Universidad del Valle de Guatemala
Facultad de Ingeniería
Departamento de Ciencias de la Computación
CC3067 Redes

Laboratorio 8

Seguridad y Redes

1 Objetivos

- Identificar objetivos de seguridad de la información
- Aplicar los conocimientos adquiridos sobre taxonomía de los ataques de red.

2 Desarrollo

2.1 Conceptos de seguridad de la información

Awesome.com es una empresa de retail que vende productos online. Debido a que realiza la entrega de los productos a domicilio, se almacena la dirección, código postal y número de teléfono del domicilio de los clientes. Para comprar, un cliente debe ingresar los datos de su tarjeta de débito/crédito y guardarla como una forma de pago. Actualmente la empresa posee un servidor web Apache que se ejecuta en el puerto 80.

a. ¿Cuál es el objetivo de seguridad principal para la información almacenada de las tarjetas de crédito? ¿Por qué?
b. Indique un control que apoye el objetivo de seguridad planteado en la respuesta anterior y explique en qué forma lo apoya.
c. ¿Cuál es el objetivo de seguridad principal para la información almacenada del domicilio de un cliente? ¿Por qué?
d. Indique un control que apoye el objetivo de seguridad planteado en la respuesta anterior y explique en qué forma lo apoya.
e. Podemos definir el riesgo como la probabilidad que una amenaza se materialice aprovechando una vulnerabilidad en un sistema. Identifique la amenaza, la vulnerabilidad, el riesgo y un posible ataque sobre la información en tránsito entre el dispositivo de un cliente y el servidor web de Awesome.com
f. ¿Cómo se puede mitigar riesgo en el inciso anterior?

2.2 Criptografía

2.2.1 One Time Pad

Alice envía el texto cifrado c1 = 1110010 a Bob utilizando One Time Pad. Eve intercepta el mensaje, pero no puede descifrarlo, solo sabe que Alice y Bob codifican el texto plano en ASCII de 7 bits y luego lo cifran.

Mas tarde, Alice envía un nuevo mensaje a Bob, c2 = 1010011, pero comete el error de utilizar la misma llave que el primer mensaje. Además, Eve se entera que Bob recibió el carácter "H" en el primer mensaje. En OTP, si una llave se utiliza dos veces ocurre lo siguiente para los mensajes m1 y m2, donde:

ci = el i-ésimo texto cifrado
mi = el i-ésimo mensaje
k = llave
$\oplus$ = XOR

c1 = m1 $\oplus$ k
c2 = m2 $\oplus$ k

c1 $\oplus$ c2 = m1 $\oplus$ k $\oplus$ m2 $\oplus$ k (XOR es conmutativo y asociativo)

Debido a que k $\oplus$ k = 0, c1 $\oplus$ c2 = m1 $\oplus$ m2. Esto por si solo no sirve para descifrar el mensaje, pero el atacante conoce más información. Debido a que Eve sabe que el primer mensaje era "H", utilice este conocimiento para descifrar el segundo mensaje. Deje constancia de las operaciones realizadas. ¿Cuál es la palabra que forman ambos mensajes?

2.2.2 Modos de operación para bloques de cifrado

Descargue la imagen tux.bmp de Canvas. Implemente un programa en Python que:

a. Convierta la imagen a bytes (sugerencia, utilice la librería Pillow para cargar la imagen). Utilice numpy para convertir la imagen en bytes, utilice un reshape de 405, 480, 4.
b. Cifre los bytes de la imagen utilizando AES 128 con modo de operación ECB (Electronic Code Book) (sugerencia, utilice la librería Crypto)
c. Convierta los bytes cifrados a una nueva imagen con extensión PNG, utilice RGBA y las dimensiones 405, 480.

Compare la imagen cifrada con la imagen original. ¿Es posible detectar alguna similitud entre ambas imágenes? En caso afirmativo, ¿por qué? ¿Es seguro utilizar este modo de operación?

Ahora, repita el procedimiento anterior, pero esta vez utilice el modo CBC (Cypher Block Chaining), pasando un vector de inicialización. Compare la imagen cifrada con la imagen original. ¿Es posible detectar alguna similitud entre ambas imágenes? En caso afirmativo, ¿por qué? ¿Es seguro utilizar este modo de operación?

2.3 Ataques a la red

2.3.1 Ataques al protocolo

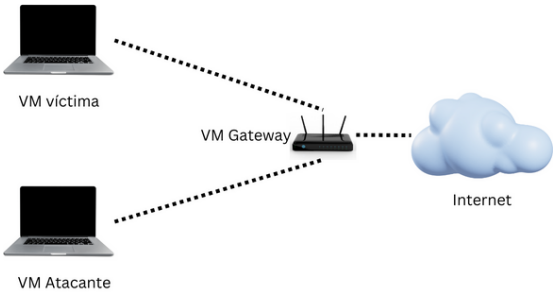
Un ataque al protocolo consiste en no seguir las reglas definidas de cómo debe funcionar, por ejemplo, enviar paquetes en desorden, o no responder a los paquetes. En este ejercicio se realizará un ataque “man in the middle” (MITM) con un envenenamiento de las tablas utilizadas por el protocolo ARP.

Se deberán utilizar dos máquinas virtuales levantadas en el mismo anfitrión, una de las cuales será la víctima (cualquier SO), y la otra será el atacante (cualquier distribución Linux, se recomienda Kali Linux). **NO es permitido realizar el procedimiento entre dos máquinas físicas en la red de la UVG**. Deben ser dos máquinas virtuales dentro del mismo anfitrión.

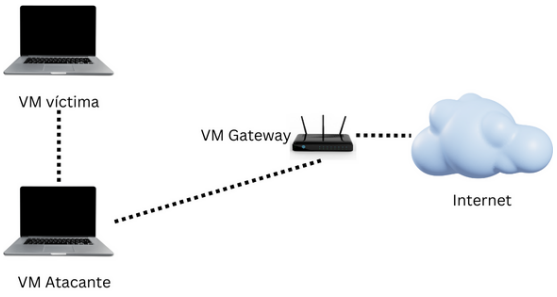
Sin modificar ningún dato de la red, ambas máquinas deberían pertenecer a la misma red, y tener la misma dirección IP para el gateway. Ejecute un comando *ipconfig/ifconfig* para obtener estos datos de ambas VMs. Verifique que puede acceder a Internet desde ambas VMs. A continuación ejecute el comando *arp -a* en ambas máquinas y muestre screenshots con la información del gateway, ponga atención a la tupla IP-MAC. Ejemplo de la máquina víctima:

```
┌──(jyass㉿kalitarget)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.64.6  netmask 255.255.255.0  broadcast 192.168.64.255
        inet6 fd31:5129:bb01:497c:1081:e3ff:fe9f:563d  prefixlen 64  scopeid
0×0<global>
        inet6 fe80::1081:e3ff:fe9f:563d  prefixlen 64  scopeid 0×20<link>
        inet6 fd31:5129:bb01:497c:8aa0:29b9:d54a:a9d6  prefixlen 64  scopeid
0×0<global>
        ether 12:81:e3:9f:56:3d  txqueuelen 1000  (Ethernet)
        RX packets 238  bytes 23922 (23.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 149  bytes 17672 (17.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(jyass㉿kalitarget)-[~]
└─$ arp -a
? (192.168.64.1) at 0e:e4:41:1f:84:64 [ether] on eth0
```

La siguiente imagen muestra la arquitectura de red actual:



Un ataque de hombre en el medio consiste en interceptar los mensajes de la máquina víctima, haciéndole creer que el atacante es el Gateway, y reenviar los mensajes al Gateway desde el atacante, haciéndose pasar por la víctima, de esta forma la víctima no nota nada extraño:

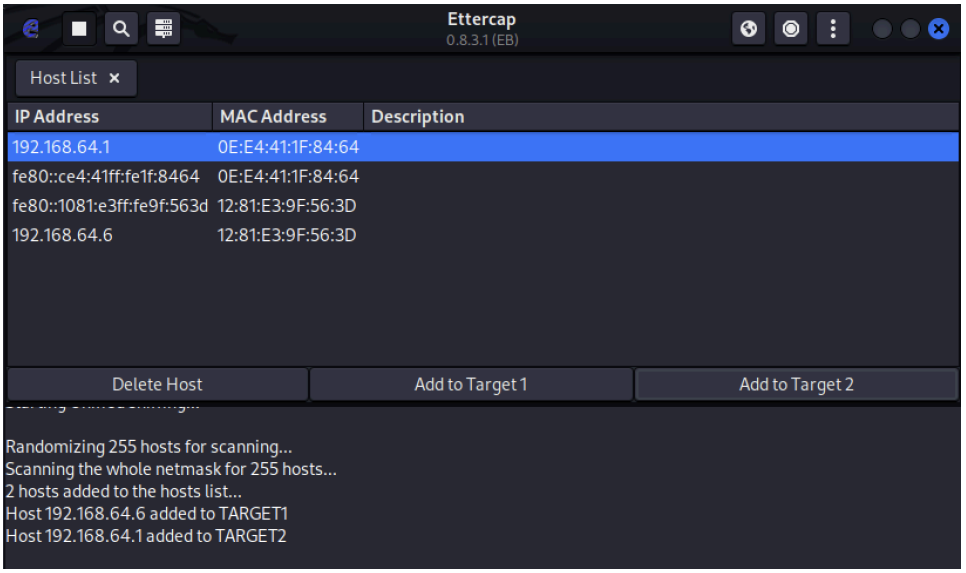


Para poder reenviar los mensajes al Gateway, la máquina atacante necesita reenviar paquetes. Para ello ejecute el siguiente comando: sysctl net.ipv4.ip_forward=1

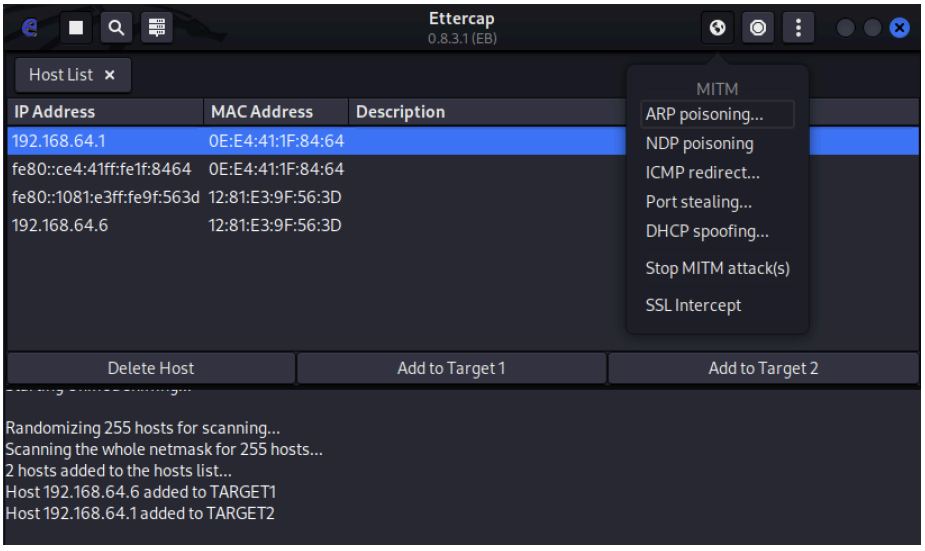
A continuación en la máquina atacante ejecute la aplicación Ettercap-graphical (si no utiliza Kali deberá instalar la aplicación manualmente). Ejecute la aplicación con la configuración por defecto haciendo clic en el botón del chequecito en la parte superior derecha de la interfaz (las UIs pueden variar dependiendo del sistema operativo):

Luego que la aplicación inicie, haga clic en el botón de la lupa para iniciar el escaneo de los hosts de la red. Deberá obtener un mensaje indicando que se encontraron dos host (el número puede cambiar si tiene más VMs activas):

A continuación haga clic en el botón Host Lists (a la par del botón de la lupa), deberá ver la información de ambos hosts. Seleccione la IP de la máquina víctima y haga clic en el botón "Add to Target 1". En este ejemplo, la máquina victima es la IP 192.168.64.6. Deberá ver un mensaje indicando que la IP fue agregada a Target 1. Realice el mismo procedimiento con la IP del Gateway, en este ejemplo, 192.168.64.1 para Target 2:



Ahora, en la máquina atacante ejecute Wireshark en la interfaz de red Eth0 (o la correspondiente) e inicie la captura de paquetes. Regrese a Ettercap y haga clic en el botón MITM menú y seleccione la opción ARP poisoning. Haga clic en OK en el cuadro de diálogo:



Detenga la captura de paquetes en Wireshark. Responda las siguientes preguntas:

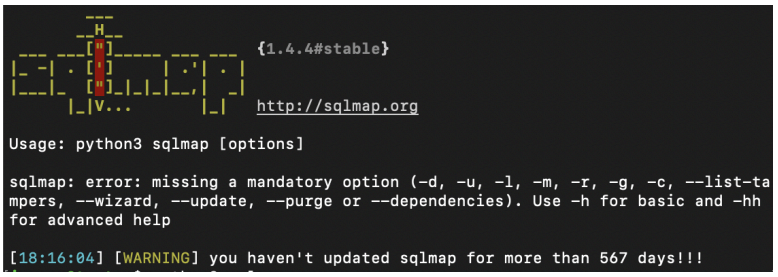
a. En la máquina víctima, ejecute nuevamente el comando arp -a ¿Qué ve de diferente sobre los resultados de la primera vez?
b. Analice las primeras dos comunicaciones que utilizaron el protocolo ARP. ¿Qué sucedió? ¿Cuáles son las reglas del protocolo ARP? ¿Por qué este ataque se considera un ataque al protocolo? Tome un screenshot de Wireshark que muestra la evidencia de los paquetes ARP enviados y la información contenida.
c. Inicie nuevamente la captura de paquetes en Wireshark. En la máquina víctima, ejecute el comando *curl* *www.google.com*. Revise los paquetes capturados en la máquina atacante. ¿Qué está sucediendo? Tome un screenshot que evidencie el tráfico capturado desde la máquina víctima.
d. ¿Cómo se podría evitar el ataque MITM con envenenamiento ARP?

2.3.2 Ataques a la aplicación

Los ataques a la aplicación son uno de los ataques más comunes en la taxonomía de los ataques a la red. Un diseño o una implementación deficiente convierte en vulnerables a las aplicaciones. Una vulnerabilidad muy conocida en los sistemas Web es la inyección SQL. Actualmente se encuentra en el tercer lugar en el OWASP Top Ten.

Para este ejercicio utilizaremos como objetivo de un ataque de inyección SQL el siguiente sitio Web: http://testphp.vulnweb.com/. Este sitio es mantenido por Acunetix, una organización que se enfoca en el desarrollo de herramientas para el escaneo de vulnerabilidades, y el propósito de este sitio es ser blanco de pruebas de seguridad. Por ética nunca debemos atacar sistemas a menos que contemos con la aprobación explícita del dueño del sistema como en este caso. Levante el sitio en su navegador web, pero no interactúe con el por ahora.

Descargue e instale la herramienta SQLMAP. Pruebe que esté instalada correctamente ingresando el comando “sqlmap”:



Ejecute el comando *sqlmap -h*, esto mostrará la categoría “Enumeration”. Aquí se describen las opciones que puede usar para recolectar información de la base de datos.

```
Enumeration:
  These options can be used to enumerate the back-end database
  management system information, structure and data contained in the
  tables

  -a, --all           Retrieve everything
  -b, --banner        Retrieve DBMS banner
  --current-user      Retrieve DBMS current user
  --current-db        Retrieve DBMS current database
  --passwords         Enumerate DBMS users password hashes
  --tables            Enumerate DBMS database tables
  --columns           Enumerate DBMS database table columns
  --schema            Enumerate DBMS schema
  --dump              Dump DBMS database table entries
  --dump-all          Dump all DBMS databases tables entries
  -D DB               DBMS database to enumerate
  -T TBL              DBMS database table(s) to enumerate
  -C COL              DBMS database table column(s) to enumerate
```

A continuación, ejecute el comando *sqlmap – u* [URL sitio Web] (dependiendo del sistema operativo, deberá incluir la URL entre comillas). Explore el sitio (se sugiere Inspeccionar Elemento como apoyo) y luego responda las siguientes preguntas:

- ¿Qué tipo de DBMS utiliza este sitio? (tip: ver las opciones que les dice -h)
- ¿Qué versión tiene el DBMS?
- Evidencie con capturas

Ejecute el comando *sqlmap – u [URL sitio Web] --dbs*

- ¿Cuáles son los nombres de las bases de datos? No olvide evidenciar lo encontrado.

Con la información del comando -h, prepare una instrucción para obtener las tablas de cada una de las bases de datos identificadas. Liste las tablas. Finalmente, seleccione algunas tablas y prepare un comando para obtener más información sobre ellas, muestre los resultados obtenidos.

3 Evaluación

Fecha de entrega: Domingo 27/10/2024 a las 11:59 p.m.
Entregable: Documento PDF con sus respuestas y capturas evidenciando su procedimiento y hallazgos, así como todo código implementado.

Rúbrica

- Conceptos de seguridad de la información: (12.5%)
- One Time Pad: (12.5%)
- Modos de operación para bloques de cifrado: (25%)
- Ataque al protocolo: (37.5%)
- Ataque a la aplicación: (12.5%)