candidato

Qué conviene capturar

- Address Resolution Protocol
- IP Multicast/Broadcast
- Spanning Tree
- Cisco Discovery Protocol
- Cualquier protocolo que sirva para un ID
  - NetBEUI

Address Resolution Protocol

- No ruteable
- Tiene una dirección IP confiable
  - Es la dirección de origen, que la revela el mismo host
- Tiene una segunda posible dirección IP
  - La dirección de destino
- Revela parte de la máscara de red
  - El origen y el destino están en la misma red
- Lo más parecido a un protocolo obligatorio

IP Local Broadcast

- No ruteable
- Tiene una dirección IP confiable
  - La dirección de origen de IP
- No aporta información de la red
  - Salvo por la dirección de origen
- Muy común en protocolos de discovery
  - NBNS

IP Multicast

- Puede ser local o remoto
  - La dirección de destino determina esto
- Una dirección confiable
  - La de origen en el header IP
- No aporta información sobre la red
- Usado en protocolos de discovery
  - mDNS
  - SSDP

IP Broadcast

- Muy común
- Muy dificil de determinar si es un broadcast sin conocer la máscara de red
  - Si se puede garantizar que es un broadcast, se obtienen todos los parámetros de red
- Problemático
  - Usualmente es local, pero hay aplicaciones que transmiten broadcasts dirigidos

Porqué esto funciona

- Generalmente la detección pasiva se basa en broadcasts periódicos de las estaciones
  - Las estaciones necesitan hacer pedidos ARP para poder comunicarse
  - Varios servicios envían periodicamente mensajes de discovery
- Generalmente no se ve la comunicación unicast (host a host)

Detalles de furtivismo

- Los dos tipos de IP broadcast y los pedidos ARP son enviados a ff:ff:ff:ff:ff:ff
  - No requieren modo promiscuo
- Los multicasts son enviados a una dirección multicast
  - Algunos switches lo repiten en todas las interfaces
  - Modo promiscuo es conveniente, pero no necesario
- En ambos casos no se asume que se conoce ningún parámetro de la red
  - El stack TCP/IP está inactivo
  - Aunque la interfaz esté en modo promiscuo, no se dan las condiciones para que los métodos de detección funcionen

Ejemplo

Ejemplo: estado inicial

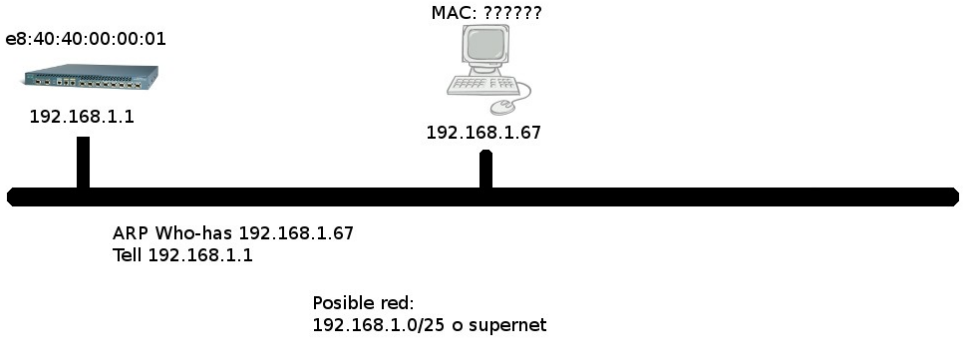
- No hay datos sobre la red
- No hay información sobre los hosts

Ejemplo: CDP

- Se recibe un paquete multicast de CDP
  - CDP no es interpretado, pero la MAC address muestra que es un dispositivo Cisco
- Si interpretáramos CDP, obtendríamos el tipo exacto y la dirección IP

Ejemplo: ARP

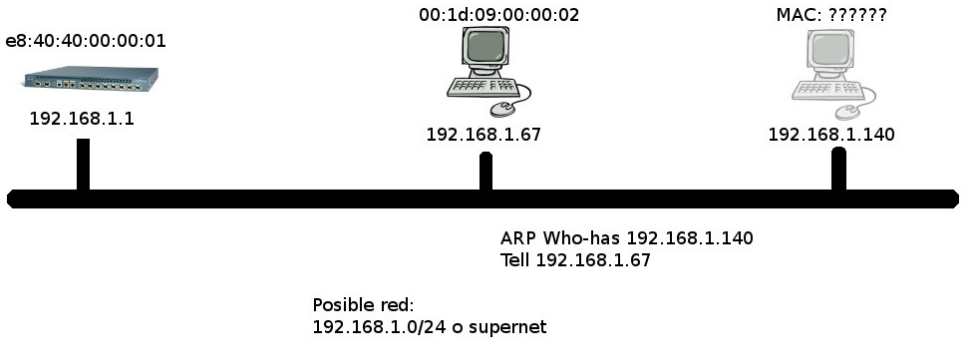
- Se recibe un paquete broadcast de ARP
  - Este paquete nos confirma la dirección IP del router
  - También nos da la dirección de una posible estación
- Todavia no podemos asegurar que 192.168.1.67 exista
- Si el origen y el destino están en la misma LAN, la red debe ser 192.168.1.0/25 o una supernet



CORE SECURITY

Ejemplo: ARP

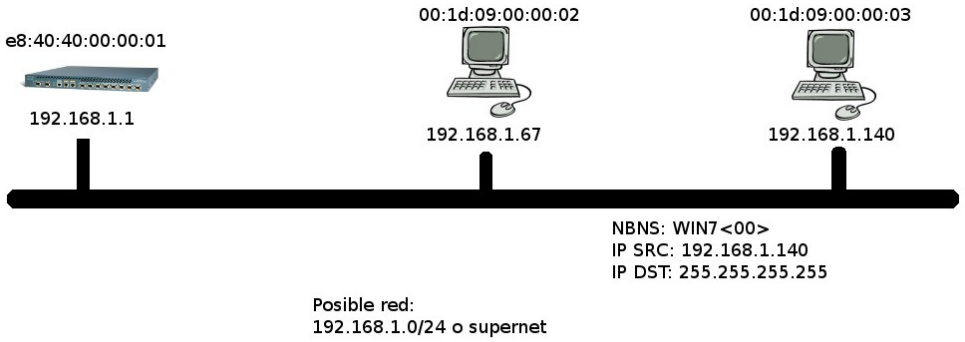
- Se recibe un pedido ARP
  - La MAC address identifica a 192.168.1.67 como un dispositivo DELL
- Ahora sabemos que la red es /24 o una supernet
- No podemos confirmar la existencia de 192.168.1.140



CORE SECURITY

Ejemplo: IP Local Bcast

- 192.168.1.140 emite un broadcast local de NBNS
  - No interpretamos NBNS, pero confirmamos que 192.168.1.140 existe
- La MAC address nos indica que es otro dispositivo DELL



Preguntas?

Muchas Gracias