

PRACTICA 4

Pregunta 1

Indique el resultado de ejecutar este script que aparece en pantalla y explique que está mostrando.

El script lo que esta haciendo básicamente es la misma función que hacia el sudo arp -na. Nos muestra cuantos dispositivos hay conectados a la red.

```
root@Atacante:~/p4# python arpping.py
WARNING: No route found for IPv6 destination :: (no default route?)
02:fd:00:00:02:01, en la IP 192.168.0.1
02:fd:00:00:00:01, en la IP 192.168.0.2
02:00:00:9f:25:0f, en la IP 192.168.0.4
root@Atacante:~/p4#
```

Pregunta 2

Escriba la tabla de ARP de ambos equipos.¿Qué observa?¿Es correcta? ¿Por qué?

```
vnx@Victima:~$ sudo arp -na
? (192.168.0.3) at 02:fd:00:00:01:01 [ether] on eth1
? (192.168.0.4) at 02:00:00:9f:25:0f [ether] on eth1
? (192.168.0.1) at 02:fd:00:00:02:01 [ether] on eth1
vnx@Victima:~$
```

Se puede observar que muestran todos los equipos de la red con los que ha habido contacto menos a si mismos.

Pregunta 3

Para completar y modificar el anterior script, escriba los valores de:

IP Victima: 192.168.0.2

IP Router: 192.168.0.1

MAC Victima: 02:fd:00:00:00:01

MAC Atacante: 02:fd:00:00:01:01

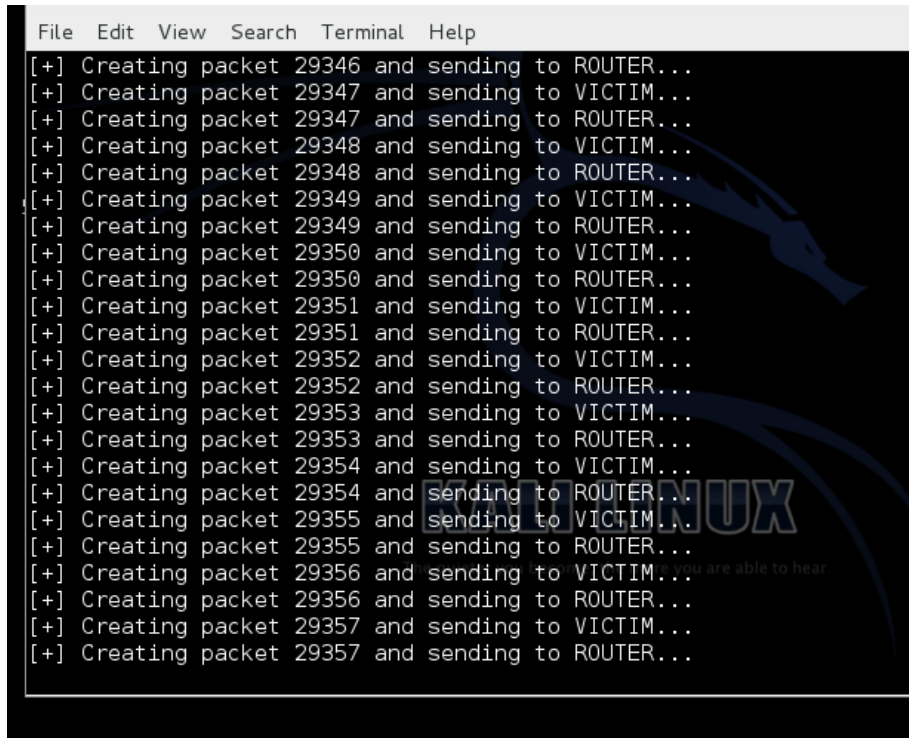
Pregunta 4

Explique lo que está sucediendo, comprobando en el equipo VÍCTIMA y en el ROUTER que se está produciendo el envenenamiento de ARP.

Es un bucle infinito que envia paquetes ARP tipo reply falsos a la victima y al router, haciendo creer a ambos que somos el destinatario de todos los datos.

```
[sudo] password for vnx:
? (192.168.0.3) at 02:fd:00:00:01:01 [ether] on eth1
? (192.168.0.4) at 02:00:00:9f:25:0f [ether] on eth1
? (192.168.0.1) at 02:fd:00:00:01:01 [ether] on eth1
vnx@Victima:~$
```

Se ha producido correctamente el envenenamiento.



```
File Edit View Search Terminal Help
[+] Creating packet 29346 and sending to ROUTER...
[+] Creating packet 29347 and sending to VICTIM...
[+] Creating packet 29347 and sending to ROUTER...
[+] Creating packet 29348 and sending to VICTIM...
[+] Creating packet 29348 and sending to ROUTER...
[+] Creating packet 29349 and sending to VICTIM...
[+] Creating packet 29349 and sending to ROUTER...
[+] Creating packet 29350 and sending to VICTIM...
[+] Creating packet 29350 and sending to ROUTER...
[+] Creating packet 29351 and sending to VICTIM...
[+] Creating packet 29351 and sending to ROUTER...
[+] Creating packet 29352 and sending to VICTIM...
[+] Creating packet 29352 and sending to ROUTER...
[+] Creating packet 29353 and sending to VICTIM...
[+] Creating packet 29353 and sending to ROUTER...
[+] Creating packet 29354 and sending to VICTIM...
[+] Creating packet 29354 and sending to ROUTER...
[+] Creating packet 29355 and sending to VICTIM...
[+] Creating packet 29355 and sending to ROUTER...
[+] Creating packet 29356 and sending to VICTIM...
[+] Creating packet 29356 and sending to ROUTER...
[+] Creating packet 29357 and sending to VICTIM...
[+] Creating packet 29357 and sending to ROUTER...
```

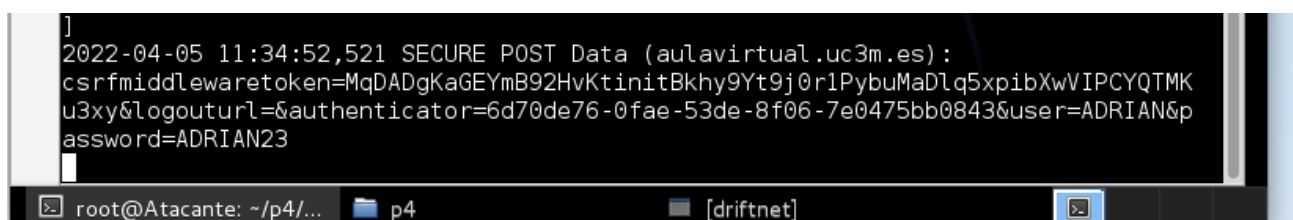
Pregunta 5

¿Qué esta sucediendo? ¿Qué sucede con las peticiones HTTPS?

Se captura la solicitud de la victima capturando asi las credenciales, solo en el caso de que se accede mediante http. En caso de acceder mediante https se convertira a http en caso posible. En el caso de solo poder acceder mediante https, este metodo no funcionara.

Pregunta 6

Indique si desde la máquina ATACANTE puede capturar las credenciales de acceso (usuario y contraseña) que ha introducido para acceder a ‘Aula Virtual’.



```
]
2022-04-05 11:34:52,521 SECURE POST Data (aulavirtual.uc3m.es):
csrfmiddlewaretoken=MqDADgKaGEYmB92HvKtinitBkhy9Yt9j0r1PybuMaDlq5xpibXwVIPCYQTMK
u3xy&logouturl=&authenticator=6d70de76-0fae-53de-8f06-7e0475bb0843&user=ADRIAN&p
assword=ADRIAN23
```

Usuario: ADRIAN

Contraseña: ADRIAN23

Pregunta 7

Indique las páginas que ha probado y cuál ha sido el funcionamiento del proceso en la captura de credenciales:

El aula virtual de uc3m y la de la universidad de Alcalá.

Cuando introduces la dirección https, se convierte a http y hace así posible la captura de credenciales.

Pregunta 8

¿Ha encontrado alguna web que sólo permita acceder obligatoriamente por HTTPS? ¿Qué solución plantea ante este problema? ¿Qué es HSTS? ¿Solventa el problema?

Si, youtube. En el momento que una pagina web tiene hsts se hace inmune frente al SSL Strip.

El hsts o Http Strict transport Security, sirve para evitar ataques de degradacion de protocolo, es decir que le dice al navegador que se conecte unicamente al sitio web mediante https. Evitando asi que puedan conectarse de alguna manera mediante http.