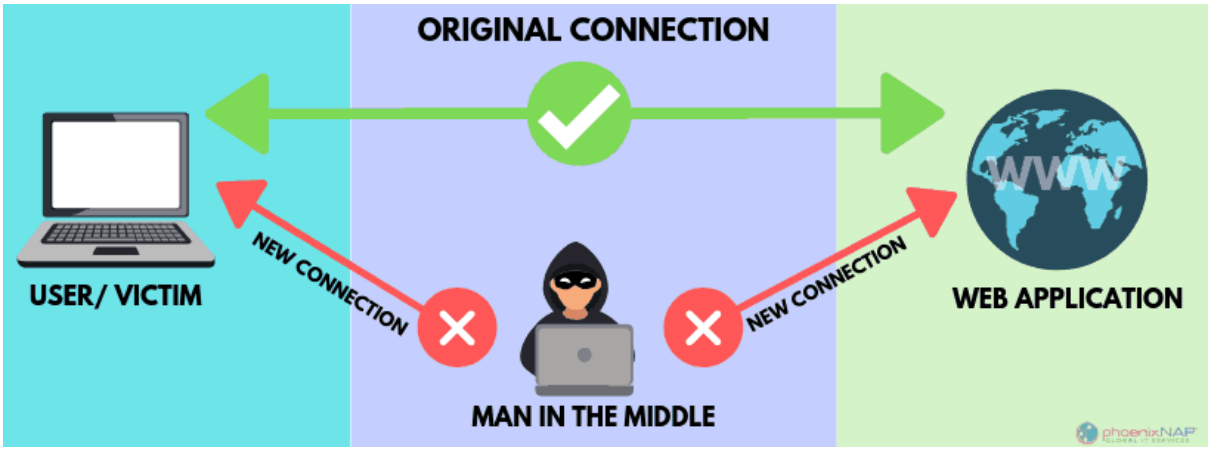
Universidad de Alcalá

Seguridad

Tema: Práctica 3 - Ataques de Hombre en el Medio en Redes de Área Local



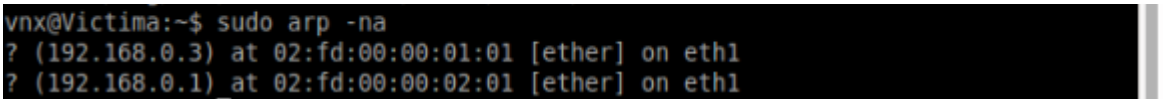
Participantes
Carlos Javier Hellín Asensio (carlos.hellin@edu.uah.es)
Darius Dumitras Tamas (darius.tamas@edu.uah.es)

Grado de Ingeniería Informática
Curso: 2021-2022

1.

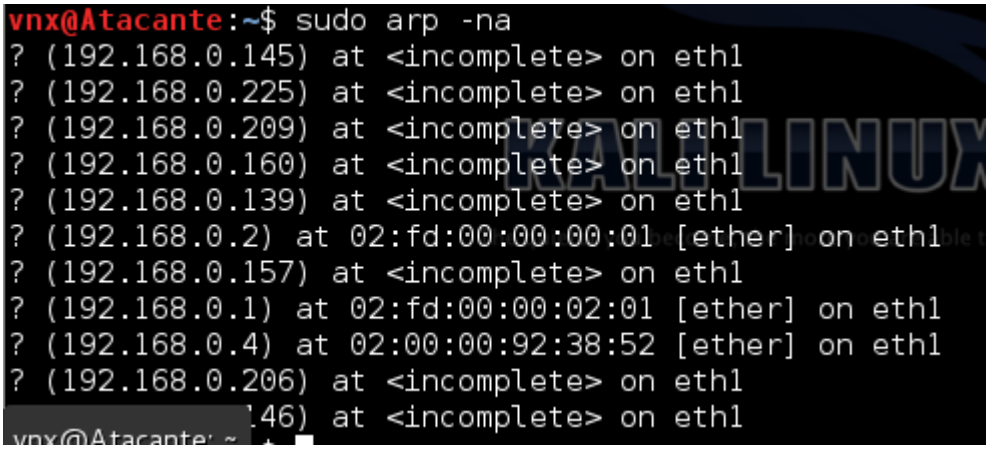
192.168.0.2 es la VÍCTIMA y 192.168.0.3 es el ATACANTE, este último es donde estamos conectados. Ambos no tienen puertos abiertos.

2.



Nos muestra la tabla ARP, donde 192.168.0.3 ATACANTE tiene una MAC (02:fd:00:00:01:01) y 192.168.0.1 es el ROUTER con otra MAC (02:fd:00:00:02:01). Ambos están conectados a eth1.

3.



```
vnx@Atacante:~$ sudo arp -na
? (192.168.0.145) at <incomplete> on eth1
? (192.168.0.225) at <incomplete> on eth1
? (192.168.0.209) at <incomplete> on eth1
? (192.168.0.160) at <incomplete> on eth1
? (192.168.0.139) at <incomplete> on eth1
? (192.168.0.2) at 02:fd:00:00:00:01 [ether] on eth1
? (192.168.0.157) at <incomplete> on eth1
? (192.168.0.1) at 02:fd:00:00:02:01 [ether] on eth1
? (192.168.0.4) at 02:00:00:92:38:52 [ether] on eth1
? (192.168.0.206) at <incomplete> on eth1
                  146) at <incomplete> on eth1
vnx@Atacante: ~
```

Se muestran más IPs seguramente debido a la caché del ARP, pero las más importantes para esta práctica son: la VÍCTIMA con IP 192.168.0.2 y MAC 02:fd:00:00:00:01, además del Router con IP 192.168.0.1 y MAC 02:fd:00:00:02:01. Ambos también conectados a eth1.

4.

```
vnx@Atacante:~$ sudo arpspoof -t 192.168.0.1 192.168.0.2
[sudo] password for vnx:
2:fd:0:0:1:1 2:fd:0:0:2:1 0806 42: arp reply 192.168.0.2 is-at 2:fd:0:0:1:1
2:fd:0:0:1:1 2:fd:0:0:2:1 0806 42: arp reply 192.168.0.2 is-at 2:fd:0:0:1:1
2:fd:0:0:1:1 2:fd:0:0:2:1 0806 42: arp reply 192.168.0.2 is-at 2:fd:0:0:1:1
2:fd:0:0:1:1 2:fd:0:0:2:1 0806 42: arp reply 192.168.0.2 is-at 2:fd:0:0:1:1
2:fd:0:0:1:1 2:fd:0:0:2:1 0806 42: arp reply 192.168.0.2 is-at 2:fd:0:0:1:1
```

```
vnx@Atacante:~$ sudo arpspoof -t 192.168.0.2 192.168.0.1
2:fd:0:0:1:1 2:fd:0:0:0:1 0806 42: arp reply 192.168.0.1 is-at 2:fd:0:0:1:1
2:fd:0:0:1:1 2:fd:0:0:0:1 0806 42: arp reply 192.168.0.1 is-at 2:fd:0:0:1:1
2:fd:0:0:1:1 2:fd:0:0:0:1 0806 42: arp reply 192.168.0.1 is-at 2:fd:0:0:1:1
2:fd:0:0:1:1 2:fd:0:0:0:1 0806 42: arp reply 192.168.0.1 is-at 2:fd:0:0:1:1
```

Lo que está sucediendo es el envenenamiento de ARP. Ahora el ATACANTE envía mensajes ARP Reply a los nodos, cuya respuesta a la MAC de la IP de la VÍCTIMA 192.168.0.2 es la MAC del ATACANTE (02:fd:00:00:01:01) y la MAC de la IP del ROUTER 192.168.0.1 es también la MAC del ATACANTE (02:fd:00:00:01:01).

Cuando se ejecuta el arpspoof, se muestra continuamente los mensajes de ARP Reply que el ATACANTE está sobrecargando a las tablas ARP. Es necesario mantener estos terminales abiertos con el arpspoof, ya que las tablas ARP son volátiles y sus entradas son eliminadas pasados unos minutos, por lo que podría volver a tener un tráfico normal sin que el ATACANTE intervenga.

5.1.

```
vnx@Victima:~$ sudo arp -na
[sudo] password for vnx:
? (192.168.0.3) at 02:fd:00:00:01:01 [ether] on eth1
? (192.168.0.1) at 02:fd:00:00:01:01 [ether] on eth1
```

5.2.

```
vnx@Router:~$ sudo arp -na
[sudo] password for vnx:
? (10.0.12.212) at <incomplete> on eth2
? (10.0.12.214) at <incomplete> on eth2
? (10.0.12.210) at 02:fd:00:00:02:02 [ether] on eth2
? (10.0.12.211) at 02:fd:00:00:02:02 [ether] on eth2
? (10.0.12.208) at 02:fd:00:00:02:02 [ether] on eth2
? (10.0.12.207) at 02:fd:00:00:02:02 [ether] on eth2
? (192.168.0.3) at 02:fd:00:00:01:01 [ether] on eth1
? (10.0.12.205) at 02:fd:00:00:02:02 [ether] on eth2
? (10.0.12.204) at 02:fd:00:00:02:02 [ether] on eth2
? (10.0.12.202) at 02:fd:00:00:02:02 [ether] on eth2
? (10.0.12.201) at 02:fd:00:00:02:02 [ether] on eth2
? (192.168.0.2) at 02:fd:00:00:01:01 [ether] on eth1
? (10.0.8.1) at dc:9f:db:28:bc:59 [ether] on eth2
```

6.

Los valores de las tablas ARP de la VÍCTIMA y del ROUTER han cambiado a lo visto anteriormente, esto está sucediendo debido a que el ATACANTE está produciendo el envenenamiento de ARP. Se puede observar en las tablas del ROUTER que la MAC (02:fd:00:00:01:01) de la VÍCTIMA (192.168.0.2) es la misma que la del ATACANTE (192.168.0.3). En el caso de las tablas de la VÍCTIMA el ROUTER (192.168.0.1) también tiene la MAC del ATACANTE (192.168.0.3) que es 02:fd:00:00:01:01.

7.

Lo que sucede es que se intenta conectar a google.es, pero no lo consigue a pesar de tener configurado las DNS (192.168.153.140) en el resolv.conf. Le está enviando las peticiones de consulta de DNS al ATACANTE debido al envenenamiento de ARP, porque la MAC del ROUTER ahora es la del ATACANTE, es decir, el ATACANTE está en el medio de la comunicación entre el ROUTER y la VÍCTIMA. Ahora mismo el ATACANTE no realiza nada con esos u otros paquetes (por ejemplo, no reenvía los paquetes al ROUTER) que recibe de la VÍCTIMA, por eso no se puede conectar a google.es por parte de la VÍCTIMA.

8.

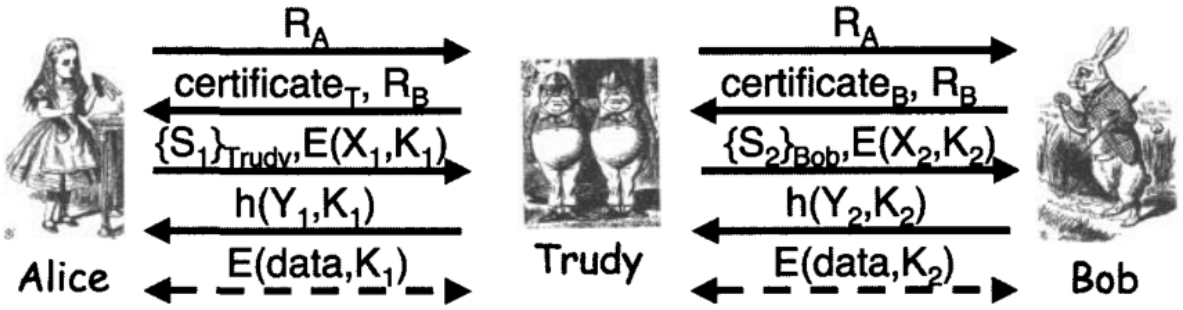
Ahora que el ATACANTE puede reenviar los paquetes que recibe al ROUTER, cuando la VÍCTIMA intenta entrar a google.es las petición DNS funciona y posteriormente también puede realizar peticiones HTTP a la IP de Google. Por ello, el motivo de por qué es necesario habilitar el reenvío de paquetes, es para que el ATACANTE pueda reenviar las peticiones necesarias (DNS, HTTP, etc..) de la VÍCTIMA a los servidores (el de DNS es 192.168.153.140, la IP de Google para HTTP, etc..) pasando por el ROUTER.

9.

El ATACANTE ahora mismo lo único que está haciendo es reenviar el tráfico al ROUTER analizando los datos con Wireshark y no modifica los datos, es decir, no interviene en la comunicación. Por lo tanto, se trata de un ataque pasivo. Con este ataque lo que se puede conseguir es visualizar, si se ha envíado en texto plano, posible información confidencial (ya sea un usuario y contraseña, por ejemplo).

10.

No se puede capturar las credenciales, porque la conexión a Blackboard se realiza con HTTPS, por lo tanto los datos van a ir cifrados. La sesión que se establece entre la VÍCTIMA y Blackboard se hace mediante el protocolo SSL, y esto evita el ataque del hombre en el medio. Además de que los datos van cifrados, se utilizan certificados con criptografía tanto asimétrica como simétrica. En el caso de que quisiéramos que el ATACANTE enviase un certificado falso a la VÍCTIMA, el navegador le avisará a la VÍCTIMA de que se ha detectado un problema con el certificado, y queda a elección de él si quiere continuar y permitir esa conexión.



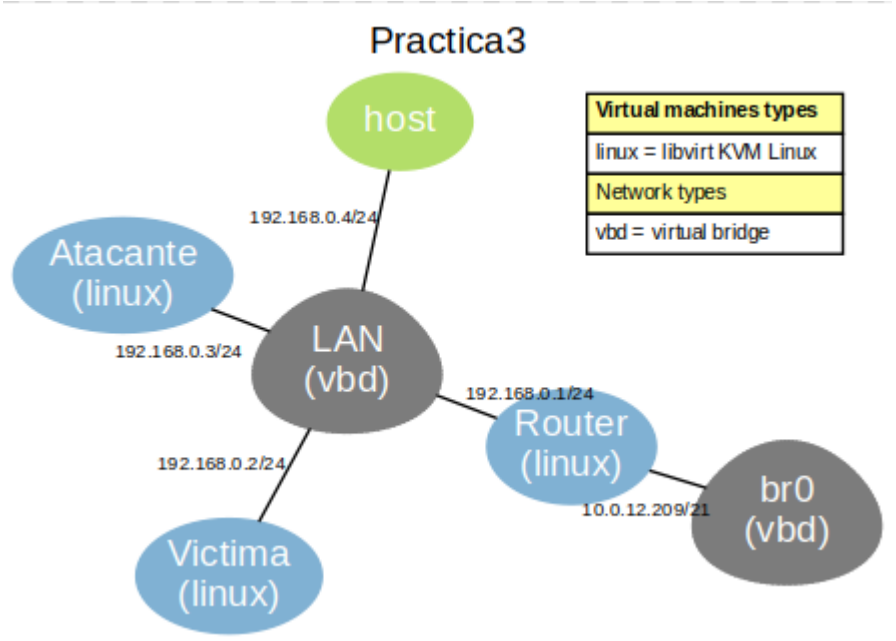
11.

El protocolo HTTP en sí no ofrece confidencialidad de datos, ya que en un principio se elaboró pensando en la comunicación, no en la seguridad. Para obtener esa confidencialidad de datos es necesario usar el protocolo SSL que se ejecuta en una capa entre los protocolos de aplicación (HTTP, SMTP, etc..) y el protocolo de transporte (TCP, UDP, etc..). Si se intenta con un formulario en HTTP, se puede ver que podemos obtener los datos en texto plano de lo que se ha envíado:

ANEXO.

Con driftnet arrancado, acceda desde el navegador del equipo VÍCTIMA a una web que contenga imágenes y fíjese en la ventana en el equipo atacante de driftnet. ¿Qué está sucediendo?
Lo que está sucediendo es que la VÍCTIMA al conectar a una página desde el protocolo HTTP, se puede ver que las imágenes de la web que se están descargando, también se pueden ver en el ATACANTE con la herramienta driftnet debido al ataque del hombre en el medio.

La red VNX de esta práctica 3 es la siguiente:



Bibliografía

Information Security: Principles and Practice (2ª Ed.) M. Stamp Wiley, 2011