Manipulación de paquetes sobre redes inalámbricas

GULTEC

inSEC // breaking IT

Rodolfo Wilhelmy <rwilhelmy@itesm.mx>

Disclaimer

- Toda la información y técnicas mostradas en esta presentación son con fines meramente educativos y para realizarse en ambientes autorizados.
- Este grupo y sus participantes, así como los expositores y el mismo Tecnológico de Monterrey se desligan de cualquier responsabilidad por la práctica ilegal, daños a la información y pérdida de dinero, causada por el mal uso de lo que a continuación se presenta.

Introducción

CONCEPTOS BÁSICOS

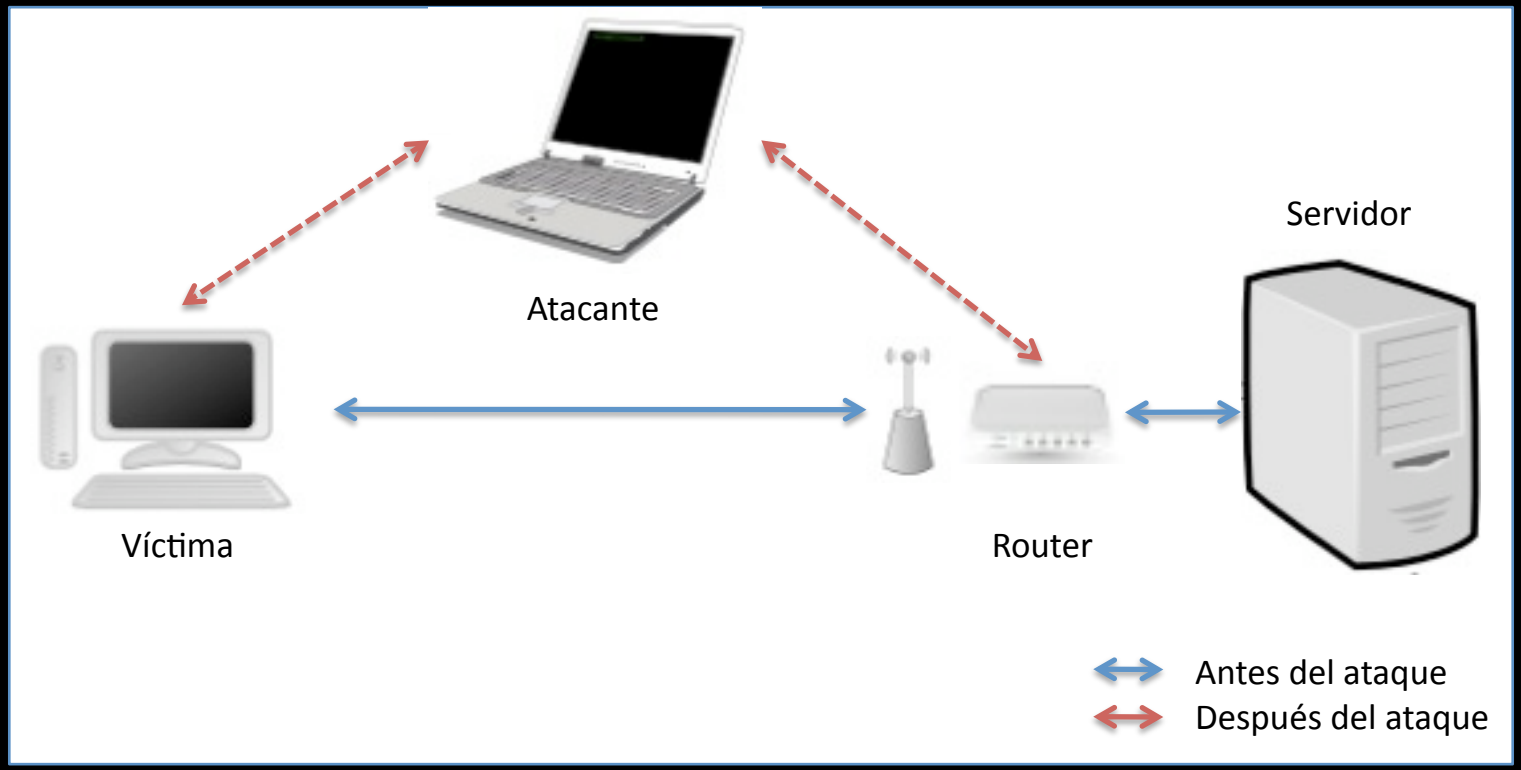
Escuchando la Red

- *Sniffing*: recopilar tráfico de la red local desde la capa de enlace de datos (capa 2 del modelo OSI). Usando un *sniffer*, un atacante o un administrador puede leer toda la información que se transmite en la red.
  - *Passive Sniffing (Hubs y WiFi)*
  - *Active Sniffing (Switch): MAC Flooding, Spoofed ARP Messages.*

ARP: Address Resolution Protocol

- Cuando una máquina quiere comunicarse con otra en la red local, debe averiguar su dirección física.
- Para esto genera un ARP Query, que básicamente pregunta a todas las máquinas ¿quién tiene la dirección MAC (física) asociada con tal IP?
- La máquina correspondiente contestará con un ARP Response con la dirección física y está última será guardada en la tabla ARP (ARP Cache) de quien preguntó.
- El grave problema de este protocolo, es que **no valida** quién realizó la respuesta ARP.

MAN-IN-THE-MIDDLE ATTACK


Atacante
Servidor
Víctima
Router
Antes del ataque
Después del ataque

ARP Poisoning

- Técnica para sobrescribir el cache ARP de la víctima con la intención de que su tráfico sea destinado al atacante, en lugar del *gateway*.

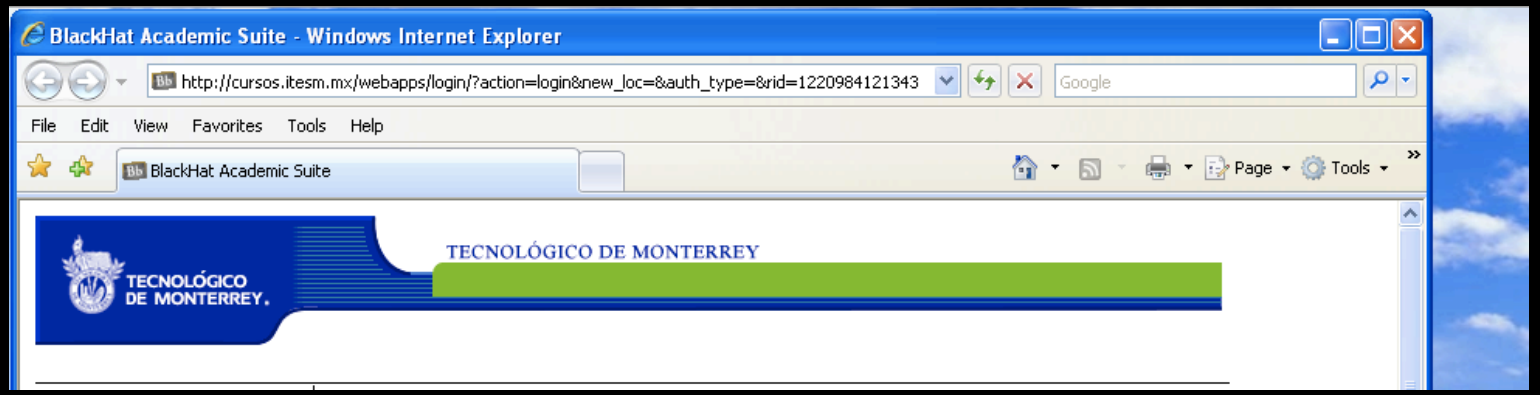
1. El atacante activa *IP Forwarding* en su sistema operativo para permitir el reenvió del tráfico de la víctima a su destino original, con la intención de evitar un DoS.
2. Envió de respuestas ARP falsas a la víctima, para reasociar la IP del router *default* con la dirección física del atacante.
3. La víctima transmite tráfico, destinado al mundo exterior, al atacante. Basándose en su tabla ARP envenenada.
4. Se lee la información de dicho enlace.
5. Los paquetes son enviados del atacante hacia el gateway default para ser enviados al mundo exterior.

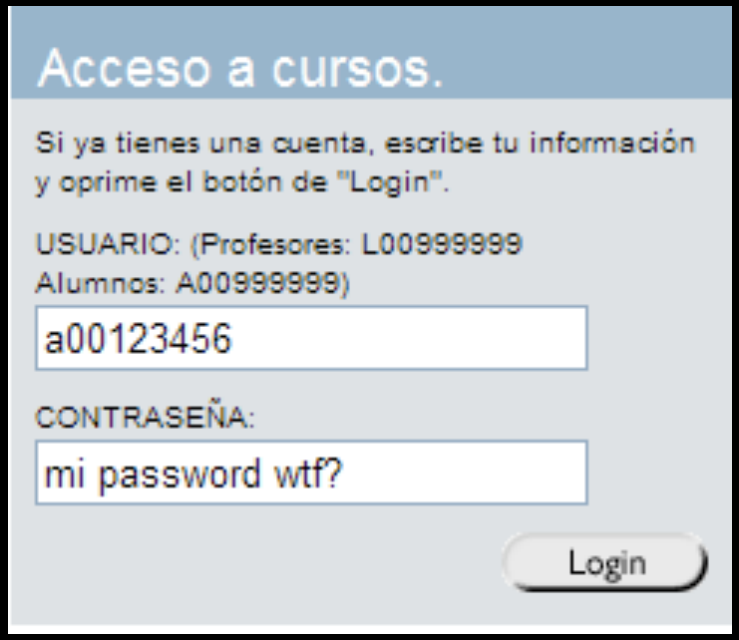
1085	133.678810	Vmware_29:96:05	Vmware_b3:c7:c2	ARP	172.16.237.2 is at 00:0c:29:29:96:05
1086	133.678966	Vmware_29:96:05	Vmware_f8:15:70	ARP	172.16.237.128 is at 00:0c:29:29:96:05
1087	133.690364	Vmware_29:96:05	Vmware_f8:15:70	ARP	172.16.237.128 is at 00:0c:29:29:96:05
1088	133.690510	Vmware_29:96:05	Vmware_b3:c7:c2	ARP	172.16.237.2 is at 00:0c:29:29:96:05

Ettercap

- Sniffer de nacimiento, pero rediseñado para realizar ataques MITM. Sirve de intermediario entre la comunicación de dos máquinas realizando ARP poisoning.
- Características:
  - Filtrado de paquetes. Se pueden buscar *strings* particulares dentro del TCP o UDP *payload* y ser reemplazados
  - Sniffing de tráfico a través de túneles
  - Soporte para SSH y SSL
  - Inyección de caracteres en una comunicación
  - Detección pasiva de SO
  - Recolección de passwords: FTP, SSH, MySQL, MSN, etc.

¿Qué hay de extraño en las siguientes imágenes?





Manipulación de paquetes

- Con ettercap y etterfilter podemos desarrollar filtros que identifiquen ciertos patrones en los paquetes que van hacia el cliente y reemplacen los datos en ellos.
- Ejemplos:
  - Cambiar imágenes o elementos de las páginas
  - Agregar código malicioso (JavaScript, PHP, Flash, etc.)

```
if (ip.proto == TCP && tcp.src == 80) {
  replace("Blackboard Academic", "BlackHat Academic  ");
}
```

DNS Spoofing

- Con el plugin dns_spoof de ettercap, podemos falsificar las respuestas DNS a una víctima.
  - *Pharming*: redirección de un sitio a otro malicioso, mediante el envenenamiento de las peticiones DNS, parecido a ARP Poisoning pero involucrando Ips y hostnames.
  - DoS: interrupción del servicio
  - Robos de sesiones, información, etc.

Blackboard, MSN, DNS, SSL

DEMOS