**Evaluación Contínua 1.1 - Redes y Sistemas**

**Chequeado**

Alumno: Gonzalo Benito

Email: [gu4n4rt@gmail.com](mailto:gu4n4rt@gmail.com)

**1. Dibuja los modelos OSI y TCP/IP e indica mediante colores la equivalencia de los niveles de ambos modelos.**

|  |  |
| --- | --- |
| OSI Model | TCP/IP Model |
| Capa de Aplicación | Capa de Aplicación |
| Capa de Presentación |
| Capa de Sesión |
| Capa de Transporte | Capa de Transporte |
| Capa de Red | Capa de Internet |
| Capa de Enlace | Capa de  Acceso a la Red |
| Capa Física |

**2. Indica los puertos y protocolos de capa de transporte que usan los siguientes protocolos: HTTP, HTTPS, DNS, SSH**

* HTTP - TCP 80
* HTTPS - TCP 443
* DNS - TCP/UDP 53
* SSH - TCP/UDP 22

**3. Explica y razona cómo realiza la retransmisión de los paquetes el protocolo UDP, cuando no se ha recibido un ACK pasados “5 tics”**

Las conexiones mediante el protocolo UDP, no utilizan el mensaje de respuesta ACK. La razón de esto es su naturaleza no fiable, puesto que no posee mecanismos que permitan el reenvío de información en caso de que los paquetes no lleguen al destino (característica que sí posee TCP).

**4. ¿Qué máscara de red (la más ajustada) debería usar si quiero disponer de, al menos, 63 máquinas conectadas a la red?**

La máscara de red que debería usar es 255.255.255.128.

No utilizamos la máscara 255.255.255.192, puesto que de las 64 direcciones que poseen las subredes, 2 están reservadas (Network ID y Broadcast), por lo que en total podremos disponer de un máximo de 62 máquinas.

**5. Explica detalladamente (y dibuja) como se establece una conexión TCP.**

El establecimiento de una conexión TCP se realiza mediante el protocolo de tres vías o *three-way handshake,* un proceso mediante el cual los dos dispositivos partícipes intercambian información (negociación) para iniciar una sesión o canal de comunicación.

El mismo consta de tres fases (en orden):

1. SYN (*synchronization*): el dispositivo emisor, cliente u origen envía un paquete con un bit de control SYN al servidor y un número de secuencia. Envía una solicitud para iniciar una comunicación con el servidor y sincronizar los números de secuencia.

2. SYN-ACK (*synchronization-acknowledgment*): el servidor recibe la petición SYN del cliente, y responde con un paquete con los bits de control:

* ACK, como acuse de recibo, que incluye un número de reconocimiento o *acknowledgment*, equivalente al incremento en 1 del número de secuencia recibido del paquete SYN. Por ejemplo, si recibe un número de secuencia 2001, responde con un 2002.
* SYN, que incluye el número de secuencia del servidor.

3. ACK (acknowledgment): el cliente recibe y responde el SYN-ACK enviado por el servidor, mediante otro ACK (también con un número equivalente al incremento en 1 del número de secuencia recibido), con el que se confirma la sincronización entre ambas partes.



Una vez finalizado el handshake, comienza la transmisión de los datos, hasta que la misma finaliza y se cierran las sesiones y la conexión (esto no es parte del proceso de establecimiento de la conexión)

**6. Representa la IP 192.168.1.23 con máscara 255.255.192.0 en notación CIDR**

192.168.1.23/18

**7. Define, con tus propias palabras, los siguientes conceptos:**

**Switch**: es un dispositivo de red que permite conectar distintos dispositivos en una red, para que puedan intercomunicarse.

**Router**: es un dispositivo de red que permite el enrutamiento de los datos de una red hacia otra. De esta manera, se podrá realizar el intercambio de datos entre dispositivos de redes diferentes.

**Firewall**: es un hardware o software diseñado para permitir o bloquear conexiones (entrantes o salientes) entre dos equipos mediante reglas.

**NAT** (Network Address Translation): es un mecanismo por el cual los routers “traducen” las direcciones IP privadas de los dispositivos de una red, de manera que las conexiones hacia otra red (por ejemplo, Internet) se realicen mediante una única IP pública compartida por todos los dispositivos de la red privada.

También hace una “traducción” de los puertos, de manera que varios dispositivos puedan utilizar un mismo puerto local, pero de cara a la siguiente red, elegirá un puerto externo distinto a utilizar.

**8. Dado el siguiente paquete IP (paquete teórico), indica cuales son las direcciones IP y puertos se están comunicando, así como el protocolo de capa 7 que se seguramente se esté empleando. Además, indica cuantos “saltos” dará el paquete antes de descartarse**



Direcciones IP:

* Source: 192.168.4.59
* Destination: 2.212.13.165

Puertos:

* Source: 34908
* Destination: 22

Protocolo de capa 7: SSH

TTL: 2

**9. Dada la red 192.160.0.0/11, indica y razona:**

a. **La máscara de red** - 255.224.0.0

La notación CIDR expresa la cantidad de bits utilizados para identificar la dirección de red (11).

En binario se expresaría como 11111111.11100000.00000000.00000000

Como las direcciones IP se dividen en 4 octetos, los primeros 8 bits “encendidos” (los 1, que identifican a la red) en notación decimal se expresan como 255, o 11111111 en binario.

Los 3 bits del segundo octeto (11100000), pertenecientes al segundo octeto, también forman parte de los bits que identifican a la red.

Por el contrario, todos los bits restantes (21) serán ceros que identificarán a los hosts.

b. **El número de host disponibles** - 2.097.150

La cantidad de hosts está determinada por la máscara de red, la cual indica, en este caso, 21 bits para las direcciones de host.

Por lo tanto, el cálculo de direcciones de host disponibles es:

221 - 2 = 2.097.152 - 2 => 2.097.150

Las dos direcciones que restamos son la dirección de red y la dirección de broadcast.

c. **La dirección de broadcast** - 192.191.255.255

La dirección de broadcast es la dirección más grande dentro de una red, o, mejor dicho, es la que posee todos los bits de host en 1.

De esta manera, la dirección de broadcast será:

|  |  |  |  |
| --- | --- | --- | --- |
| Octeto 1 | Octeto 2 | Octeto 3 | Octeto 4 |
| 11000000 | 10111111 | 11111111 | 11111111 |
| 192 | 191 | 255 | 255 |

\*En amarillo se indican los bits de red, y sin color los bits de host.

d. **Calcula si 192.191.13.80 y 192.168.90.45 están en la misma red**

Si, están en la misma red. El rango de direcciones IP es:

192.160.0.0 - 192.191.255.255

Ambas direcciones se encuentran dentro de este rango, por lo que pertenecen a la misma red.

**10. Enumera y explica detalladamente (con tus propias palabras) todos los ataques de red que conoces, tanto para IPv4 como para IPv6**

**VLAN Hopping**

Este ataque aprovecha vulnerabilidades en la conexión por puertos troncales en los switch para tener acceso a una VLAN a la que no está autorizado.

Utilizamos la técnica de doble etiquetado, que consiste en utilizar dos etiquetas VLAN ID en un paquete dirigido a un switch: la primera con el ID de una VLAN nativa (en routers Cisco, de manera predeterminada la 1), y la segunda con el ID de la VLAN objetivo.

Cuando el switch recibe el paquete, elimina la primer etiqueta y lo reenvía a los demás switches de la VLAN 1 o nativa. Esos switches recibirán el paquete con la segunda etiqueta, interpretando que el paquete tiene como destino la VLAN especificada, por lo que lo reenvía a dicha VLAN que, en principio, no poseía acceso.

*Todos los siguientes ataques son variantes de un ataque MITM o se encuentran relacionados con el mismo.*

**Man In The Middle**

Un ataque Man In The Middle se da cuando una máquina atacante se interpone en la comunicación de dos máquinas víctimas pertenecientes a su misma red, pudiendo interceptar el tráfico, leerlo, manipularlo (Network Packet Manipulation), redirigirlo o enrutarlo, o descartarlo (produciendo una denegación de servicio, por ejemplo).

Existen varias técnicas que pueden colocar al atacante en esa posición de intermediario, como ARP Spoofing o ataques a DHCP.

De este ataque se derivan otros, como DNS Spoofing

**ARP Poisoning o ARP Spoofing**

Podríamos considerarlos como dos ataques distintos, o simplemente como el mismo. Para fines explicativos, lo dividiré en dos partes.

El primero, ARP Poisoning, alude al acto de “envenenar” las tablas ARP o caché ARP de las máquinas víctimas para que se corrompan, y luego poder realizar la suplantación. Esto se realiza enviando mensajes ARP falsos a la víctima, de manera que su tabla ARP se llene y tengamos la oportunidad de agregar un registro con nuestra dirección (spoofing).

Mientras que el segundo, ARP Spoofing, hace referencia al acto de suplantar la dirección MAC de otra máquina dentro de la red una vez las tablas ARP de las víctimas fueron corrompidas.

Para realizar un ataque MITM, por un lado, el atacante suplanta la identidad de la víctima en la red, por lo que los demás dispositivos creerán que el atacante es la máquina verdadera. Por otro lado, la víctima creerá que la dirección del atacante es, por ejemplo, la gateway, logrando que todo el tráfico en ambas direcciones pase por él.

**DNS Spoofing**

Las solicitudes DNS pueden ser interceptadas y modificadas durante un ataque MITM, permitiendo al atacante falsificar respuestas DNS bajo determinadas reglas o registros DNS (e.g archivos *hosts*), devolviendo a la víctima un registro malicioso con una dirección IP arbitraria que, generalmente, la redirige hacia un sitio web malicioso para realizar, por ejemplo, un ataque de phishing, entre otros.

**IP Spoofing**

Mediante este ataque, cambiamos la IP arbitrariamente, de manera que el receptor de nuestros paquetes crea que somos otro dispositivo.

Esto tiene varias aplicaciones, pero la más común es para realizar un *ataque de amplificación.*

**Ataques de Amplificación (en protocolo DNS)**

Estos ataques se implementan en el protocolo UDP, ya que, al no estar orientado a conexión, el receptor de los paquetes contestará en caso de tener el puerto receptor en escucha (abierto).

Así, simplemente debemos enviar consultas a un servidor DNS en nombre de la IP de la máquina víctima, solicitando todos los registros DNS disponibles (consulta ANY) al servidor DNS, que posteriormente enviará la respuesta hacia la víctima.

La razón de la consulta ANY radica en que, una solicitud DNS posee menos datos (y, por ende, consume menos ancho de banda) que la respuesta con los todos los registros de un dominio. A esto lo podemos considerar como amplificación: ingresamos una cantidad pequeña de datos, y como salida obtenemos una cantidad significativamente mayor.

Dependiendo de la cantidad de solicitudes realizadas, podremos realizar un ataque más o menos potente, saturando en mayor o menor medida el ancho de banda de la red y al dispositivo víctima.

Como el tráfico será redirigido hacia la víctima, en consecuencia, podríamos conseguir una denegación de servicio (**DoS**).

**Envenenamiento de Caché (IPv6)**

Podríamos considerarlo el equivalente a ARP Poisoning, pero en redes IPv6. La diferencia está en el protocolo utilizado: ICMPv6.

El funcionamiento de este protocolo para averiguar las direcciones MAC también es muy similar a ARP, por lo que su explotación para obtener un MITM mantiene los mismos principios.

El emisor envía un mensaje “Neighbor Solicitation” a la dirección multicast consultando la dirección MAC de una máquina, que, al recibirlo, responderá de vuelta con un mensaje “Neighbor Advertisment” y su MAC, para que el emisor la almacene en su tabla.

Este último mensaje es el que aprovecharemos para el Cache Poisoning, enviando al multicast varios mensajes maliciosos para actualizar las tablas caché de las víctimas con la MAC del atacante.

**DHCP Attacks**

Teniendo en cuenta la función básica de un servidor DHCP en una red, y otras características particulares (como que, si en una red existen dos servidores DHCP, el que responda la petición de una máquina primero, le proporcionará su propia configuración).

Partiendo de esto, si el atacante implementa un servidor DHCP, podría asignar una configuración arbitraria a las máquinas de la red que la soliciten (como su gateway, servidor DNS, o su dirección IP).

El proceso de configuración de una máquina en una red mediante DHCP, consiste en:

* El cliente envía un paquete DISCOVERY al servidor, solicitando la configuración.
* El servidor responde con un paquete OFFER con la configuración que le asignará al cliente.
* El cliente elige y acepta la configuración mediante un paquete REQUEST.
* El servidor reconoce mediante un paquete DHCP ACK la configuración y la reserva.

Durante este proceso pueden surgir complicaciones, como la falta de información de las IPs que podemos asignar. Por ello, surgen variantes del ataque que actúan respondiendo paquetes a la mitad del proceso de negociación entre un servidor DHCP legítimo y el cliente. Esto es posible porque la comunicación DHCP funciona enviando paquetes a la dirección de *broadcast*.

Variante DHCP ACL Injection

Esta variante funciona en la etapa final de la configuración, monitoreando la red en busca de peticiones, para luego enviar un paquete DHCP ACK malicioso con nuestra configuración, de manera que llegue antes que el paquete DHCP ACK legítimo.

**Ataques SLAAC (IPv6)**

Este ataque explota una funcionalidad propia de las redes IPv6: la capacidad de que un router de proporcionar la configuración de red a una máquina. Además, por defecto muchos sistemas operativos prefieren utilizar el protocolo IPv6 de ser posible, lo que propicia el escenario perfecto para el ataque.

Teniendo en cuenta que el router cumple la función de servidor DHCP, podríamos explotar esto de manera similar a un ataque DHCP, teniendo en cuenta ciertos aspectos importantes:

* Para realizar un MITM, deberemos también realizar la función de router, enrutando el tráfico IPv6 de la red hacia Internet, que funciona sobre IPv4.
* Debemos realizar la conversión de IPv4 a IPv6 y viceversa, a través de un mecanismo llamado NAT-PT (actualmente obsoleto, pero que puede ser aprovechado para ataques como este, por ejemplo).
* Para ello, se necesitarán dos interfaces de red, una para la red interna IPv6 y otra para Internet IPv4, y el software adecuado.
* Por último, se debe implementar un servidor proxy DNS para resolver los registros.

Hecho esto, el tráfico pasará por la máquina atacante, y encontrándose en una posición de MITM.