UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

DEPARTAMENTO DE ELECTRONICA

VALPARAISO - CHILE



SEGURIDAD EN REDES TCP

ANGEL ANDRADE

201521063-2

ING CIVIL ELECTRONICA

**Resumen**

Se analizarán las distintas formas de ataques informáticos efectuados en redes tcp/ip y ciertas protecciones contra estos. En cada caso se hará una breve descripción del tipo de ataque y se verá si es posible o no interceptarlo de manera satisfactoria.

**Sniffing**

Este ataque consiste en supervisar el tráfico generado en una red.

El elemento utilizado para escuchar todo lo que se mueve por la red se denomina sniffer o analizador de red, que puede ser tanto software como hardware

El software utilizado como sniffer activa lo que se conoce como “modo promiscuo de la tarjeta de red” en la máquina donde se ejecuta, lo que permite obtener todas las tramas Ethernet que se envían dentro de la misma Red de Área Local

Los sniffers activan este modo de manera automática

Actualmente, las conexiones a través de cable se llevan a cabo mediante switches, en lugar de los antiguos hubs, lo que hace que el tráfico sea dirigido a su destino, de forma que se complica el uso de sniffers

Para la escucha en redes inalámbricas el sniffing sigue siendo muy eficaz y utilizado

**Proposito de los Sniffers**

Analizar el tráfico de red dentro de nuestra empresa o de nuestro hogar para poder encontrar incidencias, como congestiones en la red, cuellos de botella, intrusiones, etc.

Detectar fallos en los paquetes, ya sea porque llegan corruptos, no llegan las tramas de confirmación o se duplican

Convertir el tráfico que viaja por la red (ceros y unos) en señales analógicas comprensibles para el humano

Crear ficheros con las capturas realizadas y establecer filtros sobre ellas para ver lo que queramos en concreto, y así analizar el tráfico de la red

Crear estadísticas y gráficos de todo tipo, por ejemplo por tipo de protocolo, por dirección IP, por dirección MAC, …

Capturar nombres de usuario y contraseñas que viajan por la red sin encriptar

**Protección contra sniffers**

Hacer uso de otros sniffers

Utilizar switches

Utilizar firewalls

Encriptar la información que viaja por la red

SSL (Secure Sockets Layer), para el caso de la Web

PGP (Pretty Good Privacy) y S/MIME (Secure Multipurpose Internet Mail Extensions), para el caso del correo electrónico

SSH (Secure SHell), para el caso del acceso remoto a servidores UNIX

VPN (Virtual Private Network)

**Spoofing**

Este ataque consiste en suplantar la identidad de otra máquina de la red para tener acceso a los recursos de un tercer sistema de manera maliciosa, basándose en algún tipo de confianza, ya sea el nombre o la dirección IP del host suplantado

Las técnicas de spoofing van desde engañar al propio servidor falseando simplemente una dirección IP, hasta lo que sería engañar directamente al usuario final (entrando ya en Ingeniería Social)

Uno de los ejemplos más típicos de spoofing es el phishing

Existen varias técnicas de spoofing:

* IP Spoofing
* ARP Spoofing
* DNS Spoofing

En un ataque de tipo spoofing existen tres máquinas en juego:

1. Máquina atacante
2. Máquina atacada
3. Máquina a suplantar

**IP Spoofing**

Esta técnica consiste en conseguir una dirección IP de un host o un servidor, y hacerse pasar por él con el objetivo de obtener información confidencial o provocar un ataque DoS

La dirección IP la sustituimos dentro de un paquete TCP/IP, como pueden ser los clásicos ICMP, UDP o TCP, y el sistema atacado responderá a esta dirección suplantada, no a la nuestra

Un ejemplo de ataque IP Spoofing consistiría en mandar un ping con la dirección IP origen falseada. El host atacado respondería al ping, lo que provocaría que el sistema suplantado recibiera respuesta sin haberla solicitado

Hoy en día un ataque clásico de IP Spoofing es bastate difícil de conseguir, ya que los enrutadores actuales no permiten que se envíen paquetes con direciones IP que no pertenezcan a la red, por lo que los paquetes que intentemos mandar no van a pasar del router

**ARP Spoofing**

Consiste en la construcción de tramas ARP de solicitud y respuesta falseadas, de manera que se fuerce al host atacado a enviar los paquetes al atacante en vez de hacerlos directamente al sistema de destino

Las comunicaciones TCP/IP se basan en la resolución de la dirección IP en función de la dirección MAC y, para ello, en nuestra máquina residen tablas ARP que asocian las direcciones MAC con las direcciones IP de la red. Este ataque trataría de falsear estas direcciones MAC basándose en el envenenamiento de la tabla ARP (ARP Poisoning)

Para ver la tabla ARP de nuestro equipo ejecutamos el comando arp –a desde una consola o terminal

Las tarjetas de red en nuestro equipo se visualizan ejecutando el comando ipconfig /all (Windows) o ifconfig –a (Linux) desde una consola o terminal

Cuando una máquina de la red necesita resolver una dirección IP, hace un ARP request a la red preguntando por dicha dirección IP. Cuando la máquina con esa dirección IP recibe la petición, hace un ARP reply con su dirección MAC

Un típico ataque ARP Spoofing es Man In The Middle. El atacante recoge la información del atacado y se la envía al equipo suplantado para que parezca que se trata de una comunicación normal

La única manera de detectar este ataque sería analizando el tráfico de red y viendo que existen dos máquinas con diferentes direcciones IP y con las mismas direcciones MAC

Haciendo este ataque conseguimos ver todo el tráfico que va dirigido de una máquina a otra. Si las conexiones que se realizan entre ambas no van cifradas, podríamos obtener información confidencial mediante el uso de un sniffer

**DNS Spoofing**

Trata de asociar el nombre del dominio de una página web con la dirección IP de una máquina que no es la real, es decir, engañar al usuario final con una dirección IP de un servidor donde se alojaría otra página web

Este ataque podría también realizarse de manera más facil si directamente pudiéramos acceder al fichero de asociación de DNS de un host en concreto (C:\Windows\System32\drivers\etc\hosts)

También se podría comprometer un servidor DNS infectando la caché de otro, es decir, haciendo lo que se conoce como Envenenamiento DNS o DNS Poisoning

**DoS**

DoS (Denial of Service -Denegación de Servicio-) es un ataque dirigido a una máquina, o conjunto de máquinas, con el objetivo de terminar parcial o totalmente con los servicios que ofrece

El ataque DoS se basa en intentar consumir todos los recursos de una máquina (ancho de banda o ciclos de procesador) sin dejar espacio libre para peticiones legítimas

**DDoS**

En el ataque DoS tradicional, una máquina lanza el ataque a otra; en el ataque DDoS (Distributed Denial of Service -Denegación de Servicio Distribuida-) es un conjunto de máquinas distribuidas las que apuntan a un mismo objetivo

Este tipo de ataque se suele hacer mediante botnets, conjunto de máquinas robots que se pueden ejecutar de manera autónoma, pero controlada por otra

Normalmente, se infectan varias máquinas dispersadas geográficamente (máquinas zombies) y se lanza el ataque desde todas ellas, muy difícil de interceptar

**Métodos de ataque DoS**

**Dirigidos a consumo de ancho de banda:**

* Inundación ICMP (ICMP Flood)
* Smurf
* Inundación UDP (UDP Flood)
* Fraggle

**Dirigidos a atacar la conectividad:**

* Inundación SYN (SYN Flood)

**ICMP Flood**

Inundación ICMP, Ping Flood o ICMP Flood es un ataque, por lo general DDoS, que trata de saturar la red con un gran número de paquetes ICMP

Una manera de realizar este ataque es mediante botnets. Si conseguimos instalar un ping flooder en multitud de máquinas y ejecutamos el ping flood desde todas esas máquinas de manera simultánea hacia un servidor, probablemente se colapsará y se producirá la denegación del servicio

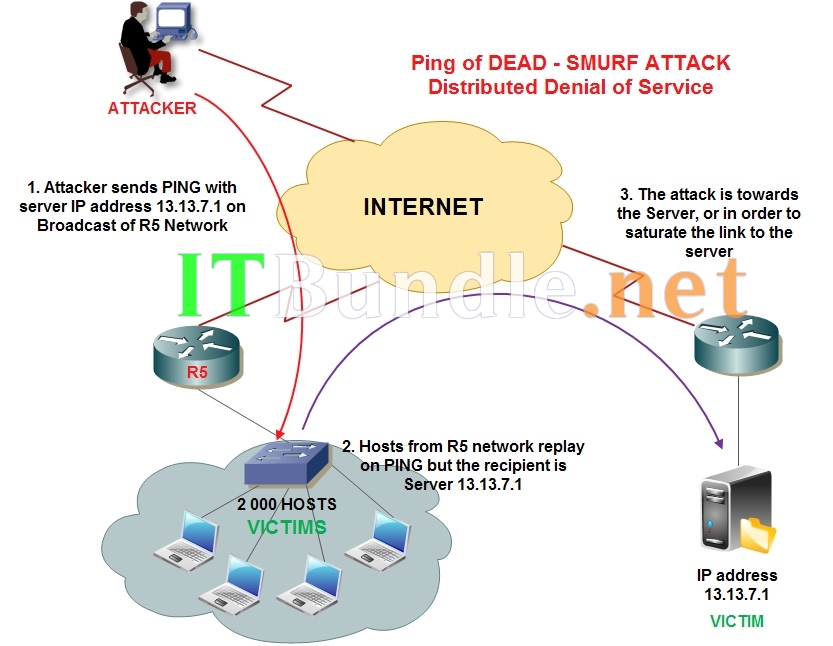
**Smurf**

Versión de ICMP Flood que utiliza también la inundación por ping, pero se envía a toda la red, es decir, el efecto que tiene el ataque está amplificado

Se basa en el uso de servidores de difusión para poder analizar una red entera

Pasos del ataque:

1. El atacante envía una solicitud echo request mediante un ping a uno o varios servidores de difusión falsificando la dirección IP origen por el de la víctima
2. El servidor lo envía al resto de la red
3. Las máquinas de la red responden al servidor
4. El servidor de difusión envía la respuesta al equipo destino



**UDP Flood**

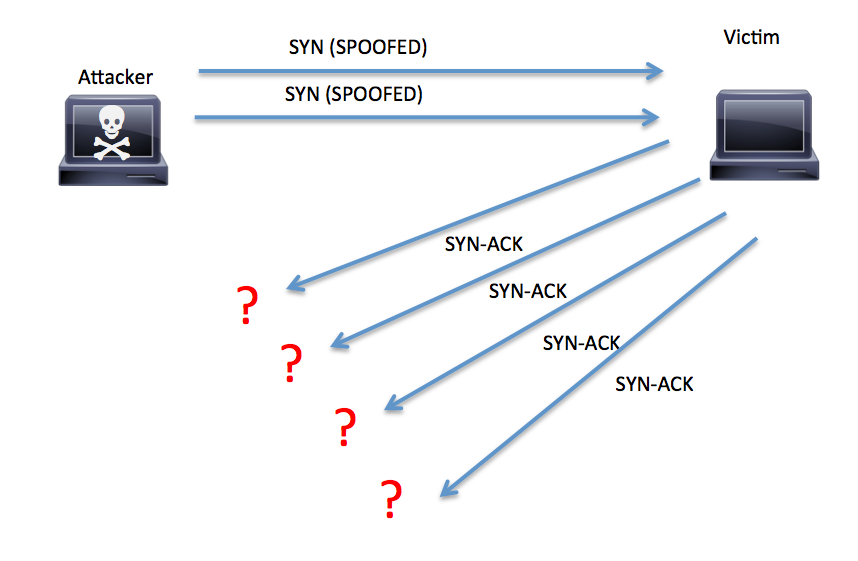
Este ataque consiste en generar grandes cantidades  
de paquetes UDP contra la víctima elegida

**Fraggle**

Ataque similar al Smurf, pero haciendo uso de  
paquetes UDP en lugar de ICMP

**SYN Flood**

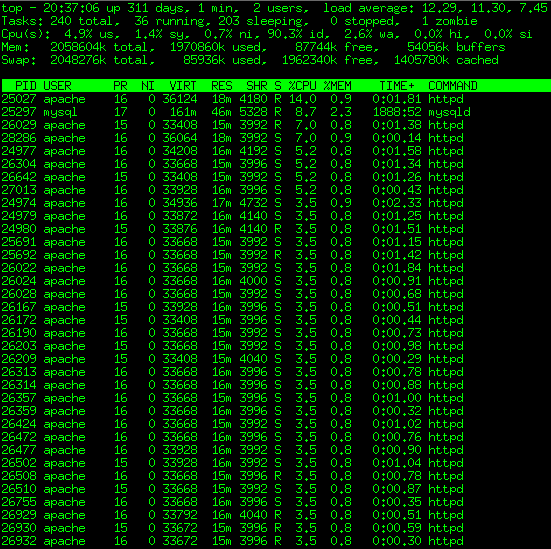
Ataque DoS que consiste en saturar el tráfico de red  
aprovechando el mecanismo de negociación Threeway handshake que realiza el protocolo TCP al iniciar una conexión

Consiste en enviar a una máquina (normalmente un servidor) muchas solicitudes SYN con una dirección de usuario inexistente, lo que causa que la máquina atacada se quede en espera del ACK que mandaría el supuesto usuari

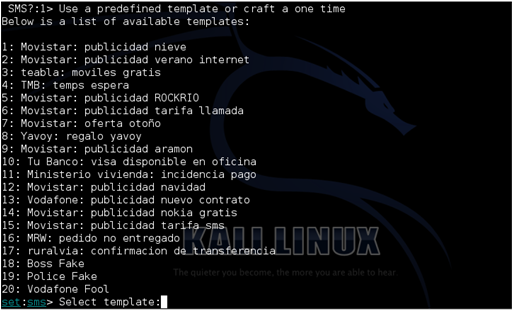
Capturas de pantalla:

Nota para el evaluador: Estas imágenes son para fines ilustrativos con el fin de mostrar que es lo que ve el usuario en cada ataque.

**Ataque DDoS**



**Servidor siendo atacado, en la imagen puede observarse el número de conexiones mantenidas por el servidor (240), en este caso el ataque se efectúa desde servidores web Apache.**



**Captura antes de efectuar un ataque spoofing (SMS Spoofing), bajo la plataforma de Kali Linux, el atacante ahora solo tiene que elegir que texto insertar en el SMS, si el atacante tiene éxito el afectado responderá con información de interés para el atacante.**

**Bibliografia**

* García-Moran, J.P.; Fernández Hansen, Y.;  
  Martínez Sánchez, R.; Ochoa Martín, Ángel;  
  Ramos Varón, A.A.: “Hacking y Seguridad en  
  Internet. Edición 2011”. Ra-Ma. 2011
* Jimeno García, M.T.; Míguez Pérez, C.; Heredia  
  Soler, E.; Caballero Velasco, M.A.: “Destripa la  
  Red. Edición 2011”. ANAYA MULTIMEDIA.  
  2011
* Analizador de paquetes. En Wikipedia. Recuperado el 19 de mayo del 2016 de <https://es.wikipedia.org/wiki/Analizador_de_paquetes>
* Transmission control protocol. En Wikipedia. Recuperado el 19 de mayo del 2016 de <https://es.wikipedia.org/wiki/Transmission_Control_Protocol>
* Spoofing. En Wikipedia. Recuperado el 19 de mayo del 2016 de <https://es.wikipedia.org/wiki/Spoofing>
* DDos. En Wikipedia. Recuperado el 19 de mayo del 2016 de <https://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio>
* ICMP. En Wikipedia. Recuperado el 19 de mayo del 2016 de https://es.wikipedia.org/wiki/Internet\_Control\_Message\_Protocol